Sklyanin Algebras and their Symbols

Lieven Le Bruyn*

Department of Mathematics & Comp. Sci., UIA,
Belgium

December, 1992

Report no. 92-56

Division of Pure Mathematics
Department of Mathematics & Computer Science

universitaire
instelling
antwerpen

Universiteitsplein 1 B-2610 Wilrijk-Antwerpen
BELGIUM

Sklyanin Algebras and their Symbols

Lieven Le Bruyn*

Department of Mathematics & Comp. Sci., UIA,
Belgium

December, 1992 Report no. 92-56

Abstract

3-dimensional Sklyanin algebras are a new class of possible counterexamples to the cyclicity problem. In this paper we collect a few observations concerning this problem.

Key Words
Sklyanin algebras, cyclicity problem

AMS-Class. :
16W50, 14K07

* Research Associate of the NFWO (Belgium)

Sklyanin algebras and their symbols

lieven Le Bruyn*
Dept. Wiskunde en Informatica
Universitaire Instelling Antwerpen
B-2610 Wilrijk (Belgium)
lebruyn@wins.uia.ac.be

December 14, 1992

1 Introduction

The question whether every finite dimensional division algebra of prime degree is cyclic remains unsettled even after 60 years. The algebras discovered by M. Artin and W. Schelter [2] (which we now call the 3-dimensional Sklyanin algebras) provide a new construction for possible counterexamples. These algebras $A_\tau(E)$ are determined by an elliptic curve E and a point $\tau \in E$ of order p. Artin and Schelter showed that these algebras are virtually never skew polynomial rings [2, 6.11]. Still from work of M. Artin,J. Tate and M. Van den Bergh [3], [4] and especially the recent work of S.P. Smith and J. Tate [13] we can compute explicitly with these algebras. Though $A_\tau(E)$ arises from a very cyclic situation (an isogeny of elliptic curves) it turned out to be hard to prove cyclicity even for small values of $p = ord(\tau)$. In this paper we collect a few observations on the problem.

The 3-dimensional Sklyanin algebra $A_\tau(E)$ determines a sheaf of maximal orders $\mathcal{A}$ over $I\!P^2$ whose ramification divisor is the isogeneous elliptic curve $E' = E/ < \tau >$. Moreover, $A_\tau(E)$ has a cyclic division ring of fractions if and only if $\mathcal{A}$ has one. A possible approach to disprove cyclicity is as follows :

*research associate of the NFWO (Belgium) assume that $\mathcal{A}$ is cyclic and that the basefield K contains a primitive p-th root of unity. Then, $\mathcal{A}$ determines a symbol $(f(u,v),g(u,v))_p \in k_2(K(u,v))_p = K_2(K(u,v))/pK_2(K(u,v))$ with $f,g \in K[u,v]$ (u and v are affine coordinates on $\mathbb{P}^2$). If P is a point of $\mathbb{P}^2$ not lying on E' or the curves determined by f and g, then the residue central simple K-algebra $\mathcal{A}(P)$ must be cyclic with symbol $(f(P),g(P))_p \in k_2(K)_p$. If we find another way to prove cyclicity of $\mathcal{A}(P)$ allowing us to calculate its symbol,this will put restriction on the possible polynomials f and g hopefully leading to a contradiction. Similarly, we may investigate the symbols of line (or more generally curve) quotients of $\mathcal{A}$.

In section 2 we briefly recall the construction and basic properties of the Sklyanin algebras focussing on the computational point of view. As an example we include the defining equations of $A_\tau(E)$ and its center $Z_\tau(E)$ in case $ord(\tau) = 5$ as we need these facts in the final section. Similar results on the torsion cases with $ord(\tau) \leq 12$ can be found in [10].

In section 3 we prove that the point quotients $\mathcal{A}(P)$ are indeed cyclic and determine a lot of dihedral splitting fields arising from lifting points through the isogeny $\pi : E \rightarrow E'$. From this it follows that if $\mathcal{A}$ is cyclic with symbol $(f,g)_p$ then the polynomials f and g must be important invariants of the isogeny. This may in particular be useful in case K is a number field or the function field of the modular curve $X_1(p)$.

In section 4 we perform a similar study for certain line quotients $\mathcal{A}(l)$. The motivation here is not only to impose further restrictions on the possible symbol $(f,g)_p$ but equally the search of 'good' quotientalgebras $A_\tau(E)/(L)$ where $L \in Z_\tau(E)_p$. Recall that most structural results on $A_\tau(E)$ are proved using the fact that the quotient modulo a canonical central element of degree 3 is the twisted coordinate ring of the elliptic curve. It would be interesting to have more skew-ring like central quotients. Using the non-commutative Riemann-Roch theorem [14] we show that if l is the tangent line to E' in a K-rational point not lying in the image of the isogeny and if $\mathcal{A}(l)$ is a domain, then it is an order in a skew polynomial ring. Computing the tame symbols then puts heavy restrictions of f and g.

In section 5 we compute the symbol of $\mathcal{A}$ in the quaternionic case using the theory of quadratic forms. Some of the easiest line quotient symbols are also calculated.Maybe the arithmetical invariants of the conic bundle surfaces corresponding to line (or conic) quotients may prove interesting invariants of the isogeny.

In section 6 we prove that $\mathcal{A}$ is cyclic (over any basefield K) in case $p = 5$ and if $p = 7$ cyclicity follows if K is sufficiently large to contain a K-rational intersection point of a specific cubic and sextic curve in $\mathbb{P}^2$.

Summarizing, even if the 3-dimensional Sklyanin algebras turn out not to be counterexamples to the cyclicity problem, the determination of their symbol will give us a valuable new invariant containing a lot of information on the isogeny $E \to E'$.

Acknowledgement

Thanks are due to S.P. Smith for sharing preliminary versions of [13] and to J. Van Geel for explaining me the use of tame symbols.

2 Sklyanin algebras

In this section we recall some of the basic properties of 3-dimensional Sklyanin algebras. For more details we refer to the original papers [3] and [4]. For our purposes we like to stress some of the more computational points of the theory. We refer to [10] for more details.

Throughout, K will be an arbitrary field, p will be a prime number different from 3 and (E, τ) will be a K-rational point on the modular curve $X_1(p)$. That is, E will be a K-defined elliptic curve in Weierstrass form

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

(all $a_i \in K$) and $\tau \in E(K)$ will be a K-rational point of E of order p.

To such a setting we associate a quadratic Auslander regular K-algebra on three generators X, Y and Z, the 3-dimensional Sklyanin algebra $A_\tau(E)$. Its defining equations can be computed as follows. Let P_1, P_2 and P_3 be K-rational points on E s.t. $P_1 + P_2 + P_3 \neq -[3]\tau$ in the Abelian group $E(K)$,then the defining relations of $A_\tau(E)$ are generated by

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

where the subscripts i are taken modulo 3, $l_{P,Q}$ denotes the linear term in X, Y, Z determining the line in $\mathbb{P}^2 = \mathbb{P}(A_1^*)$ through P and Q and the coefficients α_i can be calculated by evaluating in a point $P \in E(K)$ s.t. P

nor $P+\tau$ lie on any of these lines. In [10] it is shown that one can always arrange things s.t. all relations have coefficients from K,i.e. $A_\tau(E)$ is a K-defined algebra.

It turns out that $A_\tau(E)$ has a central element of degree 3 which we will denote with c_3 and which plays the role of a twisted Weierstrass equation. One of the key facts in studying Sklyanin algebras is that the quotient $A_\tau(E)/(c_3)$ is the twisted coordinate ring $\mathcal{O}_\tau(E)$ of E with respect to te automorphism given by translation with τ, see [3] and [6].

Example 1 *Let $p=5$. Any K-rational point (E,τ) of $X_1(5)$ can be represented by the elliptic curve*

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

where $d \in K$ s.t. $d^5(d^2-11d-1) \neq 0$ and where $\tau = [0:0:1]$. Using the points in the cyclic subgroup generated by τ (and varying the P_i in the above construction until one has a 3-dimensional set of equations) one deduces that the quadratic relations for $A_\tau(E)$ are generated by

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

and that the twisted Weierstrass equation is given by

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

From [3] and [4] we recall that $A_\tau(E)$ is a domain of p.i.-degree p which is a finite module over its center $Z_\tau(E)$. M. Artin,W. Schelter, S.P. Smith and J. Tate [5] and [13] proved that the center $Z_\tau(E)$ is generated by c_3 (the twisted Weierstrass equation) and 3 central elements of degree p (which we will denote by U,V and W) satisfying one equation of the form

$$c_3^p = f(U,V,W)$$

where f is a cubic form describing the isogenous elliptic curve $E' = E/<\tau>$.

In [10] a computational method was given (based on results of J. Vélu [17]) to find the central elements U,V,W and the cubic f. On the level of the twisted coordinate ring $\mathcal{O}_\tau(E) = A_\tau(E)/(c_3)$ we proved that the center is generated by the following three degree p elements

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

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

$$w = Z^p$$

where $x(P)$ resp. $y(P)$ denotes the x (resp. y) coordinate of the point $P \in E(K)$. 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 can be computed explicitly from the a_i and the coordinates of $[i]\tau$ see [10, Prop.6] for more details.

By [13] we can lift every central element of $\mathcal{O}_\tau(E)$ to $Z_\tau(E)$,that is, there exist homogeneous elements u', v' and w' of $A_\tau(E)$ of degree $p-3$ s.t. $U = u + c_3u', V = v + c_3v'$ and $W = c_3w'$ and the defining equation of $Z_\tau(E)$ then has to be of the following form

$$\alpha c_3^p = U^3 + A_2U^2W + A_4UW^2 + A_6W^3 - V^2W - A_1UVW - A_3VW^2 - A_3VW^2$$

where only the coefficient α still has to be determined.

Example 2 *Continuing the $p = 5$ example above, one can compute that*

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

The elements u, v, w as defined above can be lifted to $Z_\tau(E)$ using the following 'error-correcting' terms

$$u' \;=\; \frac{1}{d^5}(d(d-2)ZX - d(d=1)XZ + (2d-1)XY)$$

$$\begin{aligned} v' &= \frac{1}{d^5}(d(1-2d)ZX - d(d+1)YZ - (d+1)Y^2 \\ &\quad +d(d-2)XY + d(d+1)X^2) \\ w' &= -\frac{1}{d^6}(d(d+1)ZX + (d+1)XY) \end{aligned} \tag{3}$$

and finally the coefficient α can be calculated to be $\alpha = -\frac{1}{d^{13}}$ giving the precise description of $Z_\tau(E)$. For more details we refer to [10, 4.2.3].

3 Fat point symbols

The connection between $A_\tau(E)$ and its center $Z_\tau(E)$ can best be understood using the following geometric picture. Let $I\!P^2$ be the projective plane $I\!P(A_\tau(E)_1^*)$ (with coordinates X, Y and Z), then E is embedded in it using the Weierstrass equation with coefficients a_i. On the other hand, define $I\!P^2_c$ be the projective plane $I\!P(Z_\tau(E)_p^*)$ (with coordinates U, V and W), then the isogeneous curve E' can be embedded in $I\!P^2_c$ using the Weierstrass equation with coefficients A_i described above. Moreover, using Vélu's formulae [17] we have an explicit map $\pi : E \rightarrow E'$.

We observe that this picture corresponds to taking determinants for degree 1 elements in $A_\tau(E)$ as follows. Let $L = aX + bY + cZ \in A_\tau(E)_1$ then L determines a line l in $I\!P^2$ which intersects E in three points P_1, P_2 and P_3. As $A_\tau(E)$ is a finite module over $Z_\tau(E)$, $det(L)$ has to belong to $Z_\tau(E)_p$ and from our knowledge on the generators of $Z_\tau(E)$ it must be a linear term in U, V and W. This linear term coresponds to the line $\pi(l)$ in $I\!P^2_c$ through the points $\pi(P_i)$ (observe that they are colinear as π is a groupmorphism). A similar argument can be used to calculate the determinant of a quadratic element of $A_\tau(E)$.

Let us see how M. Artin's theory of fat points of $A_\tau(E)$ [1] fits into this geometric picture. Let us assume for a moment that $K = \overline{K}$ is algebraically closed. A fat point-module F is a cyclic graded $A_\tau(E)$-module with Hilbert series $\frac{p}{1-t}$ and it can be shown that it has a presentation

$$F = A_\tau(E)/(A_\tau L + A_\tau M)$$

where $L \in A_\tau(E)_1$ and $M \in Z_\tau(E)_p$. Hence, F determines a unique point in $I\!P^2_c - E'$ namely the intersection of the lines determined by M and $det(L)$.

If F has the above presentation, we say that F lies on the line(module) $l = A_\tau(E)/A_\tau(E)L$. Using this description we see that two line modules l and l' determine the same set of fat points iff l and l' have the same image under the isogeny. As each of the intersection points of $\pi(l)$ with E' can be lifted to p points on E we see that there are p^2 lines l' with this property as was proved in [1].

How can we define K-rational fat point modules ? A first idea might be to take the points $I\!P^2_c(K) - E(K)$ but it may happen that no K-defined line through such a point can be lifted through the isogeny to a K-defined line in $I\!P^2$. Hence there is no K-defined fat point module with a presentation as above.

As $A_\tau(E)$ is a finite module over $Z_\tau(E)$, it defines a sheaf of orders $\mathcal{A}$ over $I\!P^2_c$ by taking as the sections over an open piece determined by an homogenous form F in the variables U, V and W the degree zero part of the central localization of $A_\tau(E)$ at powers of $F(U, V, W)$. As the ramification divisor of the order $\mathcal{A}$ is E' we have that for every point $P \in I\!P^2_c(K) - E'(K)$ the residue algebra $\mathcal{A}(P)$ is a central simple K-algebra of degree p.

If P is a fat pointmodule lying on a K-defined line module l determined by $L \in A_\tau(E)_1$, then the image of $det(L)$ in $\mathcal{P}(P)$ becomes zero and hence the image of L in $\mathcal{A}(P)$ is a zero divisor (use the Cayley-Hamilton equation). Therefore $\mathcal{A}(P)$ has to be the full matrixalgebra $M_p(K)$. This suggests the following definition

Definition 1 *A point $P \in I\!P^2_c(K) - E'(K)$ is said to represent a K-rational fat point iff $\mathcal{A}(P) \simeq M_p(K)$.*

If we can prove that $\mathcal{A}(P)$ is a cyclic K-algebra, i.e. if $\mathcal{A}(P)$ represents a symbol $(a, b)_p \in k_2(K)_p = K_2(K)/pK_2(K)$, then we can use symbol manipulation to verify whether P is a K-rational fat point.

Proposition 1 *Assume that K contains a primitive p-th root of unity. If $P \in I\!P^2_c(K) - E'(K)$, then $\mathcal{A}(P)$ is a cyclic algebra,i.e. it is a symbol $(a, b)_p$ for some $a, b \in K$.*

Proof : We will construct a splitting field L for $\mathcal{A}(P)$ by lifting a K-defined line in $I\!P^2_c$ passing through P through the isogeny to an L-defined line.

Let l_c be the line in $I\!P_c^2$ through P and $O = [0 : 1 : 0]$. Then $l_c \cap E'$ consists of two other points Q_1 and Q_2 with coordinates in $L_1 = K(l \cap E')$ which is an at most quadratic extension of K. Now, over an at worst cyclic degree p extension $L = L_1(\pi^{-1}(Q_i))$ of L_1 we can lift Q_1 through the isogeny to a point R of $E(L)$. The line l through R and τ in $I\!P^2$ has as its image under π the line l_c, so $\mathcal{A}(P) \otimes L$ has a zero-divisor whence is split. Now, L is a splitting field for $\mathcal{A}(P)$ which is at worst dihedral. Invoking a result of L.H. Rowen and D. Saltman [11] we may conclude that $\mathcal{A}(P)$ is cyclic. □

In the above proof we can replace the origin O by any point in $\pi(E(K))$ giving plenty of dihedral splitting fields for $\mathcal{A}(P)$.

Hence, if $\mathcal{A}$ were cyclic with symbol $(f, g)_p$, then these polynomials $f, g \in K[u, v]$ must be closely related to the isogeny $\pi : E \to E'$.

4 Some line symbols

In this section we study cyclicity of the central simple ring of fractions of line quotients $\mathcal{A}(l_c)$ for some line l_c in $I\!P_c^2$. Not only is this the next simplest case after having proved that all point quotients are cyclic but it is also of independent interest in the study of the Sklyanin algebra $A_\tau(E)$. Virtually all structural results on Sklyanin algebras are proved using the fact that the quotient $A_\tau(E)/(c_3) = \mathcal{O}_\tau(E)$ is a twisted coordinate ring. If τ has finite order it would be nice to know whether certain quotients of the form $A_\tau(E)/(L_c)$ with $L_c \in Z_\tau(E)_p$ have a simple structure. Translating this to the corresponding line quotent algebra $\mathcal{A}(l_c)$ we want to know whether it can be an order in a skew polynomial ring over $K(u)$.

Using the same argument as in the case of point-quotients we can prove

Proposition 2 *If l_c is a K-defined line in $I\!P_2^2$ such that $l_c \cap E'$ contains a K-rational point, then $\mathcal{A}(l_c)$ is cyclic,i.e. it determines a symbol over $K(u)$.*

Using the argument of Rowen and Saltman in [11] one can (in principle) calculate the symbol from knowledge of the dihedral splitting field $L = K(\pi^{-1}(l_c \cap E')))$. In particular, we see that $\mathcal{A}(l_c)$ has algebraic splitting fields.

We will restrict our study here to the following very special situation : l_c will be the tangent line to E' in a point $P \in E'(K)$. If $P \in \pi(E(K))$ then l_c

is the norm of the tangent line in $I\!P^2$ to E in a preimage of P whence $\mathcal{A}(l_c)$ is an order in $M_p(K(u))$. Hence we wil assume that $P \notin \pi(E(K))$ and that $\mathcal{A}(l_c)$ is an order in a division algebra $D(l_c)$.

We want to calculate the non-commutative genus of $D(l_c)$ and invoke Witt's non-commutative Riemann-Roch theorem to conclude that $D(l_c)$ is a skew polynomial ring. For more details the reader is referred to [14],[15] and [16].

Let Λ be a maximal $\mathcal{O}_{l_c}$-order in $D(l_c)$ containing $\mathcal{A}(l_c)$. Then, Λ can only be ramified in P and $-[2]P = Q$ i.e. in $l_c \cap E'$ (because the ramification divisor of $\mathcal{A}$ is E'). Moreover, Λ is totally ramified in those points. From [14, Thm 0.3.(6)] it follows that the genus of $D(l_c)$ equals

$$g_{D(l_c)} = 1 - p < 0$$

We can now invoke an unpublished result of M. Van den Bergh's Ph.D. thesis [16, Prop.6,p.20] (see [15, Prop.3.2] for a published slight extension and more details) in order to conclude

Proposition 3 *Let $P \in E'(K) - \pi(E(K))$ and l_c the tangent line in P to E'. If $\mathcal{A}(l_c)$ is an order in a division algebra $D(l_c)$ then*

$$D(l_c) \simeq L(X, \phi)$$

where L is a cyclic degree p extension of K with generating automorphism ϕ and X is a function in $K(u)$ with divisor $(P) - (Q)$ where $\{P, Q\} = l_c \cap E'$.

Two subtle points should be stressed here. First, there is no a priori reason why L should be the obvious splitting field $K(\pi^{-1}(P))$ except in cases where this is implied e.g. if K is a local field by [16, Prop.5 p 17]. Secondly, the automorphism is in general only a K-algebra automorphism i.e. it may restrict to a non-trivial automorphism on $K(u)$ see [15, p.204]. Still one can show that the algebras have the same tame symbols.

For $L(X, \phi)$ the tame symbols are as follows. Let $L = K(\alpha)$ and $u(P) = a, u(Q) = b$ then the symbol of $L(X.\phi)$ is

$$s = (\alpha, (u-a)^{p-1}(u-b))_p \in k_2(K(u))_p$$

and therefore (see e.g. [8, 20.4])

$$\partial_P(s) \quad = \quad \alpha^{p-1} \bmod K^{*p}$$

$$\begin{aligned}\partial_Q(s) &= \alpha \bmod K^{*p} \\ \partial_R(s) &= 1 \bmod K^{*p} \qquad (4)\end{aligned}$$

for all primes R of $K[u]$ different from P and Q.

If $\mathcal{A}$ is cyclic with corresponding symbol $(f(u,v), g(u,v))_p$ then the symbol of $D(l_c)$ must be $(f(l_c), g(l_c))_p$. It is clear that specifying the above tame symbols puts heavy restrictions on f and g. Moreover, this set of restriction varies if P runs through $E'(K) - \pi(E'(K))$.

5 Global symbol for $p = 2$

By now we may wonder whether $\mathcal{A}$ can ever be a symbol. Clearly, if $p = 2$ $\mathcal{A}$ is a quaternion algebra and so has to be cyclic. The theory of quadratic forms as in e.g. [9] can then be used to compute the global symbol.

We will briefly recall some of the computations performed in [10, §3.2.2 and §4.2.1].

If $\tau = [0:0:1]$ is a point of order 2 on the elliptic curve E, then E has defining equation

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

for some $a, b \in K$ such that $b^2(a^2 - 4b) \neq 0$.The defining equations of $A_\tau(E)$ are generated in this case by the following three quadratic relations

$$\begin{aligned}XZ + ZX + \frac{1}{b}Y^2 + aZ^2 &= 0 \\ XY + YX &= 0 \\ X^2 - bZ^2 &= 0 \qquad (5)\end{aligned}$$

and the twisted Weierstrass equation is given by the central cubic element

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

The center of $A_\tau(E)$ is generated by c_3 and the three degree 2 elements :

$$\begin{aligned}U &= XZ + ZX \\ V &= YZ + ZY \\ W &= Z^2 \qquad (6)\end{aligned}$$

These four generators satisfy one relation

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

Although all these facts follow from general Sklyanin algebra theory, they can in this case also derived from the classical results of Clifford algebras. For, $A_\tau(E)$ is the Clifford algebra of the (degenerate) ternary quadratic form over $K[U, V, W]$ associated to the symmetric matrix

$$\begin{pmatrix} bW & 0 & \frac{U}{2} \\ 0 & -b(U + aW) & \frac{V}{2} \\ \frac{U}{2} & \frac{V}{2} & W \end{pmatrix}$$

As the determinant of this matrix

$$D = \frac{b}{4}(U^3 + aU^2W - 4bUW^2 - 4abW^3 - V^2W)$$

is not a square in $K[U, V, W]$, the center of the Clifford algebra (at least when we localize at D) is a quadratic extension of $K[U, V, W]$ generated by the square root of $-D$ (the signed determinant) which in our notation is $\frac{c_3}{2b}$.

Here is how we can compute the symbol of the fat point corresponding to $P = [a : b : c] \in \mathbb{P}^2_c$. Substituting a, b, c for resp. U, V, W in the above symmetric matrix we obtain a ternary quadratic form over K which is non-degenerate (i.e. its determinant is a unit in K) provided $P \notin E'$. Hence we can diagonalize it to say

$$Q = (\alpha_1, \alpha_2, \alpha_3)$$

Then, there are two elements of $Br(K)_2$ we can associate to this form. The first , the Hasse invariant

$$s(Q) = [(\alpha_1, \alpha_2)_2 \otimes (\alpha_2, \alpha_3)_2 \otimes (\alpha_1, \alpha_3)_2] \in Br(K)_2$$

enables us to verify whether the quadratic form is isotropic using [9, 5.3.22]. The second one,the Witt invariant $c(Q)$ is the class in $Br(K)_2$ of the degree zero part (in the usual $\mathbb{Z}/2\mathbb{Z}$ gradation) of the Clifford algebra. This is clearly the symbol we have to compute.It can be deduced from the Hasse-invariant (which is easy to calculate knowing a diagonal representation of the quadratic form) via the relation

$$c(Q) = [s(Q) \otimes (-1, -\alpha_1\alpha_2\alpha_3)] \in Br(K)_2$$

see e.g. [9, 5.3.20].

If we want to compute the fat point symbol in points not lying on the lines $W = 0$ or $U + aW = 0$ we can diagonalize the symmetric matrix via the change of coordinates represented by the matrix

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ -\frac{U(U+aW)}{2} & \frac{VW}{2} & bW(U+aW) \end{pmatrix}$$

and obtain the diagonal form with

$$\begin{aligned} \alpha_1 &= bW \\ \alpha_2 &= -b(U+aW) \\ \alpha_3 &= \frac{bW}{4}(U+aW)(V^2W - U^3 - aU^2W + 4bUW^2 + 4abW^3) \end{aligned} \tag{7}$$

If we set $W = 1$, $f = u + a$ and $g = v^2 - u^3 - au^2 + 4bu + 4ab$, where $u = U/W, v = V/W$ then we compute the Hasse invariant to be

$$\begin{aligned} (b, -bf).(b, bfg).(-bf, bfg) &= (b, f)(bfg, -f) \\ &= (b, f).(b, -f).(g, -f) \\ &= (b, -1).(g, -f) \end{aligned} \tag{8}$$

On the other hand, the determinant is (upto squares) equal to $-bg$. Hence, the Witt-invariant is

$$\begin{aligned} (b, -1).(g, -f).(-1, bg) &= (b, -1).(g, -f).(-1, b).(-1, g) \\ &= (f, g) \end{aligned} \tag{9}$$

Lemma 1 *If $p = [u : v : 1]$ is a fat point with $u \neq -a$ then the fat point symbol is equal to*

$$(u + a, v^2 - u^3 - au^2 + 4bu + 4ab)_2 \in Br(K)_2$$

Remark 1 *To include the points at infinity we can use a different diagonalization for all points not lying on the lines $U = 0$ and $U + aW = 0$.If $p = [1 : y : z]$ is a fat point with $z \neq -\frac{1}{a}$ then the fat point symbol is equal to*

$$(y^2 + 4bz + 4abz^2, (1 + az)(1 + az - 4bz^2 - 4abz^3 - y^2))_2 \in Br(K)_2$$

One verifies that these two symbols coincide on the open set $uw \neq 0$. Finally, on the line $u + aw = 0$ the Witt-invariant (or the fat point symbol) is trivial.

Knowing the global symbol,we can calculate some of the line symbols. If we perform a change of variables $u \to u - a$ then the symbol is

$$(u, v^2 - u^3 + 2au^2 + (4b - a^2)u)$$

Let l_c be a line in $I\!P^2_c$ with $l \cap E' = \{P_1, P_2, P_3\}$ and all $P_i \in E'(K)$ with u-coordinate α_i, then the line symbol is

$$(u, -(u - \alpha_1)(u - \alpha_2)(u - \alpha_3))_2$$

From elementary elliptic curve theory it is known that $\alpha_1.\alpha_2.\alpha_3 \in K^{*2}$ and that $\alpha_i \in K^{*2}$ if $P_i \in \pi(E(K))$ see for example [12].

If all P_i lie in $\pi(E(K))$ then l_c is the norm of a K-defined line in $I\!P^2$ and hence the symbol is trivial.

If $P_1 \notin \pi(E(K))$ and l_c is the tangent line to E' in P_1, then $P_2 = P_1$ and $P_3 = -[2]P_1$ belongs to $\pi(E(K))$ (use the dual isogeny). The line symbol is

$$(u, -(u - \alpha_1)^2(u - \alpha_3))_2 = (u, -(u - \alpha_3))_2$$

and as $\alpha_3 \in K^{*2}$ all tame symbols are trivial. That is, the division algebra of $\mathcal{A}$ is unramified so it is of the form $H \otimes_K K(u)$ for some quaternion algebra H over K. However,there are plently of K-rational fat points on l_c so $H = M_2(K)$ and so the line symbol is trivial. Observe that $\mathcal{A}(l_c)$ is not a maximal order.

Observe that this case is special to $p = 2$. In this case the negative genus situation does occur when $P_1, P_2 \notin \pi(E(K))$ and $P_3 \in \pi(E(K))$. The line symbol becomes

$$(u, -(u - \alpha_1)(u - \alpha_2))_2$$

and the tame symbols in P_1 and P_2 are non-trivial. So, $\mathcal{A}(l_c)$ is an order in a division algebra and hence there will be K-defined non K-rational fat points on l_c. This division algebra is split by $L = K(\pi^{-1}(P_1)) = K\sqrt{\alpha}$ for some $\alpha \in K^*$. The line symbol is then similar to (possibly upto a term from $k_2(K)_2$)

$$(\alpha, -(u - \alpha_1)(u - \alpha_2)$$

and $\mathcal{A}(l_c)$ is an order in $L(X, \phi)$ where ϕ is conjugation on L and $X = \frac{u-\alpha_1}{u-\alpha_2}$. Observe that $\mathcal{A}(l_c)$ is not a maximal order as the division algebra is unramified in P_3 but $\mathcal{A}$ is.

If we take more general lines l_c (or conics q_c) we get division algebras over $K(u)$ whose corresponding conic bundle surfaces do no longer have to be K-rational and may have more equivalence classes of rational points under Manin's R-equivalence. This may give new interesting arithmetical invariants associated to the isogeny.

6 Global symbols for $p \leq 7$

In this section we will show that $A_\tau(E)$ is cyclic if $p = ord(\tau) \leq 7$ and K is sufficiently large. If $p = 5$ then further calculations shows that $A_\tau(E)$ is cyclic for any basefield K.

Theorem 1 *If $p \leq 7$ and if K is sufficiently large, then $A_\tau(E)$ is cyclic. Here, sufficiently large means that there is a K-rational point on a specific cubic curve (if $p = 5$) or a K-rational intersection of a specific cubic and sextic curve (if $p = 7$).*

Proof : As $A_\tau(E)$ is a graded ring and a finite module over its center $Z_\tau(E)$, the Cayley-Hamilton polynomial of every homogeneous element is homogeneous with coefficients in $Z_\tau(E)$.

In particular, let $L = \alpha X + \beta Y + \gamma Z$ be a degree one element from $A_\tau(E)$, then using the description of $Z_\tau(E)$ recalled before,we know that the Cayley-Hamilton polynomial of L must have the following form

$$L^p + g_3(\alpha, \beta, \gamma) c_3 L^{p-3} + g_6(\alpha, \beta, \gamma) c_3^2 L^{p-6} + (-1)^n Det(L) = 0$$

where g_3 (resp. g_6) is a homogeneous form of degree 3 (resp. 6) in the coefficients α, β, γ. Now, let $[\alpha : \beta : \gamma]$ be one of the intersection points of the cubic and sextic curve in $\mathbb{P}^2$ determined by g_3 and g_6 (which exists if K is sufficiently large) then the corresponding degree one element L has Cayley-Hamilton polynomial

$$L^p = Det(L) \in Z_\tau(E)$$

finishing the proof. □

If we want to remove the condition on K we have to make the above proof more explicite. It follows from the Newton-formulas that the coefficient of

X^{p-3} in the Cayley-Hamilton equation of X in a p.i.-algebra of degree p is equal to

$$\frac{1}{6}(3Tr(X)Tr(X^2) - 2Tr(X^3) - Tr(X)^3)$$

Therefore, if $L = \alpha X + \beta Y + \gamma Z$ is a degree one element in $A_\tau(E)$ we see that the cubic curve determined by $g_3(\alpha, \beta, \gamma)$ is given by

$$g_3(\alpha, \beta, \gamma).c_3 = \frac{1}{3}Tr((\alpha X + \beta Y + \gamma Z)^3)$$

Hence we have to study the K-rational points on the cubic trace curve

$$E_c : Tr((\alpha X + \beta Y + \gamma Z)^3) = 0$$

Here is how one can calculate the defining equation of E_c : first one has to know the traces of trinomials in X, Y and Z. As a trace of a trinomial is determined upto cyclic permutation of the terms,there are only 11 such traces to determine,namely the traces of

$$X^3, X^2Y, X^2Z, XY^2, XYZ, XZY, XZ^2, Y^3, Y^2Z, YZ^2, Z^3$$

On the other hand, $A_\tau(E)$ is defined via three quadratic equations. Multiplying each of these equations with X, Y and Z and taking traces we get a linear system of 9 equations among the 11 trinomial traces. The remaining degrees of freedom can then be removed by bringing in the knowledge of the trace of the central degree 3 element c_3 and the trace of X^3 (and if necessary Y^3 or Z^3) which can be read off from the Cayley-Hamilton equation of X (resp. Y or Z). Having the traces of all trinomials one then dot-simplifies $(\alpha X + \beta Y + \gamma Z)^3$ and substitues in it the trinomial traces to obtain the equation for E_c.

Let us apply this general procedure in case $p = 5$. As we know the defining equations of $A_\tau(E)$ we get the following linear system of equations among the traces of trinomials

	X^3	X^2Y	X^2Z	XY^2	XYZ	XZY	XZ^2	Y^3	Y^2Z	YZ^2	Z^3
$eq_1.X$	d	-1	$-d^2$	-1	0	d	0	0	0	0	0
$eq_1.Y$	0	d	0	-1	$-d^2$	0	0	-1	d	0	0
$eq_1.Z$	0	0	d	0	-1	0	$-d^2$	0	-1	d	0
$eq_2.X$	$d-1$	-2	d	0	0	0	0	0	0	0	0
$eq_2.Y$	0	$d-1$	0	-2	0	d	0	0	0	0	0
$eq_2.Z$	0	0	$d-1$	0	-1	-1	d	0	0	0	0
$eq_3.X$	0	1	d	0	0	0	$-d^2$	0	0	0	0
$eq_3.Y$	0	0	0	1	d	0	0	0	0	$-d^2$	0
$eq_3.Z$	0	0	0	0	1	0	d	0	0	0	$-d^2$

This system has a 2-dimensional space of solutions.One can remove the remaining degrees of freedom by observing that $Tr(c_3) = 5c_3$ and that $X^5 - \frac{1}{d}c_3X^2 \in Z_\tau(E)$ (whence $Tr(X^3) = \frac{3}{d}c_3$. This gives us all the traces of trinomials and if we substitute these values in $Tr((uX+vY+wZ)^3)$ we get that the cubic trace curve has defining equation

$$d^3u^3 + d^4u^2v - d^5v^3 + (3d^2 - d^3)u^2w + (4d^3 - d^4)uvw$$

$$-d^4v^2w + 3duw^2 + 3d^2vw^2 + (1+d)w^3$$

Perhaps surprisingly, this cubic has a K-rational point namely $[1 : 0 : -d]$, or equivalently

$$(X - dZ)^5 \in Z_\tau(E)$$

This concludes the proof of

Theorem 2 *If $p = 5$, then $A_\tau(E)$ is cyclic over any basefield K.*

If we want to study all degree one elements whose fifth power is central it is best to bring this cubic to Weierstrass form as in [7] and study its rational points by standard methods,e.g. [12]. If we perform the required transformations,the cubic has Weierstass form

$$y^2 = x^3 + (d^2 - 12d - 8)x^2 + 16(1 + 11d - d^2)x$$

which has discriminant

$$\Delta = 4096(d-8)^3d(d^2 - 11d - 1)^2$$

Hence the cubic trace curve is always a smooth elliptic curve provided $d \neq 8$.

Clearly, one may perform similar calculations for $p = 7$. Using the defining equations of [10] one obtains that

$$Tr((uX + vY + wZ)^3) = \frac{3}{e^6 d^5} f(u, v, w)$$

where $f(u, v, w)$ is the following cubic

$$(d^3 - d^2 + 3d - 2)w^3 + 3e^2 d^3 (2d - 1)vw^2 + 3ed^2(3d - 2)uw^2$$

$$-e^2 d^3 (2d^3 - 9d^2 + 3d + 1)u^2 w + e^3 d^5 (2d - 1)u^3 - e^3 d^3 (2d^4 - 9d^3 + d^2 - d + 1)uvw$$
$$-e^4 d^5 (2 - 7d + 2d^2)v^2 w - e^4 d^5 (2d^2 + 2d - 1)u^2 v + 3e^5 d^7 uv^2 - e^6 d^7 (d - 2)v^3$$

which does not have any obvious rational points.

Clearly this does not show that $A_\tau(E)$ is non-cyclic for such values of d. It merely says that no 7-th power of a degree one element in $A_\tau(E)$ belongs to the center. It is still that the 7-th power of a non-central homogeneous element of degree > 1 becomes central.

References

[1] M. Artin, Geometry of quantum planes, Contemp. Math. 124 (1992) 1-15

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

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

[4] M. Artin,J. Tate,M. Van den Bergh, Modules over regular algebras of dimension 3, Invent. Math. 106 (1991) 335-388

[5] M. Artin,W. Schelter,J. Tate, The centers of 3-dimensional Sklyanin algebras, Proceedings of the Barsotti Memorial Conference 1991, to appear

[6] M. Artin,M. Van den Bergh, Twisted homogeneous coordinate rings, J. Alg. 133 (1990) 249-271

[7] C.H. Clemens, A scrapbook of complex curve theory (1980) New York

[8] I. Kersten, Brauergruppen von Körpern, Aspects of Math. D 6 (1990) Vieweg

[9] T.Y. Lam, Algebraic theory of quadratic forms, (1973) Benjamin

[10] L. Le Bruyn, The arithmetic of Sklyanin algebras I : the defining equations, UIA-preprint 92-25 (1992) to appear

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

[12] J.H. Silverman, The arithmetic of elliptic curves, Graduate texts in math. 106 (1986) Springer

[13] S.P. Smith,J. Tate, The center of the 3 and 4-dimensional Sklyanin algebras,Artin Conference Proceedings, this volume

[14] J. Van Geel,M. Van den Bergh, Algebraic elements in division algebras over function fields of curves, Isr.J.Math 52 (1985) 33-45

[15] J. Van Geel, Maximal orders over curves, LNM 1296 (1987) 193-213

[16] M. Van den Bergh, Algebraic subfields and splitting fields of division algebras over function fields, Ph.D. thesis UIA (1985)

[17] J. Velu,Isogenies entre courbes elliptiques, C.R. Acad. Sc. Paris 273 (1971) 238-241