CHUO MATH NO.122(2018)

GEOMETRIC ASPECTS OF LUCAS SEQUENCES, I

by

NORIYUKI SUWA

DEPARTMENT OF MATHEMATICS
CHUO UNIVERSITY
BUNKYOKU TOKYO JAPAN

Mar. 24 , 2018

GEOMETRIC ASPECTS OF LUCAS SEQUENCES, I

NORIYUKI SUWA*)

Abstract. We present a way of viewing Lucas sequences in the framework of group scheme theory. This enables us to treat the Lucas sequences from a geometric and functorial viewpoint, which was suggested by Laxton ⟨On groups of linear recurrences, I⟩ and by Aoki-Sakai ⟨Mod p equivalence classes of linear recurrence sequences of degree two⟩.

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 intial 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 sequnces $(L_k)_{k\geq 0}$ 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 [6] as the laws of apparition and repetition in the case where m is a prime number and $(w_k)_{k\geq 0}$ is the Lucas sequence, and there have been piled up various kinds of results after then.

In this article we study the divisibility problem for Lucas sequences from a geometirc viewpoint, translating several descriptions on Lucas sequences into the language of affine group schemes. For example, the laws of apparition and repetition is formulated in our context as follows:

Theorem(=Proposition 3.23+Theorem 3.25) *Let P and Q be non-zero integers with $(P, Q) = 1$, and let $w_0, w_1 \in \mathbb{Z}$ with $(w_0, w_1) = 1$. Define the sequence $(w_k)_{k\geq 0}$ by the recurrence relation $w_{k+2} = Pw_{k+1} - Qw_k$ with initial terms w_0 and w_1, and put $\mu = \mathrm{ord}_p(w_1^2 - Pw_0w_1 + Qw_0^2)$. Let p be an odd prime with $(p, Q) = 1$ and n a positive integer. Then we have*

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

Furthermore, there exists $k \geq 0$ such that $w_k \equiv 0 \mod p^n$ if and only if $(w_0 : w_1) \in (0 : 1).\Theta$ in $\mathbb{P}^1(\mathbb{Z}/p^n\mathbb{Z})$. Here Θ denotes the subgroup of $G_{(D)}(\mathbb{Z}_{(p)})$ generated by $\beta(\theta) = (P/4Q, 1/4Q)$, and $r(p^\nu)$ denotes the rank mod p^ν of the Lucas sequence associated to (P, Q).

*) Partially supported by Grant-in-Aid for Scientific Research No.26400024

2010 *Mathematics Subject Classification* Primary 13B05; Secondary 14L15, 12G05.

Now we explain a main policy of the article. Let D be a non-square integer. Put $U(\mathbb{Q}(\sqrt{D})) = \{\alpha \in \mathbb{Q}(\sqrt{D})\ ;\ \mathrm{Nr}\,\alpha = 1\}$, and define a homomorphism of multiplicative groups $\gamma : \mathbb{Q}(\sqrt{D})^\times \to U(\mathbb{Q}(\sqrt{D}))$ by $\gamma(\alpha) = \alpha/\bar{\alpha}$. Here $\bar{\alpha} \in \mathbb{Q}(\sqrt{D})$ denotes the conjugate of α. Then, by Hilbert 90, γ induces an isomorphism $\mathbb{Q}(\sqrt{D})^\times/\mathbb{Q}^\times \xrightarrow{\sim} U(\mathbb{Q}(\sqrt{D}))$, which is useful to study arithmetic of quadratic number fields and also Lucas sequences. It is our main idea to interpret the isomorphism $\mathbb{Q}(\sqrt{D})^\times/\mathbb{Q}^\times \xrightarrow{\sim} U(\mathbb{Q}(\sqrt{D}))$ through the exact sequence of affine group schemes

$$0 \longrightarrow \mathbb{G}_{m,\mathbb{Z}} \longrightarrow \prod_{\mathbb{Z}[\sqrt{D}]/\mathbb{Z}} \mathbb{G}_{m,\mathbb{Z}[\sqrt{D}]} \xrightarrow{\beta} \prod_{\mathbb{Z}[\sqrt{D}]/\mathbb{Z}} \mathbb{G}_{m,\mathbb{Z}[\sqrt{D}]}/\mathbb{G}_{m,\mathbb{Z}} \longrightarrow 0,$$

under the identifications

$$\begin{aligned} \mathbb{Q}^\times &= \mathbb{G}_m(\mathbb{Q}), \\ \mathbb{Q}(\sqrt{D})^\times &= \Big(\prod_{\mathbb{Z}[\sqrt{D}]/\mathbb{Z}} \mathbb{G}_{m,\mathbb{Z}[\sqrt{D}]}\Big)(\mathbb{Q}), \\ \mathbb{Q}(\sqrt{D})^\times/\mathbb{Q}^\times &= \Big(\prod_{\mathbb{Z}[\sqrt{D}]/\mathbb{Z}} \mathbb{G}_{m,\mathbb{Z}[\sqrt{D}]}/\mathbb{G}_{m,\mathbb{Z}}\Big)(\mathbb{Q}), \\ U(\mathbb{Q}(\sqrt{D})) &= U_D(\mathbb{Q}). \end{aligned}$$

Here the group scheme U_D is defined by the exact sequence of affine group schemes

$$0 \longrightarrow U_D \longrightarrow \prod_{\mathbb{Z}[\sqrt{D}]/\mathbb{Z}} \mathbb{G}_{m,\mathbb{Z}[\sqrt{D}]} \xrightarrow{\mathrm{Nr}} \mathbb{G}_{m,\mathbb{Z}} \longrightarrow 0$$

and related to $\prod_{\mathbb{Z}[\sqrt{D}]/\mathbb{Z}} \mathbb{G}_{m,\mathbb{Z}[\sqrt{D}]}/\mathbb{G}_{m,\mathbb{Z}}$ by a homomorphism

$$\alpha : \prod_{\mathbb{Z}[\sqrt{D}]/\mathbb{Z}} \mathbb{G}_{m,\mathbb{Z}[\sqrt{D}]}/\mathbb{G}_{m,\mathbb{Z}} \to U_D.$$

Our method has a great merit to clarify the argument from a functorial viewpoint. For example, for a prime p and a positive integer n, the exact sequence

$$0 \longrightarrow \mathbb{G}_{m,\mathbb{Z}} \longrightarrow \prod_{\mathbb{Z}[\sqrt{D}]/\mathbb{Z}} \mathbb{G}_{m,\mathbb{Z}[\sqrt{D}]} \xrightarrow{\beta} \prod_{\mathbb{Z}[\sqrt{D}]/\mathbb{Z}} \mathbb{G}_{m,\mathbb{Z}[\sqrt{D}]}/\mathbb{G}_{m,\mathbb{Z}} \longrightarrow 0$$

yields a commutative diagram with exact rows

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

which allows us to change stages freely. It is worth while to mention that, in the case of $n = 1$, the lowest row gives an exact sequence

$$0 \longrightarrow \mathbb{F}_p^\times \xrightarrow{\text{diagonal}} \mathbb{F}_p^\times \times \mathbb{F}_p^\times \xrightarrow{\text{ratio}} \mathbb{F}_p^\times \longrightarrow 0$$

if $\left(\dfrac{D}{p}\right) = 1$, and an exact sequence

$$0 \longrightarrow \mathbb{F}_p^\times \overset{\text{inclusion}}{\longrightarrow} \mathbb{F}_p(\sqrt{D})^\times \overset{\gamma}{\longrightarrow} U(\mathbb{F}_p(\sqrt{D})) \longrightarrow 0$$

if $\left(\dfrac{D}{p}\right) = -1$. These sequences are very often used in the study on Lucas sequences.

The translation work of this sort is almost done in the previous aricle [11], however a more systematic argument is developed in this article because [11] lacks detailed considerations in the ramified cases.

Next we explain the organization of the article. The description is expository and self-contained for the reader's convenience. The Sections 1 and 2 are devoted to the construction of infrastructure. In the Section 1, we introduce the affine group schemes denoted by G_D, U_D and $G_{(D)}$, giving full explantion on the groups of $\mathbb{Q}$-rational points, $\mathbb{F}_p$-rational points and $\mathbb{Z}_{(p)}$-valued points.

In the first half of Section 2, we give full explantion on $G_D(\mathbb{Z}_p)$, $U_D(\mathbb{Z}_p)$ and $G_{(D)}(\mathbb{Z}_p)$ and deduce description on $G_D(\mathbb{Z}/p^n\mathbb{Z})$, $U_D(\mathbb{Z}/p^n\mathbb{Z})$ and $G_{(D)}(\mathbb{Z}/p^n\mathbb{Z})$ for $n \geq 2$. In the latter half of Section 2, we define an homomorphism of group schemes $\underline{p}^n : G_{(p^{2n}D)} \to G_{(D)}$, which gives a description of the kernel of the reduction map $G_{(D)}(\mathbb{Z}_{(p)}) \to G_{(D)}(\mathbb{Z}/p^n\mathbb{Z})$.

In the first half of Section 3, after relating Lucas sequences with the group schems G_D and $G_{(D)}$, we present an interpretation on the notion of rank and period for Lucas sequences in our context. Moreover, we give new proofs for more or less known facts, some of which go back to Lucas [6], Carmichael [2] and Lehmer [9], for example. In the latter half of Section 3, we reformulate and generalize remarkable results of Aoki-Sakai [1], which suggests a way to treat Lucas sequences geometrically.

In the Section 4, we reconstruct the theory developed in [7] and [8] by Laxton, who defined an interesting group $G(f)$ so that the divisibility problem for Lucas sequences might be dealt with systematically. For example, we give an explicit description of the group $G(f)$ as follows:

Theorem(=Theorem 4.2) *Let P and Q be non-zero integers with $(P, Q) = 1$, and put $f(t) = t^2 - Pt + Q$. Let p be an odd prime, and let Θ denote the subgroup of $G_{(D)}(\mathbb{Q})$ generated by $\beta(\theta) = (P/4Q, 1/4Q)$. Then the isomorphism $\omega : G_{(D)}(\mathbb{Q}) \overset{\sim}{\to} \mathcal{L}(f, \mathbb{Q})^\times/\mathbb{Q}^\times$ induces an isomorphism $\omega : G_{(D)}(\mathbb{Q})/\Theta \overset{\sim}{\to} G(f)$.*

Laxton's work is pioneering, but seems unfortunately ignored and forgotten. A main reason may be that Laxton did not give an explicit description of $G(f)$. It would be surprising that we can describe the groups $G(f)$, $H(f, p)$, $K(f, p)$ and $G(f, p^n)$ $(n \geq 1)$ defined by Laxton through the groups $G_{(D)}(\mathbb{Q}) = U_D(\mathbb{Q})$, $U_D(\mathbb{Z}_{(p)})$, $G_{(D)}(\mathbb{Z}_{(p)})$ and $G_{(p^{2n}D)}(\mathbb{Z}_{(p)})$ $(n \geq 1)$, as is shown in Theorem 4.2 and Corollaries 4.3 and 4.9.

The last three subsections form the coda of the Section 4. We summarize there argument on the divisibilty problem for Lucas sequences, recalling the related results established by Ward [12] and Laxton [7].

We conclude the introduction by referring to a related work by Ward [12]. He investigated Lucas sequences defined for p-adic integers, using systematically the p-adic logarithmic function. His method is essentially equivalent to ours employed in the Section 2. However, we put p-adic hyperbolic functions in the central position, looking back *l'esprit de Lucas*. Indeed, his bigbang article [6] on Lucas sequeces is begun by the following phrase: Ce mémoire a pour objet l'étude des fonctions symétriques des racines d'une équation du second degré, et son application à la théorie des nombres premiers. Nous indiquons dès le commencement, l'analogie complète de ces fonctions symétriques avec les fonctions circulaires et hyperboliques; ...

The author would like to express his hearty thanks to Miho Aoki for her introducing Laxton's work and related articles. The assertion of Theorem 4.2 is estabished by Aoki independently in the case of $Q = \pm 1$. He is very grateful to Akira Masuoka, who gave him an opportunity to give a talk at Tsukuba under the title $\langle$How would Grothendieck have treated the Fibonacci sequences?$\rangle$.

Notation

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

For a scheme X and a commutative group scheme G over X, $H^*(X, G)$ denotes the cohomology group with respect to the fppf-topology. It is known that, if G is smooth over X, the fppf-cohomology group coincides with the étale cohomology group (Grothendieck [4, III.11.7]).

List of sets and rings

$A_D = \mathbb{Z}[t]/(t^2 - D)$: defined in 1.1

$A_{(P,Q)} = \mathbb{Z}[t]/(t^2 - Pt + Q)$: defined in 3.1

$\mathcal{L}(f, R)$: defined in 3.1

$\mathcal{R}(f, \mathbb{Z})$: defined in 3.27

List of groups and group schemes

$\mathbb{G}_{a,A}$: the additive group scheme over A

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

$\boldsymbol{\mu}_{n,A}$: $\mathrm{Ker}[n : \mathbb{G}_{m,A} \to \mathbb{G}_{m,A}]$

$G_D = \prod_{A_D/\mathbb{Z}} \mathbb{G}_{m,A_D}$: the Weil restriction of $\mathbb{G}_m$ with respect to $A_D/\mathbb{Z}$, recalled in 1.1

$U_D = \mathrm{Ker}[\mathrm{Nr} : \prod_{A_D/\mathbb{Z}} \mathbb{G}_{m,A_D} \to \mathbb{G}_{m,\mathbb{Z}}]$: recalled in 1.1

$G_{(D)} = \prod_{A_D/\mathbb{Z}} \mathbb{G}_{m,A_D}/\mathbb{G}_{m,\mathbb{Z}}$: recalled in 1.7

$\Theta \subset G_D(\mathbb{Z}[1/Q])$: defined in 3.19

$\Theta \subset G_{(D)}(\mathbb{Z}[1/Q])$: defined in 3.19

$\Theta \subset PGL(2, \mathbb{Z}[1/Q])$: defined in 3.20

List of maps and morphisms

$\mathrm{Nr} : G_D \to \mathbb{G}_{m,\mathbb{Z}}$**:** defined in 1.1

$\xi : G_{D,R} \to \mathbb{G}_{m,R}$**:** defined in 1.3 if D is a square in R

$\xi : U_{D,R} \to \mathbb{G}_{m,R}$**:** defined in 1.3 if D is a square in R

$\iota : \mathbb{G}_{a,\mathbb{F}_p} \to G_{D,\mathbb{F}_p}$**:** defined in 1.6 if $p|D$

$\iota : \mathbb{G}_{a,\mathbb{F}_p} \to U_{D,\mathbb{F}_p}$**:** defined in 1.6 if $p|D$

$\varepsilon : U_{D,\mathbb{F}_p} \to \boldsymbol{\mu}_{2,\mathbb{F}_p}$**:** defined in 1.6 if $p|D$

$i : \mathbb{G}_{m,\mathbb{Z}} \to G_D$**:** defined in 1.7

$\beta : G_D \to G_{(D)}$**:** defined in 1.7

$\alpha : G_{(D)} \to U_D$**:** defined in 1.7

$\gamma = \alpha \circ \beta : G_D \to U_D$**:** defined in 1.7

$\tilde{\varepsilon} : U_D(\mathbb{Z}_{(p)}) \to \{\pm 1\}$**:** defined in 1.12 if $p|D$ and $p \neq 2$

$\omega_R : R \otimes_{\mathbb{Z}} A_{(P,Q)} \to R$**:** defined in 3.1

$\omega_R : R \otimes_{\mathbb{Z}} A_{(P,Q)} \to \mathcal{L}(f,R)$**:** defined in 3.1

$\omega_R : R \otimes_{\mathbb{Z}} A_{(D)} \to \mathcal{L}(f,R)$**:** defined in 3.7

$\omega_R : G_D(R) \to \mathcal{L}(f,R)$**:** defined in 3.7

$\omega_R : G_{(D)}(R) \to \mathbb{P}^1(R)$**:** defined in 3.26

List of sequences and invariants

$\boldsymbol{L} = (L_k)_{k\geq 0}$**:** the Lucas sequence assocaited to (P,Q), recalled in 3.4

$\boldsymbol{S} = (S_k)_{k\geq 0}$**:** the companion Lucas sequence assocaited to (P,Q), recalled in 3.7

$r(m)$**:** the rank mod m of the Lucas sequence $(L_k)_{k\geq 0}$, recalled in 3.9

$k(m)$**:** the period mod m of the Lucas sequence $(L_k)_{k\geq 0}$, recalled in 3.9

$\mathit{\Delta}(\boldsymbol{w}) = w_1^2 - Pw_0w_1 + Qw_0^2$**:** the invariant of $\boldsymbol{w} = (w_k)_{k\geq 0} \in \mathcal{L}(f,R)$, recalled in 3.6

1. Group schemes G_D, U_D and $G_{(D)}$

Throughout the section, we fix a *non-zero integer D*. We refer to [3] or [13] on formalisms of affine group schemes, Hopf algebras and the cohomology with coefficients in group schemes.

From 1.1 to 1.6, we recall a definition of the affine group schemes G_D and U_D with full explanation on the groups of $\mathbb{Q}$-rational points, $\mathbb{F}_p$-rational points and $\mathbb{Z}_{(p)}$-valued points.

Definition 1.1. Let D be a non-zero integer, and put

$$A_D = \mathbb{Z}[t]/(t^2 - D),$$

$$G_D = \prod_{A_D/\mathbb{Z}} \mathbb{G}_{m,A_D} \text{ (the Weil restriction of } \mathbb{G}_m \text{ with respect to the ring extension } A_D/\mathbb{Z})$$

More explicitly,

$$G_D = \operatorname{Spec} \mathbb{Z}[U, V, \frac{1}{U^2 - DV^2}],$$

and the group law of G_D is given by

$$\begin{aligned}
\mathit{\Delta} &: (U,V) \mapsto (U\otimes U + DV\otimes V, U\otimes V + V\otimes U),\\
\varepsilon &: (U,V) \mapsto (1,0),\\
S &: (U,V) \mapsto \big(\frac{U}{U^2-DV^2}, \frac{-V}{U^2-DV^2}\big).
\end{aligned}$$

Furthermore, a homomorphism of affine group schemes

$$\mathrm{Nr} : G_D = \mathrm{Spec}\,\mathbb{Z}[U,V,\frac{1}{U^2-DV^2}] \to \mathbb{G}_{m,\mathbb{Z}} = \mathrm{Spec}\,\mathbb{Z}[T,\frac{1}{T}]$$

is defined by

$$T \mapsto U^2 - DV^2 : \mathbb{Z}[T,\frac{1}{T}] \to \mathbb{Z}[U,V,\frac{1}{U^2-DV^2}].$$

Put now $U_D = \mathrm{Ker}[\mathrm{Nr} : G_D \to \mathbb{G}_{m,\mathbb{Z}}]$. More precisely,

$$U_D = \mathrm{Spec}\,\mathbb{Z}[U,V]/(U^2-DV^2-1),$$

and the group law of U_D is given by

$$\begin{aligned}
\mathit{\Delta} &: (U,V) \mapsto (U\otimes U + DV\otimes V, U\otimes V + V\otimes U),\\
\varepsilon &: (U,V) \mapsto (1,0),\\
S &: (U,V) \mapsto (U,-V).
\end{aligned}$$

For the convenience, here is given a more concrete description of 1.1.

Remark 1.2. Let R be a commutative ring. Then we have

$$G_D(R) = (R[t]/(t^2-D))^\times = \{(u,v)\in R^2\ ;\ u^2-Dv^2 \text{ is invertible in } R\},$$

identifying (u,v) to $u+v\delta$. Here δ denotes the image of t in $R[t]/(t^2-D)$. The multiplication of $G_D(R)$ is given by

$$(u,v)(u',v') = (uu'+Dvv', uv'+u'v).$$

The unit of $G_D(R)$ is given by $(1,0)$, and we have

$$(u,v)^{-1} = \Big(\frac{u}{u^2-Dv^2}, -\frac{v}{u^2-Dv^2}\Big).$$

Furthermore, for $(u,v)\in G_D(R)$, we have

$$\mathrm{Nr}(u,v) = u^2 - Dv^2,$$

and therefore,

$$U_D(R) = \mathrm{Ker}[\mathrm{Nr} : G_D(R) \to \mathbb{G}_m(R) = R^\times] = \{(u,v)\in R^2\ ;\ u^2-Dv^2 = 1\}.$$

Remark 1.3. Let R be a ring, and assume that D is a square in R. Take $r\in R$ such that $D=r^2$, and define a homomorphism of group schemes

$$\xi : G_{D,R} = \mathrm{Spec}\,R[U,V,\frac{1}{U^2-DV^2}] \to \mathbb{G}^2_{m,R} = \mathrm{Spec}\,R[T_1,T_2,\frac{1}{T_1},\frac{1}{T_2}]$$

by

$$(T_1,T_2)\mapsto(U+rV,U-rV):R[T_1,T_2,\frac{1}{T_1},\frac{1}{T_2}]\to R[U,V,\frac{1}{U^2-DV^2}],$$

and a homomorphism of group schemes

$$\xi:U_D=\operatorname{Spec}R[U,V]/(U^2-DV^2-1)\to\mathbb{G}_{m,\mathbb{Z}}=\operatorname{Spec}R[T,\frac{1}{T}]$$

by

$$T\mapsto U+rV:R[T,\frac{1}{T}]\to R[U,V]/(U^2-DV^2-1),$$

respectively. Then we obtain a commutative diagram with exact rows

$$\begin{tikzcd}
0 \arrow[r] & U_{D,R} \arrow[r] \arrow[d, "\xi"] & G_{D,R} \arrow[r, "\mathrm{Nr}"] \arrow[d, "\xi"] & \mathbb{G}_{m,R} \arrow[r] \arrow[d, equal] & 0 \\
0 \arrow[r] & \mathbb{G}_{m,R} \arrow[r, "\iota"'] & \mathbb{G}^2_{m,R} \arrow[r, "\mu"'] & \mathbb{G}_{m,R} \arrow[r] & 0
\end{tikzcd},$$

where $\iota:\mathbb{G}_{m,R}\to\mathbb{G}^2_{m,R}$ is defined by $(T_1,T_2)\mapsto(T,1/T)$ and $\mu:\mathbb{G}^2_{m,R}\to\mathbb{G}_{m,R}$ denotes the multiplication. Furthermore, the homomorphisms $\xi:G_D\to\mathbb{G}^2_{m,R}$ and $\xi:U_D\to\mathbb{G}_{m,R}$ are both isomorphic over $R\otimes_{\mathbb{Z}}\mathbb{Z}[1/2D]$.

In particular, if D is a square in $\mathbb{Z}$, we obtain a commutative diagram with exact rows

$$\begin{tikzcd}
0 \arrow[r] & U_D(\mathbb{Z}_{(p)}) \arrow[r] \arrow[d, "\wr\,\xi"] & U_D(\mathbb{Q}) \arrow[r] \arrow[d, "\wr\,\xi"] & \mathbb{Z} \arrow[r] \arrow[d, equal] & 0 \\
0 \arrow[r] & \mathbb{Z}^\times_{(p)} \arrow[r] & \mathbb{Q}^\times \arrow[r, "\mathrm{ord}_p"'] & \mathbb{Z} \arrow[r] & 0
\end{tikzcd}$$

for each prime p with $(p,2D)=1$.

Remark 1.4. Assume that D is not a square. Then by definition we have

$$U_D(\mathbb{Q})=\{\alpha\in\mathbb{Q}(\sqrt{D})\ ;\ \mathrm{Nr}\,\alpha=1\}$$

and

$$U_D(\mathbb{Z}_{(p)})=\{\alpha\in\mathbb{Z}_{(p)}[\sqrt{D}]\ ;\ \mathrm{Nr}\,\alpha=1\}$$

for each prime p.

Furthermore, let $\mathcal{O}_D$ denote the ring of integers in $\mathbb{Q}(\sqrt{D})$. We obtain

$$U_D(\mathbb{Z}_{(p)})=\{\alpha\in\mathbb{Q}(\sqrt{D})\ ;\ \mathrm{Nr}\,\alpha=1\text{ and }\mathrm{ord}_{\mathfrak{p}}\alpha=0\text{ for each prime }\mathfrak{p}\text{ of }\mathbb{Q}(\sqrt{D})\text{ over }p\},$$

assuming $\mathbb{Z}_{(p)}[\sqrt{D}]=\mathbb{Z}_{(p)}\otimes_{\mathbb{Z}}\mathcal{O}_D$. This is the case if $p\neq 2$ and $\mathrm{ord}_pD\leq 1$.

Proposition 1.5. *Let p be a prime. Then:*

(1) *If $\left(\dfrac{D}{p}\right)=1$, then we have an exact sequence*

$$0\longrightarrow U_D(\mathbb{Z}_{(p)})\longrightarrow U_D(\mathbb{Q})\longrightarrow\mathbb{Z}\longrightarrow 0.$$

(2) *If $\left(\dfrac{D}{p}\right)=-1$, then the canonical homomorphism $U_D(\mathbb{Z}_{(p)})\to U_D(\mathbb{Q})$ is bijective.*

(3) *If $p \neq 2$, $p|D$ and $\mathrm{ord}_p D = 1$, then the canonical homomorphism $U_D(\mathbb{Z}_{(p)}) \to U_D(\mathbb{Q})$ is bijective.*

Proof. (1) The assertion is verified in Remark 1.3 if D is a square.

Assume now that D is not a square. Let $\mathfrak{p}$ be a prime ideal of $\mathbb{Q}(\sqrt{D})$ over p. Then $\alpha \mapsto \mathrm{ord}_{\mathfrak{p}}\alpha$ defines a homomorphism $U_D(\mathbb{Q}) \to \mathbb{Z}$. Furthermore, the sequence

$$0 \longrightarrow U_D(\mathbb{Z}_{(p)}) \longrightarrow U_D(\mathbb{Q}) \xrightarrow{\mathrm{ord}_{\mathfrak{p}}} \mathbb{Z} \longrightarrow 0$$

is exact.

Indeed, let $\alpha \in \mathbb{Q}(\sqrt{D})$ with $\mathrm{Nr}\,\alpha = 1$ and $\mathrm{ord}_{\mathfrak{p}}\alpha = 0$. Then we obtain $\mathrm{ord}_{\mathfrak{p}}\bar{\alpha} = 0$, and therefore, $\mathrm{ord}_{\bar{\mathfrak{p}}}\alpha = 0$. Here $\bar{\alpha}$ denotes the conjugate of α, and $\bar{\mathfrak{p}}$ denotes the conjugate of $\mathfrak{p}$. This implies $\alpha \in \mathbb{Z}_{(p)}[\sqrt{D}]$. Hence, by Remark 1.4, we obtain

$$U_D(\mathbb{Z}_{(p)}) = \mathrm{Ker}[\mathrm{ord}_{\mathfrak{p}} : U_D(\mathbb{Q}) \to \mathbb{Z}].$$

Now take $\pi \in \mathbb{Q}(\sqrt{D})$ such that $\mathrm{ord}_{\mathfrak{p}}\pi = 1$ and $\mathrm{ord}_{\bar{\mathfrak{p}}}\pi = 0$, and put $\alpha = \pi/\bar{\pi}$. Then we obtain $\mathrm{Nr}\,\alpha = 1$ and $\mathrm{ord}_{\mathfrak{p}}\alpha = 1$. It follows that $\mathrm{ord}_{\mathfrak{p}} : U_D(\mathbb{Q}) \to \mathbb{Z}$ is surjective.

(2)(3) Let $\mathfrak{p}$ be the prime ideal of $\mathbb{Q}(\sqrt{D})$ over p. Then, for any $\alpha \in \mathbb{Q}(\sqrt{D})$ with $\mathrm{Nr}\,\alpha = 1$, we have $\mathrm{ord}_{\mathfrak{p}}\alpha = 0$. This implies $\alpha \in \mathbb{Z}_{(p)}[\sqrt{D}]$. Hence, again by Remark 1.4, we obtain $U_D(\mathbb{Z}_{(p)}) = U_D(\mathbb{Q})$.

Remark 1.6. Let p be a prime. Then by definition we have

$$G_D(\mathbb{F}_p) = \Big(\mathbb{F}_p[U, V, \frac{1}{U^2 - DV^2}]\Big)^{\times} = \{(u, v) \in \mathbb{F}_p^2 \,;\, u^2 - Dv^2 \neq 0\}$$

and

$$U_D(\mathbb{F}_p) = \{(u, v) \in \mathbb{F}_p^2 \,;\, u^2 - Dv^2 = 1\}.$$

First assume that $(p, 2D) = 1$. Then:

(1) If $\left(\dfrac{D}{p}\right) = 1$, then $G_D(\mathbb{F}_p)$ is isomorphic to $\mathbb{F}_p^\times \times \mathbb{F}_p^\times$, and $U_D(\mathbb{F}_p)$ is isomorphic to the multiplicative group $\mathbb{F}_p^\times$, as is remarked in 1.3. It follows that $U_D(\mathbb{F}_p)$ is a cyclic group of order $p - 1$.

(2) If $\left(\dfrac{D}{p}\right) = -1$, then $G_D(\mathbb{F}_p)$ is isomorphic to the multiplicative group $\mathbb{F}_p(\sqrt{D})^\times$, and $U_D(\mathbb{F}_p)$ is isomorphic to $\mathrm{Ker}[\mathrm{Nr} : \mathbb{F}_p(\sqrt{D})^\times \to \mathbb{F}_p^\times]$. It follows that $U_D(\mathbb{F}_p)$ is a cyclic group of order $p + 1$.

Hereafter we assume that D is divisible by p. Then

$$G_{D,\mathbb{F}_p} = \mathrm{Spec}\,\mathbb{F}_p[U, V, \frac{1}{U}]$$

and

$$U_{D,\mathbb{F}_p} = \mathrm{Spec}\,\mathbb{F}_p[U, V]/(U^2 - 1),$$

both with the multiplication

$$\varDelta : (U, V) \mapsto (U \otimes U, U \otimes V + V \otimes U).$$

Furthermore, homomorphisms of group schemes over $\mathbb{F}_p$

$$\iota : \mathbb{G}_{a,\mathbb{F}_p} = \operatorname{Spec} \mathbb{F}_p[T] \to G_{D,\mathbb{F}_p} = \operatorname{Spec} \mathbb{F}_p[U, V, \frac{1}{U}]$$

and

$$\iota : \mathbb{G}_{a,\mathbb{F}_p} = \operatorname{Spec} \mathbb{F}_p[T] \to U_{D,\mathbb{F}_p} = \operatorname{Spec} \mathbb{F}_p[U, V]/(U^2 - 1)$$

are defined by

$$U \mapsto 1,\ V \mapsto T : \mathbb{F}_p[U, V, \frac{1}{U}] \to \mathbb{F}_p[T]$$

and by

$$U \mapsto 1,\ V \mapsto T : \mathbb{F}_p[U, V]/(U^2 - 1) \to \mathbb{F}_p[T],$$

respectively. The homomorphisms $\iota : \mathbb{G}_{a,\mathbb{F}_p} \to G_{D,\mathbb{F}_p}$ and $\iota : \mathbb{G}_{a,\mathbb{F}_p} \to U_{D,\mathbb{F}_p}$ are closed immersions, inducing a commutative diagram of group schemes over $\mathbb{F}_p$ with exact rows and columns

$$\begin{tikzcd}
 & & 0 \arrow[d] & 0 \arrow[d] & \\
0 \arrow[r] & \mathbb{G}_{a,\mathbb{F}_p} \arrow[r, "\iota"] \arrow[d, equal] & U_{D,\mathbb{F}_p} \arrow[r, "\varepsilon"] \arrow[d] & \boldsymbol{\mu}_{2,\mathbb{F}_p} \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & \mathbb{G}_{a,\mathbb{F}_p} \arrow[r, "\iota"] & G_{D,\mathbb{F}_p} \arrow[r, "\varepsilon"] \arrow[d, "\mathrm{Nr}"] & \mathbb{G}_{m,\mathbb{F}_p} \arrow[r] \arrow[d, "\mathrm{square}"] & 0 \\
 & & \mathbb{G}_{m,\mathbb{F}_p} \arrow[r, "\mathrm{id}"] \arrow[d] & \mathbb{G}_{m,\mathbb{F}_p} \arrow[d] & \\
 & & 0 & 0 &
\end{tikzcd}$$

In particular, taking the $\mathbb{F}_p$-rational points, we obtain a commutative diagram with exact rows and columns

$$\begin{tikzcd}
 & & 0 \arrow[d] & 0 \arrow[d] & \\
0 \arrow[r] & \mathbb{F}_p \arrow[r, "\iota"] \arrow[d, equal] & U_D(\mathbb{F}_p) \arrow[r, "\varepsilon"] \arrow[d] & \boldsymbol{\mu}_2(\mathbb{F}_p) \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & \mathbb{F}_p \arrow[r, "\iota"] & G_D(\mathbb{F}_p) \arrow[r, "\varepsilon"] \arrow[d, "\mathrm{Nr}"] & \mathbb{F}_p^\times \arrow[r] \arrow[d, "\mathrm{square}"] & 0 \\
 & & \mathbb{F}_p^\times \arrow[r, "\mathrm{id}"] \arrow[d] & \mathbb{F}_p^\times \arrow[d] & \\
 & & 0 & 0 &
\end{tikzcd}$$

More concretely, the maps $\varepsilon : U_D(\mathbb{F}_p) \to \boldsymbol{\mu}_2(\mathbb{F}_p)$ and $\varepsilon : G_D(\mathbb{F}_p) \to \mathbb{G}_m(\mathbb{F}_p) = \mathbb{F}_p^\times$ are given by $(u, v) \mapsto u$.

It follows also that, if $p \neq 2$, then $U_D(\mathbb{F}_p)$ is cyclic of order $2p$ and $G_D(\mathbb{F}_p)$ is cyclic of order $(p-1)p$.

From 1.7 to 1.9, we recall a definition of the affine group schemes $G_{(D)}$ with full explanation on the groups of $\mathbb{Q}$-rational points, $\mathbb{F}_p$-rational points and $\mathbb{Z}_{(p)}$-valued points.

Definition 1.7. We put

$$G_{(D)} = G_D/\mathbb{G}_{m,\mathbb{Z}} = \prod_{A_D/\mathbb{Z}} \mathbb{G}_{m,A_D}/\mathbb{G}_{m,\mathbb{Z}}.$$

More explicitly,

$$G_{(D)} = \operatorname{Spec} \mathbb{Z}[X, Y]/(X^2 - DY^2 - Y)$$

with the group structure:

$$\varDelta : (X, Y) \mapsto (X \otimes 1 + 1 \otimes X + 2DX \otimes Y + 2DY \otimes X, Y \otimes 1 + 1 \otimes Y + 2DY \otimes Y + 2X \otimes X),$$
$$\varepsilon : (X, Y) \mapsto (0, 0),$$
$$S : (X, Y) \mapsto (-X, Y),$$

as is estabished by Waterhouse-Weisfeiler [14]. The group scheme $G_{(D)}$ is smooth over $\mathbb{Z}$.

The canonical surjective homomorphism of group schemes

$$\beta : G_D = \operatorname{Spec} \mathbb{Z}[U, V, \frac{1}{U^2 - DV^2}] \to G_{(D)} = \operatorname{Spec} \mathbb{Z}[X, Y]/(X^2 - DY^2 - Y)$$

is defined by

$$X \mapsto \frac{UV}{U^2 - DV^2},\ Y \mapsto \frac{V^2}{U^2 - DV^2} : \mathbb{Z}[X, Y]/(X^2 - DY^2 - Y) \to \mathbb{Z}[U, V, \frac{1}{U^2 - DV^2}].$$

Indeed,

$$X \mapsto T,\ Y \mapsto 0 : \mathbb{Z}[U, V, \frac{1}{U^2 - DV^2}]/(UV, V^2) \to \mathbb{Z}[T, \frac{1}{T}]$$

gives rise to an isomorphism

$$\mathbb{G}_{m,\mathbb{Z}} = \operatorname{Spec} \mathbb{Z}[T, \frac{1}{T}] \xrightarrow{\sim} \operatorname{Ker}[\beta : G_D \to G_{(D)}] = \operatorname{Spec} \mathbb{Z}[U, V, \frac{1}{U^2 - DV^2}]/(UV, V^2).$$

Hence we obtain an exact sequence of group schemes

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

as is desired. Here the homomorphism of group schemes

$$i : \mathbb{G}_{m,\mathbb{Z}} = \operatorname{Spec} \mathbb{Z}[T, \frac{1}{T}] \to G_D = \operatorname{Spec} \mathbb{Z}[U, V, \frac{1}{U^2 - DV^2}]$$

is defined by

$$(U, V) \mapsto (T, 0) : \mathbb{Z}[U, V, \frac{1}{U^2 - DV^2}] \to \mathbb{Z}[T, \frac{1}{T}].$$

Moreover, a homomorphism of affine group schemes

$$\alpha : G_{(D)} = \operatorname{Spec}\mathbb{Z}[X,Y]/(X^2 - DY^2 - Y) \to U_D = \operatorname{Spec}\mathbb{Z}[U,V]/(U^2 - DV^2 - 1)$$

is defined by

$$U \mapsto 2DY + 1,\ V \mapsto 2X : \mathbb{Z}[U,V]/(U^2 - DV^2 - 1) \to \mathbb{Z}[X,Y]/(X^2 - DY^2 - Y).$$

Hence $\alpha : G_{(D)} \to U_D$ is an isomorphism over $\mathbb{Z}[1/2D]$.

The composite

$$\gamma = \alpha \circ \beta : G_D = \operatorname{Spec}\mathbb{Z}[U,V,\frac{1}{U^2 - DV^2}] \to U_D = \operatorname{Spec}\mathbb{Z}[U,V]/(U^2 - DV^2 - 1)$$

is given by

$$(U,V) \mapsto \Big(\frac{U^2 + DV^2}{U^2 - DV^2}, \frac{2UV}{U^2 - DV^2}\Big) : \mathbb{Z}[U,V]/(U^2 - DV^2 - 1) \to \mathbb{Z}[U,V,\frac{1}{U^2 - DV^2}].$$

The composite of the embedding $U_D \to G_D$ and $\gamma : G_D \to U_D$ is the square map.

Here is a more concrete description of 1.7.

Remark 1.8. Let R be a commutative ring. Then we have

$$G_{(D)}(R) = \{(a,b) \in R^2 \ ;\ a^2 - Db^2 - b = 0\},$$

and the multiplication of $G_{(D)}(R)$ is given by

$$(a,b)(a',b') = (a + a' + 2Dab' + 2Da'b, b + b' + 2Dbb' + 2aa').$$

The unit of $G_{(D)}(R)$ is given by $(0,0)$, and we have

$$(a,b)^{-1} = (-a,b).$$

Furthermore, for $(u,v) \in G_D(R)$, we have

$$\beta(u,v) = \Big(\frac{uv}{u^2 - Dv^2}, \frac{v^2}{u^2 - Dv^2}\Big) \in G_{(D)}(R)$$

and, for $(a,b) \in G_{(D)}(R)$, we have

$$\alpha(a,b) = (1 + 2Db, 2a) \in U_D(R).$$

Therefore, for $(u,v) \in G_D(R)$, we have gotten

$$\gamma(u,v) = \Big(\frac{u^2 + Dv^2}{u^2 - Dv^2}, \frac{2uv}{u^2 - Dv^2}\Big) \in U_D(R).$$

For example, assume that D is not a square. Then the map $\gamma : G_D(\mathbb{Q}) = \mathbb{Q}(\sqrt{D})^\times \to U_D(\mathbb{Q}) = \{\alpha \in \mathbb{Q}(\sqrt{D}) \ ;\ \operatorname{Nr}\alpha = 1\}$ is given by $\eta \mapsto \eta/\bar{\eta} = \eta^2/\operatorname{Nr}(\eta)$.

When R is a $\mathbb{Z}[1/2D]$-algebra, we shall often indentify the groups $G_{(D)}(R)$ and $U_D(R)$ through the isomorphism $\alpha_R : G_{(D)}(R) \xrightarrow{\sim} U_D(R)$.

Remark 1.9. Assume that D is divisible by p. Then

$$G_{(D),\mathbb{F}_p} = \operatorname{Spec}\mathbb{F}_p[X,Y]/(X^2 - Y)$$

with multiplication

$$\varDelta : (X, Y) \mapsto (X \otimes 1 + 1 \otimes X, Y \otimes 1 + 1 \otimes Y + 2Y \otimes Y).$$

Define a homomorphism

$$\eta : \mathbb{G}_{a,\mathbb{F}_p} = \operatorname{Spec} \mathbb{F}_p[T] \to G_{(D),\mathbb{F}_p} = \operatorname{Spec} \mathbb{F}_p[X, Y]/(X^2 - Y)$$

by

$$X \mapsto T,\ Y \mapsto T^2 : \mathbb{F}_p[X, Y]/(X^2 - Y) \to \mathbb{F}_p[T].$$

Then η is an isomorphism. In particular, $G_{(D)}(\mathbb{F}_p)$ is isomorphic to the additive group $\mathbb{F}_p$.

Moreover, the homomorphism

$$\alpha : G_{(D),\mathbb{F}_p} = \operatorname{Spec} \mathbb{F}_p[X, Y]/(X^2 - Y) \to U_{D,\mathbb{F}_p} = \operatorname{Spec} \mathbb{F}_p[U, V]/(U^2 - 1)$$

is given by

$$U \mapsto 1,\ V \mapsto 2X : \mathbb{F}_p[U, V]/(U^2 - 1) \to \mathbb{F}_p[X, Y]/(X^2 - Y).$$

Then we obtain a commutative diagram of group schemes over $\mathbb{F}_p$

$$\begin{tikzcd}
\mathbb{G}_{a,\mathbb{F}_p} \arrow[r, "\eta"] \arrow[d, "\text{homothety by } 2"'] & G_{(D),\mathbb{F}_p} \arrow[d, "\alpha"] \\
\mathbb{G}_{a,\mathbb{F}_p} \arrow[r, "\iota"'] & U_{D,\mathbb{F}_p}
\end{tikzcd} .$$

Furthermore, if $p \neq 2$, then the homothety by 2 on $\mathbb{G}_{a,\mathbb{F}_p}$ is isomorphic. Theorefore we obtain an exact sequence of group schemes over $\mathbb{F}_p$

$$0 \longrightarrow G_{(D),\mathbb{F}_p} \xrightarrow{\alpha} U_{D,\mathbb{F}_p} \xrightarrow{\varepsilon} \boldsymbol{\mu}_{2,\mathbb{F}_p} \longrightarrow 0,$$

modifying the exact sequence

$$0 \longrightarrow \mathbb{G}_{a,\mathbb{F}_p} \xrightarrow{\iota} U_{D,\mathbb{F}_p} \xrightarrow{\varepsilon} \boldsymbol{\mu}_{2,\mathbb{F}_p} \longrightarrow 0$$

presented in Remark 1.6.

The subsections from 1.10 to 1.14 are devoted for verification of the surjectivity of the reduction maps $G_D(\mathbb{Z}_{(p)}) \to G_D(\mathbb{Z}/p^n\mathbb{Z})$, $U_D(\mathbb{Z}_{(p)}) \to U_D(\mathbb{Z}/p^n\mathbb{Z})$ and $G_{(D)}(\mathbb{Z}_{(p)}) \to G_{(D)}(\mathbb{Z}/p^n\mathbb{Z})$.

Lemma 1.10. *Let p be a prime and n a positive integer. Then the exact sequence of group schemes*

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

yields a commutative diagram with exact rows

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

Proof. Let R be a ring. Then the exact sequence of group schemes

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

yields an exact sequence

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

and therefore, an exact sequence

$$0 \longrightarrow R^\times \xrightarrow{i} G_D(R) \xrightarrow{\beta} G_{(D)}(R) \longrightarrow 0$$

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

Corollary 1.11. *Let p be a prime and n a positive integer. Then the reduction maps $G_D(\mathbb{Z}_{(p)}) \to G_D(\mathbb{Z}/p^n\mathbb{Z})$ and $G_{(D)}(\mathbb{Z}_{(p)}) \to G_{(D)}(\mathbb{Z}/p^n\mathbb{Z})$ are surjective.*

Proof. First we verify that the reduction map $G_D(\mathbb{Z}_{(p)}) \to G_D(\mathbb{Z}/p^n\mathbb{Z})$ is surjective. Indeed, let $(\bar{u}, \bar{v}) \in G_D(\mathbb{Z}/p^n\mathbb{Z})$, and take $u, v \in \mathbb{Z}_{(p)}$ such that $u \mod p^n = \bar{u}$ and $v \mod p^n = \bar{v}$. Then we have

$$u^2 - Dv^2 \equiv \bar{u}^2 - D\bar{v}^2 \not\equiv 0 \mod p.$$

This means that $(u, v) \in G_D(\mathbb{Z}_{(p)})$.

Furthermore, by Lemma 1.10, $\beta : G_D(\mathbb{Z}/p^n\mathbb{Z}) \to G_{(D)}(\mathbb{Z}/p^n\mathbb{Z})$ is surjective. This implies the surjectivity of the composites

$$[G_D(\mathbb{Z}_{(p)}) \xrightarrow{\beta} G_{(D)}(\mathbb{Z}_{(p)}) \to G_{(D)}(\mathbb{Z}/p^n\mathbb{Z})] = [G_D(\mathbb{Z}_{(p)}) \to G_D(\mathbb{Z}/p^n\mathbb{Z}) \xrightarrow{\beta} G_{(D)}(\mathbb{Z}/p^n\mathbb{Z})].$$

Hence the reduction map $G_{(D)}(\mathbb{Z}_{(p)}) \to G_{(D)}(\mathbb{Z}/p^n\mathbb{Z})$ is also surjective.

Lemma 1.12. *Let p be an odd prime divisor of D, and let $\tilde{\varepsilon} : U_D(\mathbb{Z}_{(p)}) \to \{\pm 1\}$ denote the composite $U_D(\mathbb{Z}_{(p)}) \to U_D(\mathbb{F}_p) \xrightarrow{\varepsilon} \boldsymbol{\mu}_2(\mathbb{F}_p) = \{\pm 1\}$. Then the sequence*

$$0 \longrightarrow G_{(D)}(\mathbb{Z}_{(p)}) \xrightarrow{\alpha} U_D(\mathbb{Z}_{(p)}) \xrightarrow{\tilde{\varepsilon}} \{\pm 1\} \longrightarrow 0$$

is exact.

Proof. Let $(a, b) \in \mathrm{Ker}[\alpha : G_{(D)}(\mathbb{Z}_{(p)}) \to U_D(\mathbb{Z}_{(p)})]$. Then, by the definition of α, we have $1 + 2Db = 1$ and $2a = 0$, which implies $(a, b) = (0, 0)$.

On the other hand, let $(u,v) \in \mathrm{Ker}[\tilde{\varepsilon} : U_D(\mathbb{Z}_{(p)}) \to \{\pm 1\}]$. Then we have $u^2 - Dv^2 = 1$ and $u \equiv 1 \mod p$. Put $\nu = \mathrm{ord}_p D$. Then we obtain $u^2 \equiv 1 \mod p^\nu$, and therefore, $u \equiv 1 \mod p^\nu$. Put $a = v/2$ and $b = (u-1)/2D$. Then $a, b \in \mathbb{Z}_{(p)}$, and the relation $u^2 - Dv^2 = 1$ implies the relation $a^2 - Db^2 - b = 0$. Hence the result.

Lemma 1.13. *Let p be an odd prime divisor of D, and let $\tilde{\varepsilon} : U_D(\mathbb{Z}/p^n\mathbb{Z}) \to \{\pm 1\}$ denote the composite $U_D(\mathbb{Z}/p^n\mathbb{Z}) \to U_D(\mathbb{F}_p) \xrightarrow{\varepsilon} \boldsymbol{\mu}_2(\mathbb{F}_p) = \{\pm 1\}$. Then, for each integer $n \geq 2$, the sequence*

$$0 \longrightarrow G_{(D)}(\mathbb{Z}/p^n\mathbb{Z}) \xrightarrow{\alpha} U_D(\mathbb{Z}/p^n\mathbb{Z}) \xrightarrow{\tilde{\varepsilon}} \{\pm 1\} \longrightarrow 0$$

is exact.

Proof. Let $(a,b) \in \mathrm{Ker}[\alpha : G_{(D)}(\mathbb{Z}_{(p)}) \to U_D(\mathbb{Z}_{(p)})]$. Then, by the definition of α, we have $1 + 2Db = 1$ and $2a = 0$. This implies $Db = 0$ and $a = 0$, since 2 is invertible in $\mathbb{Z}/p^n\mathbb{Z}$. Therefore, we obtain $b = 0$, noting the relation $a^2 - Db^2 - b = 0$, .

On the other hand, let $(u,v) \in \mathrm{Ker}[\tilde{\varepsilon} : U_D(\mathbb{Z}/p^n\mathbb{Z}) \to \{\pm 1\}]$. Then we have $u^2 - Dv^2 = 1$ and $u \equiv 1 \mod p$. Put now

$$a = \frac{1}{2}\sum_{k=1}^{\infty} \binom{1/2}{k} D^{k-1} v^{2k}.$$

(The right hand side has a sence since D is nilpotent in $\mathbb{Z}/p^n\mathbb{Z}$.) Then we obtain $(1+2Da)^2 = 1 + Dv^2$. This implies $u = 1 + 2Da$, since $u^2 = 1 + Dv^2$, $u \equiv 1 \mod p$ and $1 + 2Da \equiv 1 \mod p$. Putting $b = v/2$, we obtain $\alpha(a,b) = (u,v)$.

Corollary 1.14. *Let p be an odd prime divisor of D. Then $\alpha : G_{(D)}(\mathbb{Z}_{(p)}) \to U_D(\mathbb{Z}_{(p)})$ induces a bijection* $\mathrm{Ker}[G_{(D)}(\mathbb{Z}_{(p)}) \to G_{(D)}(\mathbb{Z}/p^n\mathbb{Z})] \xrightarrow{\sim} \mathrm{Ker}[U_D(\mathbb{Z}_{(p)}) \to U_D(\mathbb{Z}/p^n\mathbb{Z})]$*, and the reduction map $U_D(\mathbb{Z}_{(p)}) \to U_D(\mathbb{Z}/p^n\mathbb{Z})$ is surjective.*

Proof. Combining Lemma 1.12 and Remark 1.9 for $n = 1$, and Lemma 1.12 and Lemma 1.13 for $n \geq 2$, we obtain a commutative diagram with exact rows

$$\begin{tikzcd}
0 \arrow[r] & G_{(D)}(\mathbb{Z}_{(p)}) \arrow[r, "\alpha"] \arrow[d] & U_D(\mathbb{Z}_{(p)}) \arrow[r, "\tilde{\varepsilon}"] \arrow[d] & \{\pm 1\} \arrow[r] \arrow[d, equal] & 0 \\
0 \arrow[r] & G_{(D)}(\mathbb{Z}/p^n\mathbb{Z}) \arrow[r, "\alpha"] & U_D(\mathbb{Z}/p^n\mathbb{Z}) \arrow[r, "\tilde{\varepsilon}"] & \{\pm 1\} \arrow[r] & 0
\end{tikzcd}.$$

Applying the snake lemma, we can conclude that $\alpha : G_{(D)}(\mathbb{Z}_{(p)}) \to U_D(\mathbb{Z}_{(p)})$ induces a bijection $\mathrm{Ker}[G_{(D)}(\mathbb{Z}_{(p)}) \to G_{(D)}(\mathbb{Z}/p^n\mathbb{Z})] \xrightarrow{\sim} \mathrm{Ker}[U_D(\mathbb{Z}_{(p)}) \to U_D(\mathbb{Z}/p^n\mathbb{Z})]$. It is readily seen that the reduction map $U_D(\mathbb{Z}_{(p)}) \to U_D(\mathbb{Z}/p^n\mathbb{Z})$ is surjective, since the reduction map $G_{(D)}(\mathbb{Z}_{(p)}) \to G_{(D)}(\mathbb{Z}/p^n\mathbb{Z})$ is surjective by Corollary 1.11.

Remark 1.15. Assume that D is not a square. Let p be a prime divisor of D. Then p ramifies in the quadratic extension $\mathbb{Q}(\sqrt{D})/\mathbb{Q}$. Let $\mathfrak{p}$ denote the prime of $\mathbb{Q}(\sqrt{D})$ over p, and assume that $p \neq 2$ and $\mathrm{ord}_p D = 1$. Then the homomorphism $\alpha : G_{(D)} \to U_D$ induces an isomophism

$$G_{(D)}(\mathbb{Z}_{(p)}) \xrightarrow{\sim} \{\alpha \in \mathbb{Q}(\sqrt{D})\ ;\ \mathrm{Nr}\,\alpha = 1,\ \mathrm{ord}_{\mathfrak{p}}(\alpha - 1) \geq 1\}$$

under the identification

$$U_D(\mathbb{Z}_{(p)}) = \{\alpha \in \mathbb{Q}(\sqrt{D})\ ;\ \mathrm{Nr}\,\alpha = 1 \text{ and } \mathrm{ord}_{\mathfrak{p}}\alpha = 0\}$$

mentioned in Remark 1.4.

Indeed, let $(u,v) \in U_D(\mathbb{Z}_{(p)})$, Then Lemma 1.12 implies the equivalence

$$(u,v) \in \mathrm{Im}[\alpha : G_{(D)}(\mathbb{Z}_{(p)}) \to U_D(\mathbb{Z}_{(p)})] \ \Leftrightarrow\ u \equiv 1 \mod p.$$

Futhermore, we can verify the equivalence

$$u \equiv 1 \mod p \ \Leftrightarrow\ u + v\sqrt{D} \equiv 1 \mod \mathfrak{p},$$

noting that $\sqrt{D} \in \mathfrak{p}$.

Summary 1.16. We conclude the section, summing up exact sequences deduced from the exact sequence of group schemes

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

in terms of quadratic extensions. The assertions mentioned below are deduced from Proposition 1.5 and Lemma 1.10 in combination.

Assume that D is not a square. Then we have $G_D(\mathbb{Q}) = \mathbb{Q}(\sqrt{D})^\times$ and $G_D(\mathbb{Z}_{(p)}) = \mathbb{Z}_{(p)}[\sqrt{D}]^\times$, and $\alpha : G_{(D)}(\mathbb{Q}) \to U_D(\mathbb{Q})$ is bijective. Moreover, if $(p, D) = 1$, then the homomorphism $\alpha : G_{(D)}(\mathbb{Z}_{(p)}) \to U_D(\mathbb{Z}_{(p)})$ is bijective.

(1) If $\left(\dfrac{D}{p}\right) = 1$, then we obtain a commutative diagram with exact rows and columns:

$$\begin{tikzcd}
 & 1 \arrow[d] & 1 \arrow[d] & 1 \arrow[d] & \\
1 \arrow[r] & \mathbb{Z}_{(p)}^\times \arrow[r] \arrow[d] & \mathbb{Z}_{(p)}[\sqrt{D}]^\times \arrow[r, "\gamma"] \arrow[d] & U_D(\mathbb{Z}_{(p)}) \arrow[r] \arrow[d] & 1 \\
1 \arrow[r] & \mathbb{Q}^\times \arrow[r] \arrow[d, "\mathrm{ord}_p"] & \mathbb{Q}(\sqrt{D})^\times \arrow[r, "\gamma"] \arrow[d, "(\mathrm{ord}_{\mathfrak{p}}, \mathrm{ord}_{\bar{\mathfrak{p}}})"] & U_D(\mathbb{Q}) \arrow[r] \arrow[d, "\mathrm{ord}_{\mathfrak{p}}"] & 1\ . \\
0 \arrow[r] & \mathbb{Z} \arrow[r, "\Delta"] \arrow[d] & \mathbb{Z} \times \mathbb{Z} \arrow[r, "\delta"] \arrow[d] & \mathbb{Z} \arrow[r] \arrow[d] & 0 \\
 & 0 & 0 & 0 &
\end{tikzcd}$$

Here $\mathfrak{p}$ is a prime of $\mathbb{Q}(\sqrt{D})$ over p, and $\bar{\mathfrak{p}}$ denotes the conjugate of $\mathfrak{p}$. Furthermore, $\Delta : \mathbb{Z} \to \mathbb{Z}\times\mathbb{Z}$ and $\delta : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ are defined by $\Delta(a) = (a,a)$ and $\delta(a,b) = a - b$, respectively.

(2) If $\left(\dfrac{D}{p}\right) = -1$, then we obtain a commutative diagram with exact rows and columns:

$$\begin{tikzcd}
 & 1 \arrow[d] & 1 \arrow[d] & & \\
1 \arrow[r] & \mathbb{Z}_{(p)}^{\times} \arrow[r] \arrow[d] & \mathbb{Z}_{(p)}[\sqrt{D}]^{\times} \arrow[r, "\gamma"] \arrow[d] & U_D(\mathbb{Z}_{(p)}) \arrow[r] \arrow[d, "\wr"] & 1 \\
1 \arrow[r] & \mathbb{Q}^{\times} \arrow[r] \arrow[d, "\mathrm{ord}_p"] & \mathbb{Q}(\sqrt{D})^{\times} \arrow[r, "\gamma"] \arrow[d, "\mathrm{ord}_p"] & U_D(\mathbb{Q}) \arrow[r] & 1 . \\
 & \mathbb{Z} \arrow[r, "\mathrm{id}"] \arrow[d] & \mathbb{Z} \arrow[d] & & \\
 & 0 & 0 & &
\end{tikzcd}$$

(3) If $p \neq 2$ and $\mathrm{ord}_p D = 1$, then we obtain a commutative diagram with exact rows and columns:

$$\begin{tikzcd}
 & 1 \arrow[d] & 1 \arrow[d] & 1 \arrow[d] & \\
1 \arrow[r] & \mathbb{Z}_{(p)}^{\times} \arrow[r] \arrow[d] & \mathbb{Z}_{(p)}[\sqrt{D}]^{\times} \arrow[r, "\beta"] \arrow[d] & G_{(D)}(\mathbb{Z}_{(p)}) \arrow[r] \arrow[d, "\alpha"] & 1 \\
1 \arrow[r] & \mathbb{Q}^{\times} \arrow[r] \arrow[d, "\mathrm{ord}_p"] & \mathbb{Q}(\sqrt{D})^{\times} \arrow[r, "\gamma"] \arrow[d, "\mathrm{ord}_{\mathfrak{p}}"] & U_D(\mathbb{Q}) \arrow[r] \arrow[d] & 1 \cdot \\
0 \arrow[r] & \mathbb{Z} \arrow[r, "2"] \arrow[d] & \mathbb{Z} \arrow[r] \arrow[d] & \mathbb{Z}/2\mathbb{Z} \arrow[r] \arrow[d] & 0 \\
 & 0 & 0 & 0 &
\end{tikzcd}$$

Here $\mathfrak{p}$ denotes the prime of $\mathbb{Q}(\sqrt{D})$ over p.

2. $G_D(\mathbb{Z}_p)$, $U_D(\mathbb{Z}_p)$ and $G_{(D)}(\mathbb{Z}_p)$

Throughout the section, we fix a *non-zero integer* D and an *odd prime* p.

Definition 2.1. We first recall elementary facts on p-adic analysis. As is well known, for $a \in p\mathbb{Z}_p$, the series

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

converges in $\mathbb{Z}_p$. The map $\exp : p\mathbb{Z}_p \to \mathbb{Z}_p$ induces an isomoprhism of the additive group $p\mathbb{Z}_p$ to the multiplicative group $1 + p\mathbb{Z}_p$. The inverse of $\exp : p\mathbb{Z}_p \xrightarrow{\sim} 1 + p\mathbb{Z}_p$ is given by

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

The hyperbolic functions and the inverse hyperbolic functions are defined by

$$\cosh a = \frac{\exp a + \exp(-a)}{2} = \sum_{k=0}^{\infty} \frac{1}{(2k)!} a^{2k},$$
$$\sinh a = \frac{\exp a - \exp(-a)}{2} = \sum_{k=0}^{\infty} \frac{1}{(2k+1)!} a^{2k+1},$$
$$\tanh^{-1} a = \frac{1}{2} \log \frac{1+a}{1-a} = \sum_{k=0}^{\infty} \frac{1}{2k+1} a^{2k+1}$$

for $a \in p\mathbb{Z}_p$ as usual.

From 2.2 to 2.5, we assume that D is *a square in* $\mathbb{Z}_p$, and we take $r \in \mathbb{Z}_p$ such that $D = r^2$.

2.2. We define a homomorphism of groups

$$\exp : p\mathbb{Z}_p \times p\mathbb{Z}_p \to G_D(\mathbb{Z}_p)$$

by

$$\exp : (a, b) \mapsto \big(\exp a \, \cosh rb, \frac{1}{r} \exp a \, \sinh rb\big)$$

and a homomorphism of groups

$$\exp : p\mathbb{Z}_p \to U_D(\mathbb{Z}_p)$$

by

$$\exp : b \mapsto \big(\cosh rb, \frac{1}{r} \sinh rb\big)$$

Furthermore, we have a commutative diagram

$$\begin{tikzcd} p\mathbb{Z}_p \arrow[r, "i_2"] \arrow[d, "\exp"'] & p\mathbb{Z}_p \times p\mathbb{Z}_p \arrow[d, "\exp"] \\ U_D(\mathbb{Z}_p) \arrow[r, "i"'] & G_D(\mathbb{Z}_p) \end{tikzcd} .$$

Here $i_2 : p\mathbb{Z}_p \to p\mathbb{Z}_p \times p\mathbb{Z}_p$ is defined by $i_2(b) = (0, b)$.

Lemma 2.3. *The map* $\exp : p\mathbb{Z}_p \times p\mathbb{Z}_p \to G_D(\mathbb{Z}_p)$ *gives rise to isomorphisms*

$$\exp : p^n\mathbb{Z}_p \times p^n\mathbb{Z}_p \xrightarrow{\sim} \mathrm{Ker}[G_D(\mathbb{Z}_p) \to G_D(\mathbb{Z}/p^n\mathbb{Z})]$$

and

$$\exp : p^n\mathbb{Z}_p \xrightarrow{\sim} \mathrm{Ker}[U_D(\mathbb{Z}_p) \to U_D(\mathbb{Z}/p^n\mathbb{Z})]$$

for each $n \geq 1$.

Proof. It suffices to verify that the inverse of $\exp : p^n\mathbb{Z}_p \times p^n\mathbb{Z}_p \to \mathrm{Ker}[G_D(\mathbb{Z}_p) \to G_D(\mathbb{Z}/p^n\mathbb{Z})]$ is given by

$$(u, v) \mapsto \Big(\frac{1}{2} \log(u^2 - Dv^2), \frac{1}{2r} \log \frac{u + rv}{u - rv}\Big) = \Big(\frac{1}{2} \log(u^2 - Dv^2), \frac{1}{2r} \tanh^{-1} \frac{rv}{u}\Big).$$

Let $a, b \in \mathbb{Z}_p$. Then it is easy to check the implication

$$a \equiv 0 \mod p^n, \ b \equiv 0 \mod p^n \ \Rightarrow \ \exp a \cosh rb \equiv 1 \mod p^n, \ \frac{\exp a \, \sinh rb}{r} \equiv 0 \mod p^n.$$

Conversely, let $u, v \in \mathbb{Z}_p$. Then it is easy also to check the implication

$$u \equiv 1 \mod p^n,\ v \equiv 0 \mod p^n \ \Rightarrow\ \log(u^2 - Dv^2) \equiv 0 \mod p^n,\ \frac{1}{r}\tanh^{-1}\frac{rv}{u} \equiv 0 \mod p^n.$$

Remark 2.4. The composite $\beta \circ \exp : p\mathbb{Z}_p \times p\mathbb{Z}_p \to G_D(\mathbb{Z}_p) \to G_{(D)}(\mathbb{Z}_p)$ is given by

$$(a, b) \mapsto \Big(\frac{1}{r}\cosh rb \sinh rb, \frac{1}{r^2}\sinh^2 rb\Big).$$

Define a homomorphism $\exp : p\mathbb{Z}_p \to G_{(D)}(\mathbb{Z}_p)$ by

$$b \mapsto \Big(\frac{1}{r}\cosh rb \sinh rb, \frac{1}{r^2}\sinh^2 rb\Big).$$

Then we obtain a commutative diagram with exact rows and columns

$$\begin{tikzcd}
 & 0 \arrow[d] & 0 \arrow[d] & 0 \arrow[d] & \\
0 \arrow[r] & p\mathbb{Z}_p \arrow[r, "i_1"] \arrow[d, "\exp"] & p\mathbb{Z}_p \times p\mathbb{Z}_p \arrow[r, "j_2"] \arrow[d, "\exp"] & p\mathbb{Z}_p \arrow[r] \arrow[d, "\exp"] & 0 \\
0 \arrow[r] & \mathbb{Z}_p^\times \arrow[r, "i"] \arrow[d] & G_D(\mathbb{Z}_p) \arrow[r, "\beta"] \arrow[d] & G_{(D)}(\mathbb{Z}_p) \arrow[r] \arrow[d] & 0\ , \\
0 \arrow[r] & \mathbb{F}_p^\times \arrow[r, "i"] \arrow[d] & G_D(\mathbb{F}_p) \arrow[r, "\beta"] \arrow[d] & G_{(D)}(\mathbb{F}_p) \arrow[r] \arrow[d] & 0 \\
 & 0 & 0 & 0 &
\end{tikzcd}$$

Here $i_1 : p\mathbb{Z}_p \to p\mathbb{Z}_p \times p\mathbb{Z}_p$ and $j_2 : p\mathbb{Z}_p \times p\mathbb{Z}_p \to p\mathbb{Z}_p$ are defined by $i_1(a) = (a, 0)$ and $j_2 : (a, b) \mapsto b$, respectively.

On the other hand, we have a commutative diagram with exact rows and columns

$$\begin{tikzcd}
 & 0 \arrow[d] & 0 \arrow[d] & 0 \arrow[d] & & \\
0 \arrow[r] & p\mathbb{Z}_p \arrow[r, "i_2"] \arrow[d, "\exp"] & p\mathbb{Z}_p \times p\mathbb{Z}_p \arrow[r, "\nu"] \arrow[d, "\exp"] & p\mathbb{Z}_p \arrow[r] \arrow[d, "\exp"] & 0 & \\
0 \arrow[r] & U_D(\mathbb{Z}_p) \arrow[r, "i"] \arrow[d] & G_D(\mathbb{Z}_p) \arrow[r, "\mathrm{Nr}"] \arrow[d] & \mathbb{Z}_p^\times \arrow[r] \arrow[d] & H^1(\mathbb{Z}_p, U_D) \arrow[r] \arrow[d, "\wr"] & 0\ \cdot \\
0 \arrow[r] & U_D(\mathbb{F}_p) \arrow[r, "i"] \arrow[d] & G_D(\mathbb{F}_p) \arrow[r, "\mathrm{Nr}"] \arrow[d] & \mathbb{F}_p^\times \arrow[r] \arrow[d] & H^1(\mathbb{F}_p, U_D) \arrow[r] & 0 \\
 & 0 & 0 & 0 & &
\end{tikzcd}$$

Here $i_2 : p\mathbb{Z}_p \to p\mathbb{Z}_p \times p\mathbb{Z}_p$ and $\nu : p\mathbb{Z}_p \times p\mathbb{Z}_p \to p\mathbb{Z}_p$ are defined by $i_2(a) = (0, a)$ and $\nu(a, b) = 2a$, respectively. Moreover, we have

$$H^1(\mathbb{F}_p, U_D) = \begin{cases} 0 & \text{if } (p, D) = 1 \\ \mathbb{F}_p^\times/(\mathbb{F}_p^\times)^2 & \text{if } p|D \end{cases}.$$

Furthermore, we obtain a commutative diagram

$$\begin{tikzcd}
p\mathbb{Z}_p \arrow[r, "2"] \arrow[d, "\exp"'] & p\mathbb{Z}_p \arrow[d, "\exp"] \\
G_{(D)}(\mathbb{Z}_p) \arrow[r, "\alpha"'] & U_D(\mathbb{Z}_p)
\end{tikzcd}$$

by the duplication formula for hyperbolic functions.

Remark 2.5. We interpret the map $\exp : p\mathbb{Z}_p \times p\mathbb{Z}_p \to G_D(\mathbb{Z}_p)$ in the context of Reamrk 1.3. Recall that the homomorphisms of group schemes

$$\xi : G_{D,\mathbb{Z}_p} = \operatorname{Spec} \mathbb{Z}_p[U, V, \frac{1}{U^2 - DV^2}] \to \mathbb{G}_{m,\mathbb{Z}_p} \times \mathbb{G}_{m,\mathbb{Z}_p} = \operatorname{Spec} \mathbb{Z}_p[T_1, T_2, \frac{1}{T_1}, \frac{1}{T_2}]$$

and

$$\xi : U_D = \operatorname{Spec} \mathbb{Z}_p[U, V]/(U^2 - DV^2 - 1) \to \mathbb{G}_{m,\mathbb{Z}} = \operatorname{Spec} \mathbb{Z}_p[T, \frac{1}{T}]$$

are defined by

$$T_1 \mapsto U + rV,\ T_2 \mapsto U - rV : \mathbb{Z}_p[T_1, T_2, \frac{1}{T_1}, \frac{1}{T_2}] \to \mathbb{Z}_p[U, V]/(U^2 - DV^2 - 1)$$

and by

$$T \mapsto U + rV : \mathbb{Z}_p[T, \frac{1}{T}] \to \mathbb{Z}_p[U, V]/(U^2 - DV^2 - 1),$$

respectively. Therefore, we obtain homomorphisms

$$\xi : G_D(\mathbb{Z}_p) \to \mathbb{G}_m(\mathbb{Z}_p) \times \mathbb{G}_m(\mathbb{Z}_p) = \mathbb{Z}_p^\times \times \mathbb{Z}_p^\times$$

and

$$\xi : U_D(\mathbb{Z}_p) \to \mathbb{G}_m(\mathbb{Z}_p) = \mathbb{Z}_p^\times.$$

More concretely, $\xi : G_D(\mathbb{Z}_p) \to \mathbb{Z}_p^\times \times \mathbb{Z}_p^\times$ is given by $(u, v) \mapsto (u+rv, u-rv)$, and $\xi : U_D(\mathbb{Z}_p) \to \mathbb{Z}_p^\times$ by $(u, v) \mapsto u + rv$. Therefore, the composite $\xi \circ \exp : p\mathbb{Z}_p \times p\mathbb{Z}_p \to G_D(\mathbb{Z}_p) \to \mathbb{Z}_p^\times \times \mathbb{Z}_p^\times$ is given by

$$(a, b) \mapsto (\exp(a + rb), \exp(a - rb)),$$

and the composite $\xi \circ \exp : p\mathbb{Z}_p \to U_D(\mathbb{Z}_p) \to \mathbb{Z}_p^\times$ is given by

$$b \mapsto \exp rb.$$

From 2.6 to 2.8, we assume that D is *not a square in* $\mathbb{Z}_p$.

Definition 2.6. Define a homomorphism

$$\exp : p\mathbb{Z}_p[\sqrt{D}] \to G_D(\mathbb{Z}_p)$$

by

$$\exp : a + b\sqrt{D} \mapsto \big(\exp a\, \cosh b\sqrt{D}, \frac{1}{\sqrt{D}} \exp a\, \sinh b\sqrt{D}\big)$$

and a homomorphism

$$\exp : p\mathbb{Z}_p \to U_D(\mathbb{Z}_p)$$

by

$$\exp : a \mapsto (\cosh a\sqrt{D}, \frac{1}{\sqrt{D}} \sinh a\sqrt{D}).$$

Then we obtain a commutative diagram

$$\begin{tikzcd} p\mathbb{Z}_p \arrow[r, "i"] \arrow[d, "\exp"'] & p\mathbb{Z}_p[\sqrt{D}] \arrow[d, "\exp"] \\ U_D(\mathbb{Z}_p) \arrow[r, "i"'] & G_D(\mathbb{Z}_p) \end{tikzcd} .$$

Here $i : p\mathbb{Z}_p \to p\mathbb{Z}_p[\sqrt{D}]$ is defined by $i(b) = b\sqrt{D}$.

Lemma 2.7. *The map* $\exp : p\mathbb{Z}_p[\sqrt{D}] \to G_D(\mathbb{Z}_p) = \mathbb{Z}_p[\sqrt{D}]^\times$ *gives rise to isomorphisms*

$$\exp : p^n\mathbb{Z}_p[\sqrt{D}] \xrightarrow{\sim} \mathrm{Ker}[G_D(\mathbb{Z}_p) \to G_D(\mathbb{Z}/p^n\mathbb{Z})]$$

and

$$\exp : p^n\mathbb{Z}_p \xrightarrow{\sim} \mathrm{Ker}[U_D(\mathbb{Z}_p) \to U_D(\mathbb{Z}/p^n\mathbb{Z})]$$

for each $n \geq 1$.

Proof. It is well known that the inverse of $\exp : p^n\mathbb{Z}_p[\sqrt{D}] \to \mathrm{Ker}[G_D(\mathbb{Z}_p) \to G_D(\mathbb{Z}/p^n\mathbb{Z})]$ is given by $\eta \mapsto \log \eta$.

Remark 2.8. The composite $\beta \circ \exp : p\mathbb{Z}_p[\sqrt{D}] \to G_D(\mathbb{Z}_p) \to G_{(D)}(\mathbb{Z}_p)$ is given by

$$a + b\sqrt{D} \mapsto \Big(\frac{1}{\sqrt{D}} \cosh b\sqrt{D}\, \sinh b\sqrt{D}, \frac{1}{D} \sinh^2 b\sqrt{D}\Big).$$

Define a homomorphism $\exp : p\mathbb{Z}_p \to G_{(D)}(\mathbb{Z}_p)$ by

$$b \mapsto \Big(\frac{1}{\sqrt{D}} \cosh b\sqrt{D}\, \sinh b\sqrt{D}, \frac{1}{D} \sinh^2 b\sqrt{D}\Big).$$

Then we obtain a commutative diagram with exact rows and columns

$$\begin{tikzcd}
 & 0 \arrow[d] & 0 \arrow[d] & 0 \arrow[d] & & \\
0 \arrow[r] & p\mathbb{Z}_p \arrow[r, "i"] \arrow[d, "\exp"] & p\mathbb{Z}_p[\sqrt{D}] \arrow[r, "j"] \arrow[d, "\exp"] & p\mathbb{Z}_p \arrow[r] \arrow[d, "\exp"] & 0 & \\
0 \arrow[r] & \mathbb{Z}_p^{\times} \arrow[r, "i"] \arrow[d] & G_D(\mathbb{Z}_p) \arrow[r, "\gamma"] \arrow[d] & U_D(\mathbb{Z}_p) \arrow[r] \arrow[d] & \operatorname{Coker}\gamma \arrow[r] \arrow[d, "\wr"] & 0 \, , \\
0 \arrow[r] & \mathbb{F}_p^{\times} \arrow[r, "i"] \arrow[d] & G_D(\mathbb{F}_p) \arrow[r, "\gamma"] \arrow[d] & U_D(\mathbb{F}_p) \arrow[r] \arrow[d] & \operatorname{Coker}\gamma \arrow[r] & 0 \\
 & 0 & 0 & 0 & &
\end{tikzcd}$$

Here $i : p\mathbb{Z}_p \to \mathbb{Z}_p[\sqrt{D}]$ and $j : p\mathbb{Z}_p[\sqrt{D}] \to p\mathbb{Z}_p$ are defined by $i(a) = a$ and $j(a + b\sqrt{D}) = b$, respectively. Moreover, we have

$$\operatorname{Coker}\gamma = \begin{cases} 0 & \text{if } (p, D) = 1 \\ \{\pm 1\} & \text{if } p|D \end{cases} .$$

On the other hand, we obtain a commutative diagram with exact rows

$$\begin{tikzcd}
 & 0 \arrow[d] & 0 \arrow[d] & 0 \arrow[d] & & \\
0 \arrow[r] & p\mathbb{Z}_p \arrow[r, "i"] \arrow[d, "\exp"] & p\mathbb{Z}_p[\sqrt{D}] \arrow[r, "\mathrm{Tr}"] \arrow[d, "\exp"] & p\mathbb{Z}_p \arrow[r] \arrow[d, "\exp"] & 0 & \\
0 \arrow[r] & U_D(\mathbb{Z}_p) \arrow[r, "i"] \arrow[d] & G_D(\mathbb{Z}_p) \arrow[r, "\mathrm{Nr}"] \arrow[d] & \mathbb{Z}_p^{\times} \arrow[r] \arrow[d] & H^1(\mathbb{Z}_p, U_D) \arrow[r] \arrow[d, "\wr"] & 0 \, \cdot \\
0 \arrow[r] & U_D(\mathbb{F}_p) \arrow[r, "i"] \arrow[d] & G_D(\mathbb{F}_p) \arrow[r, "\mathrm{Nr}"] \arrow[d] & \mathbb{F}_p^{\times} \arrow[r] \arrow[d] & H^1(\mathbb{F}_p, U_D) \arrow[r] & 0 \\
 & 0 & 0 & 0 & &
\end{tikzcd}$$

Moreover, we have

$$H^1(\mathbb{F}_p, U_D) = \begin{cases} 0 & \text{if } (p, D) = 1 \\ \mathbb{F}_p^{\times}/(\mathbb{F}_p^{\times})^2 & \text{if } p|D \end{cases} .$$

Furthermore, we have a commutative diagram

$$\begin{tikzcd}
p\mathbb{Z}_p \arrow[r, "2"] \arrow[d, "\exp"'] & p\mathbb{Z}_p \arrow[d, "\exp"] \\
G_{(D)}(\mathbb{Z}_p) \arrow[r, "\alpha"'] & U_D(\mathbb{Z}_p)
\end{tikzcd}$$

by the duplication formula for hyperbolic functions.

From the arguments developed above, we obtain the following assertions. The statements from 2.9 to 2.12 are concerning G_D, and those from 2.13 to 2.16 are concerning U_D. Remark 2.17 is concerning $G_{(D)}$.

Proposition 2.9. *Let p be an odd prime. Then the reduction map $G_D(\mathbb{Z}_p) \to G_D(\mathbb{Z}/p^n\mathbb{Z})$ is surjective. Moreover,* $\mathrm{Ker}[G_D(\mathbb{Z}_p) \to G_D(\mathbb{Z}/p^n\mathbb{Z})]$ *is isomorphic to the additive group $p^n\mathbb{Z}_p \times p^n\mathbb{Z}_p$ under the identification* $\exp : p\mathbb{Z}_p \times p\mathbb{Z}_p \xrightarrow{\sim} \mathrm{Ker}[G_D(\mathbb{Z}_p) \to G_D(\mathbb{Z}/p\mathbb{Z})]$.

Proof. By Corollary 1.11, the reduction map $G_D(\mathbb{Z}_{(p)}) \to G_D(\mathbb{Z}/p^n\mathbb{Z})$ is surjective. Hence the reduction map $G_D(\mathbb{Z}_p) \to G_D(\mathbb{Z}/p^n\mathbb{Z})$ is also surjective. The other assertion are verified in Lemma 2.3 and Lemma 2.7.

Corollary 2.10. *Let p be an odd prime and n an integer ≥ 2. Then we have an exact sequence*

$$0 \longrightarrow \mathbb{Z}/p^{n-1}\mathbb{Z} \times \mathbb{Z}/p^{n-1}\mathbb{Z} \longrightarrow G_D(\mathbb{Z}/p^n\mathbb{Z}) \longrightarrow G_D(\mathbb{Z}/p\mathbb{Z}) \longrightarrow 0$$

for each $n \geq 2$. Moreover, the above sequence splits if $(p, D) = 1$.

Proof. We obtain the assertion, applying the snake lemma to the commutative diagram with exact rows

$$\begin{tikzcd}
0 \arrow[r] & p^n\mathbb{Z}_p \times p^n\mathbb{Z}_p \arrow[r, "\exp"] \arrow[d] & G_D(\mathbb{Z}_p) \arrow[r] \arrow[d, equal] & G_D(\mathbb{Z}/p^n\mathbb{Z}) \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & p\mathbb{Z}_p \times p\mathbb{Z}_p \arrow[r, "\exp"'] & G_D(\mathbb{Z}_p) \arrow[r] & G_D(\mathbb{Z}/p\mathbb{Z}) \arrow[r] & 0
\end{tikzcd}.$$

Corollary 2.11. *Let p be an odd prime and n an integer ≥ 2. Then:*

(1) *If $\left(\dfrac{D}{p}\right) = 1$, then $G_D(\mathbb{Z}/p^n\mathbb{Z})$ is of order $(p-1)^2p^{2(n-1)}$.*

(2) *If $\left(\dfrac{D}{p}\right) = -1$, then $G_D(\mathbb{Z}/p^n\mathbb{Z})$ is of order $(p^2-1)p^{2(n-1)}$.*

(3) *If $p|D$, then $G_D(\mathbb{Z}/p^n\mathbb{Z})$ is of order $(p-1)p^{2n-1}$.*

Proof. As is remarked in 1.6, we have

$$|G_D(\mathbb{Z}/p\mathbb{Z})| = \begin{cases} (p-1)^2 & \text{if } \left(\dfrac{D}{p}\right) = 1 \\ p^2 - 1 & \text{if } \left(\dfrac{D}{p}\right) = -1 \\ (p-1)p & \text{if } p|D \end{cases}.$$

Therefore, the assertion follows from Corollary 2.10.

Corollary 2.12. *Let p be an odd prime and n an integer ≥ 1. Let $\eta \in G_D(\mathbb{Z}_p)$, and assume that*

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

Then we have

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

Proof. Let log denote the inverse of exp : $p\mathbb{Z}_p \times p\mathbb{Z}_p \overset{\sim}{\to} \operatorname{Ker}[G_D(\mathbb{Z}_p) \to G_D(\mathbb{Z}/p\mathbb{Z})]$. Then, by the assumption, we have

$$\log \eta \in p^n\mathbb{Z}_p \times p^n\mathbb{Z}_p,\ \log \eta \notin p^{n+1}\mathbb{Z}_p \times p^{n+1}\mathbb{Z}_p.$$

Hence we obtain

$$p\log \eta \in p^{n+1}\mathbb{Z}_p \times p^{n+1}\mathbb{Z}_p,\ p\log \eta \notin p^{n+2}\mathbb{Z}_p \times p^{n+2}\mathbb{Z}_p,$$

which implies the result.

Proposition 2.13. *Let p be an odd prime. Then the reduction map $U_D(\mathbb{Z}_p) \to U_D(\mathbb{Z}/p^n\mathbb{Z})$ is surjective. Moreover,* $\operatorname{Ker}[U_D(\mathbb{Z}_p) \to U_D(\mathbb{Z}/p^n\mathbb{Z})]$ *is isomorphic to the additive group $p^n\mathbb{Z}_p$ under the identification* $\exp : p\mathbb{Z}_p \xrightarrow{\sim} \operatorname{Ker}[U_D(\mathbb{Z}_p) \to U_D(\mathbb{Z}/p\mathbb{Z})]$.

Proof. We can verify the assertion similarly as Proposition 2.9, noting that, the reduction map $U_D(\mathbb{Z}_{(p)}) \to U_D(\mathbb{Z}/p^n\mathbb{Z})$ is surjective by Corollary 1.14.

Corollary 2.14. *Let p be an odd prime. Then the sequence*

$$0 \longrightarrow \operatorname{Ker}[U_D(\mathbb{Z}_p) \to U_D(\mathbb{F}_p)] \longrightarrow U_D(\mathbb{Z}_p) \longrightarrow U_D(\mathbb{F}_p) \longrightarrow 0$$

is exact, and $\operatorname{Ker}[U_D(\mathbb{Z}_p) \to U_D(\mathbb{F}_p)]$ *is isomorphic to the additive group $\mathbb{Z}_p$. Moreover, the above sequence splits if $(p, D) = 1$.*

Proof. We obtain the assertion, applying the snake lemma to the commutative diagram with exact rows

$$\begin{tikzcd}
0 \arrow[r] & p^n\mathbb{Z}_p \arrow[r, "\exp"] \arrow[d] & U_D(\mathbb{Z}_p) \arrow[r] \arrow[d, equal] & U_D(\mathbb{Z}/p^n\mathbb{Z}) \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & p\mathbb{Z}_p \arrow[r, "\exp"'] & U_D(\mathbb{Z}_p) \arrow[r] & U_D(\mathbb{Z}/p\mathbb{Z}) \arrow[r] & 0
\end{tikzcd}.$$

Corollary 2.15. *Let p be an odd prime and n an integer ≥ 2. Then:*

(1) *If $\left(\dfrac{D}{p}\right) = 1$, then $U_D(\mathbb{Z}/p^n\mathbb{Z})$ is a cyclic group of order $(p-1)p^{n-1}$.*

(2) *If $\left(\dfrac{D}{p}\right) = -1$, then $U_D(\mathbb{Z}/p^n\mathbb{Z})$ is a cyclic group of order $(p+1)p^{n-1}$.*

(3) *If $p|D$, then $U_D(\mathbb{Z}/p^n\mathbb{Z})$ is of order $2p^n$.*

Proof. As is remarked in 1.6, we have

$$|U_D(\mathbb{Z}/p\mathbb{Z})| = \begin{cases} p-1 & \text{if } \left(\dfrac{D}{p}\right) = 1 \\ p+1 & \text{if } \left(\dfrac{D}{p}\right) = -1 \\ 2p & \text{if } p|D \end{cases}.$$

Therefore, the assertion follows from Corollary 2.14.

Corollary 2.16. *Let p be an odd prime and n an integer ≥ 1. Let $\eta \in U_D(\mathbb{Z}_p)$, and assume that*

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

Then we have

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

Proof. Let log denote the inverse of $\exp : p\mathbb{Z}_p \xrightarrow{\sim} \mathrm{Ker}[U_D(\mathbb{Z}_p) \to U_D(\mathbb{Z}/p\mathbb{Z})]$. Then, by the assumption, we have

$$\log \eta \in p^n\mathbb{Z}_p \ \ \log \eta \notin p^{n+1}\mathbb{Z}_p.$$

Hence we obtain

$$p \log \eta \in p^{n+1}\mathbb{Z}_p,\ p\log\eta \notin p^{n+2}\mathbb{Z}_p,$$

which implies the result.

Remark 2.17. Let p be an odd prime divisor of D. Then, by similarly as Corollary 1.14, we have a commutative diagram with exact rows and columns

$$\begin{tikzcd}
 & 0 \arrow[d] & 0 \arrow[d] & & \\
 & \mathrm{Ker}\,\pi \arrow[r, "\sim"] \arrow[d] & \mathrm{Ker}\,\tilde{\pi} \arrow[d] & & \\
0 \arrow[r] & G_{(D)}(\mathbb{Z}_p) \arrow[r, "\alpha"] \arrow[d, "\pi"] & U_D(\mathbb{Z}_p) \arrow[r, "\tilde{\varepsilon}"] \arrow[d, "\tilde{\pi}"] & \{\pm 1\} \arrow[r] \arrow[d, "\wr"] & 0\cdot \\
0 \arrow[r] & G_{(D)}(\mathbb{Z}/p^n\mathbb{Z}) \arrow[r, "\alpha"] \arrow[d] & U_D(\mathbb{Z}/p^n\mathbb{Z}) \arrow[r, "\varepsilon"] \arrow[d] & \{\pm 1\} \arrow[r] & 0 \\
 & 0 & 0 & &
\end{tikzcd}$$

Here $\pi : G_{(D)}(\mathbb{Z}_p) \to G_{(D)}(\mathbb{Z}/p^n\mathbb{Z})$ and $\tilde{\pi} : U_D(\mathbb{Z}_p) \to U_D(\mathbb{Z}/p^n\mathbb{Z})$ denote the reduction maps. It follows also that $G_{(D)}(\mathbb{Z}/p^n\mathbb{Z})$ is of order p^n.

From 2.18 to 2.21, we study the case of $p|D$ in detail.

Definition 2.18. Let p be a prime and n a positive integer. A homomorphishm of group schemes

$$\underline{p}^n : G_{(p^{2n}D)} = \mathrm{Spec}\,\mathbb{Z}[X,Y]/(X^2 - p^{2n}DY^2 - Y) \to G_{(D)} = \mathrm{Spec}\,\mathbb{Z}[X,Y]/(X^2 - DY^2 - Y)$$

is defined by

$$(X,Y) \mapsto (p^nX, p^{2n}Y) : \mathbb{Z}[X,Y]/(X^2 - DY^2 - Y) \to \mathbb{Z}[X,Y]/(X^2 - p^{2n}DY^2 - Y).$$

Lemma 2.19. *Let p be a prime. Then we have exact sequences*

$$0 \longrightarrow G_{(p^{2n}D)}(\mathbb{Z}_{(p)}) \xrightarrow{\underline{p}^n} G_{(D)}(\mathbb{Z}_{(p)}) \longrightarrow G_{(D)}(\mathbb{Z}/p^n\mathbb{Z}) \longrightarrow 0$$

and

$$0 \longrightarrow G_{(p^{2n}D)}(\mathbb{Z}_p) \xrightarrow{\underline{p}^n} G_{(D)}(\mathbb{Z}_p) \longrightarrow G_{(D)}(\mathbb{Z}/p^n\mathbb{Z}) \longrightarrow 0.$$

Proof. We give a proof for the first sequence.

Let $(a,b) \in \mathrm{Ker}[\underline{p}^n : G_{(p^{2n}D)}(\mathbb{Z}_{(p)}) \to G_{(D)}(\mathbb{Z}_{(p)})]$. Then, by the definition of $\underline{p}^n$, we have $p^n a = 0$ and $p^{2n}b = 0$, and therefore, $(a,b) = (0,0)$.

Now let $(a,b) \in \mathrm{Ker}[G_{(D)}(\mathbb{Z}_{(p)}) \to G_{(D)}(\mathbb{Z}/p^n\mathbb{Z})]$. Then we have $a^2 = Db^2 + b$ and $\mathrm{ord}_p a \geq n$, $\mathrm{ord}_p b \geq n$, which implies $\mathrm{ord}_p(Db+1) = 0$ and $2\,\mathrm{ord}_p a = \mathrm{ord}_p b$. Put $a = p^n a'$ and $b = p^{2n}b'$ with $a', b' \in \mathbb{Z}_{(p)}$. Then the relation $a^2 - Db^2 - b = 0$ implies the relation $a'^2 - p^{2n}Db'^2 - b' = 0$. These mean $(a',b') \in G_{(p^{2n}D)}(\mathbb{Z}_{(p)})$ and $\underline{p}^n(a',b') = (a,b)$.

By Corollary 1.11, the reduction map $G_{(D)}(\mathbb{Z}_{(p)}) \to G_{(D)}(\mathbb{Z}/p^n\mathbb{Z})$ is surjective.

Proposition 2.20. *Let p be an odd prime divisor of D.*
(1) *If $p > 3$ or $p = 3$, $D \not\equiv -3 \mod 9$, then $G_{(D)}(\mathbb{Z}_p)$ is isomorphic to the additive group $\mathbb{Z}_p$.*
(2) *If $p = 3$ and $D \equiv -3 \mod 9$, the sequence*

$$0 \longrightarrow \mathrm{Ker}[G_{(D)}(\mathbb{Z}_p) \to G_{(D)}(\mathbb{F}_p)] \longrightarrow G_{(D)}(\mathbb{Z}_p) \longrightarrow G_{(D)}(\mathbb{F}_p) \longrightarrow 0$$

splits, and $\mathrm{Ker}[G_{(D)}(\mathbb{Z}_p) \to G_{(D)}(\mathbb{F}_p)]$ *is isomorphic to the additive group $\mathbb{Z}_p$.*

Proof. Put $r = \left\lceil \dfrac{\mathrm{ord}_p D}{2} \right\rceil$.

Case 1. $\mathrm{ord}_p D \equiv 0 \mod 2$ and D is a square in $\mathbb{Z}_p$. By Lemma 2.19, the homomorphisms of group schemes $\alpha : G_{(D)} \to U_D$ and $\xi : U_D \to \mathbb{G}_{m,\mathbb{Z}}$ induce an isomorphism

$$G_{(D)}(\mathbb{Z}_p) \xrightarrow{\sim} \{\alpha \in \mathbb{Z}_p \; ; \; \alpha \equiv 1 \mod p^r\}.$$

Therefore, $\alpha \mapsto \exp \alpha\sqrt{D}$ gives rise to an isomorphism $\mathbb{Z}_p \xrightarrow{\sim} G_{(D)}(\mathbb{Z}_p)$.

Case 2. $\mathrm{ord}_p D \equiv 0 \mod 2$ and D is not a square in $\mathbb{Z}_p$. By Lemma 2.19, the homomorphism of group schemes $\alpha : G_{(D)} \to U_D$ induces an isomorphism

$$G_{(D)}(\mathbb{Z}_p) \xrightarrow{\sim} \{\alpha \in \mathbb{Q}_p(\sqrt{D}) \; ; \; \mathrm{Nr}(\alpha) = 1, \; \mathrm{ord}_p(\alpha - 1) \geq r\}.$$

Noting that $\mathrm{Tr}\,\alpha\sqrt{D} = 0$ for $\alpha \in \mathbb{Z}_p$, we see that $\alpha \mapsto \exp \alpha\sqrt{D}$ gives rise to an isomorphism $\mathbb{Z}_p \xrightarrow{\sim} G_{(D)}(\mathbb{Z}_p)$.

Case 3. $\mathrm{ord}_p D \equiv 1 \mod 2$. The quadratic extension $\mathbb{Q}_p(\sqrt{D})/\mathbb{Q}_p$ is ramified. Let π be a uniformizing parameter of $\mathbb{Q}_p(\sqrt{D})$. Then, by Remark 1.15 and Lemma 2.19, the homomorphism of group schemes $\alpha : G_{(D)} \to U_D$ induces an isomorphism

$$G_{(D)}(\mathbb{Z}_p) \xrightarrow{\sim} \{\alpha \in \mathbb{Q}_p(\sqrt{D}) \; ; \; \mathrm{Nr}(\alpha) = 1, \; \mathrm{ord}_\pi(\alpha - 1) \geq \mathrm{ord}_p D\}.$$

(a) Assume that $p \geq 5$ or that $p = 3$ and $D \equiv 0 \mod 9$. Then we have $\mathrm{ord}_p D > 2/(p-1)$, which implies that $\alpha \mapsto \exp \alpha\sqrt{D}$ gives rise to an isomorphism $\mathbb{Z}_p \xrightarrow{\sim} G_{(D)}(\mathbb{Z}_p)$.

(b) Assume that $p = 3$ and $D \equiv 3 \mod 9$. Then we have $\mathbb{Z}_3[\sqrt{D}] = \mathbb{Z}_3[\sqrt{3}]$. Hence we may take $D = 3$. Put $\eta = (1/2, -1/2) \in G_{(D)}(\mathbb{Z}_3)$. Then we obtain $\eta \equiv (2,1) \mod 3$, which implies that η generates $G_{(D)}(\mathbb{F}_3)$. Furthermore, we have $\alpha(\eta) = (-2, 1) \in U_D(\mathbb{Z}_3)$. Noting that $-2+\sqrt{3} \in \mathbb{Z}_3[\sqrt{3}]$ generates topologically the multiplicative group $\{\alpha \in \mathbb{Q}_3(\sqrt{3})\ ;\ \mathrm{Nr}(\alpha) = 1,\ \mathrm{ord}_\pi(\alpha - 1) \geq 1\}$, we see that $G_{(D)}(\mathbb{Z}_3)$ is isomorphic to $\mathbb{Z}_3$.

(c) Assume that $p = 3$ and $D \equiv -3 \mod 9$. Then we have $\mathbb{Z}_3[\sqrt{D}] = \mathbb{Z}_3[\sqrt{-3}]$. Hence we may take $D = -3$. Moreover, the homomorphism of group schemes $\alpha : G_{(D)} \to U_D$ induces an isomorphism

$$\mathrm{Ker}[G_{(D)}(\mathbb{Z}_3) \to G_{(D)}(\mathbb{F}_3)] \xrightarrow{\sim} \{\alpha \in \mathbb{Q}_3(\sqrt{-3})\ ;\ \mathrm{Nr}(\alpha) = 1,\ \mathrm{ord}_\pi(\alpha - 1) \geq 3\}.$$

Noting that $3 > 2/(p-1) = 1$, we see that $\alpha \mapsto \exp \alpha\sqrt{D}$ gives rise to an isomorphism $\mathbb{Z}_3 \xrightarrow{\sim} \mathrm{Ker}[G_{(D)}(\mathbb{Z}_3) \to G_{(D)}(\mathbb{F}_3)]$.

Put now $\eta = (1/4, 1/4) \in G_{(D)}(\mathbb{Z}_3)$. Then we obtain $\eta \equiv (1,1) \mod 3$, which implies that η generates $G_{(D)}(\mathbb{F}_3)$. Furthermore, we have $\alpha(\eta) = (-1/2, 1/2) \in U_D(\mathbb{Z}_3)$. Since $(-1+\sqrt{-3})/2 \in \mathbb{Z}_3[\sqrt{-3}]$ is a primitive cubic root of unity, the map $(1,1) \mapsto \eta : G_{(D)}(\mathbb{F}_3) \to G_{(D)}(\mathbb{Z}_3)$ gives a splitting of the reduction map $G_{(D)}(\mathbb{Z}_3) \to G_{(D)}(\mathbb{F}_3)$.

Corollary 2.21. *Let p be a prime divisor of D and n an integer ≥ 2. Then:*

(1) *If $p > 3$, or $p = 3$ and $D \not\equiv -3 \mod 9$, then $G_{(D)}(\mathbb{Z}/p^n\mathbb{Z})$ is a cyclic group of order p^n;*

(2) *If $p = 3$ and $D \equiv -3 \mod 9$, then $G_{(D)}(\mathbb{Z}/p^n\mathbb{Z})$ is isomorphic to $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3^{n-1}\mathbb{Z}$.*

Summary 2.22. We conclude the section, giving a precise consideration on a descending chain of subgroups of $U_D(\mathbb{Q}) = G_{(D)}(\mathbb{Q})$. These subgroups play important roles in Section 4.

Let p be an odd prime. Put $r = [(\mathrm{ord}_p D)/2]$ and $\tilde{D} = D/p^{2r}$. Then we obtain a descending chain of subgroups of $U_D(\mathbb{Q}) = G_{(D)}(\mathbb{Q})$:

$$U_D(\mathbb{Q}) \supset U_{\tilde{D}}(\mathbb{Z}_{(p)}) \supset G_{(\tilde{D})}(\mathbb{Z}_{(p)}) \supset G_{(D)}(\mathbb{Z}_{(p)}) \supset G_{(p^2D)}(\mathbb{Z}_{(p)}) \supset G_{(p^4D)}(\mathbb{Z}_{(p)}) \supset \cdots.$$

We have

$$U_D(\mathbb{Q})/U_{\tilde{D}}(\mathbb{Z}_{(p)}) = U_{\tilde{D}}(\mathbb{Q})/U_{\tilde{D}}(\mathbb{Z}_{(p)}) = \begin{cases} \mathbb{Z} & \text{if } \left(\dfrac{\tilde{D}}{p}\right) = 1 \\ 0 & \text{if } \left(\dfrac{\tilde{D}}{p}\right) = -1 \text{ or } p|\tilde{D} \end{cases}$$

by Proposition 1.5, and

$$U_{\tilde{D}}(\mathbb{Z}_{(p)})/G_{(\tilde{D})}(\mathbb{Z}_{(p)}) = \begin{cases} 0 & \text{if } (p, \tilde{D}) = 1 \\ \{\pm 1\} & \text{if } p|\tilde{D} \end{cases}$$

as is remarked in 1.8 and 1.9.

Furthermore, if $\mathrm{ord}_p D \le 1$, then $\tilde{D} = D$ and, by Lemma 2.19, $G_{(D)}(\mathbb{Z}_{(p)})/G_{(p^{2n}D)}(\mathbb{Z}_{(p)})$ is isomorphic to $G_{(D)}(\mathbb{Z}/p^n\mathbb{Z})$. We have also

$$|G_{(D)}(\mathbb{Z}/p^n\mathbb{Z})| = \begin{cases} (p-1)p^{n-1} & \text{if } \left(\dfrac{D}{p}\right) = 1 \\ (p+1)p^{n-1} & \text{if } \left(\dfrac{D}{p}\right) = -1 \\ p^n & \text{if } p|D \end{cases}$$

by Corollary 2.15 and Remark 2.17.

On the other hand, if $\mathrm{ord}_p D \ge 2$, then $G_{(\tilde{D})}(\mathbb{Z}_{(p)})/G_{(D)}(\mathbb{Z}_{(p)})$ is isomorphic to $G_{(D)}(\mathbb{Z}/p^r\mathbb{Z})$ and $U_{\tilde{D}}(\mathbb{Z}_{(p)})/U_D(\mathbb{Z}_{(p)})$ is isomorphic to $U_{\tilde{D}}(\mathbb{Z}/p^r\mathbb{Z})$ by Lemma 2.19 and Corollary 2.14. Moreover, we have

$$|G_{(D)}(\mathbb{Z}/p^r\mathbb{Z})| = |U_{\tilde{D}}(\mathbb{Z}/p^r\mathbb{Z})| = \begin{cases} (p-1)p^{r-1} & \text{if } \left(\dfrac{\tilde{D}}{p}\right) = 1 \\ (p+1)p^{r-1} & \text{if } \left(\dfrac{\tilde{D}}{p}\right) = -1 \end{cases}$$

and

$$|G_{(D)}(\mathbb{Z}/p^r\mathbb{Z})| = p^r, \ |U_{\tilde{D}}(\mathbb{Z}/p^r\mathbb{Z})| = 2p^r \quad \text{if } p|\tilde{D}$$

by Corollary 2.15 and Remark 2.17. Finally, for each $n > 0$, $G_{(D)}(\mathbb{Z}_{(p)})/G_{(p^{2n}D)}(\mathbb{Z}_{(p)})$ is isomorphic to $G_{(D)}(\mathbb{Z}/p^n\mathbb{Z})$, which is cyclic of order p^n, by Lemma 2.19 and Corollary 2.21.

Now we simplify the descending chain of subgroups of $U_D(\mathbb{Q}) = G_{(D)}(\mathbb{Q})$:

$$U_D(\mathbb{Q}) \supset U_{\tilde{D}}(\mathbb{Z}_{(p)}) \supset G_{(\tilde{D})}(\mathbb{Z}_{(p)}) \supset G_{(D)}(\mathbb{Z}_{(p)}) \supset G_{(p^2D)}(\mathbb{Z}_{(p)}) \supset G_{(p^4D)}(\mathbb{Z}_{(p)}) \supset \cdots$$

case by case, combining the facts mentioned above.

Case 1. $\mathrm{ord}_p D = 0$ and $\left(\dfrac{D}{p}\right) = 1$. We have

$$U_D(\mathbb{Q}) \supset U_{\tilde{D}}(\mathbb{Z}_{(p)}) = G_{(\tilde{D})}(\mathbb{Z}_{(p)}) = G_{(D)}(\mathbb{Z}_{(p)}) \supset G_{(p^2D)}(\mathbb{Z}_{(p)}) \supset G_{(p^4D)}(\mathbb{Z}_{(p)}) \supset \cdots.$$

Moreover, $U_D(\mathbb{Q})/U_{\tilde{D}}(\mathbb{Z}_{(p)})$ is isomorphic to the addtive group $\mathbb{Z}$, and $G_{(D)}(\mathbb{Z}_{(p)})/G_{(p^{2n}D)}(\mathbb{Z}_{(p)})$ $= G_{(D)}(\mathbb{Z}/p^n\mathbb{Z})$ is cyclic of order $(p-1)p^{n-1}$.

Case 2. $\mathrm{ord}_p D = 0$ and $\left(\dfrac{D}{p}\right) = -1$. We have

$$U_D(\mathbb{Q}) = U_{\tilde{D}}(\mathbb{Z}_{(p)}) = G_{(\tilde{D})}(\mathbb{Z}_{(p)}) = G_{(D)}(\mathbb{Z}_{(p)}) \supset G_{(p^2D)}(\mathbb{Z}_{(p)}) \supset G_{(p^4D)}(\mathbb{Z}_{(p)}) \supset \cdots.$$

Moreover, $G_{(D)}(\mathbb{Z}_{(p)})/G_{(p^{2n}D)}(\mathbb{Z}_{(p)}) = G_{(D)}(\mathbb{Z}/p^n\mathbb{Z})$ is cyclic of order $(p+1)p^{n-1}$.

Case 3. $\mathrm{ord}_p D = 1$. We have

$$U_D(\mathbb{Q}) = U_{\tilde{D}}(\mathbb{Z}_{(p)}) \supset G_{(\tilde{D})}(\mathbb{Z}_{(p)}) = G_{(D)}(\mathbb{Z}_{(p)}) \supset G_{(p^2D)}(\mathbb{Z}_{(p)}) \supset G_{(p^4D)}(\mathbb{Z}_{(p)}) \supset \cdots.$$

Moreover, $U_{\tilde{D}}(\mathbb{Z}_{(p)})/G_{(\tilde{D})}(\mathbb{Z}_{(p)})$ is isomorphic to the multiplicative group $\{\pm 1\}$ and, by Corollary 2.21, $G_{(D)}(\mathbb{Z}_{(p)})/G_{(p^{2n}D)}(\mathbb{Z}_{(p)}) = G_{(D)}(\mathbb{Z}/p^n\mathbb{Z})$ is cyclic of order p^n except if $p = 3$ and $D \equiv -3 \mod 9$.

Case 4. $\mathrm{ord}_p D$ is even ≥ 2 and $\left(\dfrac{\tilde{D}}{p}\right) = 1$. We have

$$U_D(\mathbb{Q}) \supset U_{\tilde{D}}(\mathbb{Z}_{(p)}) = G_{(\tilde{D})}(\mathbb{Z}_{(p)}) \supset G_{(D)}(\mathbb{Z}_{(p)}) \supset G_{(p^2D)}(\mathbb{Z}_{(p)}) \supset G_{(p^4D)}(\mathbb{Z}_{(p)}) \supset \cdots .$$

Moreover, $U_D(\mathbb{Q})/U_{\tilde{D}}(\mathbb{Z}_{(p)})$ is isomorphic to the addtive group $\mathbb{Z}$, and $G_{(\tilde{D})}(\mathbb{Z}_{(p)})/G_{(D)}(\mathbb{Z}_{(p)}) = G_{(\tilde{D})}(\mathbb{Z}/p^r\mathbb{Z})$ is cyclic of order $(p-1)p^{r-1}$.

Case 5. $\mathrm{ord}_p D$ is even ≥ 2 and $\left(\dfrac{\tilde{D}}{p}\right) = -1$. We have

$$U_D(\mathbb{Q}) = U_{\tilde{D}}(\mathbb{Z}_{(p)}) = G_{(\tilde{D})}(\mathbb{Z}_{(p)}) \supset G_{(D)}(\mathbb{Z}_{(p)}) \supset G_{(p^2D)}(\mathbb{Z}_{(p)}) \supset G_{(p^4D)}(\mathbb{Z}_{(p)}) \supset \cdots .$$

Moreover, $G_{(\tilde{D})}(\mathbb{Z}_{(p)})/G_{(D)}(\mathbb{Z}_{(p)})$ is cyclic of order $(p+1)p^{r-1}$.

Case 6. $\mathrm{ord}_p D$ is odd ≥ 3. We have

$$U_D(\mathbb{Q}) = U_{\tilde{D}}(\mathbb{Z}_{(p)}) \supset G_{(\tilde{D})}(\mathbb{Z}_{(p)}) \supset G_{(D)}(\mathbb{Z}_{(p)}) \supset G_{(p^2D)}(\mathbb{Z}_{(p)}) \supset G_{(p^4D)}(\mathbb{Z}_{(p)}) \supset \cdots .$$

Moreover, $U_{\tilde{D}}(\mathbb{Z}_{(p)})/G_{(\tilde{D})}(\mathbb{Z}_{(p)})$ is isomorphic to the multiplicative group $\{\pm 1\}$ and, by Corollary 2.21, $G_{(\tilde{D})}(\mathbb{Z}_{(p)})/G_{(D)}(\mathbb{Z}_{(p)})$ is cyclic of order p^r.

3. Lucas sequences

Throughout the section, we fix *non-zero integers P, Q relatively prime to each other* with $(P, Q) \neq (\pm 2, 1)$, and put $f(t) = t^2 - Pt + Q$ and $D = P^2 - 4Q$.

The subsections from 3.1 to 3.8 are devoted for reformulation of linear recurrence sequences of order 2.

Definition 3.1. Let R be a ring. We put

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

The map $(w_k)_{k\geq 0} \mapsto (w_0, w_1)$ gives rise to an R-isomorphism $\mathcal{L}(f, R) \xrightarrow{\sim} R^2$.

Now put $A_{(P,Q)} = \mathbb{Z}[t]/(t^2 - Pt + Q)$ and $\theta = t \mod (t^2 - Pt + Q)$. We define an R-homomorphism $\omega_R : R \otimes_{\mathbb{Z}} A_{(P,Q)} \to R$ by $\omega_R(a \otimes 1 + b \otimes \theta) = b$ $(a, b \in R)$. Moreover, we define an R-homomorphism $\omega_R : R \otimes_{\mathbb{Z}} A_{(P,Q)} \to R^{\mathbb{N}}$ by $\omega_R(\eta) = (\omega_R(\eta\theta^k))_{k\geq 0}$. For $\eta = a \otimes 1 + b \otimes \theta \in R \otimes_{\mathbb{Z}} A_{(P,Q)}$, we have $\omega_R(\eta) = (b, a + Pb, \dots)$.

Proposition 3.2. *Let R be a ring. Then ω_R induces an R-isomorphism $R \otimes_{\mathbb{Z}} A_{(P,Q)} \xrightarrow{\sim} \mathcal{L}(f, R)$.*

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

$$w_{k+2} - Pw_{k+1} + Qw_k = \omega(\eta\theta^{k+2}) - P\omega(\eta\theta^{k+1}) + Q\omega(\eta\theta^k) = \omega(\eta(\theta^{k+2} - P\theta^{k+1} + Q\theta^k)) = 0.$$

Moreover, the inverse of $\omega_R : R \otimes_{\mathbb{Z}} A_{(P,Q)} \to R^{\mathbb{N}}$ is given by $(w_k)_{k\geq 0} \mapsto (w_1 - Pw_0) \otimes 1 + w_0 \otimes \theta$.

Corollary 3.3. *Let m be a positive integer, and let $\eta, \eta' \in A_{(P,Q)}$. Then $\eta \equiv \eta' \mod m$ if and only if $\omega(\eta) \equiv \omega(\eta') \mod m$ and $\omega(\eta\theta) \equiv \omega(\eta'\theta) \mod m$.*

Proof. We obtain the result, applying Proposition 3.2 to $R = \mathbb{Z}/m\mathbb{Z}$.

Example 3.4. Let $(L_k)_{k\geq 0} = (0, 1, \dots)$ denote the Lucas sequence associated to $t^2 - Pt + Q$. Then we have $\omega(1) = \{\omega(\theta^k)\}_{k\geq 0} = (L_k)_{k\geq 0}$. Therefore, $\theta^k \equiv 1 \mod m$ if and only if $L_k \equiv 0 \mod m$ and $L_{k+1} \equiv 1 \mod m$.

3.5. We define an R-algebra structure of $\mathcal{L}(f, R)$ through the R-isomorphism $\omega_R : R \otimes_{\mathbb{Z}} A_{(P,Q)} \overset{\sim}{\to} \mathcal{L}(f, R) = R \otimes_{\mathbb{Z}} \mathcal{L}(f, \mathbb{Z})$. Therefore, the Lucas sequence $(L_k)_{k\geq 0} = \omega(1)$ is the unit of the ring $\mathcal{L}(f, \mathbb{Z})$.

More precisely, let R be a ring and $\boldsymbol{w} = (w_k)_{k\geq 0}, \boldsymbol{w}' = (w'_k)_{k\geq 0} \in \mathcal{L}(f, R)$. Then the product of $\boldsymbol{w}$ and $\boldsymbol{w}'$ is given by

$$(w_0 w'_1 + w_1 w'_0 - P w_0 w'_0, w_1 w'_1 - Q w_0 w'_0, \dots).$$

It is readily seen that the multiplication by θ on $R \otimes_{\mathbb{Z}} A_{(P,Q)}$ induces the shift operation $(w_k)_{k\geq 0} \mapsto (w_{k+1})_{k\geq 0}$ on $\mathcal{L}(f, R)$ through the isomorphism $\omega_R : R \otimes_{\mathbb{Z}} A_{(P,Q)} \overset{\sim}{\to} \mathcal{L}(f, R)$.

Definition 3.6. An automorphism σ of the ring $A_{(P,Q)} = \mathbb{Z}[t]/(t^2 - Pt + Q)$ is defined by $\sigma(\theta) = P - \theta$. Under the identification $\omega : A_{(P,Q)} \overset{\sim}{\to} \mathcal{L}(f, \mathbb{Z})$, the automorphism σ of $\mathcal{L}(f, \mathbb{Z})$ is given by $(w_0, w_1, \dots) \mapsto (-w_0, w_1 - P w_0, \dots)$.

Let R be a ring and $\eta \in R \otimes_{\mathbb{Z}} A_{(P,Q)}$. We define $\operatorname{Nr} \eta \in R$ by $\operatorname{Nr} \eta = \eta\sigma(\eta)$. For example, we have $\operatorname{Nr} \theta = Q$. Obviously, η is invertible in $R \otimes_{\mathbb{Z}} A_{(P,Q)}$ if and only if $\operatorname{Nr} \eta$ is invertible in R.

Now let $\boldsymbol{w} = (w_k)_{k\geq 0} \in \mathcal{L}(f, R)$. Define $\mathit{\Delta}(\boldsymbol{w}) \in R$ by $\mathit{\Delta}(\boldsymbol{w}) = w_1^2 - P w_0 w_1 + Q w_0^2$. If $\eta \in R \otimes_{\mathbb{Z}} A_{(P,Q)}$ and $\boldsymbol{w} = \omega(\eta)$, then we have $\operatorname{Nr} \eta = \mathit{\Delta}(\boldsymbol{w})$. Therefore, the sequence $\boldsymbol{w} = (w_k)_{k\geq 0}$ is invertible in $\mathcal{L}(f, R)$ if and only if $\mathit{\Delta}(\boldsymbol{w}) = w_1^2 - P w_0 w_1 + Q w_0^2$ is invertible in R.

3.7. Put now $\delta = t \mod (t^2 - D)$ in $A_D = \mathbb{Z}[t]/(t^2 - D)$. Then $\delta \mapsto -P + 2\theta$ gives rise to a homomorphism of rings $\xi_{(\theta,\delta)} : A_D = \mathbb{Z}[t]/(t^2 - D) \to A_{(P,Q)} = \mathbb{Z}[t]/(t^2 - Pt + Q)$.

Hereafter we assume that R is a $\mathbb{Z}[1/2]$-algebra. Then $\xi_{(\theta,\delta),R} : R \otimes_{\mathbb{Z}} A_D \overset{\sim}{\to} R \otimes_{\mathbb{Z}} A_{(P,Q)}$ is an isomorphism of R-algebras. Moreover, we obtain an isomorphism of R-algebras $\omega_R \circ \xi_{(\theta,\delta),R} : R \otimes_{\mathbb{Z}} A_D \overset{\sim}{\to} \mathcal{L}(f, R)$, which sends $a \otimes 1 + b \otimes \delta$ to $(2b, a + Pb, \dots)$. The inverse is given by $(w_k)_{k\geq 0} \mapsto (w_1 - P w_0/2) \otimes 1 + (w_0/2) \otimes \delta$.

By abuse of notaion, we denote simply by ω_R the composite $\omega_R \circ \xi_{(\theta,\delta),R}$. We shall often identify the R-algebra $\mathcal{L}(f, R)$ with $R \otimes_{\mathbb{Z}} A_D$, and the multiplicative group $\mathcal{L}(f, R)^\times$ with $G_D(R) = (R \otimes_{\mathbb{Z}} A_D)^\times$ through the isomorphism $\omega_R : R \otimes_{\mathbb{Z}} A_D \overset{\sim}{\to} \mathcal{L}(f, R)$. We shall denote by θ also $\xi^{-1}_{(\theta,\delta)}(\theta) = (P + \delta)/2 \in \mathbb{Z}[1/2] \otimes_{\mathbb{Z}} A_D = \mathbb{Z}[1/2][t](t^2 - D)$.

Let $\boldsymbol{w} = (w_k)_{k\geq 0} \in \mathcal{L}(f, R)^\times$ corresponding to $\eta \in G_D(R)$. Then we obtain an equality in $G_{(D)}(R)$:

$$\beta(\eta) = \Big(\frac{(2w_1 - Pw_0)w_0}{4(w_1^2 - Pw_0w_1 + Qw_0^2)}, \frac{w_0^2}{4(w_1^2 - Pw_0w_1 + Qw_0^2)}\Big)$$

and an equality in $U_D(R)$:

$$\gamma(\eta) = \Big(\frac{2w_1^2 - 2Pw_0w_1 + (P^2 - 2Q)w_0^2}{2(w_1^2 - Pw_0w_1 + Qw_0^2)}, \frac{(2w_1 - Pw_0)w_0}{2(w_1^2 - Pw_0w_1 + Qw_0^2)}\Big).$$

For example, $\theta = (P/2, 1/2) \in G_D(\mathbb{Z}[1/2Q])$ corresponds to the shifted Lucas sequence $(L_{k+1})_{k\geq 0} = (1, P, \dots)$, and we have

$$\beta(\theta) = \Big(\frac{P}{4Q}, \frac{1}{4Q}\Big),\ \gamma(\theta) = \Big(\frac{P^2 - 2Q}{2Q}, \frac{P}{2Q}\Big).$$

Here is another interesting example. The element $\delta = (0, 1) \in G_D(\mathbb{Z}[1/D])$ corresponds to the companion Lucas sequence $(S_k)_{k\geq 0} = (2, P, \dots)$, and we have

$$\beta(\delta) = \Big(0, -\frac{1}{D}\Big),\ \gamma(\delta) = (-1, 0).$$

Assume now that D is invertible and square in R, and take $r \in R$ such that $r^2 = D$. Then, combining the isomorphism $\xi : G_{D,R} \xrightarrow{\sim} \mathbb{G}^2_{m,R}$ and the isomorphism $\omega : G_D(R) \xrightarrow{\sim} \mathcal{L}(f, R)^\times$, we obtain a commutative diagram

$$\begin{tikzcd}
R^\times \times R^\times \arrow[d, "\gamma"] & G_D(R) \arrow[l, "\xi"', "\sim"] \arrow[r, "\omega", "\sim"'] \arrow[d, "\gamma"] & \mathcal{L}(f, R)^\times \arrow[d, "\text{projection}"] \\
R^\times & U_D(R) \arrow[l, "\xi"', "\sim"] \arrow[r] & \mathbb{P}^1(R)
\end{tikzcd}$$

Here $\gamma : R^\times \times R^\times \to R^\times$ is given by $(s, t) \mapsto s/t$. Let $\boldsymbol{w} = (w_k)_{k\geq 0} \in \mathcal{L}(f, R)^\times$. Then, putting $\alpha = (P + r)/2$ and $\beta = (P - r)/2$, we obtain

$$\gamma(\xi(\omega^{-1}(\boldsymbol{w}))) = \frac{2w_1 - (P - r)w_0}{2w_1 - (P + r)w_0} = \frac{w_1 - \beta w_0}{w_1 - \alpha w_0}.$$

For example, the Lucas sequence $\boldsymbol{L} = (0, 1, \dots) \in \mathcal{L}(f, R)^\times$ corresonds to $1 \in R^\times$. If Q is invertible in R, then the sifted Lucas sequence $(1, P, \dots) \in \mathcal{L}(f, R)^\times$ corresonds to $\alpha/\beta \in R^\times$. On the other hand, the companion Lucas sequence $\boldsymbol{S} = (2, P, \dots) \in \mathcal{L}(f, R)^\times$ corresonds to $-1 \in R^\times$.

Virtually, $(\alpha^k)_{k\geq 0} \in \mathcal{L}(f, R)$ and $(\beta^k)_{k\geq 0} \in \mathcal{L}(f, R)$ correspond to ∞ and 0, respectively.

Remark 3.8. Assume that D is not a square. Then the ring $A_{(P,Q)}$ is isomorphic to $\mathbb{Z}[\dfrac{P + \sqrt{D}}{2}]$. Moreover, for $\eta \in \mathbb{Q} \otimes_{\mathbb{Z}} A_{(P,Q)} = \mathbb{Q}[\dfrac{P + \sqrt{D}}{2}]$, we have

$$\omega(\eta) = \mathrm{Tr}\frac{\eta}{\sqrt{D}},$$

taking $\theta = \dfrac{P + \sqrt{D}}{2}$.

From 3.9 to 3.17, we give an interpretation of the rank and the period of Lucas sequences and new proofs for more or less known facts in our context.

Definition 3.9. 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 $L_k \equiv 0 \mod m$ (resp. $L_k \equiv 0 \mod m$ and $L_{k+1} \equiv 1 \mod m$), if exists. We shall denote by $r(m)$ (resp. $k(m)$) the rank (resp. the period) of the Lucas sequence $(L_k)_{k\geq 0} \mod m$.

Proposition 3.11. *Let m be an odd integer with $m \geq 3$ and $(m, Q) = 1$. Then we have*:
(1) *$k(m)$ is equal to the order of $\theta = \left(\frac{P}{2}, \frac{1}{2}\right)$ in $G_D(\mathbb{Z}/m\mathbb{Z})$;*
(2) *$r(m)$ is equal to the order of $\beta(\theta) = \left(\frac{P}{4Q}, \frac{1}{4Q}\right)$ in $G_{(D)}(\mathbb{Z}/m\mathbb{Z})$.*

Proof. The assertion (1) follows from Corollary 3.3, as is explained in Example 3.4. The assertion (2) follows from Proposition 3.12.

Proposition 3.12. *Let p be an odd prime and $\eta \in \mathbb{Z}_{(p)} \otimes_{\mathbb{Z}} A_D$. Put $w_0 = \omega(\eta)$ and $w_1 = \omega(\eta\theta)$. Let n be a positive integer. Then $\mathrm{ord}_p w_0 \geq n$ and $\mathrm{ord}_p w_1 = 0$ if and only if $\eta \in G_D(\mathbb{Z}_{(p)}) = (\mathbb{Z}_{(p)} \otimes_{\mathbb{Z}} A_D)^\times$ and $\beta(\eta) \in \mathrm{Ker}[G_{(D)}(\mathbb{Z}_{(p)}) \to G_{(D)}(\mathbb{Z}/p^n\mathbb{Z})]$.*

Proof. Put $\eta = u + v\delta$. Then we obtain $w_0 = 2v$ and $w_1 = u + Pv$. If $\mathrm{ord}_p w_0 \geq n$ and $\mathrm{ord}_p w_1 = 0$, then $u^2 - Dv^2 = w_1^2 - Pw_0w_1 + Qw_0^2$ is a unit in $\mathbb{Z}_{(p)}$ and $\mathrm{ord}_p v = \mathrm{ord}_p w_0 \geq n$. It follows that $\eta = (u, v) \in G_D(\mathbb{Z}_{(p)})$ and

$$\beta(\eta) = \left(\frac{uv}{u^2 - Dv^2}, \frac{v^2}{u^2 - Dv^2}\right) \in \mathrm{Ker}[G_{(D)}(\mathbb{Z}_{(p)}) \to G_{(D)}(\mathbb{Z}/p^n\mathbb{Z})].$$

Conversely, assume that $\eta \in G_D(\mathbb{Z}_{(p)})$ and $\beta(\eta) \in \mathrm{Ker}[G_{(D)}(\mathbb{Z}_{(p)}) \to G_{(D)}(\mathbb{Z}/p^n\mathbb{Z})]$, which means that $\mathrm{ord}_p(u^2 - Dv^2) = 0$, $\mathrm{ord}_p uv \geq n$ and $\mathrm{ord}_p v^2 \geq n$. These imply $\mathrm{ord}_p v > 0$ and $\mathrm{ord}_p u = 0$, and therefore, $\mathrm{ord}_p v \geq n$. Hence we obtain $\mathrm{ord}_p w_0 \geq n$ and $\mathrm{ord}_p w_1 = 0$.

Colollary 3.13. *Let m be an odd integer with $m \geq 3$ and $(m, Q) = 1$. Then*:
(1) *Let k be a positive integer. If $L_k \equiv 0 \mod m$, then we have $r(m)|k$.*
(2) *Let k be a positive integer. If $L_k \equiv 0 \mod m$ and $L_{k+1} \equiv 1 \mod m$, then we have $k(m)|k$.*
(3) *The rank $r(m)$ divides the period $k(m)$. Moreover, if $Q = 1$, then we have*

$$k(m) = \begin{cases} r(m) & \text{if } k(m) \text{ is odd} \\ 2r(m) & \text{if } k(m) \text{ is even} \end{cases}$$

Proof. The assertions (1) and (2) follow from the standard argument on the order.

We can verify $r(m)|k(m)$, noting that the homomorphism $\beta : G_D(\mathbb{Z}/m\mathbb{Z}) \to G_{(D)}(\mathbb{Z}/m\mathbb{Z})$ is surjective. Furthermore, if $Q = 1$, then $\theta \in U_D(\mathbb{Z}/m\mathbb{Z})$. Therefore we obtain the last assertion, noting that the homomorphism $\beta : G_{(D)}(\mathbb{Z}/m\mathbb{Z}) \to U_D(\mathbb{Z}/m\mathbb{Z})$ is injective and that the composite of homomorphisms $\gamma = \alpha \circ \beta : U_D(\mathbb{Z}/m\mathbb{Z}) \to G_D(\mathbb{Z}/m\mathbb{Z}) \to U_D(\mathbb{Z}/m\mathbb{Z})$ is the square map.

Colollary 3.14. *Let p be an odd prime. Then $k(p)/r(p)$ divides $p-1$.*

Proof. It is sufficient to notice that $\mathbb{G}_m(\mathbb{Z}/p\mathbb{Z}) = \mathrm{Ker}[\beta : G_D(\mathbb{Z}/p\mathbb{Z}) \to G_{(D)}(\mathbb{Z}/p\mathbb{Z})]$ is of order $p-1$.

Corollary 3.15. *Let p be an odd prime and n a positive integer. Assume $(P,Q) \neq (\pm 1, 1)$, and put $\nu = \mathrm{ord}_p L_{r(p)}$. Then we have*:
(1) $\nu = \mathrm{ord}_p L_{k(p)}$;
(2) $r(p^n) = \begin{cases} r(p) & (n \leq \nu) \\ p^{n-\nu} r(p) & (n > \nu) \end{cases}$;
(3) $k(p^n) = \begin{cases} k(p) & (n \leq \nu) \\ p^{n-\nu} k(p) & (n > \nu) \end{cases}$.

Proof. The assumption $(P,Q) \neq (\pm 1, 1)$ assures that $L_k \neq 0$ for any $k > 0$.

First we prove the assertion (2). Assume that $n \leq \nu$. Then we have $r(p) \leq r(p^n) \leq r(p^\nu)$. On the other hand, we have $r(p^\nu) \leq r(p)$ since $L_{r(p)}$ is divisible by p^ν. These imply $r(p^n) = r(p)$.

Assume now that $n > \nu$. By the definition of ν, we have

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

and

$$\beta(\theta)^{r(p)} \not\in \mathrm{Ker}[G_{(D)}(\mathbb{Z}_{(p)}) \to G_{(D)}(\mathbb{Z}/p^{\nu+1}\mathbb{Z})].$$

Therefore, by Corollary 2.16 and Remark 2.17, we obtain

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

and

$$\beta(\theta)^{p^{n-\nu-1}r(p)} \not\in \mathrm{Ker}[G_{(D)}(\mathbb{Z}_{(p)}) \to G_{(D)}(\mathbb{Z}/p^n\mathbb{Z})].$$

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

We can prove the assertion (3) similarily by Corollary 2.12. Now we prove the assertion (1). Put $\nu' = \mathrm{ord}_p L_{k(p)}$. Assume that $\nu' < \nu$. Then we have

$$L_{k(p)} \not\equiv 0 \mod p^{\nu'+1}, \ L_{r(p)} \equiv 0 \mod p^{\nu'+1},$$

which contradicts the divisibility $r(p)|k(p)$. Assume now that $\nu' > \nu$. Then, by (3) and (2), we have $k(p^{\nu+1}) = k(p)$ and $r(p^{\nu+1}) = pr(p)$. Hence we obtain $pr(p)|k(p)$. On the other hand, by Corollary 3.14, we have $k(p)|(p-1)r(p)$. This is a contradiction.

Corollary 3.16. *Let p be an odd prime. Then*:
(1) *If* $\left(\dfrac{D}{p}\right) = 1$, *then we have $k(p)|(p-1)$ and $r(p)|(p-1)$;*
(2) *If* $\left(\dfrac{D}{p}\right) = -1$, *then we have $k(p)|(p^2-1)$ and $r(p)|(p+1)$;*

(3) *If* $p|D$, *then* $k(p)|p(p-1)$ *and* $r(p) = p$. *Furthermore, if* $p \neq 3$, *or* $p = 3$ *and* $D \not\equiv -3 \mod 9$, *then we have* $r(p^n) = p^n$, *and therefore,* $\mathrm{ord}_p L_{r(p)} = 1$.

(4) *If* $Q = 1$, *then we have*

$$\varepsilon(p) = \begin{cases} k(p)|(p+1) & \text{if } \left(\dfrac{D}{p}\right) = -1 \\ \\ k = p \text{ or } 2p & \text{if } p|D \end{cases}.$$

Proof. By Remark 1.6 and Remark 1.9, we have

$$G_D(\mathbb{Z}/p\mathbb{Z}) = \begin{cases} \mathbb{Z}/(p-1)\mathbb{Z} \times \mathbb{Z}/(p-1)\mathbb{Z} & \text{if } \left(\dfrac{D}{p}\right) = 1 \\ \mathbb{Z}/(p^2-1)\mathbb{Z} & \text{if } \left(\dfrac{D}{p}\right) = -1 \\ \mathbb{Z}/p(p-1)\mathbb{Z} & \text{if } p|D \end{cases}$$

and

$$G_{(D)}(\mathbb{Z}/p\mathbb{Z}) = \begin{cases} \mathbb{Z}/(p-1)\mathbb{Z} & \text{if } \left(\dfrac{D}{p}\right) = 1 \\ \mathbb{Z}/(p+1)\mathbb{Z} & \text{if } \left(\dfrac{D}{p}\right) = -1 \\ \mathbb{Z}/p\mathbb{Z} & \text{if } p|D \end{cases}.$$

These imply (1), (2) and the first assertion of (3).

Assume now that $p|D$ and that $p \neq 3$, or $p = 3$ and $D \not\equiv -3 \mod 9$. Then $G_{(D)}(\mathbb{Z}/p^n\mathbb{Z})$ is cyclic of order p^n by Corollary 2.21. Therefore, $\beta(\theta) = (P/4Q, 1/4Q)$ generates $G_{(D)}(\mathbb{Z}/p^n\mathbb{Z})$ for all $n > 1$ since $\beta(\theta)$ generates $G_{(D)}(\mathbb{Z}/p\mathbb{Z})$.

Now we prove the asseertion (4). If $Q = 1$, then $\theta \in U_D(\mathbb{Z}/p\mathbb{Z})$. Hence it is sufficient to note

$$U_D(\mathbb{Z}/p\mathbb{Z}) = \begin{cases} \mathbb{Z}/(p+1)\mathbb{Z} & \text{if } \left(\dfrac{D}{p}\right) = -1 \\ \\ \mathbb{Z}/2p\mathbb{Z} & \text{if } p|D \end{cases}.$$

Remark 3.17. Assume that $p = 3$ and $D \equiv -3 \mod 9$. Then $L_3 = P^2 - Q = D + 3Q$ and $\nu = \mathrm{ord}_3(D + 3Q) \geq 2$.

Conversely, for any $\nu \geq 2$, there exists non-zero integers P and Q with $(P, Q) = 1$, $D \equiv -3 \mod 9$ and $\mathrm{ord}_3 L_3 = \nu$.

Indeed, let N be a non-zero integer, and put $P = 6N - 1$ and $Q = (3N + 1)^2$. Then we have $(P, Q) = 1$, $D = -3(12N + 1)$ and $D + 3Q = 9N(3N - 2)$. These imply that $D \equiv -3 \mod 9$ and $\mathrm{ord}_3 L_3 = 2 + \mathrm{ord}_3 N$.

We conclude the section, by discussing the action of $G_{(D)}(\mathbb{Z}/p^n\mathbb{Z})$ on $\mathbb{P}^1(\mathbb{Z}/p^n\mathbb{Z})$ for an odd prime p and a positive integer n. We refer to [10, Section 2] concerning a precise argument on the action of $PGL_{2,\mathbb{Z}}$ on $\mathbb{P}^1_{\mathbb{Z}}$.

3.18. Let R be a ring. Then a homomorphism $i_R : G_D(R) \to GL(2, R)$ is defined by

$$i_R : \eta = (u, v) \mapsto \begin{pmatrix} u - Pv & -2Qv \\ 2v & u + Pv \end{pmatrix},$$

which is represented by a homomorphism of group schemes $i : G_D \to GL_2$. If 2 is invertible in R, then $i_R : G_D(R) \to GL(2, R)$ is injective. It follows that $i : G_D \to GL_2$ is a closed immersion over $\mathbb{Z}[1/2]$.

Let $\eta = (u, v) \in G_D(\mathbb{Q})$, and put $w_0 = \omega(\eta)$ and $w_1 = \omega(\eta\theta)$. Then we have

$$\begin{pmatrix} u - Pv & -2Qv \\ 2v & u + Pv \end{pmatrix} = \begin{pmatrix} w_1 - Pw_0 & -Qw_0 \\ w_0 & w_1 \end{pmatrix}$$

and

$$u^2 - Dv^2 = w_1^2 - Pw_0w_1 + Qw_0^2.$$

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

$$\begin{tikzcd}
0 \arrow[r] & \mathbb{G}_m \arrow[r] \arrow[d, equal] & G_D \arrow[r, "\beta"] \arrow[d, "i"] & G_{(D)} \arrow[r] \arrow[d, "i"] & 0 \\
1 \arrow[r] & \mathbb{G}_m \arrow[r] & GL_2 \arrow[r] & PGL_2 \arrow[r] & 1
\end{tikzcd}.$$

The induced homomorphism $i : G_{(D)} \to PGL_2$ is a closed immersion over $\mathbb{Z}[1/2]$.

Notation 3.19. We shall denote by Θ all the subgroup of $G_D(\mathbb{Z}[1/2Q])$ generated by $\theta = (P/2, 1/2)$, the subgroup of $G_{(D)}(\mathbb{Z}[1/2Q])$ generated by $\beta(\theta) = (P/4Q, 1/4Q)$ and the subgroup of $U_D(\mathbb{Z}[1/2Q])$ generated by $\gamma(\theta) = ((P^2 - 2Q)/2Q, P/2Q)$.

Notation 3.20. We have

$$i(\theta) = i(\frac{P}{2}, \frac{1}{2}) = \begin{pmatrix} 0 & -Q \\ 1 & P \end{pmatrix} \in GL(2, \mathbb{Z}[\frac{1}{Q}]).$$

By the abbreviation, we shall denote by Θ the image of the subgroup Θ of $G_{(D)}(\mathbb{Z}[1/Q])$ by $i : G_{(D)}(\mathbb{Z}[1/Q]) \to PGL(2, \mathbb{Z}[1/Q])$. Let p be a prime with $(p, Q) = 1$. Then we obtain $\Theta \subset PGL(2, \mathbb{Z}_{(p)})$.

Let $(w_n)_{n\geq 0} \in \mathcal{L}(f, \mathbb{Q})$. Then it is readily seen that

$$(w_{n+1}\ w_{n+2}) = (w_n\ w_{n+1}) \begin{pmatrix} 0 & -Q \\ 1 & P \end{pmatrix}.$$

3.21. Let p be a prime with $(p, Q) = 1$, and let $\boldsymbol{w} = (w_k)_{k\geq 0} \in \mathcal{L}(f, \mathbb{Z}_{(p)})$. Then we have

$$(w_0, w_1) = (w_1, w_2) = (w_2, w_3) = \cdots$$

in $\mathbb{Z}_{(p)}$ since $\begin{pmatrix} 0 & -Q \\ 1 & P \end{pmatrix}$ is invertible in $GL(2, \mathbb{Z}_{(p)})$. In particular, if $(w_0, w_1) = \mathbb{Z}_{(p)}$, then we have $(w_k, w_{k+1}) = \mathbb{Z}_{(p)}$ for all $k > 0$.

Notation 3.22. Let p be a prime and n a positive integer. Then we have

$$\mathbb{P}^1(\mathbb{Z}_{(p)}) = \{(w_0 : w_1) \; ; \; w_0, w_1 \in \mathbb{Z}_{(p)} \text{ and } (w_0, w_1) = \mathbb{Z}_{(p)}\}$$

and

$$\mathbb{P}^1(\mathbb{Z}/p^n\mathbb{Z}) = \{(w_0 : w_1) \; ; \; w_0, w_1 \in \mathbb{Z}/p^n\mathbb{Z} \text{ and } (w_0, w_1) = \mathbb{Z}/p^n\mathbb{Z}\},$$

by [5, Corollaire 4.2.6]. We can verify that the embeddings $\mathbb{Z} \to \mathbb{Z}_{(p)} \to \mathbb{Q}$ induce bijections $\mathbb{P}^1(\mathbb{Z}) \xrightarrow{\sim} \mathbb{P}^1(\mathbb{Z}_{(p)}) \xrightarrow{\sim} \mathbb{P}^1(\mathbb{Q})$, canceling denominators.

Proposition 3.23. *Let p be an odd prime with $(p, Q) = 1$ and n a positive integer. Then we have*

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

Proof. It is sufficient to verify that

$$\{(w_0 : w_1) \in \mathbb{P}^1(\mathbb{Z}/p^n\mathbb{Z}) \; ; \; (w_k)_{k\geq 0} \in \mathcal{L}(f, \mathbb{Z}/p^n\mathbb{Z}) \text{ and } w_k \neq 0 \text{ for any } k\} = \mathbb{P}^1(\mathbb{Z}/p^n\mathbb{Z}) - \infty.\Theta,$$

where $\infty = (0 : 1) \in \mathbb{P}^1(\mathbb{Z}/p^n\mathbb{Z})$. The assertion is deduced from the following observations: $w_k = 0$ for some $k \Leftrightarrow (w_k : w_{k+1}) = \infty$ for some $k \Leftrightarrow (w_0 : w_1) \in \infty.\Theta$.

Remark 3.24. The assertion of Proposition 3.23 is eatabished in the case of $n = 1$ and $Q = \pm 1$ by Aoki-Sakai [1, Theorem 1]. We can also interpret their reults [1, Theorem 2 and Theorem 3] as statements on the Θ-orbit decomposition in $\mathbb{P}^1(\mathbb{F}_p)$.

Theorem 3.25. *Let p be an odd prime with $(p, Q) = 1$ and n a positive integer. Let $\boldsymbol{w} = (w_k)_{k\geq 0} \in \mathcal{L}(f, \mathbb{Z}_{(p)})$, and put $\mu = \mathrm{ord}_p \mathit{\Delta}(\boldsymbol{w})$. Assume that $(w_0, w_1) = \mathbb{Z}_{(p)}$. Then we have*

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

Proof. The assertion holds true if $(w_0 : w_1) \in \infty.\Theta$.

Assume now that $(w_0 : w_1) \in \mathbb{P}^1(\mathbb{Z}/p^n\mathbb{Z}) - \infty.\Theta$. Then we can verify that

$$\frac{w_{k+1}}{w_k} - \frac{w_1}{w_0} = -\frac{w_1^2 - Pw_0w_1 + Qw_0^2}{w_0w_n} L_k = -\frac{\mathit{\Delta}(\boldsymbol{w})}{w_0w_n} L_k,$$

noting that

$$w_k = \frac{(w_1 - \beta w_0)\alpha^k - (w_1 - \alpha w_0)\beta^k}{\alpha - \beta}, \; L_k = \frac{\alpha^k - \beta^k}{\alpha - \beta}.$$

Here α and β are the roots of quadratic equation $t^2 - Pt + Q = 0$.

This implies

$$\mathrm{ord}_p\Big(\frac{w_{k+1}}{w_k} - \frac{w_1}{w_0}\Big) = \mu + \mathrm{ord}_p L_k,$$

and therefore:

(a) If $n \leq \mu$, then $\dfrac{w_{k+1}}{w_k} - \dfrac{w_1}{w_0} \equiv 0 \mod p^n$;

(b) If $n > \mu$, then we have implications

$$\frac{w_{k+1}}{w_k} - \frac{w_1}{w_0} \equiv 0 \mod p^n \;\Leftrightarrow\; L_k \equiv 0 \mod p^{n-\mu} \;\Leftrightarrow\; k \text{ is divisible by } r(p^{n-\mu}).$$

3.26. Let R be a $\mathbb{Z}[1/2]$-algebra. Then the composite

$$G_D(R) = (R \otimes_{\mathbb{Z}} A_D)^\times \to R \otimes_{\mathbb{Z}} A_D \overset{\omega}{\to} \mathcal{L}(R, \mathbb{Q}) = \mathbb{A}^2(R)$$

is given by $(u, v) \mapsto (2v, u + Pv)$ and represented by a G_D-equivariant open immersion $\omega : G_{D,\mathbb{Z}[1/2]} \to \mathbb{A}^2_{\mathbb{Z}[1/2]}$. As is mentioned in [10, Corollary 2.9], $\omega : G_{D,\mathbb{Z}[1/2]} \to \mathbb{A}^2_{\mathbb{Z}[1/2]}$ induces a $G_{(D)}$-equivariant open immersion $\omega : G_{(D),\mathbb{Z}[1/2]} \to \mathbb{P}^2_{\mathbb{Z}[1/2]}$. Moreover, if $\mathrm{Pic}(R) = 0$, then we obtain a commutative diagram

$$\begin{tikzcd}
G_D(R) \arrow[r, "\sim"] \arrow[d, "\beta"'] & \mathcal{L}(f, R)^\times \arrow[d] & \\
G_{(D)}(R) \arrow[r, "\sim"] & \mathcal{L}(f, R)^\times / R^\times \arrow[r] & \mathbb{P}^1(R)
\end{tikzcd} .$$

By abuse of notaion, we shall denote by $\omega : G_{(D)}(R) \to \mathbb{P}^1(R)$ the map induced by $\omega : G_D(R) \to \mathcal{L}(f, R) = \mathbb{A}^2(R)$. It is readily seen that $\omega : G_{(D)}(R) \to \mathbb{P}^1(R)$ is a $G_{(D)}(R)$-equivariant injection.

Remark 3.27. A sequence $\boldsymbol{w} = (w_k)_{k \geq 0} \in \mathcal{L}(f, \mathbb{Z})$ is said to be reduced if w_0 and w_1 are relatively prime to each other. We put

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

Then $(w_0, w_1) \mapsto (w_0 : w_1)$ gives rise to a bijection $\mathcal{R}(f, \mathbb{Z}) \overset{\sim}{\to} \mathbb{P}^1(\mathbb{Z}) = \mathbb{P}^1(\mathbb{Q})$.

Furthermore, a complete representative system of $\mathcal{L}(f, \mathbb{Q})^\times / \mathbb{Q}^\times \subset \mathbb{P}^1(\mathbb{Q})$ is given by

$$\{\boldsymbol{w} = (w_k)_{k \geq 0} \in \mathcal{R}(f, \mathbb{Z}) \;;\; \Delta(\boldsymbol{w}) = w_1^2 - P w_0 w_1 + Q w_0^2 \neq 0\}.$$

Indeed, the iclusion map $\{\boldsymbol{w} \in \mathcal{R}(f, \mathbb{Z}) \;;\; \Delta(\boldsymbol{w}) \neq 0\} \to \mathcal{L}(f, \mathbb{Q})^\times$ is a section of the canonical surjection $\mathcal{L}(f, \mathbb{Q})^\times \to \mathcal{L}(f, \mathbb{Q})^\times / \mathbb{Q}^\times$.

Similarly, a complete representative system of $\mathcal{L}(f, \mathbb{Z}_{(p)})^\times / \mathbb{Z}_{(p)}^\times \subset \mathbb{P}^1(\mathbb{Z}_{(p)}) = \mathbb{P}^1(\mathbb{Q})$ is given by

$$\{\boldsymbol{w} = (w_k)_{k \geq 0} \in \mathcal{R}(f, \mathbb{Z}) \;;\; \Delta(\boldsymbol{w}) = w_1^2 - P w_0 w_1 + Q w_0^2 \not\equiv 0 \mod p\}.$$

Indeed, the iclusion map $\{\boldsymbol{w} \in \mathcal{R}(f, \mathbb{Z}) \;;\; \Delta(\boldsymbol{w}) \not\equiv 0 \mod p\} \to \mathcal{L}(f, \mathbb{Z}_{(p)})^\times$ is a section of the canonical surjection $\mathcal{L}(f, \mathbb{Z}_{(p)})^\times \to \mathcal{L}(f, \mathbb{Z}_{(p)})^\times / \mathbb{Z}_{(p)}^\times$.

3.28. Let p an odd prime. Then the $G_{(D)}$-equivariant immersion $\omega : G_{(D),\mathbb{Z}[1/2]} \to \mathbb{P}^2_{\mathbb{Z}[1/2]}$ yields a commutative diagram

$$\begin{tikzcd}
G_{(D)}(\mathbb{Q}) \arrow[r, "\omega"] & \mathbb{P}^1(\mathbb{Q}) \\
G_{(D)}(\mathbb{Z}_{(p)}) \arrow[r, "\omega"] \arrow[u] \arrow[d] & \mathbb{P}^1(\mathbb{Z}_{(p)}) \arrow[u, "\wr"'] \arrow[d] \\
G_{(D)}(\mathbb{Z}/p^n\mathbb{Z}) \arrow[r, "\omega"] & \mathbb{P}^1(\mathbb{Z}/p^n\mathbb{Z})
\end{tikzcd} .$$

Note that $\#\mathbb{P}^1(\mathbb{Z}/p^n\mathbb{Z}) = (p+1)p^{n-1}$.

Now we investigate the $G_{(D)}(\mathbb{Z}_{(p)})$-orbit decompositions of $\mathbb{P}^1(\mathbb{Z}_{(p)}) = \mathbb{P}^1(\mathbb{Q})$ and $\mathbb{P}^1(\mathbb{Z}/p^n\mathbb{Z})$ in some cases.

3.28.1. Assume that D is a square. Take $r \in \mathbb{Z}$ such that $r^2 = D$, and put $\alpha = (P+r)/2$ and $\beta = (P-r)/2$. Then $(\alpha^k)_{k\geq 0}, (\beta^k)_{k\geq 0} \in \mathcal{L}(f,\mathbb{Z})$ since α and β are the roots of the quadratic equation $t^2 - Pt + Q = 0$. Moreover, $(1:\alpha), (1:\beta) \in \mathbb{P}^1(\mathbb{Q})$ are the fixed points for the action by $G_{(D)}(\mathbb{Q})$, and the $G_{(D)}(\mathbb{Q})$-orbit decompsition of $\mathbb{P}^1(\mathbb{Q})$ is given by

$$\mathbb{P}^1(\mathbb{Q}) = \infty . G_{(D)}(\mathbb{Q}) \cup \{(1:\alpha)\} \cup \{(1:\beta)\},$$

where $\infty = (0:1)$.

By chasing the commutative diagram mentioned in 3.7

$$\begin{tikzcd}
 & & G_D(\mathbb{Q}) \arrow[r, "\omega", "\sim"'] \arrow[d, "\beta"] & \mathcal{L}(f,\mathbb{Q})^\times \arrow[d, "\text{projection}"] \\
\mathbb{Q}^\times & U_D(\mathbb{Q}) \arrow[l, "\xi", "\sim"'] & G_{(D)}(\mathbb{Q}) \arrow[l, "\alpha", "\sim"'] \arrow[r, "\omega"] & \mathbb{P}^1(\mathbb{Q})
\end{tikzcd}$$

we obtain the standard $\mathbb{Q}^\times$-orbit decomposition

$$\mathbb{P}^1(\mathbb{Q}) = \mathbb{Q}^\times \cup \{\infty\} \cup \{0\}.$$

Assume now that D is not divisible by p. Then $G_{(D)}(\mathbb{Q})/G_{(D)}(\mathbb{Z}_{(p)}) = U_D(\mathbb{Q})/U_D(\mathbb{Z}_{(p)})$ is isomorphic to $\mathbb{Z}$ as is remarked in 1.3. More explicitly, for $l \in \mathbb{Z}$, put

$$\eta_l = \Big(\frac{1}{2}(p^l+1), \frac{1}{2r}(p^l-1)\Big) \in G_D(\mathbb{Q}).$$

Then we obtain

$$\gamma(\eta_l) = \alpha(\beta(\eta_l)) = \Big(\frac{1}{2}(p^l + \frac{1}{p^l}), \frac{1}{2r}(p^l - \frac{1}{p^l})\Big) \in U_D(\mathbb{Q})$$

and

$$\xi(\gamma(\eta_l)) = p^l \in \mathbb{Q}^\times.$$

Therefore, $\eta_l \mapsto l$ yields an isomorphism $U_D(\mathbb{Q})/U_D(\mathbb{Z}_{(p)}) \xrightarrow{\sim} \mathbb{Z}$.

On the other hand, we have

$$\omega(\eta_l) = \Big(\frac{1}{r}(p^l-1), \frac{1}{r}(\alpha p^l - \beta), \dots\Big) \in \mathcal{L}(f,\mathbb{Q})^\times.$$

Basing on the equality, we define $P_l \in \mathbb{P}^1(\mathbb{Z})$ by

$$P_l = \begin{cases} (1-p^l : \alpha - p^l\beta) & \text{if } l > 0 \\ (0:1) & \text{if } l = 0 \\ (p^{-l}-1 : p^{-l}\alpha - \beta) & \text{if } l < 0 \end{cases}$$

for $l \in \mathbb{Z}$, Let $F_l \subset \mathbb{P}^1(\mathbb{Q}) = \mathbb{P}^1(\mathbb{Z})$ denote the $G_{(D)}(\mathbb{Z}_{(p)})$-orbit of P_l. Then $G_{(D)}(\mathbb{Z}_{(p)})$ acts on F_l freely and transitively for each l, and the coset decomposition $G_{(D)}(\mathbb{Q})/G_{(D)}(\mathbb{Z}_{(p)}) = \mathbb{Z}$ gives a $G_{(D)}(\mathbb{Z}_{(p)})$-orbit decomposition

$$\mathbb{P}^1(\mathbb{Q}) - \{(1:\alpha), (1:\beta)\} = \bigcup_{l \in \mathbb{Z}} F_l$$

through the $G_{(D)}(\mathbb{Z}_{(p)})$-equivariant injection $\omega : G_{(D)}(\mathbb{Q}) \to \mathbb{P}^1(\mathbb{Q})$.

Under the identification $\mathbb{P}^1(\mathbb{Q}) = \mathcal{R}(f, \mathbb{Z})$, we have

$$F_0 = \{\boldsymbol{w} \in \mathcal{R}(f,\mathbb{Z}) \ ; \ \mathrm{ord}_p \varDelta(\boldsymbol{w}) = 0\},$$

and, for each $l > 0$,

$$F_{-l} \cup F_l = \{\boldsymbol{w} \in \mathcal{R}(f,\mathbb{Z}) \ ; \ \mathrm{ord}_p \varDelta(\boldsymbol{w}) = l\}.$$

Now let $F_{l,n}$ denote the image of F_l by the canonical surjection $\mathbb{P}^1(\mathbb{Q}) = \mathbb{P}^1(\mathbb{Z}) \to \mathbb{P}^1(\mathbb{Z}/p^n\mathbb{Z})$. Then we obtain $G_{(D)}(\mathbb{Z}_{(p)})$-equivariant maps

$$\begin{tikzcd}
\vdots \arrow[d] & {} \arrow[dr] & \vdots \arrow[d] & \vdots \arrow[d] & \vdots \arrow[d] & \vdots \arrow[d] & \vdots \arrow[d] & \vdots \arrow[d] & \vdots \arrow[d] & {} \arrow[dl] \\
\mathbb{P}^1(\mathbb{Z}/p^3\mathbb{Z}) \arrow[d] & & F_{-3,3} \arrow[dr] & F_{-2,3} \arrow[d] & F_{-1,3} \arrow[d] & F_{0,3} \arrow[d] & F_{1,3} \arrow[d] & F_{2,3} \arrow[d] & F_{3,3} \arrow[dl] & \\
\mathbb{P}^1(\mathbb{Z}/p^2\mathbb{Z}) \arrow[d] & & & F_{-2,2} \arrow[dr] & F_{-1,2} \arrow[d] & F_{0,2} \arrow[d] & F_{1,2} \arrow[d] & F_{2,2} \arrow[dl] & & \\
\mathbb{P}^1(\mathbb{Z}/p\mathbb{Z}) & & & & F_{-1,1} & F_{0,1} & F_{1,1} & & &
\end{tikzcd}$$

and the $G_{(D)}(\mathbb{Z}_{(p)})$-orbit decomposition

$$\mathbb{P}^1(\mathbb{Z}/p^n\mathbb{Z}) = \bigcup_{-n \le l \le n} F_{l,n}$$

for each $n > 0$. Moreover, we have

$$\#F_{0,n} = (p-1)p^{n-1}, \ \#F_{-n,n} = \#F_{n,n} = 1$$

and, for $0 < l < n$,

$$\#F_{-l,n} = \#F_{l,n} = (p-1)p^{n-l-1}.$$

The reduction map $\mathbb{P}^1(\mathbb{Z}) \to \mathbb{P}^1(\mathbb{Z}/p^n\mathbb{Z})$ sends $(1:\alpha), (1:\beta) \in \mathbb{P}^1(\mathbb{Z}) = \mathbb{P}^1(\mathbb{Q})$ into $F_{n,n}$ and $F_{-n,n}$ respectively, since we have $P_n = (1:\alpha)$ and $P_{-n} = (1:\beta)$ in $\mathbb{P}^1(\mathbb{Z}/p^n\mathbb{Z})$.

3.28.2. Assume that D is not a square. Then the isomorphism $\omega : G_D(\mathbb{Q}) \xrightarrow{\sim} \mathcal{L}(f,\mathbb{Z})^\times = \mathcal{L}(f,\mathbb{Z}) - \{0\}$ induces a bijection $\omega : G_{(D)}(\mathbb{Q}) \xrightarrow{\sim} (\mathcal{L}(f,\mathbb{Z}) - \{0\})/\mathbb{Q}^\times = \mathbb{P}^1(\mathbb{Q})$. That is is to say, $G_{(D)}(\mathbb{Q})$ acts on $\mathbb{P}^1(\mathbb{Q})$ freely and transitively.

Case 1. D is not a square and $\left(\dfrac{D}{p}\right) = 1$. We obtain a commutative diagram

$$\begin{tikzcd}
G_{(D)}(\mathbb{Q}) \arrow[r, "\overset{\omega}{\sim}"] & \mathbb{P}^1(\mathbb{Q}) \\
G_{(D)}(\mathbb{Z}_{(p)}) \arrow[u] \arrow[r, "\omega"] \arrow[d] & \mathbb{P}^1(\mathbb{Z}_{(p)}) \arrow[u, "\wr"'] \arrow[d] \\
G_{(D)}(\mathbb{Z}/p^n\mathbb{Z}) \arrow[r, "\omega"] & \mathbb{P}^1(\mathbb{Z}/p^n\mathbb{Z})
\end{tikzcd} .$$

Let $\mathfrak{p}$ be a prime ideal of $\mathbb{Q}(\sqrt{D})$ over p, and take an integer π in $\mathbb{Q}(\sqrt{D})$ such that $\mathrm{ord}_{\mathfrak{p}}\pi = 1$ and $\mathrm{ord}_{\bar{\mathfrak{p}}}\pi = 0$. Then $\pi^l \mapsto l$ yields an isomorphism $G_{(D)}(\mathbb{Q})/G_{(D)}(\mathbb{Z}_{(p)}) \xrightarrow{\sim} \mathbb{Z}$, as is proved in 1.5.

For $l \in \mathbb{Z}$, put

$$F_l = \{[\omega(\pi^l\eta)] \ ; \ \eta \in G_D(\mathbb{Z}_{(p)})\} \subset \mathbb{P}^1(\mathbb{Q}).$$

Then $G_{(D)}(\mathbb{Z}_{(p)})$ acts on F_l freely and transitively for each l, and the coset decomposition $G_{(D)}(\mathbb{Q})/G_{(D)}(\mathbb{Z}_{(p)}) = \mathbb{Z}$ gives a $G_{(D)}(\mathbb{Z}_{(p)})$-orbit decomposition

$$\mathbb{P}^1(\mathbb{Q}) = \bigcup_{l\in\mathbb{Z}} F_l$$

through the $G_{(D)}(\mathbb{Z}_{(p)})$-equivariant bijection $\omega : G_{(D)}(\mathbb{Q}) \xrightarrow{\sim} \mathbb{P}^1(\mathbb{Q})$.

Under the identification $\mathbb{P}^1(\mathbb{Q}) = \mathcal{R}(f,\mathbb{Z})$, we have

$$F_0 = \{\boldsymbol{w} \in \mathcal{R}(f,\mathbb{Z}) \ ; \ \mathrm{ord}_p\mathit{\Delta}(\boldsymbol{w}) = 0\},$$

and, for each $l > 0$,

$$F_{-l} \cup F_l = \{\boldsymbol{w} \in \mathcal{R}(f,\mathbb{Z}) \ ; \ \mathrm{ord}_p\mathit{\Delta}(\boldsymbol{w}) = l\}.$$

Now let $F_{l,n}$ denote the image of F_l by the canonical surjection $\mathbb{P}^1(\mathbb{Q}) = \mathbb{P}^1(\mathbb{Z}) \to \mathbb{P}^1(\mathbb{Z}/p^n\mathbb{Z})$. Then, as is done in 3.18.1, we obtain $G_{(D)}(\mathbb{Z}_{(p)})$-equivariant maps

$$\begin{tikzcd}
\vdots \arrow[d] & {} \arrow[dr] & \vdots \arrow[d] & \vdots \arrow[d] & \vdots \arrow[d] & \vdots \arrow[d] & \vdots \arrow[d] & \vdots \arrow[d] & \vdots \arrow[d] & {} \arrow[dl] \\
\mathbb{P}^1(\mathbb{Z}/p^3\mathbb{Z}) \arrow[d] & & F_{-3,3} \arrow[dr] & F_{-2,3} \arrow[d] & F_{-1,3} \arrow[d] & F_{0,3} \arrow[d] & F_{1,3} \arrow[d] & F_{2,3} \arrow[d] & F_{3,3} \arrow[dl] & \\
\mathbb{P}^1(\mathbb{Z}/p^2\mathbb{Z}) \arrow[d] & & & F_{-2,2} \arrow[dr] & F_{-1,2} \arrow[d] & F_{0,2} \arrow[d] & F_{1,2} \arrow[d] & F_{2,2} \arrow[dl] & & \\
\mathbb{P}^1(\mathbb{Z}/p\mathbb{Z}) & & & & F_{-1,1} & F_{0,1} & F_{1,1} & & &
\end{tikzcd}$$

and the $G_{(D)}(\mathbb{Z}_{(p)})$-orbit decomposition

$$\mathbb{P}^1(\mathbb{Z}/p^n\mathbb{Z}) = \bigcup_{-n\leq l\leq n} F_{l,n}$$

for each $n > 0$. Moreover, we have

$$\#F_{0,n} = (p-1)p^{n-1},\ \#F_{-n,n} = \#F_{n,n} = 1$$

and, for $0 < l < n$,

$$\#F_{-l,n} = \#F_{l,n} = (p-1)p^{n-l-1}.$$

Case 2. $\left(\dfrac{D}{p}\right) = 1$. In this case, by Proposition 1.5, we have $G_{(D)}(\mathbb{Z}_{(p)}) = G_{(D)}(\mathbb{Q})$. Hence we obtain a commutative diagram

$$\begin{tikzcd}
G_{(D)}(\mathbb{Q}) \arrow[r, "\overset{\omega}{\sim}"] & \mathbb{P}^1(\mathbb{Q}) \\
G_{(D)}(\mathbb{Z}_{(p)}) \arrow[u, "\wr"'] \arrow[r, "\overset{\omega}{\sim}"] \arrow[d] & \mathbb{P}^1(\mathbb{Z}_{(p)}) \arrow[u, "\wr"'] \arrow[d] \\
G_{(D)}(\mathbb{Z}/p^n\mathbb{Z}) \arrow[r, "\overset{\omega}{\sim}"] & \mathbb{P}^1(\mathbb{Z}/p^n\mathbb{Z})
\end{tikzcd},$$

and there is nothing to do.

Case 3. $\mathrm{ord}_p D = 1$. We obtain a commutative diagram

$$\begin{tikzcd}
G_{(D)}(\mathbb{Q}) \arrow[r, "\overset{\omega}{\sim}"] & \mathbb{P}^1(\mathbb{Q}) \\
G_{(D)}(\mathbb{Z}_{(p)}) \arrow[u] \arrow[r, "\omega"] \arrow[d] & \mathbb{P}^1(\mathbb{Z}_{(p)}) \arrow[u, "\wr"'] \arrow[d] \\
G_{(D)}(\mathbb{Z}/p^n\mathbb{Z}) \arrow[r, "\omega"] & \mathbb{P}^1(\mathbb{Z}/p^n\mathbb{Z})
\end{tikzcd}.$$

Let $\mathfrak{p}$ be the prime ideal of $\mathbb{Q}(\sqrt{D})$ over p, and take an integer π in $\mathbb{Q}(\sqrt{D})$ such that $\mathrm{ord}_{\mathfrak{p}}\pi = 1$, for example, $\pi = \sqrt{D}$. Then $\pi^l \mapsto l$ yields an isomorphism $G_{(D)}(\mathbb{Q})/G_{(D)}(\mathbb{Z}_{(p)}) \xrightarrow{\sim} \mathbb{Z}/2\mathbb{Z}$, as is proved in 1.5.

For $l = 0, 1$, put

$$F_l = \{[\omega(\pi^l\eta)]\ ;\ \eta \in G_D(\mathbb{Z}_{(p)})\} \subset \mathbb{P}^1(\mathbb{Q}).$$

Then $G_{(D)}(\mathbb{Z}_{(p)})$ acts on F_0 and F_1 both freely and transitively, and the coset decomposition $G_{(D)}(\mathbb{Q})/G_{(D)}(\mathbb{Z}_{(p)}) = \mathbb{Z}/2\mathbb{Z}$ gives a $G_{(D)}(\mathbb{Z}_{(p)})$-orbit decomposition

$$\mathbb{P}^1(\mathbb{Q}) = F_0 \cup F_1$$

through the $G_{(D)}(\mathbb{Z}_{(p)})$-equivariant bijection $\omega : G_{(D)}(\mathbb{Q}) \xrightarrow{\sim} \mathbb{P}^1(\mathbb{Q})$.

Under the identification $\mathbb{P}^1(\mathbb{Q}) = \mathcal{R}(f, \mathbb{Z})$, we have

$$F_l = \{\boldsymbol{w} \in \mathcal{R}(f, \mathbb{Z})\ ;\ \mathrm{ord}_p\Delta(\boldsymbol{w}) = l\}.$$

It should be mentioned that F_0 is $G_D(\mathbb{Z}_{(p)})$-the orbit of $[\boldsymbol{L}]$ and F_1 is the $G_D(\mathbb{Z}_{(p)})$-orbit of $[\boldsymbol{S}]$ in $\mathcal{L}(f,\mathbb{Q})/\mathbb{Q}^\times$. In other words, F_0 is $G_D(\mathbb{Z}_{(p)})$-the orbit of $(0:1)$ and F_1 is the $G_D(\mathbb{Z}_{(p)})$-orbit of $(2:P)$ in $\mathbb{P}^1(\mathbb{Q})$.

Now let $F_{l,n}$ denote the image of F_l by the canonical surjection $\mathbb{P}^1(\mathbb{Q}) = \mathbb{P}^1(\mathbb{Z}) \to \mathbb{P}^1(\mathbb{Z}/p^n\mathbb{Z})$. Then we obtain the $G_{(D)}(\mathbb{Z}_{(p)})$-orbit decomposition

$$\mathbb{P}^1(\mathbb{Z}/p^n\mathbb{Z}) = F_{0,n} \cup F_{1,n}$$

for each $n > 0$. Moreover, we have

$$\#F_{0,n} = p^n,\ \#F_{1,n} = p^{n-1}.$$

4. Laxton groups

Throughout the section, we fix *non-zero integers P, Q relatively prime to each other* with $(P,Q) \neq (\pm 2, 1)$, and put $f(t) = t^2 - Pt + Q$ and $D = P^2 - 4Q$.

Definition 4.1. Now we recall te defintion of the group $G(f)$ due to Laxton [7, Section 2], modifying descriptions and notations. We shall call $G(f)$ the Laxton group associated to the quadratic polynomial $f(t) = t^2 - Pt + Q$.

Put $\mathcal{L}(f,\mathbb{Z})^\circ = \{(w_k)_{k\geq 0} \in \mathcal{L}(f,\mathbb{Z})\ ;\ (w_0,w_1) \neq (0,0)\}$. We define an equivalence relation $\sim_L$ on $\mathcal{L}(f,\mathbb{Z})^\circ$ as the relation generated by the following two equivalence relations:
(1) for $\boldsymbol{v},\boldsymbol{w} \in \mathcal{L}(f,\mathbb{Z})^\circ$, 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 $\boldsymbol{v} = (v_k)_{k\geq 0}, \boldsymbol{w} = (w_k)_{k\geq 0} \in \mathcal{L}(f,\mathbb{Z})^\circ$, 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 $k \geq 0$
([7, Section 1, p724, ℓ36]).

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

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

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

([7, Section 2, p726, ℓ5]), which coincides with the multiplication mentioned in 3.5. Then $\mathcal{L}(f,\mathbb{Z})^\circ/\sim_L$ is a commutative group ([7, Proposition 2.1]).

Fix now a prime p. Put

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

for each positive integer n ([7, Section 3, p727, $\ell 16$ and Section 1, p725, $\ell 21$]). Then $G(f,p^n)$ is a subgroup $G(f)$ ([7, Proposition 3.1]). Futhermore, put

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

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 $G(f)$ ([7, Section 3, p728, $\ell 28$]).

Summing up, we have gotten a descending chain of subgroups

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

Theorem 4.2. *Put $\theta=(P/2,1/2)\in G_D(\mathbb{Q})$, and let Θ denote the subgroup of $G_{(D)}(\mathbb{Q})$ generated by $\beta(\theta)=(P/4Q,1/4Q)$. Then the isomorphism $\omega: U_D(\mathbb{Q})=G_{(D)}(\mathbb{Q})\xrightarrow{\sim}\mathcal{L}(f,\mathbb{Q})^\times/\mathbb{Q}^\times$ induces an isomorphism $\omega: U_D(\mathbb{Q})/\Theta=G_{(D)}(\mathbb{Q})/\Theta\xrightarrow{\sim}G(f)$.*

Proof. Let $\eta,\eta'\in A_D=\mathbb{Z}[t]/(t^2-D)$, and put $\boldsymbol{w}=(w_k)_{k\geq 0}=(\omega(\xi_{(\theta,\delta)}(\eta\theta^k))$ and $\boldsymbol{w}'=(w'_k)_{k\geq 0}=(\omega(\xi_{(\theta,\delta)}(\eta'\theta^k))$. Then there exist non-zero integers k and l such that $k\boldsymbol{w}=l\boldsymbol{w}'$ if and only if $\gamma(\eta)=\gamma(\eta')$ in $G_{(D)}(\mathbb{Q})=G_D(\mathbb{Q})/\mathbb{Q}^\times$. Indeed, the inclusion $\mathcal{L}(f,\mathbb{Z})^\circ\to\mathcal{L}(f,\mathbb{Q})^\times$ induces an isomorphism $\mathcal{L}(f,\mathbb{Z})^\circ/\sim'_L\xrightarrow{\sim}\mathcal{L}(f,\mathbb{Q})^\times/\mathbb{Q}^\times$.

On the other hand, there exists a positive integer n such that $w_{k+n}=w'_k$ for all $k\geq 0$ or $w_k=w'_{k+n}$ for all $k\geq 0$ if and only if $\eta\theta^n=\eta'$ or $\eta=\eta'\theta^n$ for some $n>0$. Hence the result.

Corollary 4.3. *Let p be an odd prime with $(p,Q)=1$. Then we have $\Theta\subset G_{(D)}(\mathbb{Z}_{(p)})$. Furthermore, put $r=[(\mathrm{ord}_pD)/2]$ and $\tilde{D}=D/p^{2r}$. Then the descending chain of subgroups of $U_D(\mathbb{Q})=G_{(D)}(\mathbb{Q})$:*

$$U_D(\mathbb{Q})\supset U_{\tilde{D}}(\mathbb{Z}_{(p)})\supset G_{(D)}(\mathbb{Z}_{(p)})\supset G_{(p^2D)}(\mathbb{Z}_{(p)})\supset\cdots\supset G_{(p^{2n}D)}(\mathbb{Z}_{(p)})\supset\cdots$$

gives a descending chain of subgroups of $G(f)$:

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

More precisely,

(1) *The isomorphism $\omega: G_{(D)}(\mathbb{Q})/\Theta\xrightarrow{\sim}G(f)$ inducecs isomophisms*

$$U_{\tilde{D}}(\mathbb{Z}_{(p)})/\Theta\xrightarrow{\sim}H(f,p),$$

$$G_{(D)}(\mathbb{Z}_{(p)})/\Theta\xrightarrow{\sim}K(f,p)$$

and

$$(G_{(p^{2n}D)}(\mathbb{Z}_{(p)})+\Theta)/\Theta\xrightarrow{\sim}G(f,p^n)$$

for each $n>0$.

(2) *The isomorphism* $\omega : G_{(D)}(\mathbb{Q})/\Theta \xrightarrow{\sim} G(f)$ *inducecs isomophisms*

$$U_D(\mathbb{Q})/U_{\tilde{D}}(\mathbb{Z}_{(p)}) \xrightarrow{\sim} G(f)/H(f,p),$$
$$U_{\tilde{D}}(\mathbb{Z}_{(p)})/G_{(D)}(\mathbb{Z}_{(p)}) \xrightarrow{\sim} H(f,p)/K(f,p)$$

and

$$G_{(D)}(\mathbb{Z}_{(p)})/(G_{(p^{2n}D)}(\mathbb{Z}_{(p)}) + \Theta) \xrightarrow{\sim} K(f,p)/G(f,p^n)$$

for each $n > 0$.

(3) *We have*

$$G(f)/H(f,p) = \begin{cases} \mathbb{Z} & \text{if } \left(\dfrac{\tilde{D}}{p}\right) = 1 \\ 0 & \text{if } \left(\dfrac{\tilde{D}}{p}\right) = -1 \text{ or } p|\tilde{D} \end{cases}.$$

(4) *If* $(p, D) = 1$, *then* $H(f,p) = K(f,p)$. *Otherwise, we have*

$$|H(f,p)/K(f,p)| = \begin{cases} (p-1)p^{r-1} & \textit{if } \left(\dfrac{\tilde{D}}{p}\right) = 1 \\ (p+1)p^{r-1} & \textit{if } \left(\dfrac{\tilde{D}}{p}\right) = -1 \\ 2p^r & \textit{if } p|\tilde{D} \end{cases}.$$

(5) $K(f,p)/G(f,p^n)$ *is isomorphic to* $G_{(D)}(\mathbb{Z}/p^n\mathbb{Z})/\Theta_n$. *Therefore, we have*

$$|K(f,p)/G(f,p^n)| = \begin{cases} (p-1)p^{n-1}/r(p^n) & \textit{if } \left(\dfrac{D}{p}\right) = 1 \\ (p+1)p^{n-1}/r(p^n) & \textit{if } \left(\dfrac{D}{p}\right) = -1 \\ p^n/r(p^n) & \textit{if } p|D \end{cases}.$$

Here Θ_n *denotes the image of* Θ *by the reduction map* $G_{(D)}(\mathbb{Z}_{(p)}) \to G_{(D)}(\mathbb{Z}/p^n\mathbb{Z})$.

(6) *Put* $\nu = \mathrm{ord}_p L_{r(p)}$. *Then we have* $|G(f,p^n)/G(f,p^{n+1})| = p$ *if* $n < \nu$, *and* $G(f,p^n) = G(f,p^\tau)$ *if* $n \geq \nu$.

Proof. Note that the assumption $(p, Q) = 1$ implies $\Theta \subset G_{(D)}(\mathbb{Z}_{(p)})$. First we prove the assertion (1). Under the identifications

$$G_{(D)}(\mathbb{Q}) = \mathcal{L}(f,\mathbb{Q})^\times/\mathbb{Q}^\times = \{\boldsymbol{w} = (w_k)_{k\geq 0} \in \mathcal{R}(f,\mathbb{Z}) \ ; \ \mathit{\Delta}(\boldsymbol{w}) \neq 0\},$$

we have

$$G_{(D)}(\mathbb{Z}_{(p)}) = \{\boldsymbol{w} = (w_k)_{k\geq 0} \in \mathcal{R}(f,\mathbb{Z}) \ ; \ \mathit{\Delta}(\boldsymbol{w}) \not\equiv 0 \mod p\}$$

and

$$G_{(p^{2n}D)}(\mathbb{Z}_{(p)}) = \mathrm{Ker}[G_{(D)}(\mathbb{Z}_{(p)}) \to G_{(D)}(\mathbb{Z}/p^n\mathbb{Z})] = \{(w_k)_{k\geq 0} \in \mathcal{R}(f,\mathbb{Z}) \ ; \ w_0 \equiv 0 \mod p^n\}.$$

It follows that the isomorphism $\omega : G_{(D)}(\mathbb{Q})/\Theta \xrightarrow{\sim} G(f)$ induces isomorphisms $G_{(D)}(\mathbb{Z}_{(p)})/\Theta \xrightarrow{\sim} K(f,p)$ and $(G_{(p^{2n}D)}(\mathbb{Z}_{(p)}) + \Theta)/\Theta \xrightarrow{\sim} G(f,p^n)$ for each $n > 0$.

Consider now the inclusions

$$G_{(D)}(\mathbb{Q}) \supset U_{\tilde{D}}(\mathbb{Z}_{(p)}) \supset G_{(D)}(\mathbb{Z}_{(p)}) \supset \Theta.$$

Then $U_{\tilde{D}}(\mathbb{Z}_{(p)})/G_{(D)}(\mathbb{Z}_{(p)})$ is the torsion subgroup of $G_{(D)}(\mathbb{Q})/G_{(D)}(\mathbb{Z}_{(p)})$. Indeed, as is summarized in 2.22, $G_{(D)}(\mathbb{Q})/U_{\tilde{D}}(\mathbb{Z}_{(p)}) = \mathbb{Z}$ or 0 and $U_{\tilde{D}}(\mathbb{Z}_{(p)})/G_{(D)}(\mathbb{Z}_{(p)})$ is finite.

It follows that the isomorphism $\omega : G_{(D)}(\mathbb{Q})/\Theta \overset{\sim}{\to} G(f)$ induces an isomorphism $U_{\tilde{D}}(\mathbb{Z}_{(p)})/\Theta \overset{\sim}{\to} H(f,p)$.

The assertion (2) is a direct consequence of (1). The assertions (3) and (4) are now only simple translations of the facts first summarized in 2.22.

Now we prove the assertion (5). By Lemma 2.19, $G_{(D)}(\mathbb{Z}_{(p)})/G_{(p^{2n}D)}(\mathbb{Z}_{(p)})$ is isomorphic to $G_{(D)}(\mathbb{Z}/p^n\mathbb{Z})$. Hence $G_{(D)}(\mathbb{Z}_{(p)})/(G_{(p^{2n}D)}(\mathbb{Z}_{(p)}) + \Theta)$ is isomorphic to $G_{(D)}(\mathbb{Z}/p^n\mathbb{Z})/\Theta_n$. It follows that $K(f,p)/G(f,p^n)$ is isomorphic to $G_{(D)}(\mathbb{Z}/p^n\mathbb{Z})/\Theta_n$. We can conclude that $|K(f,p)/G(f,p^n)| = |G_{(D)}(\mathbb{Z}/p^n\mathbb{Z})|/r(p^n)$, noting that $\gamma(\theta)$ is of order $r(p^n)$ in $G_{(D)}(\mathbb{Z}/p^n\mathbb{Z})$.

Finally we prove the assertion (6). Put

$$\varepsilon(p) = \begin{cases} p-1 & \mathit{if} \left(\dfrac{D}{p}\right) = 1 \\ p+1 & \mathit{if} \left(\dfrac{D}{p}\right) = -1 \\ p & \mathit{if}\, p|D \end{cases}.$$

Then, by (5), we have

$$|K(f,p)/G(f,p^n)| = \varepsilon(p)p^{n-1}/r(p^n).$$

On the other hand, by Corollary 3.15, we have

$$r(p^n) = \begin{cases} r(p) & (n < \nu) \\ p^{n-\tau}r(p) & (n \geq \nu) \end{cases}.$$

Hence we obtain

$$|K(f,p)/G(f,p^n)| = \begin{cases} \varepsilon(p)p^{n-1}/r(p) & (n < \nu) \\ p^{\tau-1}/r(p) & (n \geq \nu) \end{cases},$$

and therefore,

$$|G(f,p^n)/G(f,p^{n+1})| = \begin{cases} p & (n < \nu) \\ 1 & (n \geq \nu) \end{cases},$$

Hence the result.

Remark 4.4. Laxton established the assertions (3),(4) and (5) in the case of $n = 1$ of Corollary 4.3 as [7, Theorem 3.7 (a)(b)(c) and Theorem 3.10 (a)(b)]. It would be kind to correct some of the statements in [7].

(1) [7, Theorem 3.7 (c)] $G(f) = H(f, p)$ if $p|D$. The assertion is false if $\mathrm{ord}_p D$ is even ≥ 2 and $\left(\dfrac{\tilde{D}}{p}\right) = 1$. Indeed, we have $G(f)/H(f, p) = \mathbb{Z}$ in this case.

(2) [7, Theorem 3.7 (c)] $G(f)/G(f, p)$ is order 2 if $p|D$. The assertion is false if $\mathrm{ord}_p D \geq 2$. Indeed, we have

$$|H(f,p)/K(f,p)| = \begin{cases} (p-1)p^{r-1} & \mathit{if} \left(\dfrac{\tilde{D}}{p}\right) = 1 \\ (p+1)p^{r-1} & \mathit{if} \left(\dfrac{\tilde{D}}{p}\right) = -1 \\ 2p^r & \mathit{if}\ p|\tilde{D} \end{cases}$$

in this case.

(3) [7, Theorem 3.10 (b)] and [12, Theorem 11.1 (ii)] $G(f, p^n) = G(f, p)$ for each $n \geq 1$ if $p|D$. The assertion is false if $p = 3$ and $D \equiv -3 \mod 9$. Indeed, we have $G(f, p)/G(f, p^\nu) = p^{\nu-1}$ and $\nu \geq 2$ as is remarked in 3.17.

From 4.5 to 4.8, we simplify the descending chain of subgroups of $G(f)$:

$$G(f) \supset H(f, p) \supset K(f, p) \supset G(f, p) \supset \cdots \supset G(f, p^n) \supset \cdots$$

case by case, combining the facts mentioned above.

Example 4.5. Assume that $\left(\dfrac{D}{p}\right) = 1$ and $(p, Q) = 1$. Then the descending chain of subgroups of $G_{(D)}(\mathbb{Q}) = U_D(\mathbb{Q})$:

$$U_D(\mathbb{Q}) \supset U_D(\mathbb{Z}_{(p)}) = G_{(D)}(\mathbb{Z}_{(p)}) \supset G_{(p^2D)}(\mathbb{Z}_{(p)}) \supset \cdots \supset G_{(p^{2n}D)}(\mathbb{Z}_{(p)}) \supset \cdots$$

gives a descending chain of subgroups of $G(f)$:

$$G(f) \supset H(f, p) = K(f, p) \supset G(f, p) \supset \cdots \supset G(f, p^n) \supset \cdots .$$

Moreover,

(1) $G(f)/K(f, p)$ is isomorphic to $U_D(\mathbb{Q})/U_D(\mathbb{Z}_{(p)}) = \mathbb{Z}$;

(2) $K(f, p)/G(f, p^n)$ is isomorphic to $G_{(D)}(\mathbb{Z}/p^n\mathbb{Z})/\Theta_n = U_D(\mathbb{Z}/p^n\mathbb{Z})/\Theta_n$, which is cyclic of order $(p-1)p^{n-1}/r(p^n)$. In particular, $K(f, p)/G(f, p)$ is isomorphic to $G_{(D)}(\mathbb{F}_p)/\Theta_1 = U_D(\mathbb{F}_p)/\Theta_1$, which is cyclic of order $(p-1)/r(p)$.

Example 4.6. Assume that $\left(\dfrac{D}{p}\right) = -1$ and $(p, Q) = 1$. Then the descending chain of subgroups of $G_{(D)}(\mathbb{Q}) = U_D(\mathbb{Q})$:

$$U_D(\mathbb{Q}) = U_D(\mathbb{Z}_{(p)}) = G_{(D)}(\mathbb{Z}_{(p)}) \supset G_{(p^2D)}(\mathbb{Z}_{(p)}) \supset \cdots \supset G_{(p^{2n}D)}(\mathbb{Z}_{(p)}) \supset \cdots$$

gives a descending chain of subgroups of $G(f)$:

$$G(f) = H(f, p) = K(f, p) \supset G(f, p) \supset \cdots \supset G(f, p^n) \supset \cdots .$$

Moreover,

(1) $K(f,p)/G(f,p^n)$ is isomorphic to $G_{(D)}(\mathbb{Z}/p^n\mathbb{Z})/\Theta_n = U_D(\mathbb{Z}/p^n\mathbb{Z})/\Theta_n$, which is cyclic of order $(p{+}1)p^{n-1}/r(p^n)$. In particular, $K(f,p)/G(f,p)$ is isomorphic to $G_{(D)}(\mathbb{F}_p)/\Theta_1 = U_D(\mathbb{F}_p)/\Theta_1$, which is cyclic of order $(p+1)/r(p)$.

Example 4.7. Assume that $p \neq 2$, $\mathrm{ord}_p D = 1$ and $(p,Q) = 1$. Then the descending chain of subgroups of $G_{(D)}(\mathbb{Q}) = U_D(\mathbb{Q})$:

$$U_D(\mathbb{Q}) = U_D(\mathbb{Z}_{(p)}) \supset G_{(D)}(\mathbb{Z}_{(p)}) \supset G_{(p^2D)}(\mathbb{Z}_{(p)}) \supset \cdots \supset G_{(p^{2n}D)}(\mathbb{Z}_{(p)}) \supset \cdots$$

gives a descending chain of subgroups of $G(f)$:

$$G(f) = H(f,p) \supset K(f,p) = G(f,p) \supset \cdots \supset G(f,p^n) \supset \cdots .$$

Moreover,

(1) $G(f)/K(f,p)$ is isomorphic to $U_D(\mathbb{Z}_{(p)})/G_{(D)}(\mathbb{Z}_{(p)}) = \{\pm 1\}$. As a complete representative system of $G(f)/K(f,p)$, we can take $\{\boldsymbol{L}, \boldsymbol{S}\}$. Here $\boldsymbol{L}$ and $\boldsymbol{S}$ stand for the Lucas sequence and the companion Lucas sequence associated to $f(t) = t^2 - Pt + Q$, respectively.

(2) Assume that $p \geq 5$ or that $p = 3$, $D \not\equiv 3 \mod 9$. Then we have $G(f,p) = G(f,p^2) = G(f,p^3) = \cdots$.

Example 4.8. Consider now the case of $\mathrm{ord}_p D > 1$. The condition implies that $(p,Q) = 1$ since $(P,Q) = 1$. Put $r = [(\mathrm{ord}_p D)/2]$ and $\tilde{D} = D/p^{2r}$.

(a) Assume that $\mathrm{ord}_p D \equiv 0 \mod 2$ and $\left(\dfrac{\tilde{D}}{p}\right) = 1$. Then the descending chain of subgroups of $G_{(D)}(\mathbb{Q}) = U_D(\mathbb{Q})$:

$$U_D(\mathbb{Q}) \supset U_{\tilde{D}}(\mathbb{Z}_{(p)}) \supset G_{(D)}(\mathbb{Z}_{(p)}) \supset G_{(p^2D)}(\mathbb{Z}_{(p)}) \supset \cdots \supset G_{(p^{2n}D)}(\mathbb{Z}_{(p)}) \supset \cdots$$

gives a descending chain of subgroups of $G(f)$:

$$G(f) \supset H(f,p) \supset K(f,p) = G(f,p) = \cdots = G(f,p^n) = \cdots .$$

Moreover,

(1) $G(f)/H(f,p)$ is isomorphic to $\mathbb{Z}$;

(2) $H(f,p)/K(f,p)$ is isomorphic to $U_{\tilde{D}}(\mathbb{Z}/p^r\mathbb{Z})$, which is cyclic of order $(p-1)p^{r-1}$ by Corollary 2.15.

(b) Assume that $\mathrm{ord}_p D \equiv 0 \mod 2$ and $\left(\dfrac{\tilde{D}}{p}\right) = -1$. Then the descending chain of subgroups of $G_{(D)}(\mathbb{Q}) = U_D(\mathbb{Q})$:

$$U_D(\mathbb{Q}) = U_{\tilde{D}}(\mathbb{Z}_{(p)}) \supset G_{(D)}(\mathbb{Z}_{(p)}) \supset G_{(p^2D)}(\mathbb{Z}_{(p)}) \supset \cdots \supset G_{(p^{2n}D)}(\mathbb{Z}_{(p)}) \supset \cdots$$

gives a descending chain of subgroups of $G(f)$:

$$G(f) = H(f,p) \supset K(f,p) = G(f,p) = \cdots = G(f,p^n) = \cdots .$$

Moreover, $H(f,p)/K(f,p)$ is isomorphic to $U_{\tilde{D}}(\mathbb{Z}/p^r\mathbb{Z})$, which is cyclic of order $(p+1)p^{r-1}$ by Corollary 2.15.

(c) Assume that $\mathrm{ord}_p D \equiv 1 \mod 2$. Then the descending chain of subgroups of $G_{(D)}(\mathbb{Q}) = U_D(\mathbb{Q})$:

$$U_D(\mathbb{Q}) = U_{\tilde{D}}(\mathbb{Z}_{(p)}) \supset G_{(D)}(\mathbb{Z}_{(p)}) \supset G_{(p^2D)}(\mathbb{Z}_{(p)}) \supset \cdots \supset G_{(p^{2n}D)}(\mathbb{Z}_{(p)}) \supset \cdots$$

gives a descending chain of subgroups of $G(f)$:

$$G(f) = H(f,p) \supset K(f,p) = G(f,p) = \cdots = G(f,p^n) = \cdots .$$

Moreover, $H(f,p)/K(f,p)$ is isomorphic to $U_{\tilde{D}}(\mathbb{Z}/p^r\mathbb{Z})$, which is cyclic of order $2p^r$ by Corollary 2.15 and Corollary 2.21.

Corollary 4.9. *Let p be an odd prime with $p|Q$. Then we have $\Theta \cap G_{(D)}(\mathbb{Z}_{(p)}) = \{1\}$. Then the descending chain of subgroups of $U_D(\mathbb{Q}) = G_{(D)}(\mathbb{Q})$:*

$$U_D(\mathbb{Q}) \supset G_{(D)}(\mathbb{Z}_{(p)}) \supset G_{(p^2D)}(\mathbb{Z}_{(p)}) \supset \cdots \supset G_{(p^{2n}D)}(\mathbb{Z}_{(p)}) \supset \cdots$$

gives a descending chain of subgroups of $G(f)$:

$$G(f) \supset K(f,p) \supset G(f,p) \supset \cdots \supset G(f,p^n) \supset \cdots .$$

More precisely,

(1) The isomorphism $\omega : G_{(D)}(\mathbb{Q})/\Theta \xrightarrow{\sim} G(f)$ inducecs isomophisms

$$(G_{(D)}(\mathbb{Z}_{(p)}) + \Theta)/\Theta \xrightarrow{\sim} K(f,p)$$

and

$$(G_{(p^{2n}D)}(\mathbb{Z}_{(p)}) + \Theta)/\Theta \xrightarrow{\sim} G(f,p^n)$$

for each $n > 0$. Therefore, $K(f,p)$ is isomorphic to $G_{(D)}(\mathbb{Z}_{(p)})$, and $G(f,p^n)$ is isomorphic to $G_{(p^{2n}D)}(\mathbb{Z}_{(p)})$ for each $n > 0$.

(2) The isomorphism $\omega : G_{(D)}(\mathbb{Q})/\Theta \xrightarrow{\sim} G(f)$ inducecs isomophisms

$$U_D(\mathbb{Q})/(G_{(D)}(\mathbb{Z}_{(p)}) + \Theta) \xrightarrow{\sim} G(f,p)/K(f,p)$$

and

$$G_{(D)}(\mathbb{Z}_{(p)})/G_{(p^{2n}D)}(\mathbb{Z}_{(p)}) \xrightarrow{\sim} K(f,p)/G(f,p^n)$$

for each $n > 0$.

(3) $G(f)/K(f,p)$ is cyclic of order $\mathrm{ord}_p Q$. Therefore, we have $G(f) = H(f,p)$.

(4) $K(f,p)/G(f,p^n)$ is isomorphic to $G_{(D)}(\mathbb{Z}/p^n\mathbb{Z})$. Therefore, $K(f,p)/G(f,p^n)$ is cyclic of of order $(p-1)p^{n-1}$.

Proof. Note that the assumption $p|Q$ implies $(p,D) = 1$, $\left(\dfrac{D}{p}\right) = 1$ and $\Theta \cap G_{(D)}(\mathbb{Z}_{(p)}) = \{(0,0)\} \subset G_{(D)}(\mathbb{Q})$.

First we prove the assertion (1). As is mentioned in the proof of Corollary 4.3, under the identifications

$$G_{(D)}(\mathbb{Q}) = \mathcal{L}(f,\mathbb{Q})^\times/\mathbb{Q}^\times = \{\boldsymbol{w} = (w_k)_{k\geq 0} \in \mathcal{R}(f,\mathbb{Z})\ ;\ \Delta(\boldsymbol{w}) \neq 0\},$$

we have

$$G_{(D)}(\mathbb{Z}_{(p)}) = \{\boldsymbol{w} = (w_k)_{k\geq 0} \in \mathcal{R}(f,\mathbb{Z})\ ;\ \Delta(\boldsymbol{w}) \not\equiv 0 \mod p\}$$

and

$$G_{(p^{2n}D)}(\mathbb{Z}_{(p)}) = \mathrm{Ker}[G_{(D)}(\mathbb{Z}_{(p)}) \to G_{(D)}(\mathbb{Z}/p^n\mathbb{Z})] = \{(w_k)_{k\geq 0} \in \mathcal{R}(f,\mathbb{Z})\ ;\ w_0 \equiv 0 \mod p^n\}.$$

It follows that the isomorphism $\omega : G_{(D)}(\mathbb{Q})/\Theta \xrightarrow{\sim} G(f)$ induces isomorphisms $(G_{(D)}(\mathbb{Z}_{(p)}) + \Theta)/\Theta \xrightarrow{\sim} K(f,p)$ and $(G_{(p^nD)}(\mathbb{Z}_{(p)}) + \Theta)/\Theta \xrightarrow{\sim} G(f,p^n)$ for each $n > 0$.

The assertion (2) is a direct consequence of (1). We obtain the assertion (4), cobining (2) and Corollary 2.15.

Finally we prove the assertion (3). It is sufficient to verify that $U_D(\mathbb{Q})/(U_D(\mathbb{Z}_{(p)}) + \Theta) = G(f,p)/K(f,p)$ is cyclic of order $\mathrm{ord}_p Q$.

Assume first that D is not a square. Let $\mathfrak{p}$ denote a prime of $\mathbb{Q}(\sqrt{D})$ over p. Then the map $\eta \mapsto \mathrm{ord}_{\mathfrak{p}}\eta$ induces an isomorphism $U_D(\mathbb{Q})/U_D(\mathbb{Z}_{(p)}) \xrightarrow{\sim} \mathbb{Z}$, as is shown in 1.5. On the other hand, the subgroup Θ of $U_D(\mathbb{Q})$ is generated by $\gamma(\theta) = \theta/\bar{\theta}$, where $\theta = (P+\sqrt{D})/2$. Note now $\theta + \bar{\theta} = P$ and $(P,p) = 1$. These imply that $\mathrm{ord}_{\mathfrak{p}}\theta = 0$ or $\mathrm{ord}_{\mathfrak{p}}\bar{\theta} = 0$. On the other hand, we have $\theta\bar{\theta} = Q$, and therefore, $\mathrm{ord}_{\mathfrak{p}}\theta + \mathrm{ord}_{\mathfrak{p}}\bar{\theta} = \mathrm{ord}_{\mathfrak{p}}Q$. Hence we obtain $\mathrm{ord}_{\mathfrak{p}}\gamma(\theta) = \pm\mathrm{ord}_{\mathfrak{p}}Q$.

Next assume that D is a square. Take $r \in \mathbb{Z}$ such that $r^2 = R$. Then $(u,v) \mapsto \mathrm{ord}_p(u+rv)$ induces an isomorphism $U_D(\mathbb{Q})/U_D(\mathbb{Z}_{(p)}) \xrightarrow{\sim} \mathbb{Z}$, as is shown in 1.3. Furthermore, we have $\xi(\gamma(\theta)) = (P+r)^2/4Q$. Note now $(P+r)+(P-r) = 2P$ and $(2P,p) = 1$. These imply that $\mathrm{ord}_p(P+r) = 0$ or $\mathrm{ord}_p(P-r) = 0$. On the other hand, we have $(P+r)(P-r) = 4Q$, and therefore, $\mathrm{ord}_p(P+r) + \mathrm{ord}_p(P-r) = \mathrm{ord}_pQ$. Hence we obtain $\mathrm{ord}_p\xi(\gamma(\theta)) = \pm\mathrm{ord}_pQ$.

Remark 4.10. Laxton established the assertions (3) and (4) in the case of $n = 1$ of Corollary 4.9 as [7, Theorem 3.7 (d) and Theorem 3.10 (c)].

Here are a few numerical examples.

Example 4.11. $P = 1$, $Q = -11$, $D = 3^2 \times 5$.

In this case, we have $\left(\dfrac{5}{3}\right) = -1$, and therefore, $H(f,3)/K(f,3)$ is a cyclic group of order 4. Here are complete representative systems of $H(f,3)/K(f,3)$ in $\mathcal{L}(f,\mathbb{Z})$, $G_D(\mathbb{Q})$, $G_{(D)}(\mathbb{Q})$ and $U_D(\mathbb{Q})$. The group $H(f,3)/K(f,3)$ is generated by the class of $(1,2,\dots) \in \mathcal{L}(f,\mathbb{Z})$, to which correponds $\eta = (3/2, 1/2) \in G_D(\mathbb{Q})$.

	(w_0, w_1)	η^k	$\beta(\eta^k)$	$\gamma(\eta^k)$
$k=1$	$(1,2)$	$(\frac{3}{2},\frac{1}{2})$	$(-\frac{1}{12},-\frac{1}{36})$	$(-\frac{3}{2},-\frac{1}{6})$
$k=2$	$(1,5)$	$(\frac{9}{2},\frac{1}{2})$	$(\frac{1}{4},\frac{1}{36})$	$(\frac{7}{2},\frac{1}{2})$
$k=3$	$(2,7)$	$(6,1)$	$(-\frac{2}{3},-\frac{1}{9})$	$(-9,-\frac{4}{3})$
$k=4$	$(1,4)$	$(\frac{7}{2},\frac{1}{2})$	$(\frac{7}{4},\frac{1}{4})$	$(\frac{47}{2},\frac{7}{2})$

Example 4.12. $P = 1$, $Q = -61$, $D = 7^2 \times 5$.

In this case, we have $\left(\frac{5}{7}\right) = -1$, and therefore, $H(f, 7)/K(f, 7)$ is a cyclic group of order 8. Here are complete representative systems of $H(f, 7)/K(f, 7)$ in $\mathcal{L}(f, \mathbb{Z})$, $G_D(\mathbb{Q})$, $G_{(D)}(\mathbb{Q})$ and $U_D(\mathbb{Q})$. The group $H(f, 7)/K(f, 7)$ is generated by the class of $(1, 4, \dots) \in \mathcal{L}(f, \mathbb{Z})$, to which correponds $\eta = (7/2, 1/2) \in G_D(\mathbb{Q})$.

k	(w_0, w_1)	η^k	$\beta(\eta^k)$	$\gamma(\eta^k)$
$k=1$	$(1,4)$	$(\frac{7}{2},\frac{1}{2})$	$(-\frac{1}{28},-\frac{1}{296})$	$(-\frac{3}{2},-\frac{1}{14})$
$k=2$	$(1,11)$	$(\frac{21}{2},\frac{1}{2})$	$(\frac{3}{28},\frac{1}{296})$	$(\frac{7}{2},\frac{3}{14})$
$k=3$	$(2,15)$	$(14,1)$	$(-\frac{2}{7},-\frac{1}{49})$	$(-9,-\frac{4}{7})$
$k=4$	$(3,26)$	$(\frac{49}{2},\frac{3}{2})$	$(\frac{3}{4},\frac{9}{296})$	$(\frac{47}{2},\frac{3}{2})$
$k=5$	$(5,41)$	$(\frac{77}{2},\frac{5}{2})$	$(-\frac{55}{28},-\frac{25}{296})$	$(-\frac{123}{2},-\frac{55}{14})$
$k=6$	$(8,67)$	$(63,4)$	$(\frac{36}{7},\frac{16}{49})$	$(161,\frac{72}{7})$
$k=7$	$(13,108)$	$(\frac{203}{2},\frac{13}{2})$	$(-\frac{377}{28},-\frac{169}{296})$	$(-\frac{843}{2},-\frac{377}{14})$
$k=8$	$(3,25)$	$(\frac{47}{2},\frac{3}{2})$	$(\frac{141}{4},\frac{9}{4})$	$(\frac{2207}{2},\frac{141}{2})$

Example 4.13. $P = 1$, $Q = -151$, $D = 11^2 \times 5$.

In this case, we have $\left(\frac{5}{11}\right) = 1$, and therefore, $H(f, 11)/K(f, 11)$ is a cyclic group of order 10. Here are complete systems of $H(f, 11)/K(f, 11)$ in $\mathcal{L}(f, \mathbb{Z})$, $G_D(\mathbb{Q})$, $G_{(D)}(\mathbb{Q})$ and $U_D(\mathbb{Q})$. The group $H(f, 11)/K(f, 11)$ is generated by the class of $(1, 6, \dots) \in \mathcal{L}(f, \mathbb{Z})$, to which correponds $\eta = (11/2, 1/2) \in G_D(\mathbb{Q})$.

k	(w_0, w_1)	η^k	$\beta(\eta^k)$	$\gamma(\eta^k)$
$k = 1$	$(1, 6)$	$(\frac{11}{2}, \frac{1}{2})$	$(-\frac{1}{44}, -\frac{1}{484})$	$(-\frac{3}{2}, -\frac{1}{22})$
$k = 2$	$(1, 17)$	$(\frac{33}{2}, \frac{1}{2})$	$(\frac{3}{44}, \frac{1}{484})$	$(\frac{7}{2}, \frac{3}{22})$
$k = 3$	$(2, 23)$	$(22, 1)$	$(-\frac{2}{11}, -\frac{1}{121})$	$(-9, -\frac{4}{11})$
$k = 4$	$(3, 40)$	$(\frac{77}{2}, \frac{3}{2})$	$(\frac{21}{44}, \frac{9}{484})$	$(\frac{47}{2}, \frac{21}{22})$
$k = 5$	$(5, 63)$	$(\frac{121}{2}, \frac{5}{2})$	$(-\frac{5}{4}, -\frac{25}{484})$	$(-\frac{123}{2}, -\frac{5}{2})$
$k = 6$	$(8, 103)$	$(99, 4)$	$(\frac{36}{11}, \frac{16}{121})$	$(161, \frac{72}{11})$
$k = 7$	$(13, 166)$	$(\frac{319}{2}, \frac{13}{2})$	$(-\frac{377}{44}, -\frac{169}{484})$	$(-\frac{843}{2}, -\frac{377}{22})$
$k = 8$	$(21, 269)$	$(\frac{517}{2}, \frac{21}{2})$	$(\frac{987}{44}, \frac{441}{484})$	$(\frac{2207}{2}, \frac{987}{22})$
$k = 9$	$(34, 435)$	$(418, 17)$	$(-\frac{646}{11}, -\frac{289}{121})$	$(-2889, -\frac{1292}{11})$
$k = 10$	$(5, 64)$	$(\frac{123}{2}, \frac{5}{2})$	$(\frac{615}{4}, \frac{25}{4})$	$(\frac{15127}{2}, \frac{615}{2})$

Remark 4.14. Let p an odd prime. Then, as is discussed in 3.28, the $G_{(D)}$-equivariant immersion $\omega : G_{(D),\mathbb{Z}[1/2]} \to \mathbb{P}^2_{\mathbb{Z}[1/2]}$ yields a commutative diagram

$$\begin{tikzcd}
G_{(D)}(\mathbb{Q}) \arrow[r, "\omega"] & \mathbb{P}^1(\mathbb{Q}) \\
G_{(D)}(\mathbb{Z}_{(p)}) \arrow[r, "\omega"] \arrow[u] \arrow[d] & \mathbb{P}^1(\mathbb{Z}_{(p)}) \arrow[u, "\wr"'] \arrow[d] \\
G_{(D)}(\mathbb{Z}/p^n\mathbb{Z}) \arrow[r, "\omega"] & \mathbb{P}^1(\mathbb{Z}/p^n\mathbb{Z})
\end{tikzcd} .$$

Assume now $(p, Q) = 1$. Then we have $\Theta \subset G_{(D)}(\mathbb{Z}_{(p)})$. Passing to the quotients by the action of Θ, we obtain a commutative diagram

$$\begin{tikzcd}
G_{(D)}(\mathbb{Q})/\Theta \arrow[r, "\omega"] & \mathbb{P}^1(\mathbb{Q})/\Theta \\
G_{(D)}(\mathbb{Z}_{(p)})/\Theta \arrow[r, "\omega"] \arrow[u] \arrow[d] & \mathbb{P}^1(\mathbb{Z}_{(p)})/\Theta \arrow[u, "\wr"'] \arrow[d] \\
G_{(D)}(\mathbb{Z}/p^n\mathbb{Z})/\Theta \arrow[r, "\omega"] & \mathbb{P}^1(\mathbb{Z}/p^n\mathbb{Z})/\Theta
\end{tikzcd} ,$$

which is rewritten as

$$\begin{tikzcd}
G(f) \arrow[r, "\omega"] & \mathbb{P}^1(\mathbb{Q})/\Theta \\
K(f,p) \arrow[u] \arrow[r, "\omega"] \arrow[d] & \mathbb{P}^1(\mathbb{Z}_{(p)})/\Theta \;\; . \arrow[u, "\wr"'] \arrow[d] \\
K(f,p)/G(f,p^n) \arrow[r, "\omega"] & \mathbb{P}^1(\mathbb{Z}/p^n\mathbb{Z})/\Theta
\end{tikzcd}$$

It readily seen that the $K(f,p)$-orbit decompositions of $\mathbb{P}^1(\mathbb{Z}_{(p)})/\Theta$ and $\mathbb{P}^1(\mathbb{Z}/p^n\mathbb{Z})/\Theta$ coincide with the $G_{(D)}(\mathbb{Z}_{(p)})$-orbit decompositions of $\mathbb{P}^1(\mathbb{Z}_{(p)})$ and $\mathbb{P}^1(\mathbb{Z}/p^n\mathbb{Z})$ respectively.

We conclude the article by synthesizing the related results estabished by Laxton [7] and Ward [11] in our context.

4.15. We recall the definitions given by Ward [12] and Laxton [7] concerning the divisibility problem with a slight modification in our context.

The right action of $\Theta = \{\theta^l \ ; \ l \in \mathbb{Z}\} \subset G_D(\mathbb{Q})$ on $\mathbb{P}^1(\mathbb{Q})$ is defined by

$$(s\ t) \mapsto (s\ t) \begin{pmatrix} 0 & -Q \\ 1 & P \end{pmatrix}^l ,$$

as is mentioned in Notation 3.20. Now we give an explicit description on the right action of Θ on $\mathcal{R}(f,\mathbb{Z})$ under the identifications $\mathcal{R}(f,\mathbb{Z}) = \mathbb{P}^1(\mathbb{Z}) = \mathbb{P}^1(\mathbb{Q})$.

Let $\boldsymbol{w} = (w_k)_{k\geq 0} \in \mathcal{L}(f,\mathbb{Z})$. Then, for each $l \geq 0$, we have

$$(w_l\ w_{l+1}) = (w_0\ w_1) \begin{pmatrix} 0 & -Q \\ 1 & P \end{pmatrix}^l ,$$

which allows us to define $w_l \in \mathbb{Q}$ for $l \leq -1$ by

$$(w_l\ w_{l+1}) = (w_0\ w_1) \begin{pmatrix} 0 & -Q \\ 1 & P \end{pmatrix}^l .$$

Assume now $\boldsymbol{w} = (w_k)_{k\geq 0} \in \mathcal{R}(f,\mathbb{Z})$. Then, for each $l \in \mathbb{Z}$, there exists uniquely a relatively prime pair $(w'_0, w'_1) \in \mathbb{Z}^2$ such that $(w'_0 : w'_1) = (w_l : w_{l+1})$ in $\mathbb{P}^1(\mathbb{Q})$ and $w'_0 > 0$ or $w'_0 = 0$, $w'_1 > 0$. Moreover, $\boldsymbol{w}' = (w'_k)_{k\geq 0} \in \mathcal{L}(f,\mathbb{Z})$ is defined by the initial terms w'_0 and w'_1. It is readily seen that $\boldsymbol{w}' = \boldsymbol{w}\theta^l$ in $\mathcal{R}(f,\mathbb{Z})$.

Let p be a prime. Here are some definitions. Let $\boldsymbol{w} \in \mathcal{R}(f,\mathbb{Z})$.

(1) ([12, p41, ℓ1] and [7, p724, ℓ3]) p is said to be *a divisor of* $\boldsymbol{w}$ if there exists $\boldsymbol{w}' = (w'_k)_{k\geq 0} \in \boldsymbol{w}.\Theta \subset \mathcal{R}(f,\mathbb{Z})$ such that $w'_0 \equiv 0 \mod p$;

(2) ([7, p732, ℓ15]) p is said to be *an unbounded divisor of* $\boldsymbol{w}$ if, for any $n > 0$, there exists $\boldsymbol{w}' = (w'_k)_{k\geq 0} \in \boldsymbol{w}.\Theta \subset \mathcal{R}(f,\mathbb{Z})$ such that $w'_0 \equiv 0 \mod p^n$;

(3) ([12, p41, ℓ2]) p is said to be *a bounded divisor of* $\boldsymbol{w}$ if p is a divisor of $\boldsymbol{w}$ but p not unbounded.

Assume that p is a divisor of $\boldsymbol{w}$. Then there exists $l \in \mathbb{Z}$ such that $\boldsymbol{w}' = \boldsymbol{w}\theta^l$ in $\mathcal{R}(f, \mathbb{Z})$ and that $w'_0 \equiv 0 \mod p$. This implies

$$\varDelta(\boldsymbol{w}') = {w'_1}^2 - Pw'_0w'_1 + Q{w'_0}^2 \neq 0$$

and therefore

$$w_1^2 - Pw_0w_1 + Qw_0^2 = (w_{-l+1}^2 - Pw_{-l}w_{-l+1} + Qw_{-l}^2)Q^{-l} \neq 0.$$

Hence we obtain $\boldsymbol{w} \in \mathcal{L}(f, \mathbb{Q})^\times$. Let $\eta \in G_{(D)}(\mathbb{Q})$ corresponding to $\boldsymbol{w}$. Then, under the assumption that p is odd, we have the following implications

$$\begin{aligned} &\text{there exists } \boldsymbol{w}' = (w'_k)_{k\geq 0} \in \boldsymbol{w}.\Theta \text{ such that } w'_0 \equiv 0 \mod p^n \\ &\Leftrightarrow\ \eta \in \operatorname{Ker}[G_{(D)}(\mathbb{Z}_{(p)}) \to G_{(D)}(\mathbb{Z}/p^n\mathbb{Z})] + \Theta \\ &\Leftrightarrow\ [\boldsymbol{w}] \in G(f, p^n), \end{aligned}$$

as is mentioned in 4.3 and 4.9.

Now, for an odd prime p, we arrive at the following assertion:
(1) p is a divisor of $\boldsymbol{w}$ if and only if $[\boldsymbol{w}] \in G(f, p)$. In particuler, if $w_1^2 - Pw_0w_1 + Qw_0^2 = 0$, then p is not a divisor of $\boldsymbol{w}$.

Furthermore, assume $(p, Q) = 1$. Then we obtain the following assertions:
(2) p is a divisor of $\boldsymbol{w}$ if and only if there exists $k \geq 0$ such that $w_k \equiv 0 \mod p$;
(3) p is an unbounded divisor of $\boldsymbol{w}$ if and only if, for any $n > 0$, there exists $k \geq 0$ such that $w_k \equiv 0 \mod p^n$;
(4) Put $\nu = \operatorname{ord}_p L_{r(p)}$. Then p is a unbounded divisor of $\boldsymbol{w}$ if and only if $[\boldsymbol{w}] \in G(f, p^\nu)$.

Remark 4.16. We adopt here the definition given by Laxton [7], which is a modification of the definition given by Ward [12] in the context of Laxton group theory. Laxton avoided the case of $w_1^2 - Pw_0w_1 + Qw_0^2 = 0$, assuming that D is not a square.

The orignal definition in Ward [12] is more straightforward. 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 $(p, 2Q) = 1$.

Here are a few examples showing the difference of the two definitions. Put $P = 1$ and $Q = -3$.
(a) Define $\boldsymbol{w} = (w_k)_{k\geq 0} \in \mathcal{R}(f, \mathbb{Z})$ by $w_0 = 1$ and $w_1 = 1$. Then we obtain $w_k \equiv 1 \mod 3$ for $k \geq 0$. Therefore, 3 is not a divisor of $\boldsymbol{w}$ after Ward. On the other hand, after Laxton, 3 is a divisor of $\boldsymbol{w}$ since $w_{-1} = 0$.

(b) Define $\boldsymbol{w} = (w_k)_{k\geq 0} \in \mathcal{R}(f,\mathbb{Z})$ by $w_0 = 1$ and $w_1 = 3$. Then we obtain $w_k \equiv 0 \mod 3$ for $k \geq 1$. Therefore, 3 is a divisor of $\boldsymbol{w}$ after Ward. On the other hand, we can verify inductively

$$\mathrm{ord}_3 w_k = \begin{cases} k & \text{if } k \leq 0 \\ 1 & \text{if } k \geq 1 \end{cases}.$$

Therefore, 3 is not a divisor of $\boldsymbol{w}$ after Laxton.

It would be interesting to reformulate the argument developed by Ward [12] in our context, replacing $\mathcal{L}(f,\mathbb{Z}_{(p)})$ by $\mathcal{L}(f,\mathbb{Z}_p)$. As an example, we give a new proof of [12, Theorem 9.3] with complementary statements.

Proposition 4.17. *Let $\boldsymbol{w}$ be a reduced sequence of $\mathcal{L}(f,\mathbb{Z})$, and let p be a prime with $(p,2Q)=1$. Put $\nu = \mathrm{ord}_p L_{r(p)}$. Assume that $w_0 \equiv 0 \mod p$. Then p is a bounded divisor of $\boldsymbol{w}$ if and only if $\mathrm{ord}_p w_0 < \nu$. Moreover, in this case, we have*

$$\mathrm{ord}_p w_k = \begin{cases} \mathrm{ord}_p w_0 & \textit{if } r(p)|k \\ 0 & \textit{if } r(p) \nmid k \end{cases}.$$

Proof. First asssume that $\mathrm{ord}_p w_0 \geq \nu$. Then we obtain $[\boldsymbol{w}] \in G(f,p^\nu)$ and, by Corollary 4.3(c), $[\boldsymbol{w}] \in G(f,p^n)$ for any $n > \nu$.

Conversely, assume that p is an unbounded divisor of $\boldsymbol{w}$. Then there exists $k > 0$ such that $w_k \equiv 0 \mod p^\nu$. Now let η denote the element of $G_{(D)}(\mathbb{Z}_{(p)})$ corresponding to $\boldsymbol{w}$. Then we obtain $\eta\theta^k = 1$ in $G_{(D)}(\mathbb{Z}/p^\nu\mathbb{Z})$. Hence we have $\theta^k = 1$ in $G_{(D)}(\mathbb{Z}/p\mathbb{Z})$ since $\eta = 1$ in $G_{(D)}(\mathbb{Z}/p\mathbb{Z})$. This, together with Corollary 3.15, implies that $r(p^\nu) = r(p)$ divides k, and therefore, $\eta = \eta\theta^k = 1$ in $G_{(D)}(\mathbb{Z}/p^\nu\mathbb{Z})$, that is to say, $[\boldsymbol{w}] \in G(f,p^\nu)$.

Assume now $\mathrm{ord}_p w_0 < \nu$, and put $n = \mathrm{ord}_p w_0$. Then, by Corollary 3.15, we have $r(p^{n+1}) = r(p)$. Hence the length of the Θ-orbit $\eta\Theta$ in $G_{(D)}(\mathbb{Z}/p^{n+1}\mathbb{Z})$ is given by $r(p)$, which implies the last assertion.

References.

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

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

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

[4] A. Grothendieck, Le groupe de Brauer, Dix exposés sur la cohomologie des schémas, North-Holland (1968), 46–188.

[5] A. Grothendieck, J. Dieudonné, Éléments de géométrie algébrique, II. Inst. Hautes Etudes Sci. Publ. Math. No. 8 (1961).

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

[7] R. R. Laxton, On groups of linear recurrences, I. Duke Math. J. 36 (1969) 721–738.

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

[9] D. H. Lehmer, An extended theory of Lucas' functions. Ann. of Math. 31 (1930) 419–448.

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

[11] N. Suwa, Some remarks on Lucas pseudoprimes. Math. J. Okayama 54 (2012) 1–32.

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

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

[14] W. C. Waterhouse, B. Weisfeiler, One-dimensional affine group schemes, J. Algebra 66 (1980), 550–568.

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