The Arithmetic of Sklyanin Algebras I the defining equations

L. Le Bruyn*
Universiteit Antwerpen (UIA), Belgium

June 1992 - 92-25

Abstract

To every non-cuspidal K-rational point on the modular curve $X_1(n)$ a non-commutative Noetherian domain of global dimension 3 can be associated : the Sklyanin algebra. In this paper we give the defining equations of the Sklyanin algebras and their centers when $X_1(n)$ is rational, i.e. $n \leq 10$ or $n = 12$.

AMS-Classification
16W50, 14K07

Keywords
Sklyanin algebras, modular curves

* Research Associate of the NFWO (Belgium)

The Arithmetic of Sklyanin Algebras I
the defining equations

Lieven Le Bruyn*
Dept. Wiskunde en Informatica
Universitaire Instelling Antwerpen
email : lebruyn@ccu.uia.ac.be

June 24, 1992

Abstract

To every non-cuspidal K-rational point on the modular curve $X_1(n)$ a non-commutative Noetherian domain of global dimension 3 can be associated : the Sklyanin algebra. In this paper we give the defining equations of the Sklyanin algebras and their centers when $X_1(n)$ is rational, i.e. $n \leq 10$ or $n = 12$.

*research associate of the NFWO (Belgium)

Contents

1 Introduction

To an elliptic curve E and a rational point $\tau \in E$ (or rather the automorphism on E induced by translation with τ) one associates the 3-dimensional Sklyanin algebra $A_\tau(E)$,e.g. [4] or [18]. These are non-commutative Noetherian domains and are Auslander-regular of global dimension 3 ,[5]. The geometry of Sklyanin algebras is reasonably understood by now,see [2] or [13] for the analogously defined 4-dimensional Sklyanin algebras.

Perhaps it is interesting to look at some of the arithmetical problems connected with Sklyanin algebras. This series of notes may be seen as the first timid steps in this direction. My interest in the arithmetic of Sklyanin algebras comes from the following two motivations :

1.1 Modular curves

Let $\Upsilon = \{\alpha = x + iy \mid y > 0\}$ be the upper half plane acted upon by the modular group $SL_2(\mathbb{Z})$, then the j-function gives a holomorphic isomorphism between the fundamental domain $SL_2(\mathbb{Z}) \mid \Upsilon$ and $\mathbb{P}^1(\mathbb{C}) - \{\infty\}$. To α we can associate a lattice Λ in $\mathbb{C}$ and the j-function is the single invariant for isomorphism classes of toruses (or elliptic curves) $\mathbb{C}/\Lambda$.

For any positive integer n one considers the subgroup $\Gamma_1(n)$ of $SL_2(\mathbb{Z})$ consisting of all elements which modulo n look like

$$\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}$$

for arbirary b. We can view $1/n$ as a point of order n on the torus $\mathbb{C}/[\alpha, 1]$ and the association

$$\alpha \to (\mathbb{C}/[\alpha, 1], 1/n)$$

gives a bijection between the fundamental domain $\Gamma_1(n) \mid \Upsilon$ and isomorphism classes of toruses (or elliptic curves) together with a point of order n.

As in the case of the full modular group $SL_2(\mathbb{Z})$,there exists an affine curve $Y_1(n)$ defined over $\mathbb{Q}$ such that there is a holomorphic isomorphism between $\Gamma_1(n) \mid \Upsilon$ and $Y_1(n)(\mathbb{C})$. If K is a field containing $\mathbb{Q}$ then a point of $Y_1(n)(K)$ corresponds to a pair (E, τ) where E is an elliptic curve defined over K and τ is a K-rational point of E of order n.

The affine curve $Y_1(n)$ can be compactified to $X_1(n)$ by adjoining the cusps,i.e. points which lie above $j = \infty$. The projective curve $X_1(n)$ is called the modular curve. There are many important open questions concerning modular curves,e.g.

Question 1 *If K is a number field,does the set of rational points $X_1(n)(K)$ consists entirely of cusps for all sufficiently large n ?*

As far as I know,this question is only settled for $K = \mathbb{Q}$ by B. Mazur [14] and for quadratic number fields by Kamienny [7].

Classically, one can associate to a point (E, τ) of $X_1(n)(K)$ "only" the isogeny

$$\pi : E \rightarrow E' = E / < \tau >$$

As we mentioned above, one can associate to the couple (E, τ) a certain non-commutative algebra, the Sklyanin algebra $A_\tau(E)$. The construction and some of its properties will be recalled in the next section. For the moment think of $A_\tau(E)$ as determining an order $\mathcal{A}$ over $\mathbb{P}^2$ completing the following square diagram

$$\begin{tikzcd} E \arrow[r, hook] \arrow[d] & \mathcal{A} \arrow[d] \\ E' \arrow[r, hook] & \mathbb{P}^2 \end{tikzcd}$$

Conversely, one can recover the couple (E, τ) from the ringtheoretic structure of $A_\tau(E)$: the curve E describes the rank three divisor of point-modules and the point τ is recovered from the twist operator on point modules, the isogenous curve $E' = E/ < \tau >$ is recovered as the ramification locus of the order $\mathcal{A}$. Therefore, all invariants associated to the Sklyanin algebra $A_\tau(E)$ should ultimately be described in terms of the point $(E, \tau) \in X_1(n)(K)$. Some are merely translations, e.g. the above question can be rephrased into ringtheoretical lingo as : if K is a number field is there a bound on the p.i.-degree of Sklyanin algebras defined over K?

More interesting is that one can associate new objects to $A_\tau(E)$ or if you want to the corresponding point of $X_1(n)$. To begin,Sklyanin algebras determine at least 3 new cubic curves :

1. The Artin-Schelter curve : In [3, 6.11] Artin and Schelter associate a cubic divisor w such that $A_\tau(E)$ is a skew-polynomial rings if and only if $j(w) = \infty$.

2. The discriminant curve : By symmetrizing the three defining quadratic relations of $A_\tau(E)$ one obtains a net of conics in $I\!P^2$. Associated to such a net is a cubic divisor describing the singular conics. In [12] this discriminant curve was shown to play an important role in the study of central extensions of $A_\tau(E)$.

3. The cubic trace curve : As we will see in the second part of these notes, the division algebra of $A_\tau(E)$ will be a cyclic algebra if there exists a degree one element $g \in A_\tau(E)$ s.t. $Tr(g^3) = Tr(g^6) = ... = Tr(g^{3[\frac{n}{3}]}) =$ 0.The condition $Tr(g^3) = 0$ describes a cubic curve called the cubic trace curve.

At present it is unclear how the arithmetic of these new curves ties up with the original isogeny. Moreover, one can associate to $A_\tau(E)$ also entirely new objects such as fat-points and their endomorphism central simple algebras.In [10] we wil see how the splitting behaviour of these central simple algebras is intimately linked to the isogeny.

In short, the Sklyanin algebra $A_\tau(E)$ associates new objects to the non-cuspidal point (E, τ) of $X_1(n)$ and conversely it is hoped that any insight we will gain about them will be of use in the study of rational points on modular curves.

1.2 The cyclicity problem

There is also an entirely ringtheoretical motivation for studying Sklyanin algebras. After more than 60 years the following problem in finite dimensional division algebras is still unsolved :

Question 2 *Is every division algebra of degree p (p a prime) cyclic ? That is, does there exists a non- central element $\delta \in \Delta$ s.t. δ^p is central ?*

The answer is clearly positive for $p = 2$ or 3 but even for $p = 5$ the answer remaines unknown in spite of considerable effort of Albert [1] and Brauer [6]. Perhaps there is a slight tendency these days to expect the answer to be negative for large values of p.

One can view a division algebra Δ of degree p i.e. of dimension p^2 over its center F to be a bag containing lots of commutative separable fieldextensions of F of degree p. As p increases we get more freedom for the Galois groups of these subfields of Δ so it seems unlikely that Δ should always contain a Galois (i.e. then cyclic) subfield.

The basic obstruction in carrying through this idea is that one does not know many constructions of division algebras which are on the one hand not too easy to prevent them from being possible counterexamples (such as iterated Ore-extensions) and on the other hand not too difficult to calculate with (such as generic division algebras).

Perhaps the Sklyanin algebras constitute the first class of algebras satisfying both requirements. As we mentioned above,Artin and Schelter were able to show that they are virtually never skew polynomial rings [3, 6.11]. Still, from work of Artin,Schelter,Tate,Van den Bergh [3],[4] and [5] and especially the recent unpublished work of J. Tate [19] one can perform actual computations in $A_\tau(E)$.

Although these algebras arise from a very cyclic situation (an isogeny of elliptic curves) it turns out to be rather hard to prove cyclicity of them even for small values of the order of τ. As we will see in the second part of these notes,cyclicity follows easily if $ord(\tau) \leq 9$ and K algebraically closed but it involves some extra work to prove e.g. cyclicity over an arbitrary basefield when $ord(\tau) = 5$ and even for $ord(\tau) = 7$ cyclicity is still unsettled over say $\mathbb{Q}$.

A possible approach to disprove cyclicity for $A_\tau(E)$ is to look at division algebras of the restriction of $\mathcal{A}$ to points or curves in $\mathbb{P}^2$. In the case of points or lines through rational points of the isogenous curve $E' \hookrightarrow \mathbb{P}^2$ one can easily use the isogeny to prove that the algebras are split by an at worst dihedral extension and hence they are cyclic (at least if K contains a primitive p-th root of unity) by a result of Rowen and Saltman [16]. However, for arbitrary lines or more general curves deciding cyclicity of the corresponding quotient of $\mathcal{A}$ turns out to be substantially harder.

It is our hope that a closer investigation of the arithmetic of Sklyanin algebras (or algebras derived from them) may lead to non-cyclic division algebras of prime degree.

The present paper contains in a way the dirty work one needs to do first before one can tackle the more interesting problems, i.e. how to compute the defining equations of $A_\tau(E)$ and its center starting from a point (E, τ) in $X_1(n)(K)$.

Section 2 should be read as a rather self-contained crash course on 3-dimensional Sklyanin algebras. In it we rederive some of the basic results of [4] in the special case of elliptic curves with we hope as little machinary as possible. We have included a proof of the fact that the twisted coordiante ring $\mathcal{O}_\tau(E)$ has the same Hilbert series as the coordinate ring of the elliptic curve, a computational method to get hold of generators for the quadratic equations and some help for the proof in [4] of the existence of a "twisted" Weierstrass equation,i.e. a central degree 3 element c_3 such that the quotient $A_\tau(E)/(c_3)$ is isomorphic to the twisted coordinate ring $\mathcal{O}_\tau(E)$. This fact is the key to working with Sklyanin algebras.

In section 3 we present the defining equations for Sklyanin algebras associated to rational points on $X_1(n)$ whenever it is a rational curve, i.e. when $n \leq 10$ or $n = 12$. We also briefly recall the well known method to construct the Weierstarss equations of elliptic curves such that the origin $[0:0:1]$ is a point of order n and included the coordinates of all points in the subgroup generated by it. This information is then used later on to describe the center. Combining these computations with the result of B. Mazur mentioned above, this section can be thought of as describing all Sklyanin algebras over the ultimate base-field : $\mathbb{Q}$.

In the final section we present a computational method to describe the center of the Sklyanin algebras using recent results of J. Tate [19]. He proved that the center of $A_\tau(E)$ is generated by c_3 and three elements of degree n satisfying one relation among them. We give precise generators of the center of the twisted coordinate ring $\mathcal{O}_\tau(E)$ and the unique cubic equation satisfied by them. This is in fact a reformulation into the present setting of a result of J. Vélu [20] on computing the Weierstrass equation of an isogenous elliptic curve starting from the equation of the elliptic curve and the coordinates of the elements in the kernel. By Tate's proof we then know that we can lift these three degree n elements to central elements of $A_\tau(E)$ and that the unique relation satisfied among them and c_3 is of the form $\alpha c_3^n =$ the cubic among the three degree n centrals (at least if $(n, 3) = 1$). But even then, there remains the problem of evaluating the constant factor α which is best done by considering fat points and their endomorphism rings. We have included the results obtained for $n \leq 5$ for the center of $A_\tau(E)$ and for the center of $\mathcal{O}_\tau(E)$ when $n \leq 10$. Even for $n = 5$, verifying the equation found is beyond the computing facilities of a moderate workstation. It is hoped that better algorithms may be found for lifting the generators of $\mathcal{O}_\tau(E)$ to

$A_\tau(E)$ as well as for calculating the constant α.

Acknowledgement : I like to thank S.P. Smith and J. Tate for providing me with notes on their unpublished work on the centers of Sklyanin algebras. Also, many of the computations would have been impossible without Bill Schelter's "affine" program and computer facilities provided through an NFWO-grant.

2 The 3 dimensional Sklyanin algebras

This section is meant to be a crash-coarse on basics of the 3-dimensional Sklyanin algebras. At certain points we have included proofs when we thought they might help readers uneasy with the geometrical arguments of [4]. More details will be given in the forthcoming monograph [11].

Sklyanin algebras arose in the work of Artin and Schelter on graded regular algebras of global dimension 3. In the subsequent work of Artin,Tate and Van den Bergh [4] and [5] the central element c_3 of degree 3 and its quotient algebra $A_\tau(E)/(c_3)$ (which turns out to be a twisted coordinate ring) were introduced as tools in the study of the regular algebra $A_\tau(E)$.

I think it is more sensible to start with the twisted coordinate ring $\mathcal{O}_\tau(E)$ as a non-commutative version of the usual homogeneous coordinate ring $\mathcal{O}(E)$. The classical epimorphism $K[X,Y,Z] \rightarrow \mathcal{O}(E)$ with kernel the principal ideal generated by the Weierstrass equation of E is then realized to have a non-commutative counterpart $A_\tau(E) \rightarrow \mathcal{O}_\tau(E)$ where the Sklyanin algebra $A_\tau(E)$ is the quotient of the free associative algebra on three generators modulo the ideal of quadratic relations in $\mathcal{O}_\tau(E)$ (in the classical case we have just the three commutators giving the polynomial ring). The kernel of this epimorphism is then the ideal generated by a central degree 3 element c_3 which can be thought of as a twisted Weierstrass equation.

If we denote with $C_\tau(E)$ the center of $\mathcal{O}_\tau(E)$ and with $Z_\tau(E)$ the center of the Sklyanin algebra we will see below that Tate's results show that we have the following diagram

$$\begin{tikzcd}
A_\tau(E) \arrow[r, mapsto] & \mathcal{O}_\tau(E) \\
Z_\tau(E) \arrow[u, phantom, "\cup"] \arrow[r, mapsto] & C_\tau(E) \arrow[u, phantom, "\cup"]
\end{tikzcd}$$

where the horizontal maps are epimorphisms.By looking at parts of degree zero of localizations,this diagram gives rise to

$$\begin{tikzcd}
\mathcal{A} \arrow[r, hookleftarrow] \arrow[d] & E \arrow[d] \\
I\!P^2 \arrow[r, hookleftarrow] & E'
\end{tikzcd}$$

where E' is the isogenous elliptic curve $E/ < \tau >$ with its natural embedding in $I\!P^2$ which can be interpreted as the projective space of the 3-dimensional vectorspace of central degree n elements. The map $E \rightarrow E'$ is just the commutative isogeny and with $\mathcal{A}$ we really mean the non-commutative Proj of $A_\tau(E)$ as in e.g. [2].

Let us first fix the notation we will use throughout this paper and recall some basic facts on elliptic curves which may be found in any textbook (an excellent reference is [17]).

Let K be our favourite basefield, $\overline{K}$ its algebraic closure and $G = Gal(\overline{K}/K)$ the absolute Galois group. An elliptic curve E will be given in affine Weierstrass form :

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

see e.g. [17, III,§1]. If all $a_i \in K$ we say that the elliptic curve E is defined over K and denote this fact by E/K. The points of E carry the structure of an Abelian group, see [17, p. 58] for explicit formulas for the addition law.

The divisorgroup of E, $Div(E)$, is the additive group of the integral groupring over the points of E. The subgroup of degree zero divisors $Div^0(E)$ consists of the combinations $\sum n_P P$ such that $\sum n_P = 0$ in $\mathbb{Z}$. If $f \in \overline{K}(E)$, the functionfield of E, then $f = \frac{F}{G}$ where F, G are homogeneous forms of the same degree (say i) in $\overline{K}[X, Y, Z]$ s.t. G does not vanish on E. The divisor $div(f)$ of f is $I(F, E) - I(G, E)$ the difference of the two intersection cycles (each having degree $3i$) so it is a degree zero divisor. We have an exact sequence :

$$1 \rightarrow \overline{K}^* \rightarrow \overline{K}(E)^* \rightarrow Div^0(E) \rightarrow E(\overline{K}) \rightarrow 0$$

the maps being resp. inclusion,div and the map sending $\sum n_p P$ to $\sum [n_P]P \in E(\overline{K})$ (the addition on E). If E/K then we have the descended sequence :

$$1 \rightarrow K^* \rightarrow K(E)^* \rightarrow Div^0_K(E) \rightarrow E(K) \rightarrow 0$$

where $E(K)$ is the group of K-rational points of E and $Div^0_K(E)$ are the G-invariants of $Div^0(E)$ see [17, II §3].

For any divisor $D \in Div(E)$ one defines the vectorspace $\mathcal{L}(D) = \{f \in \overline{K}(E)^* : div(f) + D \geq 0\} \cup \{0\}$. If $D = \sum n_P P$ then the degree $deg(D)$ is the integer $\sum n_P \in \mathbb{Z}$ and the Riemann-Roch theorem for elliptic curves states that the dimension of $\mathcal{L}(D)$ equals $deg(D)$ (provided $def(D) > 0$). Moreover, if $D \in Div_K(E)$ the subgroup of G-invariants divisors, then this vectorspace has a basis consisting of functions from $K(E)$ see [17, II.Prop.5.8].

2.1 The twisted coordinate ring $\mathcal{O}_\tau(E)$

Following [4] we will now introduce for every point $\tau \in E$ a non-commutative graded ring $\mathcal{O}_\tau(E)$ having similar properties as the usual homogenous coordinate ring $\mathcal{O}(E)$ of E.

Let $\phi_\tau : E \rightarrow E$ be translation by τ on E, then this morphism extends to an automorphism on the function field $\phi^*_\tau : \overline{K}(E) \rightarrow \overline{K}(E)$ where for any funtion f the function $\phi^*_\tau(f)$ has value $f(P + \tau)$ in the point P. Hence, if $div(f) = \sum n_P P$ then $div(\phi^*_\tau(f)) = \sum n_P(P - \tau)$. If no confusion can occur (i.e. once τ is fixed) we will denote $\psi = \phi^*_\tau$.

Having an automorphism ψ on the commutative field $\overline{K}(E)$ we can form the skew polynomial ring

$$\overline{K}(E)[t, \psi]$$

which satisfies the commutation rule $t.f = \psi(f).t$ for all $f \in \overline{K}(E)$. It is classical that this skew polynomial ring is a graded Noetherian domain,a left and right principal ideal domain and that it is a finite module over its center iff ψ has finite order i.e. if τ is a torsion point on E.

In order to motivate the definition of $\mathcal{O}_\tau(E)$ let us consider the classical case, i.e. when $\tau = 0$ and $\psi = id$ so $\overline{K}(E)[t, \psi] = \overline{K}(E)[t]$. Then, it is easily verified that the homogenous coordinate ring $\mathcal{O}(E)$ of E is the subring of $\overline{K}(E)[t]$ generated by the three homogeneous elements of degree one $x.t, y.t$ and $1.t$. Hence the following comes naturally :

Definition 1 *If $\tau \in E$ and $\psi = \phi^*_\tau$, then the twisted coordiante ring $\mathcal{O}_\tau(E)$ is the subring of $\overline{K}(E)[t, \psi]$ generated by the elements $x.t, y.t$ and $1, t$,*

Clearly, $\mathcal{O}_\tau(E)$ is a graded domain

$$\mathcal{O}_\tau(E) = B_0 \oplus B_1 \oplus B_2 \oplus \ldots \text{ with } B_i \subset \overline{K}(E).t^i$$

Let us calculate the first few terms : clearly $B_0 = \overline{K}$ and $B_1 = \overline{K}x.t + \overline{K}y.t + \overline{K}1.t = \mathcal{L}(3.0).t$.Further,$B_2$ is spanned by the elements

$$1.t^2, x.t^2, y.t^2, \psi(x).t^2, \psi(y).t^2, x.\psi(x).t^2, x\psi(y).t^2, y\psi(y).t^2, y\psi(x).t^2$$

and is therefore contained in $\mathcal{L}(3.0 + 3.(-\tau)).t^2$. The following description of $\mathcal{O}_\tau(E)$ is proved in [4, §6] :

Theorem 1 (Artin et al.) *Let $\tau \in E$ and let $\sigma = -\tau \in E$ and $D_i = 3.0 + 3.\sigma + ... + 3.[i-1]\sigma \in Div(E)$. Then*

$$\mathcal{O}_\tau(E) = \sum_{i=0}^{\infty} \mathcal{L}(D_i).t^i$$

whenever $[3]\tau \neq 0$.In particular, the homogenous part of degree i has dimension $3i$.

Proof : By definition, $B_i = (B_1)^i = \mathcal{L}(3.0).t.\mathcal{L}(3.0).t...\mathcal{L}(3.0).t$ and using the commutation rule this equals

$$\mathcal{L}(3.0)\psi(\mathcal{L}(3.0))...\psi^{i-1}(\mathcal{L}(3.0)).t^i$$

which is clearly contained in $\mathcal{L}(D_i).t^i$.

To prove equality we make the following change of basis in $\mathcal{L}(3.0)$. If $(3, n) = 1$ we maintain x but if $3 \mid n$ we take x the function determined by the line through 0 and $[k]\tau$ where k is minimal s.t. $[3k]\tau = 0$. Further, we choose $l \in \mathcal{L}(3.0)$ s.t. $div(l) = P_1 + P_2 + P_3 - 3.0$ with P_i distinct points s.t. $\{P_1, P_2, P_3\} \cap [\mathbb{Z}]\tau = \emptyset$. This condition implies that the divisor of poles of $l\psi(l)...\psi^{i-1}(l) = D_n$ for all n.In addition, choose l s.t. x, l and the tangent line to E in either $[k+1]\tau$ or $[2k+1]\tau$ have no point in common. Observe, that $\mathcal{O}_\tau(E)$ is generated by $1.t, x.t$ and $l.t$.

Assume by induction that $B_{i-1} = \mathcal{L}(D_{i-1}).t^{i-1}$ then clearly $\mathcal{L}(D_{i-1}).t^i = \mathcal{L}(D_{i-1}).t^{i-1}.1.t \subset B_i$. By calculating the divisors of poles we see that the following elements of B_i belong to $(\mathcal{L}(D_i) - \mathcal{L}(D_{i-1}).t^i$:

$$(x.t)^2.(l.t)^{i-2}, x.t.(l.t)^{i-1}, l.t.(l.t)^{i-1}$$

If they are linearly dependent over $\mathcal{L}(D_{i-1}).t^{i-1}$ there exist $a, b, c \in \overline{K}$ such that

$$(ax\psi(x) + bx\psi(l) + cl\psi(l))\psi^2(l\psi(l)...\psi^{i-3}) \in \mathcal{L}(D_{i-1})$$

If the first factor is f then $div(f) = \sum_{i=1}^{6} Q_i - 3.0 - 3\sigma$ and the divisor of poles of the second factor is $3.[2]\sigma + 3.[3]\sigma + ... + 3.[i-1]\sigma$. Therefore, $Q_1 = Q_2 = Q_3 = [i-1]\sigma$,whence $[3(i-1)]\tau = 0$.

So, whenever $k \not| i-1$ we obtain a contradiction and we are done by a dimension count. If $k \mid i-1$ then we can evaluate f in $[i-1]\sigma$ to give $c = 0$ as $x([i-1]\sigma) = 0$ but neither $l([i-1]\sigma)$ nor $l([i]\sigma)$ vanishes. So, the divisor of f is $[k]\tau + [2k]\tau + R_1 + R_2 + R_3 - 2.0 - 3.\sigma$ so $[k]\tau$ (or $[2k+1]\tau$) must be a double zero of $\psi(ax + bl)$ i.e. $ax + bl$ is the tangent line to E in $[k+1]\tau$ (or $[2k+1]\tau$),but then x, l and this tangent line would be concurrent, a contradiction. □

If E/K and if $\tau \in E(K)$ then clearly all the divisors $D_n \in Div_K(E)$ and so they each have a basis consisting of functions from $K(E)$.If we denote for any divisor D by $\mathcal{L}_K(D) = \mathcal{L}(D) \cap K(E)$ then we deduce from the above proof :

Proposition 1 *If E/K and if $\tau \in E(K)$ and if there exists a K-defined line l s.t. l avoids $[\mathbb{Z}]\tau$ and l, x and the tangent lines to E described in the foregoing proof are not concurrent, then $\mathcal{O}_\tau(E)$ is defined over K i.e. the K-subalgebra of $K(E)[t, \psi]$ generated by $x.t, y.t$ and $1.t$ is*

$$\sum_{i=0}^{\infty} \mathcal{L}_K(D_i).t^i$$

2.2 The Sklyanin algebras $A_\tau(E)$

As $\mathcal{O}_\tau(E)$ is generated by three degree one elements there is an epimorphism

$$K < X, Y, Z > \rightarrow \mathcal{O}_\tau(E)$$

and the degree two part of the kernel is 3-dimensional as $B_2 = 6$ and the free algebra has 9 degree 2 forms. Recall that in the classical (i.e. $\tau = 0$) these quadratic relations are just the commutators. Hence, if we take the quotient of the free algebra modulo the ideal generated by the degree 2 relations we would expect a ring having similar properties as the polynomial ring in three variables.

Definition 2 *Let E/K be an elliptic curve and $\tau \in E(K)$, then we define the Sklyanin algebra $A_\tau(E)$ to be the quotient of $K < X, Y, Z >$ by the ideal* *generated by the degree 2 part of the natural epimorphism to $\mathcal{O}_\tau(E)$ sending X (resp. Y and Z) to $x.t$ (resp. $y.t$ and $1.t$).*

An entirely commutative description of the quadratic relations is as the kernel of the multiplication map (in the function field $K(E)$)

$$\mu : \mathcal{L}_K(3.0) \otimes_K \mathcal{L}_K(3.\sigma) \to \mathcal{L}_K(3.0 + 3.\sigma)$$

(remember that $\sigma = -\tau$). If we know enough K-points on the elliptic curve, there is a simple procedure to find a basis for this kernel :

Proposition 2 *Let P_1, P_2, P_3 be three non-collinear points of $E(K)$ such that $P_1 + P_2 + P_3 \neq [3]\sigma$. Then the kernel is generated by*

$$q_i = l_{P_i+[2]\tau, P_{i+1}-\tau} \otimes \psi(l_{P_i,P_{i+2}}) - \alpha_i l_{P_i+[2]\tau,P_{i+2}-\tau} \otimes \psi(l_{P_i,P_{i+1}})$$

where subscripts are taken mod 3, $\alpha_i \in \overline{K}$ and $l_{Q,R}$ is a fixed equation of the line through Q and R. If there is a point in $E(K)$ such that it and its translate under τ do not lie on any of these lines, then the $\alpha_i \in K$.

Proof : Let $l, l' \in \mathcal{L}(3.0)$ such that their associated lines L and L' intersect E in R_1, R_2, R_3 (resp. S_1, S_2, S_3) then the image of $l \otimes \psi(l')$ in $\mathcal{L}(3.0 + 3.\sigma)$ has divisor

$$R_1 + R_2 + R_3 + (S_1 - \tau) + (S_2 - \tau) + (S_3 - \tau) - 3.0 - 3.\sigma$$

Note that the $S_i - \tau$ are not colinear unless $[3]\tau = 0$. If we would have another line in this divisor,then we would have another element $l_1 \otimes \psi(l'_1)$ mapping to the same element and hence there is a constant $\alpha \in \overline{K}$ s.t.

$$l \otimes \psi(l') - \alpha l_1 \otimes \psi(l'_1)$$

lies in the kernel. If we assume e.g. that $R_1, S_2 - \tau$ and $S_3 - \tau$ are colinear then such a situation occurs precisely if $R_1 = S_1 + [2]\tau$. This shows that the three elements belong to the kernel of the multiplication map.

Now, assume they are linearly dependent i.e.

$$aq_1 + bq_2 + cq_3 = 0 \text{ in } \mathcal{L}(3.0) \otimes \mathcal{L}(3.\sigma)$$

If we evaluate this equality in the $\mathcal{L}(3.\sigma)$ component in the point $P_1 - \tau$ and if we use that the P_i are not colinear then we get that $l_{P_2+[2]\tau, P_1-\tau}$ and $l_{P_3+[2]\tau, P_1-\tau}$ must determine the same line. As $P_2 \neq P_3$ this means that $P_2 + [2]\tau = -P_3 - [2]\tau - P_1 + \tau$, a contradiction by assumption. The last statement is obvious by evaluating the relation in the extra point. □

Of course, if E/K and $\tau \in E(K)$ we do not really need all the points to be K-rational. It suffices that the defining lines are K-defined and we have a K-rational point not lying (as well as its translate) under τ) on any of the lines to have the three base-elements defined over K (and hence the elliptic algebra to be defined over K).

In fact, we can deduce from the proof of the first theorem

Proposition 3 *If E/K , $\tau \in E(K)$ and there exists a K-defined line l s.t. x, l and one of the two tangent line to E described above are not concurrent and l avoids $[\mathbb{Z}]\tau$. Then, the quadratic relations of $\mathcal{O}_\tau(E)$ (and hence $A_\tau(E)$) are defined over K.*

Proof : As the divisors 3.0, $3.\sigma$ and $3.0 + 3.\sigma$ are K-defined the corresponding vectorspaces have basises of functions from $K(E)$. Moreover, one observes that

$$\mu_K : \mathcal{L}_K(3.0) \otimes \mathcal{L}_K(3.\sigma) \rightarrow \mathcal{L}_K(3.0 + 3.\sigma)$$

is surjesctive. As tensoring with $\overline{K}$ gives a three dimensional kernel of $\mu_K \otimes \overline{K}$ we also have that $Ker(\mu_K)$ is three dimensional. □

2.3 The twisted Weierstrass equation

By definition, we have an epimorphism :

$$A_\tau(E) \rightarrow \mathcal{O}_\tau(E)$$

which is an isomorphism upto degree 2 and having a one-dimensional kernel in degree 3.We now want to show that this space is generated by a central element c_3 which plays the role of a twisted Weierstarss equation. That is, we ultimately want to show that

$$A_\tau(E)/(c_3) \simeq \mathcal{O}_\tau(E)$$

which will be the basis of all computations within the Sklyanin algebra. This turns out to be substantially harder than the arguments given before and we were not able to eliminate all sheaf-theory out of the proof. Still, we hope that the following may be of help to the reader of [4, §6].

Equip E with its Zariski topology and the structure sheaf $\mathcal{O}_E$ which has as sections on the open set U

$$\mathcal{O}_E(U) = \{f \in \overline{K}(E)|div(f)|U \geq 0\}$$

i.e. those functions which can only have poles in the complement. Similarly, for each $D \in Div(E)$ one defines a sheaf of $\mathcal{O}_E$-modules $\mathcal{O}(D)$ by its sections on opens

$$\mathcal{O}(D)(U) = \{f \in \overline{K}(E)|(div(f) + D)|U \geq 0\}$$

so we recover $\mathcal{L}(D)$ as the global sections.Conversely, every sheaf of $\mathcal{O}_E$-modules which is locally free of rank one is of the form $\mathcal{O}(D)$ for some $D \in Div(E)$. We also have a sheaf version of Riemann-Roch stating that

$$deg(D) = dim H^0(E, \mathcal{O}(D)) - H^1(E, \mathcal{O}(D)) = \chi(\mathcal{O}(D))$$

where H^0 are the global sections and H^1 its first derived functor. The only thing you need to know about these is that they turn short exact sequences into long exact sequences and so if $0 \rightarrow \mathcal{A} \rightarrow \mathcal{B} \rightarrow \mathcal{C} \rightarrow 0$ is an exact sequence of $\mathcal{O}_E$-modules then

$$\chi(\mathcal{A}) - \chi(\mathcal{B}) + \chi(\mathcal{C}) = 0$$

Now, let us return to our exact sequence

$$0 \rightarrow Ker(\mu) \rightarrow \mathcal{L}(30) \otimes \mathcal{L}(3\sigma) \rightarrow \mathcal{L}(30 + 3\sigma) \rightarrow 0$$

then we claim :

Proposition 4 *There is a divisor $D \in Div(E)$ with $deg(D) = -3$ such that the sequence*

$$0 \rightarrow \mathcal{O}(D) \rightarrow Ker(\mu) \otimes \mathcal{O}_E \rightarrow \mathcal{L}(30) \otimes \mathcal{O}(3\sigma) \rightarrow \mathcal{O}(30 + 3\sigma) \rightarrow 0$$

induced by the sequence above is exact

Proof : It is sufficient to prove this in the stalks or in the residue fields of any point say P. That is we have a sequence

$$Ker(\mu) \otimes \overline{K} \xrightarrow{\alpha} \mathcal{L}(30) \otimes \overline{K} \xrightarrow{\beta} \overline{K} \rightarrow 0$$

and we only have to show that $Im(\alpha)$ is at least 2-dimensional in any point P. Choose Q, R s.t. $P + Q + R \neq -4\tau$ then we know already that $Ker(\mu)$ contains the elements

$$\begin{array}{lcl} l_{Q+2\tau,R-\tau} \otimes \phi(l_{Q,P+\tau}) & - & l_{Q+2\tau,P} \otimes \phi(l_{Q,R}) \\ l_{R+2\tau,Q-\tau} \otimes \phi(l_{R,P+\tau}) & - & l_{R+2\tau,P} \otimes \phi(l_{Q,R}) \end{array} \tag{1}$$

Under α this maps are send to resp. $-l_{Q+2\tau,P} \otimes a$ and $-l_{R+2\tau,P} \otimes b$ for $a, b \in K^*$. If $Im(\alpha)$ would be one-dimensional in P then these two lines must coincide giving $P + Q + R = -4\tau$ a contradiction by assumption.

Then, $Ker(\mu) \otimes \mathcal{O}_E \rightarrow \mathcal{L}(30) \otimes \mathcal{O}(3\sigma)$ has as its kernel a locally free $\mathcal{O}_E$-module of rank one whence of the form $\mathcal{O}(D)$. Applying χ on the sequence we get

$$deg(D) = 3\chi(\mathcal{O}_E) - 3\chi(\mathcal{O}(30)) + \chi(\mathcal{O}(30 + 3\sigma)) = 0 - 9 + 6 = -3$$

□

In fact, one can see that $D = 30 - 6\sigma$. Using this sequence it is then possible to continue as in [4, p.76-79] to arrive at the isomorphism

$$A_\tau(E)/(c_3) \simeq \mathcal{O}_\tau(E)$$

For more details the reader is referred to [11].

3 Defining equations of Sklyanin algebras

In this section we will calculate the defining quadratic relations of the Sklyanin algebras $A_\tau(E)$ associated to a point $(E, \tau) \in X_1(n)(K)$ whenever $X_1(n)$ is rational,i.e. $n \leq 10$ or $n = 12$ using proposition 2.

A point in $X_1(n)(K)$ is represented by an elliptic curve E in Weierstrass form and $\tau = [0 : 0 : 1]$ of order n. If $n \geq 7$ there are enough K-rational points in the subgroup generated by τ to satisfy the requirements of proposition 2 and obtain the $\alpha_i \in K$. For smaller torsion groups we have to vary the triples of non-colinear points as well as the point in which we evaluate to determine the constant. Sometimes (as in the $n = 2$ case) we even have to use K-linear lines avoiding the subgroup.

Let us briefly recall how points in $X_1(n)(K)$ determine Weierstrass equations such that $\tau = [0 : 0 : 1]$ has order n. First, starting with a pair (E, τ) we may always apply a linear transformation to place τ at the origin.The equation of E then becomes

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x$$

It is easy to verify that the order of $\tau = [0 : 0 : 1]$ is 2 iff $a_3 = 0$ and it is 3 iff $a_2 = 0$. If $n \geq 4$ then by a substitution $x = u^2x'$ and $y = u^3y'$ we can make $a_2 = a_3 \neq 0$ and changing notation we get as the equation of the elliptic curve

$$E : y^2 + (1 - c)xy - by = x^3 - bx^2$$

for $b, c \in K$.Of course, the discriminant of this equation must be non-zero. In order to get the defining equations of the modular curves $X_1(n)$ one merely computes the coordinates $[i]\tau$ and finds the conditions on b and c to ensure that $[n]\tau = O = [0 : 1 : 0]$.

For example let us compute $X_1(4)$. We have

$$\begin{array}{rcl} \tau & = & [0 : 0 : 1] \\ [2]\tau & = & [b : bc : 1] \\ [3]\tau & = & [c : b - c : 1] \\ [4]\tau & = & [bc(b - c) : b^2(1 + c - b) : c^3] \end{array} \qquad (2)$$

So $[4]\tau = O$ iff $c = 0$ and the discriminant is $b^4(1 + 16b)$ gives the restriction on b such that the pair (E, τ) determines a point on $X_1(4)$.

For a complete list of parametrizations of the rational points on $X_1(n)$ for $n \leq 10$ or $n = 12$ we refer to [8, Table 3].

Of course, the method provided by proposition 2 to obtain the defining equations of the Sklyanin algebras is not restricted to the cases when $X_1(n)$ is rational. In the second part of these notes we will (as an example) derive the defining equations in the cases $n = 11$ (where $X_1(11)$ has genus one) and $n = 13$ (where $X_1(13)$ has genus two).

By a result of B. Mazur [14] we know that the largest order of a torsion point on an elliptic curve defined over $\mathbb{Q}$ is ≤ 10 or is 12. Therefore, the calculations in this section can also be seen as giving all Sklyanin algebras (finite over their centers) defined over $\mathbb{Q}$. If in addition to giving the largest order of torsion one specifies the full torsion group over $\mathbb{Q}$, this gives extra restrictions on the parameter d which again can be read off from [8, Table 3].

3.1 The larger torsion groups

If $ord(\tau) \geq 8$ there is a uniform procedure to get hold of the defining equations for $A_\tau(E)$:

Proposition 5 *If E/K and τ is a torsion point of order ≥ 8, then the quadratic relations of $A_\tau(E)$ are defined over K and are generated by*

$$l_{0,2,n-2} \otimes \psi(l_{0,3,n-3}) - \alpha_1 l_{2,2,n-4} \otimes \psi(l_{0,1,n-1})$$

$$l_{2,3,n-5} \otimes \psi(l_{0,1,n-1}) - \alpha_2 l_{3,n-1,n-2} \otimes \psi(l_{1,3,n-4})$$

$$l_{5,n-1,n-4} \otimes \psi(l_{1,3,n-4}) - \alpha_3 l_{0,5,n-5} \otimes \psi(l_{0,3,n-3})$$

where $l_{i,j,k}$ denotes a fixed equation of the line through $[i]\tau$, $[j]\tau$ and $[k]\tau$ and the $\alpha_i \in K$ are obtained by evaluating in τ.

Proof : This is a special case of proposition 2. We take as triple of non-colinear points $P_1 = 0, P_2 = \tau$ and $P_3 = [3]\tau$. We can obtain the α_i by evaluating at τ as τ does not lie on any of the left (relative to $\otimes$) lines and $[2]\tau$ does not lie on any of the right lines (at least if $n \geq 7$). Therefore, all $\alpha_i \in K$. □

3.1.1 8-torsion

The elliptic curve has defining equation :

$$E : y^2 + (1 - \frac{(2d-1)(d-1)}{d})xy - (2d-1)(d-1)y = x^3 - (2d-1)(d-1)x^2$$

such that the discriminant

$$\frac{1}{d^4}(d-1)^8(2d-1)^4(1-8d+8d^2)$$

is non-zero. If we put $e = d - 1$ and $f = 2d - 1$ then the coordinates of the points of the subgroup generated by τ are

$$\begin{aligned}
\tau &= [0:0:1] \\
[2]\tau &= [ef : \frac{e^2f^2}{d} : 1] \\
[3]\tau &= [\frac{ef}{d} : \frac{e^2f}{d} : 1] \\
[4]\tau &= [ed : e^2d : 1] \\
[5]\tau &= [\frac{ef}{d} : \frac{e^2f^2}{d^2} : 1] \\
[6]\tau &= [ef : 0 : 1] \\
[7]\tau &= [0 : ef : 1] \\
[8]\tau &= [0 : 1 : 0] \qquad (3)
\end{aligned}$$

The relevant lines can be taken to have the following defining equations

$$\begin{aligned}
l_{026} &= -x + efz \\
l_{035} &= -dx + efz \\
l_{224} &= -e(3d-1)x + dy + de^2fz \\
l_{017} &= x \\
l_{233} &= -2dex + dy + e^2fz \\
l_{367} &= -x - y + efz \\
l_{134} &= -ex + y \\
l_{457} &= (1 - 3d + d^2)x - dy + defz \qquad (4)
\end{aligned}$$

From these the constants are evaluated as folows

$$\begin{aligned}
\alpha_1 = \frac{l_{026}(\tau)l_{035}([2]\tau)}{l_{224}(\tau)l_{017}([2]\tau)} &= -\frac{1}{d} \\
\alpha_2 = \frac{l_{233}(\tau)l_{017}([2]\tau)}{l_{367}(\tau)l_{134}([2]\tau)} &= \frac{d}{e} \\
\alpha_3 = \frac{l_{457}(\tau)l_{134}([2]\tau)}{l_{035}(\tau)l_{035}([2]\tau)} &= -e \qquad (5)
\end{aligned}$$

Substituting these values one then obtains that the quadratic relations of $A_\tau(E)$ are generated by the follwing three elements

$$de^2f^2Z^2 - defZX + dYX - defXZ - (2d^2 - 4d + 1)X^2 = 0$$

$$\begin{aligned} defZY - de^2f^2ZX - dY^2 - dXY + defX^2 &= 0 \\ e^3f^2Z^2 + defZY - 2de^2fZX - dY^2 + deYX - de^2fXZ & \\ +(d^2 - 3d + 1)XY + e(3d-1)X^2 &= 0 \end{aligned} \tag{6}$$

But one can simplify these generators to the following three

$$\begin{aligned} -dYX + defXZ - dXY + (2d^2 - 4d + 1)X^2 &= 0 \\ -defZY + e^2f^2ZX + dY^2 + dXY - defX^2 &= 0 \\ -e^2f^2Z^2 + efZX + XY &= 0 \end{aligned} \tag{7}$$

In this case the twisted Weierstrass equation is given by the following central element

$$c_3 = -\frac{1}{ef}(Y^3 + e^2f^2X^2Z - efX^2Y - efX^3)$$

3.1.2 9-torsion

The elliptic curve has defining equation :

$E : y^2 + (1 - d^2(d-1))xy - (d-1)d^2(1-d+d^2)y = x^3 - (d-1)d^2(1-d+d^2)x^2$

such that the discriminant

$$d^9(d-1)^9(1-d+d^2)^3(1+3d-6d^2+d^3)$$

is non-zero.

If we put $e = d - 1$ and $f = 1 - d + d^2$ then the coordinates of the points of the subgroup generated by τ are

$$\begin{aligned} \tau &= [0:0:1] \\ [2]\tau &= [d^2ef : d^4e^2f : 1] \\ [3]\tau &= [d^2e : d^3e^2 : 1] \\ [4]\tau &= [def : de^2f^2 : 1] \\ [5]\tau &= [def : d^2e^2f : 1] \\ [6]\tau &= [d^2e : d^4e^2 : 1] \\ [7]\tau &= [d^2ef : 0 : 1] \\ [8]\tau &= [0, d^2ef : 1] \\ [9]\tau &= [0:1:0] \end{aligned} \tag{8}$$

In this case the relevant lines have the following equations

$$\begin{aligned}
l_{027} &= -x + d^2efz \\
l_{036} &= -x + d^2ez \\
l_{225} &= -de(d+1)x + y + d^3e^2fz \\
l_{018} &= x \\
l_{234} &= -(3d-1)ex + y + d^2e^2fz \\
l_{378} &= -x - y + d^2efz \\
l_{135} &= -dex + y \\
l_{558} &= d(d-2)x - y + d^2efz \\
l_{045} &= -x + defz
\end{aligned} \tag{9}$$

As above the constants α_i can be evaluated to be

$$\begin{aligned}
\alpha_1 &= -\frac{1}{f} \\
\alpha_2 &= \frac{1}{de} \\
\alpha_3 &= -def
\end{aligned} \tag{10}$$

Substituting these values one then obtains generators for the space of defining quadratic relations of $A_\tau(E)$. These generators can then be simplified to

$$\begin{aligned}
d^2efXZ - YX - XY + (d^3 - d^2 - 1)X^2 &= 0 \\
d^4e^2fZX - d^2efZY + Y^2 + XY - d^2efX^2 &= 0 \\
d^2efZX + XY - d^4e^2f^2Z^2 &= 0
\end{aligned} \tag{11}$$

The twisted Weierstrass equation is given by the central element

$$c_3 = -\frac{1}{d^2ef}(Y^3 + d^4e^2f^2X^2Y - d^2efX^2Y - d^2efX^3)$$

3.1.3 10-torsion

In this case the elliptic curve has defining equation :

$$y^2+(1+\frac{d(d-1)(2d-1)}{d^2-3d+1}xy-\frac{d^3(d-1)(2d-1)}{(d^2-3d+1)^2}y = x^3-\frac{d^3(d-1)(2d-1)}{(d^2-3d+1)^2}x^2$$

such that the discriminant

$$\frac{d^{10}(d-1)^{10}(2d-1)^5(-1-2d+4d^2)}{(d^2-3d+1)^{10}}$$

is non-zero.

If we put $e = d-1, f = 2d-1$ and $g = d^2-3d+1$ then the coordinates of the points of the subgroup generated by τ are

$$\begin{aligned}
\tau &= [0:0:1]\\
[2]\tau &= [\frac{d^3ef}{g^2} : -\frac{d^4e^2f^2}{g^3} : 1]\\
[3]\tau &= [-\frac{def}{g} : \frac{de^2f^2}{g^2} : 1]\\
[4]\tau &= [\frac{d^2ef}{g^2} : -\frac{d^4e^2f}{g^3} : 1]\\
[5]\tau &= [-\frac{d^3e}{g} : \frac{d^5e^2}{g^2} : 1]\\
[6]\tau &= [\frac{d^2ef}{g^2} : -\frac{d^2e^2f^2}{g^3} : 1]\\
[7]\tau &= [-\frac{def}{g} : \frac{d^2e^2f^2}{g^2} : 1]\\
[8]\tau &= [\frac{d^3ef}{g^2} : 0 : 1]\\
[9]\tau &= [0 : \frac{d^3ef}{g^2} : 1]\\
[10]\tau &= [0:1:0]
\end{aligned} \qquad (12)$$

As equations defining the relevant lines we can take

$$\begin{aligned}
l_{028} &= -g^2x + d^3efz\\
l_{037} &= gx + defz\\
l_{226} &= -(1+d)g^2efx - g^3y + d^3e^2f^2z\\
l_{019} &= x\\
l_{235} &= (d^2+f)gex + g^2y + d^3e^2fz\\
l_{389} &= -g^2x - g^2y + d^3efz\\
l_{136} &= efx + gy\\
l_{569} &= -g(ef+dg)x - g^2y + d^3efz
\end{aligned}$$

$$l_{055} \quad = \quad gx + d^3ez \tag{13}$$

The constants α_i are then evaluated to be

$$\begin{aligned}
\alpha_1 &= \frac{g}{d} \\
\alpha_2 &= -\frac{1}{ef} \\
\alpha_3 &= -\frac{d^2ef}{g}
\end{aligned} \tag{14}$$

From this we get generators for the quadratic relations, which can subsequently be simplified to :

$$\begin{aligned}
d^3efXZ - g^2YX - g^2XY - g(1-2d-2d^2+2d^3)X^2 &= 0 \\
d^3efgZY + d^4e^2f^2ZX - g^3Y^2 - g^3XY + d^3efgX^2 &= 0 \\
d^3efg^2ZX - d^6e^2f^2Z^2 + g^4XY &= 0
\end{aligned} \tag{15}$$

In this case the twisted Weierstrass equation is given by the degree 3 central element

$$c_3 = -\frac{1}{d^3efg^2}(g^4Y^3 + d^6e^2f^2X^2Z - d^3efg^2X^2Y - d^3efg^2X^3)$$

3.1.4 12-torsion

If we put $e = d-1$,$f = 2d-1$,$g = 2d^2 - 2d + 1$ and $h = 3d^2 - 3d + 1$, then the elliptic curve has defining equation

$$E : y^2 + (1 - \frac{dfh}{e^3})xy - \frac{dfgh}{e^4}y = x^3 - \frac{dfgh}{e^4}x^2$$

such that the discriminant (which is the product of $d^4f^4g^3h^4$ and a degree 12 polynomial) is non-zero.

The coordinates of the points in the subgroup generated by τ are

$$\begin{aligned}
\tau &= [0:0:1] \\
[2]\tau &= [\frac{dfgh}{e^4} : -\frac{d^2f^2gh^2}{e^7} : 1] \\
[3]\tau &= [-\frac{dfh}{e^3} : \frac{d^2f^2h}{e^4} : 1]
\end{aligned}$$

$$\begin{aligned}
[4]\tau &= [\frac{dfg}{e^2} : -\frac{d^2f^2g^2}{e^5} : 1] \\
[5]\tau &= [-\frac{dfgh}{e^5} : \frac{d^2fgh^2}{e^7} : 1] \\
[6]\tau &= [\frac{dh}{e} : -\frac{d^2h^2}{e^3} : 1] \\
[7]\tau &= [-\frac{dfgh}{e^5} : \frac{d^2f^2g^2h}{e^8} : 1] \\
[8]\tau &= [\frac{dfg}{e^2} : -\frac{d^2f^2g}{e^3} : 1] \\
[9]\tau &= [-\frac{dfh}{e^3} : \frac{d^2f^2h^2}{e^6} : 1] \\
[10]\tau &= [\frac{dfgh}{e^4} : 0 : 1] \\
[11]\tau &= [0 : \frac{dfgh}{e^4} : 1] \\
[12]\tau &= [0 : 1 : 0]
\end{aligned} \tag{16}$$

The relevant lines can be taken to have the following equations

$$\begin{aligned}
l_{02,10} &= -e^4x + dfghz \\
l_{039} &= e^3x + dfhz \\
l_{228} &= -e^2(e^2+h)dfx - e^5y + d^2f^2ghz \\
l_{01,11} &= x \\
l_{237} &= e^3(e^2+g)dfx + e^6y + d^2f^2ghz \\
l_{3,10,11} &= -e^4x - e^4y + dfghz \\
l_{138} &= dfx + ey \\
l_{58,11} &= -e^2(def+h)x - e^4y + dfghz \\
l_{057} &= e^5x + dfghz
\end{aligned} \tag{17}$$

One can then evaluate the constants α_i to be

$$\begin{aligned}
\alpha_1 &= \frac{e^3}{g} \\
\alpha_2 &= -\frac{e^2}{df} \\
\alpha_3 &= -\frac{dfg}{e^5}
\end{aligned} \tag{18}$$

After simplifying the then obtained generators of the quadratic relations we get

$$\begin{aligned} fdghXZ - e^4XY + e(1-2d-2d^2+8d^3-6d^4)X^2 - e^4YX &= 0\\ fe^3dghZY + d^2f^2gh^2ZX - e^7Y^2 - e^7XY + fe^3dghX^2 &= 0\\ fe^4dghZX - f^2d^2g^2h^2Z^2 + e^8XY &= 0 \; (19)\end{aligned}$$

The twisted Weierstrass equation is given by the following central degree 3 element

$$c_3 = -\frac{1}{fe^4dgh}(e^8Y^3 + f^2d^2g^2h^2X^2Z - fe^4dghX^2Y - fe^4dghX^3)$$

3.2 The small torsion-groups

When $n \leq 7$ the above appoach fails.However, we can hope to obtain the defining equations by choosing another triple of non-colinear points P_i s.t. $\sum P_i \neq -[3]\tau$. Unfortunately, this approach only works for $n = 7$:

3.2.1 7-torsion

The elliptic curve must then have the equation

$$y^2 + (1+d-d^2)xy + (d^2-d^3)y = x^3 + (d^2-d^3)x^2$$

where $d \in K$ satisfying the restriction

$$d^7(d-1)^7(d^3-8d^2+5d+1) \neq 0$$

If we put $e = d-1$ then the coordinates of the points of the subgroup generated by τ are

$$\begin{aligned} \tau &= [0:0:1]\\ [2]\tau &= [d^2e : d^3e^2 : 1]\\ [3]\tau &= [de : de^2 : 1]\\ [4]\tau &= [de, d^2e^2 : 1]\\ [5]\tau &= [d^2e : 0 : 1]\\ [6]\tau &= [0 : d^2e : 1]\\ [7]\tau &= [0:1:0] \qquad (20)\end{aligned}$$

In this case we can take as our triple of points : $P_1 = \tau, P_2 = [2]\tau$ and $P_3 = [3]\tau$. They clearly satisfy the requirements of proposition 2.

The relevant lines in this case are :

$$\begin{array}{lcl} l_{223} & = & (1-d^2)x + y + d^2e^2z \\ l_{124} & = & -dex + y \\ l_{133} & = & ex + y \\ l_{347} & = & x - dez \\ l_{115} & = & y \\ l_{257} & = & x - dez \end{array} \qquad (21)$$

Then the defining quadratic relations of $A_\tau(E)$ are generated by

$$\begin{array}{lcl} l_{223} \otimes \psi(l_{124}) & = & \alpha_1 l_{133} \otimes \psi(l_{133}) \\ l_{124} \otimes \psi(l_{124}) & = & \alpha_2 l_{347} \otimes \psi(l_{223}) \\ l_{115} \otimes \psi(l_{133}) & = & \alpha_3 l_{257} \otimes \psi(l_{223}) \end{array} \qquad (22)$$

Evaluating the first equation in $[4]\tau$ given $\alpha_1 = d$, the second in $[5]\tau$ gives $\alpha_2 = -d$ and the third one in $[3]\tau$ gives $\alpha_3 = -1$.

Substituting these values we get generators of the quadratic relations which can then be simplified to the following form (where $e = d - 1$ and $f = d^2 - d - 1$)

$$\begin{array}{rcl} d^4e^2Z^2 - d^2eZX - XY & = & 0 \\ d^3e^2ZX + Y^2 + XY - d^2eX^2 - d^2eZY & = & 0 \\ YX - d^2eXZ + XY - fX^2 & = & 0 \end{array} \qquad (23)$$

The twisted Weierstrass equation is given in this case by the central degree 3 element

$$c_3 = -\frac{1}{d^2e}(Y^3 + d^4e^2X^2Z - d^2eX^2Y - d^2eX^3)$$

If $n = ord(\tau) \leq 6$ there is no triple of non- colinear points P_1, P_2, P_3 satisfying $P_1 + P_2 + P_3 \neq -[3]\tau$ s.t. the three constants α_i from proposition 2 can be obtained by evaluating in a point from the subgroup generated by τ.

Of course, one can vary the triples until one has found three linear independent quadratic relations or evaluate in other (even sometimes non K-rational points) points of E. We will leave the gruesome details of the computations to the interested reader. We will merely give the defining relations and the twisted Weierstrass equation in each case.

3.2.2 2-torsion

The elliptic curve has defining equation :

$$E : y^2 = x^3 + ax^2 + bx$$

with discriminant (i.e. $a^2b^2 - 4b^3$) non-zero.

The coordianates of the points in the subgroup are

$$\begin{aligned} \tau &= [0:0:1] \\ [2]\tau &= [0:1:0] \end{aligned} \tag{24}$$

The defining relations of $A_\tau(E)$ are generated by

$$\begin{aligned} ZX + \frac{1}{b}Y^2 + XZ + aZ^2 &= 0 \\ XY + YX &= 0 \\ X^2 - bZ^2 &= 0 \end{aligned} \tag{25}$$

The twisted Weierstrass equation is given by

$$c_3 = Y^3 + bXZY - bXYZ + aX^2Y$$

3.2.3 3-torsion

The defining equation of the elliptic curve is

$$E : y^2 + axy + by = x^3$$

satisfying $a^3b^3 - 27b^4 \neq 0$.

The coordinates of the points in the subgroup generated by τ are

$$\begin{aligned} \tau &= [0:0:1] \\ [2]\tau &= [0:-b,1] \\ [3]\tau &= [0:1:0] \end{aligned} \tag{26}$$

The defining quadratic relations of $A_\tau(E)$ are generated by

$$\begin{aligned} aX^2 + YX + XY + bXZ &= 0 \\ aZX + \frac{1}{b}Y^2 + ZY + bZ^2 &= 0 \end{aligned}$$

$$XY - bZX = 0 \tag{27}$$

In this case there are four independent central elements of degree 3

$$X^3, Y^3, ZY^2 + YZY + Y^2Z$$

and the twisted Weierstrass equation

$$c_3 = Y^3 + XZY - XYZ + \frac{a}{b}X^2Y$$

3.2.4 4-torsion

The elliptic curve is given by the equation

$$E : y^2 + xy - dy = x^3 - dx^2$$

with the restriction $d^4(1 + 16d) \neq 0$.

The coordinates of the points in the subgroup generated by τ are

$$\begin{aligned} \tau &= [0 : 0 : 1] \\ [2]\tau &= [d : 0 : 1] \\ [3]\tau &= [0 : d : 1] \\ [4]\tau &= [0 : 1 : 0] \end{aligned} \tag{28}$$

The defining relations of $A_\tau(E)$ are generated by

$$\begin{aligned} dX^2 - Y^2 - XY + dZY &= 0 \\ dXZ - XY - YX - X^2 &= 0 \\ d^2Z^2 - dZX - XY &= 0 \end{aligned} \tag{29}$$

The twisted Weierstrass equation is given by :

$$c_3 = -\frac{1}{d}(y^3 + d^2X^2Z - dX^2Y - dX^3)$$

3.2.5 5-torsion

The elliptic curve has defining equation

$$E : y^2 + (1 - d)xy - dy = x^3 - dx^2$$

whith the restriction that $d^5(d^2 - 11d - 1) \neq 0$.

The coordinates of the points in the torsion group generated by τ are

$$\begin{aligned} \tau &= [0:0:1] \\ [2]\tau &= [d:d^2:1] \\ [3]\tau &= [d:0:1] \\ [4]\tau &= [0:d:1] \\ [5]\tau &= [0:1:0] \end{aligned} \tag{30}$$

The quadratic relations for $A_\tau(E)$ are generated by

$$\begin{aligned} Y^2 - dX^2 + XY + d^2ZX - dZY &= 0 \\ d^2Z^2 - XY - dZX &= 0 \\ XY + YX + (1-d)X^2 - dXZ &= 0 \end{aligned} \tag{31}$$

The twisted Weierstarss equation is given by

$$c_3 = -\frac{1}{d}(Y^3 + d^2X^2Z - dX^2Y - dX^3)$$

3.2.6 6-torsion

The elliptic curve has defining equation

$$E: y^2 + (1-d)xy - (d+d^2)y = x^3 - (d+d^2)x^2$$

satisfying the restriction $d^6(d+1)^3(9d+1) \neq 0$.

If we put $e = d+1$ then the coordinates of the points lying in the subgroup generated by τ are given by

$$\begin{aligned} \tau &= [0:0:1] \\ [2]\tau &= [de:d^2e:1] \\ [3]\tau &= [d:d^2:1] \\ [4]\tau &= [de:0:1] \\ [5]\tau &= [0:de:1] \\ [6]\tau &= [0:1:0] \end{aligned} \tag{32}$$

Still assuming $e = d+1$ the quadratic relations of $A_\tau(E)$ are generated by

$$d^2eZX + Y^2 + XY - deX^2 - deZY = 0$$

$$\begin{aligned} d^2e^2Z^2 - deZX - XY &= 0 \\ deXZ - YX - XY + (d-1)X^2 &= 0 \end{aligned} \qquad (33)$$

The twisted Weierstrass equation is given in this case by

$$c_3 = -\frac{1}{de}(Y^3 + d^2e^2X^2Z - deX^2Y - deX^3)$$

4 The center of Sklyanin algebras

In this section we want to present a computational method to derive the center of $A_\tau(E)$ as described by the following recent result

Theorem 2 (Tate et al.) *If τ has order n then the center of $A_\tau(E)$ is generated by c_3 and three linearly independent elements of degree n say u, v, w satisfying one and only one relation of the form*

$$\phi_3(u,v,w) + \phi_2(u,v,w)c_3^{n/3} + \phi_1(u,v,w)c_3^{2n/3} + \phi_0 c_3^n = 0$$

where ϕ_i has degree i and if $(3,n) = 1$ then $\phi_1 = \phi_2 = 0$.

The proof consists of two parts. First one proves that $C_\tau(E)$ (the center of the twisted coordinate ring $\mathcal{O}_\tau(E)$) is generated by three elements in degree n satisfying one cubic equation giving the defining equation of the isogenous curve E'. Next,one shows that the natural map $Z_\tau(E) \rightarrow C_\tau(E)$ obtained by dividing out c_3 is epimorphic. Or phrased differently : one can lift the three generators U, V, W of $C_\tau(E)$ to central degree n elements $u, v, w \in Z_\tau(E)$. Unfortunately, the proof does not give much help in actually finding the generators and the defining equations.

As far as $C_\tau(E)$ is concerned we give a satisfactory solution. It is generated by the following three elements

$$\begin{aligned} U &= XZ^{n-1} + ZXZ^{n-2} + \ldots + Z^{n-1}X + a_X Z^n \\ V &= YZ^{n-1} + ZYZ^{n-2} + \ldots + Z^{n-1}Y + a_Y Z^n \\ V &= Z^n \end{aligned} \qquad (34)$$

where the constants a_X and a_Y can be computed from the coordinates of the points in the cyclic subgroup generated by τ.Moreover, we can calculate explicitly the cubic equation satisfied among them which is the Weierstrass equation of E' the coefficients of which are again function of the coordinates of points from $< \tau >$. Even for small values of n it is nearly impossible to verify the obtained result. For example, for $n = 5$ it took more than 200 hours to verify the cubic relation on a DecStation 3100.

Lifting the generators U, V, W to $Z_\tau(E)$ is done as in Tate's proof by lifting inductively to the center of the quotient of $A_\tau(E)$ by powers of c_3. This procedure becomes rapidly untractable and it would be desirable (and necessary) to have a better method.

Even if we succeed in obtaining the degree n central elements u, v, w and if 3 does not divide n (in which case we know that the unique defining equation ought to be

$$\alpha c_3^n = \phi(u, v, w)$$

where ϕ is the Weierstrass equation of E' found above), there still remains the problem of determining the constant α. Again, it is impossible to find α by working with "affine" in $A_\tau(E)$ for $n \geq 4$. Perhaps the best chance we have to obtain α is working in the quotient of the Sklyanin algebra by 2 independent central elements of degree n (of course determining a point in $\mathbb{P}^2$ not lying on E') or equivalently, by evaluating the equation in the corresponding fat point. Even this approach requires considerable patience and should be improved drastically.

In this section we fully describe $Z_\tau(E)$ if $n = 2, 4$ or 5 and give generators and cubic relation for $C_\tau(E)$ for $n \leq 10$. As verifying or contradicting cyclicity crucialy depends upon knowing a precise description of $Z_\tau(E)$ it is hoped that someone can improve drastically upon the results obtained.

4.1 The center of $\mathcal{O}_\tau(E)$

Let $n = ord(\tau)$ then we know that the center of the skew polynomial ring $K[t, \psi]$ equals

$$K(E)^\psi[t^n]$$

We can consider the invariant field $K(E)^\psi$ as the functionfield of the isogenous elliptic curve $E' = E/ < \tau >$ i.e. the quotient elliptic curve by deviding out the subgroup generated by τ, see [17, III,§4] (observe that E'/K if E/K and $\tau \in E(K)$ by [17, III.4.13.2]).

Hence, we have a clear picture of the skew polynomial ring and its center. We now want to understand the center of the twisted coordinate ring $\mathcal{O}_\tau(E)$.

The following result was proved in [19] :

Theorem 3 (Tate et al.) *If $ord(\tau) = n$ then the center of $\mathcal{O}_\tau(E)$ is generated by three elements of degree m satisfying a cubic relation.*

We aim to deduce this result by giving a computational procedure to find the generators and the specific cubic relation among them starting from the Weierstrass equation of the elliptic curve E and the coordinates of the point τ. This procedure is a reformulation of results due to J. Vélu [20] which we recall briefly :

Let E be given by the affine presentation :

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

and τ a torsion point on E of order n. Then, we can consider the following two functions in $K(E') = K(E)^{\psi}$:

$$u(P) = \sum_{i=0}^{n-1} x(P + [i]\tau) - \sum_{i=1}^{n-1} x([i]\tau)$$

$$v(P) = \sum_{i=0}^{n-1} y(P + [i]\tau) - \sum_{i=1}^{n-1} y([i]\tau)$$

Vélu shows that $K(E') = K(u, v)$ and that u and v are related by a Weierstrass equation :

$$v^2 + A_1uv + A_3v = u^3 + A_2u^2 + A_4u + A_6$$

where $A_i = a_i$ for $1 \leq i \leq 3$ and the others can be computed as follows.

Define

$$\alpha = \sum_{i=1}^{\frac{m-1}{2}} f([i]\tau) + g([\frac{m}{2}]\tau)$$

$$\beta = \sum_{i=1}^{\frac{m-1}{2}} (h([i]\tau) + x([i]\tau)f([i]\tau)) + h([\frac{m}{2}]\tau) + x([\frac{m}{2}]\tau)g([\frac{m}{2}]\tau)$$

where we consider only integer multiples of τ to attribute and the functions f, g and h are defined as :

$$f \;=\; 6x^2 + b_2x + b_4$$

$$\begin{aligned} g &= 3x^2 + 2a_2x + a_4 - a_1y \\ h &= 4x^3 + b_2x^2 + 2b_4x + b_6 \end{aligned} \tag{35}$$

where as usual $b_2 = a_1^2 + 4a_2, b_4 = a_1a_3 + 2a_4$ and $b_6 = a_3^2 + 4a_6$.Then A_4 and A_6 are given by :

$$\begin{aligned} A_4 &= a_4 - 5\alpha \\ A_6 &= a_6 - b_2\alpha - 7\beta \end{aligned} \tag{36}$$

So, the Weierstrass equation of the isogenous curve $E' = E/ < \tau >$ can be readily computed from that of E and the coordinates of all $[i]\tau$.

Let us return to our study of the center of $\mathcal{O}_\tau(E)$:

Proposition 6 *Let $X = x.t, Y = y.t$ ad $Z = 1.t$ be the generators of $\mathcal{O}_\tau(E)$ where τ is a torsion point on E with order m . Then, the center of $\mathcal{O}_\tau(E)$ is generated by the following three elements in degree m :*

$$U = XZ^{m-1} + ZXZ^{m-2} + ... + Z^{m-1}X - \sum_{i=1}^{m-1} x([i]\tau)Z^m$$

$$V = YZ^{m-1} + ZYZ^{m-2} + ... + Z^{m-1}Y - \sum_{i=1}^{m-1} y([i]\tau)Z^m$$

$$W = Z^m$$

These three elements satisfy the cubic relation :

$$V^2W + A_1UVW + A_3VW^2 = U^3 + A_2U^2W + A_4UW^2 + A_6W^3$$

where the coefficients A_i are computed as above.

Proof : Using the commutation relation in $K(E)[t,\psi]$ we see that $U = ut^n, V = vt^n$ and $W = t^n$ where u and v are the functions obtained by Vélu.

The statements then follow directly from the facts mentioned above. □

We will denote the coefficient of Z^n in U (resp. V) by a_X (resp. a_Y) and record the obtoined values for the parameters a_X, a_Y, A_i for $6 \leq n \leq 10$. We have included the discriminant of the isogenous curve as a test on the calculations. The cases $n \leq 5$ will be given in the next subsection.

4.1.1 6-torsion

Using the coordinates of the points in the cyclic subgroup generated by τ given in the previous section,one computes

$$\begin{aligned}
a_X &= -d(2d+3)\\
a_Y &= -d(d^2+3d+1)\\
A_1 &= 1-d\\
A_2 &= -d-d^2\\
A_3 &= -d-d^2\\
A_4 &= -5d(1-d-4d^2-3d^3)\\
A_6 &= d(1-14d-22d^2-18d^3-33d^4-19d^5)
\end{aligned} \tag{37}$$

The isogenous curve has discriminant equal to

$$-d(d+1)^2(1+9d)^6$$

4.1.2 7-torsion

Again one can use the coordinates found in the previous section to compute the parameters

$$\begin{aligned}
a_X &= -d(d-1)(d+1)\\
a_Y &= -(d-1)(d^4+d^2-d)\\
A_1 &= 1+d-d^2\\
A_2 &= -d^2(d-1)\\
A_3 &= -d^2(d-1)\\
A_4 &= -5d(d-1)(1-d+d^2)(1-5d+2d^2+d^3)\\
A_6 &= -d(d-1)(1-18d+76d^2-182d^3+211d^4\\
&\quad -132d^5+70d^6-37d^7+9d^8+d^9)
\end{aligned} \tag{38}$$

The discriminant of the isogenous curve is

$$d(d-1)(d^3-8d^2+5d+1)^7$$

4.1.3 8-torsion

The parameters in this case are (using $e = d-1$ and $f = 2d-1$)

$$a_X = -fraced(2-2d-5d^2)$$

$$
\begin{aligned}
a_Y &= -\frac{e}{d^2}(1 - 5d + 7d^2 + d^3 - 5d^4) \\
A_1 &= -\frac{1}{d}(1 - 4d + 2d^2) \\
A_2 &= -ef \\
A_3 &= -ef \\
A_4 &= \frac{5e}{d^3}(1 - 3d - 5d^2 + 33d^3 - 59d^4 + 51d^5 - 17d^6) \\
A_6 &= \frac{e}{d^5}(1 + 3d - 77d^2 + 392d^3 - 1123d^4 + 2315d^5 \\
&\quad -3721d^6 + 4388d^7 - 3362d^8 + 1460d^9 - 275d^{10})
\end{aligned} \tag{39}
$$

The discriminant of the isogenous curve is

$$-\frac{ef^2(1 - 8d + 8d^2)^8}{d^{11}}$$

4.1.4 9-torsion

Let $e = d - 1$ and $f = 1 - d + d^2$ then the parameters are

$$
\begin{aligned}
a_X &= 2de(1 + d + d^3) \\
a_Y &= de(d^6 - d^5 + d^4 + 3d^3 - 5d^2 + 3d - 1) \\
A_1 &= 1 + d^2 - d^3 \\
A_2 &= -d^2ef \\
A_3 &= -d^2ef \\
A_4 &= -5de(1 - 9d + 28d^2 - 53d^3 + 61d^4 - 47d^5 + 25d^6 - 8d^7 + d^8) \\
A_6 &= -de(1 - 23d + 167d^2 - 698d^3 + 1861d^4 - 3518d^5 + 4938d^6 \\
&\quad -5236d^7 + 4189d^8 - 2518d^9 + 1173d^{10} - 466d^{11} \\
&\quad +175d^{12} - 55d^{13} + 8d^{14} + d^{15})
\end{aligned} \tag{40}
$$

The discriminant of the isogenous curve is

$$def^3(1 + 3d - 6d^2 + d^3)$$

4.1.5 10-torsion

Let $e = d - 1, f = 2d - 1$ and $g = d^2 - 3d + 1$ then the parameters are

$$a_X = -\frac{de}{g^2}(d^4 - 3d^3 - 15d^2 + 12d - 2)$$

$$\begin{aligned}
a_Y &= \frac{de}{g^3}(d^7 - 4d^6 - 4d^5 - d^4 + 22d^3 - 22d^2 + 8d - 1) \\
A_1 &= \frac{1}{g}(1 - 2d - 2d^2 + 2d^3) \\
A_2 &= -\frac{d^3ef}{g^2} \\
A_3 &= -\frac{d^3ef}{g^2} \\
A_4 &= -\frac{5de}{g^4}(1 - 16d + 102d^2 - 352d^3 + 729d^4 - 935d^5 \\
&\quad +739d^6 - 346d^7 + 83d^8 - 7d^9 + d^{10}) \\
A_6 &= -\frac{de}{g^6}(1 - 34d + 446d^2 - 3279d^3 + 15541d^4 \\
&\quad -50891d^5 + 119674d^6 - 206431d^7 + 263424d^8 \\
&\quad -248030d^9 + 170156d^{10} - 83206d^{11} + 27930d^{12} \\
&\quad -5875d^{13} + 543d^{14} + 33d^{15} - 3d^{16}) \qquad (41)
\end{aligned}$$

The discriminant of the isogenous elliptic curve is

$$\frac{def^2(-1 - 2d + 4d^2)^{10}}{g^7}$$

4.2 The center of $A_\tau(E)$

As every element of $C_\tau(E)$ lifts to an element of $Z_\tau(E)$ by Tate's proof,we know that there exist degree $n-3$ elements U_3, V_3, W_3 in $A_\tau(E)$ such that

$$\begin{aligned}
u &= U + c_3.U_3 \\
v &= V + c_3.V_3 \\
w &= W + c_3.W_3 \qquad (42)
\end{aligned}$$

One can determine the coefficients of these elements by setting the commutators with the generators X, Y and Z equal to zero.

For larger values of n it may be desirable to compute first U_3 modulo c_3^2 and use it to compute the degree $n-6$ element U_6 such that

$$U + c_3.U_3 + c_3^2.U_6$$

is central modulo c_3^3 until one finally obtains u. Still, it turns out to be a rather time-consuming undertaking and a better method is needed.

Havind detemined u, v and w there is still a constant to be determined which we do here by computing both sides of the equality

$$\alpha c_3^n = \phi(u, v, w)$$

(at least if 3 is not a divisor of n) in a suitable quotient of $A_\tau(E)$. A more thorough investigation of fat points may lead to a more conceptual determination of this constant.

4.2.1 2-torsion

We continue to use the notations introduced before. First we describe the center of $\mathcal{O}_\tau(E)$. The three central elements of degree 2 are

$$\begin{aligned} U = XZ + ZX &= -\frac{1}{b}(Y^2 + aX^2) \\ V = YZ + ZY &= YZ + ZY \\ W = Z^2 &= \frac{1}{b}X^2 \end{aligned} \tag{43}$$

and they satisfy the cubic relation

$$V^2W = U^3 + aU^2W - 4bUW^2 - 4abW^3$$

Now, these elements are also central in $A_\tau(E)$ as they are lifted to centrals but $deg(c_3) = 3 > 2$. So, the center of $A_\tau(E)$ is generated by U, V, W and $c_3 = Y^3 + bXZY - bXYZ + aX^2Y$ and it is readily verified that they satisfy the following equation

$$U^3 + aU^2W - 4bUW^2 - 4abW^3 - V^2W = -\frac{1}{b^3}c_3^2$$

4.2.2 4-torsion

First we will describe the center of $\mathcal{O}_\tau(E)$. The three central elements of degree 4 found by the Vélu approach are

$$\begin{aligned} U &= XZ^3 + ZXZ^2 + Z^2XZ + Z^3X - dZ^4 \\ &= \frac{1}{d^3}(dXZXY - dXYZX - dX^2YZ + X^2Y^2 - X^3Y) \\ V &= YZ^3 + ZYZ^2 + Z^2YZ + Z^3Y - dZ^4 \end{aligned}$$

$$\begin{aligned} &= \frac{1}{d^3}(dZXY^2 + dYZXY + dY^2ZX - dXZXY + dXYZX \\ &\quad +dXY^2Z + dX^2YZ - X^2Y^2 + X^3Y - 2dX^4) \\ W &= Z^4 = -\frac{1}{d^3}X^4 \end{aligned} \tag{44}$$

Using the coordinates of the elements in the subgroup generated by τ given before we can calculate the coefficients of the isogenous elliptic curve

$$\begin{aligned} A_1 &= 1 \\ A_2 &= -d \\ A_3 &= -d \\ A_4 &= 5d(1-d) \\ A_6 &= d(1-12d-3d^2) \end{aligned} \tag{45}$$

Hence the center of $\mathcal{O}_\tau(E)$ is generated by U, V and W satisfying the following equation

$$V^2W + UVW - dVW^2 = U^3 - dU^2W - 5(d^2-d)UW^2 + d(1-12d-3d^2)W^3$$

We know that these elements lift to central elements in $A_\tau(E)$. Therefore, there exist $a, b, c \in K$ such that

$$u = U + c_3(aX + bY + cZ) \in Z_\tau(E)$$

Setting $uX - Xu = 0$ and $uY - Yu = 0$ gives us the values

$$\begin{aligned} a &= \frac{1}{d^3} \\ b &= 0 \\ c &= \frac{2}{d^2} \end{aligned} \tag{46}$$

Hence, U lifts to u which dot-simplifies to

$$-\frac{1}{d^4}(Y^4 - d^2XZXY + d^2XYZX + d^2X^2YZ - dX^2Y^2 + dX^3Y - d^2X^4)$$

Similarly, V lifts to a central element

$$v = V + c_3(aX + bY + cZ)$$

and calculating the commutators with X and Y gives

$$\begin{aligned} a &= 0 \\ b &= \frac{1}{d^3} \\ c &= -\frac{1}{d^2} \end{aligned} \tag{47}$$

and the corresponding v dot-simplifies to

$$\frac{1}{d^4}(d^2ZXY^2 + d^2YZXY + d^2Y^2ZX + Y^4 - d^2XZXY + d^2XYZX$$

$$+d^2XY^2Z - dXY^3 + d^2X^2YZ - dX^2Y^2 - d^3X^3Z + (d^2+d)X^3Y - 2d^2X^4)$$

Finally, W lifts to a central element of the form

$$w = W + c_3\frac{1}{d^3}Z = -\frac{1}{d^3}X^4$$

Hence, the center of $A_\tau(E)$ is generated by u, v, w and c_3 satisfying one defining equation

$$u^3 - du^2w - 5(d^2-d)uw^2 + d(1-12d-3d^2)w^3 - v^2w - uvw - dvw^2 = \alpha c_3^4$$

where α is still to be determined. The exact value of α can best be obtained by evaluating the equation on a fat point of $A_\tau(E)$.In the next subsection we will give an example of how to do this. (I think it is $\alpha = -\frac{1}{d^8}$ here).

4.2.3 5-torsion

Using the Vélu approach and the coordinates of the points in the subgroup generated by τ we know that the center of $\mathcal{O}_\tau(E)$ is generated by the following three elements

$$\begin{aligned} U &= XZ^4 + ZXZ^3 + Z^2XZ^2 + Z^3XZ + Z^4X - 2dZ^5 \\ &= \frac{1}{d}(dXZX^2Y - dXYZX^2 - dX^2YZX + d^2X^3ZX - dX^3YZ \\ &\quad +X^3Y^2 + (d-1)X^4Y \\ V &= YZ^4 + ZYZ^3 + Z^2YZ^2 + Z^3YZ + Z^4Y - d(d+1)Z^5 \\ &= \frac{1}{d^4}(dZX^2Y^2 + dYZX^2Y + dY^2ZX^2 + (d^2-d)(XZX^2Y - XYZX^2) \end{aligned}$$

$$\begin{aligned}
& +dXY^2ZX + (d-d^2)X^2YZX + dX^2Y^2Z + (d^3-d^2)X^3ZX \\
& +(d-d^2)X^3YZ + (d-1)X^3Y^2 + (d^2-2d+1)X^4Y - (d^2+2d)X^5 \\
W &= Z^5 = -\frac{1}{d^4}X^5 \qquad (48)
\end{aligned}$$

Using the Vélu formulas we obtain the coefficients of the isogenous elliptic curve

$$\begin{aligned}
A_1 &= 1-d \\
A_2 &= -d \\
A_3 &= -d \\
A_4 &= -5d(d^2+2d-1) \\
A_6 &= -d(d^4+10d^3-5d^2+15d-1) \qquad (49)
\end{aligned}$$

Therefore, the center of $\mathcal{O}_\tau(E)$ is generated by U, V and W satisfying the defining equation

$$V^2W + (1-b)UVW - bVW^2 =$$

$$U^3 - bU^2W - 5b(b^2+2b-1)UW^2 - b(b^4+10b^3-5b^2+15b-1)W^3$$

Again, using Tate's result we know that U, V and W lift to central elements of $A_\tau(E)$.For example, there exist $\alpha, \beta, \gamma, \delta, \epsilon, \varepsilon \in K$ such that $u = U + c_3(\alpha X^2 + \beta XY + \gamma XZ + \delta Y^2 + \epsilon YZ + \varepsilon ZX)$ is central. Again, one can determine these coefficients by computing the commutators with X, Y or Z.

One obtains after some computation that

$$\begin{aligned}
u &= U + \frac{1}{d^5}(d(d-2)ZX - d(d+1)XZ + (2d-1)XY)c_3 \\
v &= V + \frac{1}{d^5}(d(1-2d)ZX - d(d+1)YZ - (d+1)Y^2 \\
& +d(d-2)XY + d(d+1)X^2)c_3 \\
w &= W - \frac{1}{d^6}(d(d+1)ZX + (d+1)XY)c_3 \qquad (50)
\end{aligned}$$

One can dot-"simplify" these elements to obtain

$$\begin{aligned}
u &= \frac{1}{d^6}(Y^5 + d^3XZX^2Y - d^3XYZX^2 - d^3X^2YZX \\
& -3dX^2Y^3 + d^4X^3ZX - d^3X^3YZ + d^2X^3Y^2
\end{aligned}$$

$$\begin{array}{rcl} & & -3d^3X^4Z + (d^3 + 2d^2)X^4Y + (3d^2 - d^3)X^5) \\ v & = & \frac{1}{d^5}(d^2ZX^2Y^2 + d^2YZX^2Y + d^2Y^2ZX^2 + (d^3 - d^2)XZX^2Y \\ & & +(d^2 - d^3)XYZX^2 + d^2XY^2ZX + XY^4 + (d^2 - d^3)X^2YZX \\ & & +d^2X^2Y^2Z - 3dX^2Y^3 + d^4X^3ZX + (d^2 - d^3)X^3YZ \\ & & +(d^2 - d)X^3Y^2 - 3d^3X^4Z + (d^3 + d^2 + d)X^4Y - d^3X^5) \\ w & = & -\frac{1}{d^6}(X^2Y^3 + d^2X^4Z - dX^4Y + (d^2 - d)X^5) \end{array} \qquad (51)$$

Therefore, we obtain that the center of $A_\tau(E)$ is generated by the elements u, v, w and c_3 satisfying one defining equation

$$u^3 + A_2u^2w + A_4uw^2 + A_6w^3 - v^2w - A_1uvw - A_3vw^2 = \alpha c_3^5$$

where the constant α is still to be determined.

A way to obtain this constant is as follows : let us compute this equality in the quotient-algebra

$$A_\tau(E)/(v, w)$$

The right-hand side becomes in this quotient

$$c_3^5 = \frac{1}{d^5}(-Y^{15} + d^{10}X^{14}Z - d^9X^{14}Y - d^9X^{15})$$

whereas the left-hand side simplifies in it to u^3 of which one can compute the coefficient of Y^{15} to be $\frac{1}{d^{18}}$. Therefore,

$$\alpha = -\frac{1}{d^{13}}$$

and we have completely determined the center of $A_\tau(E)$.

References

[1] A.A. Albert,Bull.AMS 44 (1938) 64-652, Proc. AMS 16(1965) 799-802,J.Alg. 5 (1967) 110-132, Bull.AMS 74 (1968) 438-454,J.Alg. 14 (1970) 70-72

[2] M. Artin, "Geometry of Quantum Planes",preprint MIT (1990)

[3] M. Artin,W. Schelter,Graded algebras of gobal dimension 3,Adv.Math. 66 (1987) 171-216

[4] M. Artin,J. Tate,M. Van den Bergh, "Some algebras related to automorphisms of elliptic curves",The Grothendieck Festschrift Vol 1 33-85,Birkhäuser,Boston (1990)

[5] M. Artin,J. Tate,M. Van den Bergh, "Modules over regular algebras of dimension 3",Invent. Math. (1991)

[6] R. Brauer,On normal division algebras of index five, Proc. Nat. Acad. Sci. USA 24 (1938) 243-246

[7] S. Kamienny,Torsion points on elliptic curves and q-coefficients of modular forms,preprint

[8] D. Kubert,Universal bounds on the torsion of elliptic curves,Proc. LMS 33 (1976) 193-237

[9] S.Lang,Number theory III,Encyclopaedia of Math. Sciences Vol. 60,Springer (1991)

[10] L. Le Bruyn,The arithmetic of Sklyanin algebras II : the cyclicity problem,in preparation

[11] L. Le Bruyn,"Sklyanin algebras,an introduction",in preparation

[12] L. Le Bruyn,S.P. Smith,M. Van den Bergh, Central extensions of 3-dimensional Artin-Schelter regular algebras, preprint UIA (1992)

[13] T. Levasseur,S.P. Smith,Modules over the 4-dimensional Sklyanin algebra,Bull.Soc.Math.France,to appear

[14] B. Mazur,Rational isogenies of prime degree, Inv.Math. 44 (1978) 129-162

[15] R.S, Pierce,"Associative algebras",Graduate texts in math. 88,Springer (1982)

[16] L.H. Rowen,D.J. Saltman,Dihedral algebras are cyclic,Proc. AMS 84 (1982) 162-164

[17] J. Silverman, "The Arithmetic of Elliptic Curves" Graduate texts in math. 106 Springer-Verlag (1986)

[18] E.K. Sklyanin,Some algebraic structures connected to the Yang-Baxter equation,Func.Anal.Appl. 16 (1982) 27-34

[19] J. Tate,handwritten notes (1991)

[20] J. Vélu, "Isogénies entre courbes elliptiques",C.R.Acad.Sc.Paris 273 (1971) 238-241