sciendo

Discussiones Mathematicae
General Algebra and Applications 41 (2021) 283–298
https://doi.org/10.7151/dmgaa.1371

CLASSIFICATION OF ELEMENTS IN ELLIPTIC CURVE OVER THE RING $\mathbb{F}_q[\varepsilon]$

Bilel Selikh, Douadi Mihoubi

and

Nacer Ghadbane

Laboratory of Pures and Applied Mathematics
Department of Mathematics
Mohamed Boudiaf University of M'sila
M'sila 28000, Algeria

e-mail: bilel.selikh@univ-msila.dz
douadi.mihoubi@univ-msila.dz
nacer.ghadbane@univ-msila.dz

Abstract

Let $\mathbb{F}_q[\varepsilon] := \mathbb{F}_q[X]/(X^4 - X^3)$ be a finite quotient ring where $\varepsilon^4 = \varepsilon^3$, with $\mathbb{F}_q$ is a finite field of order q such that q is a power of a prime number p greater than or equal to 5. In this work, we will study the elliptic curve over $\mathbb{F}_q[\varepsilon]$, $\varepsilon^4 = \varepsilon^3$ of characteristic $p \neq 2, 3$ given by homogeneous Weierstrass equation of the form $Y^2Z = X^3 + aXZ^2 + bZ^3$ where a and b are parameters taken in $\mathbb{F}_q[\varepsilon]$. Firstly, we study the arithmetic operation of this ring. In addition, we define the elliptic curve $E_{a,b}(\mathbb{F}_q[\varepsilon])$ and we will show that $E_{\pi_0(a),\pi_0(b)}(\mathbb{F}_q)$ and $E_{\pi_1(a),\pi_1(b)}(\mathbb{F}_q)$ are two elliptic curves over the finite field $\mathbb{F}_q$, such that π_0 is a canonical projection and π_1 is a sum projection of coordinate of element in $\mathbb{F}_q[\varepsilon]$. Precisely, we give a classification of elements in elliptic curve over the finite ring $\mathbb{F}_q[\varepsilon]$.

Keywords: elliptic curves, finite ring, finite field, projective space.

2010 Mathematics Subject Classification: 14H52, 11T55, 20K30, 20K27.

1. Introduction

Elliptic curves play an important role in many areas of mathematics. They are the basis of the demonstration of fermat's great theorem by Andrew Wiles, it

was proposed for the asymmetrical cryptography by Koblitz [7] and Miller [8] in 1985 separately.

In 2016, Boulbot, Chillali and Mouhib [2] had constructed a non local ring $\mathbb{F}_q[e] = \mathbb{F}_q[X]/(X^3-X^2)$, $e^3 = e^2$, defined an elliptic curve over $\mathbb{F}_q[e]$ and they had given the classification of elements in $E_{a,b}(\mathbb{F}_q[e])$. In this paper, we will extend the construction of $\mathbb{F}_q[X]/(X^3-X^2)$ to $\mathbb{F}_q[X]/(X^4-X^3)$. Our goal in this paper is to study the elliptic curve over the ring $\mathbb{F}_q[\varepsilon] := \mathbb{F}_q[X]/(X^4-X^3)$. We start this work by studying the arithmetic of the ring $\mathbb{F}_q[\varepsilon]$, $\varepsilon^4 = \varepsilon^3$, in particular we show that $\mathbb{F}_q[\varepsilon]$ is not a local ring. In Section 3, the study of the discriminant and the homogeneous Weierstrass equation of the elliptic curve $E_{a,b}(\mathbb{F}_q[\varepsilon])$, allow us to define two elliptic curves $E_{\pi_0(a),\pi_0(b)}(\mathbb{F}_q)$ and $E_{\pi_1(a),\pi_1(b)}(\mathbb{F}_q)$ over the finite field $\mathbb{F}_q$, where π_0 and π_1 are two surjective morphisms of rings defined by

$$\begin{array}{rcl} \pi_0 : \mathbb{F}_q[\varepsilon] & \longrightarrow & \mathbb{F}_q \\ X = \sum_{i=0}^{3} x_i\varepsilon^i & \longmapsto & x_0 \end{array} \quad \text{and} \quad \begin{array}{rcl} \pi_1 : \mathbb{F}_q[\varepsilon] & \longrightarrow & \mathbb{F}_q \\ X = \sum_{i=0}^{3} x_i\varepsilon^i & \longmapsto & \sum_{i=0}^{3} x_i. \end{array}$$

We conclude this section by giving a classification of the elements of the elliptic curve $E_{a,b}(\mathbb{F}_q[\varepsilon])$ into three types.

2. The finite ring $\mathbb{F}_q[\varepsilon], \varepsilon^4 = \varepsilon^3$

In this section, we follow the approach in [2, 5] and [10]. The ring $\mathbb{F}_q[\varepsilon]$, $\varepsilon^4 = \varepsilon^3$ can be constructed by using the quotient ring of $\mathbb{F}_q[X]$ by the polynomial X^4-X^3. $\mathbb{F}_q$ is a finite field of order q where q is a power of a prime number p, $p \geq 5$. An element X in $\mathbb{F}_q[\varepsilon]$ can be written in the form $X = x_0 + x_1\varepsilon + x_2\varepsilon^2 + x_3\varepsilon^3$ where $(x_0, x_1, x_2, x_3) \in \mathbb{F}_q^4$.

2.1. Arithmetic operations

The arithmetic operations in $\mathbb{F}_q[\varepsilon]$ can be decomposed into operations in $\mathbb{F}_q$ and they are computed as follows:

$$\begin{aligned} X + Y &= (x_0 + y_0) + (x_1 + y_1)\varepsilon + (x_2 + y_2)\varepsilon^2 + (x_3 + y_3)\varepsilon^3 \text{ and} \\ X \cdot Y &= x_0y_0 + (x_0y_1 + x_1y_0)\varepsilon + (x_0y_2 + x_1y_1 + x_2y_0)\varepsilon^2 \\ &\quad + ((x_0 + x_1 + x_2 + x_3)y_3 + (x_1 + x_2 + x_3)y_2 + (x_2 + x_3)y_1 + x_3y_0)\varepsilon^3, \end{aligned}$$

where $X = x_0 + x_1\varepsilon + x_2\varepsilon^2 + x_3\varepsilon^3$ and $Y = y_0 + y_1\varepsilon + y_2\varepsilon^2 + y_3\varepsilon^3$.

Lemma 2.1. *$(\mathbb{F}_q[\varepsilon], +, \cdot)$ is a finite unitary commutative ring isomorphic to the quotient ring $\mathbb{F}_q[X]/(X^4 - X^3)$.*

Lemma 2.2. *The ring $\mathbb{F}_q[\varepsilon]$ is a vector space over $\mathbb{F}_q$ of dimension 4, and we have $\{1, \varepsilon, \varepsilon^2, \varepsilon^3\}$ as basis, then: $\mathbb{F}_q[\varepsilon] = \mathbb{F}_q + \mathbb{F}_q\varepsilon + \mathbb{F}_q\varepsilon^2 + \mathbb{F}_q\varepsilon^3$.*

Proof. Let $X = \sum_{i=0}^{3} x_i\varepsilon^i$ and $Y = \sum_{i=0}^{3} y_i\varepsilon^i$ be two elements of $\mathbb{F}_q[\varepsilon]$ and k in $\mathbb{F}_q$, we have

- $X + Y = (x_0 + y_0) + (x_1 + y_1)\varepsilon + (x_2 + y_2)\varepsilon^2 + (x_3 + y_3)\varepsilon^3$
- $k \cdot X = \sum_{i=0}^{3} kx_i\varepsilon^i = kx_0 + kx_1\varepsilon + kx_2\varepsilon^2 + kx_3\varepsilon^3$. ∎

Proposition 2.3. *The product operation in $\mathbb{F}_q[\varepsilon]$ can be written as*

$$\begin{aligned} X \cdot Y &= x_0y_0 + \Theta_{XY}\varepsilon + \Omega_{XY}\varepsilon^2 \\ &\quad + ((x_0 + x_1 + x_2 + x_3)(y_0 + y_1 + y_2 + y_3) - x_0y_0 - \Theta_{XY} - \Omega_{XY})\varepsilon^3, \textit{ where} \\ \Theta_{XY} &= (x_0 + x_1)(y_0 + y_1) - x_0y_0 - x_1y_1 = x_0y_1 + x_1y_0 \textit{ and} \\ \Omega_{XY} &= (x_0 + x_1 + x_2)(y_0 + y_1 + y_2) - x_0(y_0 + y_1) - x_1(y_0 + y_2) - x_2(y_1 + y_2) \\ &= x_0y_2 + x_1y_1 + x_2y_0. \end{aligned}$$

Proof. We have

$$\begin{aligned} &(x_0 + x_1 + x_2 + x_3)(y_0 + y_1 + y_2 + y_3) - x_0y_0 - \Theta_{XY} - \Omega_{XY} \\ &= (x_0 + x_1 + x_2 + x_3)y_3 + (x_1 + x_2 + x_3)y_2 + (x_2 + x_3)y_1 + x_3y_0. \end{aligned}$$ ∎

Corollary 2.4. *Let $X = x_0 + x_1\varepsilon + x_2\varepsilon^2 + x_3\varepsilon^3 \in \mathbb{F}_q[\varepsilon]$. We have*

$$X^2 = x_0^2 + \Theta_{X^2}\varepsilon + \Omega_{X^2}\varepsilon^2 + \big((x_0 + x_1 + x_2 + x_3)^2 - x_0^2 - x_1^2 - 2x_0x_1 - 2x_0x_2\big)\varepsilon^3$$
$$X^3 = x_0^3 + \Theta_{X^3}\varepsilon + \Omega_{X^3}\varepsilon^2 + \big((x_0 + x_1 + x_2 + x_3)^3 - x_0^3 - 3\big(x_0x_1^2 + x_2x_0^2 + x_1x_0^2\big)\big)\varepsilon^3$$

where

$$\Theta_{X^2} = (x_0 + x_1)^2 - x_0^2 - x_1^2,$$
$$\Omega_{X^2} = (x_0 + x_1 + x_2)^2 - x_0^2 - x_2^2 - 2x_0x_1 - 2x_1x_2,$$
$$\Theta_{X^3} = (x_0 + x_1)^3 - x_0^3 - x_1^3 - 3x_0x_1^2 \textit{ and}$$
$$\Omega_{X^3} = (x_0 + x_1 + x_2)^3 - x_0^3 - x_1^3 - x_2^3 - 3\left(x_0x_2^2 + x_1x_2^2 + x_1x_0^2 + x_2x_1^2\right) - 6x_0x_1x_2.$$

The next proposition characterize the set $(\mathbb{F}_q[\varepsilon])^\times$ of invertible elements in $\mathbb{F}_q[\varepsilon]$.

Proposition 2.5. *Let $X = x_0 + x_1\varepsilon + x_2\varepsilon^2 + x_3\varepsilon^3 \in \mathbb{F}_q[\varepsilon]$. The element X is invertible if and only if x_0 and $x_0 + x_1 + x_2 + x_3$ are invertible in $\mathbb{F}_q$. The inverse of X is given by*

$$\begin{aligned} X^{-1} &= x_0^{-1} - x_1x_0^{-2}\varepsilon + \left(x_1^2x_0^{-3} - x_2x_0^{-2}\right)\varepsilon^2 \\ &\quad + \left((x_0 + x_1 + x_2 + x_3)^{-1} + x_1x_0^{-2} + x_2x_0^{-2} - x_1^2x_0^{-3} - x_0^{-1}\right)\varepsilon^3. \end{aligned}$$

Proof. Let $X = x_0 + x_1\varepsilon + x_2\varepsilon^2 + x_3\varepsilon^3$ and $Y = y_0 + y_1\varepsilon + y_2\varepsilon^2 + y_3\varepsilon^3$ be two elements of $\mathbb{F}_q[\varepsilon]$. We have

$$\begin{aligned} X \cdot Y &= x_0y_0 + \Theta_{XY}\varepsilon + \Omega_{XY}\varepsilon^2 \\ &\quad + \big((x_0 + x_1 + x_2 + x_3)(y_0 + y_1 + y_2 + y_3) - x_0y_0 - \Theta_{XY} - \Omega_{XY}\big)\varepsilon^3, \end{aligned}$$

where $\Theta_{XY} = x_0y_1 + x_1y_0$ and $\Omega_{XY} = x_0y_2 + x_1y_1 + x_2y_0$. Then

$$
\begin{aligned}
& X \cdot Y = 1 \\
\Leftrightarrow & \begin{cases} x_0 y_0 = 1 \\ \Theta_{XY} = 0 \\ \Omega_{XY} = 0 \\ (x_0 + x_1 + x_2 + x_3)(y_0 + y_1 + y_2 + y_3) - x_0 y_0 - \Theta_{XY} - \Omega_{XY} = 0 \end{cases} \\
\Leftrightarrow & \begin{cases} x_0 y_0 = 1 \\ x_0 y_1 + x_1 y_0 = 0 \\ x_0 y_2 + x_1 y_1 + x_2 y_0 = 0 \\ (x_0 + x_1 + x_2 + x_3)(y_0 + y_1 + y_2 + y_3) = 1 \end{cases} \\
\Leftrightarrow & \begin{cases} y_0 = x_0^{-1} \\ y_1 = -x_1 x_0^{-2} \\ y_2 = -x_2 x_0^{-2} + x_1^2 x_0^{-3} \\ y_3 = (x_0 + x_1 + x_2 + x_3)^{-1} + x_1 x_0^{-2} + x_2 x_0^{-2} - x_1^2 x_0^{-3} - x_0^{-1} \end{cases}
\end{aligned}
$$

so $X \in (\mathbb{F}_q[\varepsilon])^\times$ if and only if $x_0 \not\equiv 0[p]$ and $x_0 + x_1 + x_2 + x_3 \not\equiv 0[p]$.

In this case we have

$$
\begin{aligned}
X^{-1} = {} & x_0^{-1} - x_1 x_0^{-2}\varepsilon + \left(x_1^2 x_0^{-3} - x_2 x_0^{-2}\right)\varepsilon^2 \\
& + \left((x_0 + x_1 + x_2 + x_3)^{-1} + x_1 x_0^{-2} + x_2 x_0^{-2} - x_1^2 x_0^{-3} - x_0^{-1}\right)\varepsilon^3.
\end{aligned}
$$

■

Corollary 2.6. *Let $X \in \mathbb{F}_q[\varepsilon]$, then X is not invertible if and only if $x_0 \equiv 0[p]$ or $x_0 + x_1 + x_2 + x_3 \equiv 0[p]$ where $(x_0, x_1, x_2, x_3) \in \mathbb{F}_q^4$.*

Lemma 2.7. *$\mathbb{F}_q[\varepsilon]$ is a non local ring.*

Proof. We consider the two ideals of $\mathbb{F}_q[\varepsilon]$ defined by

$$
\begin{aligned}
J_0 &= \left\{x_1\varepsilon + x_2\varepsilon^2 + x_3\varepsilon^3 \mid (x_1, x_2, x_3) \in \mathbb{F}_q^3\right\} \quad \text{and} \\
J_1 &= \left\{x_0 + x_1\varepsilon + x_2\varepsilon^2 - (x_0 + x_1 + x_2)\varepsilon^3 \mid (x_0, x_1, x_2) \in \mathbb{F}_q^3\right\},
\end{aligned}
$$

it's clear that $J_0 \cup J_1$ is the set of non invertible elements in $\mathbb{F}_q[\varepsilon]$ and for all $x_0, x_1, x_2, x, y,$ and z in $\mathbb{F}_q$ we have

$$
\begin{aligned}
& x_0 + x_1\varepsilon + x_2\varepsilon^2 - (x_0 + x_1 + x_2)\varepsilon^3 = x\varepsilon + y\varepsilon^2 + z\varepsilon^3 \\
\Rightarrow\ & x_0 + (x_1 - x)\varepsilon + (x_2 - y)\varepsilon^2 - (x_0 + x_1 + x_2 + z)\varepsilon^3 = 0 \\
& \Rightarrow \begin{cases} x_0 = 0 \\ x_1 - x = 0 \\ x_2 - y = 0 \\ x_0 + x_1 + x_2 + z = 0 \end{cases} \qquad \Rightarrow \begin{cases} x_0 = 0 \\ x_1 = x \\ x_2 = y \\ x_1 + x_2 = -z \end{cases}
\end{aligned}
$$

we have $J_0 \cap J_1 = \{x\varepsilon + y\varepsilon^2 - z\varepsilon^3 \mid (x,y,z) \in \mathbb{F}_q^3\}$, so $J_0 \cup J_1$ is not an ideal. Finally, the ring $\mathbb{F}_q[\varepsilon]$ is not local. ∎

Lemma 2.8. *π_0 and π_1 are two surjective morphisms of rings.*

Proof. Let $X = x_0 + x_1\varepsilon + x_2\varepsilon^2 + x_3\varepsilon^3$ and $Y = y_0 + y_1\varepsilon + y_2\varepsilon^2 + y_3\varepsilon^3$ be two elements of $\mathbb{F}_q[\varepsilon]$.

From the definition of the sum and product law in $\mathbb{F}_q[\varepsilon]$, we have

$$\pi_0(X+Y) = x_0 + y_0 = \pi_0(X) + \pi_0(Y) \text{ and } \pi_0(X \cdot Y) = x_0 \cdot y_0 = \pi_0(X) \cdot \pi_0(Y)$$

so π_0 is morphism of rings.

$$\begin{aligned} \pi_1(X+Y) &= x_0 + y_0 + x_1 + y_1 + x_2 + y_2 + x_3 + y_3 \\ &= \pi_1(X) + \pi_1(Y) \text{ and} \\ \pi_1(X \cdot Y) &= (x_0 + x_1 + x_2 + x_3) \cdot (y_0 + y_1 + y_2 + y_3) \\ &= \pi_1(X) \cdot \pi_1(Y), \end{aligned}$$

so π_1 is morphism of rings.

Finally for all $x \in \mathbb{F}_q \subset \mathbb{F}_q[\varepsilon]$, we have $\pi_0(x) = \pi_1(x) = x$, so π_0 and π_1 are two surjective morphisms. ∎

Remark 2.9. The kernel of π_0, and π_1 is an ideal such that:

$$\begin{aligned} \ker \pi_0 &= \{X \in \mathbb{F}_q[\varepsilon] \mid \pi_0(X) = 0\}. \\ \ker \pi_1 &= \{X \in \mathbb{F}_q[\varepsilon] \mid \pi_1(X) = 0\}. \end{aligned}$$

Corollary 2.10. *For all $i \in \{0,1\}$ the mapping $\bar{\pi}_i$ given by:*

$$\begin{aligned} \bar{\pi}_i : \mathbb{F}_q[\varepsilon]/\ker \pi_i &\longrightarrow \operatorname{Im} \pi_i = \pi_i(\mathbb{F}_q[\varepsilon]) \\ \bar{X} = X + \ker \pi_i &\longmapsto \pi_i(X) \end{aligned}$$

is an isomorphism.

Proof. For $i \in \{0,1\}$ we have π_i is a ring morphism and $\ker \pi_i$ is an ideal. The mapping $\bar{\pi}_i$ is well defined. Let $\bar{X}$, $\bar{X}' \in \mathbb{F}_q[\varepsilon]$ such that

$$\begin{cases} \bar{\pi}_i(\bar{X}) = \pi_i(X) \\ \bar{\pi}_i(\bar{X}') = \pi_i(X') \end{cases}$$

$$\begin{aligned} \bar{X} = \bar{X}' &\Leftrightarrow X - X' \in \ker \pi_i \\ &\Leftrightarrow \pi_i(X - X') = 0 \\ &\Leftrightarrow \pi_i(X) - \pi_i(X') = 0 \\ &\Leftrightarrow \pi_i(X) = \pi_i(X') \\ &\Leftrightarrow \bar{\pi}_i(\bar{X}) = \bar{\pi}_i(\bar{X}') \end{aligned}$$

$\bar{\pi_i}$ is a ring morphism:

$$\begin{aligned}
\bar{\pi_i}(\bar{X}+\bar{X'}) &= \bar{\pi_i}(\overline{X+X'}) \\
&= \pi_i(X+X') \\
&= \pi_i(X)+\pi_i(X') \\
&= \bar{\pi_i}(\bar{X})+\bar{\pi_i}(\bar{X'}) \\
\bar{\pi_i}(\bar{X}\cdot\bar{X'}) &= \bar{\pi_i}(\overline{X\cdot X'}) \\
&= \pi_i(X\cdot X') \\
&= \pi_i(X)\cdot\pi_i(X') \\
&= \bar{\pi_i}(\bar{X})\cdot\bar{\pi_i}(\bar{X'})
\end{aligned}$$

$\bar{\pi_i}$ is a surjective:

$$\begin{aligned}
&\text{If } y \in \operatorname{Im}\pi_i = \pi_i(\mathbb{F}_q[\varepsilon]), \text{ then} \\
&\exists X \in \mathbb{F}_q[\varepsilon] \text{ such that } y = \pi_i(X) \\
&\exists \bar{X} \in \mathbb{F}_q[\varepsilon]/\ker\pi_i \text{ such that } y = \bar{\pi_i}(\bar{X})
\end{aligned}$$

$\bar{\pi_i}$ is a injective:

$$\begin{aligned}
\bar{\pi_i}(\bar{X}) = \bar{\pi_i}(\bar{X'}) &\Leftrightarrow \pi_i(X) = \pi_i(X') \\
&\Leftrightarrow \pi_i(X)-\pi_i(X') = 0 \\
&\Leftrightarrow \pi_i(X-X') = 0 \\
&\Leftrightarrow X-X' \in \ker\pi_i \\
&\Leftrightarrow \bar{X} = \bar{X'}.
\end{aligned}$$

Finally, $\mathbb{F}_q[\varepsilon]/\ker\pi_i \cong \operatorname{Im}\pi_i$ for all $i \in \{0,1\}$. ∎

Corollary 2.11. *$\bar{\pi_i}$ is an isomophism for $i \in \{0,1\}$, in particular we have*

$$\frac{card(\mathbb{F}_q[\varepsilon])}{card(\ker\pi_i)} = card(\mathbb{F}_q[\varepsilon]/\ker\pi_i) = card(\operatorname{Im}\pi_i).$$

2.2. Costs of arithmetic operations

Let s, m and i denote the costs of addition, multiplication and inversion in $\mathbb{F}_q$, respectively and let S, M and I denote the costs of addition, multiplication and inversion in $\mathbb{F}_q[\varepsilon]$, respectively.

We have $S = 4s$, $M = 11s + 8m$ and $I = 7s + 3m + 4i$ where M is calculated by the propsition 2.3.

3. Elliptic curve over $\mathbb{F}_q[\varepsilon], \varepsilon^4 = \varepsilon^3$

In this section, we consider X, Y, Z, a and b are elements of the ring $\mathbb{F}_q[\varepsilon]$ fixed by $X = x_0 + x_1\varepsilon + x_2\varepsilon^2 + x_3\varepsilon^3$, $Y = y_0 + y_1\varepsilon + y_2\varepsilon^2 + y_3\varepsilon^3$, $Z = z_0 + z_1\varepsilon + z_2\varepsilon^2 + z_3\varepsilon^3$

and $a = a_0 + a_1\varepsilon + a_2\varepsilon^2 + a_3\varepsilon^3$ and $b = b_0 + b_1\varepsilon + b_2\varepsilon^2 + b_3\varepsilon^3$, with the prime number p is greater than or equal to 5.

The discriminant of elliptic curve over the ring $\mathbb{F}_q[\varepsilon]$ is $\triangle := 4a^3 + 27b^2$ and we denote by $\triangle_0$ and $\triangle_1$ the images of the discriminant $\triangle$ by π_0 and π_1 the respectively, $\triangle_0 = \pi_0(\triangle) = 4a_0^3 + 27b_0^2$ and $\triangle_1 = \pi_1(\triangle) = 4(a_0 + a_1 + a_2 + a_3)^3 + 27(b_0 + b_1 + b_2 + b_3)^2$.

Definition. We define an elliptic curve over the ring $\mathbb{F}_q[\varepsilon]$, as a curve in the projective space $\mathbb{P}^2(\mathbb{F}_q[\varepsilon])$, which is given by the homogeneous equation of degree 3, by $Y^2Z = X^3 + aXZ^2 + bZ^3$ where a and b in $\mathbb{F}_q[\varepsilon]$ such that the discriminant $\triangle$ is invertible in $\mathbb{F}_q[\varepsilon]$. In this case we denote the elliptic curve over $\mathbb{F}_q[\varepsilon]$ by $E_{a,b}(\mathbb{F}_q[\varepsilon])$ and we write:

$$E_{a,b}(\mathbb{F}_q[\varepsilon]) = \big\{[X : Y : Z] \in \mathbb{P}^2(\mathbb{F}_q[\varepsilon]) \mid Y^2Z = X^3 + aXZ^2 + bZ^3\big\}.$$

Proposition 3.1. *The discriminant $\triangle$ is invertible in $\mathbb{F}_q[\varepsilon]$ if and only if $\triangle_0$ and $\triangle_1$ are invertible in $\mathbb{F}_q$.*

Proof. It is clear that $\triangle = \triangle_0 + \Theta\varepsilon + \Omega\varepsilon^2 + (\triangle_1 - \triangle_0 - \Theta - \Omega)\varepsilon^3$ where $\Theta = 4\Theta_{a^3} + 27\Theta_{b^2}$ and $\Omega = 4\Omega_{a^3} + 27\Omega_{b^2}$. Then from the Proposition 2.5 we deduce the result. ∎

Corollary 3.2. *If $\triangle$ is invertible in $\mathbb{F}_q[\varepsilon]$, then we can talk about the elliptic curves $E_{\pi_0(a),\pi_0(b)}(\mathbb{F}_q)$ and $E_{\pi_1(a),\pi_1(b)}(\mathbb{F}_q)$ defined over the finite field $\mathbb{F}_q$ by*

$$E_{\pi_0(a),\pi_0(b)}(\mathbb{F}_q) = \big\{[x : y : z] \in \mathbb{P}^2(\mathbb{F}_q) |\ y^2z = x^3 + a_0xz^2 + b_0z^3\big\} \text{ and}$$
$$E_{\pi_1(a),\pi_1(b)}(\mathbb{F}_q) = \big\{[x : y : z] \in \mathbb{P}^2(\mathbb{F}_q) |\ y^2z = x^3 + \big(\textstyle\sum_{i=0}^3 a_i\big)xz^2 + (\sum_{i=0}^3 b_i)z^3\big\}.$$

Proposition 3.3. *Let X, Y and Z in $\mathbb{F}_q[\varepsilon]$, then $[X : Y : Z]$ is a point of $\mathbb{P}^2(\mathbb{F}_q[\varepsilon])$ if and only if $[\pi_i(X) : \pi_i(Y) : \pi_i(Z)]$ is a point of $\mathbb{P}^2(\mathbb{F}_q)$, where $i \in \{0, 1\}$.*

Proof. Suppose that $[X : Y : Z] \in \mathbb{P}^2(\mathbb{F}_q[\varepsilon])$, then there exist the triple $(\alpha, \beta, \gamma) \in (\mathbb{F}_q[\varepsilon])^3$ such that $\alpha X + \beta Y + \gamma Z = 1$. Hence, we have

$$\pi_0(\alpha)\pi_0(X) + \pi_0(\beta)\pi_0(Y) + \pi_0(\gamma)\pi_0(Z) = 1, \quad \text{and}$$
$$\pi_1(\alpha)\pi_1(X) + \pi_1(\beta)\pi_1(Y) + \pi_1(\gamma)\pi_1(Z) = 1$$

so $(\pi_0(X), \pi_0(Y), \pi_0(Z)) \neq (0, 0, 0)$ and $(\pi_1(X), \pi_1(Y), \pi_1(Z)) \neq (0, 0, 0)$, which proves that $[\pi_i(X) : \pi_i(Y) : \pi_i(Z)] \in \mathbb{P}^2(\mathbb{F}_q)$ for $i \in \{0, 1\}$.

Reciprocally, let $[\pi_i(X) : \pi_i(Y) : \pi_i(Z)] \in \mathbb{P}^2(\mathbb{F}_q)$ where $i \in \{0, 1\}$. suppose that $x_0 \not\equiv 0[p]$, then we distinguish between two cases of $x_0 + x_1 + x_2 + x_3$:

(a) $x_0 + x_1 + x_2 + x_3 \not\equiv 0[p]$, then X is invertible in $\mathbb{F}_q[\varepsilon]$, so the projective point $[X : Y : Z] \in \mathbb{P}^2(\mathbb{F}_q[\varepsilon])$.

(b) $x_0+x_1+x_2+x_3 \equiv 0[p]$, then $y_0+y_1+y_2+y_3 \not\equiv 0[p]$ or $z_0+z_1+z_2+z_3 \not\equiv 0[p]$.

1. if $y_0+y_1+y_2+y_3 \not\equiv 0[p]$, then
$x_0+x_1\varepsilon+x_2\varepsilon^2+(y_0+y_1+y_2+y_3-x_0-x_1-x_2)\varepsilon^3$
$=x_0+x_1\varepsilon+x_2\varepsilon^2-(x_0+x_1+x_2)\varepsilon^3+(y_0+y_1+y_2+y_3)\varepsilon^3$
$=X+\varepsilon^3Y\in(\mathbb{F}_q[\varepsilon])^\times$, so there exist $\Psi\in\mathbb{F}_q[\varepsilon]$:
$\Psi X+\varepsilon^3\Psi Y=1$, hence $[X:Y:Z]\in\mathbb{P}^2(\mathbb{F}_q[\varepsilon])$.
2. if $z_0+z_1+z_2+z_3 \not\equiv 0[p]$, then
$x_0+x_1\varepsilon+x_2\varepsilon^2+(z_0+z_1+z_2+z_3-x_0-x_1-x_2)\varepsilon^3$
$=x_0+x_1\varepsilon+x_2\varepsilon^2-(x_0+x_1+x_2)\varepsilon^3+(z_0+z_1+z_2+z_3)\varepsilon^3$
$=X+\varepsilon^3Z\in(\mathbb{F}_q[\varepsilon])^\times$, so there exist $\Phi\in\mathbb{F}_q[\varepsilon]$:
$\Phi X+\varepsilon^3\Phi Z=1$, hence $[X:Y:Z]\in\mathbb{P}^2(\mathbb{F}_q[\varepsilon])$.

In the case where $y_0\not\equiv 0[p]$ or $z_0\not\equiv 0[p]$, we follow the same proof. ∎

Proposition 3.4. *Let X,Y and Z in $\mathbb{F}_q[\varepsilon]$, if the point $[X:Y:Z]$ is a solution of the Weierstrass equation in $E_{a,b}(\mathbb{F}_q[\varepsilon])$, then $[\pi_i(X):\pi_i(Y):\pi_i(Z)]$ where $i\in\{0,1\}$ is a solution of the same equation in $E_{\pi_i(a),\pi_i(b)}(\mathbb{F}_q)$.*

Proof. From the Proposition 2.3 and the corollary 2.4, we have:

- $Y^2=y_0^2+\Theta_{Y^2}\varepsilon+\Omega_{Y^2}\varepsilon^2+\big(\big(\sum_{i=0}^3 y_i\big)^2-y_0^2-\Theta_{Y^2}-\Omega_{Y^2}\big)\varepsilon^3$
- $Z^2=z_0^2+\Theta_{Z^2}\varepsilon+\Omega_{Z^2}\varepsilon^2+\big(\big(\sum_{i=0}^3 z_i\big)^2-z_0^2-\Theta_{Z^2}-\Omega_{Z^2}\big)\varepsilon^3$
- $aX=a_0x_0+\Theta_{aX}\varepsilon+\Omega_{aX}\varepsilon^2+\big(\big(\sum_{i=0}^3 a_i\big)\big(\sum_{i=0}^3 x_i\big)-a_0x_0-\Theta_{aX}-\Omega_{aX}\big)\varepsilon^3$
- $Z^3=z_0^3+\Theta_{Z^3}\varepsilon+\Omega_{Z^3}\varepsilon^2+\big(\big(\sum_{i=0}^3 z_i\big)^3-z_0^3-\Theta_{Z^3}-\Omega_{Z^3}\big)\varepsilon^3$,

then

$$\begin{aligned}Y^2Z &= y_0^2z_0+\Theta_{Y^2Z}\varepsilon+\Omega_{Y^2Z}\varepsilon^2\\ &+\big(\big(\textstyle\sum_{i=0}^3 y_i\big)^2\big(\sum_{i=0}^3 z_i\big)-y_0^2z_0-\Theta_{Y^2Z}-\Omega_{Y^2Z}\big)\varepsilon^3\end{aligned}$$

$$X^3 = x_0^3+\Theta_{X^3}\varepsilon+\Omega_{X^3}\varepsilon^2+\big(\big(\textstyle\sum_{i=0}^3 x_i\big)^3-x_0^3-\Theta_{X^3}-\Omega_{X^3}\big)\varepsilon^3$$

$$\begin{aligned}aXZ^2 &= a_0x_0z_0^2+\Theta_{aXZ^2}\varepsilon+\Omega_{aXZ^2}\varepsilon^2\\ &+\big(\big(\textstyle\sum_{i=0}^3 a_i\big)\big(\sum_{i=0}^3 x_i\big)\big(\sum_{i=0}^3 z_i\big)^2-a_0x_0z_0^2-\Theta_{aXZ^2}-\Omega_{aXZ^2}\big)\varepsilon^3\end{aligned}$$

$$\begin{aligned}bZ^3 &= b_0z_0^3+\Theta_{bZ^3}\varepsilon+\Omega_{bZ^3}\varepsilon^2\\ &+\big(\big(\textstyle\sum_{i=0}^3 b_i\big)\big(\sum_{i=0}^3 z_i\big)^3-b_0z_0^3-\Theta_{bZ^3}-\Omega_{bZ^3}\big)\varepsilon^3\end{aligned}$$

hence $Y^2Z=X^3+aXZ^2+bZ^3$ if and only if

$$y_0^2z_0=x_0^3+a_0x_0z_0^2+b_0z_0^3$$

$$\Theta_{Y^2Z} = \Theta_{X^3} + \Theta_{aXZ^2} + \Theta_{bZ^3}$$

$$\Omega_{Y^2Z} = \Omega_{X^3} + \Omega_{aXZ^2} + \Omega_{bZ^3}$$

$$\begin{aligned}\big(\textstyle\sum_{i=0}^{3} y_i\big)^2\big(\textstyle\sum_{i=0}^{3} z_i\big) &= \big(\textstyle\sum_{i=0}^{3} x_i\big)^3 + \big(\textstyle\sum_{i=0}^{3} a_i\big)\big(\textstyle\sum_{i=0}^{3} x_i\big)\big(\textstyle\sum_{i=0}^{3} z_i\big)^2 \\ &\quad + \big(\textstyle\sum_{i=0}^{3} b_i\big)\big(\textstyle\sum_{i=0}^{3} z_i\big)^3\end{aligned}$$

which proves that for $i \in \{0,1\}$, $[\pi_i(X) : \pi_i(y) : \pi_i(Z)]$ is a solution of the Weierstrass equation in $E_{\pi_i(a),\pi_i(b)}(\mathbb{F}_q)$. ∎

Theorem 3.5. *Let $a = \tilde{a} + a_3\varepsilon^3$, $b = \tilde{b} + b_3\varepsilon^3$, $X = \tilde{X} + x_3\varepsilon^3$, $Y = \tilde{Y} + y_3\varepsilon^3$, and $Z = \tilde{Z} + z_3\varepsilon^3$, the elements of $\mathbb{F}_q[\varepsilon]$, which verified the equation of Weierstrass*

$$Y^2Z = X^3 + aXZ^2 + bZ^3,$$

then

$$\tilde{Y}^2\tilde{Z} = \tilde{X}^3 + \tilde{a}\tilde{X}\tilde{Z}^2 + \tilde{b}\tilde{Z}^3 + (D - (Ax_3 + By_3 + Cz_3))\varepsilon^3$$

where

$$\begin{cases} D = a_3(x_0+x_1+x_2)(z_0+z_1+z_2)^2 + b_3(z_0+z_1+z_2)^3 \\ \quad + 3x_3^2(x_0+x_1+x_2) + x_3^3 - y_3^2(z_0+z_1+z_2+z_3) \\ \quad + z_3^2((x_0+x_1+x_2+x_3)(a_0+a_1+a_2+a_3) \\ \quad + 3(z_0+z_1+z_2)(b_0+b_1+b_2+b_3)) \\ A = -3(x_0+x_1+x_2)^2 - (z_0+z_1+z_2)^2(a_0+a_1+a_2+a_3) \\ B = 2(y_0+y_1+y_2)(z_0+z_1+z_2+z_3) \\ C = -2(z_0+z_1+z_2)(x_0+x_1+x_2+x_3)(a_0+a_1+a_2+a_3) \\ \quad - 3(z_0+z_1+z_2)^2(b_0+b_1+b_2+b_3) + (y_0+y_1+y_2)^2. \end{cases}$$

Proof. We have

$$\begin{aligned} Y^2 &= \big(\tilde{Y} + y_3\varepsilon^3\big)^2 = \tilde{Y}^2 + 2\tilde{Y}y_3\varepsilon^3 + y_3^2\varepsilon^3 = \tilde{Y}^2 + \big(2y_3(y_0+y_1+y_2) + y_3^2\big)\varepsilon^3 \\ Y^2Z &= \big(\tilde{Y} + y_3\varepsilon^3\big)^2\big(\tilde{Z} + z_3\varepsilon^3\big) = \big(\tilde{Y}^2 + (2y_3(y_0+y_1+y_2) + y_3^2)\varepsilon^3\big)(\tilde{Z} + z_3\varepsilon^3) \\ &= \tilde{Y}^2\tilde{Z} + \big(z_3(y_0+y_1+y_2)^2 + 2y_3(y_0+y_1+y_2)(z_0+z_1+z_2+z_3) \\ &\quad + y_3^2(z_0+z_1+z_2+z_3)\big)\varepsilon^3 \\ X^3 &= \big(\tilde{X} + x_3\varepsilon^3\big)^3 = \tilde{X}^3 + 3\tilde{X}^2x_3\varepsilon^3 + 3\tilde{X}x_3^2\varepsilon^3 + x_3^3\varepsilon^3 \\ &= \tilde{X}^3 + \big(3\tilde{X}^2x_3 + 3\tilde{X}x_3^2 + x_3^3\big)\varepsilon^3 \\ &= \tilde{X}^3 + \big(3x_3(x_0+x_1+x_2)^2 + 3x_3^2(x_0+x_1+x_2) + x_3^3\big)\varepsilon^3 \\ aXZ^2 &= (\tilde{a} + a_3\varepsilon^3)(\tilde{X} + x_3\varepsilon^3)(\tilde{Z} + z_3\varepsilon^3)^2 \\ &= (\tilde{a} + a_3\varepsilon^3)(\tilde{X}\tilde{Z}^2 + (x_3(z_0+z_1+z_2)^2 \\ &\quad + 2z_3(z_0+z_1+z_2)(x_0+x_1+x_2+x_3) + z_3^2(x_0+x_1+x_2+x_3))\varepsilon^3) \end{aligned}$$

$$
\begin{aligned}
&= \tilde{a}\tilde{X}\tilde{Z}^2 + (x_3(z_0+z_1+z_2)^2(a_0+a_1+a_2+a_3)\\
&+ 2z_3(z_0+z_1+z_2)(x_0+x_1+x_2+x_3)(a_0+a_1+a_2+a_3)\\
&+ z_3^2(x_0+x_1+x_2+x_3)(a_0+a_1+a_2+a_3)\\
&+ a_3(x_0+x_1+x_2)(z_0+z_1+z_2)^2)\varepsilon^3\\
bZ^3 &= (\tilde{b}+b_3\varepsilon^3)(\tilde{Z}+z_3\varepsilon^3)^3\\
&= (\tilde{b}+b_3\varepsilon^3)(\tilde{Z}^3+(3z_3(z_0+z_1+z_2)^2+3z_3^2(z_0+z_1+z_2)+z_3^3)\varepsilon^3)\\
&= \tilde{b}\tilde{Z}^3+(3z_3(z_0+z_1+z_2)^2(b_0+b_1+b_2+b_3)\\
&+ 3z_3^2(z_0+z_1+z_2)(b_0+b_1+b_2+b_3)+b_3(z_0+z_1+z_2)^3)\varepsilon^3
\end{aligned}
$$

since $Y^2Z = X^3 + aXZ^2 + bZ^3$, then

$$\tilde{Y}^2\tilde{Z} = \tilde{X}^3 + \tilde{a}\tilde{X}\tilde{Z}^2 + \tilde{b}\tilde{Z}^3 + (D - (Ax_3 + By_3 + Cz_3))\varepsilon^3$$

where

$$
\begin{cases}
D = a_3(x_0+x_1+x_2)(z_0+z_1+z_2)^2 + b_3(z_0+z_1+z_2)^3\\
\quad + 3x_3^2(x_0+x_1+x_2) + x_3^3 - y_3^2(z_0+z_1+z_2+z_3)\\
\quad + z_3^2((x_0+x_1+x_2+x_3)(a_0+a_1+a_2+a_3)\\
\quad + 3(z_0+z_1+z_2)(b_0+b_1+b_2+b_3))\\
A = -3(x_0+x_1+x_2)^2 - (z_0+z_1+z_2)^2(a_0+a_1+a_2+a_3)\\
B = 2(y_0+y_1+y_2)(z_0+z_1+z_2+z_3)\\
C = -2(z_0+z_1+z_2)(x_0+x_1+x_2+x_3)(a_0+a_1+a_2+a_3)\\
\quad - 3(z_0+z_1+z_2)^2(b_0+b_1+b_2+b_3) + (y_0+y_1+y_2)^2
\end{cases}
$$

then, we deduce the theorem. ∎

Corollary 3.6. *If $D = Ax_3 + By_3 + Cz_3$, then $\tilde{a}$, $\tilde{b}$, $\tilde{X}$, $\tilde{Y}$, and $\tilde{Z}$ are satisfy the equation of Weierstrass $\tilde{Y}^2\tilde{Z} = \tilde{X}^3 + \tilde{a}\tilde{X}\tilde{Z}^2 + \tilde{b}\tilde{Z}^3$.*

From the Propositions 3.1, 3.3, and 3.4, we deduce the theorem.

Theorem 3.7. *Let X, Y and Z in $\mathbb{F}_q[\varepsilon]$. If $[X : Y : Z] \in E_{a,b}(\mathbb{F}_q[\varepsilon])$, then $[\pi_i(X) : \pi_i(Y) : \pi_i(Z)] \in E_{\pi_i(a),\pi_i(b)}(\mathbb{F}_q)$ where $i \in \{0, 1\}$.*

Theorem 3.8. *The set $E_{a,b}(\mathbb{F}_q[\varepsilon])$ is an abelian group, written additively, and has $[0 : 1 : 0]$ as its zero element, and for all $P = [X_1 : Y_1 : Z_1]$ and $Q = [X_2 : Y_2 : Z_2]$ in $E_{a,b}(\mathbb{F}_q[\varepsilon])$ we have $P + Q = [X_3 : Y_3 : Z_3]$, where:*

- *If $P = Q$, then*

$$\begin{aligned}
X_3 &= (Y_1Y_2 - a(X_1Z_2 + X_2Z_1) - 3bZ_1Z_2)(X_1Y_2 + X_2Y_1) \\
&+ (a^2Z_1Z_2 - 3b(X_1Z_2 + X_2Z_1) - aX_1X_2)(Y_1Z_2 + Y_2Z_1), \\
Y_3 &= Y_1^2Y_2^2 + a(3X_1^2X_2^2 - a^2Z_1^2Z_2^2) + 9b(X_1^2X_2Z_2 + X_1X_2^2Z_1 - bZ_1^2Z_2^2) \\
&- a^2(X_2^2Z_1^2 + 2X_1X_2Z_1Z_2) - 3ab(X_1Z_1Z_2^2 + X_2Z_1^2Z_2), \\
Z_3 &= (3X_1X_2 + aZ_1Z_2)(X_1Y_2 + X_2Y_1) \\
&+ (Y_1Y_2 + a(X_1Z_2 + X_2Z_1) + 3bZ_1Z_2)(Y_1Z_2 + Y_2Z_1).
\end{aligned}$$

- *If $P \neq Q$, then*

$$\begin{aligned}
X_3 &= (X_1Y_2 - X_2Y_1)(Y_1Z_2 + Y_2Z_1) + (Y_1Y_2 - 3bZ_1Z_2)(X_1Z_2 - X_2Z_1) \\
&+ a(X_2^2Z_1^2 - X_1^2Z_2^2), \\
Y_3 &= (3X_1X_2 + aZ_1Z_2)(X_2Y_1 - X_1Y_2) \\
&+ (a(X_1Z_2 + X_2Z_1) + 3bZ_1Z_2 - Y_1Y_2)(Y_1Z_2 - Y_2Z_1), \\
Z_3 &= (aZ_1Z_2 + 3X_1X_2)(X_1Z_2 - X_2Z_1) - Y_1^2Z_2^2 + Y_2^2Z_1^2.
\end{aligned}$$

Proof. Just like on a field, an elliptical curve can also be defined on a ring under some conditions. The conditions:

(i) ($6 \in R^*$), as Lenstra indicates in [6] is not needed for this definition, but just to use a precise form of the elliptic curve equation.

(ii) (any projective R-module of rank 1 is free), is on the other hand necessary, it is verified by the finished rings. This is therefore a sufficient condition to be able to define an elliptic curve over a ring, while preserving the group law defined geometrically by the secant and the tangent.

So, using the explicit formulae of Bosma and Lenstra article, see [1] [page: 236–238], we prove the theorem. ∎

Corollary 3.9. *For $i \in \{0, 1\}$ The mappings φ_i given by*

$$\begin{aligned}
\varphi_i : E_{a,b}(\mathbb{F}_q[\varepsilon]) &\longrightarrow E_{\pi_i(a),\pi_i(b)}(\mathbb{F}_q) \\
[X : Y : Z] &\longmapsto [\pi_i(X) : \pi_i(Y) : \pi_i(Z)]
\end{aligned}$$

is well defined.

Proof. Let $[X : Y : Z] \in E_{a,b}(\mathbb{F}_q[\varepsilon])$. From the previous theorem 3.7, we have $[\pi_i(X) : \pi i(Y) : \pi_i(Z)] \in E_{\pi_i(a),\pi_i(b)}(\mathbb{F}_q)$ where $i \in \{0, 1\}$.

If $[X : Y : Z] = [X' : Y' : Z']$, then there exist $\Phi \in (\mathbb{F}_q[\varepsilon])^\times$ such that $X' = \Phi X$, $Y' = \Phi Y$ and $Z' = \Phi Z$, then

$$\begin{aligned}
\varphi_i([X' : Y' : Z']) &= [\pi_i(X') : \pi_i(Y') : \pi_i(Z')] \\
&= [\pi_i(\Phi X) : \pi_i(\Phi Y) : \pi_i(\Phi Z)]
\end{aligned}$$

$$\begin{aligned}
&= \underbrace{[\pi_i(\Phi)\pi_i(X) : \pi_i(\Phi)\pi_i(Y) : \pi_i(\Phi)\pi_i(Z)]}_{\pi_i(\Phi)\in\mathbb{F}_q^*} \\
&= [\pi_i(X) : \pi_i(Y) : \pi_i(Z)] \\
&= \varphi_i([X : Y : Z]).
\end{aligned}$$

■

Corollary 3.10. *φ_i is a morphism of group where $i \in \{0, 1\}$.*

Proof. Let $[X_1 : Y_1 : Z_1]$, $[X_2 : Y_2 : Z_2] \in E_{a,b}(\mathbb{F}_q[\varepsilon])$

$$\begin{aligned}
\varphi_i([X_1 : Y_1 : Z_1] + [X_2 : Y_2 : Z_2]) &= \varphi_i([X_3 : Y_3 : Z_3]) \\
&= [\pi_i(X_3) : \pi_i(Y_3) : \pi_i(Z_3)],
\end{aligned}$$

by the Theorem 3.8 and π_i is a morphism of ring we have

$$\begin{aligned}
[\pi_i(X_3) : \pi_i(Y_3) : \pi_i(Z_3)] &= [\pi_i(X_1) : \pi_i(Y_1) : \pi_i(Z_1)] + [\pi_i(X_2) : \pi_i(Y_2) : \pi_i(Z_2)] \\
&= \varphi_i([X_1 : Y_1 : Z_1]) + \varphi_i([X_2 : Y_2 : Z_2]),
\end{aligned}$$

thus

$$\varphi_i([X_1 : Y_1 : Z_1] + [X_2 : Y_2 : Z_2]) = \varphi_i([X_1 : Y_1 : Z_1]) + \varphi_i([X_2 : Y_2 : Z_2]).$$

Then φ_i is a morphism of group where $i \in \{0, 1\}$. ■

Corollary 3.11. *φ_0 is a surjective mapping.*

Proof. Let $[x : y : z] \in E_{\pi_0(a),\pi_0(b)}(\mathbb{F}_q)$, then

- If $y \not\equiv 0[p]$, then $[x : y : z] \sim [x : 1 : z]$ hence $[x(1 - \varepsilon - \varepsilon^2 + \varepsilon^3) : 1 : z(1 - \varepsilon - \varepsilon^2 + \varepsilon^3)]$ is an antecedent of $[x : 1 : z]$.
- If $y \equiv 0[p]$, then $z \not\equiv 0[p]$ and $[x : y : z] \sim [x : 0 : 1]$ hence $[x(1- \varepsilon- \varepsilon^2 + \varepsilon^3) : \varepsilon + \varepsilon^2 + \varepsilon^3 : 1- \varepsilon-\varepsilon^2 + \varepsilon^3]$ is a antecedent of $[x : 0 : 1]$. ■

Corollary 3.12. *φ_1 is a surjective mapping.*

Proof. Let $[x : y : z] \in E_{\pi_1(a),\pi_1(b)}(\mathbb{F}_q)$, then

- If $y \not\equiv 0[p]$, then $[x : y : z] \sim [x : 1 : z]$ hence $[x(\varepsilon - \varepsilon^2 + \varepsilon^3) : 1 : z(\varepsilon - \varepsilon^2 + \varepsilon^3)]$ is a antecedent of $[x : 1 : z]$.
- If $y \equiv 0[p]$, then $z \not\equiv 0[p]$ and $[x : y : z] \sim [x : 0 : 1]$ hence $[x(\varepsilon - \varepsilon^2 + \varepsilon^3) : 1 + \varepsilon - \varepsilon^2 - \varepsilon^3 : \varepsilon - \varepsilon^2 + \varepsilon^3]$ is an antecedent of $[x : 0 : 1]$. ■

Lemma 3.13. *The kernel of φ_i is a sub-group such that*

$$\ker\varphi_i = \left\{[X:Y:Z] \in E_{a,b}(\mathbb{F}_q[\varepsilon]) \mid [\pi_i(X):\pi_i(Y):\pi_i(Z)] = [0:1:0]\right\}$$

where $i \in \{0,1\}$.

Proposition 3.14. *The mapping* $\bar{\varphi}_i$ *where* $i \in \{0,1\}$ *given by*

$$\begin{aligned}\bar{\varphi}_i : E_{a,b}(\mathbb{F}_q[\varepsilon])/\ker\varphi_i &\longrightarrow \operatorname{Im}\varphi_i = E_{\pi_i(a),\pi_i(b)}(\mathbb{F}_q)\\ [X:Y:Z] + \ker\varphi_i &\longmapsto [\pi_i(X):\pi_i(Y):\pi_i(Z)]\end{aligned}$$

is an isomorphism of group.

Proof. Let $\bar{P},\ \bar{Q} \in E_{a,b}(\mathbb{F}_q[\varepsilon])/\ker\varphi_i$ such that $\bar{P} = P + \ker\varphi_i$ and $\bar{Q} = Q + \ker\varphi_i$ where $P = [X_1 : Y_1 : Z_1]$ and $Q = [X_2 : Y_2 : Z_2]$. For all $i \in \{0,1\}$ we have

$$\begin{cases}\bar{\varphi}_i(\bar{P}) = \varphi_i(P)\\ \bar{\varphi}_i(\bar{Q}) = \varphi_i(Q)\end{cases}$$

$\bar{\varphi}_i$ is well defined:

$$\begin{aligned}\bar{P} = \bar{Q} &\Leftrightarrow P - Q \in \ker\varphi_i\\ &\Leftrightarrow \varphi_i(P-Q) = [0:1:0]\\ &\Leftrightarrow \varphi_i(P) - \varphi_i(Q) = [0:1:0] \ (\varphi_i \textit{ is a morphism group})\\ &\Leftrightarrow \varphi_i(P) = \varphi_i(Q)\\ &\Leftrightarrow \bar{\varphi}_i(\bar{P}) = \bar{\varphi}_i(\bar{Q})\end{aligned}$$

$\bar{\varphi}_i$ is a morphism of group:

$$\begin{aligned}\bar{\varphi}_i(\bar{P}+\bar{Q}) &= \bar{\varphi}_i(\overline{P+Q})\\ &= \varphi_i(P+Q)\\ &= \varphi_i(P) + \varphi_i(Q)\\ &= \bar{\varphi}_i(\bar{P}) + \bar{\varphi}_i(\bar{Q})\end{aligned}$$

$\bar{\varphi}_i$ is a surjective:

$$\begin{aligned}&\text{If } M \in \operatorname{Im}\varphi_i = E_{\pi_i(a),\pi_i(b)}(\mathbb{F}_q)\\ &\exists P \in E_{a,b}(\mathbb{F}_q[\varepsilon]) \text{ such that } M = \varphi_i(P)\\ &\exists \bar{P} \in E_{a,b}(\mathbb{F}_q[\varepsilon])/\ker\varphi_i \text{ such that } M = \bar{\varphi}_i(\bar{P})\end{aligned}$$

$\bar{\varphi}_i$ is a injective:

$$\begin{aligned}\bar{\varphi}_i(\bar{P}) = \bar{\varphi}_i(\bar{Q}) &\Leftrightarrow \varphi_i(P) = \varphi_i(Q)\\ &\Leftrightarrow \varphi_i(P) - \varphi_i(Q) = [0:1:0]\\ &\Leftrightarrow \varphi_i(P-Q) = [0:1:0]\\ &\Leftrightarrow P - Q \in \ker\varphi_i\\ &\Leftrightarrow \bar{P} = \bar{Q}.\end{aligned}$$

Finally, $E_{a,b}(\mathbb{F}_q[\varepsilon])/\ker\varphi_i \cong \operatorname{Im}\varphi_i$ for all $i \in \{0,1\}$. ∎

Corollary 3.15. *$\bar{\varphi_i}$ is an isomorphism for $i \in \{0,1\}$, in particular we have*

$$\begin{aligned}\frac{card(E_{a,b}(\mathbb{F}_q[\varepsilon]))}{card(\ker\varphi_i)} &= card\big(E_{a,b}(\mathbb{F}_q[\varepsilon])\big/\ker\varphi_i) = card(\operatorname{Im}\varphi_i)\\ &= card\big(E_{\pi_i(a),\pi_i(b)}(\mathbb{F}_q)\big).\end{aligned}$$

In the rest of this article, we will classify the elements of the elliptic curve $E_{a,b}(\mathbb{F}_q[\varepsilon])$ into three types, depending on whether the third projective coordinate Z is invertible or not. The result is in the following proposition.

Proposition 3.16. *Every element of the elliptic curve $E_{a,b}(\mathbb{F}_q[\varepsilon])$ has one of the forms:*

1. $[X : Y : 1]$, *where* $X, Y \in \mathbb{F}_q[\varepsilon]$.
2. $\big[x_1\varepsilon + x_2\varepsilon^2 + x_3\varepsilon^3 : 1 : z_1\varepsilon + z_2\varepsilon^2 + z_3\varepsilon^3\big]$
   such that $[x_1 + x_2 + x_3 : 1 : z_1 + z_2 + z_3] \in E_{\pi_1(a),\pi_1(b)}(\mathbb{F}_q)$.
3. $\big[x_1\varepsilon + x_2\varepsilon^2 + x_3\varepsilon^3 : 1 + y_1\varepsilon + y_2\varepsilon^2 - (1 + y_1 + y_2)\varepsilon^3 : z_1\varepsilon + z_2\varepsilon^2 + z_3\varepsilon^3\big]$
   such that $[x_1 + x_2 + x_3 : 0 : z_1 + z_2 + z_3] \in E_{\pi_1(a),\pi_1(b)}(\mathbb{F}_q)$.
4. $\big[x_0 + x_1\varepsilon + x_2\varepsilon^2 - \sum_{i=0}^{2} x_i\varepsilon^3 : 1 : z_0 + z_1\varepsilon + z_2\varepsilon^2 - \sum_{i=0}^{2} z_i\varepsilon^3\big]$
   such that $[x_0 : 1 : z_0] \in E_{\pi_0(a),\pi_0(b)}(\mathbb{F}_q)$.
5. $\big[x_0 + x_1\varepsilon + x_2\varepsilon^2 - \sum_{i=0}^{2} x_i\varepsilon^3 : y_1\varepsilon + y_2\varepsilon^2 + y_3\varepsilon^3 : z_0 + z_1\varepsilon + z_2\varepsilon^2 - \sum_{i=0}^{2} z_i\varepsilon^3\big]$
   such that $y_1 + y_2 + y_3 \not\equiv 0[p]$ *and* $[x_0 : 0 : 1] \in E_{\pi_0(a),\pi_0(b)}(\mathbb{F}_q)$.

Proof. Let $\Gamma = [X : Y : Z] \in E_{a,b}(\mathbb{F}_q[\varepsilon])$, we have three cases of third projective coordinate Z:

1. If Z is invertibe, then $[X : Y : Z] \sim [X : Y : 1]$.
2. If $Z = z_1\varepsilon + z_2\varepsilon^2 + z_3\varepsilon^3$ where $(z_1, z_2, z_3) \in (\mathbb{F}_q)^3$,
   then $\varphi_0([X : Y : Z]) = [x_0 : y_0 : 0]$ so $x_0 \equiv 0[p]$ and $y_0 \not\equiv 0[p]$, hence $[X : Y : Z] = \big[x_1\varepsilon + x_2\varepsilon^2 + x_3\varepsilon^3 : 1 + y_1\varepsilon + y_2\varepsilon^2 + y_3\varepsilon^3 : z_1\varepsilon + z_2\varepsilon^2 + z_3\varepsilon^3\big]$ and there are two sub-cases of $y_1 + y_2 + y_3 \in \mathbb{F}_q$:
   - $y_1 + y_2 + y_3 \not\equiv -1[p]$, then $1 + y_1\varepsilon + y_2\varepsilon^2 + y_3\varepsilon^3$ is invertible in $\mathbb{F}_q[\varepsilon]$, so we have: $[X : Y : Z] \sim \big[x_1\varepsilon + x_2\varepsilon^2 + x_3\varepsilon^3 : 1 : z_1\varepsilon + z_2\varepsilon^2 + z_3\varepsilon^3\big]$, where $[x_1 + x_2 + x_3 : 1 : z_1 + z_2 + z_3] \in E_{\pi_1(a),\pi_1(b)}(\mathbb{F}_q)$.
   - $y_1 + y_2 + y_3 \equiv -1[p]$, then $1 + y_1\varepsilon + y_2\varepsilon^2 - (1 + y_1 + y_2)\varepsilon^3$ is not invertible in $\mathbb{F}_q[\varepsilon]$, so we have $[X : Y : Z]$ is equal to $\big[x_1\varepsilon + x_2\varepsilon^2 + x_3\varepsilon^3 : 1 + y_1\varepsilon + y_2\varepsilon^2 - (1 + y_1 + y_2)\varepsilon^3 : z_1\varepsilon + z_2\varepsilon^2 + z_3\varepsilon^3\big]$, where $[x_1 + x_2 + x_3 : 0 : z_1 + z_2 + z_3] \in E_{\pi_1(a),\pi_1(b)}(\mathbb{F}_q)$.
3. If $Z = z_0 + z_1\varepsilon + z_2\varepsilon^2 - (z_0 + z_1 + z_2)\varepsilon^3$ where $(z_0, z_1, z_2) \in (\mathbb{F}_q)^3$, then $\varphi_1([X : Y : Z]) = [x_0 + x_1 + x_2 + x_3 : y_0 + y_1 + y_2 + y_3 : 0]$,
   so $x_0 + x_1 + x_2 + x_3 \equiv 0[p]$ and $y_0 + y_1 + y_2 + y_3 \not\equiv 0[p]$, hence $[X : Y : Z]$

is equal to $\left[x_0+x_1\varepsilon+x_2\varepsilon^2-\sum_{i=0}^{2}x_i\varepsilon^3 : y_0+y_1\varepsilon+y_2\varepsilon^2+y_3\varepsilon^3 : z_0+z_1\varepsilon+z_2\varepsilon^2-\sum_{i=0}^{2}z_i\varepsilon^3\right]$, so we have two sub-cases of $y_0\in\mathbb{F}_q$:

- $y_0\not\equiv 0[P]$, then $y_0+y_1\varepsilon+y_2\varepsilon^2+y_3\varepsilon^3$ is invertible in $\mathbb{F}_q[\varepsilon]$, then $[X:Y:Z]\sim\left[x_0+x_1\varepsilon+x_2\varepsilon^2-\sum_{i=0}^{2}x_i\varepsilon^3 : 1 : z_0+z_1\varepsilon+z_2\varepsilon^2-\sum_{i=0}^{2}z_i\varepsilon^3\right]$, where $[x_0:1:z_0]\in E_{\pi_0(a),\pi_0(b)}(\mathbb{F}_q)$.
- $y_0\equiv 0[P]$, then $Y=y_1\varepsilon+y_2\varepsilon^2+y_3\varepsilon^3$ is not invertible in $\mathbb{F}_q[\varepsilon]$, so we have: $[X:Y:Z]$ is equal to $\left[x_0+x_1\varepsilon+x_2\varepsilon^2-\sum_{i=0}^{2}x_i\varepsilon^3 : y_1\varepsilon+y_2\varepsilon^2+y_3\varepsilon^3 : z_0+z_1\varepsilon+z_2\varepsilon^2-\sum_{i=0}^{2}z_i\varepsilon^3\right]$, where $[x_0:0:z_0]\in E_{\pi_0(a),\pi_0(b)}(\mathbb{F}_q)$, then necessary $z_0\not\equiv 0[p]$ and $[X:Y:Z]=\left[x_0+x_1\varepsilon+x_2\varepsilon^2-\sum_{i=0}^{2}x_i\varepsilon^3 : y_1\varepsilon+y_2\varepsilon^2+y_3\varepsilon^3 : 1+\alpha\varepsilon+\beta\varepsilon^2-(1+\alpha+\beta)\varepsilon^3\right]$, where $y_1+y_2+y_3\not\equiv 0[p]$ and $[x_0:0:1]\in E_{\pi_0(a),\pi_0(b)}(\mathbb{F}_q)$.

Which proves the proposition. ∎

4. Conclusion

In this paper, we have studied the elliptic curve over the non local ring $\mathbb{F}_q[\varepsilon]$, $\varepsilon^4=\varepsilon^3$ of the characteristic $p\neq 2,3$. And we have given a classification of the elements in $E_{a,b}(\mathbb{F}_q[\varepsilon])$ using two elliptic curves over the finite field $\mathbb{F}_q$ which they are $E_{\pi_0(a),\pi_0(b)}(\mathbb{F}_q)$ and $E_{\pi_1(a),\pi_1(b)}(\mathbb{F}_q)$.

Acknowledgements

The authors are deeply gratful to the referees and the editors for their kind comments on improving the presentation of this paper.

References

[1] W. Bosma and H.W. Lenstra, *Complete System of Two Addition Laws for Elliptic Curves*, J. Number Theory **53** (1995) 229–240. https://doi.org/10.1006/jnth.1995.1088

[2] A. Boulbot, A. Chillali and A. Mouhib, *Elliptic curves over the ring* $\mathbb{F}_q[e]$, $e^3=e^2$, Gulf J. Math. **4** (2016) 123–129.

[3] A. Boulbot, A. Chillali and A. Mouhib, *Elliptic curves over the ring R*, Boletim da Sociedade Paranaense de Matematica **38** (2017) 193–201. https://doi.org/10.5269/bspm.v38i3.39868

[4] A. Boulbot, A. Chillali and A. Mouhib, *Elliptic curve over a finite ring generated by* 1 *and an idempotent element* ε *with coefficients in the finite field* $\mathbb{F}_{3^d}$, Boletim da Sociedade Paranaense de Matematica (2018) 1–19. https://doi.org/10.5269/bspm.43654

[5] A. Chillali, *Elliptic Curves of the Ring* $\mathbb{F}_q[\varepsilon]$, $\varepsilon^n=0$, Internat. Math. **6** (2011) 1501–1505.

[6] H.W. Lenstra, Jr., *Elliptic curves and number-theoretic algorithms* (Proceedings of the International Congress of Mathematicians, Berkely, California, USA, 1986).

[7] N. Koblitz, *Elliptic curve cryptosystems*, Math. Comp. **48** (1987) 203–209. https://doi.org/10.1090/S0025-5718-1987-0866109-5

[8] V. Miller, *Use of elliptic curves in cryptography*, Advanced cryptology-CRYPTO'85 **218** (1986) 417–426. https://doi.org/10.1007/3-540-39799-X_−31

[9] J.H. Silverman, *Advanced topics in the arithmetic of elliptic curves* (Springer-Verlag, 1994). https://doi.org/10.1007/978-1-4612-0851-8

[10] M. Virat, *Courbe elliptique sur un anneau et applications cryptographiques*, Doctoral thesis (Universite Nice-Sophia Antipolis, Nice, France, 2009).

Received 8 May 2020
Revised 6 September 2020
Accepted 6 September 2020