CHUO MATH NO.125(2018)

# Geometric aspects of Lucas sequences, II

by

Noriyuki Suwa

*DEPARTMENT OF MATHEMATICS*
*CHUO UNIVERSITY*
*BUNKYOKU TOKYO JAPAN*

*Oct. 5 , 2018*

# GEOMETRIC ASPECTS OF LUCAS SEQUENCES, II

NORIYUKI SUWA*)

ABSTRACT. This article is a sequel of ⟨Geometric aspects of Lucas sequences, I⟩, which presents 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 2⟩.

## Introduction

This article is a sequel of [14], which treats of the divisibility problem for Lucas sequences from a geometirc viewpoint, more precisely, in framework of the group scheme theory.

First we explain the divisibility problem for Lucas sequences. 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 sequence $(L_k)_{k\geq 0}$ 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 $m$. Edouard Lucas [7] formulated results on the divisibility problem 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 $(L_k)_{k\geq 0}$. There have been piled up various kinds of results since then.

In this article we study the divisibility problem in the case where $m$ is a power of 2, while in [14] we deal with the case where $m$ is an odd prime power. The following fact is a key to our study:

Key Proposition(=Proposition 3.5) *Let $m$ be an integer with $m \geq 2$ and $(m, Q) = 1$. Then:*

(1) *the period of the Lucas sequence $(L_k)_{k\geq 0} \mod m$ is equal to the order of $\theta$ in $G_{P,Q}(\mathbb{Z}/m\mathbb{Z})$;*

(2) *the rank of the Lucas sequence $(L_k)_{k\geq 0} \mod m$ is equal to the order of $\beta(\theta)$ in $G_{(P,Q)}(\mathbb{Z}/m\mathbb{Z})$.*

Recall that 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. Moreover, $G_{P,Q} = \prod_{A/\mathbb{Z}} \mathbb{G}_{m,A}$ and $G_{(P,Q)} = (\prod_{A/\mathbb{Z}} \mathbb{G}_{m,A})/\mathbb{G}_{m,\mathbb{Z}}$, where $A = \mathbb{Z}[t]/(t^2 - Pt + Q)$ and $\theta$ stands for the image of $t$ in $A$. ($\prod_{A/\mathbb{Z}}$ denotes the Weil restriction functor associated to the ring extension $A/\mathbb{Z}$. A detailed accout is given concerning $G_{P,Q}$, $G_{(P,Q)}$ and the homomorphism $\beta : G_{P,Q} \to G_{(P,Q)}$ in Section 1.)

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

The assertion above mentioned is an analogue of the Fermat-Euler theorem, which is nowadays understood as a consequece of Lagrange's theorem applied to the multiplicative group $\mathbb{G}_m(\mathbb{Z}/m\mathbb{Z}) = (\mathbb{Z}/m\mathbb{Z})^\times$. The assertion (1) is first verified in [13, Lemma 2.7] and the assertion (2) is added in [14, Corollary 3.13], both under the assumption $(m, 2) = 1$.

Here is an example of reformulation in our context of the laws of apparition and repetition: Theorem(=Proposition 3.26+Theorem 3.27) *Let $P$ and $Q$ be non-zero integers, 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 a 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 $\Theta$ denotes the subgroup of $G_{(P,Q)}(\mathbb{Z}_{(p)})$ generated by $\beta(\theta)$, and $r(p^\nu)$ denotes the rank mod $p^\nu$ of the Lucas sequence associated to $(P, Q)$.*

The assertions above are verified by Aoki-Sakai [1, Theorem 1] under the assumption $p > 2$, $n = 1$ and $Q = \pm 1$, and in [14, Proposition 3.23 and Theorem 3.25] under the assumption $p > 2$. It should be mentioned that we have to employ the group schemes $G_{P,Q}$ and $G_{(P,Q)}$ in this article instead of $G_D$ and $G_{(D)}$ employed in [14]. It is the reason that we need deal with the residue ring $\mathbb{Z}[t]/(t^2 - Pt + Q)$, not $\mathbb{Z}[t]/(t^2 - D)$. We may recall that $\mathbb{Z}[D]$ does not coincide with the ring of integers in the quadratic extension $\mathbb{Q}(\sqrt{D})$ when $D \equiv 1 \mod 4$.

Now we explain the organization of the article. There are some descriptions overlapping [14], which we repeat with a slight modification 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 $G_{P,Q}$, $U_{P,Q}$ and $G_{(P,Q)}$ as examples of the affine group schemes

$$G_{\tilde{R}/R} = \prod_{\tilde{R}/R} \mathbb{G}_{m,\tilde{R}},$$
$$U_{\tilde{R}/R} = \mathrm{Ker}[\mathrm{Nr} : \prod_{\tilde{R}/R} \mathbb{G}_{m,\tilde{R}} \to \mathbb{G}_{m,R}],$$
$$G_{(\tilde{R}/R)} = \Big(\prod_{\tilde{R}/R} \mathbb{G}_{m,\tilde{R}}\Big)/\mathbb{G}_{m,R},$$

where $\tilde{R}/R$ is a quadratic extension of rings. We conclude the section by recalling the action by the group scheme $G_{(\tilde{R}/R)}$ on the projective line $\mathbb{P}^1_R$.

It should be mentioned that Lemmermeyer [11] sketches out a plan to study the group scheme $U_D$, called the Pell conics there. It would be intereseting to relate his study with ours.

In the Section 2, we give precise description on $G_{P,Q}(\mathbb{Z}/2^n\mathbb{Z})$ and $G_{(P,Q)}(\mathbb{Z}/2^n\mathbb{Z})$ for $n \geq 1$, which requires much more efforts than describing $G_{P,Q}(\mathbb{Z}/p^n\mathbb{Z})$ and $G_{(P,Q)}(\mathbb{Z}/p^n\mathbb{Z})$ for a prime $> 2$. In fact, we have to examine $G_D(\mathbb{Z}/2^n\mathbb{Z})$ and $G_{(D)}(\mathbb{Z}/2^n\mathbb{Z})$ in case by case as follows:

Proposition 2.9: $G_D(\mathbb{Z}/2^n\mathbb{Z})$ when $D \equiv 0 \mod 2$

Proposition 2.10: $G_D(\mathbb{Z}/2^n\mathbb{Z})$ when $D \equiv 1 \mod 8$

Proposition 2.11: $G_D(\mathbb{Z}/2^n\mathbb{Z})$ when $D \equiv -1 \mod 8$

Proposition 2.12: $G_D(\mathbb{Z}/2^n\mathbb{Z})$ when $D \equiv 5 \mod 8$

Proposition 2.13: $G_D(\mathbb{Z}/2^n\mathbb{Z})$ when $D \equiv -5 \mod 8$

Proposition 2.15: $G_{(D)}(\mathbb{Z}/2^n\mathbb{Z})$ when $D \equiv 0 \mod 2$

Proposition 2.16: $G_{(D)}(\mathbb{Z}/2^n\mathbb{Z})$ when $D \equiv 1 \mod 2$

Proposition 2.21: $G_{P,Q}(\mathbb{Z}/2^n\mathbb{Z})$ when $P \equiv 1 \mod 2$ and $Q \equiv 1 \mod 2$

Corollary 2.22: $G_{(P,Q)}(\mathbb{Z}/2^n\mathbb{Z})$ when $P \equiv 1 \mod 2$ and $Q \equiv 1 \mod 2$

In the first half of Section 3, after relating Lucas sequences with the group schems $G_{P,Q}$ and $G_{(P,Q)}$, 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 [7], Carmichael [2] and Lehmer [10], for example. Here we have to describe $r(2^n)$ and $k(2^n)$ in case by case as follows:

Theorem 3.7: $r(2^n)$ when $P \equiv 0 \mod 2$ and $Q \equiv 1 \mod 2$

Theorem 3.8: $k(2^n)$ when $P \equiv 0 \mod 2$ and $Q \equiv 1 \mod 2$

Theorem 3.12: $r(2^n)$ when $P \equiv 1 \mod 2$ and $Q \equiv 1 \mod 4$

Theorem 3.13: $r(2^n)$ when $P \equiv 1 \mod 2$ and $Q \equiv -1 \mod 4$

Theorem 3.14: $k(2^n)$ when $P \equiv 1 \mod 2$ and $Q \equiv -1 \mod 4$

Theorem 3.15: $k(2^n)$ when $P \equiv 5 \mod 8$ and $Q \equiv 1 \mod 4$

Theorem 3.16: $k(2^n)$ when $P \equiv -5 \mod 8$ and $Q \equiv 1 \mod 4$

Theorem 3.17: $k(2^n)$ when $P \equiv 1 \mod 8$ and $Q \equiv 1 \mod 4$

Theorem 3.18: $k(2^n)$ when $P \equiv -1 \mod 8$ and $Q \equiv 1 \mod 4$

In the latter half of Section 3, we add the case of $p = 2$ to the main results in [14] concerning the action by $\Theta \subset G_{(P,Q)}(\mathbb{Z}/p^n\mathbb{Z})$ on $\mathbb{P}^1(\mathbb{Z}/p^n\mathbb{Z})$. Here $\Theta$ denotes the subgroup of $G_{(P,Q)}(\mathbb{Z}/p^n\mathbb{Z})$ generated by $\beta(\theta)$.This is a reformulation and generalization of remarkable notices of Aoki-Sakai [1] from a geometric viewpoint, as is mentioned before.

In the Section 4, we reconstruct the theory developed in [8] and [9] by Laxton, eliminating the assumptions on $P$ and $Q$ imposed in [8], except $Q \neq 0$, but respecting Laxton's original idea. The main result on explicit description of the group $G(f)$ is stated as follows:

Theorem(=Theorem 4.2) *Let $P$ and $Q$ be integers with $Q \neq 0$, and put $f(t) = t^2 - Pt + Q$. Let $p$ be a prime, and let $\Theta$ denote the subgroup of $G_{(P,Q)}(\mathbb{Q})$ generated by $\beta(\theta)$. Then the isomorphism $\omega : G_{(P,Q)}(\mathbb{Q}) \overset{\sim}{\to} \mathcal{L}(f,\mathbb{Q})^\times/\mathbb{Q}^\times$ induces an isomorphism $\omega : G_{(P,Q)}(\mathbb{Q})/\Theta \overset{\sim}{\to} G(f)$.*

The assertions mentiond above are verified in [14, Theorem 4.2] under the assumption $p > 2$. (The map $\omega : G_{(P,Q)}(\mathbb{Q}) \to \mathcal{L}(f, \mathbb{Q})^\times/\mathbb{Q}^\times$ is defined in 4.1.)

Here we have to describe the descending chain of subgroups of $G(f)$

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

in case by case as follows:

| | |
|---|---|
| Corollary 4.3: | $Q \equiv 1 \mod 2,\ D \neq 0$ |
| Corollary 4.3.1: | $P \equiv 1 \mod 2,\ Q \equiv 1 \mod 2,\ D \neq 0$ |
| Corollary 4.3.2: | $P \equiv 0 \mod 2,\ Q \equiv 1 \mod 2$, or $P \equiv 2 \mod 4,\ Q \equiv -1 \mod 4$ |
| Corollary 4.3.4: | $P \equiv 2 \mod 4,\ Q \equiv 1 \mod 4$ |
| Corollary 4.5: | $P \equiv 1 \mod 2,\ Q \equiv 0 \mod 2$ |
| Corollary 4.6: | $P \equiv 2 \mod 4,\ Q \equiv 2 \mod 4,\ D \neq 0$ |
| Corollary 4.7: | $P \equiv 0 \mod 4,\ Q \equiv 2 \mod 4,\ P \neq 0$ |

The section 5 is a complement to the previous article [14], where we assume after Laxton [8] that $P$ and $Q$ are relatively prime and $D = P^2 - 4Q \neq 0$. From 5.1 to 5.3, we discuss the case where both $P$ and $Q$ are divisible by a prime $p$. In 5.4, we deal with case where $D = P^2 - 4Q = 0$. We conclude the article by giving an interpretation of a result due to Ward [14] and Hall [5] in our context. We would look for an essence behind their skillful calculation.

The author would like to express his hearty thanks to Masato Kurihara for his advise and encouragement. He is very grateful to Akira Masuoka, who reveal his interest from a point view of Hopf algebra thoery.

### 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

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

$\mathcal{R}(f, \mathbb{Z})$**:** defined in 3.25

### List of groups and group schemes

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

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

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

$G_{\tilde{R}/R} = \prod_{\tilde{R}/R} \mathbb{G}_{m,\tilde{R}}$**:** the Weil restriction of $\mathbb{G}_m$ with respect to $\tilde{R}/R$, recalled in 1.1

$U_{\tilde{R}/R} = \mathrm{Ker}[\mathrm{Nr} : \prod_{\tilde{R}/R} \mathbb{G}_{m,\tilde{R}} \to \mathbb{G}_{m,R}]$**:** recalled in 1.2

$G_{(\tilde{R}/R)} = \prod_{\tilde{R}/R} \mathbb{G}_{m,\tilde{R}}/\mathbb{G}_{m,R}$**:** recalled in 1.3

$G_{P,Q}$: defined in 1.5

$U_{P,Q}$: defined in 1.5

$G_{(P,Q)}$: defined in 1.5

$G_D$: recalled in 1.5

$U_D$: recalled in 1.5

$G_{(D)}$: recalled in 1.5

$\Theta \subset G_{P,Q}(\mathbb{Z}[1/Q])$: defined in 3.21

$\Theta \subset G_{(P,Q)}(\mathbb{Z}[1/Q])$: defined in 3.21

$\Theta \subset PGL(2,\mathbb{Z}[1/Q])$: defined in 3.22

**List of maps and morphisms**

$\mathrm{Nr} : G_{\tilde{R}/R} \to \mathbb{G}_{m,R}$: recalled in 1.1

$i : \mathbb{G}_{m,R} \to G_{\tilde{R}/R}$: recalled in 1.1

$\xi : G_{\tilde{R}/R} \otimes \tilde{R} \to \mathbb{G}^2_{m,\tilde{R}}$: defined in 1.1

$\xi : U_{\tilde{R}/R} \otimes \tilde{R} \to \mathbb{G}_{m,\tilde{R}}$: defined in 1.2

$\beta : G_{\tilde{R}/R} \to G_{(\tilde{R}/R)}$: recalled in 1.3

$\alpha : G_{(\tilde{R}/R)} \to U_{\tilde{R}/R}$: recalled in 1.3

$\gamma = \alpha \circ \beta : G_{\tilde{R}/R} \to U_{\tilde{R}/R}$: recalled in 1.3

$\xi : G_{(\tilde{R}/R)} \otimes \tilde{R} \to \mathbb{G}_{m,\tilde{R}}$: defined in 1.3.1

$\eta : G_{(\tilde{R}/R)} \to \mathbb{G}_{a,R}$: defined in 1.4.1

$\omega : \tilde{R} \to \mathcal{L}(f,R)$: 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 3.1

$r(m)$: the rank mod $m$ of the Lucas sequence $(L_k)_{k\geq 0}$, recalled in 3.4

$k(m)$: the period mod $m$ of the Lucas sequence $(L_k)_{k\geq 0}$, recalled in 3.4

$\Delta(\boldsymbol{w}) = w_1^2 - Pw_0w_1 + Qw_0^2$: the invariant of $\boldsymbol{w} = (w_k)_{k\geq 0} \in \mathcal{L}(f,R)$, recalled in 3.1

## 1. Group schemes $G_{P,Q}$, $U_{P,Q}$ and $G_{(P,Q)}$

In this section, we fix a ring $R$ and $P, Q \in R$, putting $\tilde{R} = R[t]/(t^2 - Pt + Q)$. We refer to [3] or [17] on formalisms of affine group schemes, Hopf algebras and the cohomology with coefficients in group schemes.

**Definition 1.1.** Let $R$ be a ring and $P, Q \in A$. Put $D = P^2 - 4Q$ and $\tilde{R} = R[t]/(t^2 - Pt + Q)$. Let $\theta$ denote the image of $t$ in $\tilde{R}$. Then $\{1, \theta\}$ is an $R$-basis of $\tilde{R}$, and the multiplication of $\tilde{R}$ is given by

$$(a + b\theta)(a' + b'\theta) = (aa' - Qbb') + (ab' + a'b + Pbb')\ (a, b, a', b' \in R).$$

Then we can describe explicitly the Weil restriction $\prod_{\tilde{R}/R}\mathbb{G}_{m,\tilde{R}}$ of the multiplicative group scheme $\mathbb{G}_{m,\tilde{R}}$ with respect to the ring extension $\tilde{R}/R$ in terms of Hopf algebras as follows:

$$\prod_{\tilde{R}/R}\mathbb{G}_{m,\tilde{R}} = \operatorname{Spec} R[U, V, \frac{1}{U^2+PUV+QV^2}]$$

with

(a) the multiplication

$$U \mapsto U\otimes U - QV\otimes V,\ V \mapsto U\otimes V + V\otimes U + PV\otimes V;$$

(b) the unit

$$U \mapsto 1,\ V \mapsto 0;$$

(c) the inverse

$$U \mapsto \frac{U+PV}{U^2+PUV+QV^2},\ V \mapsto -\frac{V}{U^2+PUV+QV^2}.$$

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

$$i : \mathbb{G}_{m,R} = \operatorname{Spec} R[T, \frac{1}{T}] \to \prod_{\tilde{R}/R}\mathbb{G}_{m,\tilde{R}} = \operatorname{Spec} R[U, V, \frac{1}{U^2+rUV+sV^2}],$$

defined by

$$U \mapsto T,\ V \mapsto 0.$$

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

$$\mathrm{Nr} : \prod_{\tilde{R}/R}\mathbb{G}_{m,\tilde{R}} = \operatorname{Spec} R[U, V, \frac{1}{U^2+PUV+QV^2}] \to \mathbb{G}_{m,R} = \operatorname{Spec} R[T, \frac{1}{T}],$$

defined by

$$T \mapsto U^2+PUV+QV^2.$$

It is readily seen that

(1) $i : \mathbb{G}_{m,R} \to \prod_{\tilde{R}/R}\mathbb{G}_{m,\tilde{R}}$ is a closed immersion;

(2) $\mathrm{Nr} : \prod_{\tilde{R}/R}\mathbb{G}_{m,\tilde{R}} \to \mathbb{G}_{m,R}$ is faithfully flat;

(3) $\mathrm{Nr}\circ i : \mathbb{G}_{m,R} \to \mathbb{G}_{m,R}$ is the square map.

If $D$ is not nilpotent in $R$, then $\left(\prod_{\tilde{R}/R}\mathbb{G}_{m,\tilde{R}}\right)\otimes_R R[1/D]$ is a torus over $R[1/D]$, splitting over $\tilde{R}[1/D]$. Indeed,

$$T_1 \mapsto U+\theta V,\ T_2 \mapsto U+(P-\theta)V$$

defines a homomorphism

$$\xi : \Big(\prod_{\tilde{R}/R}\mathbb{G}_{m,\tilde{R}}\Big)\otimes_R \tilde{R} = \operatorname{Spec} \tilde{R}[U, V, \frac{1}{U^2+PUV+QV^2}] \to \mathbb{G}^2_{m,\tilde{R}} = \operatorname{Spec} \tilde{R}[T_1, T_2, \frac{1}{T_1}, \frac{1}{T_2}],$$

inducing an isomorphism over $\tilde{R}[1/D]$. The inverse of $\xi \otimes_R \tilde{R}[1/D]$ is given by

$$U \mapsto \frac{1}{P-2\theta}\{(P-\theta)T_1 - \theta T_2\},\ V \mapsto \frac{1}{P-2\theta}(-T_1+T_2).$$

**Definition 1.2.** Put

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

Then

$$U_{\tilde{R}/R} = \operatorname{Spec} R[U,V]/(U^2+PUV+QV^2-1)$$

with

(a) the multiplication

$$U \mapsto U\otimes U - QV\otimes V,\ V \mapsto U\otimes V + V\otimes U + PV\otimes V;$$

(b) the unit

$$U \mapsto 1,\ V \mapsto 0;$$

(c) the inverse

$$U \mapsto U+PV,\ V \mapsto -V.$$

If $D$ is not nilpotent in $R$, then $U_{\tilde{R}/R}\otimes_R R[1/D]$ is a torus over $R[1/D]$, splitting over $\tilde{R}[1/D]$. Indeed, $T \mapsto U+\theta V$ defines a homomorphism

$$\xi : U_{\tilde{R}/R}\otimes_R \tilde{R} = \operatorname{Spec}\tilde{R}[U,V]/(U^2+PUV+QV^2-1) \to \mathbb{G}_{m,\tilde{R}} = \operatorname{Spec}\tilde{R}[T,\frac{1}{T}],$$

inducing an isomorphism over $\tilde{R}[1/D]$. Moreover, we obtain a commutative diagram with exact rows

$$\begin{tikzcd}
0 \arrow[r] & U_{\tilde{R}/R}\otimes_R \tilde{R} \arrow[r] \arrow[d, "\xi"] & (\prod_{\tilde{R}/R}\mathbb{G}_{m,\tilde{R}})\otimes_R \tilde{R} \arrow[r, "\mathrm{Nr}"] \arrow[d, "\xi"] & \mathbb{G}_{m,\tilde{R}} \arrow[r] \arrow[d, equal] & 0 \\
0 \arrow[r] & \mathbb{G}_{m,\tilde{R}} \arrow[r, "\iota"'] & \mathbb{G}^2_{m,\tilde{R}} \arrow[r, "\mu"'] & \mathbb{G}_{m,\tilde{R}} \arrow[r] & 0
\end{tikzcd}.$$

Here

$$\iota : \mathbb{G}_{m,\tilde{R}} = \operatorname{Spec}\tilde{R}[T,\frac{1}{T}] \to \mathbb{G}^2_{m,\tilde{R}} = \operatorname{Spec}\tilde{R}[T_1,T_2,\frac{1}{T_1},\frac{1}{T_2}]$$

is defined by $(T_1,T_2)\mapsto (T,T^{-1})$, and $\mu : \mathbb{G}^2_{m,\tilde{R}} \to \mathbb{G}_{m,\tilde{R}}$ denotes the multiplication.

**Definition 1.3.** We put

$$G_{(\tilde{R}/R)} = \prod_{\tilde{R}/R}\mathbb{G}_{m,\tilde{R}}/\mathbb{G}_{m,R}.$$

More explicitly,

$$G_{(\tilde{R}/R)} = \operatorname{Spec} R[X,Y]/(X^2+PXY+QY^2-Y)$$

with

(a) the multiplication

$$X \mapsto X\otimes 1 + 1\otimes X - PX\otimes X - 2QX\otimes Y - 2QY\otimes X - PQY\otimes Y,$$
$$Y \mapsto Y\otimes 1 + 1\otimes Y + (P^2-2Q)Y\otimes Y + PX\otimes Y + PY\otimes X + 2X\otimes X;$$

(b) the unit

$$X\mapsto 0,\ Y\mapsto 0;$$

as is described by Waterhouse-Weisfeiler [18]. It should be mentioned that $G_{\tilde{R}/R}$ is smooth over $R$.

Furthermore, a homomorphism of group schemes

$$\beta : \prod_{\tilde{R}/R}\mathbb{G}_{m,\tilde{R}} = \operatorname{Spec} R[U,V,\frac{1}{U^2+PUV+QV^2}]$$
$$\to G_{\tilde{R}/R} = \operatorname{Spec} R[X,Y]/(X^2+PXY+QY^2-Y)$$

is defined by

$$X\mapsto \frac{UV}{U^2+PUV+QV^2},\ Y\mapsto \frac{V^2}{U^2+PUV+QV^2}.$$

It is readily seen that the sequence

$$0 \longrightarrow \mathbb{G}_{m,R} \xrightarrow{i} \prod_{\tilde{R}/R}\mathbb{G}_{m,\tilde{R}} \xrightarrow{\beta} G_{(\tilde{R}/R)} \to 0$$

is exact.

The two group schemes $U_{\tilde{R}/R}$ and $G_{\tilde{R}/R}$ are related by a homomorphism

$$\alpha : G_{\tilde{R}/R} = \operatorname{Spec} R[X,Y]/(X^2+PXY+QY^2-Y) \to U_{\tilde{R}/R} = \operatorname{Spec} R[U,V]/(U^2+PUV+QV^2-1)$$

defined by

$$U\mapsto 1-PX-2QY,\ V\mapsto 2X+PY.$$

If $D$ is not nilpotent in $R$, then $\alpha$ is isomorphic over $R[1/D]$. Indeed, the inverse of $\alpha\otimes_R R[1/D]$ is given by

$$X\mapsto \frac{P-PU-2QV}{D},\ Y\mapsto \frac{-2+2U+PV}{D}.$$

We define also a homomorphism

$$\gamma : \prod_{\tilde{R}/R}\mathbb{G}_{m,\tilde{R}} = \operatorname{Spec} R[U,V,\frac{1}{U^2+PUV+QV^2}] \to U_{\tilde{R}/R} = \operatorname{Spec} R[U,V]/(U^2+PUV+QV^2-1)$$

as the composite

$$\prod_{\tilde{R}/R}\mathbb{G}_{m,\tilde{R}} \xrightarrow{\beta} G_{\tilde{R}/R} \xrightarrow{\alpha} U_{\tilde{R}/R}.$$

Then $\gamma$ is given by

$$U\mapsto \frac{U^2-QV^2}{U^2+PUV+QV^2},\ V\mapsto \frac{2UV+PV^2}{U^2+PUV+QV^2}.$$

**Remark 1.3.1.** Assume that $D$ is not nilpotent in $R$. A homomorphism of group schemes over $\tilde{R}$

$$\xi : G_{(\tilde{R}/R)} \otimes_R \tilde{R} = \operatorname{Spec} \tilde{R}[X,Y]/(X^2 + PXY + QY^2 - Y) \to \mathbb{G}_{m,\tilde{R}} = \operatorname{Spec} \tilde{R}[T, \frac{1}{T}]$$

is defined by

$$T \mapsto 1 - (P - 2\theta)(X + \theta Y) : \tilde{R}[T, \frac{1}{T}] \to \tilde{R}[X,Y]/(X^2 + PXY + QY^2 - Y),$$

and we obtain a commutative diagram with exact rows

$$\begin{tikzcd}
0 \arrow[r] & \mathbb{G}_{m,\tilde{R}} \arrow[r, "i"] \arrow[d, equal] & (\prod_{\tilde{R}/R} \mathbb{G}_{m,\tilde{R}}) \otimes_R \tilde{R} \arrow[r, "\beta"] \arrow[d, "\xi"] & G_{(\tilde{R}/R)} \otimes_R \tilde{R} \arrow[r] \arrow[d, "\xi"] & 0 \\
0 \arrow[r] & \mathbb{G}_{m,\tilde{R}} \arrow[r, "\varDelta"'] & \mathbb{G}^2_{m,\tilde{R}} \arrow[r, "\delta"'] & \mathbb{G}_{m,\tilde{R}} \arrow[r] & 0
\end{tikzcd}.$$

Here

$$\varDelta : \mathbb{G}_{m,\tilde{R}} = \operatorname{Spec} \tilde{R}[T, \frac{1}{T}] \to \mathbb{G}^2_{m,\tilde{R}} = \operatorname{Spec} \tilde{R}[T_1, T_2, \frac{1}{T_1}, \frac{1}{T_2}]$$

is defined by $(T_1, T_2) \mapsto (T, T)$, and

$$\delta : \mathbb{G}^2_{m,\tilde{R}} = \tilde{R}[T_1, T_2, \frac{1}{T_1}, \frac{1}{T_2}] \to \mathbb{G}_{m,\tilde{R}} = \tilde{R}[T, \frac{1}{T}]$$

is defined by $T \mapsto T_1 T_2^{-1}$.

Moreover, the diagram of group schemes over $\tilde{R}$

$$\begin{tikzcd}
G_{(\tilde{R}/R)} \otimes_R \tilde{R} \arrow[r, "\alpha"] \arrow[d, "\xi"] & U_{\tilde{R}/R} \otimes_R \tilde{R} \arrow[d, "\xi"] \\
\mathbb{G}_{m,\tilde{R}} \arrow[r, equal] & \mathbb{G}_{m,\tilde{R}}
\end{tikzcd}$$

is commutative.

**Remark 1.4.1.** Let $a \in R$, and put $P = 2a$ and $Q = a^2$. Then we have $D = 0$ and $U^2 + PUV + QV^2 = (U + aV)^2$. Moreover, $G_{\tilde{R}/R} = \operatorname{Spec} R[U, V, 1/(U^2 + PUV + QY^2)$ is isomorphic to $\mathbb{G}_{m,R} \times \mathbb{G}_{a,R} = \operatorname{Spec} R[U, 1/U, T]$. Indeed,

$$(U,T) \mapsto \Big(U + aV, \frac{V}{U + aV}\Big) : R[U, \frac{1}{U}, T] \to R[U, V, \frac{1}{U^2 + PUV + QV^2}]$$

gives an isomorphism $\eta : G_{\tilde{R}/R} \xrightarrow{\sim} \mathbb{G}_{m,R} \times \mathbb{G}_{a,R}$. The inverse of $\eta$ is given by

$$(U,V) \mapsto (U(1 - aT), UT) : R[U, V, \frac{1}{U^2 + PUV + QV^2}] \to R[U, \frac{1}{U}, T].$$

Therefore, we obtain commutative diagram with exact rows

$$\begin{tikzcd}
0 \arrow[r] & \mathbb{G}_{m,R} \arrow[r] \arrow[d, equal] & G_{\tilde{R}/R} \arrow[r, "\beta"] \arrow[d, "\wr\, \eta"] & G_{(\tilde{R}/R)} \arrow[r] \arrow[d, "\wr\, \eta"] & 0 \\
0 \arrow[r] & \mathbb{G}_{m,R} \arrow[r] & \mathbb{G}_{m,R} \times \mathbb{G}_{a,R} \arrow[r] & \mathbb{G}_{a,R} \arrow[r] & 0
\end{tikzcd}.$$

More precisely, the isomorphism

$$\xi : G_{(\tilde{R}/R)} = \operatorname{Spec} R[X,Y]/(X^2 + PXY + QY^2 - Y) \xrightarrow{\sim} \mathbb{G}_{a,R} = \operatorname{Spec} R[T]$$

is given by

$$T \mapsto X + aY : R[T] \to R[X,Y]/(X^2 + PXY + QY^2 - Y),$$

and the inverse of $\eta$ is given by

$$(X,Y) \mapsto (T - aT^2, T^2) : R[X,Y]/(X^2 + PXY + QY^2 - Y) \to R[T].$$

On the other hand, $\mathbb{G}_{m,R} \to \mathbb{G}_{m,R} \times \mathbb{G}_{a,R}$ denotes the canonical injection, and $\mathbb{G}_{m,R} \times \mathbb{G}_{a,R} \to \mathbb{G}_{a,R}$ denotes the canonical projection.

Furthermore, we have a commutative diagram with exact rows and columns

$$\begin{tikzcd}
 & 0 \arrow[d] & 0 \arrow[d] & & \\
0 \arrow[r] & \boldsymbol{\mu}_{2,R} \arrow[r] \arrow[d] & U_{\tilde{R}/R} \arrow[r] \arrow[d] & \mathbb{G}_{a,R} \arrow[r] \arrow[d, equal] & 0 \\
0 \arrow[r] & \mathbb{G}_{m,R} \arrow[r] \arrow[d, "\text{square}"] & G_{\tilde{R}/R} \arrow[r, "\eta\circ\beta"] \arrow[d, "\text{Nr}"] & \mathbb{G}_{a,R} \arrow[r] & 0 \cdot \\
 & \mathbb{G}_{m,R} \arrow[r, equal] \arrow[d] & \mathbb{G}_{m,R} \arrow[d] & & \\
 & 0 & 0 & &
\end{tikzcd}$$

More precisely, the homomorphism

$$U_{\tilde{R}/R} = \operatorname{Spec} R[U,V]/(U^2 + PUV + QY^2 - 1) \to \mathbb{G}_{a,R} = \operatorname{Spec} R[T]$$

is given by

$$T \mapsto \frac{V}{U + aV} : R[T] \to R[U,V]/(U^2 + PUV + QV^2 - 1).$$

We have also a commutative diagram with exact rows

$$\begin{tikzcd}
 & & G_{(\tilde{R}/R)} \arrow[r, "\sim", "\xi"'] \arrow[d, "\alpha"] & \mathbb{G}_{a,R} \arrow[d, "2"] & \\
0 \arrow[r] & \boldsymbol{\mu}_{2,R} \arrow[r] & U_{\tilde{R}/R} \arrow[r] & \mathbb{G}_{a,R} \arrow[r] & 0
\end{tikzcd} \quad .$$

Recall that the homomorphism

$$\begin{aligned}\alpha : G_{(\tilde{R}/R)} &= \operatorname{Spec} R[X,Y]/(X^2 + PXY + QY^2 - Y) \\ &\to U_{\tilde{R}/R} = \operatorname{Spec} R[U,V]/(U^2 + PUV + QY^2 - 1)\end{aligned}$$

is given by

$$U \mapsto 1 - PX - 2QY = 1 - 2a(X + aY), \ V \mapsto 2X + PY = 2(X + aY).$$

**Remark 1.4.2.** Assume that $D$ is not invertible in $R$, and put $R_0 = R/(D)$. If $D$ is a non-zero divisor of $R$, then $\alpha : G_{\tilde{R}/R}(R) \to U_{\tilde{R}/R}(R)$ is injective and $\mathrm{Im}[G_{\tilde{R}/R}(R) \to U_{\tilde{R}/R}(R)] \subset$

$\mathrm{Ker}[U_{\tilde{R}/R}(R) \to U_{\tilde{R}/R}(R_0)]$, as is shown in [12]. Here $U_{\tilde{R}/R}(R) \to U_{\tilde{R}/R}(R_0)$ denotes the reduction map.

**Notation 1.5.** We shall often denote $G_{P,Q} = \prod_{\tilde{R}/R} \mathbb{G}_{m,\tilde{R}}$, $U_{P,Q} = U_{\tilde{R}/R}$ and $G_{(P,Q)} = G_{\tilde{R}/R}$, specifying the elements $P, Q \in R$. When $P = 0$ and $Q = D$, we shall denote also $G_D = G_{P,Q}$, $U_D = U_{P,Q}$ and $G_{(D)} = G_{(P,Q)}$ as in [14].

**Remark 1.6.1.** Let $P, Q \in \mathbb{Z}$, and put $D = P^2 - 4Q$. First assume $P \equiv 0 \mod 2$. Then we have $D \equiv 0 \mod 4$. Let $\theta$ and $\delta$ denote the image of $t$ in the residue rings $\mathbb{Z}[t]/(T^2 - Pt + Q)$ and $\mathbb{Z}[t]/(t^2 - D/4)$, respectively. Then $\theta \mapsto P/2 + \delta$ gives rise to an isomorphism of rings $\mathbb{Z}[t]/(T^2 - Pt + Q) \xrightarrow{\sim} \mathbb{Z}[t]/(t^2 - D/4)$, and therefore isomorphisms of group schemes $G_{P,Q} \xrightarrow{\sim} G_{D/4}$, $U_{P,Q} \xrightarrow{\sim} U_{D/4}$ and $G_{(P,Q)} \xrightarrow{\sim} G_{(D/4)}$.

Now assume $P \equiv 1 \mod 2$, and let $\theta$ and $\delta$ denote the image of $t$ in the residue rings $\mathbb{Z}[t]/(T^2 - 2Pt + 4Q)$ and $\mathbb{Z}[t]/(t^2 - D)$, respectively. Then $\theta \mapsto P + \delta$ gives rise to isomorphisms of group schemes $G_{2P,4Q} \xrightarrow{\sim} G_D$, $U_{2P,4Q} \xrightarrow{\sim} U_D$ and $G_{(2P,4Q)} \xrightarrow{\sim} G_{(D)}$.

**Remark 1.6.2.** Let $P, Q \in \mathbb{Z}$. If $D \neq 0$ and $D$ is a square in $\mathbb{Z}$, then we obtain a commutative diagram with exact rows

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

for each prime $p$ with $(p, D) = 1$. Here the map $\xi : U_{P,Q}(\mathbb{Q}) \to \mathbb{Q}^{\times}$ is given by $(u, v) \mapsto u + v\alpha$ ($\alpha \in \mathbb{Z}$ is a root of the quadratic equation $t^2 - Pt + Q = 0$), as is remarked in 1.2.

**Remark 1.6.3.** Let $P, Q \in \mathbb{Z}$. If $D = 0$, then we obtain a commutative diagram with exact rows

$$\begin{tikzcd}
0 \arrow[r] & G_{(P,Q)}(\mathbb{Z}_{(p)}) \arrow[r] \arrow[d, "\wr\ \eta"] & G_{(P,Q)}(\mathbb{Q}) \arrow[r] \arrow[d, "\wr\ \eta"] & \mathbb{Q}_p/\mathbb{Z}_p \arrow[r] \arrow[d, equal] & 0 \\
0 \arrow[r] & \mathbb{Z}_{(p)} \arrow[r] & \mathbb{Q} \arrow[r] & \mathbb{Q}_p/\mathbb{Z}_p \arrow[r] & 0
\end{tikzcd}$$

for each prime $p$. Here the map $\eta : G_{(P,Q)}(\mathbb{Q}) \to \mathbb{Q}^{\times}$ is given by $(a, b) \mapsto a + b\alpha$ ($\alpha \in \mathbb{Z}$ is the root of the quadratic equation $t^2 - Pt + Q = 0$), as is remarked in 1.4.1.

**Definition 1.7.** Let $c \in R$. We define homomorphisms of group schemes

$$\begin{aligned}
\underline{c} : G_{cP,c^2Q} &= \mathrm{Spec}\, R\big[U, V, \frac{1}{U^2 + cPUV + c^2QV^2}\big] \\
&\to G_{P,Q} = \mathrm{Spec}\, R\big[U, V, \frac{1}{U^2 + PUV + QV^2}\big]
\end{aligned}$$

and

$$\begin{aligned}
\underline{c} : U_{cP,c^2Q} &= \mathrm{Spec}\, R[U, V]/(U^2 + cPUV + c^2QV^2 - 1) \\
&\to U_{P,Q} = \mathrm{Spec}\, R[U, V]/(U^2 + PUV + QV^2 - 1)
\end{aligned}$$

by

$$(U,V) \mapsto (U,cV).$$

Moreover, we define a homomorphism of group schemes

$$\begin{aligned}\underline{c} : G_{(cP,c^2Q)} &= \operatorname{Spec} R[X,Y]/(X^2+cPXY+c^2QY^2-Y)\\ &\to G_{(P,Q)} = \operatorname{Spec} R[X,Y]/(X^2+PXY+QY^2-Y)\end{aligned}$$

by

$$(X,Y) \mapsto (cX,c^2Y).$$

If $c$ is not a zero-divisor of $R$, the map $\underline{c} : G_{cP,c^2Q}(R) \to G_{P,Q}(R)$ is nothing but the inclusion map $R[c\theta]^\times \to \tilde{R}^\times = R[\theta]^\times$.

We have commutative diagrams with exact rows

$$\begin{tikzcd}
0 \arrow[r] & U_{cP,c^2Q} \arrow[r] \arrow[d, "\underline{c}"] & G_{cP,c^2Q} \arrow[r, "\mathrm{Nr}"] \arrow[d, "\underline{c}"] & \mathbb{G}_{m,R} \arrow[r] \arrow[d, equal] & 0 \\
0 \arrow[r] & U_{P,Q} \arrow[r] & G_{P,Q} \arrow[r, "\mathrm{Nr}"'] & \mathbb{G}_{m,R} \arrow[r] & 0
\end{tikzcd}$$

and

$$\begin{tikzcd}
0 \arrow[r] & \mathbb{G}_{m,R} \arrow[r] \arrow[d, equal] & G_{cP,c^2Q} \arrow[r, "\beta"] \arrow[d, "\underline{c}"] & G_{(cP,c^2Q)} \arrow[r] \arrow[d, "\underline{c}"] & 0 \\
0 \arrow[r] & \mathbb{G}_{m,R} \arrow[r] & G_{P,Q} \arrow[r, "\beta"'] & G_{(P,Q)} \arrow[r] & 0
\end{tikzcd}.$$

The diagram

$$\begin{tikzcd}
G_{(cP,c^2Q)} \arrow[r, "\alpha"] \arrow[d, "\underline{c}"] & U_{cP,c^2Q} \arrow[d, "\underline{c}"] \\
G_{(P,Q)} \arrow[r, "\alpha"'] & U_{P,Q}
\end{tikzcd}$$

is also commutative.

**Lemma 1.8.** *Let $c \in R$, and put $R_0 = R/cR$. Assume that $c$ is neither a unit nor a zero divisor of $R$. Then the sequence*

$$0 \longrightarrow G_{(cP,c^2Q)}(R) \xrightarrow{\underline{c}} G_{(P,Q)}(R) \longrightarrow G_{(P,Q)}(R_0)$$

*is exact. Here $G_{(P,Q)}(R) \to G_{(P,Q)}(R_0)$ denotes the reduction map.*

**Proof.** The map $\underline{c} : (u,v) \mapsto (cu, c^2v)$ is injective since $c$ is a non-zero divisor of $R$.

Now let $(u,v) \in G_{(P,Q)}(R)$, and assume that $u \equiv 0 \mod c$ and $v \equiv 0 \mod c$. Then we obtain $v \equiv 0 \mod c^2$ by the equality $v = u^2 + Puv + Qv^2$. Hence there exist $u', v' \in R$ such that $u = cu'$ and $v = c^2v'$. These imply $c^2v'^2 = c^2(u'^2 + cPu'v' + c^2Qv'^2)$ and therefore $v'^2 = u'^2 + cPu'v' + c^2Qv'^2$ since $c$ is a non-zero divisor of $R$. Therefore we obtain $(u',v') \in G_{(cP,c^2Q)}(R)$.

**Remark 1.9.** Let $R$ be a ring and $P, Q, c \in R$. Then the following conditions are equivalent.

(a) $c$ is invertible;

(b) $\underline{c} : G_{cP,c^2Q} \to G_{P,Q}$ is isomorphic;

(c) $\underline{c} : U_{cP,c^2Q} \to U_{P,Q}$ is isomorphic;

(d) $\underline{c} : G_{(cP,c^2Q)} \to G_{(P,Q)}$ is isomorphic.

The implications (a)⇒(b),(c),(d) are trivial. We obtain the implications (b)⇔(c) and (b)⇔(d), applying the snake lemma to the commutative diagrams with exact rows

$$\begin{tikzcd}
0 \arrow[r] & U_{cP,c^2Q} \arrow[r] \arrow[d, "\underline{c}"] & G_{cP,c^2Q} \arrow[r, "\mathrm{Nr}"] \arrow[d, "\underline{c}"] & \mathbb{G}_{m,R} \arrow[r] \arrow[d, equal] & 0 \\
0 \arrow[r] & U_{P,Q} \arrow[r] & G_{P,Q} \arrow[r, "\mathrm{Nr}"'] & \mathbb{G}_{m,R} \arrow[r] & 0
\end{tikzcd}$$

and

$$\begin{tikzcd}
0 \arrow[r] & \mathbb{G}_{m,R} \arrow[r] \arrow[d, equal] & G_{cP,c^2Q} \arrow[r, "\beta"] \arrow[d, "\underline{c}"] & G_{(cP,c^2Q)} \arrow[r] \arrow[d, "\underline{c}"] & 0 \\
0 \arrow[r] & \mathbb{G}_{m,R} \arrow[r] & G_{P,Q} \arrow[r, "\beta"'] & G_{(P,Q)} \arrow[r] & 0
\end{tikzcd}.$$

Finally we verify the implications (d)⇒(a). Assume that $c$ is not invertible, and put $R_0 = R/cR$. Then the homomorphism $\alpha : G_{(cP,c^2Q)}(R_0) \to G_{(P,Q)}(R_0)$ is trivial, and $G_{(cP,c^2Q)}(R_0)$ is isomorphic to the addtive group $R_0$, as is remarked in 1.4.1. It follows that $\underline{c} : G_{(cP,c^2Q)} \to G_{(P,Q)}$ is not isomorphic.

We conclude the section, by recalling the action of $G_{(P,Q)}$ on $\mathbb{P}^1_R$. We refer to [12, Section 2] concerning detailed accounts.

**1.10.** Let $R$ be a ring. Then the group $G_{P,Q}(R) = \tilde{R}^\times$ acts $R$-linearly on the $R$-algebra $\tilde{R}$ by the multiplication. Hence the regular represention $\rho_R : G_{P,Q}(R) \to GL(2,R)$ with respect to the $R$-basis $\{1, \theta\}$ is given by

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

The homomorphism $\rho_R : G_{P,Q}(R) \to GL(2,R)$ is represented by a homomorphism of group schemes $\rho : G_{P,Q} \to GL_{2,R}$. It is readily seen that $\rho : G_{P,Q} \to GL_{2,R}$ is a closed immersion.

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

$$\begin{tikzcd}
0 \arrow[r] & \mathbb{G}_m \arrow[r] \arrow[d, equal] & G_{P,Q} \arrow[r, "\beta"] \arrow[d, "\rho"] & G_{(P,Q)} \arrow[r] \arrow[d, "\rho"] & 0 \\
1 \arrow[r] & \mathbb{G}_m \arrow[r] & GL_{2,R} \arrow[r] & PGL_{2,R} \arrow[r] & 1
\end{tikzcd}.$$

The induced homomorphism $\rho : G_{(P,Q)} \to PGL_{2,R}$ is a closed immersion, and $G_{(P,Q)}$ acts on $\mathbb{P}^1_R$ through $\rho : G_{(P,Q)} \to PGL_{2,R}$.

## 2. $G_{P,Q}(\mathbb{Z}/2^n\mathbb{Z})$, $U_{P,Q}(\mathbb{Z}/2^n\mathbb{Z})$ and $G_{(P,Q)}(\mathbb{Z}/2^n\mathbb{Z})$

**2.1.** Let $P, Q \in \mathbb{Z}$, and let $p$ be a prime and $n$ a positive integer. Then we can verify (1) and (2), tracing the proofs of [14, Lemma 1.10 and Corollary 1.11].

(1) The exact sequence of group schemes

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

yields a commutative diagram with exact rows

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

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

Furthermore, $\mathrm{Coker}[\underline{p^n} : G_{p^nP,p^{2n}Q}(\mathbb{Z}_{(p)}) \to G_{P,Q}(\mathbb{Z}_{(p)})]$ is isomorphic to $G_{(P,Q)}(\mathbb{Z}/p^n\mathbb{Z})$. Therefore, we obtain an isomorphism

$$\mathrm{Coker}[\underline{p^n} : G_{p^nP,p^{2n}Q}(\mathbb{Z}_{(p)}) \to G_{P,Q}(\mathbb{Z}_{(p)})] \xrightarrow{\sim} G_{(P,Q)}(\mathbb{Z}/p^n\mathbb{Z}),$$

applying the snake lemma to the commutative diagram with exact rows

$$\begin{tikzcd}
0 \arrow[r] & \mathbb{Z}_{(p)}^\times \arrow[r] \arrow[d, equal] & G_{p^nP,p^{2n}Q}(\mathbb{Z}_{(p)}) \arrow[r, "\beta"] \arrow[d, "\underline{p^n}"] & G_{(p^nP,p^{2n}Q)}(\mathbb{Z}_{(p)}) \arrow[r] \arrow[d, "\underline{p^n}"] & 0 \\
0 \arrow[r] & \mathbb{Z}_{(p)}^\times \arrow[r] & G_{P,Q}(\mathbb{Z}_{(p)}) \arrow[r, "\beta"'] & G_{(P,Q)}(\mathbb{Z}_{(p)}) \arrow[r] & 0
\end{tikzcd}.$$

**Proposition 2.2.** *Let $P, Q \in \mathbb{Z}$, and put $D = P^2 - 4Q$. Then:*

(1) *If $D \equiv 1 \mod 8$, then $U_{P,Q}(\mathbb{Q})/U_{P,Q}(\mathbb{Z}_{(2)})$ is isomorphic to $\mathbb{Z}$.*

(2) *If $D \equiv 5 \mod 8$, then the canonical homomorphism $U_{P,Q}(\mathbb{Z}_{(2)}) \to U_{P,Q}(\mathbb{Q})$ is bijective.*

(3) *If $D/4 \equiv 2, 3 \mod 4$, then the canonical homomorphism $U_{P,Q}(\mathbb{Z}_{(2)}) \to U_{P,Q}(\mathbb{Q})$ is bijective.*

**Proof.** We can verify the assertions, tracing the proof of [14, Proposition 1.5]. For the reader's convenience, we repeat the argument in the case where $D$ is not a square. Let $\mathcal{O}_D$ denote the ring of integers in $\mathbb{Q}(\sqrt{D})$. By definition, we have

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

and, under the assumption $D \equiv 1 \mod 4$ or $D/4 \equiv 2, 3 \mod 4$,

$$U_{P,Q}(\mathbb{Z}_{(2)}) = \{\alpha \in \mathcal{O}_D \otimes \mathbb{Z}_{(2)}\ ;\ \mathrm{Nr}\,\alpha = 1\}.$$

(1) Let $\mathfrak{p}$ be a prime ideal of $\mathbb{Q}(\sqrt{D})$ over 2. Then $\alpha \mapsto \mathrm{ord}_{\mathfrak{p}}\alpha$ defines a homomorphism $U_{P,Q}(\mathbb{Q}) \to \mathbb{Z}$. Furthermore, the sequence

$$0 \longrightarrow U_D(\mathbb{Z}_{(2)}) \longrightarrow U_D(\mathbb{Q}) \xrightarrow{\mathrm{ord}_{\mathfrak{p}}} \mathbb{Z} \longrightarrow 0$$

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 $\alpha$, and $\bar{\mathfrak{p}}$ denotes the conjugate of $\mathfrak{p}$. This implies $\alpha \in \mathcal{O}_D \otimes \mathbb{Z}_{(2)}$. Hence we obtain

$$U_D(\mathbb{Z}_{(2)}) = \mathrm{Ker}[\mathrm{ord}_{\mathfrak{p}} : U_D(\mathbb{Q}) \to \mathbb{Z}].$$

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) Note first that 2 remains prime in $Q(\sqrt{D})/\mathbb{Q}$ if $D \equiv 5 \mod 8$ and that 2 inerts in $Q(\sqrt{D})/\mathbb{Q}$ if $D/4 \equiv 2, 3 \mod 4$. Let $\mathfrak{p}$ be the prime ideal of $\mathbb{Q}(\sqrt{D})$ over 2. Then, for any $\alpha \in \mathbb{Q}(\sqrt{D})$ with $\mathrm{Nr}\,\alpha = 1$, we have $\mathrm{ord}_{\mathfrak{p}}\alpha = 0$. This implies $\alpha \in \mathcal{O}_D \otimes_{\mathbb{Z}} \mathbb{Z}_{(2)}$. Hence we obtain $U_{P,Q}(\mathbb{Z}_{(2)}) = U_{P,Q}(\mathbb{Q})$.

We fix $D \in \mathbb{Z}$. We denote by $\delta$ the image of $t$ in the residue ring $\mathbb{Z}[t]/(t^2 - D)$.

**Proposition 2.3.** *If $D \equiv 2, 3 \mod 4$, then $\mathrm{Coker}[\alpha : G_{(D)}(\mathbb{Z}_{(2)}) \to U_D(\mathbb{Z}_{(2)})]$ is isomorphic to $\mathbb{Z}/2\mathbb{Z}$.*

**Proof.** By definition, we have

$$U_D(\mathbb{Z}_{(2)}) = \{\alpha \in \mathbb{Z}_{(2)}[\sqrt{D}]\ ;\ \mathrm{Nr}\,\alpha = 1\} = \{(u, v) \in \mathbb{Z}_{(2)}^2\ ;\ u^2 - Dv^2 = 1\}$$

and

$$\mathrm{Im}[\alpha : G_{(D)}(\mathbb{Z}_{(2)}) \to U_D(\mathbb{Z}_{(2)})] = \{(1 + 2Db, 2a)\ ;\ (a, b) \in \mathbb{Z}_{(2)}^2,\ a^2 - Db^2 - b = 0\}.$$

Assume first $D \equiv 2 \mod 4$. Then the condition $u^2 - Dv^2 = 1$ implies $u \equiv 1 \mod 2$ since $D \equiv 0 \mod 2$. On the other hand, we have

$$\mathrm{Im}[\alpha : G_{(D)}(\mathbb{Z}_{(2)}) \to U_D(\mathbb{Z}_{(2)})] = \{(u, v) \in \mathbb{Z}_{(2)}^2\ ;\ u^2 - Dv^2 = 1,\ u \equiv 1 \mod 4\}.$$

Indeed, it is readily seen that $1+2Db \equiv 1 \mod 4$ since $D \equiv 0 \mod 2$. Conversely, let $u, v \in \mathbb{Z}_{(2)}$ with $u^2 - Dv^2 = 1$ and $u \equiv 1 \mod 4$, and put $a = v/2$ and $b = (u - 1)/2D$. Then we obtain $a, b \in \mathbb{Z}_{(2)}$ and $u^2 - Dv^2 = 1$ since $\mathrm{ord}_2(u - 1) \geq 2$, $\mathrm{ord}_2 D = 1$ and $\mathrm{ord}_2 v \geq 1$.

Furthermore, we obtain a splitting exact sequence

$$0 \longrightarrow G_{(D)}(\mathbb{Z}_{(2)}) \xrightarrow{\alpha} U_D(\mathbb{Z}_{(2)}) \longrightarrow \{\pm 1\} \longrightarrow 0,$$

noting $(-1, 0) \in U_D(\mathbb{Z}_{(2)})$.

Assume now $D \equiv 3 \mod 4$. Then the condition $u^2 - Dv^2 = 1$ implies $u \equiv 1 \mod 2$, $v \equiv 0 \mod 2$, or $u \equiv 0 \mod 2$, $v \equiv 1 \mod 2$, since $D \equiv 1 \mod 2$. On the other hand, we have

$$\mathrm{Im}[\alpha : G_{(D)}(\mathbb{Z}_{(2)}) \to U_D(\mathbb{Z}_{(2)})] = \{(u,v) \in \mathbb{Z}_{(2)}^2 \ ; \ u^2 - Dv^2 = 1, \ u \equiv 1 \mod 2\}.$$

Indeed, it is readily seen that $1 + 2Db \equiv 1 \mod 2$. Conversely, let $u, v \in \mathbb{Z}_{(2)}$ with $u^2 - Dv^2 = 1$ and $u \equiv 1 \mod 2$, and put $a = v/2$ and $b = (u-1)/2D$. Then we obtain $a, b \in \mathbb{Z}_{(2)}$ and $u^2 - Dv^2 = 1$ since $\mathrm{ord}_2(u-1) \geq 1$, $\mathrm{ord}_2 D = 0$ and $\mathrm{ord}_2 v \geq 1$.

Furthermore, $((1+D)/(1-D), 2/(1-D)) \in U_D(\mathbb{Z}_{(2)})$ and $((1+D)/(1-D), 2/(1-D)) \notin \mathrm{Im}[\alpha : G_{(D)}(\mathbb{Z}_{(2)}) \to U_D(\mathbb{Z}_{(2)})]$ since $\mathrm{ord}_2(1-D) = 1$ and $\mathrm{ord}_2(1+D) \geq 2$. These imply $\#\mathrm{Coker}[\alpha : G_{(D)}(\mathbb{Z}_{(2)}) \to U_D(\mathbb{Z}_{(2)})] = 2$.

**2.4.** Hereafter we invetigate the group structure of $G_D(\mathbb{Z}/2^n\mathbb{Z})$ and $G_{(D)}(\mathbb{Z}/2^n\mathbb{Z})$. By definition, we have $G_D(\mathbb{Z}/2^n\mathbb{Z}) = \{(u,v) \in (\mathbb{Z}/2^n\mathbb{Z})^2 \ ; \ u^2 - Dv^2 \equiv 1 \mod 2\}$ and therefore $\#G_D(\mathbb{Z}/2^n\mathbb{Z}) = 2^{2n-1}$. In particular, $G_D(\mathbb{Z}/2\mathbb{Z})$ is isomorphic to $\mathbb{Z}/2\mathbb{Z}$.

**Lemma 2.5.** *Let $a \in \mathbb{Z}$. If $D \equiv 0 \mod 2$ and $a \equiv 1 \mod 2$, then the order of $a + \delta \mod 2^n$ is equal to $2^n$ for $n \geq 1$.*

Proof. Since $a \equiv 1 \mod 2$ and $D \equiv 0 \mod 2$, we have

$$a + \delta \equiv 1 + \delta \mod 2$$

and therefore

$$(a+\delta)^2 \equiv (1+\delta)^2 = \pm 1 + 2\delta \mod 4.$$

Hence, for $n \geq 3$, we obtain inductively

$$(a+\delta)^{2^{n-1}} \equiv 1 + 2^{n-1}\delta \mod 2^n, \ (a+\delta)^{2^n} \equiv 1 \mod 2^n.$$

Hence the result.

**Corollary 2.6.** *Let $a \in \mathbb{Z}$. If $D \equiv 0 \mod 2$ and $a \equiv 1 \mod 2$, then the order of $\beta(a+\delta) = \left(\dfrac{a}{a^2 - D}, \dfrac{1}{a^2 - D}\right)$ in $G_{(D)}(\mathbb{Z}/2^n\mathbb{Z})$ is equal to $2^n$ for $n \geq 1$.*

Proof. The homomorphism $\beta : G_D(\mathbb{Z}/2^n\mathbb{Z}) \to G_{(D)}(\mathbb{Z}/2^n\mathbb{Z})$ sends $(a+\delta)^{2^{n-1}} = 1 + 2^{n-1}\delta$ to $(2^{n-1}, 0) \neq 0$. Hence the result.

**Lemma 2.7.** *Let $a \in \mathbb{Z}$. If $a \equiv 1 \mod 2$, then the order of $a + 2\delta \mod 2^n$) is equal to $2^{n-1}$ for $n \geq 1$.*

Proof. Since $a \equiv 1 \mod 2$, we have

$$a + 2\delta \equiv \pm 1 + 2\delta \mod 4.$$

Hence, for $n \geq 3$, we obtain inductively

$$(a+2\delta)^{2^{n-2}} \equiv 1 + 2^{n-1}\delta \text{ or } 1 + 2^{n-1}(1+\delta) \mod 2^n, \ (a+2\delta)^{2^{n-1}} \equiv 1 \mod 2^n,$$

Hence the result.

**Corollary 2.8.** *Let $a \in \mathbb{Z}$. If $D \equiv 1 \mod 2$ and $a \equiv 1 \mod 2$, then the order of $\beta(a+2\delta) = \left(\frac{2a}{a^2-4D}, \frac{4}{a^2-4D}\right)$ in $G_{(D)}(\mathbb{Z}/2^n\mathbb{Z})$ is equal to $2^{n-1}$ for $n \geq 2$.*

Proof. If $n \geq 3$, then the homomorphism $\beta : G_D(\mathbb{Z}/2^n\mathbb{Z}) \to G_{(D)}(\mathbb{Z}/2^n\mathbb{Z})$ sends $(a+2\delta)^{2^{n-2}} = 1 + 2^{n-1}(1+\delta)$ to $(2^{n-1}, 0) \neq 0$. On the other hand, $\beta : G_D(\mathbb{Z}/4\mathbb{Z}) \to G_{(D)}(\mathbb{Z}/4\mathbb{Z})$ sends $a + 2\delta = \pm 1 + 2\delta$ to $(2, 0) \neq 0$. Hence the result.

**Proposition 2.9.** *Assume that $D \equiv 0 \mod 2$. Then:*

*(1) $G_D(\mathbb{Z}/4\mathbb{Z})$ is isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$.*

*(2) $G_D(\mathbb{Z}/2^n\mathbb{Z})$ is isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{n-2}\mathbb{Z} \times \mathbb{Z}/2^n\mathbb{Z}$ for $n \geq 3$.*

Proof. First note that $G_D(\mathbb{Z}/2\mathbb{Z}) = \{1, 1+\delta\}$ and

$$G_D(\mathbb{Z}/4\mathbb{Z}) = \begin{cases} \{\pm 1\} \times \{1, 1+\delta, 1+2\delta, 1+3\delta\} & \text{if } D \equiv 0 \mod 4 \\ \{\pm 1\} \times \{1, 1+\delta, -1+2\delta, -1+\delta\} & \text{if } D \equiv 2 \mod 4. \end{cases}$$

Assume now $n \geq 3$. Then:

(a) the order of 5 in $(\mathbb{Z}/2^n\mathbb{Z})^\times \subset G_D(\mathbb{Z}/2^n\mathbb{Z}) = 2^{n-2}$;

(b) the order of $1+\delta$ in $G_D(\mathbb{Z}/2^n\mathbb{Z}) = 2^n$ by Lemma 2.1.

Moreover, we have $(1+\delta)^{2^{n-1}} = 1 + 2^{n-1}\delta \neq 5^{2^{n-3}}$ in $G_D(\mathbb{Z}/2^n\mathbb{Z})$. Hence we obtain a decomposition

$$G_D(\mathbb{Z}/2^n\mathbb{Z}) = \{\pm 1\} \times (\text{the subgroup generated by } 5) \times (\text{the subgroup generated by } 1+\delta).$$

**Proposition 2.10.** *Assume that $D \equiv 1 \mod 8$. Then:*

*(1) $G_D(\mathbb{Z}/4\mathbb{Z})$ is isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.*

*(2) $G_D(\mathbb{Z}/2^n\mathbb{Z})$ is isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{n-2}\mathbb{Z} \times \mathbb{Z}/2^{n-1}\mathbb{Z}$ for $n \geq 3$.*

Proof. First note that $G_D(\mathbb{Z}/2\mathbb{Z}) = \{1, \delta\}$ and $G_D(\mathbb{Z}/4\mathbb{Z}) = \{\pm 1\} \times \{1, \delta\} \times \{1, 1+2\delta\}$.

Assume now $n \geq 3$. There exists $r \in \mathbb{Z}_2$ such that $r^2 = D$ since $D \equiv 1 \mod 8$. Then:

(a) $\delta/r$ is of the order 2 in $G_D(\mathbb{Z}/2^n\mathbb{Z})$;

(b) 5 is of the order $2^{n-2}$ in $(\mathbb{Z}/2^n\mathbb{Z})^\times \subset G_D(\mathbb{Z}/2^n\mathbb{Z})$;

(c) $1+2\delta$ is of the order $2^{n-1}$ in $G_D(\mathbb{Z}/2^n\mathbb{Z})$ by Lemma 2.4.

Moreover, we have $(1+2\delta)^{2^{n-2}} = 1 + 2^{n-1}(1+\delta) \neq 5^{2^{n-3}}$ in $G_D(\mathbb{Z}/2^n\mathbb{Z})$. Hence we obtain a decomposition

$$G_D(\mathbb{Z}/2^n\mathbb{Z}) = \\ \{\pm 1\} \times \{1, \delta/r\} \times (\text{the subgroup generated by } 5) \times (\text{the subgroup generated by } 1+2\delta).$$

**Proposition 2.11.** *Assume that $D \equiv -1 \mod 8$. Then:*

*(1) $G_D(\mathbb{Z}/4\mathbb{Z})$ is isomorphic to $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.*

*(2) $G_D(\mathbb{Z}/2^n\mathbb{Z})$ is isomorphic to $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2^{n-2}\mathbb{Z} \times \mathbb{Z}/2^{n-1}\mathbb{Z}$ for $n \geq 3$.*

Proof. First note that $G_D(\mathbb{Z}/2\mathbb{Z}) = \{1, \delta\}$ and $G_D(\mathbb{Z}/4\mathbb{Z}) = \{\pm 1, \pm\delta\} \times \{1, 1+2\delta\}$.

Assume now $n \geq 3$. There exits $r \in \mathbb{Z}_2$ such that $r^2 = -D$ since $-D \equiv 1 \mod 8$. Then:

(a) $\delta/r$ is of the order 4 in $G_D(\mathbb{Z}/2^n\mathbb{Z}) = 4$;

(b) 5 is of the order $2^{n-2}$ in $(\mathbb{Z}/2^n\mathbb{Z})^\times \subset G_D(\mathbb{Z}/2^n\mathbb{Z})$;

(c) $1+2\delta$ is of the order $2^{n-1}$ in $G_D(\mathbb{Z}/2^n\mathbb{Z})$ by Lemma 2.4.

Moreover, we have $= 1 + 2^{n-1}$ and $(1+2\delta)^{2^{n-2}} = 1 + 2^{n-1}(1+\delta) \neq 5^{2^{n-3}}$ in $G_D(\mathbb{Z}/2^n\mathbb{Z})$. Hence we obtain a decomposition

$$G_D(\mathbb{Z}/2^n\mathbb{Z}) = \\ \{\pm 1, \pm\delta/r\} \times (\text{the subgroup generated by } 5) \times (\text{the subgroup generated by } 1+2\delta).$$

**Proposition 2.12.** *Assume that $D \equiv 5 \mod 8$. Then $G_D(\mathbb{Z}/2^n\mathbb{Z})$ is isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{n-1}\mathbb{Z} \times \mathbb{Z}/2^{n-1}\mathbb{Z}$ for $n \geq 2$.*

Proof. First note that $G_D(\mathbb{Z}/2\mathbb{Z}) = \{1, \delta\}$ and $G_D(\mathbb{Z}/4\mathbb{Z}) = \{\pm 1\} \times \{1, \delta\} \times \{1, 1+2\delta\}$.

Assume now $n \geq 3$. Then:

(a) $\delta$ is of the order $2^{n-1}$ in $G_D(\mathbb{Z}/2^n\mathbb{Z})$ since $\delta^2 \equiv 5 \mod 8$;

(b) $1+2\delta$ is of the order $2^{n-1}$ in $G_D(\mathbb{Z}/2^n\mathbb{Z}) = 2^{n-1}$ by Lemma 2.4.

Moreover, we have $= 1 + 2^{n-1}$ and $(1+2\delta)^{2^{n-2}} = 1 + 2^{n-1}(1+\delta) \neq 5^{2^{n-3}} = \delta^{2^{n-2}}$ in $G_D(\mathbb{Z}/2^n\mathbb{Z})$. Hence we obtain a decomposition

$$G_D(\mathbb{Z}/2^n\mathbb{Z}) = \{\pm 1\} \times (\text{the subgroup generated by } \delta) \times (\text{the subgroup generated by } 1+2\delta).$$

**Proposition 2.13.** *Assume that $D \equiv -5 \mod 8$. Then*:

(1) *$G_D(\mathbb{Z}/4\mathbb{Z})$ is isomorphic to $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.*

(2) *$G_D(\mathbb{Z}/2^n\mathbb{Z})$ is isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{n-1}\mathbb{Z} \times \mathbb{Z}/2^{n-1}\mathbb{Z}$ for $n \geq 3$.*

Proof. First note that $G_D(\mathbb{Z}/2\mathbb{Z}) = \{1, \delta\}$ and $G_D(\mathbb{Z}/4\mathbb{Z}) = \{\pm 1, \pm\delta\} \times \{1, 1+2\delta\}$.

Assume now $n \geq 3$. Then:

(a) $\delta$ is of the order $2^{n-1}$ in $G_D(\mathbb{Z}/2^n\mathbb{Z}) = 2^{n-1}$ since $\delta^2 \equiv -5 \mod 8$;

(b) $1+2\delta$ is of the order $2^{n-1}$ in $G_D(\mathbb{Z}/2^n\mathbb{Z}) = 2^{n-1}$ by Lemma 2.4.

Moreover, we have $(1+2\delta)^{2^{n-2}} = 1 + 2^{n-1}(1+\delta) \neq (-5)^{2^{n-3}} = \delta^{2^{n-2}}$ in $G_D(\mathbb{Z}/2^n\mathbb{Z})$. Hence we obtain a decomposition

$$G_D(\mathbb{Z}/2^n\mathbb{Z}) = \{\pm 1\} \times (\text{the subgroup generated by } \delta) \times (\text{the subgroup generated by } 1+2\delta).$$

**Remark 2.14.** Contrary to the differences among Propositions 2.9∼2.13, we obtain a common result as follows, examining each case.

Let $D \in \mathbb{Z}$, and let $n$ be an integer$\geq 3$. Then $\mathrm{Ker}[G_D(\mathbb{Z}/2^n\mathbb{Z}) \to G_D(\mathbb{Z}/4\mathbb{Z})]$ is isomorphic to $\mathbb{Z}/2^{n-2}\mathbb{Z} \times \mathbb{Z}/2^{n-2}\mathbb{Z}$. More precisely, we have a decomposition

$$\mathrm{Ker}[G_D(\mathbb{Z}/2^n\mathbb{Z}) \to G_D(\mathbb{Z}/4\mathbb{Z})] = \\ (\text{the subgroup generated by } 5) \times (\text{the subgroup generated by } 1+4\delta).$$

**Proposition 2.15.** *Assume that* $D \equiv 0 \mod 2$. *Then* $G_{(D)}(\mathbb{Z}/2^n\mathbb{Z})$ *is isomorphic to* $\mathbb{Z}/2^n\mathbb{Z}$ *for* $n \geq 1$.

Proof. Noting that $\beta(1+\delta)$ is of the order $2^n$ in $G_{(D)}(\mathbb{Z}/2^n\mathbb{Z})$ and $\#G_{(D)}(\mathbb{Z}/2^n\mathbb{Z}) = 2^n$, we obtain the conclusion immediately.

**Proposition 2.16.** *Assume that* $D \equiv 1 \mod 2$. *Then*:
(1) $G_{(D)}(\mathbb{Z}/2\mathbb{Z})$ *is isomorphic to* $\mathbb{Z}/2\mathbb{Z}$.
(2) $G_{(D)}(\mathbb{Z}/2^n\mathbb{Z})$ *is isomorphic to* $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{n-1}\mathbb{Z}$ *for* $n \geq 2$.

Proof. Assume that $n \geq 2$. Then:
(a) the order of $\beta(\delta) = (0, -1/D)$ in $G_{(D)}(\mathbb{Z}/2^n\mathbb{Z}) = 2$;
(b) the order of $\beta(1+2\delta)$ in $G_{(D)}(\mathbb{Z}/2^n\mathbb{Z}) = 2^{n-1}$ by Corollary 2.5.

Moreover, we have $\beta(1+2\delta)^{2^{n-2}} = \beta(1+2^{n-1}(1+\delta)) = (2^{n-1}, 0)$ in $G_{(D)}(\mathbb{Z}/2^n\mathbb{Z})$. Hence we obtain a decomposition

$$G_{(D)}(\mathbb{Z}/2^n\mathbb{Z}) =$$
$$\text{(the subgroup generated by } \beta(\delta) = (0, -1/D)) \times \text{(the subgroup generated by } \beta(1+2\delta)).$$

**Remark 2.17.** We obtain the following assertion similarly as Remark 2.14, basing the argument on Propositions 2.15 and 2.16.

Let $D \in \mathbb{Z}$, and let $n$ be an integer$\geq 3$. Then $\mathrm{Ker}[G_{(D)}(\mathbb{Z}/2^n\mathbb{Z}) \to G_{(D)}(\mathbb{Z}/2\mathbb{Z})]$ is cyclic of order $2^{n-1}$ and generated by $\beta(1+2\delta)$.

**Remark 2.18.** Let $D \in \mathbb{Z}$ with $D \equiv 2, 3 \mod 4$, and let $n$ be an integer $\geq 2$. We regard $G_{(4^nD)}(\mathbb{Z}_{(2)})$ as a subgroup of $G_{(D)}(\mathbb{Z}_{(2)})$, and $G_{(D)}(\mathbb{Z}_{(2)})$ as a subgroup of $U_D(\mathbb{Z}_{(2)})$ by the injective homomophisms $\underline{2^n} : G_{(4^nD)}(\mathbb{Z}_{(2)}) \to G_{(D)}(\mathbb{Z}_{(2)})$ and $\alpha : G_{(D)}(\mathbb{Z}_{(2)}) \to U_D(\mathbb{Z}_{(2)})$, respectively. Then we have

$$|G_{(D)}(\mathbb{Z}_{(2)})/G_{(4^nD)}(\mathbb{Z}_{(2)})| = |G_{(D)}(\mathbb{Z}/2^n\mathbb{Z})| = 2^n$$

by Propositions 2.15 and 2.16, and

$$|U_D(\mathbb{Z}_{(2)})/G_{(D)}(\mathbb{Z}_{(2)})| = 2$$

by Proposition 2.3. Therefore, we obtain

$$|U_D(\mathbb{Z}_{(2)})/G_{(4^nD)}(\mathbb{Z}_{(2)})| = 2^{n+1}.$$

More precisely,
(a) If $D \equiv 2 \mod 4$ or $D \equiv -5 \mod 8$, then $U_D(\mathbb{Z}_{(2)})/G_{(4^nD)}(\mathbb{Z}_{(2)})$ is isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^n\mathbb{Z}$.
(b) If $D \equiv -1 \mod 8$, then $U_D(\mathbb{Z}_{(2)})/G_{(4^nD)}(\mathbb{Z}_{(2)})$ is isomorphic to $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2^{n-1}\mathbb{Z}$.

Indeed, assume $D \equiv 2 \mod 4$. Then we obtain an exact sequence

$$0 \to G_{(D)}(\mathbb{Z}_{(2)})/G_{(D)}(\mathbb{Z}_{(2)}) \to U_D(\mathbb{Z}_{(2)})/G_{(4^nD)}(\mathbb{Z}_{(2)}) \to U_D(\mathbb{Z}_{(2)})/G_{(D)}(\mathbb{Z}_{(2)}) \to 0.$$

Moreover, $G_{(D)}(\mathbb{Z}_{(2)})/G_{(4^nD)}(\mathbb{Z}_{(2)}) = G_{(D)}(\mathbb{Z}/2^n\mathbb{Z})$ is generated by $\beta(1+\delta)$ by Proposition 2.15, and $U_D(\mathbb{Z}_{(2)})/G_{(4^nD)}(\mathbb{Z}_{(2)}) = G_{(D)}(\mathbb{Z}/2^n\mathbb{Z})$ is generated by $\gamma(\delta) = -1$ as is remarked in the proof of Proposition 2.3. The above exact sequence splits since $-1$ is order of 2 in $U_D(\mathbb{Z}_{(2)})$, and we obtain a decomposition

$$U_D(\mathbb{Z}_{(2)})/G_{(4^nD)}(\mathbb{Z}_{(2)}) = \\ \text{(the subgroup generated by } \gamma(\delta) = -1)\times\text{(the subgroup generated by } \gamma(1+\delta)).$$

Assume now $D \equiv -5 \mod 8$. Then we have a decompostion

$$\begin{aligned} G_{(D)}(\mathbb{Z}_{(2)})/G_{(4^nD)}(\mathbb{Z}_{(2)}) &= G_{(D)}(\mathbb{Z}/2^n\mathbb{Z}) \\ &= \text{(the subgroup generated by } \beta(\delta))\times\mathrm{Ker}[G_{(D)}(\mathbb{Z}/2^n\mathbb{Z}) \to G_{(D)}(\mathbb{Z}/2\mathbb{Z})] \\ &= \text{(the subgroup generated by } \beta(\delta))\times\text{(the subgroup generated by } \beta(1+2\delta)), \end{aligned}$$

$U_D(\mathbb{Z}_{(2)})/G_{(4^nD)}(\mathbb{Z}_{(2)}) = G_{(D)}(\mathbb{Z}/2^n\mathbb{Z})$ is generated by $\gamma(1+\delta)$. Moreover, we have

$$(1+\delta)^2 = \frac{2}{\delta}\Big(D + \frac{1+D}{2}\delta\Big)$$

and therefore

$$\beta(1+\delta)^2 = \beta(\delta)\beta\big(D + \frac{1+D}{2}\delta\big) = \beta(\delta)\beta(-1+2\delta) \in G_{(D)}(\mathbb{Z}/4\mathbb{Z})$$

since $(D+1)/2 \equiv 2 \mod 4$. Hence $\beta(1+\delta)^2$ is of order $2^{n-1}$ in $G_{(D)}(\mathbb{Z}/2^n\mathbb{Z})$, and $\gamma(1+\delta)$ is of order $2^n$ in $U_D(\mathbb{Z}_{(2)})/G_{(4^nD)}(\mathbb{Z}_{(2)})$. Therefore we obtain a decomposition

$$U_D(\mathbb{Z}_{(2)})/G_{(4^nD)}(\mathbb{Z}_{(2)}) = \\ \text{(the subgroup generated by } \gamma(\delta) = -1)\times\text{(the subgroup generated by } \gamma(1+\delta)).$$

Finally assume $D \equiv -1 \mod 8$. Then there exists $r \in \mathbb{Z}_2$ such that $r^2 = -D$. Moroever, we have $\beta(\delta/r) = (0, 1/r^2) \in G_{(D)}(\mathbb{Z}_2)$, $\gamma(\delta/r) = -1 \in U_D(\mathbb{Z}_2)$ and $\beta(1+\delta/r) = (1/2r, 1/2r^2) \in G_{(D)}(\mathbb{Q}_2)$, $\gamma(1+\delta/r) = \delta/r \in U_D(\mathbb{Z}_2)$. Note now that $\gamma(1+\delta/r)$ is of order 4 in $U_D(\mathbb{Z}_{(2)})/G_{(4^nD)}(\mathbb{Z}_{(2)})$ since $(\delta/r)^2 = -1$. Hence we obtain a decomposition

$$U_D(\mathbb{Z}_{(2)})/G_{(4^nD)}(\mathbb{Z}_{(2)}) = \\ \text{(the subgroup generated by } \gamma(1+\delta/r) = \delta/r)\times\text{(the subgroup generated by } \gamma(1+2\delta))$$

from the decompostion

$$G_{(D)}(\mathbb{Z}_{(2)})/G_{(4^nD)}(\mathbb{Z}_{(2)}) = G_{(D)}(\mathbb{Z}/2^n\mathbb{Z}) = \\ \text{(the subgroup generated by } \beta(\delta))\times\text{(the subgroup generated by } \beta(1+2\delta)).$$

**2.19.** Let $P, Q \in \mathbb{Z}$, and put $D = P^2 - 4Q$. If $P \equiv 0 \mod 2$, then we have $D \equiv 0 \mod 4$ and there exist isomorphisms $G_{P,Q} \xrightarrow{\sim} G_{D/4}$ and $G_{(P,Q)} \xrightarrow{\sim} G_{(D/4)}$, as is remarked in 1.6.1.

On the other hand, if $P \equiv 1 \mod 2$, then we have $D \equiv 1 \mod 4$ and there exist isomorphisms $G_{2P,4Q} \xrightarrow{\sim} G_D$ and $G_{(2P,4Q)} \xrightarrow{\sim} G_{(D)}$. Moreover, if $Q \equiv 0 \mod 2$, then we have $G_{(P,Q)}(\mathbb{Z}/2\mathbb{Z}) = \{0\}$. Hence the homomorphisms $\underline{2} : G_{2P,4Q}(\mathbb{Z}_{(2)}) \to G_{P,Q}(\mathbb{Z}_{(2)})$ and $\underline{2} : G_{(2P,4Q)}(\mathbb{Z}_{(2)}) \to G_{(P,Q)}(\mathbb{Z}_{(2)})$ are bijective, and therefore, we obtain isomorphisms $G_D(\mathbb{Z}_{(2)}) \xrightarrow{\sim} G_{P,Q}(\mathbb{Z}_{(2)})$ and $G_{(D)}(\mathbb{Z}_{(2)}) \xrightarrow{\sim} G_{(P,Q)}(\mathbb{Z}_{(2)})$.

**Notation 2.20.** Assume $P \equiv 1 \mod 2$ and $Q \equiv 1 \mod 2$, and let $\theta$ denote the image of $t$ in the residue ring $\mathbb{Z}[t]/(t^2 - Pt + Q)$, and put $\delta = -P + 2\theta$. Then we have $\delta^2 = D$. Moreover, there exists $r \in \mathbb{Z}_2$ such that $r^2 = -D/3$ since $D \equiv 5 \mod 8$. We may assume $r \equiv 1 \mod 4$, replacing $r$ by $-r$ if $r \equiv -1 \mod 4$. Put

$$\omega = \frac{-r + \delta}{2r} = -\frac{r + P}{2r} + \frac{\theta}{r} \in \mathbb{Z}_2[t]/(t^2 - Pt + Q).$$

Then we have $(\delta/r)^2 = -3$ and therefore $\omega^3 = 1$. It is readily seen that $\{1, \omega\}$ is a $\mathbb{Z}_2$-basis of $\mathbb{Z}_2[t]/(t^2 - Pt + Q)$.

**Proposition 2.21.** *Let $P$ and $Q$ be odd integers. Then:*
(1) *$G_{P,Q}(\mathbb{Z}/2\mathbb{Z})$ is isomorphic to $\mathbb{Z}/3\mathbb{Z}$.*
(2) *$G_{P,Q}(\mathbb{Z}/4\mathbb{Z})$ is isomorphic to $\mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.*
(3) *$G_{P,Q}(\mathbb{Z}/2^n\mathbb{Z})$ is isomorphic to $\mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/2^{n-1}\mathbb{Z} \times \mathbb{Z}/2^{n-2}\mathbb{Z}$ for $n \geq 3$.*

Proof. By the definition, we have $G_{P,Q}(\mathbb{Z}/2^n\mathbb{Z}) = \{(u, v) \in \mathbb{Z}/2^n\mathbb{Z}\ ;\ u^2 + uv + v^2 \equiv 1 \mod 2\}$. Then we obtain $|G_{P,Q}(\mathbb{Z}/2^n\mathbb{Z})| = 3 \cdot 2^{2(n-1)}$, noting the implications: $u^2 + uv + v^2 \equiv 1 \mod 2$ $\Leftrightarrow u \equiv 1 \mod 2$ or $v \equiv 1 \mod 2$. We obtain also

$$G_{P,Q}(\mathbb{Z}/2\mathbb{Z}) = \{1, 1 + \theta, \theta\} = \{1, \omega, \omega^2\}$$

and

$$G_{P,Q}(\mathbb{Z}/4\mathbb{Z}) = \{\pm 1, \pm(1 + \theta), \pm\theta\} \times \{1, 1 + 2\theta\} = \{\pm 1, \pm\omega, \pm\omega^2\} \times \{1, 1 + 2\omega\}.$$

Assume now $n \geq 3$. Then:
(a) the order of $1 + 2\omega$ in $G_{P,Q}(\mathbb{Z}/2^n\mathbb{Z}) = 2^{n-1}$ since $(1 + 2\omega)^2 = -3$;
(b) the order of $1 + 4\omega$ in $G_{P,Q}(\mathbb{Z}/2^n\mathbb{Z}) = 2^{n-2}$ since $(1 + 4\omega)^{2^{n-3}} = 1 + 2^{n-1}\omega \mod 2^n$ and $(1 + 4\omega)^{2^{n-2}} = 1 + 2^{n-1}\omega \mod 2^n$.

Moreover, we have $(1 + 2\omega)^{2^{n-2}} = 1 + 2^{n-1}$ and $(1 + 4\omega)^{2^{n-3}} = 1 + 2^{n-1}\omega \neq (-3)^{2^{n-3}} = (1 + 2\omega)^{2^{n-2}}$ in $G_{P,Q}(\mathbb{Z}/2^n\mathbb{Z})$. Hence we obtain a decomposition

$G_{P,Q}(\mathbb{Z}/2^n\mathbb{Z}) =$

$\{\pm 1, \pm\omega, \pm\omega^2\} \times$ (the subgroup generated by $1 + 2\omega$) $\times$ (the subgroup generated by $1 + 4\omega$).

**Corollary 2.22.** *Let $P$ and $Q$ be odd integers. Then:*
(1) *$G_{(P,Q)}(\mathbb{Z}/2\mathbb{Z})$ is isomorphic to $\mathbb{Z}/3\mathbb{Z}$.*
(2) *$G_{(P,Q)}(\mathbb{Z}/4\mathbb{Z})$ is isomorphic to $\mathbb{Z}/6\mathbb{Z}$.*

(3) *$G_{(P,Q)}(\mathbb{Z}/2^n\mathbb{Z})$ is isomorphic to $\mathbb{Z}/6\mathbb{Z}\times\mathbb{Z}/2^{n-2}\mathbb{Z}$ for $n\geq 3$.*

Proof. The homomorphism $\alpha: G_{(P,Q)}(\mathbb{Z}/2^n\mathbb{Z})\to U_{P,Q}(\mathbb{Z}/2^n\mathbb{Z})$ is bijective since $(D,2)=1$. Therefore, it is sufficient to verify the assertions for $U_{P,Q}(\mathbb{Z}/2^n\mathbb{Z})$ instead of $G_{(P,Q)}(\mathbb{Z}/2^n\mathbb{Z})$.

First note that $U_{P,Q}(\mathbb{Z}/2\mathbb{Z})=\{1,\omega,\omega^2\}$ and $U_{P,Q}(\mathbb{Z}/4\mathbb{Z})=\{\pm1,\pm\omega,\pm\omega^2\}$. Assume now $n\geq 3$. Then we have an exact sequence

$$0\longrightarrow(\mathbb{Z}/2^n\mathbb{Z})^\times\longrightarrow G_{P,Q}(\mathbb{Z}/2^n\mathbb{Z})\xrightarrow{\gamma}U_{P,Q}(\mathbb{Z}/2^n\mathbb{Z})\longrightarrow 0.$$

Noting the relations $\gamma(\pm\omega)=\omega^2$, $\gamma(1+2\omega)=-1$ and $\gamma(1+4\omega)^{2^{n-2}}=\gamma(1+2^{n-1}\omega)=1+2^{n-1}\neq\pm1$ in $U_{P,Q}(\mathbb{Z}/2^n\mathbb{Z})$, we obtain a decomposition

$$U_{P,Q}(\mathbb{Z}/2^n\mathbb{Z})=\{\pm1,\pm\omega,\pm\omega^2\}\times(\text{the subgroup generated by }\gamma(1+4\omega)).$$

**Remark 2.23.** Similarly as Remarks 2.14 and 2.17, we obtain the following assertion.

Let $P$ and $Q$ be odd integers, and let $n$ be an integer $\geq 3$. Then $\mathrm{Ker}[G_{P,Q}(\mathbb{Z}/2^n\mathbb{Z})\to G_{P,Q}(\mathbb{Z}/4\mathbb{Z})]$ is isomorphic to $\mathbb{Z}/2^{n-2}\mathbb{Z}\times\mathbb{Z}/2^{n-2}\mathbb{Z}$. More precisely, we have a decomposition

$$\begin{aligned}&\mathrm{Ker}[G_{P,Q}(\mathbb{Z}/2^n\mathbb{Z})\to G_{P,Q}(\mathbb{Z}/4\mathbb{Z})]=\\&\qquad(\text{the subgroup generated by }5)\times(\text{the subgroup generated by }1+4\omega).\end{aligned}$$

On the other hand, $\mathrm{Ker}[G_{(P,Q)}(\mathbb{Z}/2^n\mathbb{Z})\to G_{(P,Q)}(\mathbb{Z}/4\mathbb{Z})]$ is cyclic of order $2^{n-2}$ and generated by $\beta(1+4\omega)$. Furthermore, the exact sequence

$$0\to\mathrm{Ker}[G_{(P,Q)}(\mathbb{Z}/2^n\mathbb{Z})\to G_{(P,Q)}(\mathbb{Z}/4\mathbb{Z})]\to G_{(P,Q)}(\mathbb{Z}/2^n\mathbb{Z})\to G_{(P,Q)}(\mathbb{Z}/4\mathbb{Z})\to 0$$

splits.

**Remark 2.24.** We recall elementary facts on $p$-adic analysis. As is well known, for $a\in 4\mathbb{Z}_2$, the series

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

converges in $\mathbb{Z}_2$. The map $\exp: 4\mathbb{Z}_2\to\mathbb{Z}_2$ induces an isomoprhism of the additive group $4\mathbb{Z}_2$ to the multiplicative group $1+4\mathbb{Z}_2$. The inverse of $\exp: 4\mathbb{Z}_2\xrightarrow{\sim}1+4\mathbb{Z}_2$ 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 $a \in 4\mathbb{Z}_p$ as usual.

Assume first that $D$ is a square in $\mathbb{Z}_2$, and we take $r \in \mathbb{Z}_2$ such that $D = r^2$. We define a homomorphism of groups

$$\exp : 4\mathbb{Z}_2 \times 4\mathbb{Z}_2 \to G_D(\mathbb{Z}_4)$$

by

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

The composite $\beta \circ \exp : 4\mathbb{Z}_2 \times 4\mathbb{Z}_2 \to G_D(\mathbb{Z}_2) \to G_{(D)}(\mathbb{Z}_2)$ is given by

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

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

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

Then we obtain a commutative diagram with exact rows and columns

$$\begin{tikzcd}
 & 0 \arrow[d] & 0 \arrow[d] & 0 \arrow[d] & \\
0 \arrow[r] & 4\mathbb{Z}_2 \arrow[r, "i_1"] \arrow[d, "\exp"] & 4\mathbb{Z}_2 \times 4\mathbb{Z}_2 \arrow[r, "j_2"] \arrow[d, "\exp"] & 4\mathbb{Z}_2 \arrow[r] \arrow[d, "\exp"] & 0 \\
0 \arrow[r] & \mathbb{Z}_2^\times \arrow[r, "i"] \arrow[d] & G_D(\mathbb{Z}_2) \arrow[r, "\beta"] \arrow[d] & G_{(D)}(\mathbb{Z}_2) \arrow[r] \arrow[d] & 0 , \\
0 \arrow[r] & (\mathbb{Z}/4\mathbb{Z})^\times \arrow[r, "i"] \arrow[d] & G_D(\mathbb{Z}/4\mathbb{Z}) \arrow[r, "\beta"] \arrow[d] & G_{(D)}(\mathbb{Z}/4\mathbb{Z}) \arrow[r] \arrow[d] & 0 \\
 & 0 & 0 & 0 &
\end{tikzcd}$$

Here $i_1 : 4\mathbb{Z}_2 \to 4\mathbb{Z}_2 \times 4\mathbb{Z}_2$ and $j_2 : 4\mathbb{Z}_2 \times 4\mathbb{Z}_2 \to 4\mathbb{Z}_2$ are defined by $i_1(a) = (a, 0)$ and $j_2 : (a, b) \mapsto b$, respectively.

Now assume that $D$ is not a square in $\mathbb{Z}_2$. Define a homomorphism

$$\exp : 4\mathbb{Z}_2[\sqrt{D}] \to G_D(\mathbb{Z}_2)$$

by

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

The composite $\beta \circ \exp : 4\mathbb{Z}_2[\sqrt{D}] \to G_D(\mathbb{Z}_2) \to G_{(D)}(\mathbb{Z}_2)$ is given by

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

Define a homomorphism $\exp : 4\mathbb{Z}_2 \to G_{(D)}(\mathbb{Z}_2)$ by

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

Then we obtain a commutative diagram with exact rows and columns

$$\begin{tikzcd}
 & 0 \arrow[d] & 0 \arrow[d] & 0 \arrow[d] & \\
0 \arrow[r] & 4\mathbb{Z}_2 \arrow[r, "i"] \arrow[d, "\exp"] & 4\mathbb{Z}_2[\sqrt{D}] \arrow[r, "j"] \arrow[d, "\exp"] & 4\mathbb{Z}_p \arrow[r] \arrow[d, "\exp"] & 0 \\
0 \arrow[r] & \mathbb{Z}_2^\times \arrow[r, "i"] \arrow[d] & G_D(\mathbb{Z}_2) \arrow[r, "\beta"] \arrow[d] & G_{(D)}(\mathbb{Z}_2) \arrow[r] \arrow[d] & 0\ , \\
0 \arrow[r] & (\mathbb{Z}/4\mathbb{Z})^\times \arrow[r, "i"] \arrow[d] & G_D(\mathbb{Z}/4\mathbb{Z}) \arrow[r, "\beta"] \arrow[d] & G_{(D)}(\mathbb{Z}/4\mathbb{Z}) \arrow[r] \arrow[d] & 0 \\
 & 0 & 0 & 0 &
\end{tikzcd}$$

Here $i : 4\mathbb{Z}_2 \to 4\mathbb{Z}_2[\sqrt{D}]$ and $j : 4\mathbb{Z}_2[\sqrt{D}] \to 4\mathbb{Z}_2$ are defined by $i(a) = a$ and $j : a + b\sqrt{D} \mapsto b$, respectively.

We can verify the following assertions similarly as [14, Proposition 2.9, Corollary 2.10 and Corollary 2.12].

(1) The reduction map $G_D(\mathbb{Z}_2) \to G_D(\mathbb{Z}/2^n\mathbb{Z})$ is surjective. Moreover, let $n$ be an integer $\geq 3$. Then $\mathrm{Ker}[G_D(\mathbb{Z}_2) \to G_D(\mathbb{Z}/2^n\mathbb{Z})]$ is isomorphic to the additive group $2^n\mathbb{Z}_2 \times 2^n\mathbb{Z}_2$ under the identification through the isomorphim $\exp : 4\mathbb{Z}_2 \times 4\mathbb{Z}_2 \xrightarrow{\sim} \mathrm{Ker}[G_D(\mathbb{Z}_2) \to G_D(\mathbb{Z}/4\mathbb{Z})]$.

(2) Let $n$ be an integer $\geq 3$. We have an exact sequence

$$0 \longrightarrow \mathbb{Z}/2^{n-2}\mathbb{Z} \times \mathbb{Z}/2^{n-2}\mathbb{Z} \longrightarrow G_D(\mathbb{Z}/2^n\mathbb{Z}) \longrightarrow G_D(\mathbb{Z}/4\mathbb{Z}) \longrightarrow 0$$

(3) Let $n$ be an integer $\geq 2$. Let $\eta \in G_D(\mathbb{Z}_2)$, and assume that

$$\eta \in \mathrm{Ker}[G_D(\mathbb{Z}_2) \to G_D(\mathbb{Z}/2^n\mathbb{Z})],\ \eta \notin \mathrm{Ker}[G_D(\mathbb{Z}_2) \to G_D(\mathbb{Z}/2^{n+1}\mathbb{Z})].$$

Then we have

$$\eta^2 \in \mathrm{Ker}[G_D(\mathbb{Z}_2) \to G_D(\mathbb{Z}/2^{n+1}\mathbb{Z})],\ \eta^2 \notin \mathrm{Ker}[G_D(\mathbb{Z}_2) \to G_D(\mathbb{Z}/p^{n+2}\mathbb{Z})].$$

**Summary 2.25.** We conclude the section, summing up exact sequences deduced from the exact sequence of group schemes

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

in terms of quadratic extensions. The assertions mentioned below are deduced from Proposition 1.10 and Corollary 1.11 in combination.

Assume that $D = P^2 - 4Q$ is not a square. Then we have $G_{P,Q}(\mathbb{Q}) = \mathbb{Q}(\sqrt{D})^\times$ and $G_{P,Q}(\mathbb{Z}_{(2)}) = (\mathcal{O}_D \otimes_{\mathbb{Z}} \mathbb{Z}_{(2)})^\times$, and the homomorphism $\alpha : G_{(P,Q)}(\mathbb{Q}) \to U_{P,Q}(\mathbb{Q})$ is bijective. Moreover, if $D \equiv 1 \mod 4$, then the homomorphism $\alpha : G_{(P,Q)}(\mathbb{Z}_{(2)}) \to U_{P,Q}(\mathbb{Z}_{(2)})$ is bijective.

(1) If $D \equiv 1 \mod 8$, then we obtain a commutative diagram with exact rows and columns:

$$\begin{tikzcd}
 & 1 \arrow[d] & 1 \arrow[d] & 1 \arrow[d] & \\
1 \arrow[r] & \mathbb{Z}_{(2)}^{\times} \arrow[r] \arrow[d] & (\mathcal{O}_D \otimes_{\mathbb{Z}} \mathbb{Z}_{(2)})^{\times} \arrow[r, "\gamma"] \arrow[d] & U_{P,Q}(\mathbb{Z}_{(2)}) \arrow[r] \arrow[d] & 1 \\
1 \arrow[r] & \mathbb{Q}^{\times} \arrow[r] \arrow[d, "\mathrm{ord}_p"] & \mathbb{Q}(\sqrt{D})^{\times} \arrow[r, "\gamma"] \arrow[d, "(\mathrm{ord}_{\mathfrak{p}}{,}\mathrm{ord}_{\bar{\mathfrak{p}}})"] & U_{P,Q}(\mathbb{Q}) \arrow[r] \arrow[d, "\mathrm{ord}_{\mathfrak{p}}"] & 1\,. \\
0 \arrow[r] & \mathbb{Z} \arrow[r, "\mathit{\Delta}"] \arrow[d] & \mathbb{Z} \times \mathbb{Z} \arrow[r, "\delta"] \arrow[d] & \mathbb{Z} \arrow[r] \arrow[d] & 0 \\
 & 0 & 0 & 0 &
\end{tikzcd}$$

Here $\mathfrak{p}$ is a prime of $\mathbb{Q}(\sqrt{D})$ over 2, and $\bar{\mathfrak{p}}$ denotes the conjugate of $\mathfrak{p}$. Furthermore, $\mathit{\Delta} : \mathbb{Z} \to \mathbb{Z} \times \mathbb{Z}$ and $\delta : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ are defined by $\mathit{\Delta}(a) = (a, a)$ and $\delta(a, b) = a - b$, respectively.

(2) If $D \equiv 5 \mod 8$, then we obtain a commutative diagram with exact rows and columns:

$$\begin{tikzcd}
 & 1 \arrow[d] & 1 \arrow[d] & & \\
1 \arrow[r] & \mathbb{Z}_{(2)}^{\times} \arrow[r] \arrow[d] & (\mathcal{O}_D \otimes_{\mathbb{Z}} \mathbb{Z}_{(2)})^{\times} \arrow[r, "\gamma"] \arrow[d] & U_{P,Q}(\mathbb{Z}_{(2)}) \arrow[r] \arrow[d, "\wr"] & 1 \\
1 \arrow[r] & \mathbb{Q}^{\times} \arrow[r] \arrow[d, "\mathrm{ord}_2"] & \mathbb{Q}(\sqrt{D})^{\times} \arrow[r, "\gamma"] \arrow[d, "\mathrm{ord}_2"] & U_D(\mathbb{Q}) \arrow[r] & 1\,. \\
 & \mathbb{Z} \arrow[r, "\mathrm{id}"] \arrow[d] & \mathbb{Z} \arrow[d] & & \\
 & 0 & 0 & &
\end{tikzcd}$$

(3) If $D/4 \equiv 2, 3 \mod 4$, then we obtain a commutative diagram with exact rows and columns:

$$\begin{tikzcd}
 & 1 \arrow[d] & 1 \arrow[d] & 1 \arrow[d] & \\
1 \arrow[r] & \mathbb{Z}_{(2)}^{\times} \arrow[r] \arrow[d] & (\mathcal{O}_D \otimes_{\mathbb{Z}} \mathbb{Z}_{(2)})^{\times} \arrow[r, "\beta"] \arrow[d] & G_{(P,Q)}(\mathbb{Z}_{(2)}) \arrow[r] \arrow[d, "\alpha"] & 1 \\
1 \arrow[r] & \mathbb{Q}^{\times} \arrow[r] \arrow[d, "\mathrm{ord}_2"] & \mathbb{Q}(\sqrt{D})^{\times} \arrow[r, "\gamma"] \arrow[d, "\mathrm{ord}_{\mathfrak{p}}"] & U_{P,Q}(\mathbb{Q}) \arrow[r] \arrow[d] & 1\,\cdot \\
0 \arrow[r] & \mathbb{Z} \arrow[r, "2"] \arrow[d] & \mathbb{Z} \arrow[r] \arrow[d] & \mathbb{Z}/2\mathbb{Z} \arrow[r] \arrow[d] & 0 \\
 & 0 & 0 & 0 &
\end{tikzcd}$$

Here $\mathfrak{p}$ denotes the prime of $\mathbb{Q}(\sqrt{D})$ over 2.

## 3. Lucas sequences

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

**Notation 3.1.** Let $R$ be a ring and $P, Q \in R$. 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 $\tilde{R} = R[t]/(t^2 - Pt + Q)$ and $\theta = t \mod (t^2 - Pt + Q)$. We define an $R$-homomorphism $\omega : \tilde{R}$ by $\omega(a + b\theta) = b$ $(a, b \in R)$. Moreover, we define an $R$-homomorphism $\omega : \tilde{R} \to R^{\mathbb{N}}$ by $\omega(\eta) = (\omega(\eta\theta^k))_{k\geq 0}$. For $\eta = a + b\theta \in \tilde{R}$, we have $\omega(\eta) = (b, a + Pb, \dots)$.

We can verify the following statements, paraphrasing the proofs of [14, Proposition 3.2 and Corollary 3.3].

(1) The $R$-homomorphism $\tilde{R} \to \mathcal{L}(f, R)$ is bijective.

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

(3) We define an $R$-algebra structure of $\mathcal{L}(f, R)$ through the $R$-isomorphism $\omega : \tilde{R} \xrightarrow{\sim} \mathcal{L}(f, R)$. Then the Lucas sequence $(L_k)_{k\geq 0} = \omega(1)$ is the unit of the ring $\mathcal{L}(f, R)$.

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

$$(w_0w'_1 + w_1w'_0 - Pw_0w'_0, w_1w'_1 - Qw_0w'_0, \dots).$$

It is readily seen that the multiplication by $\theta$ on $\tilde{R}$ induces the shift operation $(w_k)_{k\geq 0} \mapsto (w_{k+1})_{k\geq 0}$ on $\mathcal{L}(f, R)$ through the isomorphism $\omega : \tilde{R} \xrightarrow{\sim} \mathcal{L}(f, R)$.

(4) For $\eta \in \tilde{R} = R/(t^2 - Pt + Q)$, we define $\mathrm{Nr}\,\eta \in R$ by $\mathrm{Nr}\,\eta = \eta(P - \eta)$. For example, we have $\mathrm{Nr}\,\theta = Q$. Obviously, $\eta$ is invertible in $\tilde{R}$ if and only if $\mathrm{Nr}\,\eta$ is invertible in $R$.

Now let $\boldsymbol{w} = (w_k)_{k\geq 0} \in \mathcal{L}(f, R)$. Define $\varDelta(\boldsymbol{w}) \in R$ by $\varDelta(\boldsymbol{w}) = w_1^2 - Pw_0w_1 + Qw_0^2$. If $\eta \in \tilde{R}$ and $\boldsymbol{w} = \omega(\eta)$, then we have $\mathrm{Nr}\,\eta = \varDelta(\boldsymbol{w})$. Therefore, the sequence $\boldsymbol{w} = (w_k)_{k\geq 0}$ is invertible in $\mathcal{L}(f, R)$ if and only if $\varDelta(\boldsymbol{w}) = w_1^2 - Pw_0w_1 + Qw_0^2$ is invertible in $R$.

Hereafter we fix $P, Q \in \mathbb{Z}$, putting $f(t) = t^2 - Pt + Q$ and $D = P^2 - 4Q$.

**Remark 3.2.** Assume that $Q \neq 0$. Then $\theta \in G_{(P,Q)}(\mathbb{Q})$. Moreover, let $(L_k)_{k\geq 0}$ denote the Lucas sequence associated to $(P, Q)$. Then, for $k \geq 1$, we obtain inductively

$$\theta^k = -QL_{k-1} + L_k\theta,$$

and therefore

$$\beta(\theta)^k = \Big(-\frac{L_{k-1}L_k}{Q^{k-1}}, \frac{L_k^2}{Q^k}\Big) \text{ in } G_{(P,Q)}(\mathbb{Q}).$$

**Remark 3.3.** Assume $Q \neq 0$, and let $\Theta$ denote the subgroup of $G_{(P,Q)}(\mathbb{Q})$ generated by $\beta(\theta)$. If $\Theta$ is finite, then $\Theta$ is cyclic of 2, 3, 4 or 6. Furthermore,

$$\begin{aligned} |\Theta| = 2 &\Leftrightarrow P = 0, \\ |\Theta| = 3 &\Leftrightarrow P^2 - Q = 0, \\ |\Theta| = 4 &\Leftrightarrow P^2 - 2Q = 0, \\ |\Theta| = 6 &\Leftrightarrow P^2 - 3Q = 0 \end{aligned}$$

Indeed, $G_{(P,Q)}(\mathbb{Q})$ is isomorphic to the additive group $\mathbb{Q}$ if $D = 0$, and $G_{(P,Q)}(\mathbb{Q})$ is isomorphic to the multiplicative group $\mathbb{Q}^\times$ if $D$ is a square $\neq 0$. On the other hand, if $D$ is note a square, then $G_{(P,Q)}(\mathbb{Q})$ is isomorphic to a subgroup of the multiplicative group $\mathbb{Q}(\sqrt{D})^\times$. These imply the first assertion.

To verify the second assertion, we have only to note

$$\begin{aligned} \beta(\theta^2) &= \Big(-\frac{P}{Q}, \frac{P^2}{Q^2}\Big), \\ \beta(\theta^3) &= \Big(-\frac{P(P^2-Q)}{Q^2}, \frac{(P^2-Q)^2}{Q^3}\Big), \\ \beta(\theta^4) &= \Big(-\frac{P(P^2-Q)(P^2-2Q)}{Q^3}, \frac{P^2(P^2-2Q)^2}{Q^4}\Big), \\ \beta(\theta^6) &= \Big(-\frac{P(P^2-Q)(P^2-3Q)(P^4-3P^2Q+Q^2)}{Q^5}, \frac{P^2(P^2-Q)^2(P^2-3Q)^2}{Q^6}\Big), \end{aligned}$$

which follow from

$$L_1 = 0,\ L_2 = P,\ L_3 = P^2 - Q,$$
$$L_4 = P(P^2 - 2Q),\ L_5 = P^4 - 3P^2Q + Q^2,\ L_6 = P(P^2 - Q)(P^2 - 3Q).$$

From 3.4 to 3.19, 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 3.4.** 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 3.5.** *Let $m$ be an integer with $m \geq 2$ and $(m, Q) = 1$. Then we have*:

(1) *$k(m)$ is equal to the order of $\theta = (0, 1)$ in $G_{P,Q}(\mathbb{Z}/m\mathbb{Z})$;*

(2) *$r(m)$ is equal to the order of $\beta(\theta) = (0, 1/Q)$ in $G_{(P,Q)}(\mathbb{Z}/m\mathbb{Z})$.*

**Proof.** Consider the commutative diagram with exact rows

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

Let $\eta \in G_{P,Q}(\mathbb{Z}/m\mathbb{Z})$ and $a \in (\mathbb{Z}/m\mathbb{Z})^\times$. Then $\omega(\eta) = (0, a, \dots)$ in $\mathcal{L}(f, \mathbb{Z}/m\mathbb{Z})$ if and only if $\omega(\eta) = \omega(a)$, which means $\beta(\eta) = 1$. Hence the results.

**Notation 3.6.** Let $P, Q \in \mathbb{Z}$, and put $f(t) = t^2 - Pt + Q$ and $D = P^2 - 4Q$. Assume that $P \equiv 0 \mod 2$ and $Q \equiv 1 \mod 2$. Let $\theta$ denote the image of $t$ in the residue rings $\mathbb{Z}[t]/(t^2 - Pt + Q)$, and put $\delta = -P/2 + \theta$. Then we have $\delta^2 = D/4$ and $\omega(\delta) = (1, P/2, \dots)$.

As is remarked in 2.19, $\theta \mapsto P/2 + \delta$ gives rise to an isomorphism of rings $\mathbb{Z}[t]/(t^2 - Pt + Q) \xrightarrow{\sim} \mathbb{Z}[t]/(t^2 - D/4)$, and therefore isomorphisms of group schemes $G_{P,Q} \xrightarrow{\sim} G_{D/4}$ and $G_{(P,Q)} \xrightarrow{\sim} G_{(D/4)}$. For a ring $R$, we shall often indentify $G_{P,Q}(R)$ with $G_{D/4}(R)$ and $G_{(P,Q)}(R)$ with $G_{(D/4)}(R)$ through the isomorphisms $G_{P,Q} \xrightarrow{\sim} G_{D/4}$ and $G_{(P,Q)} \xrightarrow{\sim} G_{(D/4)}$.

**Theorem 3.7.** *Let $P, Q \in \mathbb{Z}$. Assume that $P \equiv 0 \mod 2$ and $Q \equiv 1 \mod 2$, and put $\nu = \mathrm{ord}_2 P$.*

(1) *If $P \neq 0$, then we have*

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

(2) *If $P = 0$, then we have $r(2^n) = 2$ for any $n \geq 1$.*

Proof. Assume first $\nu = 1$. Then we obtain $P/2 \equiv 1 \mod 2$ and $D/4 = (P/2)^2 - Q \equiv 0 \mod 2$. Therefore, by Corollary 2.6, $\beta(\theta) = \beta(P/2 + \delta)$ is of order $2^n$ in $G_{(P,Q)}(\mathbb{Z}/2^n\mathbb{Z}) = G_{D/4}(\mathbb{Z}/2^n\mathbb{Z})$. Hence the result.

Assume now that $P \neq 0$ and $\nu \geq 2$. Then we obtain $r(2) = \cdots = r(2^\nu) = 2$ and $r(2^{\nu+1}) > 2$. Hence, for $n \geq \nu + 1$, we have

$$\beta(\theta)^2 \in \mathrm{Ker}[G_{(P,Q)}(\mathbb{Z}/2^n\mathbb{Z}) \to G_{(P,Q)}(\mathbb{Z}/2^\nu\mathbb{Z})]$$

but

$$\beta(\theta)^2 \notin \mathrm{Ker}[G_{(P,Q)}(\mathbb{Z}/2^n\mathbb{Z}) \to G_{(P,Q)}(\mathbb{Z}/2^{\nu+1}\mathbb{Z})].$$

Moreover, we have

$$\begin{aligned} \beta(\theta)^2 &\in \mathrm{Ker}[G_{(P,Q)}(\mathbb{Z}/2^n) \to G_{(P,Q)}(\mathbb{Z}/4\mathbb{Z})] \\ &= (\text{the subgroup of } G_{(P,Q)}(\mathbb{Z}/2^n\mathbb{Z}) \text{ generated by } \beta(1+4\delta)) \end{aligned}$$

since $\nu \geq 2$. It follows that $\beta(\theta)^2 = \beta(1 + 4\delta)^{2^\nu c}$ with $(c, 2) = 1$ in $G_{(P,Q)}(\mathbb{Z}/2^n\mathbb{Z})$. Hence $\beta(\theta)$ is of order $2^{n-\nu+1}$ in $G_{(P,Q)}(\mathbb{Z}/2^n\mathbb{Z})$.

**Theorem 3.8.** *Let $P, Q \in \mathbb{Z}$. Assume that $P \equiv 0 \mod 2$ and $Q \equiv 1 \mod 2$, and put $\nu = \mathrm{ord}_2 P$. Then:*

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

(2) *If* $\nu \geq 2$ *and* $P \neq 0$, *then*

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

(3) *If* $P = 0$, *then* $k(2^n) = 2\times$(the order of $-Q \bmod 2^n$) *for any* $n \geq 1$.

Proof. (1) It follows from the assumption that $P/2 \equiv 1 \mod 2$ and $D/4 = (P/2)^2 - Q \equiv 0 \mod 2$. Hence, by Lemma 2.5, $\theta = P/2 + \delta$ is of order $2^n$ in $G_{P,Q}(\mathbb{Z}/2^n\mathbb{Z}) = G_{D/4}(\mathbb{Z}/2^n\mathbb{Z})$ for $n \geq 1$.

(2)(3) If $P = 0$, then we obtain $L_{2k} = 0$ and $L_{2k+1} = (-Q)^k$ for $k \geq 0$. Hence the result.

Assume now $P \neq 0$. Then we have $P \equiv 2^\nu \mod 2^{\nu+1}$ and therefore $P^2 \equiv 2^{2\nu} \mod 2^{\nu+2}$. Hence we obtain $P^2/2 \equiv 0 \mod 2^{\nu+1}$ since $\nu \geq 2$. This, together with $\delta^2 = P^2/4 - Q$, implies

$$\theta^2 = \left(\frac{P}{2}\right)^2 + P\delta + \delta^2 = \frac{P^2}{2} - Q + P\delta \equiv -Q + 2^\nu\delta \mod 2^{\nu+1}.$$

Moreover, if $n \leq \nu$, then we obtain $\theta^2 \equiv -Q \mod 2^n$ and therefore

$$\text{(the order of } \theta \bmod 2^n) = 2\times(\text{the order of } -Q \bmod 2^n).$$

If $n \geq \nu + 1$, we can verify inductively

$$\theta^{2^{n-\nu}} \equiv (-Q)^{2^{n-\nu-1}} + 2^{n-1}\delta \mod 2^n,\ \theta^{2^{n-\nu+1}} \equiv (-Q)^{2^{n-\nu}} \mod 2^n.$$

These imply that

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

**Remark 3.8.1.** Let $P, Q \in \mathbb{Z}$, and assume $Q \neq 0$ and $D = 0$. Then there exists $a \in \mathbb{Z}$ such that $P = 2a$ and $Q = a^2$, and we obtain

$$\xi(\theta) = \left(a, \frac{1}{a}\right) \text{ in } (\mathbb{G}_m \times \mathbb{G}_a)(\mathbb{Q}) = \mathbb{Q}^\times \times \mathbb{Q}, \text{ and } \xi(\beta(\theta)) = \frac{1}{a} \text{ in } \mathbb{G}_a(\mathbb{Q}) = \mathbb{Q}.$$

Furthermore, let $p$ be a prime with $(a, p) = 1$. Then $\beta(\theta) \in G_{(P,Q)}(\mathbb{Z}_{(p)})$, and $\beta(\theta)$ generates $G_{(P,Q)}(\mathbb{Z}/p^n\mathbb{Z}) = \mathbb{Z}/p^n\mathbb{Z}$ for $n \geq 1$. This implies that, for $n \geq 1$, we have

$$r(p^n) = p^n$$

and

$$k(p^n) = \begin{cases} p^n s & \text{if } p > 2 \\ 2^n & \text{if } p = 2. \end{cases}$$

Here $s$ denotes the order of $a$ in $(\mathbb{Z}/p\mathbb{Z})^\times$.

The assertion above is a special case of Theorem 3.7 (1), Theorem 3.8 (1) and [14, Corollary 3.16 (3)]. Here is an elementary verification. The Lucas sequence associated to $(P, Q)$ is given by $(L_k)_{k\geq 0} = (ka^{k-1})_{k\geq 0}$. Then we have the following implications:

$$L_k \equiv 0 \mod p^n \ \Leftrightarrow \ p^n|k,$$
$$L_k \equiv 0 \mod p^n, \ L_{k+1} \equiv 0 \mod p^n \ \Leftrightarrow \ p^n|k, \ p^n|(a^k-1) \ \Leftrightarrow \ p^n|k, \ s|k.$$

**Corollary 3.9.** *Let $P, Q \in \mathbb{Z}$. Assume that $\nu = \mathrm{ord}_2 P \geq 2$ and $P \neq 0$. Then*:
(1) *If $Q \equiv 1 \mod 2^\nu$, then*

$$k(2^n) = \begin{cases} 2 & \text{if } n = 1 \\ 4 & \text{if } 2 \leq n \leq \nu \\ 2^{n-\nu+1} & \text{if } n \geq \nu+1 \end{cases} \cdot$$

(2) *If $Q \equiv -1 \mod 2^\nu$, then*

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

**Notation 3.10.** Let $P$ and $Q$ be odd integers. Let $\theta$ denote the image of $t$ in the residue ring $\mathbb{Z}[t]/(t^2 - Pt + Q)$, and put $\delta = -P + 2\theta$. Then we have $\delta^2 = D$. Moreover, there exists $r \in \mathbb{Z}_2$ such that $r^2 = -D/3$ since $D \equiv 5 \mod 8$. We may assume $r \equiv 1 \mod 4$, replacing $r$ by $-r$ if $r \equiv -1 \mod 4$. Put

$$\omega = \frac{-r+\delta}{2r} = -\frac{r+P}{2r} + \frac{\theta}{r} \in \mathbb{Z}_2[t]/(t^2 - Pt + Q).$$

Then we have $(\delta/r)^2 = -3$ and there $\omega^3 = 1$.

**Lemma 3.11.** *Under the notations above, we have* $\mathrm{ord}_2(r-1) = \mathrm{ord}_2(D+3) - 1$.

Proof. By the definition, we obtain $3(r^2-1) = -(D+3)$ and therefore $\mathrm{ord}_2(r^2-1) = \mathrm{ord}_2(D+3)$. Moreover, we have $\mathrm{ord}_2(r+1) = 1$ since $r \equiv 1 \mod 4$. Hence the result.

**Theorem 3.12.** *Let $P, Q \in \mathbb{Z}$. Assume that $P \equiv 1 \mod 2$ and $Q \equiv 1 \mod 4$, and put $\nu = \mathrm{ord}_2(P^2 - Q)$. Then we have $\nu \geq 2$. Furhtermore,*
(1) *If $P^2 - Q \neq 0$, then we have*

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

(2) *If $P^2 - Q = 0$, then we have $r(2^n) = 3$ for any $n \geq 1$.*

Proof. First note that $L_3 = P^2 - Q$ and that $\mathrm{ord}_2(P^2 - Q) \geq 2$ follows from the assumptions $P \equiv 1 \mod 2$ and $Q \equiv 1 \mod 4$. If $P^2 - Q = 0$, then we have $r(2^n) = 3$ for any $n \geq 1$.

Assume now that $P^2 - Q \neq 0$. Then we obtain $r(2) = \cdots = r(2^\nu) = 3$ and $r(2^{\nu+1}) > 3$. Hence, for $n \geq \nu + 1$, we have

$$\beta(\theta)^3 \in \mathrm{Ker}[G_{(P,Q)}(\mathbb{Z}/2^n\mathbb{Z}) \to G_{(P,Q)}(\mathbb{Z}/2^\nu\mathbb{Z})]$$

but

$$\beta(\theta)^3 \notin \mathrm{Ker}[G_{(P,Q)}(\mathbb{Z}/2^n\mathbb{Z}) \to G_{(P,Q)}(\mathbb{Z}/2^{\nu+1}\mathbb{Z})].$$

Moreover, we have

$$\begin{aligned}\beta(\theta)^3 &\in \mathrm{Ker}[G_{(P,Q)}(\mathbb{Z}/2^n) \to G_{(P,Q)}(\mathbb{Z}/4\mathbb{Z})]\\ &= (\text{the subgroup of } G_{(P,Q)}(\mathbb{Z}/2^n\mathbb{Z}) \text{ generated by } \beta(1+4\delta))\end{aligned}$$

since $\nu \geq 2$. This means

$$\begin{aligned}\gamma(\theta)^3 &\in \mathrm{Ker}[U_{(P,Q)}(\mathbb{Z}/2^n) \to U_{(P,Q)}(\mathbb{Z}/4\mathbb{Z})]\\ &= (\text{the subgroup of } U_{(P,Q)}(\mathbb{Z}/2^n\mathbb{Z}) \text{ generated by } \gamma(1+4\omega))\end{aligned}$$

since the homomorphism $\alpha : G_{(P,Q)} \to U_{P,Q}$ is isomorphic. Therefore we obtain $\gamma(\theta)^3 = \gamma(1+4\omega)^{2^{\nu-2}c}$ with $(c,2) = 1$ in $U_{P,Q}(\mathbb{Z}/2^n\mathbb{Z})$. This implies that $\gamma(\theta)$ is of order $3 \times 2^{n-\nu}$ in $U_{P,Q}(\mathbb{Z}/2^n\mathbb{Z})$ and therefore $\beta(\theta)$ is of order $3 \times 2^{n-\nu}$ in $G_{(P,Q)}(\mathbb{Z}/2^n\mathbb{Z})$.

**Remark 3.12.1.** If $Q \equiv 5 \mod 8$, then $\nu = \mathrm{ord}_2(P^2 - Q) = 2$.

**Theorem 3.13.** *Let $P, Q \in \mathbb{Z}$. Assume that $P \equiv 1 \mod 2$ and $Q \equiv -1 \mod 4$, and put $\nu = \mathrm{ord}_2(P^2 - Q)(P^2 - 3Q)$. Then we have $\nu \geq 3$. Futhermore,*
(1) *If $P^2 - 3Q \neq 0$, then*

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

(2) *If $P^2 - 3Q = 0$, then $r(2) = 3$ and $r(2^n) = 6$ for any $n \geq 2$.*

Proof. First note that $L_6 = P(P^2 - Q)(P - 3Q^2)$ and that the assumption $P \equiv 1 \mod 2$ and $Q \equiv -1 \mod 4$ implies $\mathrm{ord}_2(P^2 - Q) = 1$ and $\mathrm{ord}_2(P^2 - 3Q) \geq 2$. If $P - 3Q^2 = 0$, then we have $r(2^n) = 6$ for any $n \geq 2$.

Assume now that $P^2 - 3Q \neq 0$. Then we obtain $r(2) = 3$, $r(4) = \ldots = r(2^\nu) = 6$ and $r(2^{\nu+1}) > 6$. Hence, for $n \geq \nu + 1$, we have

$$\beta(\theta)^6 \in \mathrm{Ker}[G_{(P,Q)}(\mathbb{Z}/2^n\mathbb{Z}) \to G_{(P,Q)}(\mathbb{Z}/2^\nu\mathbb{Z})]$$

but

$$\beta(\theta)^6 \notin \mathrm{Ker}[G_{(P,Q)}(\mathbb{Z}/2^n\mathbb{Z}) \to G_{(P,Q)}(\mathbb{Z}/2^{\nu+1}\mathbb{Z})].$$

Moreover, we have

$$\begin{aligned}\beta(\theta)^6 &\in \mathrm{Ker}[G_{(P,Q)}(\mathbb{Z}/2^n) \to G_{(P,Q)}(\mathbb{Z}/4\mathbb{Z})]\\ &= (\text{the subgroup of } G_{(P,Q)}(\mathbb{Z}/2^n\mathbb{Z}) \text{ generated by } \beta(1+4\delta))\end{aligned}$$

since $\nu \geq 3$. This means

$$\begin{aligned}\gamma(\theta)^6 &\in \mathrm{Ker}[U_{(P,Q)}(\mathbb{Z}/2^n) \to U_{(P,Q)}(\mathbb{Z}/4\mathbb{Z})]\\ &= (\text{the subgroup of } U_{(P,Q)}(\mathbb{Z}/2^n\mathbb{Z}) \text{ generated by } \gamma(1+4\omega)).\end{aligned}$$

Therefore we obtain $\gamma(\theta)^6 = \gamma(1+4\omega)^{2^{\nu-2}c}$ with $(c,2)=1$ in $U_{P,Q}(\mathbb{Z}/2^n\mathbb{Z})$. This implies that $\gamma(\theta)$ is of order $6\times 2^{n-\nu}$ in $U_{P,Q}(\mathbb{Z}/2^n\mathbb{Z})$ and therefore $\beta(\theta)$ is of order $6\times 2^{n-\nu}$ in $G_{(P,Q)}(\mathbb{Z}/2^n\mathbb{Z})$.

**Remark 3.13.1.** If $Q \equiv -1 \mod 8$, then $\mathrm{ord}_2(P^2-3Q)=2$. This implies $\nu = 3$.

**Theorem 3.14.** *Let $P, Q \in \mathbb{Z}$. Assume that $P \equiv 1 \mod 2$ and $Q \equiv -1 \mod 4$. Then we have $k(2^n) = 3\times 2^{n-1}$ for $n \geq 1$.*

Proof. By the assumption we have $4Q \equiv -4 \mod 16$. Then we obtain $D \equiv 5 \mod 16$ and $r \equiv 5 \mod 8$ if $P \equiv \pm 1 \mod 8$, and $D \equiv -3 \mod 16$ and $r \equiv 1 \mod 8$ if $P \equiv \pm 5 \mod 8$. This implies:

(1) if $P \equiv 1, 5 \mod 8$, then $P + r \equiv -2 \mod 8$ and therefore $\theta \equiv -1+\omega \mod 4$;

(2) if $P \equiv -1, -5 \mod 8$, then $P + r \equiv 4 \mod 8$ and therefore $\theta \equiv 2+\omega \mod 4$.

In both the cases, we have $\theta^3 \equiv -1 + 2\omega \mod 4$. Then we can verify inductively $\theta^{3\cdot 2^{n-2}} \equiv 1 + 2^{n-1}\omega \mod 2^n$ and $\theta^{3\cdot 2^{n-1}} \equiv 1 \mod 2^n$ for $n \geq 2$.

**Theorem 3.15.** *Let $P, Q \in \mathbb{Z}$. Assume that $P \equiv 5 \mod 8$ and $Q \equiv 1 \mod 4$. Then we have*

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

Proof. By the assumption, we have $4Q \equiv 4 \mod 16$, $D \equiv 5 \mod 16$ and $r \equiv 5 \mod 8$. These imply $P+r \equiv 2 \mod 8$ and therefore $\theta \equiv (1+\omega)+4\omega \mod 8$. Hence we obtain $\theta^3 \equiv -1+4(1+\omega) \mod 8$, and we can verify inductively $\theta^{3\cdot 2^{n-3}} \equiv 1+2^{n-1}(1+\omega) \mod 2^n$ and $\theta^{3\cdot 2^{n-2}} \equiv 1 \mod 2^n$ for $n \geq 3$.

**Theorem 3.16.** *Let $P, Q \in \mathbb{Z}$. Assume that $P \equiv -5 \mod 8$ and $Q \equiv 1 \mod 4$. Then we have*

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

Proof. By the assumption, we have $4Q \equiv 4 \mod 16$, $D \equiv 5 \mod 16$ and $r \equiv 5 \mod 8$. These imply $P + r \equiv 0 \mod 8$ and therefore $\theta \equiv 5\omega \mod 8$. Hence we obtain $\theta^3 \equiv 5 \mod 8$, and we can verify inductively $\theta^{3\cdot 2^{n-3}} \equiv 1 + 2^{n-1} \mod 2^n$ and $\theta^{3\cdot 2^{n-2}} \equiv 1 + 2^{n-1} \mod 2^n$ for $n \geq 3$.

**Theorem 3.17.** *Let $P, Q \in \mathbb{Z}$. Assume that $P \equiv 1 \mod 8$, $Q \equiv 1 \mod 4$ and $P^2 - Q \neq 0$, and put $\mu = \min[\mathrm{ord}_2(P + r - 2) - 1, \mathrm{ord}_2(r - 1)]$. Then we have $\mu \geq 2$ and*

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

Proof. By the assumption, we have $P^2 \equiv 1 \mod 16$ and $4Q \equiv 4 \mod 16$ and therefore $D+3 \equiv 0 \mod 16$. Then $\mathrm{ord}_2(r - 1) \geq 3$. On the other hand, we have $\mathrm{ord}_2(P - 1) \geq 3$. Then we obtain $\mu \geq 2$. Moreover, we have $\mu < \infty$.

Indeed, note the implications:

$$\mu = \infty \ \Leftrightarrow \ P + r - 2 = 1,\ r = 1 \Leftrightarrow \ P = 1,\ D = -3 \ \Leftrightarrow \ P = 1, Q = 1.$$

Therefore, the possibility of $\mu = \infty$ is excluded by the assumption $P^2 - Q \neq 0$.

By the definition of $\mu$, we have

$$\frac{P + r}{2} \equiv 1 \mod 2^\mu,\ r \equiv 1 \mod 2^\mu.$$

and therefore $\theta \equiv (1 + \omega) + 2^\mu \eta \mod 2^{\mu+1}$, where $\eta \in \{1, \omega, 1 + \omega\}$. Hence we obtain $\theta^3 \equiv -1 + 2^\mu \omega \eta \mod 2^{\mu+1}$, and we can verify inductively $\theta^{3 \cdot 2^{n-\mu-1}} \equiv 1 + 2^{n-1}\omega\eta \mod 2^n$ and $\theta^{3\cdot 2^{n-\mu}} \equiv 1 \mod 2^n$ for $n \geq \mu + 2$. Hence the result.

**Theorem 3.18.** *Let $P, Q \in \mathbb{Z}$. Assume that $P \equiv -1 \mod 8$, $Q \equiv 1 \mod 4$ and $P^2 - Q \neq 0$. Put $\mu = \min[\mathrm{ord}_2(P + r), \mathrm{ord}_2(r - 1)]$. Then we have $\mu \geq 2$ and*

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

Proof. By the assumption, we have $P^2 \equiv 1 \mod 16$ and $4Q \equiv 4 \mod 16$ and therefore $D+3 \equiv 0 \mod 16$. Then $\mathrm{ord}_2(r - 1) \geq 3$. On the other hand, we have $\mathrm{ord}_2(P + 1) \geq 3$. Then we obtain $\mu \geq 2$. Moreover, we have $\mu < \infty$.

Indeed, note the implications:

$$\mu = \infty \ \Leftrightarrow \ P + r = 0,\ r = 1 \Leftrightarrow \ P = -1,\ D = -3 \ \Leftrightarrow \ P = -1, Q = 1.$$

Therefore, the possibility of $\mu = \infty$ is excluded by the assumption $P^2 - Q \neq 0$.

By the definition of $\mu$, we have

$$\frac{P + r}{2} \equiv 0 \mod 2^\mu,\ r \equiv 1 \mod 2^\mu.$$

and therefore $\theta \equiv \omega + 2^\mu \eta \mod 2^{\mu+1}$, where $\eta \in \{1, \omega, 1 + \omega\}$. Hence we obtain $\theta^3 \equiv 1 + 2^\mu \omega^2 \eta \mod 2^{\mu+1}$, and we can verify inductively $\theta^{3\cdot 2^{n-\mu-1}} \equiv 1 + 2^{n-1}\omega^2\eta \mod 2^n$ and $\theta^{3\cdot 2^{n-\mu}} \equiv 1 \mod 2^n$ for $n \geq \mu + 1$. Hence the result.

**Remark 3.19.** Let $P, Q \in \mathbb{Z}$, and assume $P^2 - Q = 0$, Then there exists $a \in \mathbb{Z}$ such that $P = a$ and $Q = a^2$. Moreover, for $k \geq 0$, we have

$$L_{3k} = 0,\ L_{3k+1} = (-a^3)^k,\ L_{3k+2} = (-a^3)^k a.$$

Therefore, if $a \equiv 1 \mod 2$, then we have $k(2^n) = 3\times$(the order of $-a$ in $(\mathbb{Z}/2^n\mathbb{Z})^\times$).

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 a prime $p$ and a positive integer $n$. We refer to [12, Section 2] concerning a precise argument on the action of $PGL_{2,\mathbb{Z}}$ on $\mathbb{P}^1_{\mathbb{Z}}$.

**3.20.** Let $R$ be a ring. Then the group $G_{P,Q}(R)$ acts $R$-linearly on the $R$-algebra $\mathcal{L}(f, R)$ through the isomorphism $\omega : G_{P,Q}(R) \xrightarrow{\sim} \mathcal{L}(f, R)^\times$. This defines an $R$-linear action of $G_{P,Q}(R)$ on $R^2$ through the $R$-isomorphism $\mathcal{L}(f, R) \xrightarrow{\sim} R^2$ given by $(w_k)_{k\geq 0} \mapsto (w_0, w_1)$. Hence we obtain a homomorphism $i_R : G_{P,Q}(R) \to GL(2, R)$, which is described explicitly as

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

The homomorphism $i_R : G_{P,Q}(R) \to GL(2, R)$ is represented by a homomorphism of group schemes $i : G_{P,Q} \to GL_2$. It is readily seen that $i : G_{P,Q} \to GL_2$ is a closed immersion.

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

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

and

$$u^2 + Puv + Qv^2 = w_1^2 - Pw_0w_1 + Qw_0^2.$$

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

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

The induced homomorphism $i : G_{(P,Q)} \to PGL_2$ is a closed immersion.

**Notation 3.21.** We shall denote by $\Theta$ all the subgroup of $G_{P,Q}(\mathbb{Z}[1/Q])$ generated by $\theta = (0, 1)$, the subgroup of $G_{(P,Q)}(\mathbb{Z}[1/Q])$ generated by $\beta(\theta) = (0, 1/Q)$ and the subgroup of $U_D(\mathbb{Z}[1/Q])$ generated by $\gamma(\theta) = (-1, P/Q)$.

**Notation 3.22.** We have

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

By the abbreviation, we shall denote by $\Theta$ the image of the subgroup $\Theta$ of $G_{(P,Q)}(\mathbb{Z}[1/Q])$ by $i : G_{(P,Q)}(\mathbb{Z}[1/Q]) \to PGL(2, \mathbb{Z}[1/Q])$. Let $(w_n)_{n\geq 0} \in \mathcal{L}(f, \mathbb{Q})$. Then it is readily seen that

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

**3.23.** 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 3.24.** 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.

**Notation 3.25.** 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 $\mathcal{R}(f, \mathbb{Z}) \xrightarrow{\sim} \mathbb{P}^1(\mathbb{Z}) = \mathbb{P}^1(\mathbb{Q})$.

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

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

Indeed, the inclusion 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

$$\{\boldsymbol{w} = (w_k)_{k\geq 0} \in \mathcal{R}(f, \mathbb{Z})\ ;\ \Delta(\boldsymbol{w}) = w_1^2 - Pw_0w_1 + Qw_0^2 \not\equiv 0 \mod p\}.$$

Indeed, the inclusion 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 $\mathcal{L}(f, \mathbb{Z}_{(p)})^\times \to \mathcal{L}(f, \mathbb{Z}_{(p)})^\times/\mathbb{Z}_{(p)}^\times$.

We can now mention the main result on the action of $G_{(D)}(\mathbb{Z}/p^n\mathbb{Z})$ on $\mathbb{P}^1(\mathbb{Z}/p^n\mathbb{Z})$. The following assertions was established as [14, Proposition 3.23 and Theorem 3.25] in the case of $p > 2$. We can verify the assertions, only replacing $G_{(D)}(\mathbb{Z}_{(p)})$ by $G_{(P,Q)}(\mathbb{Z}_{(p)})$, so we omit the proof.

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

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

**Theorem 3.27.** *Let $p$ be a prime with $(p, Q) = 1$ and $n$ a positive integer. Let $\boldsymbol{w} = (w_k)_{k\geq 0} \in \mathcal{L}(f, \mathbb{Z}_{(p)})$, and put $\mu = \mathrm{ord}_p \varDelta(\boldsymbol{w})$. Assume that $(w_0, w_1) = \mathbb{Z}_{(p)}$. Then we have*

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

Here are a few numerical examples.

**Example 3.28.1.** $P = 1$, $Q = 3$. In this case, the $\Theta$-orbits in $\mathbb{P}^1(\mathbb{Z}/16\mathbb{Z})$ are given by

$$\{(0:1),(1:1),(1:14),(2:5),(1:3),(1:0)\},\ \{(1:2),(2:7),(1:7),(1:12),(1:13),(1:5)\},$$
$$\{(1:4),(4:1),(1:5),(1:10),(2:3),(1:15)\},\ \{(1:6),(2:1),(1:11),(1:8),(8:5),(1:9)\}.$$

Note that

$$\varDelta(0,1) = 1,\ \varDelta(1,2) = 5,\ \varDelta(1,4) = 15,\ \varDelta(1,6) = 33.$$

**Example 3.28.2.** $P = 8$, $Q = 7$. In this case, the $\Theta$-orbits in $\mathbb{P}^1(\mathbb{Z}/16\mathbb{Z})$ are given by

$$\{(0:1),(1:8),(8:1),(1:0)\},\ \{(1:2),(2:1),(1:10),(2:5)\},$$
$$\{(1:4),(4:1),(1:12),(4:3)\},\ \{(1:6),(2:3),(1:14),(2:7)\},$$
$$\{(1:3),(1:11)\},\ \{(1:5),(1:13)\},$$
$$\{(1:9)\},\ \{(1:15)\},\ \{(1:1)\},\ \{(1:7)\}$$

Note that

$$\varDelta(0,1) = 1,\ \varDelta(1,2) = -5,\ \varDelta(1,4) = -9,\ \varDelta(1,6) = -5,$$
$$\varDelta(1,3) = -8,\ \varDelta(1,5) = -8,\ \varDelta(1,9) = 16,\ \varDelta(1,15) = 112,\ \varDelta(1,1) = 0,\ \varDelta(1,7) = 0.$$

## 4. Laxton groups

Throughout the section, we fix $P, Q \in \mathbb{Z}$, putting $f(t) = t^2 - Pt + Q$ and $D = P^2 - 4Q$. We denote by $\theta$ the image of $t$ in the residue ring $\mathbb{Z}[t]/(t^2 - Pt + Q)$.

**Definition 4.1.** First we recall the defintion of the group $G(f)$ due to Laxton [8, Section 2], modifying descriptions and notations, for the reader's convenience though a copy and paste from [14, Defintion 4.1]. 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 $k \geq 0$.

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

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

which coincides with the multiplication mentioned in 3.1. Then $\mathcal{L}(f,\mathbb{Z})^\circ / \sim_L$ is a commutative group.

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 $n$. Then $G(f,p^n)$ is a subgroup $G(f)$. 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 $G(f)$.

Summing up, we have gotten a descending chain of subgroups

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

**Remark 4.1.1.** To define the group $G(f)$, Laxton assumed in [8] that $(P,Q) = 1$ and $P \neq 0$, $P^2 - Q \neq 0$, $P^2 - 2Q \neq 0$, $P^2 - 3Q \neq 0$, $D = P^2 - 4Q \neq 0$, probably for simplicity. We followed his way in [14], however, we treat here also the cases excluded by Laxton because of its own interest in each case.

**Theorem 4.2.** *Let $P, Q \in \mathbb{Z}$, and assume $Q \neq 0$. Then we have $\theta \in G_{P,Q}(\mathbb{Q})$. Furthermore, let $\Theta$ denote the subgroup of $G_{(D)}(\mathbb{Q})$ generated by $\beta(\theta) = (0, 1/Q)$. Then the isomorphism $\omega : U_{P,Q}(\mathbb{Q}) = G_{(P,Q)}(\mathbb{Q}) \xrightarrow{\sim} \mathcal{L}(f,\mathbb{Q})^\times/\mathbb{Q}^\times$ induces an isomorphism $\omega : U_{P,Q}(\mathbb{Q})/\Theta = G_{(P,Q)}(\mathbb{Q})/\Theta \xrightarrow{\sim} G(f)$.*

**Proof.** Let $\eta, \eta' \in \mathbb{Z}[t]/(t^2 - Pt + Q)$, and put $\boldsymbol{w} = (w_k)_{k\geq 0} = \omega(\eta)$ and $\boldsymbol{w}' = (w'_k)_{k\geq 0} = \omega(\eta')$. 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

$G_{(P,Q)}(\mathbb{Q}) = G_{P,Q}(\mathbb{Q})/\mathbb{Q}^\times$. Indeed, the inclusion $\mathcal{L}(f,\mathbb{Z})^\circ \to \mathcal{L}(f,\mathbb{Q})^\times$ induces an isomorphism $\mathcal{L}(f,\mathbb{Z})^\circ/\sim'_L \overset{\sim}{\to} \mathcal{L}(f,\mathbb{Q})^\times/\mathbb{Q}^\times$.

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 $P, Q \in \mathbb{Z}$ with $Q \equiv 1 \mod 2$ and $D = P^2 - 4Q \neq 0$. Then we have $\Theta \subset G_{(P,Q)}(\mathbb{Z}_{(2)})$. Furthermore, put*

$$r = \left[\frac{\mathrm{ord}_2 D}{2}\right], \ \tilde{D} = \frac{D}{4^r}$$

*and*

$$(\tilde{P},\tilde{Q}) = \begin{cases} \left(-1, \dfrac{1-\tilde{D}}{4}\right) & \text{if } \tilde{D} \equiv 1 \mod 4 \\ (0, \tilde{D}) & \text{if } \tilde{D} \equiv 2, 3 \mod 4 \end{cases}.$$

*Then the descending chain of subgroups of $G_{(P,Q)}(\mathbb{Q}) = U_{P,Q}(\mathbb{Q})$:*

$$U_{P,Q}(\mathbb{Q}) \supset U_{\tilde{P},\tilde{Q}}(\mathbb{Z}_{(2)}) \supset G_{(P,Q)}(\mathbb{Z}_{(2)}) \supset G_{(2^2P,4^2Q)}(\mathbb{Z}_{(2)}) \supset \cdots \supset G_{(2^nP,4^nQ)}(\mathbb{Z}_{(2)}) \supset \cdots$$

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

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

*More precisely,*

*(1) The isomorphism $\omega : G_{(P,Q)}(\mathbb{Q})/\Theta \overset{\sim}{\to} G(f)$ induces isomorphisms*

$$U_{\tilde{P},\tilde{Q}}(\mathbb{Z}_{(2)})/\Theta \xrightarrow{\sim} H(f,2),$$
$$G_{(P,Q)}(\mathbb{Z}_{(2)})/\Theta \xrightarrow{\sim} K(f,2)$$

*and*

$$(G_{(2^nP,4^nQ)}(\mathbb{Z}_{(2)}) + \Theta)/\Theta \xrightarrow{\sim} G(f,2^n)$$

*for each $n > 0$.*

*(2) The isomorphism $\omega : G_{(P,Q)}(\mathbb{Q})/\Theta \xrightarrow{\sim} G(f)$ induces isomorphisms*

$$U_{\tilde{P},\tilde{Q}}(\mathbb{Z}_{(2)})(\mathbb{Z}_{(2)})/G_{(P,Q)}(\mathbb{Z}_{(2)}) = (U_{\tilde{P},\tilde{Q}}(\mathbb{Z}_{(2)})(\mathbb{Z}_{(2)})/\Theta)/(G_{(P,Q)}(\mathbb{Z}_{(2)})/\Theta) \xrightarrow{\sim} H(f,2)/K(f,2)$$

*and*

$$G_{(P,Q)}(\mathbb{Z}_{(2)})/(G_{(2^nP,4^nQ)}(\mathbb{Z}_{(2)}) + \Theta) \xrightarrow{\sim} K(f,2)/G(f,2^n)$$

*for each $n > 0$. Therefore, $K(f,2)/G(f,2^n)$ is isomorphic to $G_{(P,Q)}(\mathbb{Z}/2^n\mathbb{Z})/\Theta$.*

*(3) For each $n > 0$, we have*

$$|G(f,2^n)/G(f,2^{n+1})| = |K(f,2)/G(f,2^{n+1})|/|K(f,2)/G(f,2^n)|.$$

**Proof.** Note first that $r = 0$ if and only if $P \equiv 1 \mod 2$ and $Q \equiv 1 \mod 2$. In this case, we obtain an isomorhism $G_{(\tilde{P},\tilde{Q})} \overset{\sim}{\to} G_{(P,Q)}$ through the identity

$$\left(t - \frac{P-1}{2}\right)^2 - \left(t - \frac{P-1}{2}\right) + \frac{1-D}{4} = t^2 - Pt + Q.$$

On the other hand, if $r \geq 1$, then $G_{(P,Q)}$ is isomorphic to $G_{(D/4)}$ as is reamrked in 2.19. Moreover, $G_{(\tilde{D})}$ is isomorphic to $G_{(2\tilde{P},4\tilde{Q})}$ if $\tilde{D} \equiv 1 \mod 4$, and $G_{(\tilde{D})} = G_{(\tilde{P},\tilde{Q})}$ if $\tilde{D} \equiv 2,3 \mod 4$.

First we prove the main assertion except $K(2,f) = G(f,2)$, which we verify after proving the assertion (2). The assumption $(2,Q) = 1$ implies $\Theta \subset G_{(P,Q)}(\mathbb{Z}_{(2)})$. Furthermore, by Proposition 2.2, we have

$$U_{\tilde{P},\tilde{Q}}(\mathbb{Q})/U_{\tilde{P},\tilde{Q}}(\mathbb{Z}_{(2)}) = \begin{cases} \mathbb{Z} & \text{if } \tilde{D} \equiv 1 \mod 8 \\ 0 & \text{otherwise} \end{cases}.$$

On the other hand, $U_{\tilde{P},\tilde{Q}}(\mathbb{Z}_{(2)})/G_{P,Q}(\mathbb{Z}_{(2)})$ is finite. Indeed, by Proposition 2.3, we have

$$U_{\tilde{P},\tilde{Q}}(\mathbb{Z}_{(2)})/G_{(\tilde{P},\tilde{Q})}(\mathbb{Z}_{(2)}) = \begin{cases} 0 & \text{if } \tilde{D} \equiv 1 \mod 4 \\ \mathbb{Z}/2\mathbb{Z} & \text{if } \tilde{D} \equiv 2,3 \mod 4 \end{cases}.$$

Moreover, we have

$$G_{(P,Q)}(\mathbb{Z}_{(2)}) = \begin{cases} G_{(2^r\tilde{P},4^r\tilde{Q})}(\mathbb{Z}_{(2)}) & \text{if } \tilde{D} \equiv 1 \mod 4 \\ G_{(2^{r-1}\tilde{P},4^{r-1}\tilde{Q})}(\mathbb{Z}_{(2)}) & \text{if } \tilde{D} \equiv 2,3 \mod 4 \end{cases}$$

as is mentioned above. Hence we obtain

$$G_{(\tilde{P},\tilde{Q})}(\mathbb{Z}_{(2)})/G_{(P,Q)}(\mathbb{Z}_{(2)}) = \begin{cases} G_{(\tilde{P},\tilde{Q})}(\mathbb{Z}/2^r\mathbb{Z}) & \text{if } \tilde{D} \equiv 1 \mod 4 \\ G_{(\tilde{P},\tilde{Q})}(\mathbb{Z}/2^{r-1}\mathbb{Z}) & \text{if } \tilde{D} \equiv 2,3 \mod 4 \end{cases}$$

as is remarked in 2.1.

These yield that the torsion part of $G_{P,Q}(\mathbb{Q})/G_{P,Q}(\mathbb{Z}_{(2)}) = G(f)/K(f,2)$ coincides with $U_{\tilde{P},\tilde{Q}}(\mathbb{Z}_{(2)})/G_{P,Q}(\mathbb{Z}_{(2)})$.

Now we prove the assertion (1). Under the identifications

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

we have

$$G_{(P,Q)}(\mathbb{Z}_{(2)}) = \{\boldsymbol{w} = (w_k)_{k\geq 0} \in \mathcal{R}(f,\mathbb{Z}) \ ; \ \Delta(\boldsymbol{w}) \equiv 1 \mod 2\}$$

and, by Lemma 1.9,

$$\begin{aligned} G_{(2^nP,4^nQ)}(\mathbb{Z}_{(2)}) &= \mathrm{Ker}[G_{(P,Q)}(\mathbb{Z}_{(2)}) \to G_{(P,Q)}(\mathbb{Z}/2^n\mathbb{Z})] \\ &= \{(w_k)_{k\geq 0} \in \mathcal{R}(f,\mathbb{Z}) \ ; \ w_0 \equiv 0 \mod 2^n\}. \end{aligned}$$

It follows that the isomorphism $\omega : G_{(P,Q)}(\mathbb{Q})/\Theta \xrightarrow{\sim} G(f)$ induces isomorphisms

$$G_{(P,Q)}(\mathbb{Z}_{(2)})/\Theta \xrightarrow{\sim} K(f,2)$$

and

$$(G_{(2^nP,4^nQ)}(\mathbb{Z}_{(2)}) + \Theta)/\Theta \xrightarrow{\sim} G(f,2^n)$$

for each $n > 0$.

Next we prove the assertion (2). Combining the isomorphisms

$$G_{(P,Q)}(\mathbb{Z}_{(2)})/\Theta \xrightarrow{\sim} K(f,2)$$

and

$$(G_{(2^nP,4^nQ)}(\mathbb{Z}_{(2)})+\Theta)/\Theta \xrightarrow{\sim} G(f,2^n),$$

we obtain an isomorphism

$$G_{(P,Q)}(\mathbb{Z}_{(2)})/(G_{(2^nP,4^nQ)}(\mathbb{Z}_{(2)})+\Theta) \xrightarrow{\sim} K(f,2)/G(f,2^n).$$

Furthemore, using the isomorphism

$$\mathrm{Coker}[\underline{2^n}: G_{(2^nP,4^nQ)}(\mathbb{Z}_{(2)}) \to G_{(P,Q)}(\mathbb{Z}_{(2)})] \xrightarrow{\sim} G_{(P,Q)}(\mathbb{Z}/2^n\mathbb{Z}),$$

established by Lemma 1.9 and 2.1(2), we obtain an isomorphism

$$G_{(P,Q)}(\mathbb{Z}/2^n\mathbb{Z})/\Theta \xrightarrow{\sim} K(f,2)/G(f,2^n).$$

In particular, $K(f,2)/G(f,2)$ is isomorphic to $G_{(P,Q)}(\mathbb{Z}/2\mathbb{Z})/\Theta$. Note now that, by Propositions 2.15, 2.16 and 2.22, we have $|G_{(P,Q)}(\mathbb{Z}/2\mathbb{Z})| = 2$ or 3 and that $\beta(\theta) = (0,1/Q)$ is not trivial in $G_{(P,Q)}(\mathbb{Z}/2\mathbb{Z})$. These imply that $G_{(P,Q)}(\mathbb{Z}/2\mathbb{Z})/\Theta = 0$ and therefore $K(f,2) = G(f,2)$.

The assertion (3) is a standard fact. Indeed, it is sufficient to notice the canonical isomorphism

$$(K(f,2)/G(f,2^{n+1}))/(G(f,2^n)/G(f,2^{n+1})) \xrightarrow{\sim} K(f,2)/G(f,2^n).$$

**Corollary 4.3.1.** *Let $P, Q \in \mathbb{Z}$ with $P \equiv 1 \mod 2$, $Q \equiv 1 \mod 2$ and $D = P^2 - 4Q \neq 0$. Then:*

(1) *We have $G(f) = H(f,2) = K(f,2)$.*

(2) *Put*

$$\nu = \begin{cases} \mathrm{ord}_2(P^2-Q) & \text{if } Q \equiv 1 \mod 4 \\ \mathrm{ord}_2(P^2-Q)(P^2-3Q) & \text{if } Q \equiv -1 \mod 4 \end{cases}.$$

*Then:*

(a) *If $Q \equiv 5 \mod 8$, then we have $\nu = 2$ and*

$$K(f,2)/G(f,2^n) = \begin{cases} 0 & \text{if } n = 1 \\ \mathbb{Z}/2\mathbb{Z} & \text{if } n \geq 2 \end{cases}.$$

(b1) *If $Q \equiv 1 \mod 8$ and $P^2 - Q \neq 0$, then we have $\nu \geq 3$ and*

$$K(f,2)/G(f,2^n) = \begin{cases} 0 & \text{if } n = 1 \\ \mathbb{Z}/2\mathbb{Z} & \text{if } n = 2 \\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{n-2}\mathbb{Z} & \text{if } 3 \leq n \leq \nu \\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{\nu-2}\mathbb{Z} & \text{if } n \geq \nu + 1 \end{cases}.$$

(b2) *If $P^2 - Q = 0$, then we have*

$$K(f,2)/G(f,2^n) = \begin{cases} 0 & \text{if } n = 1 \\ \mathbb{Z}/2\mathbb{Z} & \text{if } n = 2 \\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{n-2}\mathbb{Z} & \text{if } n \geq 3 \end{cases} \cdot$$

(c1) *If $Q \equiv -1 \mod 4$ and $P^2 - 3Q \neq 0$, then we have $\nu \geq 3$ and*

$$K(f,2)/G(f,2^n) = \begin{cases} 0 & \text{if } n = 1,2 \\ \mathbb{Z}/2^{n-2}\mathbb{Z} & \text{if } 3 \leq n \leq \nu \\ \mathbb{Z}/2^{\nu-2}\mathbb{Z} & \text{if } n \geq \nu + 1 \end{cases} \cdot$$

(c2) *If $P^2 - 3Q = 0$, then we have*

$$K(f,2)/G(f,2^n) = \begin{cases} 0 & \text{if } n = 1,2 \\ \mathbb{Z}/2^{n-2}\mathbb{Z} & \text{if } n \geq 3 \end{cases}.$$

(3) *If $Q \equiv 1 \mod 4$, then we have $|G(f,2^n)/G(f,2^{n+1})| = 2$ for $1 \leq n < \nu$, and $G(f,2^n) = G(f,2^\nu)$ for $n \geq \nu$. On the other hand, if $Q \equiv -1 \mod 4$, then we have $|G(f,2^n)/G(f,2^{n+1})| = 2$ for $2 \leq n < \nu$, and $G(f,2^n) = G(f,2^\nu)$ for $n \geq \nu$ and $n = 1$.*

**Proof.** First we prove the assertion (1). We have $U_{P,Q}(\mathbb{Q}) = U_{P,Q}(\mathbb{Z}_{(2)})$ by Proposition 2.2(1), and $U_{P,Q}(\mathbb{Z}_{(2)}) = G_{(P,Q)}(\mathbb{Z}_{(2)})$ since $\alpha : G_{(P,Q)}(\mathbb{Z}_{(2)}) \to U_{P,Q}$ is isomorphic. Hence the result.

Now we prove the assertion (2) in each case.

(a) By the assumption, we obtain $D \equiv 5 \mod 8$ and $P^2 - Q \equiv 4 \mod 8$, i.e. $\mathrm{ord}_2(P^2 - Q) = 2$. Hence, by Theorem 3.10, we have

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

Furthermore, by Corollary 2.22, we have

$$|G_{(P,Q)}(\mathbb{Z}/2^n\mathbb{Z})| = \begin{cases} 3 & \text{if } n = 1 \\ 3 \times 2^{n-1} & \text{if } n \geq 2 \end{cases}.$$

These imply

$$|G_{(P,Q)}(\mathbb{Z}/2^n\mathbb{Z})/\Theta| = \begin{cases} 0 & \text{if } n = 1 \\ 2 & \text{if } n \geq 2 \end{cases}.$$

(b1) By the assumption $Q \equiv 1 \mod 8$, we obtain $D \equiv 5 \mod 8$ and $P^2 - Q \equiv 0 \mod 8$, i.e. $\mathrm{ord}_2(P^2 - Q) \geq 3$. Hence, for $n \geq 3$, we have a decompsition

$$U_{P,Q}(\mathbb{Z}/2^n\mathbb{Z}) = \{\pm 1, \pm\omega, \pm\omega^2\} \times (\text{the subgroup generated by } \gamma(1 + 4\omega)) = \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/2^{n-2}\mathbb{Z},$$

as is shown in the proof of Corollary 2.22. On the other hand, $\nu < \infty$ since $P^2 - Q \neq 0$. Therefore, for $n \geq 3$, we have a decompsition

$$\text{the image of } \Theta \text{ in } U_{P,Q}(\mathbb{Z}/2^n\mathbb{Z}) = \{1, \omega, \omega^2\} \times (\text{the subgroup generated by } \gamma(1+4\omega)^{2^{\nu-2}}),$$

as is shown in the proof of Theorem 3.12. These imply

$$U_{P,Q}(\mathbb{Z}/2^n\mathbb{Z})/\Theta = \begin{cases} 0 & \text{if } n = 1 \\ \mathbb{Z}/2\mathbb{Z} & \text{if } n = 2 \\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{n-2}\mathbb{Z} & \text{if } 3 \leq n \leq \nu \\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{\nu-2}\mathbb{Z} & \text{if } n \geq \nu + 1 \end{cases}.$$

Therefore we obtain the result since the homomorphism $\alpha : G_{(P,Q)} \to U_{P,Q}$ is isomorphic.

(b2) By the assumption, we have

$$\Theta = \{1, \omega, \omega^2\} \subset U_{P,Q}(\mathbb{Z}_{(2)})$$

This implies

$$U_{P,Q}(\mathbb{Z}/2^n\mathbb{Z})/\Theta = \begin{cases} 0 & \text{if } n = 1 \\ \mathbb{Z}/2\mathbb{Z} & \text{if } n = 2 \\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{n-2}\mathbb{Z} & \text{if } n \geq 3 \end{cases} \cdot$$

(c1) By the assumption $Q \equiv -1 \mod 4$, we obtain $D \equiv 5 \mod 8$ and $P^2 - Q \equiv 2 \mod 4$, $P^2 - 3Q \equiv 0 \mod 4$, i.e. $\mathrm{ord}_2(P^2 - Q)(P^2 - 3Q) \geq 3$. Hence, for $n \geq 3$, we have a decompsition

$$U_{P,Q}(\mathbb{Z}/2^n\mathbb{Z}) = \{\pm 1, \pm\omega, \pm\omega^2\} \times (\text{the subgroup generated by } \gamma(1+4\omega)) = \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/2^{n-2}\mathbb{Z},$$

as is shown in the proof of Corollary 2.22. On the other hand, $\nu < \infty$ since $P^2 - 3Q \neq 0$. Therefore, for $n \geq 3$, we have a decompsition

$$\text{the image of } \Theta \text{ in } U_{P,Q}(\mathbb{Z}/2^n\mathbb{Z}) = \{\pm 1, \pm\omega, \pm\omega^2\} \times (\text{the subgroup generated by } \gamma(1+4\omega)^{2^{\nu-2}}),$$

as is shown in the proof of Theorem 3.13. These imply

$$U_{P,Q}(\mathbb{Z}/2^n\mathbb{Z})/\Theta = \begin{cases} 0 & \text{if } n = 1, 2 \\ \mathbb{Z}/2^{n-2}\mathbb{Z} & \text{if } 3 \leq n \leq \nu \\ \mathbb{Z}/2^{\nu-2}\mathbb{Z} & \text{if } n \geq \nu + 1 \end{cases} \cdot$$

(c2) By the assumption, we have

$$\Theta = \{\pm 1, \pm\omega, \pm\omega^2\} \subset U_{P,Q}(\mathbb{Z}_{(2)})$$

This implies

$$U_{P,Q}(\mathbb{Z}/2^n\mathbb{Z})/\Theta = \begin{cases} 0 & \text{if } n = 1, 2 \\ \mathbb{Z}/2^{n-2}\mathbb{Z} & \text{if } n \geq 3 \end{cases}.$$

The assertion (3) is a direct consequence of (2).

**Corollary 4.3.2.** *Let $P, Q \in \mathbb{Z}$ with $P \equiv 0 \mod 4$, $Q \equiv 1 \mod 2$ or $P \equiv 2 \mod 4$, $Q \equiv -1 \mod 4$. Then we have $r = [(\mathrm{ord}_2 D)/2] = 1$. Furthermore:*
(1) *We have*

$$G(f)/H(f,2) = \begin{cases} \mathbb{Z} & \text{if } (P,Q) \equiv (0,-1),(4,-5) \mod 8 \\ 0 & \text{otherwise} \end{cases}$$

*and*

$$H(f,2)/K(f,2) = \begin{cases} 0 & \text{if } (P,Q) \equiv (0,-1),(4,-5) \mod 8 \\ \mathbb{Z}/3\mathbb{Z} & \text{if } (P,Q) \equiv (0,-5),(4,-1) \mod 8 \\ \mathbb{Z}/2\mathbb{Z} & \text{if } (P,Q) \equiv (0,1),(2,-1) \mod 4 \end{cases} \cdot$$

(2) *Assume $P \neq 0$, and put $\nu = \mathrm{ord}_2 P$.*
(a) *If $\nu = 1$, then we have $K(f,2)/G(f,2^n) = 0$ for any $n \geq 1$.*
(b) *If $\nu \geq 2$, then we have*

$$K(f,2)/G(f,2^n) = \begin{cases} 0 & \text{if } n = 1 \\ \mathbb{Z}/2^{n-1}\mathbb{Z} & \text{if } 2 \leq n \leq \nu \\ \mathbb{Z}/2^{\nu-1}\mathbb{Z} & \text{if } n \geq \nu + 1 \end{cases} \cdot$$

(3) *We have $|G(f,2^n)/G(f,2^{n+1})| = 2$ for $1 \leq n < \nu$, and $G(f,2^n) = G(f,2^\nu)$ for $n \geq \nu$.*

**Proof.** First note the implications

$$P \equiv 0 \mod 4 \Rightarrow D/4 \equiv -Q \mod 4,$$
$$P \equiv 2 \mod 4 \Rightarrow D/4 \equiv 1 - Q \mod 4.$$

Hence the assumption on $P$ and $Q$ implies that $[(\mathrm{ord}_2 D)/2] = 1$. Moreover, $G_{(P,Q)}$ is isomorphic to $G_{(D/4)}$, as is remarked in 2.19.

We begin with a verification of the assertion (2). We have $|G_{(D/4)}(\mathbb{Z}/2^n\mathbb{Z})| = 2^n$ by Propositions 2.15 and 2.16, and

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

by Theorem 3.7. Hence we obtain

$$|K(f,2)/G(f,2^n)| = |G_{(D/4)}(\mathbb{Z}/2^n\mathbb{Z})/\Theta| = \begin{cases} 1 & \text{if } n = 1 \\ 2^{n-1} & \text{if } 2 \leq n \leq \nu \\ 2^{\nu-1} & \text{if } n \geq \nu + 1 \end{cases} \cdot$$

Note now that the surjective homomorphism

$$\omega : G_{(D)}(\mathbb{Z}_{(2)}) = \mathrm{Ker}[G_{(D/4)}(\mathbb{Z}_{(2)}) \to G_{(D/4)}(\mathbb{Z}/2\mathbb{Z})] \to G(f,2)$$

induces a surjection

$$\operatorname{Ker}[G_{(D/4)}(\mathbb{Z}/2^n\mathbb{Z}) \to G_{(D/4)}(\mathbb{Z}/2\mathbb{Z})] \to G(f,2)/G(f,2^n) = K(f,2)/G(f,2^n).$$

Therefore, $K(f,2)/G(f,2^n)$ is cyclic since $\operatorname{Ker}[G_{(D/4)}(\mathbb{Z}/2^n\mathbb{Z}) \to G_{(D/4)}(\mathbb{Z}/2\mathbb{Z})]$ is cyclic, as is remarked in 2.17. Hence the result.

Now we verify the assertions (1) case by case.

(a) $P \equiv 2 \mod 4$, $Q \equiv -1 \mod 4$, or $P \equiv 0 \mod 4$, $Q \equiv 1 \mod 4$. In this case, we have $\tilde{D} = D/4 \equiv 2, 3 \mod 4$. Hence, by the definition of $\tilde{P}$ and $\tilde{Q}$, we have $U_{\tilde{P},\tilde{Q}} = U_{D/4}$ and $G_{(\tilde{P},\tilde{Q})} = G_{(D/4)}$. Therefore, we obtain $U_{P,Q}(\mathbb{Q}) = U_{P,Q}(\mathbb{Z}_{(2)})$ by Proposition 2.2(3), and $|U_{P,Q}(\mathbb{Z}_{(2)})/G_{(P,Q)}(\mathbb{Z}_{(2)})| = 2$ by Proposition 2.3. Hence the result.

(b) $P \equiv 0 \mod 4$, $Q \equiv -1 \mod 4$, $P \neq 0$. In this case, $\tilde{D} = D/4 \equiv 1 \mod 4$. We have also implications

$$P \equiv 0 \mod 8,\ Q \equiv -1 \mod 8, \text{ or } P \equiv 4 \mod 8,\ Q \equiv -5 \mod 8 \Rightarrow D/4 \equiv 1 \mod 8,$$
$$P \equiv 0 \mod 8,\ Q \equiv -5 \mod 8, \text{ or } P \equiv 4 \mod 8,\ Q \equiv -1 \mod 8 \Rightarrow D/4 \equiv 5 \mod 8.$$

Moreover, there exist isomorphisms $U_{2\tilde{P},4\tilde{Q}} \xrightarrow{\sim} U_{D/4} \xrightarrow{\sim} U_{P,Q}$ and $G_{(2\tilde{P},4\tilde{Q})} \xrightarrow{\sim} G_{(D/4)} \xrightarrow{\sim} G_{(P,Q)}$ as is remarked in the proof of Corollary 4.3. Therefore, we have

$$U_{P,Q}(\mathbb{Q})/U_{\tilde{P},\tilde{Q}}(\mathbb{Z}_{(2)}) = U_{\tilde{P},\tilde{Q}}(\mathbb{Q})/U_{\tilde{P},\tilde{Q}}(\mathbb{Z}_{(2)}) = \begin{cases} \mathbb{Z} & \text{if } (P,Q) \equiv (0,-1),(4,-5) \mod 8 \\ 0 & \text{if } (P,Q) \equiv (0,-5),(4,-1) \mod 8 \end{cases}$$

by Proposition 2.2(1)(2), and

$$\begin{aligned} U_{\tilde{P},\tilde{Q}}(\mathbb{Z}_{(2)})/G_{(P,Q)}(\mathbb{Z}_{(2)}) &= G_{(\tilde{P},\tilde{Q})}(\mathbb{Z}_{(2)})/G_{(2\tilde{P},4\tilde{Q})}(\mathbb{Z}_{(2)}) \\ &= \begin{cases} 0 & \text{if } (P,Q) \equiv (0,-1),(4,-5) \mod 8 \\ \mathbb{Z}/3\mathbb{Z} & \text{if } (P,Q) \equiv (0,-5),(4,-1) \mod 8 \end{cases} \end{aligned}$$

by Corollary 2.22. Hence the result.

**Remark 4.3.3.** If $P = 0$ and $Q \equiv 1 \mod 2$, then we have

$$|K(f,2)/G(f,2^n)| = \begin{cases} 1 & \text{if } n = 1 \\ 2^{n-1} & \text{if } n \geq 2 \end{cases}.$$

**Corollary 4.3.4.** *Let $P, Q \in \mathbb{Z}$ with $P \equiv 2 \mod 4$, $Q \equiv 1 \mod 4$. Then we have $r = [(\operatorname{ord}_2 D)/2] \geq 2$. Furthermore:*

(1) *We have*

$$G(f)/H(f,2) = \begin{cases} \mathbb{Z} & \text{if } \tilde{D} \equiv 1 \mod 8 \\ 0 & \text{otherwise} \end{cases}$$

*and*

$$H(f,2)/K(f,2) = \begin{cases} \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{r-1}\mathbb{Z} & \text{if } \tilde{D} \equiv 0 \mod 2 \text{ or } \tilde{D} \equiv -5 \mod 8 \\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{r-2}\mathbb{Z} & \text{if } \tilde{D} \equiv 1 \mod 8 \\ \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/2^{r-2}\mathbb{Z} & \text{if } \tilde{D} \equiv 5 \mod 8 \\ \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2^{r-2}\mathbb{Z} & \text{if } \tilde{D} \equiv -1 \mod 8 \end{cases}.$$

(2) *We have* $G(f,2^n) = K(f,2)$ *for* $n \geq 1$.

**Proof.** First note that the assumption $P \equiv 2 \mod 4$ and $Q \equiv 1 \mod 4$ implies $P^2 - 4Q \equiv 4 - 4Q \equiv 0 \mod 16$. Hence we obtain $[(\mathrm{ord}_2 D)/2] \geq 2$.

We verify now the assertion (1). There exist isomorphisms $U_{2^r\tilde{P},4\tilde{Q}} \overset{\sim}{\to} U_{4^{r-1}\tilde{D}} \overset{\sim}{\to} U_{P,Q}$ and $G_{(2^r\tilde{P},4^r\tilde{Q})} \overset{\sim}{\to} G_{(4^{r-1}D)} \overset{\sim}{\to} G_{(P,Q)}$ if $\tilde{D} \equiv 1 \mod 4$, and there exist isomorphisms $U_{2^{r-1}\tilde{P},4^{r-1}\tilde{Q}} \overset{\sim}{\to} U_{4^{r-1}\tilde{D}} \overset{\sim}{\to} U_{P,Q}$ and $G_{(2^{r-1}\tilde{P},4^{r-1}\tilde{Q})} \overset{\sim}{\to} G_{(4^{r-1}D)} \overset{\sim}{\to} G_{(P,Q)}$ if $\tilde{D} \equiv 2,3 \mod 4$, as is remarked in the proof of Corollary 4.3. Therefore, we have

$$H(f,2)/K(f,2) = U_{\tilde{P},\tilde{Q}}(\mathbb{Q})/U_{\tilde{P},\tilde{Q}}(\mathbb{Z}_{(2)}) = \begin{cases} \mathbb{Z} & \text{if } (P,Q) \equiv (0,-1),(4,-5) \mod 8 \\ 0 & \text{if } (P,Q) \equiv (0,-5),(4,-1) \mod 8 \end{cases}$$

by Proposition 2.2(1)(2).

Furthermore, if $\tilde{D} \equiv 1 \mod 4$, then we have $G_{(P,Q)}(\mathbb{Z}_{(2)}) = G_{(2^r\tilde{P},4^r\tilde{Q})}(\mathbb{Z}_{(2)})$. Hence we obtain isomorphisms

$$H(f,2)/K(f,2) \overset{\sim}{\longleftarrow} G_{(\tilde{P},\tilde{Q})}(\mathbb{Z}_{(2)})/G_{(2^r\tilde{P},4^r\tilde{Q})}(\mathbb{Z}_{(2)}) \overset{\sim}{\longrightarrow} G_{(\tilde{P},\tilde{Q})}(\mathbb{Z}/2^r\mathbb{Z}).$$

Now we have

$$G_{(\tilde{P},\tilde{Q})}(\mathbb{Z}/2^r\mathbb{Z}) = \begin{cases} \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{r-2}\mathbb{Z} & \text{if } \tilde{D} \equiv 1 \mod 8 \\ \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/2^{r-2}\mathbb{Z} & \text{if } \tilde{D} \equiv 5 \mod 8 \end{cases}$$

by Corollary 2.22.

On the other hand, if $\tilde{D} \equiv 2,3 \mod 4$, then we have $G_{(P,Q)}(\mathbb{Z}_{(2)}) = G_{(2^{r-1}\tilde{P},4^{r-1}r\tilde{Q})}(\mathbb{Z}_{(2)})$. Hence we obtain isomorphisms

$$K(f,2)/G(f,2^n) \overset{\sim}{\longleftarrow} G_{(\tilde{P},\tilde{Q})}(\mathbb{Z}_{(2)})/G_{(2^{r-1}\tilde{P},4^{r-1}\tilde{Q})}(\mathbb{Z}_{(2)}) \overset{\sim}{\longrightarrow} G_{(\tilde{P},\tilde{Q})}(\mathbb{Z}/2^{r-1}\mathbb{Z}).$$

Now we have

$$G_{(\tilde{P},\tilde{Q})}(\mathbb{Z}/2^{r-1}\mathbb{Z}) = \begin{cases} \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{r-1}\mathbb{Z} & \text{if } \tilde{D} \equiv 0 \mod 2 \text{ or } \tilde{D} \equiv -5 \mod 8 \\ \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2^{r-2}\mathbb{Z} & \text{if } \tilde{D} \equiv -1 \mod 8 \end{cases}$$

by Remark 2.18.

Finally we verify the assertion (2). By Theorem 3.7, we have $r(2^n) = 2^n$ for $n \geq 1$. This means that $\beta(\theta)$ generates $G_{(P,Q)}(\mathbb{Z}_{(2)})/G_{(2^nP,4^nQ)}(\mathbb{Z}_{(2)}) = G_{(P,Q)}(\mathbb{Z}/2^n) = \mathbb{Z}/2^n$. Hence the result.

**Remark 4.4.** Laxton established in [8]:

(1) the assertion $G(f) = H(f,2)$ mentioned in Corollay 4.3.1 as [8, Theorem 3.7. (a)]. (When $p = 2$, the condition $m = p + 1$ is equivalent to the condition $P \equiv 1 \mod 2$, $Q \equiv 1 \mod 2$. Here $m$ denotes the maximal rank of $p$ in $G(f)$, defined by Laxton [8, p.728].)
(2) the assertion $K(f) = G(f,2)$ mentioned in Corollay 4.3 as [8, Theorem 3.7 (a)(c)]. (When $p = 2$, the condition $m = p$ is equivalent to the condition $P \equiv 0 \mod 2$, $Q \equiv 1 \mod 2$.)
(3) Corollary 4.3.1 (3), Corollary 4.3.2 (3) and Corollary 4.3.4 (2) as [8, Theorem 3.10 (a)(c)].

It would be kind to correct a statement in [8].
(1) [8, Theorem 3.7 (c)] $G(f) = H(f,2)$ if $P \equiv 0 \mod 2$ and $Q \equiv 1 \mod 2$. The assertion is false if $\tilde{D} \equiv 1 \mod 8$. Indeed, we have $G(f)/H(f,p) = \mathbb{Z}$ in this case as is shown in Corollaries 4.3.2 and 4.3,4.

**Corollary 4.5.** *Let $P, Q \in \mathbb{Z}$ with $P \equiv 1 \mod 2$ and $Q \equiv 0 \mod 2$. Assume that $Q \neq 0$. Then we have $G_{(P,Q)}(\mathbb{Z}_{(2)}) \cap \Theta = \{1\}$, and the descending chain of subgroups of $U_{P,Q}(\mathbb{Q}) = G_{(P,Q)}(\mathbb{Q})$:*

$$G_{(P,Q)}(\mathbb{Q}) \supset G_{(P,Q)}(\mathbb{Z}_{(2)}) = G_{(2P,4Q)}(\mathbb{Z}_{(2)}) \supset G_{(2^2P,4^2Q)}(\mathbb{Z}_{(2)}) \supset \cdots \supset G_{(2^nP,4^nQ)}(\mathbb{Z}_{(2)}) \supset \cdots$$

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

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

*More precisely,*
*(1) The isomorphism $\omega : G_{(P,Q)}(\mathbb{Q})/\Theta \xrightarrow{\sim} G(f)$ induces isomorphisms*

$$(G_{(P,Q)}(\mathbb{Z}_{(2)}) + \Theta)/\Theta \xrightarrow{\sim} K(f,p)$$

*and*

$$(G_{(2^nP,4^nQ)}(\mathbb{Z}_{(2)}) + \Theta)/\Theta \xrightarrow{\sim} G(f,2^n)$$

*for each $n > 0$. Therefore, $K(f,2)$ is isomorphic to $G_{(P,Q)}(\mathbb{Z}_{(2)})$, and $G(f,2^n)$ is isomorphic to $G_{(2^nP,4^nQ)}(\mathbb{Z}_{(2)})$ for each $n > 0$.*
*(2) The isomorphism $\omega : G_{(P,Q)}(\mathbb{Q})/\Theta \xrightarrow{\sim} G(f)$ induces isomorphisms*

$$U_{P,Q}(\mathbb{Q})/(G_{(P,Q)}(\mathbb{Z}_{(2)}) + \Theta) \xrightarrow{\sim} H(f,2)/K(f,2)$$

*and*

$$G_{(P,Q)}(\mathbb{Z}_{(2)})/G_{(2^nP,4^nQ)}(\mathbb{Z}_{(2)}) \xrightarrow{\sim} K(f,2)/G(f,2^n)$$

*for each $n \geq 1$. Therefore, $K(f,2)/G(f,2)$ is isomorphic to $G_{(P,Q)}(\mathbb{Z}/2\mathbb{Z}) = \mathbb{Z}/2\mathbb{Z}$, and $K(f,p)/G(f,2^n)$ is isomorphic to $G_{(P,Q)}(\mathbb{Z}/2^n\mathbb{Z}) = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{n-1}\mathbb{Z}$ for $n \geq 2$.*
*(3) $G(f)/K(f,2)$ is cyclic of order* $\mathrm{ord}_2 Q$. *Therefore, we have $G(f) = H(f,2)$.*
*(4) We have $|G(f,2^n)/G(f,2^{n+1})| = 2$ for $n \geq 1$.*

**Proof.** The assumption $P \equiv 1 \mod 2$ and $Q \equiv 0 \mod 2$ implies $D = P^2 - 4Q \equiv 1 \mod 8$, Hence, by Proposition 2.2(1), $G_{(P,Q)}(\mathbb{Q})/G_{(P,Q)}(\mathbb{Z}_{(2)})$ is isomorphic to $\mathbb{Z}$. On the other hand, we have $\beta(\theta) \notin G_{(P,Q)}(\mathbb{Z}_{(2)})$ since $\beta(\theta) = (0, 1/Q)$ and $\mathrm{ord}_2(1/Q) < 0$. It follows that $G_{(P,Q)}(\mathbb{Z}_{(2)}) \cap \Theta = \{1\} \subset G_{(P,Q)}(\mathbb{Q})$.

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

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

we have

$$G_{(P,Q)}(\mathbb{Z}_{(2)}) = \{\boldsymbol{w} = (w_k)_{k \geq 0} \in \mathcal{R}(f, \mathbb{Z}) \ ; \ \Delta(\boldsymbol{w}) \equiv 1 \mod 2\}$$

and

$$\begin{aligned} G_{(2^nP,4^nQ)}(\mathbb{Z}_{(2)}) &= \mathrm{Ker}[G_{(P,Q)}(\mathbb{Z}_{(p)}) \to G_{(P,Q)}(\mathbb{Z}/2^n\mathbb{Z})] \\ &= \{(w_k)_{k \geq 0} \in \mathcal{R}(f, \mathbb{Z}) \ ; \ w_0 \equiv 0 \mod p^n\}. \end{aligned}$$

It follows that the isomorphism $\omega : G_{(P,Q)}(\mathbb{Q})/\Theta \xrightarrow{\sim} G(f)$ induces isomorphisms

$$G_{(P,Q)}(\mathbb{Z}_{(2)}) \xrightarrow{\sim} (G_{(P,Q)}(\mathbb{Z}_{(2)}) + \Theta)/\Theta \xrightarrow{\sim} K(f, 2)$$

and

$$G_{(2^nP,4^nQ)}(\mathbb{Z}_{(2)}) \xrightarrow{\sim} (G_{(2^nP,4^nQ)}(\mathbb{Z}_{(2)}) + \Theta)/\Theta \xrightarrow{\sim} G(f, 2^n)$$

for each $n \geq 1$.

The assertion (2) is a direct consequence of (1). Moreover, the fact $D \equiv 1 \mod 8$ implies $G_{(P,Q)}(\mathbb{Z}_{(2)}) = G_{(2P,4Q)}(\mathbb{Z}_{(2)})$ as is remarked in 2.19, and $G_{(2^{n+1}P,4^{n+1}Q)}$ is isomorphic to $G_{(4^nD)}$ for $n \geq 0$ as is remarked in 1.6.1. Therefore we obtain the last assertion by Proposition 2.16.

Finally we prove the assertion (3). It is sufficient to verify that $G_{(P,Q)}(\mathbb{Q})/(G_{(P,Q)}(\mathbb{Z}_{(2)}) + \Theta) = G(f, 2)/K(f, 2)$ 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 2. Then the map $\eta \mapsto \mathrm{ord}_\mathfrak{p}\eta$ induces an isomorphism $G_{(P,Q)}(\mathbb{Q})/G_{(P,Q)}(\mathbb{Z}_{(2)}) \xrightarrow{\sim} \mathbb{Z}$ by Prpposition 2.3(1). On the other hand, the subgroup $\Theta$ of $G_{(P,Q)}(\mathbb{Q})$ is generated by $\beta(\theta) = (0, 1/Q)$, where $\theta = (P + \sqrt{D})/2$. Note now $\theta + \bar{\theta} = P$ and $(P, 2) = 1$. 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 $G_{(P,Q)}(\mathbb{Q})/G_{(P,Q)}(\mathbb{Z}_{(2)}) \xrightarrow{\sim} \mathbb{Z}$. Furthermore, we have

$$\xi(\gamma(\theta)) = -1 + \frac{P}{Q}\frac{P + r}{2} = 1 + \frac{2r}{P - r}.$$

Note now $(P + r)/2 + (P - r)/2 = P$ and $(P, 2) = 1$. These imply that $\mathrm{ord}_2(P + r)/2 = 0$ or $\mathrm{ord}_2(P - r)/2 = 0$. On the other hand, we have $(P + r)(P - r)/4 = Q$, and therefore, $\mathrm{ord}_p(P + r)/2 + \mathrm{ord}_2(P - r) = \mathrm{ord}_2Q$. Hence we obtain $\mathrm{ord}_2\xi(\gamma(\theta)) = \pm\mathrm{ord}_2Q$.

**Corollary 4.6.** *Let $P, Q \in \mathbb{Z}$ with $P \equiv 2 \mod 4$, $Q \equiv 2 \mod 4$ and $P^2 - 2Q \neq 0$. Put $s = \operatorname{ord}_2(P^2 - 2Q)$. Then we have $s \geq 3$, and the descending chain of subgroups of $U_{P,Q}(\mathbb{Q}) = G_{(P,Q)}(\mathbb{Q})$:*

$$\begin{aligned} U_{P,Q}(\mathbb{Q}) = U_{P,Q}(\mathbb{Z}_{(2)}) \supset G_{(P,Q)}(\mathbb{Z}_{(2)}) \supset G_{(2P,4Q)}(\mathbb{Z}_{(2)}) \supset \cdots \\ \supset G_{(2^{s-1}P,4^{s-1}Q)}(\mathbb{Z}_{(2)}) \supset G_{(2^sP,4^sQ)}(\mathbb{Z}_{(2)}) \supset G_{(2^{s+1}P,4^{s+1}Q)}(\mathbb{Z}_{(2)}) \supset \cdots \end{aligned}$$

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

$$G(f) = H(f,2) = K(f,2) = G(f,2) \supset \cdots \supset G(f,2^{s-1}) = G(f,2^s) = G(f,2^{s+1}) = \cdots .$$

*More precisely, let $\Theta_1$ and $\Theta_2$ denote the subgroup of $\Theta$ generated by $\beta(\theta)^2$ and $\beta(\theta)^4$. Then we have $G_{(P,Q)}(\mathbb{Z}_{(2)}) \cap \Theta = \Theta_1$ and $G_{(2^nP,4^nQ)}(\mathbb{Z}_{(2)}) \cap \Theta = \Theta_2$ for $1 \leq n \leq s-1$. Therefore, the isomorphism $\omega : G_{(P,Q)}(\mathbb{Q})/\Theta \xrightarrow{\sim} G(f)$ induces isomorphisms*

$$G_{(P,Q)}(\mathbb{Z}_{(2)})/\Theta_1 \xrightarrow{\sim} G_{(P,Q)}(\mathbb{Z}_{(2)}) + \Theta)/\Theta \xrightarrow{\sim} K(f,p)$$

*and*

$$G_{(2^nP,4^n)}(\mathbb{Z}_{(2)})/\Theta_2 \xrightarrow{\sim} (G_{(2^nP,4^n)}(\mathbb{Z}_{(2)}) + \Theta)/\Theta \xrightarrow{\sim} G(f,2^n)$$

*for $1 \leq n \leq s-1$.*

**Proof.** Note first that the assumption $P \equiv 2 \mod 4$ and $Q \equiv 2 \mod 4$ implies

$$D \equiv 0 \mod 4, \ \frac{D}{4} = \Big(\frac{P}{2}\Big)^2 - Q \equiv -1 \mod 4$$

and

$$P^2 - 2Q \equiv 0 \mod 8.$$

Hence $U_{P,Q}$ is isomorphic to $U_{D/4}$, and $G_{(2^nP,4^nQ)}$ is isomorphic to $G_{(4^{n-1}D)}$ for $n \geq 0$ as is remarked in 1.6.1. Moreover we have $U_{P,Q}(\mathbb{Q}) = U_{P,Q}(\mathbb{Z}_{(2)})$ by Proposiiton 2.2(3), and $U_{P,Q}(\mathbb{Z}_{(2)})/G_{(P,Q)}(\mathbb{Z}_{(2)}) = U_{D/4}(\mathbb{Z}_{(2)})/G_{(D/4)}(\mathbb{Z}_{(2)})$ is isomorphic to $\mathbb{Z}/2\mathbb{Z}$ by Proposition 2.3.

Now we prove the last assertion. Noting

$$\theta^2 = -Q + P\theta, \ \frac{\theta}{\bar{\theta}} = \frac{\theta^2}{\operatorname{Nr}\theta} = \frac{-Q + p\theta}{Q}, \ \theta^4 = -Q(P^2 - Q) + P(P^2 - 2Q)\theta,$$

we obtain

$$\gamma(\theta) = \Big(-1, \frac{P}{Q}\Big) \text{ in } U_{P,Q}(\mathbb{Q}), \ \beta(\theta) = \Big(0, \frac{1}{Q}\Big) \text{ in } G_{(P,Q)}(\mathbb{Q}),$$

$$\beta(\theta)^2 = \Big(-\frac{P}{Q}, \frac{P^2}{Q^2}\Big) \text{ in } G_{(P,Q)}(\mathbb{Q}),$$

$$\beta(\theta)^4 = \Big(-\frac{P(P^2 - Q)(P^2 - 2Q)}{Q^3}, \frac{P^2(P^2 - 2Q)^2}{Q^4}\Big) \text{ in } G_{(P,Q)}(\mathbb{Q}).$$

These imply that

$$\gamma(\theta) \in U_{P,Q}(\mathbb{Z}_{(2)}),\ \beta(\theta) \notin G_{(P,Q)}(\mathbb{Z}_{(2)}),$$
$$\beta(\theta)^2 \in G_{(P,Q)}(\mathbb{Z}_{(2)}),\ \beta(\theta)^2 \notin \mathrm{Ker}[G_{(P,Q)}(\mathbb{Z}_{(2)}) \to G_{(P,Q)}(\mathbb{Z}/2\mathbb{Z})],$$
$$\beta(\theta)^4 \in \mathrm{Ker}[G_{(P,Q)}(\mathbb{Z}_{(2)}) \to G_{(P,Q)}(\mathbb{Z}/p^{s-1}\mathbb{Z})],\ \beta(\theta)^4 \notin \mathrm{Ker}[G_{(P,Q)}(\mathbb{Z}_{(2)}) \to G_{(P,Q)}(\mathbb{Z}/2^s\mathbb{Z})]$$

since

$$\mathrm{ord}_2\frac{1}{Q} = -1,\ \mathrm{ord}_2\frac{P}{Q} = 0,$$
$$\mathrm{ord}_2\frac{P(P^2-Q)(P^2-2Q)}{Q^3} = s-1 \geq 2,\ \frac{P^2(P^2-Q)^2}{Q^4} = 2(s-1) \geq 4.$$

Moreover, we have

$$U_{P,Q}(\mathbb{Z}_{(2)})/G_{(P,Q)}(\mathbb{Z}_{(2)}) = \mathbb{Z}/2\mathbb{Z},$$

and

$$G_{(P,Q)}(\mathbb{Z}_{(2)})/G_{(2P,4Q)}(\mathbb{Z}_{(2)}) = G_{(D/4)}(\mathbb{Z}_{(2)})/G_{(D)}(\mathbb{Z}_{(2)}) = \mathbb{Z}/2\mathbb{Z}$$

by Proposition 2.16,

$$G_{(2^{s-1}P,4^{s-1}Q)}(\mathbb{Z}_{(2)})/G_{(2^{s-1+n}P,4^{s-1+n}Q)}(\mathbb{Z}_{(2)}) = G_{(4^{s-2}D)}(\mathbb{Z}_{(2)})/G_{(4^{s-2+n}D)}(\mathbb{Z}_{(2)}) = \mathbb{Z}/2^n\mathbb{Z}$$

for $n \geq 1$ by Proposition 2.15. Hence we obtain

$$U_{P,Q}(\mathbb{Z}_{(2)}) = G_{(P,Q)}(\mathbb{Z}_{(2)}) + \Theta,$$
$$G_{(P,Q)}(\mathbb{Z}_{(2)}) \supset \Theta_1,\ G_{(P,Q)}(\mathbb{Z}_{(2)}) = G_{(2P,4Q)}(\mathbb{Z}_{(2)}) + \Theta_1,$$
$$G_{(2^{s-1}P,4^{s-1}Q)}(\mathbb{Z}_{(2)}) \supset \Theta_2,\ G_{(2^{s-1}P,4^{s-1}Q)}(\mathbb{Z}_{(2)}) = G_{(2^{s-1+n}P,4^{s-1+n}Q)}(\mathbb{Z}_{(2)}) + \Theta_2 \text{ for } n \geq 1,$$

and the results.

**Remark 4.6.1.** Let $P, Q \in \mathbb{Z}$ with $P \equiv 2 \mod 4$, $Q \equiv 2 \mod 4$ and $P^2 - 2Q = 0$. Then we have $\beta(\theta)^2 = (-P/Q, P^2/Q^2)$ and $\beta(\theta)^4 = (0,0)$ in $G_{(P,Q)}(\mathbb{Q})$. Hence $U_{P,Q}(\mathbb{Z}_{(2)})/G_{(2P,4Q)}(\mathbb{Z}_{(2)})$ is isomorphic to $\Theta$, and the exact sequence

$$0 \longrightarrow G_{(2P,4Q)}(\mathbb{Z}_{(2)}) \longrightarrow U_{P,Q}(\mathbb{Z}_{(2)}) \longrightarrow U_{P,Q}(\mathbb{Z}_{(2)})/G_{(2P,4Q)}(\mathbb{Z}_{(2)}) \longrightarrow 0$$

splits. Therefore, the descending chain of subgroups of $U_{P,Q}(\mathbb{Q}) = G_{(P,Q)}(\mathbb{Q})$:

$$U_{P,Q}(\mathbb{Q}) = U_{P,Q}(\mathbb{Z}_{(2)}) \supset G_{(P,Q)}(\mathbb{Z}_{(2)}) \supset G_{(2P,4Q)}(\mathbb{Z}_{(2)}) \supset \cdots \supset G_{(2^nP,4^nQ)}(\mathbb{Z}_{(2)}) \supset \cdots$$

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

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

More precisely, the isomorphism $\omega : G_{(P,Q)}(\mathbb{Q})/\Theta \xrightarrow{\sim} G(f)$ induces isomorphisms

$$(G_{(P,Q)}(\mathbb{Z}_{(2)}) + \Theta)/\Theta \xrightarrow{\sim} K(f,p)$$

and

$$G_{(2^nP,4^n)}(\mathbb{Z}_{(2)}) \overset{\sim}{\to} (G_{(2^nP,4^n)}(\mathbb{Z}_{(2)}) + \Theta)/\Theta \overset{\sim}{\to} G(f, 2^n)$$

for $n \geq 1$.

**Corollary 4.7.** *Let $P, Q \in \mathbb{Z}$ with $P \equiv 0 \mod 4$, $Q \equiv 2 \mod 4$ and $P \neq 0$. Put $s = \mathrm{ord}_2 P$. Then we have $s \geq 2$, and the descending chain of subgroups of $U_{P,Q}(\mathbb{Q}) = G_{(P,Q)}(\mathbb{Q})$:*

$$\begin{aligned} U_{P,Q}(\mathbb{Q}) = U_{P,Q}(\mathbb{Z}_{(2)}) \supset G_{(P,Q)}(\mathbb{Z}_{(2)}) \supset G_{(2P,4Q)}(\mathbb{Z}_{(2)}) \supset \cdots \\ \supset G_{(2^{s-1}P,4^{s-1}Q)}(\mathbb{Z}_{(2)}) \supset G_{(2^sP,4^sQ)}(\mathbb{Z}_{(2)}) \supset G_{(2^{s+1}P,4^{s+1}Q)}(\mathbb{Z}_{(2)}) \supset \cdots \end{aligned}$$

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

$$G(f) = H(f, 2) = K(f, 2) \supset G(f, 2) \supset \cdots \supset G(f, 2^{s-1}) = G(f, 2^s) = G(f, 2^{s+1}) = \cdots .$$

*More precisely, let $\Theta_1$ denote the subgroup of $\Theta$ generated by $\beta(\theta)^2$. Then, for $0 \leq n \leq s-1$, we have $G_{(2^nP,4^nQ)}(\mathbb{Z}_{(2)}) \cap \Theta = \Theta_1$. Therefore, the isomorphism $\omega : G_{(P,Q)}(\mathbb{Q})/\Theta \overset{\sim}{\to} G(f)$ induces isomorphisms*

$$G_{(P,Q)}(\mathbb{Z}_{(2)})/\Theta_1 \overset{\sim}{\to} G_{(P,Q)}(\mathbb{Z}_{(2)}) + \Theta)/\Theta \overset{\sim}{\to} K(f, p)$$

*and*

$$G_{(2^nP,4^n)}(\mathbb{Z}_{(2)})/\Theta_1 \overset{\sim}{\to} (G_{(2^nP,4^n)}(\mathbb{Z}_{(2)}) + \Theta)/\Theta \overset{\sim}{\to} G(f, 2^n)$$

*for $1 \leq n \leq s-1$.*

**Proof.** Note first that the assumption $P \equiv 0 \mod 4$ and $Q \equiv 2 \mod 4$ implies

$$D \equiv 0 \mod 4, \ \frac{D}{4} = \Big(\frac{P}{2}\Big)^2 - Q \equiv 2 \mod 4.$$

Hence $U_{P,Q}$ is isomorphic to $U_{D/4}$, and $G_{(2^nP,4^nQ)}$ is isomorphic to $G_{(4^{n-1}D)}$ for $n \geq 0$ as is remarked in 1.6.1. Moreover we have $U_{P,Q}(\mathbb{Q}) = U_{P,Q}(\mathbb{Z}_{(2)})$ by Proposiiton 2.2(3), and $U_{P,Q}(\mathbb{Z}_{(2)})/G_{(P,Q)}(\mathbb{Z}_{(2)}) = U_{D/4}(\mathbb{Z}_{(2)})/G_{(D/4)}(\mathbb{Z}_{(2)})$ is isomorphic to $\mathbb{Z}/2\mathbb{Z}$ by Proposition 2.3.

Note now that we have

$$\gamma(\theta) = \Big(-1, \frac{P}{Q}\Big) \text{ in } U_{P,Q}(\mathbb{Q}), \ \beta(\theta) = \Big(0, \frac{1}{Q}\Big) \text{ in } G_{(P,Q)}(\mathbb{Q}),$$

$$\beta(\theta)^2 = \Big(-\frac{P}{Q}, \frac{P^2}{Q^2}\Big) \text{ in } G_{(P,Q)}(\mathbb{Q}),$$

These imply that

$$\gamma(\theta) \in U_{P,Q}(\mathbb{Z}_{(2)}), \ \beta(\theta) \notin G_{(P,Q)}(\mathbb{Z}_{(2)}),$$

$$\beta(\theta)^2 \in \mathrm{Ker}[G_{(P,Q)}(\mathbb{Z}_{(2)}) \to G_{(P,Q)}(\mathbb{Z}/2^{s-1}\mathbb{Z})], \ \beta(\theta)^2 \notin \mathrm{Ker}[G_{(P,Q)}(\mathbb{Z}_{(2)}) \to G_{(P,Q)}(\mathbb{Z}/2^s\mathbb{Z})]$$

since

$$\mathrm{ord}_2\frac{1}{Q} = -1, \ \mathrm{ord}_2\frac{P}{Q} = s - 1 \geq 1, \ \mathrm{ord}_2\frac{P^2}{Q^2} = 2(s-1) \geq 2.$$

Moreover, we have

$$U_{P,Q}(\mathbb{Z}_{(2)})/G_{(P,Q)}(\mathbb{Z}_{(2)}) = \mathbb{Z}/2\mathbb{Z},$$

and

$$G_{(2^{s-1}P,4^{s-1}Q)}(\mathbb{Z}_{(2)})/G_{(2^{s-1+n}P,4^{s-1+n}Q)}(\mathbb{Z}_{(2)}) = G_{(4^{s-2}D)}(\mathbb{Z}_{(2)})/G_{(4^{s-2+n}D)}(\mathbb{Z}_{(2)}) = \mathbb{Z}/2^n\mathbb{Z}$$

for $n \geq 1$ by Proposition 2.15. Hence we obtain

$$U_{P,Q}(\mathbb{Z}_{(2)}) = G_{(P,Q)}(\mathbb{Z}_{(2)}) + \Theta,$$

$$G_{(2^{s-1}P,4^{s-1}Q)}(\mathbb{Z}_{(2)}) \supset \Theta_1,\ G_{(2^{s-1}P,4^{s-1}Q)}(\mathbb{Z}_{(2)}) = G_{(2^{s-1+n}P,4^{s-1+n}Q)}(\mathbb{Z}_{(2)}) + \Theta_1 \text{ for } n \geq 1,$$

and the results.

**Remark 4.7.1.** Let $Q \in \mathbb{Z}$ with $Q \equiv 2 \mod 4$, and put $P = 0$. Then we have $\beta(\theta)^2 = (0,0)$. Hence $U_{P,Q}(\mathbb{Z}_{(2)})/G_{(2P,4Q)}(\mathbb{Z}_{(2)})$ is isomorphic to $\Theta$, and the exact sequence

$$0 \longrightarrow G_{(P,Q)}(\mathbb{Z}_{(2)}) \longrightarrow U_{P,Q}(\mathbb{Z}_{(2)}) \longrightarrow U_{P,Q}(\mathbb{Z}_{(2)})/G_{(P,Q)}(\mathbb{Z}_{(2)}) \longrightarrow 0$$

splits. Therefore, the descending chain of subgroups of $U_{P,Q}(\mathbb{Q}) = G_{(P,Q)}(\mathbb{Q})$:

$$U_{P,Q}(\mathbb{Q}) = U_{P,Q}(\mathbb{Z}_{(2)}) \supset G_{(P,Q)}(\mathbb{Z}_{(2)}) \supset G_{(2P,4Q)}(\mathbb{Z}_{(2)}) \supset \cdots \supset G_{(2^nP,4^nQ)}(\mathbb{Z}_{(2)}) \supset \cdots$$

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

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

More precisely, the isomorphism $\omega : G_{(P,Q)}(\mathbb{Q})/\Theta \xrightarrow{\sim} G(f)$ induces isomorphisms

$$G_{(P,Q)}(\mathbb{Z}_{(2)}) \xrightarrow{\sim} (G_{(P,Q)}(\mathbb{Z}_{(2)}) + \Theta)/\Theta \xrightarrow{\sim} K(f,p)$$

and

$$G_{(2^nP,4^n)}(\mathbb{Z}_{(2)}) \xrightarrow{\sim} (G_{(2^nP,4^n)}(\mathbb{Z}_{(2)}) + \Theta)/\Theta \xrightarrow{\sim} G(f,2^n)$$

for $n \geq 1$.

**Remark 4.8.** Laxton established the assertions (3) and (4) of Corollary 4.5 as [8, Theorem 3.7 (d) and Theorem 3.10 (c)].

**4.9.** Here are a few numerical examples. For $\boldsymbol{w} = (w_k)_{k\geq 0} \in \mathcal{L}(f,Q)^\times$, we denote by $[w_0, w_1]$ the class of $\boldsymbol{w}$ in the Laxton group $G(f)$.

**Example 4.9.1.** $P = 1$, $Q = 5$. In this case, we have $D = -19$ and $\nu = \mathrm{ord}_2(P^2 - Q) = 2$. Therefore, Corollary 4.3.1 implies

$$G(f) = H(f,2) = K(f,2) = G(f,2) \supset G(f,2^2) = G(f,2^3) = \cdots .$$

Moreover, $K(f,2)/G(f,2^2) = G_{(P,Q)}(\mathbb{Z}/2^2\mathbb{Z})/\Theta = \mathbb{Z}/2\mathbb{Z}$ is generated by $[1,2]$, and we have

$$\omega(1+\theta) = (1,2),\ \beta(1+\theta) = \big(\frac{1}{7}, \frac{1}{7}\big),\ \gamma(1+\theta) = \frac{-4+3\theta}{7}.$$

**Example 4.9.2.** $P = 1$, $Q = 9$. In this case, we have $D = -35$ and $\nu = \mathrm{ord}_2(P^2 - Q) = 3$. Therefore, Corollary 4.3.1 implies

$$G(f) = H(f,2) = K(f,2) = G(f,2) \supset G(f,2^2) \supset G(f,2^3) = G(f,2^4) = \cdots .$$

Moreover, $K(f,2)/G(f,2^3) = G_{(P,Q)}(\mathbb{Z}/2^3\mathbb{Z})/\Theta = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} = \{[0,1],[1,3],[1,5],[1,7]\}$, and we have

$$\begin{aligned}
\omega(2+\theta) &= (1,3),\ \beta(1+\theta) = (\frac{2}{15},\frac{1}{15}),\ \gamma(2+\theta) = \frac{-1+\theta}{3},\\
\omega(4+\theta) &= (1,5),\ \beta(4+\theta) = (\frac{4}{29},\frac{1}{29}),\ \gamma(2+\theta) = \frac{7+9\theta}{29},\\
\omega(6+\theta) &= (1,7),\ \beta(6+\theta) = (\frac{6}{51},\frac{1}{51}),\ \gamma(6+\theta) = \frac{27+13\theta}{51}.
\end{aligned}$$

**Example 4.9.3.** $P = 1, Q = 3$. In this case, we have $D = -11$ and $\nu = \mathrm{ord}_2(P^2-Q)(P^2-3Q) = 4$. Therefore, Corollary 4.3.1 implies

$$G(f) = H(f,2) = K(f,2) = G(f,2) = G(f,2^2) \supset G(f,2^3) \supset G(f,2^4) = G(f,2^5) = \cdots$$

Moreover, $K(f,2)/G(f,2^4) = G_{(P,Q)}(\mathbb{Z}/2^4\mathbb{Z})/\Theta = \mathbb{Z}/4\mathbb{Z} = \{[0,1],[1,2],[1,6],[1,4]\}$ is generated by $[1,2]$, and we have

$$\begin{aligned}
\omega(1+\theta) &= (1,2),\ \beta(1+\theta) = (\frac{1}{5},\frac{1}{5}),\ \gamma(1+\theta) = \frac{-2+3\theta}{5},\\
\omega(5+\theta) &= (1,6),\ \beta(5+\theta) = (\frac{5}{33},\frac{1}{33}),\ \gamma(5+\theta) = \frac{2+\theta}{3},\\
\omega(3+\theta) &= (1,4),\ \beta(3+\theta) = (\frac{1}{5},\frac{1}{15}),\ \gamma(3+\theta) = \frac{6+7\theta}{15}.
\end{aligned}$$

**Example 4.9.4.** $P = 8$, $Q = 7$. In this case, we have $D = 36$, $r = 1$, $\tilde{D} = D/4 = 9$ and $\nu = \mathrm{ord}_2 P = 3$. Therefore, Corollary 4.3.2 implies

$$G(f) \supset H(f,2) = K(f,2) = G(f,2) \supset G(f,2^2) \supset G(f,2^3) = G(f,2^4) = \cdots .$$

Moreover, $K(f,2)/G(f,2^3) = G_{(P,Q)}(\mathbb{Z}/2^2\mathbb{Z})/\Theta = \mathbb{Z}/4\mathbb{Z} = \{[0,1],[1,2],[1,4],[1,6]\}$ is generated by $[1,2]$, and we have

$$\begin{aligned}
\omega(-6+\theta) &= (1,2),\ \beta(-6+\theta) = (\frac{6}{5},-\frac{1}{5}),\ \gamma(-6+\theta) = \frac{-29+4\theta}{5},\\
\omega(-4+\theta) &= (1,4),\ \beta(-4+\theta) = (\frac{4}{9},-\frac{1}{9}),\ \gamma(-4+\theta) = -1,\\
\omega(-2+\theta) &= (1,6),\ \beta(-2+\theta) = (\frac{2}{5},-\frac{1}{5}),\ \gamma(-2+\theta) = \frac{3-4\theta}{5}.
\end{aligned}$$

On the other hand, $H(f,2)/K(f,2) = \mathbb{Z}$ is generated by $[1,3]$, and we have

$$\omega(-5+\theta) = (1,3),\ \beta(-5+\theta) = (\frac{5}{8},-\frac{1}{8}),\ \gamma(-5+\theta) = \frac{-9+\theta}{4}.$$

**Example 4.9.5.** $P = 8$, $Q = 3$. In this case, we have $D = 52$, $r = 1$, $\tilde{D} = D/4 = 13$ and $\nu = \mathrm{ord}_2 P = 3$. Therefore, Corollary 4.3.2 implies

$$G(f) = H(f,2) \supset K(f,2) = G(f,2) \supset G(f,2^2) \supset G(f,2^3) = G(f,2^4) = \cdots .$$

Moreover, $K(f,2)/G(f,2^3) = G_{(P,Q)}(\mathbb{Z}/2^3\mathbb{Z})/\Theta = \mathbb{Z}/4\mathbb{Z} = \{[0,1],[1,2],[1,4],[1,6]\}$ is generated by $[1,2]$, and we have

$$\omega(-6+\theta) = (1,2),\ \beta(-6+\theta) = \big(\frac{2}{3}, -\frac{1}{9}\big),\ \gamma(-6+\theta) = \frac{-33+4\theta}{9},$$
$$\omega(-4+\theta) = (1,4),\ \beta(-4+\theta) = \big(\frac{4}{13}, -\frac{1}{13}\big),\ \gamma(-4+\theta) = -1,$$
$$\omega(-2+\theta) = (1,6),\ \beta(-2+\theta) = \big(\frac{2}{9}, -\frac{1}{9}\big),\ \gamma(-2+\theta) = \frac{-1-4\theta}{9}.$$

On the other hand, $H(f,2)/K(f,2) = \mathbb{Z}/3\mathbb{Z} = \{[0,1],[1,1],[1,3]\}$ is generated by $[1,1]$, and we have

$$\omega(-7+\theta) = (1,1),\ \beta(-7+\theta) = \big(\frac{7}{4}, -\frac{1}{4}\big),\ \gamma(-7+\theta) = \frac{-23+3\theta}{2},$$
$$\omega(-5+\theta) = (1,3),\ \beta(-5+\theta) = \big(\frac{5}{12}, -\frac{1}{12}\big),\ \gamma(-5+\theta) = \frac{11-\theta}{6}.$$

**Example 4.9.6.** $P = 4$, $Q = 1$. In this case, we have $D = 12$, $r = 1$, $\tilde{D} = D/4 = 3$ and $\nu = \mathrm{ord}_2 P = 2$. Therefore, Corollary 4.3.2 implies

$$G(f) = H(f,2) \supset K(f,2) = G(f,2) = G(f,2^2) \supset G(f,2^3) = G(f,2^4) = \cdots .$$

Moreover, $K(f,2)/G(f,2^2) = G_{(P,Q)}(\mathbb{Z}/2^2\mathbb{Z})/\Theta = \mathbb{Z}/2\mathbb{Z}$ is generated by $[1,2]$, and we have

$$\omega(-2+\theta) = (1,2),\ \beta(-2+\theta) = \big(-\frac{2}{3}, -\frac{1}{3}\big),\ \gamma(-2+\theta) = -1.$$

On the other hand, $H(f,2)/K(f,2) = \mathbb{Z}/2\mathbb{Z}$ is generated by $[1,1]$, and we have

$$\omega(-3+\theta) = (1,1),\ \beta(-3+\theta) = \big(\frac{3}{2}, -\frac{1}{2}\big),\ \gamma(-3+\theta) = -4+\theta.$$

**Example 4.9.7.** $P = 2$, $Q = 9$. In this case, we have $D = -32$, $r = 2$ and $\tilde{D} = D/4^2 = -2$. Therefore, Corollary 4.3.4 implies

$$G(f) = H(f,2) \supset K(f,2) = G(f,2) = G(f,2^2) \supset G(f,2^3) = G(f,2^4) = \cdots .$$

Moreover, $H(f,2)/K(f,2) = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} = \{[0,1],[1,1],[1,3],[1,5]\}$, and we have

$$\omega(-1+\theta) = (1,1),\ \beta(-1+\theta) = \big(-\frac{1}{8}, \frac{1}{8}\big),\ \gamma(-1+\theta) = -1,$$
$$\omega(1+\theta) = (1,3),\ \beta(1+\theta) = \big(\frac{1}{12}, \frac{1}{12}\big),\ \gamma(1+\theta) = \frac{-2+\theta}{3},$$
$$\omega(3+\theta) = (1,5),\ \beta(3+\theta) = \big(\frac{1}{8}, \frac{1}{24}\big),\ \gamma(3+\theta) = \frac{\theta}{3}.$$

## 5. Complements

**Proposition 5.1.** *Let $P, Q \in \mathbb{Z}$, and let $p$ be a prime and $s$ a positive integer. Put $f_s(t) = t^2 - p^sPt + p^{2s}Q$. Then the isomorphism $\underline{p^s} : G_{(p^sP,p^{2s}Q)}(\mathbb{Q}) \xrightarrow{\sim} G_{(P,Q)}(\mathbb{Q})$ induces isomorphisms $G(f_s) \xrightarrow{\sim} G(f)$, $K(f_s, p) \xrightarrow{\sim} G(f, p^s)$ and $G(f_s, p^n) \xrightarrow{\sim} G_(f, p^{n+s})$ for $n \geq 1$. Furthermore,*
(1) *Assume* $\mathrm{ord}_pP = 0$ *and* $\mathrm{ord}_pQ = 1$. *Then we have an exact sequence*

$$0 \longrightarrow G_{(D)}(\mathbb{Z}/p^s\mathbb{Z}) \longrightarrow H(f_s, p) \longrightarrow H(f, p) \longrightarrow 0.$$

(2) *Assume* $\mathrm{ord}_pP \geq 1$ *and* $\mathrm{ord}_pQ = 1$. *Let $\Theta_1$ denote the subgroup of $\Theta$ generated by $\beta(\theta^2)$. Then we have $G_{(P,Q)}(\mathbb{Z}_{(p)}) \cap \Theta = \Theta_1$, and we have an exact sequence*

$$0 \longrightarrow G_{(D)}(\mathbb{Z}/p^s\mathbb{Z})/\Theta_1 \longrightarrow H(f_s, p) \longrightarrow H(f, p) \longrightarrow 0.$$

(3) *Assume* $\mathrm{ord}_pQ = 0$. *Then we have an exact sequence*

$$0 \longrightarrow G_{(D)}(\mathbb{Z}/p^s\mathbb{Z})/\Theta \longrightarrow H(f_s, p) \longrightarrow H(f, p) \longrightarrow 0.$$

Proof. Let $\theta$ denote the image of $t$ in $\mathbb{Z}[t]/(t^2 - Pt + Q)$, and let $\theta_s$ denote $\mathbb{Z}[t]/(t^2 - p^sPt + p^{2s}Q)$. Then $\theta_s \mapsto \theta$ defines an embedding of rings $\mathbb{Z}[t]/(t^2 - p^sPt + p^{2s}Q) \to \mathbb{Z}[t]/(t^2 - Pt + Q)$. Moreover, then we have

$$\beta(\theta) = \left(0, \frac{1}{Q}\right) \text{ in } G_{(P,Q)}(\mathbb{Q}),\ \beta(\theta_s) = \left(0, \frac{1}{p^{2s}Q}\right) \text{ in } G_{(p^sP,p^{2s}Q)}(\mathbb{Q})$$

and therefore

$$\underline{p^s}(\beta(\theta_s)) = \beta(\theta).$$

Now let $\Theta$ denote the subgroup of $G_{(P,Q)}(\mathbb{Q})$ generated by $\beta(\theta)$, and let $\Theta'$ denote the subgroup of $G_{(p^sP,p^{2s}Q)}(\mathbb{Q})$ generated by $\beta(\theta_s)$. Then the isomorphisms $\omega : G_{(P,Q)}(\mathbb{Q})/\Theta \xrightarrow{\sim} G(f)$ and $\omega : G_{(p^sP,p^{2s}Q)}(\mathbb{Q})/\Theta' \xrightarrow{\sim} G(f_s)$ give a commutative diagram

$$\begin{tikzcd}
G_{(p^sP,p^{2s}Q)}(\mathbb{Q})/\Theta' \arrow[r, "\sim"] \arrow[d, "\wr\ \omega"] & G_{(P,Q)}(\mathbb{Q})/\Theta \arrow[d, "\wr\ \omega"] \\
G(f_s) \arrow[r, "\sim"] & G(f)
\end{tikzcd}.$$

Moreover, under the identification $G(f_s) = G(f)$, we have

$$K(f_s, p) = (G_{(p^sP,p^{2s}Q)}(\mathbb{Z}_{(p)}) + \Theta')/\Theta' = (G_{(p^sP,p^{2s}Q)}(\mathbb{Z}_{(p)}) + \Theta)/\Theta = G(f, p^s)$$

and

$$G(f_s, p^n) = (G_{(p^{n+s}P,p^{2(n+s)}Q)}(\mathbb{Z}_{(p)}) + \Theta')/\Theta' = (G_{(p^{n+s}P,p^{2(n+s)}Q)}(\mathbb{Z}_{(p)}) + \Theta)/\Theta = G(f, p^{n+s})$$

for $n > 0$.

Now we verify the last assertions in each case. We obtain an exact sequence

$$0 \longrightarrow K(f, p)/K(f_s, p) \longrightarrow H(f)/K(f_s, p) \longrightarrow H(f)/K(f, p) \longrightarrow 0,$$

taking the torsion part of each term for the exact sequence

$$0 \longrightarrow K(f,p)/K(f_s,p) \longrightarrow G(f)/K(f_s,p) \longrightarrow G(f)/K(f,p) \longrightarrow 0$$

and noting that $K(f,p)/K(f_s,p) = K(f,p)/G(f,p^s)$ is finite.

(1) Assume $\mathrm{ord}_p P = 0$ and $\mathrm{ord}_p Q = 1$. Then we obtain $\left(\dfrac{D}{p}\right) = 1$ if $p > 2$, and $D \equiv 1 \mod 8$ if $p = 2$. These, together with [14, Proposition 1.5] and Proposition 2.2 (1), imply that $G_{(P,Q)}(\mathbb{Q})/G_{(P,Q)}(\mathbb{Z}_{(p)})$ is isomorphic to $\mathbb{Z}$. Moreover, we have $\beta(\theta) \notin G_{(P,Q)}(\mathbb{Z}_{(p)})$ since $\beta(\theta) = (0, 1/Q)$ and $\mathrm{ord}_p(1/Q) = -1$. It follows that $G_{(P,Q)}(\mathbb{Z}_{(p)}) \cap \Theta = \{1\}$ and that the isomorphism $G_{(P,Q)}(\mathbb{Q})/\Theta \xrightarrow{\sim} G(f)$ induces isomorphisms

$$G_{(P,Q)}(\mathbb{Z}_{(p)}) \xrightarrow{\sim} K(f,p)$$

and

$$G_{(p^sP,p^{2s}Q)}(\mathbb{Z}_{(p)}) \xrightarrow{\sim} G(f,p^s) = K(f_s,p).$$

Hence we obtain an isomorphism

$$G_{(P,Q)}(\mathbb{Z}/p^s\mathbb{Z}) = G_{(P,Q)}(\mathbb{Z}_{(p)})/G_{(p^sP,p^{2s}Q)}(\mathbb{Z}_{(p)}) \xrightarrow{\sim} K(f,p)/K(f_s,p).$$

(2) Assume $\mathrm{ord}_p P \geq 1$ and $\mathrm{ord}_p Q = 1$. Then we have $\beta(\theta) \notin G_{(P,Q)}(\mathbb{Z}_{(p)})$ since $\beta(\theta) = (0, 1/Q)$ and $\mathrm{ord}_p(1/Q) = -1$. Moreover, we have

$$\beta(\theta^2) = \left(-\frac{P}{Q}, \frac{P^2}{Q^2}\right) \text{ in } G_{(P,Q)}(\mathbb{Q}).$$

since $\theta^2 = -Q + P\theta$ in $\mathbb{Z}[t]/(t^2 - Pt + Q)$. Hence we obtain $\beta(\theta^2) \in G_{(P,Q)}(\mathbb{Z}_{(p)})$ since $\mathrm{ord}_p(P/Q) = \mathrm{ord}_p P - \mathrm{ord}_p Q \geq 0$. It follows that $G_{(P,Q)}(\mathbb{Z}_{(p)}) \cap \Theta = \Theta_1$ and that the isomorphism $G_{(P,Q)}(\mathbb{Q})/\Theta \xrightarrow{\sim} G(f)$ induces isomorphisms

$$G_{(P,Q)}(\mathbb{Z}_{(p)})/\Theta_1 \xrightarrow{\sim} (G_{(P,Q)}(\mathbb{Z}_{(p)}) + \Theta)/\Theta \xrightarrow{\sim} K(f,p)$$

and

$$(G_{(p^sP,p^{2s}Q)}(\mathbb{Z}_{(p)}) + \Theta_1)/\Theta_1 \xrightarrow{\sim} (G_{(p^sP,p^{2s}Q)}(\mathbb{Z}_{(p)}) + \Theta)/\Theta \xrightarrow{\sim} G(f,p^s) = K(f_s,p).$$

Hence we obtain an isomorphism

$$G_{(P,Q)}(\mathbb{Z}/p^s\mathbb{Z})/\Theta_1 = G_{(P,Q)}(\mathbb{Z}_{(p)})/(G_{(p^sP,p^{2s}Q)}(\mathbb{Z}_{(p)}) + \Theta_1) \xrightarrow{\sim} K(f,p)/K(f_s,p).$$

(3) Assume $\mathrm{ord}_p Q = 0$. Then we have $\beta(\theta) \in G_{(P,Q)}(\mathbb{Z}_{(p)})$ since $\beta(\theta) = (0, 1/Q)$ and $\mathrm{ord}_p(1/Q) = 0$. It follows that $G_{(P,Q)}(\mathbb{Z}_{(p)}) \supset \Theta$ and that the isomorphism $G_{(P,Q)}(\mathbb{Q})/\Theta \xrightarrow{\sim} G(f)$ induces isomorphisms

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

and

$$(G_{(p^sP,p^{2s}Q)}(\mathbb{Z}_{(p)}) + \Theta)/\Theta \xrightarrow{\sim} G(f,p^s) = K(f_s,p).$$

Hence we obtain an isomorphism

$$G_{(P,Q)}(\mathbb{Z}/p^s\mathbb{Z})/\Theta = G_{(P,Q)}(\mathbb{Z}_{(p)})/(G_{(p^sP,p^{2s}Q)}(\mathbb{Z}_{(p)}) + \Theta) \overset{\sim}{\to} K(f,p)/K(f_s,p).$$

**Remark 5.2.** Proposition 5.1 allows us to reduce the case of $p|P$ and $p|Q$ to the case of $\mathrm{ord}_pP = 0$ or $\mathrm{ord}_pQ \leq 1$ on examination of Laxton groups.

In [14], assuming $p > 2$, we make an examination of Laxton groups in [14, Corollary 4.3] when $\mathrm{ord}_pQ = 0$ and in [14, Colloary 4.9] when $\mathrm{ord}_pP = 0$ and $\mathrm{ord}_pQ$=1. We assume there that $P$ and $Q$ is prime to each other, however the argument developed there works well also under the assumption $\mathrm{ord}_pQ = 0$ or $\mathrm{ord}_pP = 0$. We shall complement the case of $\mathrm{ord}_pP \geq 1$ and $\mathrm{ord}_pQ = 1$ as Proposition 5.3.

On the other hand, we treat the case of $p = 2$ in this article, referring to Corollary 4.3 when $\mathrm{ord}_2Q = 0$, to Corollary 4.5 when $\mathrm{ord}_2P = 0$, to Corollary 4.6 when $\mathrm{ord}_2Q = 1$ and $\mathrm{ord}_2P = 1$, and to Corollary 4.7 when $\mathrm{ord}_2Q = 1$ and $\mathrm{ord}_2P \geq 2$.

**Proposition 5.3.** *Let $P, Q \in \mathbb{Z}$, and let $p$ be a prime $> 2$. Assume $\mathrm{ord}_pP \geq 1$ and $\mathrm{ord}_pQ = 1$, and put $s = \mathrm{ord}_pP$. Then:*

(1) *Assume that $s = 1$ and that $p > 3$ or $p = 3$, $D \equiv 3 \mod 9$. Then the descending chain of subgroups of $U_{P,Q}(\mathbb{Q}) = G_{(P,Q)}(\mathbb{Q})$:*

$$U_{P,Q}(\mathbb{Q}) = U_{P,Q}(\mathbb{Z}_{(p)}) \supset G_{(P,Q)}(\mathbb{Z}_{(p)}) \supset G_{(pP,p^2Q)}(\mathbb{Z}_{(p)}) \supset \cdots \supset G_{(p^nP,p^{2n}Q)}(\mathbb{Z}_{(p)}) \supset \cdots$$

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

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

(2) *Assume that $p = 3$, $s = 1$ and $D \equiv 3 \mod 9$. and put $s' = \mathrm{ord}_3(P^2 - 3Q)$. Then we have $s' \geq 2$, and the descending chain of subgroups of $U_{P,Q}(\mathbb{Q}) = G_{(P,Q)}(\mathbb{Q})$:*

$$\begin{aligned} U_{P,Q}(\mathbb{Q}) = U_{P,Q}(\mathbb{Z}_{(p)}) \supset G_{(P,Q)}(\mathbb{Z}_{(p)}) \supset G_{(pP,p^2Q)}(\mathbb{Z}_{(p)}) \supset \cdots \\ \supset G_{(p^{s'-1}P,p^{2(s'-1)}Q)}(\mathbb{Z}_{(p)}) \supset G_{(p^{s'}P,p^{2s'}Q)}(\mathbb{Z}_{(p)}) \supset G_{(p^{s'+1}P,p^{2(s'+1)}Q)}(\mathbb{Z}_{(p)}) \supset \cdots \end{aligned}$$

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

$$G(f) = H(f,2) = K(f,2) = G(f,2) \supset \cdots \supset G(f,2^{s'-1}) = G(f,2^{s'}) = G(f,2^{s'+1}) = \cdots .$$

*More precisely, let $\Theta_1$ and $\Theta_2$ denote the subgroup of $\Theta$ generated by $\beta(\theta)^2$ and $\beta(\theta)^6$. Then we have $G_{(P,Q)}(\mathbb{Z}_{(p)}) \cap \Theta = \Theta_1$ and $G_{(p^nP,4^nQ)}(\mathbb{Z}_{(p)}) \cap \Theta_2 = \Theta_2$ for $1 \leq n \leq s' - 1$. Therefore, the isomorphism $\omega : G_{(P,Q)}(\mathbb{Q})/\Theta \overset{\sim}{\to} G(f)$ induces isomorphisms*

$$G_{(P,Q)}(\mathbb{Z}_{(p)})/\Theta_1 \overset{\sim}{\to} (G_{(P,Q)}(\mathbb{Z}_{(p)}) + \Theta)/\Theta \overset{\sim}{\to} K(f,p)$$

and

$$G_{(p^nP,p^{2n}Q)}(\mathbb{Z}_{(p)})/\Theta_2 \overset{\sim}{\to} (G_{(P,Q)}(\mathbb{Z}_{(p)}) + \Theta)/\Theta \overset{\sim}{\to} G(f,p^n)$$

for $1 \leq n \leq s' - 1$.

(3) *Assume that $s \geq 2$. Then the descending chain of subgroups of $U_{P,Q}(\mathbb{Q}) = G_{(P,Q)}(\mathbb{Q})$:*

$$U_{P,Q}(\mathbb{Q}) = U_{P,Q}(\mathbb{Z}_{(p)}) \supset G_{(P,Q)}(\mathbb{Z}_{(p)}) \supset G_{(pP,p^2Q)}(\mathbb{Z}_{(p)}) \supset \cdots$$
$$\supset G_{(p^{s-1}P,p^{2(s-1)}Q)}(\mathbb{Z}_{(p)}) \supset G_{(p^sP,p^{2s}Q)}(\mathbb{Z}_{(p)}) \supset G_{(p^{s+1}P,p^{2(s+1)}Q)}(\mathbb{Z}_{(p)}) \supset \cdots$$

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

$$G(f) = H(f,2) = K(f,2) = G(f,2) \supset \cdots \supset G(f,2^{s-1}) = G(f,2^s) = G(f,2^{s+1}) = \cdots .$$

*More precisely, let $\Theta_1$ denote the subgroup of $\Theta$ generated by $\beta(\theta)^2$. Then we have $G_{(P,Q)}(\mathbb{Z}_{(p)}) \cap \Theta = \Theta_1$. Therefore, the isomorphism $\omega : G_{(P,Q)}(\mathbb{Q})/\Theta \overset{\sim}{\to} G(f)$ induces an isomorphism*

$$G_{(P,Q)}(\mathbb{Z}_{(p)})/\Theta_1 \overset{\sim}{\to} (G_{(P,Q)}(\mathbb{Z}_{(p)}) + \Theta)/\Theta \overset{\sim}{\to} K(f,p).$$

Proof. Note first that the assumption $\mathrm{ord}_p P \geq 1$ and $\mathrm{ord}_p Q = 1$ implies $\mathrm{ord}_p D = 1$. Hence we have $U_{P,Q}(\mathbb{Q}) = U_{P,Q}(\mathbb{Z}_{(p)})$ by [13, Proposiiton 2.2(3)], and $U_{P,Q}(\mathbb{Z}_{(p)})/G_{(P,Q)}(\mathbb{Z}_{(p)}) = U_D(\mathbb{Z}_{(p)})/G_{(D)}(\mathbb{Z}_{(p)})$ is isomorphic to $\mathbb{Z}/2\mathbb{Z}$ by [14, Proposition 2.3].

Furthermore, noting

$$\theta^2 = -Q + P\theta,\ \frac{\theta}{\bar{\theta}} = \frac{\theta^2}{\mathrm{Nr}\,\theta} = \frac{-Q + p\theta}{Q},$$

we obtain

$$\gamma(\theta) = \Big(-1, \frac{P}{Q}\Big) \text{ in } U_{P,Q}(\mathbb{Q}),\ \beta(\theta) = \Big(0, \frac{1}{Q}\Big) \text{ in } G_{(P,Q)}(\mathbb{Q}).$$

Moreover, we have $\mathrm{ord}_p(1/Q) = -1$ and $\mathrm{ord}_p(P/Q) = s - 1 \geq 1$. These imply that $\gamma(\theta) \in U_{P,Q}(\mathbb{Z}_{(p)})$, $\beta(\theta) \notin G_{(P,Q)}(\mathbb{Z}_{(p)})$. Hence we obtain

$$U_{P,Q}(\mathbb{Z}_{(p)}) = G_{(P,Q)}(\mathbb{Z}_{(p)}) + \Theta$$

since $U_{P,Q}(\mathbb{Z}_{(p)})/G_{(P,Q)}(\mathbb{Z}_{(p)})$ is isomorphic to $\mathbb{Z}/2\mathbb{Z}$.

Note now that

$$\beta(\theta)^2 = \Big(-\frac{P}{Q}, \frac{P^2}{Q^2}\Big) \text{ in } G_{(P,Q)}(\mathbb{Q})$$

and $\mathrm{ord}_p(P/Q) = s - 1 \geq 0$. It follows:

(a) If $s = 1$, then we have

$$\beta(\theta)^2 \in G_{(P,Q)}(\mathbb{Z}_{(p)}),\ \beta(\theta)^2 \notin \mathrm{Ker}[G_{(P,Q)}(\mathbb{Z}_{(p)}) \to G_{(P,Q)}(\mathbb{Z}/p\mathbb{Z})].$$

Moreover, we have $\mathrm{ord}_p(1/Q) = -1$ and $\mathrm{ord}_p(P/Q) = s - 1 \geq 1$. Hence we obtain

$$G_{(P,Q)}(\mathbb{Z}_{(p)}) \cap \Theta = \Theta_1,$$

and

$$G_{(P,Q)}(\mathbb{Z}_{(p)}) = G_{(pP,p^2Q)}(\mathbb{Z}_{(p)}) + \Theta_1$$

since $G_{(P,Q)}(\mathbb{Z}_{(p)})/G_{(pP,p^2Q)}(\mathbb{Z}_{(p)})$ is isomorphic to $\mathbb{Z}/p\mathbb{Z}$ by [14, Corollary 2.21].

(b) If $s \geq 2$, then we have

$$\beta(\theta)^2 \in \mathrm{Ker}[G_{(P,Q)}(\mathbb{Z}_{(p)}) \to G_{(P,Q)}(\mathbb{Z}/p^{s-1}\mathbb{Z})],\ \beta(\theta)^2 \notin \mathrm{Ker}[G_{(P,Q)}(\mathbb{Z}_{(p)}) \to G_{(P,Q)}(\mathbb{Z}/p^s\mathbb{Z})].$$

Hence we obtain

$$G_{(p^{s-1}P,p^{2(s-1)}Q)}(\mathbb{Z}_{(p)}) \cap \Theta = \Theta_1,$$

and

$$G_{(p^{s-1}P,p^{2(s-1)}Q)}(\mathbb{Z}_{(p)}) = G_{(p^sP,p^{2s}Q)}(\mathbb{Z}_{(p)}) + \Theta_1$$

since $G_{(p^{s-1}P,p^{2(p-1)}Q)}(\mathbb{Z}_{(p)})/G_{(p^2P,p^{2s}Q)}(\mathbb{Z}_{(p)})$ is isomorphic to $\mathbb{Z}/p\mathbb{Z}$.

Now we prove the assertions in each case.

(1) Assume that $s = 1$ and that $p > 3$ or $p = 3$, $D \equiv 3 \mod 9$. Then, it follows from [14, Corollary 2.21 (1)] that

$$G_{(P,Q)}(\mathbb{Z}_{(p)})/G_{(p^nP,p^{2n}Q)}(\mathbb{Z}_{(p)}) = G_{(P,Q)}(\mathbb{Z}/p^n\mathbb{Z}) \xrightarrow{\sim} \mathbb{Z}/p^n\mathbb{Z}$$

for $n \geq 1$. Hence we obtain

$$G_{(P,Q)}(\mathbb{Z}_{(p)}) = G_{(p^nP,p^{2^n}Q)}(\mathbb{Z}_{(p)}) + \Theta_1$$

for $n \geq 1$, which implies the conclusion.

(2) Assume that $p = 3$, $s = 1$ and $D \equiv -3 \mod 9$. Noting

$$\theta^6 = -Q(P^4 - 3P^2Q + Q^2) + P(P^2 - Q)(P^2 - 3Q)\theta,$$

we obtain

$$\beta(\theta)^6 = \Big( - \frac{P(P^2 - Q)(P^2 - 3Q)(P^4 - 3P^2Q + Q^2)}{Q^5}, \frac{P^2(P^2 - Q)^2(P^2 - 3Q)^2}{Q^6} \Big) \text{ in } G_{(P,Q)}(\mathbb{Q}).$$

Moreover, we have

$$\frac{P(P^2 - Q)(P^2 - 3Q)(P^4 - 3P^2Q + Q^2)}{Q^5} = (1 + 1 + s' + 2) - 5 = s' - 1,$$

$$\mathrm{ord}_p \frac{P^2(P^2 - Q)^2(P^2 - 3Q)^2}{Q^6} = (2 + 2 + 2s') - 6 = 2(s' - 1).$$

These imply that

$$\beta(\theta)^6 \in \mathrm{Ker}[G_{(P,Q)}(\mathbb{Z}_{(p)}) \to G_{(P,Q)}(\mathbb{Z}/p^{s'-1}\mathbb{Z})],\ \beta(\theta)^6 \notin \mathrm{Ker}[G_{(P,Q)}(\mathbb{Z}_{(p)}) \to G_{(P,Q)}(\mathbb{Z}/p^{s'}\mathbb{Z})],$$

and therefore

$$G_{(p^{s'-1}P,p^{2(s'-1)}Q)}(\mathbb{Z}_{(p)}) \cap \Theta = \Theta_2.$$

Furthermore, it follows from [13, Corollary 2.21 (1)] and the fact $s' - 1 \geq 1$ that

$$G_{(p^{s'-1}P,p^{2(s'-1)}Q)}(\mathbb{Z}_{(p)})/G_{(p^{s'-1+n}P,p^{2(s'-1+n)}Q)}(\mathbb{Z}_{(p)}) = G_{(p^{s'-1}P,p^{2(s'-1)}Q)}(\mathbb{Z}/p^n\mathbb{Z}) \xrightarrow{\sim} \mathbb{Z}/p^n\mathbb{Z}$$

for $n \geq 1$. Hence we obtain

$$G_{(p^{s'-1}P,p^{2(s'-1)}Q)}(\mathbb{Z}_{(p)}) = G_{(p^{s'-1+n}P,p^{2(s'-1+n)}Q}(\mathbb{Z}_{(p)}) + \Theta_2,$$

for $n \geq 1$, which implies the conclusion.

(3) Assume that $s \geq 2$. Then it follows from [14, Corollary 2.21 (1)] and the fact $s-1 \geq 1$ that

$$G_{(p^{s-1}P,p^{2(s-1)}Q)}(\mathbb{Z}_{(p)})/G_{(p^{s-1+n}P,p^{2(s-1+n)}Q)}(\mathbb{Z}_{(p)}) = G_{(p^{s-1}P,p^{2(s-1)}Q)}(\mathbb{Z}/p^n\mathbb{Z}) \xrightarrow{\sim} \mathbb{Z}/p^n\mathbb{Z}$$

for $n \geq 1$. Hence we obtain

$$G_{(p^{s-1}P,p^{2(s-1)}Q)}(\mathbb{Z}_{(p)}) = G_{(p^{s-1+n}P,p^{2(s-1+n)}Q}(\mathbb{Z}_{(p)}) + \Theta_1,$$

for $n \geq 1$, which implies the conclusion.

**5.4.** Let $P, Q \in \mathbb{Z}$, and put $f(t) = t^2 - Pt + Q$. Assume that $D = P^2 - 4Q = 0$ and $Q \neq 0$. Then there exists $a \in \mathbb{Z}$ such that $P = 2a$ and $Q = a^2$. Hence we have $t^2 - Pt + Q = (t-a)^2$, $\theta \in G_{P,Q}(\mathbb{Q})$ and

$$\xi(\theta) = \Big(a, \frac{1}{a}\Big),\ \xi(\beta(\theta)) = \frac{1}{a}.$$

Let $p$ be a prime. If $a$ is prime to $p$, then the descending chain of subgroups of $G_{(P,Q)}(\mathbb{Q})$:

$$G_{(P,Q)}(\mathbb{Q}) \supset G_{(P,Q)}(\mathbb{Z}_{(p)}) \supset G_{(pP,p^2Q)}(\mathbb{Z}_{(p)}) \supset \cdots \supset G_{(p^nP,p^{2n}Q)}(\mathbb{Z}_{(p)}) \supset \cdots$$

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

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

Note that $G(f) = H(f,p)$ and $H(f,p)/K(f,p) = \mathbb{Q}_p/\mathbb{Z}_p$ since $G_{(P,Q)}(\mathbb{Q})/G_{(P,Q)}(\mathbb{Z}_{(p)}) = \mathbb{Q}/\mathbb{Z}_{(p)}$ $= \mathbb{Q}_p/\mathbb{Z}_p$ and $\mathbb{Q}_p/\mathbb{Z}_p$ is a torsion group.

We interpret the assertion mentioned above more concretely. Take $\boldsymbol{w} = (w_k)_{k\geq 0} \in \mathcal{L}(f,\mathbb{Z})$. Then we have $w_k = w_0a^k + k(w_1 - aw_0)a^{k-1}$ for $k \geq 0$, and $\mathit{\Delta}(\boldsymbol{w}) = w_1^2 - Pw_0w_1 + Qw_0^2 = (w_1 - aw_0)^2$. Moreover, we have $\omega((w_1 - 2aw_0) + w_0\theta) = \boldsymbol{w}$. Take now $\boldsymbol{w} = (w_k)_{k\geq 0} \in \mathcal{R}(f,\mathbb{Z})$. Then, $p^n|w_k$ if and only if $p^n|(aw_0 + k(w_1 - aw_0))$. Therefore we have the following implications:

$$\begin{aligned} p \nmid (w_1 - aw_0) \ &\Leftrightarrow \ \text{for any } n > 0, \text{ there exists } k \text{ such that } p^n|w_k, \\ p|(w_1 - aw_0) \ &\Leftrightarrow \ \text{there does not exist } k \text{ such that } p|w_k. \end{aligned}$$

Indeed, if $p|(w_1 - aw_0)$ and $p|(aw_0 + k(w_1 - aw_0))$, then we obtain $p|aw_0$ and therefore $p|w_0$ and $p|w_1$. This contradicts $\boldsymbol{w} \in \mathcal{R}(f,\mathbb{Z})$.

Now put $\eta = (w_1 - 2aw_0) + w_0\theta$. Then we have

$$\beta(\eta) = \Big(\frac{(w_1 - 2aw_0)w_0}{(w_1 - aw_0)^2}, \frac{w_0^2}{(w_1 - aw_0)^2}\Big) \text{ in } G_{(P,Q)}(\mathbb{Q})$$

and

$$\xi(\beta(\eta)) = \frac{w_0}{w_1 - aw_0} \text{ in } \mathbb{G}_a(\mathbb{Q}) = \mathbb{Q}.$$

Hence we obtain the implication

$$p \nmid (w_1 - aw_0) \ \Leftrightarrow \ \beta(\theta) \in G_{(P,Q)}(\mathbb{Z}_{(p)}).$$

This means $K(f,p) = G(f,p) = G(f,p^2) = \cdots = G(f,p^n) = \cdots$.

We conclude the article by remarking on a result in Ward [15], which was refined by Hall [6].

**Notation 5.5.** Let $P, Q \in \mathbb{Z}$, and put $f(t) = t^2 - Pt + Q$ and $D = P^2 - 4Q$. Let $\theta$ denote the image of $t$. in the residue ring $\mathbb{Z}[t]/(t^2 - Pt + Q)$. Fix a prime number $p$ with $(p, Q) = 1$. Then we have $\theta \in G_{P,Q}(\mathbb{Z}_{(p)})$ and therefore $\beta(\theta) = (0, 1/Q) \in G_{(P,Q)}(\mathbb{Z}_{(p)})$.

Take now $\boldsymbol{w} = (w_k)_{k\geq 0} \in \mathcal{L}(f, \mathbb{Z})$, and put

$$\eta = (w_1 - Pw_0) + w_0\theta \in \mathbb{Z}[t]/(t^2 - Pt + Q).$$

Then we have $\omega(\eta) = \boldsymbol{w}$. Assume $\varDelta(\boldsymbol{w}) = w_1^2 - Pw_0w_1 + Qw_0^2 \neq 0$. Then we have $\eta \in G_{P,Q}(\mathbb{Q})$ and

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

Moreover, if $p \nmid \varDelta(\boldsymbol{w})$, then we have $\eta \in G_{P,Q}(\mathbb{Z}_{(p)})$ and therefore $\beta(\eta) \in G_{(P,Q)}(\mathbb{Z}_{(p)})$.

Assume now $w_0 \neq 0$. Put

$$\tilde{P} = Pw_0 - 2w_1,\ \tilde{Q} = w_1^2 - Pw_0w_1 + Qw_0^2,\ \tilde{D} = \tilde{P}^2 - 4\tilde{Q}.$$

Then we obtain

$$\tilde{P}^2 - 4\tilde{Q} = w_0^2(P^2 - 4Q).$$

Let $\tilde{\theta}$ denote the image of $t$ in $\mathbb{Z}[t]/(t^2 - \tilde{P}t + \tilde{Q})$. Then we obtain

$$\beta(\tilde{\theta}) = \Big(0, \frac{1}{\tilde{Q}}\Big) = \Big(0, \frac{1}{w_1^2 - Pw_0w_1 + Qw_0^2}\Big) \in G_{(\tilde{P},\tilde{Q})}(\mathbb{Q}).$$

Moreover, $\tilde{\theta} \mapsto (Pw_0 - w_1) - w_0\theta$ gives rise to a homomorphism of rings $\psi : \mathbb{Z}[t]/(t^2 - \tilde{P}t + \tilde{Q}) \to \mathbb{Z}[t]/(t^2 - Pt - Q)$. Hence a homomorphism group schemes

$$\psi : G_{\tilde{P},\tilde{Q}} = \operatorname{Spec} \mathbb{Z}\big[X, Y, \frac{1}{X^2 + \tilde{P}XY + \tilde{Q}Y^2}\big] \to G_{P,Q} = \operatorname{Spec} \mathbb{Z}\big[X, Y, \frac{1}{X^2 + PXY + QY^2}\big]$$

is defined by

$$X \mapsto X{+}(Pw_0 - w_1)Y,\ Y \mapsto -w_0Y :$$
$$\mathbb{Z}\big[X, Y, \frac{1}{X^2 + \tilde{P}XY + \tilde{Q}Y^2}\big] \to \mathbb{Z}\big[X, Y, \frac{1}{X^2 + PXY + QY^2}\big].$$

Moreover, $\psi : G_{\tilde{P},\tilde{Q}} \to G_{P,Q}$ induces a homomorphism

$$\psi : G_{(\tilde{P},\tilde{Q})} = \operatorname{Spec} \mathbb{Z}[X, Y]/(X^2 + \tilde{P}XY + \tilde{Q}Y^2 - Y)$$
$$\to G_{(P,Q)} = \operatorname{Spec} \mathbb{Z}[X, Y](X^2 + PXY + QY^2 - Y)].$$

Indeed, $\psi : G_{\tilde{P},\tilde{Q}} \to G_{P,Q}$ is given by

$$X \mapsto -w_0X{-}(Pw_0 - w_1)Y,\ Y \mapsto w_0^2Y :$$
$$\mathbb{Z}[X, Y](X^2 + \tilde{P}XY + \tilde{Q}Y^2 - Y)] \to \mathbb{Z}[X, Y]/(X^2 + PXY + QY^2 - Y).$$

In particular, we have $\psi(\tilde{\theta}) = -\eta$ in $G_{P,Q}(\mathbb{Q})$ and $\psi(\beta(\tilde{\theta})) = \beta(\eta)$ in $G_{(P,Q)}(\mathbb{Q})$.

**Proposition 5.6.** *Let $\tilde{\boldsymbol{L}}$ denote the Lucas sequence associated to $(\tilde{P},\tilde{Q})$, and assume that $w_0\Delta(\boldsymbol{w})$ is not divisible by $p$. Then we have*

$$\text{the order of } \beta(\eta) \text{ in } G_{(P,Q)}(\mathbb{Z}/p^n\mathbb{Z}) = \text{the rank of the Lucas sequence } \tilde{\boldsymbol{L}} \bmod p^n.$$

Proof. The assumption $p \nmid w_0\Delta(\boldsymbol{w})$ implies that the homomorphism $\psi : G_{\tilde{P},\tilde{Q}} \to G_{P,Q}$ is isomorphic over $\mathbb{Z}_{(p)}$ and that $\tilde{\theta} \in G_{(\tilde{P},\tilde{Q})}(\mathbb{Z}_{(p)})$. In particular, the homomorphism $\psi : G_{(\tilde{P},\tilde{Q})}(\mathbb{Z}/p^n\mathbb{Z}) \to G_{(P,Q)}(\mathbb{Z}/p^n\mathbb{Z})$ is bijective, and we have $\psi(\beta(\tilde{\theta})) = \beta(\eta)$ in $G_{(P,Q)}(\mathbb{Z}/p^n\mathbb{Z})$. Therefore it is sufficient note that the rank of the Lucas sequence $\tilde{\boldsymbol{L}}$ mod $p^n$ is nothing but the order of $\beta(\tilde{\theta})$ in $G_{(\tilde{P},\tilde{Q})}(\mathbb{Z}/p^n\mathbb{Z})$.

**Corollary 5.7.** *Besides the assumption in Proposition 5.6, we suppose that $G_{(P,Q)}(\mathbb{Z}/p^n\mathbb{Z})$ is a cyclic group. Then, there exists $k \geq 0$ such that $w_k$ is divisible by $p^n$ if and only if the rank of the Lucas sequence $\boldsymbol{L}$ mod $p^n$ is divisible by the rank of the Lucas sequence $\tilde{\boldsymbol{L}}$ mod $p^n$.*

Proof. By abus of notaion, let $\Theta$ denote the subgroup of $G_{(P,Q)}(\mathbb{Z}/p^n\mathbb{Z})$ generated by $\beta(\theta)$. Then, there exists $k \geq 0$ such that $w_k$ is divisible by $p^n$ if and only $\beta(\eta) \in \Theta$ in $G_{(P,Q)}(\mathbb{Z}/p^n\mathbb{Z})$. Now let $r(p^n)$ and $\tilde{r}(p^n)$ denote the rank of $\boldsymbol{L}$ mod $p^n$ and $\tilde{\boldsymbol{L}}$ mod $p^n$, respectively. Then, $\beta(\eta) \in \Theta$ if and only $r(p^n)$ is divisible by $\tilde{r}(p^n)$, since $G_{(P,Q)}(\mathbb{Z}/p^n\mathbb{Z})$ is cyclic and $\Theta \subset G_{(P,Q)}(\mathbb{Z}/p^n\mathbb{Z})$ is of order $r(p^n)$.

**Remark 5.8.** $G_{(P,Q)}(\mathbb{Z}/p^n\mathbb{Z})$ is a cyclic group in the following cases.
(1) $n = 1$;
(2) $p > 3$, or $p = 3$ and $D \not\equiv -3 \mod 9$ ([14, Corollary 2.21]);
(3) $p = 2$ and $\mathrm{ord}_2 D \geq 2$ (Proposition 2.16).

**Remark 5.9.** The assertion of Corollary 5.7 in the case of $n = 1$ was established by Ward [15] and Hall [6]. As is mentioned in the introduction of [15], Ward's study was motivated by the following assertion established by Lucas [7]:

Let $P, Q \in \mathbb{Z}$, and put $f(t) = t^2 - Pt + Q$ and $D = P^2 - 4Q$. Let $\boldsymbol{S} = (S_k)_{k \geq 0}$ denote the companion Lucas sequence associated to $(P, Q)$, that is to say, $\boldsymbol{S} \in \mathcal{L}(f, \mathbb{Z})$ with the initial terms $S_0 = 2$ and $S_1 = P$. Moreover, let $p$ be an odd prime, and assume that $p \nmid Q$ and $p \nmid D$. Then, there exists $k \geq 0$ such that $S_k$ is divisible by $p$ if and only if $r(p)$ is divisible by 2. Here $r(p)$ denotes the rank of the Lucas sequence assocaited to $(P, Q)$ mod $p$.

**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] M. Hall, Divisors of second-order sequences. Bull. Amer. Math. Soc. 43 (1937) 78–80

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

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

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

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

[11] F. Lemmermeyer, Conics, a poor man's elliptic curves. arXiv: math/0311306.

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

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

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

[15] M. Ward, An arithmetical property of recurring series of the second order. Bull. Amer. Math. Soc. 40 (1934) 825–828

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

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

[18] 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