Elliptic curve on a family of finite ring

MOHAMMED SAHMOUDI
Ibn Tofail University
Department of Computer Science,
Logistics and Mathematics
ENSA, BP 242, University Street, Kenitra
Morocco
mohammed.sahmoudi@uit.ac.ma

ABDELHAKIM CHILLALI
Sidi Mohamed Ben Abdellah University
Polydisciplinary Faculty,
Engineering sciences laboratory
Oujda Road, B.P. 1223 Taza
Morocco
abdelhakim.chillali@usmba.ac.ma

Abstract: Let $L/\mathbb{Q}$ be a Sextic extension, namely $L = \mathbb{Q}(\sqrt{d}, \beta)$ which is a rational quadratic over a pure cubic subfield $K = \mathbb{Q}(\beta)$ where d is a rational square free integer and β is a root of monic irreducible polynomial of degree 3. We are interested in finding a commutative and associative ring denoted by $\mathbb{Z}_q[\sqrt{d}, \beta]$ using the integral closure O_L of sextic extension L. Furthermore, we study the elliptic curve over this ring. Consequently, we will prove the following principal result:

$$E^q_{t,s}(\alpha, \beta) \cong \mathbb{F}^5_q \oplus E^q_{a_0,b_0}.$$

Key–Words: Integral basis, Finite ring, Local ring, Elliptic curve.

1 Introduction

The theory of elliptic curves is distinguished by its diversity of the methods that have been used in its study. The idea to examine and make sense to elliptic curve over a local commutative ring was started by Marie Virat see [10], she has defined the elliptic curve over the ring $\mathbb{F}_p[X]/(X^2)$, where p is a prime number $\neq 2$ *and* 3. His work has been generalized in [1] for the ring $\mathbb{F}_p[X]/(X^n)$ after successive works on rings of characteristic 3 [4] and 2 [3]. Silverman, Joseph H. [5], treats the arithmetic approach in its modern formulation, through the use of basic algebraic number theory and algebraic geometry.
The purpose of this paper is to highlight a complete study of elliptic curve over the integral closure O_L of a family of sextic number field, namely $L = \mathbb{Q}(\sqrt{d}, \beta)$ which is a rational quadratic over a pure cubic field $K = \mathbb{Q}(\beta)$ where d is a rational square free integer and β is a root of monic irreducible polynomial of degree 3.

2 Computing an integral basis of O_L

Let A be a dedekind ring, the ideal $\mathfrak{I}$ of A is a said to be square free in A if $\nu_{\mathfrak{p}}(\mathfrak{I}) \leq 1$ for a fixed prime ideal $\mathfrak{p}$ in A. An element a in A is said a square free element if the principal ideal aA is a square free ideal of R, which implies that $a \in A - A^2$.

For each prime p and each non zero algebraic integer n, $\nu_p(n)$ denotes the greatest nonnegative integer l such that p^l divides n.

Let P be any polynomial in $A[X]$. S_P denote the set of all prime square divisors of $discP$ (The discriminant of P):

$$S_P = \{\, \mathfrak{p} \in specA \mid \mathfrak{p}^2 divides\, discP \,\}.$$

First, we recall the result that gives necessary and sufficient conditions for an extension L/K to be monogenic.

Theorem 1. *Let A be a Dedekind ring, K its quotient field, L a finite separable extension of K, O_L the integral closure of A in L, $\alpha \in O_L$ a primitive element of L, and $P(X) \in A[X]$ the monic irreducible polynomial of α over A. For a fixed prime ideal $\mathfrak{p}$ of A, let the decomposition of P into monic irreducible polynomials in $A/\mathfrak{p}[X]$ take the form*

$$\overline{P(X)} = \prod_{i=1}^{r} \overline{P_i}^{e_i}(X) \in A/\mathfrak{p}[X]. \tag{1}$$

For $i = 1, ..., r$, let $P_i \in A[X]$ be a monic lift of P_i, set

$$\begin{aligned} G(X) &= \prod_{1 \leq i \leq r, e_i \geq 2} P_i(X), \\ H(X) &= \prod_{i=1}^{r} P_i^{e_i}(X)/G(X), \end{aligned} \tag{2}$$

where the empty product is to mean that $G(X) = 1$, and let $P(X) = G(X)H(X) + aT(X)$ for some $T(X) \in A[X]$ and $a \in \mathfrak{p} \setminus \mathfrak{p}^2$. Then, If $disc_A(P)$ is not square free, then the following are equivalent:

1. *$\{1, \alpha, \alpha^2\}$ is a basis for O_L over A (we say that α is a PBG).*
2. *For any prime ideal $\mathfrak{p} \in S_P$, either (P is square free in $A/\mathfrak{p}[X]$) or (P is not square free in $A/\mathfrak{p}[X]$ and in this case $T \neq 0 \, modulo \, \mathfrak{p}$ and $\nu_{\mathfrak{p}}(Res(P, G)) = deg(G)$).*

Proof: See (Theorem 3.1. [7]).

Secondly, We give a sufficient condition for relative quadratic extension to have PBG.

Theorem 2. *Let A be a Dedekind ring with quotient field K. Let $L = K(\alpha)$ be a pure quadratic extension of K, where α is a root of a monic irreducible polynomial $P(X) = X^2 - d \in A[X]$. Suppose that $\upsilon_{\mathfrak{p}}(d) = 1$ for all prime divisors $\mathfrak{p}$ such that $\mathfrak{p}/2d$. Then α is a PBG of L/K.*

Proof: Let $\mathfrak{p} \in S_P$. As $\text{disc}_A(P) = 4dA$, then $\mathfrak{p}|4d$ yields $\upsilon_{\mathfrak{p}}(2A) + \upsilon_{\mathfrak{p}}(2dA) \geq 1$. It is clear that $\upsilon_{\mathfrak{p}}(2dA) \geq 1$ otherwise, we must have $\upsilon_{\mathfrak{p}}(2A) \geq 1$ which contradicts the fact that $\mathfrak{p}$ does not divides $2dA$ and hence $\mathfrak{p}|2d$. Now with the supposition $\upsilon_{\mathfrak{p}}(d) = 1$, reducing P modulo $\mathfrak{p}$ yields $\overline{P(X)} = \overline{X^2}$. Then, by keeping the notation of Theorem 1, we have,

$$P(X) = G(X)H(X) + d.T(X)$$

with $G(X) = H(X) = X$ and $T(X) = 1$. Moreover, $Res_A(X^2 - d, X) = dA$. Then

$$\nu_{\mathfrak{p}}(Res_A(X^2 - d, X)) = \nu_{\mathfrak{p}}(dA) = 1.$$

So α is a PBG of O_L over O_K.

Finally, in the following result we provides an intrinsic characterization to construct an integral basis of a sextic extension with a non-pure and monogenic cubic subfield.

Theorem 3. *For a given square free integral integer d. Let α defined by*

$$\alpha = \begin{cases} \sqrt{d} & \text{if } d \equiv 2, 3 \bmod 4, \\ \frac{1+\sqrt{d}}{2}, & \text{if } d \equiv 1 \bmod 4. \end{cases} \tag{3}$$

Let $K = \mathbb{Q}(\beta)$ be a non-pure and monogenic cubic field, where β is a root of a monic irreducible polynomial

$$T(X) = X^3 - aX + b \in \mathbb{Z}[X]$$

Let $L = \mathbb{Q}(\alpha, \beta)$ be a pure quadratic extension of K, where α is a root of a monic irreducible polynomial $P(X) = X^2 - d \in O_K$. Suppose that the p-adic valuation υ_p of b equals to 1 ($\upsilon_p(b) = 1$), for all prime integer p in $\mathbb{Z}$. Then the sextic field $L = \mathbb{Q}(\alpha, \beta)$ has an integral basis given by

$$\mathfrak{B} = \{1, \alpha, \beta, \beta^2, \alpha\beta, \alpha\beta^2\}.$$

To prove this theorem, we first remind the lemma:

Lemma 4. *(see [7, Lemma 3.2.]) Let $A \subseteq B \subseteq C$ be rings. If B is finitely generated as an A-module, and C is finitely generated as a B-module, then C is finitely generated as an A-module. Moreover if $\{\alpha_1, ..., \alpha_n\}$ is a basis for B as an A-module, and $\{\beta_1, ..., \beta_m\}$ is a basis for C as a B-module, then $\{\alpha_i\beta_k \, 1 \leq i \leq n \, ; 1 \leq j \leq m$ form a basis of C as an A-module.*

Proof: of Theorem 3. Indeed $B = \{1, \beta, \beta^2\}$ is an integral basis of K by [6, Theorem 5.1.], therefore we use Lemma 4 and 2.

We are interested in finding a commutative and associative ring denoted by $\mathbb{Z}_q[\sqrt{d}, \beta]$ from the integral closure O_L of sextic extension L. Furthermore, we study the elliptic curve over this ring. Consequently, we will prove the following principal result:

$$E^q_{t,s}(\alpha, \beta) \cong \mathbb{F}^q_5 \oplus E^q_{a_0,b_0}.$$

3 A new structure on the ring O_L

In this section we introduce a new commutative structure on the algebraic closure $O_L = \mathbb{Z}[\alpha, \beta]$ unlike to the non-commutative law introduced in [8]. In what follows, $\mathbb{D}_{\mathfrak{p}}(a, d)$ stands for all communs primes divisors of a and d.
Let $X, Y \in O_L$ given by:

$$\begin{aligned} X &= x_0 + x_1\alpha + x_2\beta + x_3\beta^2 + x_4\alpha\beta + x_5\alpha\beta^2, \\ Y &= y_0 + y_1\alpha + y_2\beta + y_3\beta^2 + y_4\alpha\beta + y_5\alpha\beta^2, \end{aligned} \tag{4}$$

Where $(x_i)_{0 \leq i \leq 5}$ and $(x_i)_{0 \leq i \leq 5}$ are in $\mathbb{Z}$

We define on the field L the following structure:

$$\begin{aligned} X + Y &= s_0 + s_1\alpha + s_2\beta + s_3\beta^2 + s_4\alpha\beta + s_5\alpha\beta^2, \\ X \, . \, Y &= p_0 + p_1\alpha + p_2\beta + p_3\beta^2 + p_4\alpha\beta + p_5\alpha\beta^2, \end{aligned} \tag{5}$$

where

$$\begin{aligned}
&s_i = x_i + y_i, \quad \text{for all } i \in \{0,1,2,3,4,5\},\\
&p_0 = x_0y_0 + ax_2y_3 + dax_5y_4 + dx_1y_1 + ax_3y_2\\
&\quad + dax_4y_5,\\
&p_1 = ax_4y_3 + ax_3y_4 + x_0y_1 + ax_5y_2 + x_1y_0 + ax_2y_5,\\
&p_2 = dx_1y_4 + dx_4y_1 + x_2y_0 + x_0y_2 + dax_5y_5 + ax_3y_3,\\
&p_3 = dx_5y_1 + x_3y_0 + dx_1y_5 + dx_4y_4 + x_0y_3 + x_2y_2,\\
&p_4 = x_2y_1 + x_4y_0 + x_0y_4 + ax_5y_3 + ax_3y_5 + x_1y_2,\\
&p_5 = x_4y_2 + x_0y_5 + x_5y_0 + x_2y_4 + x_1y_3 + x_3y_1\,.
\end{aligned} \tag{6}$$

The following construction was motivated by [8] and [2]. Let $q \in \mathbb{D}_{\mathfrak{p}}(a,d)$, for X, Y as defined in the beginning of this section, we define the binary relation " $\cong$ " by:

$$X \cong Y \, modulo \; q \;\; if \, and \, only \, if \quad x_i \equiv y_i \; modulo \; q. \tag{7}$$

Remark 5. *It's clair that*

1. *" $\cong$ " is an equivalence relation. The equivalence class of X under " $\cong$ ", denoted $[X]$ is defined as*

$$[X] = \{Y \in \mathbb{Z}[\alpha,\beta] \mid X \;\cong\; Y modulo \;\; q\}$$

2. *For X, Y in $\mathbb{Z}[\alpha,\beta]$, we have:*

$$[X] + [Y] = [X+Y],$$
$$[X].[Y] = [X.Y]$$

For a prime integer q, let us denote by $\mathbb{Z}_q[\alpha,\beta]$ the set:

$$\mathbb{Z}_q[\alpha,\beta] := \{[X] \mid X \in \mathbb{Z}[\alpha,\beta]\}$$

For simplicity of notation, we write X instead of $[X]$. We are now in a place to give a number of results concerning the set $\mathbb{Z}_q[\alpha,\beta]$.

Theorem 6. *$(\mathbb{Z}_q[\alpha,\beta],+,.)$ is a commutative ring.*

Proof: By [2, Theorem 2.], we know that $(\mathbb{Z}_q[\alpha,\beta],+)$ is a commutative group with unit element 0, furthermore the product is commutative with unit element 1. It remains to prove that $(.)$ is associative and distributive. we put:

$$Z := z_0 + z_1\alpha + z_2\beta + z_3\beta^2 + z_4\alpha\beta + z_5\alpha\beta^2,$$

then the coefficients of $(X\,.\,Y)\,.\,Z$ in a bass of O_L are given by formula:

$$\begin{aligned}
t_0 &= x_0y_0z_0 \, mod\, q,\\
t_1 &= (x_0(y_0z_1 + y_1z_0) + x_1y_0z_0) \, mod\, q,\\
t_2 &= (x_2y_0z_0 + x_0(y_2z_0 + y_0z_2)) \, mod\, q,\\
t_3 &= (x_3y_0z_0 + x_0(y_3z_0 + y_0z_3 + y_2z_2)\\
&\quad + x_2(y_2z_0 + y_0z_2)) \, mod\, q,\\
t_4 &= (x_2(y_0z_1 + y_1z_0) + x_0(y_2z_1 + y_0z_4 + y_1z_2\\
&\quad + y_4z_0) + x_1(y_2z_0 + y_0z_2) + x_4y_0z_0) \, mod\, q,\\
t_5 &= (x_4(y_2z_0 + y_0z_2) + x_2(y_2z_1 + y_0z_4\\
&\quad + y_1z_2 + y_4z_0) + x_0(y_4z_2 + y_2z_4 + y_0z_5\\
&\quad + y_5z_0 + y_1z_3 + y_3z_1) + x_5y_0z_0 + x_1(y_3z_0\\
&\quad + y_0z_3 + y_2z_2) + x_3(y_0z_1 + y_1z_0)) \, mod\, q.
\end{aligned}$$

With the same way we compute $X\,.\,(Y.\,Z)$, we find the same coefficients as in $(X\,.\,Y)\,.\,Z$.
It remains to prove the distributivity on the left and on the right is similar. Using a computing package, we check that:

$$\begin{aligned}
(Y+Z)\,.\,X &= h_0 + h_1\alpha + h_2\beta + h_3\beta^2 + h_4\alpha\beta\\
&\quad + h_5\alpha\beta^2 \, mod\, q,\\
Y.\,X + Z.\,X &= g_0 + g_1\alpha + g_2\beta + g_3\beta^2 + g_4\alpha\beta\\
&\quad + g_5\alpha\beta^2 \, mod\, q.
\end{aligned} \tag{8}$$

with

$$\begin{aligned}
h_0 &= x_0(y_0 + z_0) \, mod\, q,\\
h_1 &= (y_1 + z_1)x_0 + (y_0 + z_0)x_1 \, mod\, q,\\
h_2 &= (x_2(y_0 + z_0) + x_0(y_2 + z_2)) \, mod\, q,\\
h_3 &= (x_3(y_0 + z_0) + x_0(y_3 + z_3) + x_2(y_2 + z_2)) \, mod\, q,\\
h_4 &= (x_2(z_1 + y_1) + x_0(z_4 + y_4) + x_1(y_2 + z_2)\\
&\quad + x_4(y_0 + z_0)) \, mod\, q,\\
h_5 &= (x_4(y_2 + z_2) + x_2(z_4 + y_4) + x_0(z_5 + y_5)\\
&\quad + x_5(y_0 + z_0) + x_1(y_3 + z_3) + x_3(z_1 + y_1)) \, mod\, q,
\end{aligned}$$

and,

$$\begin{aligned}
g_0 &= x_0y_0 + x_0z_0 \, mod\, q,\\
g_1 &= (x_0z_1 + x_1z_0 + x_0y_1 + x_1y_0) \, mod\, q,\\
g_2 &= (x_2y_0 + x_0y_2 + x_2z_0 + x_0z_2) \, mod\, q,\\
g_3 &= (x_3y_0 + x_0y_3 + x_2y_2 + x_3z_0 + x_0z_3\\
&\quad + x_2z_2) \, mod\, q,\\
g_4 &= (x_2z_1 + x_0z_4 + x_1z_2 + x_4z_0 + x_2y_1\\
&\quad + x_0y_4 + x_1y_2 + x_4y_0) \, mod\, q,\\
g_5 &= (x_4z_2 + x_2z_4 + x_0z_5 + x_5z_0 + x_1z_3\\
&\quad + x_3z_1 + x_4y_2 + x_2y_4 + x_0y_5 + x_5y_0 + x_1y_3\\
&\quad + x_3y_1) \, mod\, q.
\end{aligned}$$

It's clear that for all i in $\{0,\ldots,5\}$; $h_i = g_i$.

Lemma 7. *Let $X \in \mathbb{Z}_q[\alpha,\beta]$ given by: $X = x_0 + x_1\alpha + x_2\beta + x_3\beta^2 + x_4\alpha\beta + x_5\alpha\beta^2$. Then X is invertible in $\mathbb{Z}_q[\alpha,\beta]$ if and only if $x_0 \neq 0$. Indeed, the inverse*

$$X^{-1} = j_0 + j_1\alpha + j_2\beta + j_3\beta^2 + j_4\alpha\beta + j_5\alpha\beta^2\,,$$

where

$$\begin{aligned} j_0 =& x_0^{-1} \,mod\, q,\\ j_1 =& -x_0^{-2}x_1 \,mod\, q,\\ j_2 =& -x_2x_0^{-2} \,mod\, q,\\ j_3 =& -x_3x_0^{-2} + x_2^2x_0^{-3} \,mod\, q,\\ j_4 =& 2x_1x_2x_0^{-3} - x_4x_0^{-2} \,mod\, q,\\ j_5 =& 2x_4x_2x_0^{-3} - x_5x_0^{-2} - 3x_1x_2^2x_0^{-4}x_3x_0^{-3}x_1\\ &+ x_2x_1x_0^{-3} \,mod\, q. \end{aligned} \tag{9}$$

Proof: In view of 6, it suffice to resolve the following system modulo q, which give X^{-1}

$$\begin{cases} x_0j_0 = 1,\\ x_0j_1 + x_1j_0 = 0,\\ x_2j_0 + x_0j_2 = 0,\\ x_3j_0 + x_0j_3 + x_2j_2 = 0,\\ x_2j_1 + x_4j_0 + x_0j_4 + x_1j_2 = 0,\\ x_4j_2 + x_0j_5 + x_5j_0 + x_2j_4 + x_1j_3 + x_3j_1 = 0\,. \end{cases}$$

It is simple, but less natural to check directly with the given formulas of unit element $e = 1$ that; $X.X^{-1} = X^{-1}.X = e$. Using the product law, one finds immediately that the inverse of X is equal to X^{-1}.

We now need to introduce a map which will be basic to Our work. We put $\pi^q_{t,s}$ the following canonical projection: $\pi^q_{t,s} : \mathbb{Z}_q(\alpha,\beta) \to \mathbb{F}_q$ sending each element $X = x_0 + x_1\alpha + x_2\beta + x_3\beta^2 + x_4\alpha\beta + x_5\alpha\beta^2$ of $\mathbb{Z}_q(\alpha,\beta)$ onto $\pi^q_{t,s}(X) = x_0$ of $\mathbb{F}_q$.

We have the following basic results:

Proposition 8. *1. $\pi^q_{t,s}$ is a ring homomorphism.*

2. The set $\mathfrak{I} = \{X - \pi^q_{t,s}(X) \mid X \in \mathbb{Z}_q(\alpha,\beta)\}$ is a unique maximal ideal in $\mathbb{Z}_q(\alpha,\beta)$.

Proof: Let

$$\begin{aligned} X =& x_0 + x_1\alpha + x_2\beta + x_3\beta^2 + x_4\alpha\beta + x_5\alpha\beta^2\\ Y =& y_0 + y_1\alpha + y_2\beta + y_3\beta^2 + y_4\alpha\beta + y_5\alpha\beta^2. \end{aligned} \tag{10}$$

1. The first part our proposition comes immediately from the definition of $X + Y$ and $X.Y$.

2. - If $X \in \mathbb{Z}_q(\alpha,\beta)$ and $Y \in \mathfrak{J}$, then $X.Y = x_0y_1\alpha + x_0y_2\beta + (x_0y_3 + x_2y_2)\beta^2 + (x_2y_1 + x_0y_4 + x_1y_2)\alpha\beta + (x_4y_2 + x_2y_4 + x_0y_5 + x_1y_3 + x_3y_1)\alpha\beta^2$, and this proves that $\mathfrak{I}$ is an ideal.
   - Let $\mathfrak{k}$ be in ideal in $\mathbb{Z}_q(\alpha,\beta)$ such that $\mathfrak{I} \subseteq \mathfrak{k} \subseteq \mathbb{Z}_q(\alpha,\beta)$. As $\mathfrak{I}$ content all non invertible elements in $\mathbb{Z}_q(\alpha,\beta)\}$, if $\mathfrak{k} \neq \mathfrak{I}$ then $1 \in \mathfrak{k}$ which implies that $\mathfrak{k} = \mathbb{Z}_q(\alpha,\beta)$. This shows that $\mathfrak{I}$ is a maximal ideal.
   - Let $\mathfrak{l}$ be a maximal ideal in $\mathbb{Z}_q(\alpha,\beta)$. Let $X \in \mathfrak{l}$, we have $\pi(X) = 0$, so $X \in \mathfrak{I}$ hence $\mathfrak{I} = \mathfrak{l}$.

Corollary 9. *The ring $\mathbb{Z}_q(\alpha,\beta)$ is a local ring with maximal ideal $\mathfrak{I}$ and the residual field $\mathbb{F}_q$.*

Proof: We have $ker(\pi) = \mathfrak{I}$, then by the first isomorphism theorem $\mathbb{Z}_q(\alpha,\beta)/\mathfrak{I}$ is isomorphic to $\mathbb{F}_q$.

Consequence 10. *$\mathbb{Z}_q(\alpha,\beta)$ is a vector space over $\mathbb{F}_q$ of dimension 6.*

4 Elliptic curve on $\mathbb{Z}_q(\alpha,\beta)$

In this section, we assume that the prime number q is greater than or equal to 5. We put $t = a_0 + a_1\alpha + a_2\beta + a_3\beta^2 + a_4\alpha\beta + a_5\alpha\beta^2$ and $s = b_0 + b_1\alpha + b_2\beta + b_3\beta^2 + b_4\alpha\beta + b_5\alpha\beta^2$. We denote $\Delta := 4t^3 + 27s^2$. We show easily that $\Delta = \Delta_0 + \Delta_1$ with $\Delta_1 \in \mathfrak{I}$ and $\Delta_0 = 4a_0^3 + 27b_0^2$. As a consequence of Lemma 7 we can check that Δ is invertible in $\mathbb{Z}_q(\alpha,\beta)$ if and only if $\Delta_0 \neq 0$ in $\mathbb{F}_q$.
Finally, We reply that an elliptic curve over $\mathbb{F}_q$ is defined by Weierstrass equation:

$$(E^q_{t,s}) \;:\; Y^2Z = X^3 + tXZ^2 + sZ^3,\ (t,s) \in \mathbb{F}_q^2$$

whose invertible discriminant. In what follows, $\mathbb{E}^q$ stands for the set:

$$\mathbb{E}^q := \{E^q_{t,s} \mid t,s \in \mathbb{F}_q\}.$$

Definition 11. *We define an elliptic curve over the ring $\mathbb{Z}_q(\alpha,\beta)$ as a curve in projective space $P^2(\mathbb{Z}_q(\alpha,\beta))$, which is given by the homogeneous equation of degree 3, $Y^2Z = X^3 + tXZ^2 + sZ^3$ where t and s in $\mathbb{Z}_q(\alpha,\beta)$ such that the discriminant Δ is invertible. In this case we write:*

$$\begin{aligned} E^q_{t,s}(\alpha,\beta) =& \{[X:Y:Z] \in P^2(\mathbb{Z}_q(\alpha,\beta))| \\ & Y^2Z = X^3 + tXZ^2 + sZ^3\}. \end{aligned} \tag{11}$$

We denote $\mathbb{E}^q_{\alpha,\beta}$ the set of elliptic curve over $\mathbb{Z}_q(\alpha,\beta)$:

$$\mathbb{E}^q_{\alpha,\beta} := \{E^q_{t,s}(\alpha,\beta) \mid t,s \in \mathbb{Z}_q(\alpha,\beta)\}$$

Theorem 12. *$E^q_{t,s}(\alpha,\beta)$ is an elliptic curve over the ring $\mathbb{Z}_q(\alpha,\beta)$ if and only if $E^q_{a_0,b_0}$ is an elliptic curve over the field $\mathbb{F}_q$.*

4.1 Elements of $E^q_{t,s}(\alpha,\beta)$ - Classification

Proposition 13. *Every element in $E^q_{t,s}(\alpha,\beta)$ is of the form*

- $[X\ : Y : 1]$*; where* $X,\ Y \in \mathbb{Z}_q[\alpha,\beta]$,
- $[X : 1 : Z]$*; where* $X,\ Z \in \mathfrak{I}$.

and we write:

$$E^q_{t,s}(\alpha,\beta) = \{[X:Y:1]|\, Y^2 = X^3 + tX + s\} \cup \{[X:1:Z]|\, Z = X^3 + tXZ^2 + sZ^3, \text{ and } X,\ Z \in \mathfrak{I}\}. \tag{12}$$

Proof: Let $[X\ : Y\ : Z] \in E^q_{t,s}(\alpha,\beta)$, where $X,\ Y$ and $Z \in \mathbb{Z}_q[\alpha,\beta]$.

1. If Z is invertible then $[X : Y : Z] = [XZ^{-1} : YZ^{-1} : 1] \sim [X : Y : 1]$. So, $Y^2 = X^3 + tX^2 + s$.
2. If Z is non invertible, then $Z \in \mathfrak{I}$, so, we need to consider the following tow cases for Y;
   (a) If Y is non invertible: we have Y and $Z \in \mathfrak{I}$ and since $X^3 = Z(Y^2 - tXZ - sZ^2) \in \mathfrak{I}$, then $X \in \mathfrak{I}$, we deduce that $[X\ : Y : Z]$ is not a projective point since $(X,\ Y,\ Z)$ is not a primitive triple [7, p. 104-105].
   (b) If Y is invertible then $[X : Y : Z] = [XY^{-1} : 1 : ZY^{-1}] \sim [X : 1 : Z]$. In addition, we check that $Z \in \mathfrak{I}$ and $X^3 = Z(1 - tXZ - sZ^2) \in \mathfrak{I}$, which give $X \in \mathfrak{I}$. Hence, the proposition is proved.

Corollary 14. *Let $[X : 1 : Z] \in E^q_{t,s}(\alpha,\beta)$.*
If $X = x_1\alpha + x_2\beta + x_3\beta^2 + x_4\alpha\beta + x_5\alpha\beta^2$, then $Z = 3x_2^2x_1\alpha\beta^2$.

Proof: Since $[X\ : 1 : Z] \in E^q_{t,s}(\alpha,\beta),\ X = x_1\alpha + x_2\beta + x_3\beta^2 + x_4\alpha\beta + x_5\alpha\beta^2$ and $Z = z_1\alpha + z_2\beta + z_3\beta^2 + z_4\alpha\beta + z_5\alpha\beta^2$ then, by using maple package $Z - aXZ^2 - bZ^3 - X^3 = z_1\alpha + z_2\beta + z_3\beta^2 + z_4\alpha\beta + (z_5 - 3x_2^2x_1 - 3bz_2^2z_1)\alpha\beta^2$ which equal to 0, then $z_5 = 3x_2^2x_1$.

4.2 A group law over $E^q_{t,s}(\alpha,\beta)$

After having given explicitly all elements of $E^q_{t,s}(\alpha,\beta)$, we define the group law over it. Now, We consider the mapping $\widetilde{\pi^q_{t,s}}$:

$$\begin{array}{rccc} \widetilde{\pi^q_{t,s}}: & E^q_{t,s}(\alpha,\beta) & \to & E^q_{a_0,b_0} \\ & [X:Y:Z] & \mapsto & [\pi^q_{t,s}(X) : \pi^q_{t,s}(Y) : \pi^q_{t,s}(Z)]. \end{array}$$

Theorem 15. *Let $P = [X : Y : Z]$ and $Q = [X' : Y' : Z']$ two points in $E^q_{t,s}(\alpha,\beta)$, and $P + Q = [X'' : Y'' : Z'']$.*

1. *If $\widetilde{\pi^q_{t,s}}(P) \neq \widetilde{\pi^q_{t,s}}(Q)$ then,*
   - $X'' = Y^2X'Z' - ZXY'^2 - t(ZX' + XZ')(ZX' - XZ') + (2YY' - 3sZZ')(ZX' - XZ')$
   - $Y'' = YY'(Z'Y - ZY') - t(XYZ'^2 - Z^2X'Y') + (-2tZZ' - 3XX')(X'Y - XY') - 3sZZ'(Z'Y - ZY')$
   - $Z'' = (ZY' + Z'Y)(Z'Y - ZY') + (3XX' + tZZ')(ZX' - XZ')$
2. *If $\widetilde{\pi^q_{t,s}}(P) = \widetilde{\pi^q_{t,s}}(Q)$ then,*
   - $X'' = (YY' - 6sZZ')(X'Y + XY') + (t^2ZZ' - 2tXX')(ZY' + Z'Y) - 3s(XYZ'^2 + Z^2X'Y') - t(YZX'^2 + X^2Y'Z')$
   - $Y'' = Y^2Y'^2 + 3tX^2X'^2 + (-t^3 - 9s^2)Z^2Z'^2 - t^2(ZX' + XZ')^2 - 2t^2ZXZ'X' + (9sXX' - 3tsZZ')(ZX' + XZ')$
   - $Z'' = (YY' + 3sZZ')(ZY' + Z'Y) + (3XX' + 2tZZ')(X'Y + XY') + t(XYZ'^2 + Z^2X'Y')$.

Proof: By using the explicit formulas in [1, p. 236–238] we prove the theorem.

Lemma 16. *$\widetilde{\pi^q_{t,s}}$ is a surjective group homomorphism.*

Proof:

- By Lemma 8, we have $\widetilde{\pi^q_{t,s}}$ is surjective.
- The proof is completed by showing that $\widetilde{\pi^q_{t,s}}$ is a group homomorphism. So, let $P = [X : Y : Z]$

and $Q = [X' : Y' : Z']$ in $E^q_{t,s}(\alpha,\beta)$, we put $P+Q = [X" : Y" : Z"]$ then

$$\begin{aligned}\widetilde{\pi^q_{t,s}}(P+Q) &= [\pi^q_{t,s}(X") : \pi^q_{t,s}(Y") : \pi^q_{t,s}(Z")] \\ &= \widetilde{\pi^q_{t,s}}(P) + \widetilde{\pi^q_{t,s}}(Q).\end{aligned}$$

By 2, Theorem 15 and proposition 8

Lemma 17. *Let $P = [X\ : 1 : 3x_2^2x_1\alpha\beta^2]$ and $Q = [X'\ : 1 : 3x_2'^2x_1'\alpha\beta^2]$ in $E^q_{t,s}(\alpha,\beta)$, then we have:*

$$P+Q = [X+X' : 1 : 3(x_1+x_1')(x_2+x_2')^2\alpha\beta^2].$$

Proof: As $\widetilde{\pi^q_{t,s}}(P) = \widetilde{\pi^q_{t,s}}(Q)$, we have by Theorem 15, $X" = X + X'$, $Y" = 1$ *and* $Z" = 3(x_1 + x_1')(x_2 + x_2')^2\alpha\beta^2$, which completes the proof.

In the next we consider the set:

$$\begin{aligned}G^q :=\{&[x_1\alpha + x_2\beta + x_3\beta^2 + x_4\alpha\beta + x_5\alpha\beta^2 \\ &: 1 : 3x_2^2x_1\alpha\beta^2]\ |x_i \in \mathbb{F}_q,\ i = 1,..,5\}.\end{aligned} \tag{13}$$

Now we have the following fundamental theorem which gives the structure of the set G^q:

Theorem 18. *The set $(G^q,+)$ is a p-subgroup of $E^q_{t,s}(\alpha,\beta)$, isomorphic to $(\mathbb{F}_q^5,+)$.*

Proof: This result is particularly useful when we are given a map, we define ϕ^q as follows,

$$\begin{array}{rccc}\phi^q : & (\mathbb{F}_q^5,+) & \to & (G^q,+) \\ & T = (x_1,x_2,x_3,x_4,x_5) & \mapsto & \phi^q(T).\end{array}$$

Where, $\phi^q(T) = [x_1\alpha+x_2\beta+x_3\beta^2+x_4\alpha\beta+x_5\alpha\beta^2 : 1 : 3x_2^2x_1\alpha\beta^2]$.
The map ϕ^q is well defined since if we take another $(x_1',x_2',x_3',x_4',x_5')$ in $\mathbb{F}_q^5$ we get the same image.

With the property that $\phi^q(x+y) = \phi^q(x)+\phi^q(y)$ coming from Lemma 17 for all $x,\ y$ in $\mathbb{F}_q^5$; for then we can immediately deduce that ϕ^q is an homomorphism.

It follows from definition of G^q that ϕ^q is surjective.

Now, Given an arbitrary element $x = (x_1,x_2,x_3,x_4,x_5) \in \mathbb{F}_q^5$. So, if $\phi^q(x) = [0 : 1 : 0]$, then $x_1\alpha + x_2\beta + x_3\beta^2 + x_4\alpha\beta + x_5\alpha\beta^2 = 0$, and therefore $x = 0$, since $\mathfrak{B} = \{1,\alpha,\beta,\beta^2,\alpha\beta,\alpha\beta^2\}$ is a basis.

Finally observe that $\phi^q(px) = p\phi^q(x) = 0$. Therefore we conclude that G^q is a p-subgroup.

Thus, as a further consequence of the above theorem, we get an injective homomorphism from $\mathbb{F}_q^5$ into the set $E^q_{t,s}(\alpha,\beta)$.

Theorem 19. *The sequence: $0 \to \mathbb{F}_q^5 \to^{\widetilde{\phi^q}} E^q_{t,s}(\alpha,\beta) \to^{\widetilde{\pi^q_{t,s}}} E^q_{a_0,b_0} \to 0$ is exact, where $\widetilde{\phi^q}(x_1,x_2,x_3,x_4,x_5) = \phi^q(x_1,x_2,x_3,x_4,x_5)$.*

Proof:

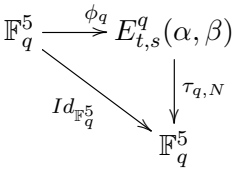
- By Theorem 15, $\widetilde{\phi^q}$ is injective.
- By Lemma 16, $\widetilde{\pi^q_{t,s}}$ is surjective.
- We are now in a position to show $ker\widetilde{\pi^q_{t,s}} = Im\widetilde{\phi^q}$. Consider $[x_1\alpha + x_2\beta + x_3\beta^2 + x_4\alpha\beta + x_5\alpha\beta^2\ : 1 : 3x_2^2x_1\alpha\beta^2] \in Im\widetilde{\phi^q}$, then $\tilde{\pi^q_{t,s}}([x_1\alpha + x_2\beta + x_3\beta^2 + x_4\alpha\beta + x_5\alpha\beta^2 : 1 : 3x_2^2x_1\alpha\beta^2]) = [0 : 1 : 0]$ and so, $ker\widetilde{\pi^q_{t,s}} \supseteq Im\widetilde{\phi^q}$. Conversely let $[X\ : Y : Z] \in \ker\tilde{\pi^q_{t,s}}$, then $[x_0,\ y_0,\ z_0] = [0 : 1 : 0]$, so Y is invertible, and from proposition 13 : $X,\ Z \in \mathfrak{I}$ so, $[X : Y : Z] \sim [X : 1 : Z]$; and from Corollary 14, $[X : Y : Z] \sim [x_1\alpha + x_2\beta + x_3\beta^2 + x_4\alpha\beta + x_5\alpha\beta^2 : 1 : 3x_2^2x_1\alpha\beta^2] \in Im\widetilde{\phi^q}$, which completes the proof.

Theorem 20. *There is an isomorphism from $E^q_{t,s}(\alpha,\beta)$ to the direct sum of $E^q_{a_0,b_0}$ and $\mathbb{F}_q^5$.*

To prove this theorem, we first prove the following lemma.

Lemma 21. *Let $N =\neq E^q_{a_0,b_0}$. If p doesn't divide N, then the short exact sequence: $0 \to \mathbb{F}_q^5 \to^{\widetilde{\phi^q}} E^q_{t,s}(\alpha,\beta) \to^{\widetilde{\pi^q_{t,s}}} E^q_{a_0,b_0} \to 0$ is split.*

Proof: It suffices to show; there is an homomorphism map denoted by $\tau_{q,N}$ such that the following diagram be commutative



Let $N_0 \in \mathbb{Z}$ such that $1 - NN_0 = tp$ for somme integer t. Let $\tau_{q,N}$ the homomorphism defined by:

$$\begin{array}{rccc}\tau_{q,N} : & E^q_{t,s}(\alpha,\beta) & \to^{[NN_0]} & G^q \\ & P & \mapsto & (1-tp).P.\end{array}$$

$$\begin{array}{rccc}\phi_q^{-1} : & G^q & \to^{\phi_q^{-1}} & \mathbb{F}_q^5 \\ & (1-tp).P & \mapsto & (x_1,x_2,x_3,x_4,x_5).\end{array}$$

Let $P = (x_1, x_2, x_3, x_4, x_5) \in \mathbb{F}_q^5$, then

$$\begin{aligned}\tau_{q,N} \circ \widetilde{\phi_q}(P) =&\phi_q^{-1} \circ [NN_0] \circ \widetilde{\phi_q}(x_1, x_2, x_3, x_4, x_5)\\ =&\phi_q^{-1} \circ [NN_0]([x_1\alpha + x_2\beta + x_3\beta^2\\ &+ x_4\alpha\beta + x_5\alpha\beta^2 : 1 : 3x_2^2x_1\alpha\beta^2])\\ =&\phi_q^{-1}((1-tp).[x_1\alpha + x_2\beta + x_3\beta^2\\ &+ x_4\alpha\beta + x_5\alpha\beta^2 : 1 : 3x_2^2x_1\alpha\beta^2])\\ =&(1-tp).\phi_q^{-1}[x_1\alpha + x_2\beta + x_3\beta^2\\ &+ x_4\alpha\beta + x_5\alpha\beta^2 : 1 : 3x_2^2x_1\alpha\beta^2])\\ =&(1-tp)(x_1, x_2, x_3, x_4, x_5)\\ =&(x_1, x_2, x_3, x_4, x_5) - tp(x_1, x_2, x_3, x_4, x_5)\\ =&(x_1, x_2, x_3, x_4, x_5).\end{aligned} \tag{14}$$

This shows that the short exact sequence of groups is left split and the proof is complete.

Proof: of Theorem 20. Since the groups are abelians, the short sequence is split which show the theorem and complete the proof.

4.3 Example

It is very difficult to construct an elliptic curve over $E_{t,s}^q(\alpha, \beta)$, hence the interest in using the isomorphic Theorem 20. to give an example of elliptic curve over $\mathbb{F}_q$ under the previews conditions.
Let $q = 7$, $d = 7$, $a = 14$ and $b = 1$.
α is a root of monic polynomial $X^2 - 7$.
β a root of monic polynomial $X^3 - 14X + 1$.
We put

$$\begin{aligned}t =&1 + 3\alpha + 5\beta + 3\beta^2 + \alpha\beta + 2\alpha\beta^2,\\ s =&1 + 3\alpha + 6\beta + 4\beta^2 + 2\alpha\beta.\end{aligned}$$

We have $\Delta_0 = 4a_0^3 + 27b_0^2 = 3\, mod\, 7$.
As a consequence of Lemma 7 we concludes that Δ is invertible in $\mathbb{Z}_q(\alpha, \beta)$. So, $E_{t,s}(\alpha, \beta)$ is well defined on $\mathbb{Z}_q(\alpha, \beta)$.

Now we have;

$$E_{1,1}^7 = \{[x : y : 1]/y^2 = x^3 + x + 1\} \cup \{[0 : 1 : 0]\}$$

From the following table, we give all elements of $E_{1,1}^7$.

x	y	y^2	$x^3 + x + 1$
0	0	0	**1**
1	1	**1**	3
2	2	**4**	**4**
3	3	2	3
4	4	2	6
5	5	**4**	5
6	6	**1**	6

Hence,

$$E_{1,1}^7 = \{[0 : 1 : 1], [0 : 6 : 1], [2 : 2 : 1], [2 : 5 : 1], [0 : 1 : 0]\}$$

As a consequence

$$E_{t,s}^7(\alpha, \beta) \cong \mathbb{F}_7^5 \oplus E_{1,1}^7.$$

which content 84035 elements.

5 Consequences and illustrations

We have the following results:

1. We get from Theorem 20; $|E_{t,s}^q(\alpha, \beta)| = q^5N$.
2. The Discrete Logarithm on the elliptic curve $E_{t,s}^q(\alpha, \beta)$ is equivalent to the one on E_{a_0,b_0}^q.
3. The elliptic curve on this ring can be used for both cryptography and cryptoanalysis. So, if the Discrete Logarithm on $E_{t,s}^q(\alpha, \beta)$ is trivial then we can break it on the elliptic curve E_{a_0,b_0}^q with trivial attacks.
4. This work can be generalited to an upper degree for the extension L, knowing that the difficulty of the problem becomes more difficult every time the degree of the extension becomes bigger?
5. We can replace Theorem 3 by [[7], Theorem 3.1.], to produce similar but totally different results.

Acknowledgements. The authors would like to thank CSLM, Ensa-Kenitra, UIT and FP, TICSM, LSI in Taza, USMBA, MOROCCO for its valued support.

References:

[1] A. Chillali *Elliptic curves of the ring* $F_q(\epsilon)$, $\epsilon^n = 0$, Int. Math Forum, 6 (2011), 1501-1505

[2] A. Chillali and M. Sahmoudi, *Cryptography over sextic extension with cubic subfield*, World Academy Sci. Engrg. Technol. **9** (2015), 246-249.

[3] A. Tadmori, A. Chillali and M. Ziane, *Cryptography over the elliptic curve* $E_{a,b}(A_3)$, Journal of Taibah University for Science, **9** 3, (2015), 326-331.

[4] H. Hassib, A. Chillali and M. Abdou Elomary, *Elliptic curves over a chain ring of characteristic 3*, Journal of Taibah University for Science, **9** 3, (2015), 276-287.

[5] JH.Silverman , *The Arithmetic of Elliptic Curves*, Graduate Texts in Mathematics, 2009

[6] M. E. Charkani and M. Sahmoudi, *Sextic extension with cubic subfield*, JP J Algebra, Number Theory Appl. **34** (2014), 139-150.

[7] M. Sahmoudi, *Explicit integral basis for a family of sextic field*, Gulf J. Math. **4** (2016), 217-222.

[8] M. Sahmoudi and A. Chillali, *Key exchange over particular algebaic closure ring*, Tatra Mt. Math. Publ. **70** (2017), 151-162.

[9] M. Sahmoudi and A. Soullami, *On Sextic Integral Bases Using Relative Quadratic Extention*, Bol. Soc. Paran. Mat.. (3s.)v.**38** 4 (2020), 175180.

[10] M. Virat, *Courbe elliptique sur un anneau et applications cryptographiques*, Thse Docteur en Sciences, Nice-Sophia Antipolis, (2009).