CHUO MATH NO.129(2019)

GEOMETRIC ASPECTS OF CULLEN-BALLOT SEQUENCES

by
NORIYUKI SUWA

DEPARTMENT OF MATHEMATICS
CHUO UNIVERSITY
BUNKYOKU TOKYO JAPAN

NOV. 22 , 2019

GEOMETRIC ASPECTS OF CULLEN-BALLOT SEQUENCES

NORIYUKI SUWA*)

Abstract. In this article, we study the divisibility problem for Lucas sequences of higher orders in the framework of group scheme theory, following the lead of works achieved by Ward and Ballot. In particuler, we treat Cullen-Ballot sequences, which Ballot defines as a generalization of the Cullen sequences.

Introduction

The Cullen sequence $(C_k)_{k\geq 0}$ is defined by $C_k = k2^k + 1$. It is easily verified that $(C_k)_{k\geq 0}$ is a linear recurrence sequence with the characteristic polynomial $(t-1)(t-2)^2$. Here is a remarkable divisibilty property of the Cullen sequence: for any odd prime p, we have congruence relations

$$C_{p-2} \equiv 0 \mod p,\ C_{p-1} \equiv 0 \mod p,\ C_p \equiv 1 \mod p.$$

This means that all the odd prime numbers are maximal divisors of the linear recurrence sequence $(C_k)_{k\geq 0}$ of third order in terms of Ward [12]. (We recall a definiton in 2.8.)

Ballot deepened in [1] an argument on the divisivility problem for Lucas sequences in higher orders studied first by Ward [12], and then he generalized in [2] the Cullen sequence, invoking Laxton groups defined by Laxton [6] and clarifying the mechanism lying behind divisibility properties.

Recently the author reformulated Laxton groups in the framework of affine group scheme theory in [8], [9] and [10]. In this article we study the divisibility problem from a geometric viewpoint for Lucas sequences in higher orders, particularly for Cullen-Ballot sequences, translating several descriptions on linear recurrence sequences into the language of affine group schemes. The main result is given as follows:

Theorem(=Theorem 3.8) *Let $\alpha \in \mathbb{Z}$ and $Q(t) = t^m - \beta_1 t^{m-1} - \cdots - \beta_{m-1}t - \beta_m \in \mathbb{Z}[t]$, and put $P(t) = (t-\alpha)^2 Q(t)$ and $P(t) = (t-\alpha)Q(t)$. Let D denote the discriminant of $P_1(t)$, and let p be a prime with $(p, \alpha\beta_m D) = 1$. Then we have $\Theta \supset \mathrm{Ker}[\pi : G_{(P)}(\mathbb{Z}/p\mathbb{Z}) \to G_{(P_1)}(\mathbb{Z}/p\mathbb{Z})]$ in $G_{(P)}(\mathbb{Z}/p\mathbb{Z})$.*

(The affine group schemes $G_{(P)}$ and $G_{(P_1)}$ are defined in Definition 2.1. The subgroup Θ of $G_{(D)}(\mathbb{Z}/p\mathbb{Z})$ is defined in Notation 3.7.) This is a geometirc expression of main results in Ballot [2], that is to say, Theorem 8 and Theorem 18.

*) Partially supported by Grant-in-Aid for Scientific Research No.19K03408

2005 *Mathematics Subject Classification* Primary 13B05; Secondary 14L15, 12G05.

Now we explain the organization of the article. The Section 1 is a summary on Lucas sequences, which is based on algebras of linear recurrence sequences. The formulation ascends to Ward [11] and Hall [4]. In Example 1.4, we remark a relation between the Lagrange interpolation formula and the Binet formula for linear recurrence sequences. The subsections after Notation 1.5 are prepared for Section 3.

In the first half of Section 2, introducing the affine group schemes G_P and $G_{(P)}$, we recall needed facts on reformulation of Lucas sequences mentioned in [10] in terms of the group schemes G_P and $G_{(P)}$. In the latter half of Section 2, we reformulate and generalize some results of Ward [12] on divisibility of Lucas sequences of higher orders. For example, we obtain the following:

Theorem(=Theorem 2.11) *Let* $P(t) = t^n - P_1 t^{n-1} - \cdots - P_{n-1}t - P_n \in \mathbb{Z}[t]$ *and* $\boldsymbol{w} = (w_k)_{k\geq 0} \in \mathcal{L}(P, \mathbb{Z})$*, and let* m *be an integer* ≥ 2 *with* $(m, P_n) = 1$ *and* $(m, w_0, \ldots, w_{n-1}) = 1$*. Then,* m *is a maximal divisor of* $\boldsymbol{w}$ *if and only* $[\boldsymbol{w}]$ *is in the orbit* $(0 : \ldots : 0 : 1)\Theta$ *in* $\mathbb{P}^{n-1}(\mathbb{Z}/m\mathbb{Z})$*.*

We also discuss the notion of twin divisors defined by Ballot [1, Ch.4].

In the Section 3, we paraphrase the argument developed by Ballot [2] in our context. It is a key to consider the exact sequence of group schemes

$$0 \longrightarrow \mathbb{G}_{a,\mathbb{Z}} \longrightarrow G_{(P)} \longrightarrow G_{(P_1)} \longrightarrow 0.$$

Here $\alpha \in \mathbb{Z}$ and $Q(t) = t^m - \beta_1 t^{m-1} - \cdots - \beta_{m-1}t - \beta_m \in \mathbb{Z}[t]$, and we put $P(t) = (t-\alpha)^2 Q(t)$ and $P_1(t) = (t-\alpha)Q(t)$. We conclude the article by presenting a cross-breed of the Fibonacci sequence and the Cullen sequence.

Ballot presents in [1] and [2] remarkable results on the density of primes p such that p is a maximal divisor of a fixed linear recurrence sequence, developing methods given by Lagarias [5]. It would be interesting to try a reformulation also for the density problem.

The author would like to express his hearty thanks to Masato Kurihara and Akira Masuoka for their advices and encouragement.

Notation

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

$\tilde{R} = R[t]/(P(t))$**:** defined in 1.1

$\mathcal{L}(P, R)$**:** defined in 1.1

$\mathbb{G}_{m,R}$**:** the multiplicative group scheme over R

$G_P = \prod_{\tilde{R}/R} \mathbb{G}_{m,\tilde{R}}$**:** the Weil restriction of $\mathbb{G}_{m,\tilde{R}}$ with respect to $\tilde{R}/R$, 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 2.10 and 3.7

$\Theta \subset G_{(P)}(R)$**:** defined in 2.10 and 3.7

1. Linear recurrence sequences

First we recall a formulation on algebras of linear recurrence sequences as generally as possible. For details we refer to [10, Section 3].

Notation 1.1. Let R be a ring and $P(t) = t^n - P_1 t^{n-1} - \cdots - P_{n-1}t - P_n \in R[t]$. We put

$$\mathcal{L}(P,R) = \{(w_k)_{k\geq 0} \in R^{\mathbb{N}}\ ;\ w_{k+n} = P_1 w_{k+n-1} + \cdots + P_{n-1}w_{k+1} + P_n w_k \text{ for each } k \geq 0\}.$$

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 $\mathcal{L}(P,R) \xrightarrow{\sim} R^n$.

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 $\tilde{R}$. 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 $\operatorname{Nr}\eta = \operatorname{Nr}_{\tilde{R}/R}\eta$ is given by $\operatorname{Nr}\eta = \det\rho(\eta)$. It is readily seen that η is invertible in $\tilde{R}$ if and only if $\operatorname{Nr}\eta$ is invertible in R. For example, θ is invertible in $\tilde{R}$ if and only if P_n is invertible in 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

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

The R-homomorphism $\tilde{\omega} : \tilde{R} \to R^{\mathbb{N}}$ induces an R-isomorphism $\tilde{\omega} : \tilde{R} \to \mathcal{L}(P,R)$. The inverse of $\tilde{\omega} : \tilde{R} \to \mathcal{L}(P,R)$ is given by

$$(w_0, w_1, \dots, w_{n-1}, \dots) \mapsto$$
$$w_0\theta^{n-1} + (w_1 - P_1 w_0)\theta^{n-2} + \cdots + (w_{n-1} - P_1 w_{n-2} - \cdots - P_{n-2}w_1 - P_{n-1}w_0).$$

We define an R-algebra structure of $\mathcal{L}(P,R)$ through the R-isomorphism $\tilde{\omega} : \tilde{R} \xrightarrow{\sim} \mathcal{L}(P,R)$. 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 $\omega : \tilde{R} \xrightarrow{\sim} \mathcal{L}(P,R)$.

Definition 1.2. 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 $L_{n-1} = 1$.

Remark 1.3. Let $P_1(t) = t^n - \alpha_1 t^{n-1} - \cdots - \alpha_{n-1}t - \alpha_n$, $P_2(t) = t^m - \beta_1 t^{m-1} - \cdots - \beta_{m-1}t - \beta_m \in R[t]$, and put $P(t) = P_1(t)P_2(t)$. Then we obtain a commutative diagram

$$\begin{array}{ccc} R[t]/(P(t)) & \xrightarrow{\tilde{\omega}} & \mathcal{L}(P,R) \\ {\scriptstyle \text{canonical surjection}}\big\downarrow & & \big\downarrow \\ R[t]/(P_1(t)) & \xrightarrow[\tilde{\omega}]{} & \mathcal{L}(P_1,R) \end{array}.$$

The map $\mathcal{L}(P,R) \to \mathcal{L}(P_1,R)$ is given by

$$(w_k)_{k\geq 0} \mapsto (w_{k+m} - \beta_1 w_{k+m-1} - \cdots - \beta_{m-1}w_{k+1} - \beta_m w_k)_{k\geq 0}.$$

Example 1.4. Let $\alpha_1, \alpha_2, \ldots, \alpha_n \in R$, and put $P(t) = (t-\alpha_1)(t-\alpha_2)\cdots(t-\alpha_n)$. Assume that $\alpha_1, \alpha_2, \ldots, \alpha_n$ are distinct to each other. Then

$$\theta \mapsto (\alpha_1, \alpha_2, \ldots, \alpha_n)$$

gives rise to an injective homomorphism of R-algebras

$$\xi : R[t]/(P(t)) \to R^n.$$

Furthermore, assume that the discriminant of $P(t)$ is invertible in R. Then ξ is bijective. Indeed, put

$$e_i(t) = \frac{1}{P'(\alpha_i)}\frac{P(t)}{t-\alpha_i} \in R[t]$$

for $1 \leq i \leq n$. Then we have

$$\tilde{\omega} : e_i(\theta) \mapsto \Big(\frac{\alpha_i^k}{P'(\alpha_i)}\Big)_{k\geq 0}$$

Moreover,

$$(A_1, A_2, \ldots, A_n) \mapsto \sum_{i=1}^n A_i e_i(\theta)$$

gives the inverse of $\xi : R[t]/(P(t)) \to R^n$.

We have gotten also

$$\tilde{\omega}\circ\xi^{-1} : (A_1, A_2, \ldots, A_n) \mapsto \Big(\sum_{i=1}^n \frac{A_i}{P'(\alpha_i)}\alpha_i^k\Big)_{k\geq 0}$$

Put $\eta = \sum_{i=1}^n A_i e_i(\theta)$ and $\boldsymbol{w} = \tilde{\omega}(\eta)$. Then we have

$$\operatorname{Nr}\eta = (-1)^{n(n-1)/2}\Delta(\boldsymbol{w}) = A_1 A_2 \cdots A_n.$$

Hereafter we arrange several notations needed in Section 3.

Notation 1.5. Let ε denote the image of t in the residue ring $R[t]/(t^2)$. Then we have $R[t]/(t^2) = R[\varepsilon] = \{a + b\varepsilon \ ; \ a, b \in R\}$. The element ε is traditionally called the dual number.

Example 1.6. Let $\alpha \in R$ and $Q(t) = t^m - \beta_1 t^{m-1} - \cdots - \beta_{m-1}t - \beta_m \in R[t]$, and put $P(t) = (t-\alpha)^2 Q(t)$ and $P(t) = (t-\alpha)Q(t)$. Then we have a commutative diagram of R-algebras

$$\begin{array}{ccc} R[t]/(P(t)) & \xrightarrow{\tilde{\omega}} & \mathcal{L}(P,R) \\ {\scriptstyle \text{reduction map}}\downarrow & & \downarrow \\ R[t]/(P_1(t)) & \xrightarrow[\tilde{\omega}]{} & \mathcal{L}(P_1,R) \end{array}.$$

The map $\mathcal{L}(P,R) \to \mathcal{L}(P_1,R)$ is given by $(w_k)_{k\geq 0} \mapsto (w_{k+1} - \alpha w_k)_{k\geq 0}$.

Now let θ, θ_1 and θ_Q denote the image of t in the residue rings $R[t]/(P(t))$, $R[t]/(P_1(t))$ and $R[t]/(Q(t))$, respectively, and put $\tilde{R}_Q = R[t]/(Q(t))$. Moreover, let D denote the discriminant of $P_1(t)$, and assume $D \neq 0$. Then

$$\theta \mapsto (\alpha + \varepsilon, \theta_Q)$$

gives rise to an injective homomorphism of R-algebras

$$\xi : R[t]/(P(t)) \to R[\varepsilon] \times \tilde{R}_Q,$$

and

$$\theta \mapsto (\alpha, \theta_Q)$$

gives rise to an injective homomorphism of R-algebras

$$\xi_1 : R[t]/(P_1(t)) \to R \times \tilde{R}_Q.$$

Furthermore, we obtain a commutative diagram of R-algebras

$$\begin{array}{ccc} R[t]/(P(t)) & \xrightarrow{\xi} & R[\varepsilon] \times \tilde{R}_Q \\ {\scriptstyle \text{reduction map}}\downarrow & & \downarrow \\ R[t]/(P_1(t)) & \xrightarrow[\xi_1]{} & R \times \tilde{R}_Q \end{array}.$$

If D is invertible in R, then ξ and ξ_1 are bijective.

Remark 1.7. We can describe $\xi : R[t]/(P(t)) \to R[\varepsilon] \times \tilde{R}_Q$ and $\xi_1 : R[t]/(P(t)) \to R \times \tilde{R}_Q$ more precisely when $Q(t)$ splits completely in $R[t]$.

Let $\alpha, \beta_1, \ldots, \beta_m \in R$, and put

$$P(t) = (t-\alpha)^2(t-\beta_1)\cdots(t-\beta_m),\ P_1(t) = (t-\alpha)(t-\beta_1)\cdots(t-\beta_m).$$

Let D denote the discriminant of $P_1(t)$, and assume that $D \neq 0$. Then

$$\theta \mapsto (\alpha + \varepsilon, \beta_1, \ldots, \beta_m)$$

gives rise to an injective homomorphism of R-algebras

$$\xi : R[t]/(P(t)) \to R[\varepsilon] \times R^m,$$

and

$$\theta \mapsto (\alpha, \beta_1, \ldots, \beta_m)$$

gives rise to an injective homomorphism of R-algebras

$$\xi : R[t]/(P_1(t)) \to R^{m+1}.$$

Furthermore, we obtain a commutative diagram of rings

$$\begin{array}{ccc} R[t]/(P(t)) & \xrightarrow{\xi} & R[\varepsilon] \times R^m \\ {\scriptstyle \text{reduction map}}\downarrow & & \downarrow \\ R[t]/(P_1(t)) & \xrightarrow{\xi_1} & R^{m+1} \end{array}.$$

If D is invertible in R, then ξ and ξ_1 are is bijective. Indeed, put

$$e_i(t) = \frac{1}{P'(\beta_i)} \frac{P(t)}{t-\beta_i} \in R[t]$$

for $1 \leq i \leq m$, and

$$e(t) = 1 - \sum_{i=1}^{m} e_i(t),\ \varepsilon(t) = \frac{1}{P'(\alpha)} \frac{P_1(t)}{t-\alpha} = \frac{1}{(\alpha-\beta_1)\cdots(\alpha-\beta_m)}(t-\beta_1)\cdots(t-\beta_m).$$

Then

$$(A_1 + A_2\varepsilon, B_1, \dots, B_m) \mapsto A_1 e(\theta) + A_2\varepsilon(\theta) + \sum_{i=1}^{m} B_i e_i(\theta)$$

gives the inverse of $\xi : R[t]/(P(t)) \to R[\varepsilon] \times R^m$.

Moreover, we have

$$\begin{aligned} &\tilde{\omega} : e_i(\theta) \mapsto \Big(\frac{\beta_i^k}{P'(\beta_i)}\Big)_{k\geq 0}, \\ &\tilde{\omega} : e(\theta) \mapsto \Big(\frac{1}{P_1'(\alpha)} k\alpha^{k-1} - \Big\{\sum_{i=1}^{m} \frac{1}{P'(\beta_i)}\Big\}\alpha^k\Big)_{k\geq 0}, \\ &\tilde{\omega} : \varepsilon(\theta) \mapsto \Big(\frac{\alpha^k}{P_1'(\alpha)}\Big)_{k\geq 0}. \end{aligned}$$

The Lucas sequence $(L_k)_{k\geq 0}$ with the characteristic polynomial $P(t)$ is given by

$$L_k = \frac{1}{P_1'(\alpha)} k\alpha^{k-1} - \Big\{\sum_{i=1}^{m} \frac{1}{P'(\beta_i)}\Big\}\alpha^k + \sum_{i=1}^{m} \frac{\beta_i^k}{P'(\beta_i)}$$

We have gotten also

$$\tilde{\omega} \circ \xi^{-1} : (A_1 + A_2\varepsilon, B_1, \dots, B_m) \mapsto$$
$$\Big(\frac{A_1}{P_1'(\alpha)} k\alpha^{k-1} - A_1\Big\{\sum_{i=1}^{m} \frac{1}{P'(\beta_i)}\Big\}\alpha^k + \frac{A_2}{P_1'(\alpha)}\alpha^k + \sum_{i=1}^{m} \frac{B_i}{P'(\beta_i)}\beta_i^k\Big)_{k\geq 0}.$$

Put $\eta = A_1 e(\theta) + A_2\varepsilon(\theta) + \sum_{i=1}^{n} B_i e_i(\theta)$ and $\boldsymbol{w} = \tilde{\omega}(\eta)$. Then we have

$$\operatorname{Nr} \eta = (-1)^{(m+2)(m+1)/2} \Delta(\boldsymbol{w}) = A_1^2 B_1 \cdots B_m.$$

Example 1.7.1. Let R be a ring and $\alpha, \beta \in R$ with $\alpha \neq \beta$. Put $P(t) = (t-\alpha)^2(t-\beta)$, $P(t) = (t-\alpha)(t-\beta)$ and $D = (\alpha-\beta)^2$. Let θ and θ_1 denote the image of t in $R[t]/(P(t))$ and in $R[t]/(P_1(t))$, respectively.

The homomorphisms of R-algebras $\xi : R[t]/(P(t)) \to R[\varepsilon] \times R$ and $\xi_1 : R[t]/(P_1(t)) \to R \times R$ are defined by

$$\xi(\theta) = (\alpha + \varepsilon, \beta)$$

and

$$\xi_1(\theta_1) = (\alpha, \beta),$$

repectively.

If D is invertible in R, then ξ and ξ_1 are bijective. Moreover, we have

$$\begin{aligned} e_1(t) &= \frac{1}{(\beta-\alpha)^2}(t-\alpha)^2, \\ e(t) &= 1 - \frac{1}{(\beta-\alpha)^2}(t-\alpha)^2, \\ \varepsilon(t) &= \frac{1}{\alpha-\beta}(t-\alpha)(t-\beta) \end{aligned}$$

and

$$\begin{aligned} \tilde{\omega} : e_1(\theta) = \Big(\frac{\theta-\alpha}{\beta-\alpha}\Big)^2 &\mapsto \Big(\frac{\beta^k}{(\beta-\alpha)^2}\Big)_{k\geq 0}, \\ \tilde{\omega} : e(\theta) = 1 - \Big(\frac{\theta-\alpha}{\beta-\alpha}\Big)^2 &\mapsto \Big(\frac{1}{\alpha-\beta}k\alpha^{k-1} - \frac{\alpha^k}{(\alpha-\beta)^2}\Big)_{k\geq 0}, \\ \tilde{\omega} : \varepsilon(\theta) = \frac{(\theta-\alpha)(\theta-\beta)}{\alpha-\beta} &\mapsto \Big(\frac{\alpha^k}{\alpha-\beta}\Big)_{k\geq 0}. \end{aligned}$$

The Lucas sequence $(L_k)_{k\geq 0}$ with the characteristic polynomial $P(t)$ is given by

$$L_k = \frac{1}{\alpha-\beta}k\alpha^{k-1} - \frac{\alpha^k}{(\alpha-\beta)^2} + \frac{\beta^k}{(\alpha-\beta)^2}.$$

We have gotten also

$$\tilde{\omega} \circ \xi^{-1} : (A_1 + A_2\varepsilon, B) \mapsto \Big(\frac{A_1}{\alpha-\beta}k\alpha^{k-1} + \frac{-A_1 + (\alpha-\beta)A_2}{(\alpha-\beta)^2}\alpha^k + \frac{B}{(\alpha-\beta)^2}\beta^k\Big)_{k\geq 0}$$

Example 1.7.2. Let R be a ring and $\alpha, \beta_1, \beta_2 \in R$. Assume that α, β_1, β_2 are distinct to each other. Put $P(t) = (t-\alpha)^2(t-\beta_1)(t-\beta_2)$, $P(t) = (t-\alpha)(t-\beta_1)(t-\beta_2)$ and $D = (\alpha-\beta_1)^2(\alpha-\beta_2)^2(\beta_1-\beta_2)^2$. Let θ and θ_1 denote the image of t in $R[t]/(P(t))$ and in $R[t]/(P_1(t))$, respectively.

The homomorphisms of R-algebras $\xi : R[t]/(P(t)) \to R[\varepsilon] \times R$ and $\xi_1 : R[t]/(P_1(t)) \to R \times R$ are defined by

$$\xi(\theta) = (\alpha + \varepsilon, \beta_1, \beta_2)$$

and

$$\xi_1(\theta_1) = (\alpha, \beta_1, \beta_2),$$

repectively.

If D is invertible in R, then ξ and ξ_1 are bijective. Moreover, we have

$$\begin{aligned}
e_1(t) &= \frac{1}{(\beta_1-\alpha)^2(\beta_1-\beta_2)}(t-\alpha)^2(t-\beta_2),\\
e_2(t) &= \frac{1}{(\beta_2-\alpha)^2(\beta_2-\beta_1)}(t-\alpha)^2(t-\beta_1),\\
e(t) &= 1-\frac{1}{(\beta_1-\alpha)^2(\beta_1-\beta_2)}(t-\alpha)^2(t-\beta_2)-\frac{1}{(\beta_2-\alpha)^2(\beta_2-\beta_1)}(t-\alpha)^2(t-\beta_1),\\
\varepsilon(t) &= \frac{1}{(\theta-\alpha)(\theta-\beta)}(t-\alpha)(t-\beta_1)(t-\beta_2)
\end{aligned}$$

and

$$\begin{aligned}
\tilde{\omega}: e_1(\theta) &= \frac{(\theta-\alpha)^2(\theta-\beta_2)}{(\beta_1-\alpha)^2(\beta_1-\beta_2)} \mapsto \Big(\frac{\beta_1^k}{(\beta_1-\alpha)^2(\beta_1-\beta_2)}\Big)_{k\geq 0},\\
\tilde{\omega}: e_2(\theta) &= \frac{(\theta-\alpha)^2(\theta-\beta_1)}{(\beta_2-\alpha)^2(\beta_2-\beta_1)} \mapsto \Big(\frac{\beta_2^k}{(\beta_2-\alpha)^2(\beta_2-\beta_1)}\Big)_{k\geq 0},\\
\tilde{\omega}: e(\theta) &= 1-e_1(\theta)-e_2(\theta) \mapsto \Big(\frac{1}{(\alpha-\beta_1)(\alpha-\beta_2)}k\alpha^{k-1}+\frac{\beta_1+\beta_2-2\alpha}{(\alpha-\beta_1)^2(\alpha-\beta_2)^2}\alpha^k\Big)_{k\geq 0},\\
\tilde{\omega}: \varepsilon(\theta) &= \frac{(\theta-\alpha)(\theta-\beta_1)(\theta-\beta_2)}{(\alpha-\beta_1)(\alpha-\beta_2)} \mapsto \Big(\frac{\alpha^k}{(\alpha-\beta_1)(\alpha-\beta_2)}\Big)_{k\geq 0}.
\end{aligned}$$

The Lucas sequence $(L_k)_{k\geq 0}$ with the characteristic polynomial $P(t)$ is given by

$$L_k = \frac{1}{(\alpha-\beta_1)(\alpha-\beta_2)}k\alpha^{k-1}+\frac{\beta_1+\beta_2-2\alpha}{(\alpha-\beta_1)^2(\alpha-\beta_2)^2}\alpha^k+\frac{\beta_1^k}{(\beta_1-\alpha)^2(\beta_1-\beta_2)}+\frac{\beta_2^k}{(\beta_2-\alpha)^2(\beta_2-\beta_1)}.$$

2. Goup schemes G_P and $G_{(P)}$

We recall needed facts on reformulations of Lucas sequences mentioned in [10, Section 2 and Section 4] in the framework of affine group scheme theory, referring to [3] or [13] on formalisms of affine group schemes and Hopf algebras.

Definition 2.1. Let R be a ring and $P(t) = t^n - P_1t^{n-1} - \cdots - P_{n-1}t - P_n \in R[t]$. Put $\tilde{R} = R[t]/(P(t))$ and $G_P = \prod_{\tilde{R}/R}\mathbb{G}_{m,\tilde{R}}$ (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 a homomorphism of group schemes

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

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.

We put

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

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

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

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

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathbb{G}_{m,R} & \longrightarrow & G_P & \xrightarrow{\beta} & G_{(P)} & \longrightarrow & 0 \\ & & \| & & \downarrow \rho & & \downarrow \rho & & \\ 1 & \longrightarrow & \mathbb{G}_{m,R} & \longrightarrow & GL_{n,R} & \longrightarrow & PGL_{n,R} & \longrightarrow & 1 \end{array} .$$

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 $n = 2$.

More concretely, $G_P(R)$ acts on $\mathcal{L}(P, R)$ by multiplication through the isomorphism $\tilde{\omega} : G_P(R) \xrightarrow{\sim} \mathcal{L}(P, R)^\times$. Now put

$$\mathcal{L}(P, R)^\circ = \{\boldsymbol{w} = (w_k)_{k\geq 0} \in \mathcal{L}(P, R)\ ;\ (w_0, w_1, \dots, w_{n-1}) = R\}.$$

Then $\mathcal{L}(P, R)^\circ$ is stable under the action of $G_P(R)$ on $\mathcal{L}(P, R)$. Furthermore, we obtain an action $G_P(R)/R^\times$ on $\mathcal{L}(P, R)^\circ/R^\times$. If $\mathrm{Pic}(R) = 0$, then we have $G_{(P)}(R) = G_P(R)/R^\times$ and $\mathbb{P}^{n-1}(R) = \mathcal{L}(P, R)^\circ/R^\times$.

Hereafter, we assume that $R = \mathbb{Z}$ and $P(t) = t^n - P_1 t^{n-1} - \cdots - P_{n-1}t - P_n \in \mathbb{Z}[t]$.

2.3. Let p be a prime. Then the following assertions hold true:

(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

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \mathbb{Q}^{\times} & \xrightarrow{i} & G_P(\mathbb{Q}) & \xrightarrow{\beta} & G_{(P)}(\mathbb{Q}) & \longrightarrow & 0 \\
 & & \uparrow & & \uparrow & & \uparrow & & \\
0 & \longrightarrow & \mathbb{Z}_{(p)}^{\times} & \xrightarrow{i} & G_P(\mathbb{Z}_{(p)}) & \xrightarrow{\beta} & G_{(P)}(\mathbb{Z}_{(p)}) & \longrightarrow & 0. \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & (\mathbb{Z}/p^N\mathbb{Z})^{\times} & \xrightarrow{i} & G_P(\mathbb{Z}/p^N\mathbb{Z}) & \xrightarrow{\beta} & G_{(P)}(\mathbb{Z}/p^N\mathbb{Z}) & \longrightarrow & 0
\end{array}$$

(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.

Notation 2.4. Let θ denote the image of t in the residue ring $\tilde{R} = \mathbb{Z}[t]/(P(t))$. Assume that $P_n \neq 0$. Then θ is invertible in the residue ring $\mathbb{Z}[1/P_n] \otimes_{\mathbb{Z}} \tilde{R} = \mathbb{Z}[1/P_n][t]/(P(t))$. We shall denote by Θ all the subgroup of $G_P(\mathbb{Z}[1/P_n])$ generated by θ, the subgroup of $G_{(P)}(\mathbb{Z}[1/P_n])$ generated by $\beta(\theta)$ and the subgroup of $PGL(n, \mathbb{Z}[1/P_n])$ generated by $\rho(\theta)$. Furthermore, let m be an integer≥ 2 with $(m, P_n) = 1$. By abuse of notation, we shall denote by Θ also the image of Θ in $G_P(\mathbb{Z}/m\mathbb{Z})$ and in $G_{(P)}(\mathbb{Z}/m\mathbb{Z})$.

Definition 2.5. Let $(L_k)_{k\geq 0}$ denote the Lucas sequence with the characteristic polynomial $P(t)$. 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 2.6. ([10, 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 θ in $G_{(P)}(\mathbb{Z}/m\mathbb{Z}) = (\mathbb{Z}[t]/(m, P(t)))^{\times}/(\mathbb{Z}/m\mathbb{Z})^{\times}$.*

Corollary 2.7. ([10, 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 $k(m)$.*

Proposition 2.8. ([10, 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*

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

and

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

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 $N > \nu'$,

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

Now we reformuate the argument on divisibility of Lucas sequences, which is developed by Ward [12].

Definition 2.9. (Ward [12, Introduction]) Let $P(t) = t^n - P_1 t^{n-1} - \cdots - P_{n-1}t - P_n \in \mathbb{Z}[t]$ and $\boldsymbol{w} = (w_k)_{k\geq 0} \in \mathcal{L}(P, \mathbb{Z})$. An integer $m \geq 2$ is said to be a maximal divisor of $\boldsymbol{w}$ if there exists k such that $m | w_k, \ldots, m | w_{k+n-2}$ and $m \nmid w_{k+n-1}$.

Notation 2.10. Let $P(t) = t^n - P_1 t^{n-1} - \cdots - P_{n-1}t - P_n \in \mathbb{Z}[t]$, and let m be an integer ≥ 2 with $(m, P_n) = 1$. Then θ is invertible in the residue ring $\tilde{R} = \mathbb{Z}[t]/(m, P(t))$. By abuse of notation, we denote by Θ the subgroup of $G_P(\mathbb{Z}/m\mathbb{Z})$ or $G_{(P)}(\mathbb{Z}/m\mathbb{Z})$ generated by θ.

Theorem 2.11. *Let $P(t) = t^n - P_1 t^{n-1} - \cdots - P_{n-1}t - P_n \in \mathbb{Z}[t]$ and $\boldsymbol{w} = (w_k)_{k\geq 0} \in \mathcal{L}(P, \mathbb{Z})$, and let m be an integer ≥ 2 with $(m, P_n) = 1$ and $(m, w_0, \ldots, w_{n-1}) = 1$. Then, m is a maximal divisor of $\boldsymbol{w}$ if and only $[\boldsymbol{w}]$ is in the orbit $(0 : \ldots : 0 : 1)\Theta$ in $\mathbb{P}^{n-1}(\mathbb{Z}/m\mathbb{Z})$.*

Proof. It is sufficient to note that the multiplication by θ on $(\mathbb{Z}/m\mathbb{Z}) \otimes_{\mathbb{Z}} \tilde{R} = \mathbb{Z}[t]/(m, P(t))$ induces the shift operation $(w_k)_{k\geq 0} \mapsto (w_{k+1})_{k\geq 0}$ on $\mathcal{L}(P, \mathbb{Z}/m\mathbb{Z})$ through the isomorphism $\omega : (\mathbb{Z}/m\mathbb{Z}) \otimes_{\mathbb{Z}} \tilde{R} \xrightarrow{\sim} \mathcal{L}(P, \mathbb{Z}/m\mathbb{Z})$.

Remark 2.11.1. Put $\eta = \tilde{\omega}^{-1}(\boldsymbol{w}) \in \tilde{R} = \mathbb{Z}[t]/(P(t))$. Then, $[\boldsymbol{w}]$ is in the orbit $(0 : \ldots : 0 : 1)\Theta$ in $\mathbb{P}^{n-1}(\mathbb{Z}/m\mathbb{Z})$ if and only if $\Delta(\boldsymbol{w})$ is prime to m and $\beta(\eta) \in \Theta \subset G_{(P)}(\mathbb{Z}/m\mathbb{Z})$.

Remark 2.12. Let $P(t) = t^n - P_1 t^{n-1} - \cdots - P_{n-1}t - P_n \in \mathbb{Z}[t]$ and $\eta \in G_P(\mathbb{Z}_{(p)})$, and let p a prime with $(p, P_n) = 1$. Then the rank $r(p)$ of the Lucas sequence with the characteristic polynomial $P(t)$ is nothing but the order of the group $\Theta \subset G_{(P)}(\mathbb{Z}/p\mathbb{Z})$ by Theorem 2.6. It follows that, if $\beta(\eta) \in \Theta \subset G_{(P)}(\mathbb{Z}/p\mathbb{Z})$, then $r(p)$ is divisible by the order of $\beta(\eta)$.

The converse holds true under the assumption that $G_{(P)}(\mathbb{Z}/p\mathbb{Z})$ is a cyclic group. This is the case when $P(t)$ is irreducible in $\mathbb{F}_p[t]$, or $P(t) = (t - \alpha)Q(t)$ in $\mathbb{F}_p[t]$ with $Q(t)$ irreducible over $\mathbb{F}_p$.

Remark 2.13. The assertions of Remark 2.12 is a generalization of some result in Ward [12].

Indeed, let $P(t) = t^n - P_1 t^{n-1} - \cdots - P_{n-1}t - P_n \in \mathbb{Z}[t]$ with the discriminant $D \neq 0$ and $\boldsymbol{w} = (w_k)_{k\geq 0} \in \mathcal{L}(P, \mathbb{Z})$. Put $\eta = \tilde{\omega}^{-1}(\boldsymbol{w}) \in \tilde{R} = \mathbb{Z}[t]/(P(t))$. Moreover, let p a prime with $p \nmid D$, $p \nmid P_n$ and $p \nmid \Delta(\boldsymbol{w})$. It is verified by Ward that:
(1) [12, Theorem 4.1] If p is a maximal divisor of $\boldsymbol{w}$, then then $r(p)$ is divisible by the order of $\beta(\eta)$ in and $G_{(P)}(\mathbb{Z}/p\mathbb{Z})$.
(2) [12, Theorem 4.2] The converse of (1) holds true provided that (a) n is odd, (b) $p-1$ is prime to n, (c) $P(t)$ is irreducible in $\mathbb{F}_p[t]$.

Remark 2.14. Let $P(t) = t^n - P_1 t^{n-1} - \cdots - P_{n-1}t - P_n \in \mathbb{Z}[t]$ with the discriminant $D \neq 0$. Let K denote the splitting field of $P(t)$ over $\mathbb{Q}$ and $\mathcal{O}_K$ the ring of integers in K. Put $R = \mathcal{O}_K[1/D]$. Then we obtain an embedding of rings

$$\mathcal{L}(P, \mathbb{Z}) \longrightarrow \mathcal{L}(P, R) \overset{\xi\circ\tilde{\omega}^{-1}}{\underset{\sim}{\longrightarrow}} R^n.$$

Therefore, if p is a prime with $(p, D) = 1$, then we obtain an embedding of rings

$$\mathcal{L}(P, \mathbb{Z}_{(p)}) \longrightarrow \mathcal{L}(P, \mathbb{Z}_{(p)} \otimes_{\mathbb{Z}} R) \overset{\xi\circ\tilde{\omega}^{-1}}{\underset{\sim}{\longrightarrow}} (\mathbb{Z}_{(p)} \otimes_{\mathbb{Z}} R)^n$$

and embeddings of groups

$$\begin{array}{ccccc} G_P(\mathbb{Z}_{(p)}) & \longrightarrow & G_P(\mathbb{Z}_{(p)} \otimes_{\mathbb{Z}} R) & \overset{\xi\circ\tilde{\omega}^{-1}}{\underset{\sim}{\longrightarrow}} & \mathbb{G}_m(\mathbb{Z}_{(p)} \otimes_{\mathbb{Z}} R)^n \\ \downarrow & & \downarrow & & \downarrow \\ G_P(\mathbb{Z}/p^N\mathbb{Z}) & \longrightarrow & G_P(R/p^N R) & \overset{\xi\circ\tilde{\omega}^{-1}}{\underset{\sim}{\longrightarrow}} & \mathbb{G}_m(R/p^N R)^n \end{array}.$$

Now let $\eta \in G_P(\mathbb{Z}_{(p)})$, and put

$$\xi^{-1}(\tilde{\omega}(\eta)) = \Big(\sum_{i=1}^{n} \frac{A_i}{P'(\alpha_i)}\alpha_i^k\Big)_{k\geq 0}.$$

Here $P(t) = (t-\alpha_1)(t-\alpha_2)\cdots(t-\alpha_n)$ in $K[t]$. Then we have

$$\text{the order of } \beta(\eta) \text{ in } G_{(P)}(\mathbb{Z}/p^N\mathbb{Z}) = \text{the least positive integer } \nu \text{ such that } A_1^\nu \equiv A_2^\nu \equiv \cdots \equiv A_n^\nu \mod p^N,$$

as is suggested by Ward just after [3, Lemma 5.2]. In particular, we have

$$r(p^N) = \text{the least positive integer } \nu \text{ such that } \alpha_1^\nu \equiv \alpha_2^\nu \equiv \cdots \equiv \alpha_n^\nu \mod p^N,$$

as is suggested by Ward at the beginning of [12, Section 3].

Remark 2.15. Let $P(t) = t^n - P_1 t^{n-1} - \cdots - P_{n-1}t - P_n \in \mathbb{Z}[t]$ with $P_n \neq 0$. Then θ is invertible in the residue ring $\mathbb{Q} \otimes_{\mathbb{Z}} \tilde{R} = \mathbb{Q}[t]/((P(t))$. Let Θ denote the subgroup of $G_{(P)}(\mathbb{Q})$ generated by the image of θ. We may define the Laxton group associated to $P(t)$ as the residue group $G_{(P)}(\mathbb{Q})/\Theta$. Indeed, $G_{(P)}(\mathbb{Q})/\Theta$ is isomorphic to the Laxton group $G(P)$ defined by Laxton [6]

in the case of $n = 2$, as is verified in [8, Theorem 4.2], and to the Laxton group $G(P)$ defined by Ballot [1, Ch.4.3 and Ch.5.3]. In both the articles, $P(t)$ is assumed to be separable.

Let p be a prime with (p, P_n), and put

$$G(P,p) = \{[\boldsymbol{w}] \in G_{(P)}(\mathbb{Q})/\Theta \ ; \ p \text{ is a maximal divisor of } \boldsymbol{w}\}.$$

Ballot [1, Theorem 5.4.9] asserts that $G(P,p)$ is a subgroup of $G_{(P)}(\mathbb{Q})/\Theta$. We can verify $G(P,p) = \mathrm{Ker}[G_{(P)}(\mathbb{Z}_{(p)})/\Theta \to G_{(P)}(\mathbb{Z}/p\mathbb{Z})/\Theta]$ without assuming that $P(t)$ is separable.

Remark 2.16. Let $P(t) = t^3 - P_1t^2 - P_2t - P_3 \in \mathbb{Z}[t]$. Let $\boldsymbol{w} = (w_k)_{k\geq 0} \in \mathcal{L}(P,\mathbb{Z})$, and let p be a prime. We call p a twin divisor if there exists l such that $p|w_l$, $p|w_{l+2}$ and $p \nmid w_{l+1}$, following Ballot [1, Ch.4.8]. Similarly as Theorem 2.11, we can verify the following:

Proposition 2.16.1. *Assume that $(p, P_3) = 1$. Then, p is a twin divisor of $\boldsymbol{w}$ if and only $[\boldsymbol{w}]$ is in the orbit $(0:1:0)\Theta$ in $\mathbb{P}^2(\mathbb{Z}/p\mathbb{Z})$.*

Remark 2.16.2. Put $\boldsymbol{w} = (0,1,0,\dots) \in \mathcal{L}(P,\mathbb{Z})$ and $\eta = \tilde{\omega}^{-1}(\boldsymbol{w}) \in \tilde{R} = \mathbb{Z}[t]/(P(t))$. Assume $P_3 + P_1P_2 \neq 0$. Ballot verifies, in our terminology, that:
(1) η is invertible in $\mathbb{Q}[t]/(P(t))$;
(2) $(P_3 + P_1P_2)\tilde{\omega}(\eta^{-1})$ is given by $(1, P_1, P_1^2, \dots)$ ([1, Lemma 4.8.3]).

We can generalize the argument on twin divisors as follows.

Remark 2.17. Let R be a ring and $P(t) = t^n - P_1t^{n-1} - \cdots - P_{n-1}t - P_n \in R[t]$. Put

$$\eta_j = -P_j - P_{j-1}\theta - \cdots - P_1\theta^{j-1} + \theta^j$$

for $1 \leq j \leq n-1$. Then $\{1, \eta_1, \eta_2, \dots, \eta_{n-1}\}$ is an R-basis of $\tilde{R} = R[t]/(P(t))$. Moreover, we have

$$\tilde{\omega}(\eta_j)_k = \begin{cases} 1 & (k = n-1-j) \\ 0 & (0 \leq k < n, \ k \neq n-1-j) \end{cases}.$$

Similarly as Theorem 2.11 and Proposition 2.16.1, we can verify the following:

Proposition 2.17.1. *Let $P(t) = t^n - P_1t^{n-1} - \cdots - P_{n-1}t - P_n \in \mathbb{Z}[t]$ with $P_n \neq 0$ and $\boldsymbol{w} = (w_k)_{k\geq 0} \in \mathcal{L}(P,\mathbb{Z})$. Let p be a prime with $(p, P_n) = 1$. Then, there exists l such that $p|w_{l+i}$ for all i with $0 \leq i < n$, $i \neq n-1-j$ and $p \nmid w_{l+n-1-j}$ if and only $[\boldsymbol{w}]$ is in the orbit $\tilde{\omega}(\eta_j)\Theta$ in $\mathbb{P}^{n-1}(\mathbb{Z}/p\mathbb{Z})$.*

Remark 2.18. Let R be a ring and $P(t) = t^n - P_1t^{n-1} - \cdots - P_{n-1}t - P_n \in R[t]$. Moreover, put $P(t) = (t - P_1)Q(t) + r$ ($Q(t) \in R[t]$, $r \in R$). Then we obtain

$$(-P_1 + \theta)Q(\theta) = -r = -P(P_1) = P_n + P_{n-1}P_1 + \cdots + P_2P_1^{n-2}$$

in $\tilde{R} = R[t]/(P(t))$, which implies $\mathrm{Nr}\,\eta_1 = P_n + P_{n-1}P_1 + \cdots + P_2P_1^{n-2}$. Furthermore, we obtain inductively

$$\theta^k Q(\theta) = P_1^k Q(\theta) - (P_1^{k-1} + P_1^{k-2}\theta + \cdots + P_1\theta^{k-2} + \theta^{k-1})r$$

for $k > 0$. This implies

$$\tilde{\omega}(Q(\theta)) = (1, P_1, P_1^2, \dots, P_1^{n-1}, \dots)$$

since $Q(t) = t^{n-1} + \cdots$.

It is easy to verify $\operatorname{Nr} \eta_{n-1} = \eta_{n-1}\theta = P_n$. However, it is more subtle to calculate $\operatorname{Nr} \eta_j$ for $1 < j < n-1$. Here are few examples.

Example 2.18.1. Case of $n = 4$. Put

$$\tilde{\eta}_2 = P_3^2 + (P_1P_3 + P_4)\theta^2 - P_3\theta^3.$$

Then we obtain

$$\operatorname{Nr} \eta_2 = \eta_2\tilde{\eta}_2 = P_1P_3P_4 - P_2P_3^2 + P_4^2$$

and

$$\tilde{\omega}(\tilde{\eta}_2) = (-P_3, P_4, P_1P_4 - P_2P_3, -P_1P_2P_3 + P_1^2P_4 + P_2P_4, \dots).$$

Example 2.18.2. Case of $n = 5$. Put

$$\tilde{\eta}_2 = (P_1P_3P_4 - P_2P_3^2 - P_3P_5 + P_4^2) + (P_1P_3^2 + P_3P_4)\theta^2 + (P_1^2P_3 + P_2P_3 + P_1P_4 + P_5)\theta^3 - (P_1P_3 + P_4)\theta^4$$

Then we obtain

$$\operatorname{Nr} \eta_2 = \eta_2\tilde{\eta}_2 = -P_1P_2P_3P_4 + P_1^2P_3P_5 + P_1P_4P_5 + P_2^2P_3^2 + 2P_2P_3P_5 - P_2P_4^2 + P_5^2$$

and

$$\tilde{\omega}(\eta_2) = (-P_1P_3 - P_4, P_2P_3 + P_5, P_1P_5 - P_2P_4, -P_1P_2P_4 + P_1^2P_5 + P_2^2P_3 + P_2P_5, \dots).$$

Put now

$$\tilde{\eta}_3 = P_4^3 + (-P_1P_4P_5 + P_2P_4 - P_5^2)\theta^2 + (P_1P_4^2 + P_4P_5)\theta^3 - P_4^2\theta^4.$$

Then we obtain

$$\operatorname{Nr} \eta_3 = \eta_3\tilde{\eta}_3 = -P_1P_4P_5 + P_2P_4^2P_5 - P_3P_4^3 - P_5^3$$

and

$$\tilde{\omega}(\eta_3) =$$
$$(-P_4^2, P_4P_5, -P_5^2, -P_1P_5^2 + P_2P_4P_5 - P_3P_4^2, P_1P_2P_4P_5 - P_1P_3P_4^2 - P_1^2P_5^2 - P_2P_5^2 + P_3P_4P_5, \dots).$$

3. Cullen-Ballot sequences

Notation 3.1. Let $\alpha \in R$ and $Q(t) = t^m - \beta_1 t^{m-1} - \cdots - \beta_{m-1}t - \beta_m \in R[t]$, and put $P(t) = (t-\alpha)^2 Q(t)$ and $P_1(t) = (t-\alpha)Q(t)$. Let D denote the discriminant of $P_1(t)$. Moreover, we put

$$\tilde{R} = R[t]/(P(t)),\ \tilde{R}_1 = R[t]/(P_1(t)),\ \tilde{R}_Q = R[t]/(Q(t))$$

and

$$G_P = \prod_{\tilde{R}/R} \mathbb{G}_{m,\tilde{R}},\ G_{P_1} = \prod_{\tilde{R}_1/R} \mathbb{G}_{m,\tilde{R}_1},\ G_Q = \prod_{\tilde{R}_Q/R} \mathbb{G}_{m,\tilde{R}_Q},$$

as is done in 2.1.

The reduction map $\tilde{R}^\times = (R[t]/(P(t)))^\times \to \tilde{R}_1^\times = (R[t]/(P_1(t)))^\times$ is represented by a homomorphim of group R-schemes $\pi : G_P = \prod_{\tilde{R}/R} \mathbb{G}_{m,\tilde{R}} \to G_{P_1} = \prod_{\tilde{R}_1/R} \mathbb{G}_{m,\tilde{R}_1}$. Futhermore we obtain a commutative digaram with exact rows

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathbb{G}_{m,R} & \longrightarrow & G_P & \longrightarrow & G_{(P)} & \longrightarrow & 0 \\ & & \| & & \downarrow \pi & & \downarrow \pi & & \\ 0 & \longrightarrow & \mathbb{G}_{m,R} & \longrightarrow & G_{P_1} & \longrightarrow & G_{(P_1)} & \longrightarrow & 0 \end{array}.$$

Proposition 3.2. *The homomorphism $\pi : G_P \to G_{P_1}$ is faithfully flat, and* $\mathrm{Ker}[\pi : G_P \to G_{P_1}]$ *is isomorphic to the additive group scheme $\mathbb{G}_{a,R}$.*

Proof. Let S be an R-algebra. Then we have

$$\mathrm{Ker}[G_P(S) \to G_{P_1}(S)] = \{1 + a(\theta - \alpha)Q(\theta)\ ;\ a \in S\}.$$

The map $a \mapsto 1 + a(\theta - \alpha)Q(\theta)$ gives rise to an isomorphism $S \xrightarrow{\sim} \mathrm{Ker}[G_P(S) \to G_{P_1}(S)]$, and the injective homomorphism $S \to G_P(S)$ is represented by a homomorphism of group R-schemes $\mathbb{G}_{a,R} \to G_P$. On the other hand, the reduction map $G_P(S) = (S[t]/((t-\alpha)^2Q(t)))^\times \to G_{P_1}(S) = (S[t]/((t-\alpha)Q(t)))^\times$ is surjective since $\mathbb{G}_{m,S}$ is smooth over R and $\mathrm{Ker}[S[t]/((t-\alpha)^2Q(t)) \to S[t]/((t-\alpha)Q(t))]$ is a nilpotent ideal of $S[t]/((t-\alpha)^2Q(t))$.

Remark 3.3. Combining the exact sequence

$$0 \longrightarrow \mathbb{G}_{a,R} \longrightarrow G_P \xrightarrow{\pi} G_{P_1} \longrightarrow 0.$$

with the commutative diagram in 3.1, we obtain a commutative diagram with exact rows and columns

$$\begin{array}{ccccccccc} & & & & 0 & & 0 & & \\ & & & & \downarrow & & \downarrow & & \\ & & & & \mathbb{G}_{m,R} & = & \mathbb{G}_{m,R} & & \\ & & & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & \mathbb{G}_{a,R} & \longrightarrow & G_P & \xrightarrow{\pi} & G_{P_1} & \longrightarrow & 0. \\ & & \| & & \downarrow \beta & & \downarrow \beta & & \\ 0 & \longrightarrow & \mathbb{G}_{a,R} & \longrightarrow & G_{(P)} & \xrightarrow{\pi} & G_{(P_1)} & \longrightarrow & 0 \\ & & & & \downarrow & & \downarrow & & \\ & & & & 0 & & 0 & & \end{array}$$

Notation 3.4. Define a map $\eta : R[\varepsilon]^\times \to R^\times \times R$ by $\eta(a + b\varepsilon) = (a, b/a)$. Then η is an isomorphism and represented by an isomorphism of group R-schemes $\eta : \prod_{R[\varepsilon]/R} \mathbb{G}_{m,R[\varepsilon]} \xrightarrow{\sim} \mathbb{G}_{m,R} \times \mathbb{G}_{a,R}$.

Remark 3.5. Let D denote the discriminant of $P_1(t)$, and assume $D \neq 0$. Moreover, let θ, θ_1 and θ_Q denote the image of t in the residue rings $R[t]/(P(t))$, $R[t]/(P_1(t))$ and $R[t]/(Q(t))$, respectively. As in 1.6, define a homomorphism of R-algebras

$$\xi : \tilde{R} = R[t]/(P(t)) \to R[\varepsilon] \times \tilde{R}_Q$$

by

$$\theta \mapsto (\alpha + \varepsilon, \theta_Q)$$

and a homomorphism of R-algebras

$$\xi_1 : \tilde{R}_1 = R[t]/(P_1(t)) \to R[\varepsilon] \times \tilde{R}_Q$$

by $\theta \mapsto (\alpha, \theta_Q)$. Then the homomorphisms of multiplicative groups

$$\xi : \tilde{R}^\times \to R[\varepsilon]^\times \times \tilde{R}_Q^\times$$

and

$$\xi_1 : \tilde{R}_1^\times \to R^\times \times \tilde{R}_Q^\times$$

are represented by homomorphisms of group R-schemes

$$\xi : G_P = \prod_{\tilde{R}/R} \mathbb{G}_{m,\tilde{R}} \to (\mathbb{G}_{m,R} \times \mathbb{G}_{a,R}) \times G_Q = (\mathbb{G}_{m,R} \times \mathbb{G}_{a,R}) \times \prod_{\tilde{R}_Q/R} \mathbb{G}_{m,\tilde{R}_Q}$$

and

$$\xi_1 : G_{P_1} = \prod_{\tilde{R}_1/R} \mathbb{G}_{m,\tilde{R}_1} \to \mathbb{G}_{m,R} \times G_Q = \mathbb{G}_{m,R} \times \prod_{\tilde{R}_Q/R} \mathbb{G}_{m,\tilde{R}_Q},$$

respectively. Moreover, we have a commutative diagram with exact rows

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathbb{G}_{a,R} & \longrightarrow & G_P & \xrightarrow{\pi} & G_{P_1} & \longrightarrow & 0 \\ & & \text{homothety by } Q(\alpha)\big\downarrow & & \xi\big\downarrow & & \xi_1\big\downarrow & & \\ 0 & \longrightarrow & \mathbb{G}_{a,R} & \longrightarrow & (\mathbb{G}_{m,R} \times \mathbb{G}_{a,R}) \times G_Q & \longrightarrow & \mathbb{G}_{m,R} \times G_Q & \longrightarrow & 0 \end{array} .$$

Here $\mathbb{G}_{a,R} \to (\mathbb{G}_{m,R} \times \mathbb{G}_{a,R}) \times G_Q$ is defined by $a \mapsto (1, a, 1)$, and $(\mathbb{G}_{m,R} \times \mathbb{G}_{a,R}) \times G_Q \to \mathbb{G}_{m,R} \times G_Q$ by $(a, b, \eta) \mapsto (a, \eta)$, respectively. As is remarked at the end of Example 1.6, $\xi : G_P \to (\mathbb{G}_{m,R} \times \mathbb{G}_{a,R}) \times G_Q$ and $\xi_1 : G_{P_1} \to \mathbb{G}_{m,R} \times G_Q$ are isomorphic over $R[1/D]$.

Remark 3.6. Define homomorphisms

$$\beta : (\mathbb{G}_{m,R} \times \mathbb{G}_{a,R}) \times G_Q \to \mathbb{G}_{a,R} \times G_Q$$

and

$$\beta_1 : \mathbb{G}_{m,R} \times G_Q \to G_Q$$

by $(a, b, \eta) \mapsto (b, \eta/a)$ and $(a, \eta) \mapsto \eta/a$, respectively. Then we obtain commutative diagrams

$$\begin{array}{ccc} G_P & \xrightarrow[\xi]{} & (\mathbb{G}_{m,R} \times \mathbb{G}_{a,R}) \times G_Q \\ \big\downarrow \beta & & \big\downarrow \beta \\ G_{(P)} & \xrightarrow[\xi]{} & \mathbb{G}_{a,R} \times G_Q \end{array}$$

and

$$\begin{array}{ccc} G_{P_1} & \xrightarrow[\xi_1]{} & \mathbb{G}_{m,R} \times G_Q \\ \downarrow{\scriptstyle \beta} & & \downarrow{\scriptstyle \beta_1} \\ G_{(P_1)} & \xrightarrow[\xi_1]{} & G_Q \end{array} .$$

Moreover, we have a commutative diagram with exact rows

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathbb{G}_{a,R} & \longrightarrow & G_{(P)} & \xrightarrow{\pi} & G_{(P_1)} & \longrightarrow & 0 \\ & & {\scriptstyle \text{homothety by } Q(\alpha)}\downarrow & & {\scriptstyle \xi}\downarrow & & {\scriptstyle \xi_1}\downarrow & & \\ 0 & \longrightarrow & \mathbb{G}_{a,R} & \longrightarrow & \mathbb{G}_{a,R} \times G_Q & \longrightarrow & G_Q & \longrightarrow & 0 \end{array} .$$

Furthermore, $\xi : G_{(P)} \to \mathbb{G}_{a,R} \times G_Q$ and $\xi_1 : G_{P_1} \to G_Q$ are isomorphic over $R[1/D]$.

Notation 3.7. Let $\alpha \in \mathbb{Z}$ and $Q(t) = t^m - \beta_1 t^{m-1} - \cdots - \beta_{m-1}t - \beta_m \in \mathbb{Z}[t]$, and put $P(t) = (t-\alpha)^2 Q(t)$ and $P(t) = (t-\alpha)Q(t)$. Let D denote the discriminant of $P_1(t)$. We assume $D \neq 0$.

Now take a prime p with $(p, \alpha\beta_m) = 1$. Then θ is invertible in $\tilde{R} = R[t]/(P(t))$. By abuse of notation, we denote by Θ the subgroup of $G_{(P)}(\mathbb{Z}_{(p)})$ or $G_{(P)}(\mathbb{Z}/p^N\mathbb{Z})$ generated by the image of $\theta \in G_P(\mathbb{Z}_{(p)})$, and by Θ_1 the subgroup of $G_{(P_1)}(\mathbb{Z}_{(p)})$ or $G_{(P_1)}(\mathbb{Z}/p^N\mathbb{Z})$ generated by the image of $\theta_1 \in G_{P_1}(\mathbb{Z}_{(p)})$.

Theorem 3.8. *Assume $(p, D) = 1$. Then we have $\Theta \supset \mathrm{Ker}[\pi : G_{(P)}(\mathbb{Z}/p\mathbb{Z}) \to G_{(P_1)}(\mathbb{Z}/p\mathbb{Z})]$ in $G_{(P)}(\mathbb{Z}/p\mathbb{Z})$.*

Proof. Let $r_1(p)$ denote is the order of θ_1 in $G_{(P_1)}(\mathbb{Z}/p\mathbb{Z})$. Then $r_1(p)$ is prime to p. Indeed, the order of the multiplicative group $G_{P_1}(\mathbb{Z}/p\mathbb{Z}) = (\mathbb{F}_p[t]/(P_1(t)))^\times$ is prime to p since $P_1(t)$ is separable over $\mathbb{F}_p$. Therefore, the order of $G_{(P_1)}(\mathbb{Z}/p\mathbb{Z})$ is also prime to p.

On the other hand, by Remark 3.6, the homomorphisms $\xi : G_{(P)}(\mathbb{Z}/p\mathbb{Z}) \to \mathbb{G}_a(\mathbb{Z}/p\mathbb{Z}) \times G_Q(\mathbb{Z}/p\mathbb{Z})$ and $\xi_1 : G_{(P_1)}(\mathbb{Z}/p\mathbb{Z}) \to G_Q(\mathbb{Z}/p\mathbb{Z})$ are bijective, and we have $\xi(\theta) = (1/\alpha, \theta_Q/\alpha)$ and $\xi_1(\theta_1) = \theta_Q/\alpha$. Hence we obtain

$$\xi(\theta^{r_1(p)}) = (r_1(p)/\alpha, 1) \neq 0 \text{ in } \mathbb{G}_a(\mathbb{Z}/p\mathbb{Z}) \times G_Q(\mathbb{Z}/p\mathbb{Z}),$$

which implies that $\xi(\theta^{r_1(p)})$ generates $\mathbb{Z}/p\mathbb{Z} = \mathrm{Ker}[\pi : G_{(P)}(\mathbb{Z}/p\mathbb{Z}) \to G_{(P_1)}(\mathbb{Z}/p\mathbb{Z})]$. Hence the result.

Combining Theorem 3.8 and Theorem 2.11, we obtain the following:

Corollary 3.9. *Let $\boldsymbol{w} = (w_k)_{k\geq 0} \in \mathcal{L}(P, \mathbb{Z})$ with $(w_0, w_1, \ldots, w_{n-1}) = 1$, and define $\boldsymbol{v} = (v_k)_{k\geq 0} \in \mathcal{L}(P_1, \mathbb{Z})$ by $v_k = w_{k+1} - \alpha w_k$. Then, p is a maximal divisor of $\boldsymbol{w}$ if and only p is a maximal divisor of $\boldsymbol{v}$.*

Corollary 3.10. *Let p be an odd prime and N a positive integer, and let $r(p^N)$ denote the rank mod p^N of the Lucas sequence with the characteristic polynomial $P(t)$. Then we have $r(p^N) = p^N r_1(p)$.*

Proof. First note that $r(p^N)$ is nothing but the order of θ in $G_{(P)}(\mathbb{Z}/p^N\mathbb{Z})$, as is recalled in Theorem 2.6. By Theorem 3.8, we obtain $r(p) = pr_1(p)$. Furthermore, we have

$$\xi(\theta^{pr_1(p)}) = (pr_1(p)/\alpha, 1) \neq 0 \text{ in } \mathbb{G}_a(\mathbb{Z}/p^2\mathbb{Z}) \times G_Q(\mathbb{Z}/p^2\mathbb{Z})$$

since $r_1(p)$ is prime to p. Therefore, by Proposition 2.8, we obtain $r(p^N) = p^{N-1}r(p)$ for $N > 1$. Hence the result.

Example 3.11. (Ballot [3, Section 3, pp.341]) Let $\alpha, \beta \in \mathbb{Z}$ with $\alpha \neq \beta$. We shall call the sequence $(c_k)_{k\geq 0}$ defined by

$$c_k = \Big\{\frac{k}{\alpha-\beta} - \frac{2\beta-\alpha}{(\alpha-\beta)^2}\Big\}\alpha^k + \frac{\beta}{(\alpha-\beta)^2}\beta^k$$

the Cullen-Ballot sequence associated to (α, β). It is easily verified that, for every prime p with $(p, \alpha\beta(\alpha-\beta)) = 1$, we have $c_{p-2} \equiv 0 \mod p$, $c_{p-1} \equiv 0 \mod p$ and $c_p \equiv 1 \mod p$.

The Cullen-Ballot sequence associated to $(2, 1)$ is nothing but the Cullen sequence $(k2^k+1)_{k\geq 0}$. We now reformulate the Cullen-Ballot sequences in our own way.

Put $P(t) = (t-\alpha)^2(t-\beta)$ and $\Delta = \alpha\beta(\alpha-\beta)$, and let θ denote the image of t in the residue ring $\mathbb{Z}[t]/(P(t))$. The homomorphism of rings $\xi : \mathbb{Z}[t]/(P(t)) \to \mathbb{Z}[\varepsilon] \times \mathbb{Z}$ by $\xi(\theta) = (\alpha+\varepsilon, \beta)$, and the homomorphism of group schemes $\xi : G_{(P)} \otimes_{\mathbb{Z}} \mathbb{Z}[1/\Delta] \to \mathbb{G}_{a,\mathbb{Z}[1/\Delta]} \times \mathbb{G}_{m,\mathbb{Z}[1/\Delta]}$ is given by $\xi(\theta) = (1/\alpha, \beta/\alpha)$. Hence we obtain

$$\Theta = \Big\{\Big(\frac{k}{\alpha}, \frac{\beta^k}{\alpha^k}\Big)\ ;\ k \in \mathbb{Z}\Big\} \subset \mathbb{Q} \times \mathbb{Q}^\times$$

under the identification $\xi : G_{(P)}(\mathbb{Q}) \xrightarrow{\sim} \mathbb{G}_a(\mathbb{Q}) \times \mathbb{G}_m(\mathbb{Q}) = \mathbb{Q} \times \mathbb{Q}^\times$. Moreover, the Lucas sequence $(L_k)_{k\geq 0}$ with the characteristic polynomial $P(t)$ is given by

$$L_k = \frac{1}{\alpha-\beta}k\alpha^{k-1} - \frac{\alpha^k}{(\alpha-\beta)^2} + \frac{\beta^k}{(\alpha-\beta)^2},$$

as is remarked in 1.7.1.

Put now

$$\eta = \theta + \frac{1}{\alpha-\beta}(\theta-\alpha)(\theta-\beta).$$

Then we have

$$\tilde{\omega}(\eta) = \Big(L_{k+1} + \frac{\alpha^k}{\alpha-\beta}\Big)_{k\geq 0} = (c_k)_{k\geq 0}.$$

Furthermore, we have

$$\xi(\eta) = \Big(\frac{2}{\alpha}, \frac{\beta}{\alpha}\Big)$$

in $\mathbb{G}_a(\mathbb{Q}) \times \mathbb{G}_m(\mathbb{Q}) = \mathbb{Q} \times \mathbb{Q}^\times$, which implies that $\eta \notin \Theta \subset \mathbb{Q} \times \mathbb{Q}^\times$. On the other hand, let p be a prime with $(p, \alpha\beta(\alpha-\beta)) = 1$. Then we obtain

$$\xi(\theta^{p-2}\eta) = \Big(\frac{p}{\alpha}, \frac{\beta^{p-1}}{\alpha^{p-1}}\Big) \equiv (0, 1) = \xi(1) \mod p,$$

as is desired.

Remark 3.12. We adapt the argument developed by Ballot [2, Section 3 and Section 6] to our context. First we recall Ballot's argument, replacing his notations to ours.

Let $\alpha \in \mathbb{Z}$ and $Q(t) \in \mathbb{Z}[t]$, and put $P(t) = (t-\alpha)^2 Q(t)$ and $P(t) = (t-\alpha)Q(t)$. Assume that $Q(t)$ is separable with the factorization $Q(t) = (t-\beta_1)\cdots(t-\beta_m)$ in $\mathbb{C}[t]$ and that $\alpha\beta_1\cdots\beta_m \neq 0$.

The Lucas sequence with the characteristic polynomial has the closed form

$$(\gamma k + \gamma')\alpha^k + \gamma_1\beta_1^k + \cdots + \gamma_m\beta_m^k.$$

Indeed, we have

$$\gamma = \frac{1}{\alpha P_1'(\alpha)},\ \gamma_1 = \frac{1}{P'(\beta_1)}, \dots,\ \gamma_m = \frac{1}{P'(\beta_m)},\ \gamma' = -(\gamma_1 + \cdots + \gamma_m),$$

as is recalled in Remarked 1.7.

Here are some definitons:

(1) the standard form for a sequence $\boldsymbol{w} \in \mathcal{L}(P, \mathbb{Z})$ is defined by

$$w_k = (A\gamma k + A'\gamma')\alpha^k + A_1\gamma_1\beta_1^k + \cdots + A_m\gamma_m\beta_m^k,$$

which is written as $\boldsymbol{w} = \langle A, A', A_1, \dots, A_m\rangle$.

(2) the product of $\boldsymbol{w} = \langle A, A', A_1, \dots, A_m\rangle$ and $\boldsymbol{v} = \langle B, B', B_1, \dots, B_m\rangle$ is defined by

$$\boldsymbol{w}\cdot\boldsymbol{v} = \langle AB, A'B', A_1B_1, \dots, A_mB_m\rangle.$$

(3) we say that $\boldsymbol{w} = \langle A, A', A_1, \dots, A_m\rangle$ and $\boldsymbol{v} = \langle B, B', B_1, \dots, B_m\rangle$ are weakly equivalent (write $\boldsymbol{w} \sim \boldsymbol{w}$) if there exist $q \in \mathbb{Q}$ and $s \in \mathbb{Z}$ such that $qA = B\alpha^s$, $qA_1 = B_1\beta_1^s, \dots, qA_m = B_m\beta_m^s$.

(4) $G(P)$ denotes the set of equivalence classes by the equivalence relation $\sim$ on

$$\{\langle A, A', A_1, \dots, A_m\rangle \in \mathcal{L}(P, \mathbb{Z})\ ;\ AA_1\cdots A_m \neq 0\}.$$

Ballot verifies the following assertions:

(I) ([2, Theorem 4 and Theorem 18]) The projection $\pi : \langle A, A', A_1, \dots, A_m\rangle \mapsto \langle A, A_1, \dots, A_m\rangle$ induces an isomorphism $G(P) \xrightarrow{\sim} G(P_1)$. Here $G(P_1)$ denotes the Laxton group associated to $P_1(t)$ defined by Laxton [6] and Ballot[1].

(II) ([2, Theorem 8]) Let p be a prime, and define $G(P, p)$ as the set of weak equivalence classes in $G(P)$ having p as a maximal divisor. Then the projection map π induces an isomorphism $G(P, p) \xrightarrow{\sim} G(P_1, p)$. Here $G(P_1, p)$ denotes the set of equivalence classes in $G(P_1)$ having p as a maximal divisor, defined by Laxton [6] and Ballot[1].

It would be safe to repair a part of the infrastructure built by Ballot. A standard form for a sequence $\boldsymbol{w} \in \mathcal{L}(P, \mathbb{Z})$ should be defined by

$$w_k = \{A(\gamma k + \gamma') + A'\gamma''\}\alpha^k + A_1\gamma_1\beta_1^k + \cdots + A_m\gamma_m\beta_m^k,$$

where $\gamma'' = 1/P_1'(\alpha)$. Moreover, the product of two sequences $\boldsymbol{w} = \langle A, A', A_1, \dots, A_m\rangle$ and $\boldsymbol{v} = \langle B, B', B_1, \dots, B_m\rangle$ is given by

$$\boldsymbol{w}\cdot\boldsymbol{v} = \langle AB, AB' + A'B, A_1B_1, \dots, A_mB_m\rangle.$$

Now let θ and θ_1 denote the image of t in the residue ring $\mathbb{Q}[t]/(P(t))$ and the image of t in the residue ring $\mathbb{Q}[t]/(P_1(t))$, respectively. Moreover, let Θ and Θ_1 denote the subgroup of $G_{(P)}(\mathbb{Q})$ generated by $\beta(\theta)$ and the subgroup of $G_{(P_1)}(\mathbb{Q})$ generated by $\beta(\theta_1)$, respectively. Then we can verify that $G(P)$ is isomorphic to $G_{(P)}(\mathbb{Q})/(\Theta + \mathrm{Ker}[G_{(P)}(\mathbb{Q}) \to G_{(P_1)}(\mathbb{Q})])$ and $G(P_1)$ to $G_{(P_1)}(\mathbb{Q})/\Theta_1$. It is also readily seen that the projection map $G_{(P)}(\mathbb{Q}) \to G_{(P_1)}(\mathbb{Q})$ induces an isomorphism

$$G_{(P)}(\mathbb{Q})/(\Theta + \mathrm{Ker}[G_{(P)}(\mathbb{Q}) \to G_{(P_1)}(\mathbb{Q})]) \xrightarrow{\sim} G_{(P_1)}(\mathbb{Q})/\Theta_1.$$

Now let p be a prime with $(p, \alpha\beta_1\cdots\beta_m) = 1$. Then it follows from Theorem 3.8 that the projection map $G_{(P)}(\mathbb{Z}/p\mathbb{Z}) \to G_{(P_1)}(\mathbb{Z}/p\mathbb{Z})$ induces an isomorphism

$$G_{(P)}(\mathbb{Z}/p\mathbb{Z})/\Theta \xrightarrow{\sim} G_{(P_1)}(\mathbb{Z}/p\mathbb{Z})/\Theta_1.$$

Hence the exact sequence

$$0 \to (\Theta + \mathrm{Ker}[G_{(P)}(\mathbb{Z}_{(p)}) \to G_{(P_1)}(\mathbb{Z}_{(p)})])/\Theta \to G_{(P)}(\mathbb{Z}_{(p)})/\Theta \to G_{(P_1)}(\mathbb{Z}_{(p)})/\Theta_1 \to 0$$

induces an exact sequence

$$\begin{aligned} 0 \to{}& (\Theta + \mathrm{Ker}[G_{(P)}(\mathbb{Z}_{(p)}) \to G_{(P_1)}(\mathbb{Z}_{(p)})])/\Theta \\ &\to \mathrm{Ker}[G_{(P)}(\mathbb{Z}_{(p)})/\Theta \to G_{(P)}(\mathbb{Z}/p\mathbb{Z})/\Theta] \to \mathrm{Ker}[G_{(P_1)}(\mathbb{Z}_{(p)})/\Theta_1 \to G_{(P_1)}(\mathbb{Z}/p\mathbb{Z})/\Theta_1] \to 0. \end{aligned}$$

Furthermore, by Theorem 2.11, we obtain

$$G(P,p) = \mathrm{Ker}[G_{(P)}(\mathbb{Z}_{(p)})/\Theta \to G_{(P)}(\mathbb{Z}/p\mathbb{Z})/\Theta]/(\Theta + \mathrm{Ker}[G_{(P)}(\mathbb{Z}_{(p)}) \to G_{(P_1)}(\mathbb{Z}_{(p)})])/\Theta$$

and

$$G(P_1,p) = \mathrm{Ker}[G_{(P_1)}(\mathbb{Z}_{(p)})/\Theta_1 \to G_{(P_1)}(\mathbb{Z}/p\mathbb{Z})/\Theta_1].$$

Fortunately, there have not occurred any accidents because the term A' in $\langle A, A', A_1, \dots, A_m\rangle$ is ignored in the theorems established by Ballot.

Finally we present a cross-breed of the Fibonacci sequence and the Cullen sequence as in a rosery.

Example 3.13. Put

$$\begin{aligned} P(t) &= (t-2)^2(t^2-t-1) = t^4 - 5t^3 + 7t^2 - 4, \\ P_1(t) &= (t-2)(t^2-t-1) = t^3 - 3t^2 + t + 2, \\ Q(t) &= t^2 - t - 1. \end{aligned}$$

Let $(F_k)_{k\geq 0}$ denote the Fibonacci sequence, that is to say, $(F_k)_{k\geq 0}$ is defined by the linear recurrence $F_{k+2} = F_{k+1} + F_k$ with the initial terms $F_0 = 0$, $F_1 = 1$. Then the Lucas sequence $(\tilde{F}_k)_{k\geq 0}$ with the characteristic polynomial $P(t)$ is given by

$$\tilde{F}_k = k \cdot 2^{k-1} - 3 \cdot 2^k + F_{k+4}.$$

Let θ and θ_Q denote the images of t in $\mathbb{Z}[t]/(P(t))$ and in $\mathbb{Z}[t]/(t^2 - t - 1)$, respectively. The homomorphism of rings $\xi : \mathbb{Z}[t]/(P(t)) \to \mathbb{Z}[\varepsilon] \times \mathbb{Z}[t]/(t^2 - t - 1)$ by $\xi(\theta) = (2 + \varepsilon, \theta_Q)$, and the homomorphism of group schemes $\xi : G_{(P)} \otimes_{\mathbb{Z}} \mathbb{Z}[1/2] \to (\mathbb{G}_{a,\mathbb{Z}} \times G_Q) \otimes_{\mathbb{Z}} \mathbb{Z}[1/2]$ is given by $\xi(\theta) = (1/2, \theta_Q/2)$. Hence we obtain

$$\Theta = \left\{ \left(\frac{k}{2}, \frac{\theta_Q^k}{2^k} \right) \; ; \; k \in \mathbb{Z} \right\} \subset \mathbb{Q} \times \mathbb{Q}^\times$$

under the identification $\xi : G_{(P)}(\mathbb{Q}) \tilde{\to} \mathbb{G}_a(\mathbb{Q}) \times G_Q(\mathbb{Q}) = \mathbb{Q} \times (\mathbb{Q}[t]/(t^2 - t - 1))^\times$.

Put now

$$\eta = \theta + P_1(\theta) = \theta + (\theta - 2)(\theta^2 - \theta - 1)$$

and

$$(\tilde{C}_k)_{k\geq 0} = \tilde{\omega}(\eta).$$

Then we have

$$\tilde{C}_k = \tilde{L}_{k+1} + 2^k = (k-4)2^k + F_{k+5}$$

for $k \geq 0$. Furthermore, we have

$$\xi(\eta) = \left(1, \frac{\theta_Q}{2}\right)$$

in $\mathbb{G}_a(\mathbb{Q}) \times G_Q(\mathbb{Q}) = \mathbb{Q} \times (\mathbb{Q}[t]/(t^2 - t - 1))^\times$, which implies that $\eta \notin \Theta \subset \mathbb{Q} \times (\mathbb{Q}[t]/(t^2 - t - 1))^\times$. On the other hand, let p be a prime with $(p, 10) = 1$. Then we obtain

$$\xi(\theta^{p^2-2}\eta) = \left(\frac{p^2}{2}, \frac{\theta_Q^{p^2-1}}{2^{p^2-1}} \right) \equiv (0, 1) = \xi(1) \mod p,$$

which implies that

$$\tilde{C}_{p^2-2} \equiv \tilde{C}_{p^2-1} \equiv \tilde{C}_{p^2} \equiv 0 \mod p, \; \tilde{C}_{p^2+1} \equiv 1 \mod p.$$

Furthermore, if $p \equiv 1, 4 \mod 5$, then we obtain

$$\xi(\theta^{p-2}\eta) = \left(\frac{p}{2}, \frac{\theta_Q^{p-1}}{2^{p-1}} \right) \equiv (0, 1) = \xi(1) \mod p,$$

which implies that

$$\tilde{C}_{p-2} \equiv \tilde{C}_{p-1} \equiv \tilde{C}_p \equiv 0 \mod p, \; \tilde{C}_{p+1} \equiv 1 \mod p.$$

References.

[1] C. Ballot, Density of prime divisors of linear recurrences. Memoir of the A. M. S. 115 (1995)

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

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

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

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

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

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

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

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

[10] N. Suwa, Geometric aspects of Lucas sequences, A survey. Preprint series No.126, Department of Mathematics, Chuo University (2019)

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

[12] M. Ward, The maximal prime divisors of linear recurrences. Canadian J. Math. 6 (1954) 455–462

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

Department of Mathematics, Chuo University, 1-13-27 Kasuga,
Bunkyo-ku, Tokyo 112-8551, JAPAN
E-mail address: suwa@math.chuo-u.ac.jp