Math. Res. Lett. **17** (2010), *no.* 06, 1013–1028

MUSINGS ON $\mathbb{Q}(1/4)$: ARITHMETIC SPIN STRUCTURES ON ELLIPTIC CURVES

Kirti Joshi

Abstract. We introduce and study arithmetic spin structures on elliptic curves. We show that there is a unique isogeny class of elliptic curves over $\mathbb{F}_{p^2}$ which carries a unique arithmetic spin structure and provides a geometric object of weight $1/2$ in the sense of Deligne and Grothendieck. This object is thus a candidate for $\mathbb{Q}(1/4)$.

मधुर भावनओं की सुमधुर नित्य बनाता हूँ हाला,
भरता हूँ इस मधु से अपने अंतर का प्यासा प्याला,
उठा कल्पना के हाथों से स्वयं उसे पी जाता हूँ,
अपने ही में हुँ मैं साकी, पीनेवाला, मधुशाला।
मधुशाला, हरीवंश राय बच्चन [1]

1. Introduction and statement of the principal results

1.1. The problem. In this paper we attempt to provide an intrinsic approach to the problem of constructing $\mathbb{Q}(1/4)$. We show that there is, up to isomorphism, a unique geometric object which lives over $\mathbb{F}_{p^2}$, and which is equipped with ℓ-adic and p-adic realizations of weight $1/2$ in the sense of [4]. This object is thus a candidate for $\mathbb{Q}(1/4)$. This object is constructed using what we call *arithmetic spin structures on elliptic curves*. Our approach to $\mathbb{Q}(1/4)$ may be considered to be a twisted analogue of the constructions of [8, 3]. We note that the problem of constructing "fractional motives" and "exotic" Tate motives has also been studied in [1, 9, 5, 11].

We say that an elliptic curve is of *spinorial type* if its algebra of endomorphisms (we consider endomorphisms defined over the field of definition of the curve) carries a non-trivial involution of the *first kind* (see 4.1). The classification of endomorphism algebras of elliptic curves shows that an elliptic curve is of spinorial type if and only if it is supersingular and its endomorphism algebra is a quaternion algebra (see Proposition 4.1.1). Thus a supersingular elliptic curve with all its endomorphisms defined over the ground field is of spinorial type; and every supersingular elliptic curve becomes of spinorial type over some quadratic extension. By the well-known classification of isogeny classes of elliptic curves over a finite field one sees that for a given finite field there are at most two isogeny classes of elliptic curves which are of spinorial type.

Involutions of the first kind on an algebra are classified as *orthogonal or symplectic* depending on what they look like over any splitting field of the algebra. A *spin structure* (B, σ) on an elliptic curve of spinorial type is a choice of an involution σ

Received by the editors November 18, 2009.

[1] From the "Madhushālā" by Harivansh Rāi Bachchan.

of the first kind and orthogonal type (i.e of an orthogonal involution–see 2.5) on the endomorphism algebra (denoted here by B) of the curve. On a quaternion algebra, orthogonal involutions of the first kind are classified (up to isomorphism) by their discriminant. Every spin structure comes equipped with a (even) Clifford algebra (see 2.10). In the present situation, because the quaternion algebra B of endomorphisms of a supersingular elliptic curve is ramified at infinity (and at p, the characteristic of ground field), the (even) Clifford algebras $C^+(B,\sigma)$ which can arise are imaginary quadratic extensions of $\mathbb{Q}$ (see Theorem 6.2.1).

1.2. The results over $\mathbb{F}_{p^2}$. We now describe the results we obtain over $\mathbb{F}_{p^2}$ (they are also proved here for $\mathbb{F}_{p^{2n}}$ with n odd). We show (in Proposition 4.3.1) that the Frobenius endomorphism of E is a *proper similitude* of this spin structure, and the *group of proper similitudes*, denoted here by $\mathrm{GO}^+(B,\sigma)$, is the non-split torus (obtained by the restriction of scalars of $\mathbb{G}_m$ from the Clifford algebra $C^+(B,\sigma)$ of the spin structure–see Proposition 3.1.3). The *spin group (rather the general spin group)* associated to (B,σ) is again a non-split torus and is a cover of the group of similitudes (see 3.3). This allows us to speak of constructing square roots of the Frobenius endomorphism. A necessary and sufficient condition that Frobenius endomorphism have a square root in the Clifford algebra is that the Clifford algebra of the spin structure is $\mathbb{Q}[x]/(x^2+p)$ (Theorem 5.3.1). This means that the involution underlying the spin structure has discriminant $-p$; moreover as the Frobenius endomorphism is a central element operating by $\pm p$, one sees that there are spin structures for which Frobenius does not have a square root.

We show (see Theorem 6.2.1 and Corollary 6.2.3) that for an elliptic curve $E/\mathbb{F}_{p^2}$ of spinorial type, whose Frobenius endomorphism acts by multiplication by $-p$, carries a unique spin structure of discriminant $-p$ (uniqueness is up to isomorphism). For this spin structure the Frobenius endomorphism admits square roots ($\pm\sqrt{-p}$) in the Clifford algebra. This gives rise to a spinorial representation of the Weil group

$$\rho^{spin}_{E,\sigma} : W(\bar{\mathbb{F}}_{p^2}/\mathbb{F}_{p^2}) \to \mathrm{GSpin}(B,\sigma)$$

(here $B = \mathrm{End(E)}$) which lifts the canonical *similitude representation*

$$\rho_{E,\sigma} : W(\bar{\mathbb{F}}_{p^2}/\mathbb{F}_{p^2}) \to \mathrm{GO}^+(B,\sigma).$$

This spinorial representation is of weight $1/2$ in the sense that the absolute value of the eigenvalues of Frobenius is

$$\sqrt{p} = (p^2)^{1/4} = (p^2)^{(\frac{1}{2})/2}.$$

Spin structures for which the similitude representation admits a spinorial lifting are said to be *arithmetic spin structures*. Over $\mathbb{F}_{p^2}$, arithmetic spin structures of discriminant $-p$ can exists on elliptic curve of spinorial type if and only if the Frobenius endomorphism operates by $-p$; and a fortiori, there are no orthogonal involutions on the algebra $B = \mathrm{End(E)}$ with positive discriminant (where E is of spinorial type). So not all spin structures can exist or when they exist are arithmetic. The data $(E,(B,\sigma))$ consisting of elliptic curve $E/\mathbb{F}_{p^2}$ together with an arithmetic spin structure (B,σ) on E is a geometric object whose weight is half: this our candidate for $\mathbb{Q}(1/4)$. There is exactly one isogeny class of elliptic curves over $\mathbb{F}_{p^2}$ which provides such a structure and the spin structure is unique up to isomorphism. In 7.2 and 7.3 we construct the ℓ-adic and the crystalline realizations of $\mathbb{Q}(1/4)$. We note that

the Clifford algebra of spin structures (arithmetic or not) are imaginary quadratic extensions of $\mathbb{Q}$ (and so are not isomorphic to $\mathbb{Q} \times \mathbb{Q}$).

In [11] one finds a formula for the values of the Hasse-Weil zeta function of a smooth, projective variety over $\mathbb{F}_{p^2}$ at $s = 1/2$. It has been expected that this formula must have an arithmetic explanation in terms of a motive $\mathbb{Z}(1/2)$. As a consequence of our theory we prove a simple relation (see Theorem 7.6.1) between the L-function of the elliptic curve with an arithmetic spin structure and the associated spinorial representation. This is similar (in spirit) to the formula proved in [11].

The theory developed here should be viewed as a $\mathbb{Q}$-theory rather than a $\mathbb{Z}$-theory because we have worked throughout with the quaternion algebra (so up to isogeny). But for a $\mathbb{Z}$-theory one should work with orders in the quaternion algebra, as endomorphism rings arise more naturally as orders). We hope to return to this in later paper. The theory developed here can be also applied to rank two supersingular Drinfeld modules, but we will defer this to a subsequent paper as well.

1.3. Acknowledgements. This paper grew out of a talk given by N. Ramachandran on [11]. We thank him for conversations and correspondence about [11]. Thanks are also due to Preeti Raman for conversations on Clifford groups and for help with identifying $\mathrm{GSpin}(B, \sigma)$ in the case we need here. Thanks are also due to Dinesh Thakur for encouragement and for a careful reading of the manuscript. We would like to thank Christopher Deninger for comments and suggestions which have improved this manuscript. Some part of this work was carried out while the author was visiting the Tata Institute and the Université Montpellier II and we thank both for their hospitality.

2. Recollections from the theory of Clifford algebras

2.1. Preparatory remarks. The fundamental reference for what we need here is [7]. Readers unfamiliar with the theory of Clifford algebras may first want to read [2] but should bear in mind that unlike [2] we will work with a twisted situation. All facts we need about Clifford algebras constructed from quaternion algebras with orthogonal involutions are found in [7]. The reader is advised to keep that work handy while reading the present paper. Since the machinery of twisted quadratic spaces may not be familiar to the readers we have, for the reader's convenience, inserted a "recurring example" which explains the machinery in the context we need to use for the main results of this paper.

Throughout the paper F will denote a field of characteristic not equal to two (zero is allowed). The results can probably be carried out in case the characteristic is two but the details are more complicated so we will leave them aside for the moment.

2.2. Inner automorphisms. In what follows, we will work with finite dimensional algebras over a field F. Let A be a finite dimensional algebra over a field F. For an invertible $u \in A$, we write $\mathrm{int}(u) : A \to A$ for the inner automorphism of A defined by u, given explicitly by $\mathrm{int}(u)(a) = u \circ a \circ u^{-1}$ for any $a \in A$.

2.3. Involutions. Let F be a field of characteristic not equal to two. Let A/F be a finite dimensional algebra over F. An *involution of the first kind* on A is a map $\sigma : A \to A$ such that $\forall x, y \in A$,

(1) $\sigma(x+y) = \sigma(x) + \sigma(y)$,
(2) $\sigma(xy) = \sigma(y)\sigma(x)$ (so σ is an anti-morphism)
(3) $\sigma^2(x) = x$,
(4) σ is identity on the center of A.

2.4. Classification of involutions.

2.4.1. *The split case.* Let V be a finite dimensional vector space over a field extension K/F and let $b : V \times V \to K$ be a non-degenerate bilinear form with values in K. Then for any $f \in \mathrm{End_K(V)}$ we define $\sigma_b(f) \in \mathrm{End_K(V)}$ by the following property: for all $v, w \in V$ we have

$$b(v, f(w)) = b(\sigma_b(f)(v), w).$$

Then $f \mapsto \sigma_b(f)$ is a K-linear anti-automorphism of $\mathrm{End_K(V)}$, called the adjoint automorphism of $\mathrm{End_K(V)}$ with respect to the non-degenerate bilinear form b. The mapping $b \mapsto \sigma_b$ is a bijection between the equivalence classes of non-degenerate bilinear forms on V up to scalar multiples and the set of K-linear anti-automorphisms of $\mathrm{End_K(V)}$. Under this equivalence σ_b provides an involution (i.e. a K-linear anti-automorphism of order two) if and only if b is symmetric or skew-symmetric. For a proof see [7, Page 1].

2.4.2. *The general case.* We now describe involutions σ on arbitrary central simple algebras. Let (A, σ) be a pair where A/F is a central simple algebra and $\sigma : A \to A$ is an involution. Let K/F be a splitting field of A/F. Then $\sigma_K : A \otimes_F K \to A \otimes_F K$ is an involution of A_K and by the previous paragraph, we see that σ_K arises from a non-singular bilinear form which is either symmetric or skew-symmetric.

2.5. Orthogonal and symplectic involutions. Let (A, σ) be a pair as above. We say that σ is *symplectic* (resp. *orthogonal*) involution if for any splitting field K/F (and any isomorphism $A_K \to \mathrm{End_K(V)}$, the involution σ_K of A_K arises from a non-degenerate skew-symmetric (resp. symmetric) bilinear form on V.

2.6. Twisted quadratic spaces. Let F be a field (of characteristic not equal to two). A *twisted quadratic space* over F is a pair (A, σ) where A/F is a central simple algebra over F and $\sigma : A \to A$ is an involution of first kind and of orthogonal type. Morphisms of twisted quadratic spaces are defined in the obvious way.

2.7. Twisted quadratic spaces and quadratic spaces. If (A, σ) is a twisted quadratic space over F and if A is split with $A = \mathrm{End_F(V)}$, then $\sigma = \sigma_b$ for a symmetric bilinear form $b : V \times V \to F$ and the pair (A, σ) is isomorphic to the pair $(\mathrm{End_F(V)}, \sigma_\mathrm{b})$ and this is equivalent to the data (V, q_b) where $q_b : V \to F$ is the quadratic form associated to the symmetric bilinear form b. Thus in the split case the data of a twisted quadratic space is simply the data of a quadratic space. We note that the term "twisted quadratic space" was not introduced in [7] but clearly seems appropriate.

2.8. Recurring Example. This example will recur throughout and is the case we want to consider for the main results of this paper. So we provide this along for the convenience of the reader.

Let B/F be a quaternion algebra. Then B has a basis $1, i, j, k$ with $i^2, j^2 \in F^*$, $ij = k = -ji$. If $i^2 = a, j^2 = b$ we will write this algebra as $B = \left(\frac{a,b}{F}\right)$. The map $\gamma : B \to B$ given by sending

$$\gamma(x_0 + ix_1 + jx_2 + kx_3) = x_0 - ix_1 - jx_2 - kx_3$$

is the unique symplectic involution on B (see [7, Proposition 2.21, page 26]).

Every orthogonal involution σ on B is of the form

$$\sigma = \mathrm{int}(u) \circ \gamma$$

where $\gamma(u) = -u$ and $u \in B^*$ is uniquely determined up to a scalar in F^* by σ (see [7, Proposition 2.21, page 26]).

By [7, Corollary 2.8 (page 18) and Proposition 2.21 (page 26)] every quaternion algebra B/F carries both symplectic and orthogonal involutions. The reduced norm of $u \in B$ is given $\mathrm{Nrd}(u) = u\gamma(u)$, the reduced trace of $u \in B$ is given by $\mathrm{Trd}(u) = u + \gamma(u)$. Observe that u has reduced trace zero if and only if $\gamma(u) = -u$ (i.e., u is a "pure quaternion").

2.9. Discriminants.

2.9.1. *The split case.* We first describe the discriminant of a quadratic space. Let (V, q) be a non-degenerate quadratic space over F. Let b be the associated bilinear form. For a basis $e_1, \ldots, e_n$ of V, the matrix $\det(b(e_i, e_j)) \neq 0$ and its class in F^*/F^{*2} is independent of the choice of the basis $e_1, \ldots, e_n$ of V. We denote this class in F^*/F^{*2} by $\mathrm{disc}(b)$. The discriminant of (V, q) is the class

$$\mathrm{disc}(V, q) = \mathrm{disc}(q) = (-1)^{\frac{n(n-1)}{2}} \det(b) \in F^*/F^{*2}.$$

2.9.2. *The general case.* For an even degree central simple algebra A and any orthogonal involution σ, we define the determinant

$$\det(\sigma) = \mathrm{Nrd}_A(a) \in F^*/F^{*2},$$

for any element $a \in A^*$ such that $\sigma(a) = -a$. This class is again independent of the choice of such an a. The discriminant of σ is given by

$$\mathrm{disc}(\sigma) = (-1)^{\frac{\deg(A)}{2}} \det(\sigma) \in F^*/F^{*2}.$$

If $\sigma = \mathrm{int}(u) \circ \gamma$ then

$$\mathrm{disc}(\sigma) = -\mathrm{Nrd}_A(u) \in F^*/F^{*2}.$$

For a proof see [7, Page 81, Proposition 7.3(2)]. We note that the sign given in that reference is not correct (ours is correct) as can be easily seen from the proof given on [7, Pages 81-82, Proposition 7.3].

Moreover if A is a quaternion division algebra then A does not carry any orthogonal involutions with trivial discriminant (see [7, page 82, Example 7.4]).

2.10. Clifford Algebra associated to a twisted quadratic space (A, σ). Let (A, σ) be a twisted quadratic space. Then there exits a (even) Clifford algebra denoted by $C^+(A, \sigma)$ which is functorial in the pair and if $A = \mathrm{End(V)}$ for a vector space V/F, then $C^+(A, \sigma)$ agrees with the *even* clifford algebra constructed in the usual manner. See [7, page 91].

2.11. The center of the Clifford algebra. Let us assume from now on that (A, σ) is a twisted quadratic space over F with $\deg(A) = 2m$, $m \geq 1$. The main case of interest to us will be the case $m = 1$, though we will not assume this preferring to work out the general theory instead and specializing when we need to do so.

The center $Z(A, \sigma)$ of $C^+(A, \sigma)$ is an étale (=separable) quadratic F-algebra. If Z is a field, then $C^+(A, \sigma)$ is a central simple algebra of degree 2^{m-1} over Z; if $Z = F \times F$, then $C^+(A, \sigma)$ is a direct product of two copies of central simple F-algebras of degree 2^{m-1}. Moreover the center Z of $C^+(A, \sigma)$ is given by the following recipe (see [7, Theorem 8.10, page 94]).

Theorem 2.11.1. *Let (A, σ) be a twisted quadratic space over F. Let $C^+(A, \sigma)$ be the associated even Clifford algebra. Let $Z = Z(A, \sigma) \subset C^+(A, \sigma)$ be its center. If the characteristic of F is not two, then $Z = F[X]/(X^2 - \delta_\sigma)$ where $\delta_\sigma \in F^*$ is a representative of the discriminant of σ, $disc(\sigma) \in F^*/F^{*2}$.*

Corollary 2.11.2. *Let B/F be a quaternion algebra and σ be an orthogonal involution on B. Then the even Clifford algebra $C^+(B, \sigma)$ is commutative and we have*

$$C^+(B, \sigma) = Z = F[X]/(X^2 - \delta_\sigma),$$

where $\delta_\sigma = disc(\sigma) \mod F^{*2}$.

2.12. Similitudes and the group of similitudes. Let (A, σ) be a twisted quadratic space over F as before. We study several groups which arise in the present context.

A *similitude* of (A, σ) is an element $g \in A$ such that $\sigma(g)g \in F^*$. Then $\mu(g) = \sigma(g)g$ is called the multiplier of the similitude g of (A, σ). Similitudes of (A, σ) form a subgroup of A^* which we denote by $\mathrm{GO}(A, \sigma)$. We have a homomorphism $\mu : \mathrm{GO}(A, \sigma) \to F^*$ given by $g \mapsto \mu(g) = \sigma(g)g$. We define $\mathrm{PGO}(A, \sigma) = \mathrm{GO}(A, \sigma)/F^*$ and we have the exact sequence

$$1 \to F^* \to \mathrm{GO}(A, \sigma) \to \mathrm{PGO}(A, \sigma) \to 1.$$

Similitudes $g \in \mathrm{GO}(A, \sigma)$ with $\mu(g) = 1$ are called *isometries* and we have a subgroup $O(A, \sigma) = \ker(\mu) \subset \mathrm{GO}(A, \sigma)$ of isometries of (A, σ). We have an exact sequence of algebraic groups

$$1 \to O(A, \sigma) \to \mathrm{GO}(A, \sigma) \to \mathbb{G}_m \to 1.$$

2.13. Recurring Example. Let (B, σ) be a twisted quadratic space over F with B a quaternion division algebra (see 2.8). Let $\sigma = \mathrm{int}(u) \circ \gamma$ where $u \in B^*$ is a pure quaternion (so $\gamma(u) = -u$) and γ the canonical symplectic involution. Then $\mathrm{GO}(A, \sigma) = F(u)^* \cup F(u)^* v$ where v is an invertible quaternion which anti-commutes with u (i.e. $uv = -vu$).

2.14. Proper similitudes. Let $\deg(A) = n = 2m$. For every $g \in \mathrm{GO}(A,\sigma)$ we have $\mathrm{Nrd}_A(g) = \pm\mu(g)^m$, where $\mathrm{Nrd}(g)$ is the reduced norm of g. We say that g is a *proper similitude* of (A,σ) if $\mathrm{Nrd}_A(g) = \mu(g)^m$. The set of proper similitudes of (A,σ) is a subgroup of $\mathrm{GO}(A,\sigma)$ denoted by $\mathrm{GO}^+(A,\sigma)$. We let $\mathrm{PGO}^+(A,\sigma) = \mathrm{GO}^+(A,\sigma)/F^*$ and $O^+(A,\sigma) = \mathrm{GO}^+(A,\sigma) \cap O(A,\sigma)$ be the subgroup of proper isometries of (A,σ).

2.15. Recurring Example. Let (B,σ) be a twisted quadratic space, with B/F a quaternion division algebra (see 2.8, 2.13). Suppose that $\sigma = \mathrm{int}(u) \circ \gamma$, let $N_{F(u)/F} : F(u)^* \to F^*$ be the norm map. Then we have

$$\mathrm{GO}^+(B,\sigma) = F(u)^*,$$

and $O^+(B,\sigma) = O(B,\sigma) = \left\{z \in F(u) | N_{F(u)/F}(z) = 1\right\}$ if B is not split.

2.16. The Clifford Group. In the twisted quadratic case, there is a Special Clifford group but not the Clifford group and we recall this now.

Let (A,σ) be a twisted quadratic space over a field F. We have associated to (A,σ) a subgroup $\Gamma^+(A,\sigma) \subset C^+(A,\sigma)^*$ of the group of units of the even Clifford algebra associated to the pair (A,σ). If (A,σ) is split then $\Gamma^+(A,\sigma)$ can be identified with the special clifford group of [2].

We caution the reader that we use the notation $\Gamma^+(A,\sigma)$ instead of $\Gamma(A,\sigma)$ used in [7] because in the split case we get the special clifford group using the above construction (and not the Clifford group which we note, is denoted by $\Gamma(V,q)$, in [2] while the special Clifford group is denoted by $\Gamma^+(V,q)$). It seems to the author that it is better to follow established conventions of the theory in split case for psychological reasons.

We have an exact sequence of groups

$$1 \to F^* \to \Gamma^+(A,\sigma) \to O^+(A,\sigma) \to 1 \tag{2.16.1}$$

2.17. Recurring Example. Let (B,σ) be a twisted quadratic space, with B/F a quaternion division algebra (see 2.8, 2.13, 2.15), and suppose that $\sigma = \mathrm{int}(u) \circ \gamma$. Let $F(u)^1$ be the subgroup

$$F(u)^1 = \{z \in F(u) : z\gamma(z) = 1\} \tag{2.17.1}$$

Then we have and isomorphism of F-algebras

$$C^+(B,\sigma) = F(u),$$

and the group $O^+(B,\sigma)$ is given by

$$O^+(A,\sigma) = F(u)^1, \tag{2.17.2}$$

while the special Clifford group $\Gamma^+(B,\sigma)$ can be identified with

$$\Gamma^+(B,\sigma) = C^+(B,\sigma)^* = F(u)^*.$$

We have an exact sequence of groups

$$1 \to F^* \to \Gamma^+(B,\sigma) \to O^+(B,\sigma) \to 1. \tag{2.17.3}$$

3. The groups GSpin and Spin

3.1. The group of proper similitudes. From now on we will exclusively work with quaternion algebras over a field F. In other words A has $\deg(A) = 2$. Let (A, σ) be a twisted quadratic space over a field F with A a quaternion algebra. We will assume that F is not of characteristic two for simplicity. Then we have a group $\mathrm{GO}^+(A, \sigma)$. In the following subsections we will construct a group, which we will denote by $\mathrm{GSpin}(A, \sigma)$ which bears a relation to $\mathrm{GO}^+(A, \sigma)$ similar to the relation the usual Spin group bears to the special orthogonal group.

Let $\mathbb{G}_m/F$ be the multiplicative group over F. If K/F is a finite extension we will write $R_{K/F}\mathbb{G}_m$ for torus obtained by the restriction of scalars. Let $N_{K/F} : K \to F$ be the norm map. We have an induced map $N_{K/F} : R_{K/F}\mathbb{G}_m \to \mathbb{G}_m$ and let

$$\mathbb{G}^1_{mK/F} = \mathrm{Ker}(N_{K/F} : R_{K/F}\mathbb{G}_m \to \mathbb{G}_m) \tag{3.1.1}$$

be its kernel. This is a group scheme whose group of F-rational points,

$$\mathbb{G}^1_{mK/F}(F) = \left\{x \in K^* | N_{K/F}(x) = 1\right\},$$

is the subgroup of K^* consisting of norm one elements in K. Similarly define the group scheme

$$\mu^1_{K/F} = \mathrm{Ker}(N_{K/F} : R_{K/F}\mu_2 \to \mu_2). \tag{3.1.2}$$

Proposition 3.1.3. *Let (A, σ) be a twisted quadratic space over a field F and assume that A is a quaternion algebra. Let $K = C^+(A, \sigma)$. Then the group scheme of proper similitudes and the group scheme of proper isometries are given by*

$$\begin{aligned} \mathrm{GO}^+(A, \sigma) &= R_{K/F}\mathbb{G}_m. \\ \mathrm{O}^+(A, \sigma) &= \mathbb{G}^1_{mK/F} \end{aligned}$$

For a proof see [7, Example 12.2.5, page 164].

3.2. Spin groups in the split case. Let us recall a few standard facts from the theory of spin groups. Let us assume that (V, q) be a quadratic space over F with q an isotropic form and assume that $\dim(V) = 2$. In this case we have groups $SO(q) = SO(2) = \mathbb{G}_m$. The Clifford algebra construction yields a spin group as well. This situation is degenerate from the classical point of view (because $SO(2) = \mathbb{G}_m$). We have $\mathrm{Spin}(2) = \mathbb{G}_m$ and we also have an exact sequence of algebraic groups.

$$1 \to \mu_2 \to \mathrm{Spin}(2) \to SO(2) \to 1 \tag{3.2.1}$$

This is none other than the Kummer sequence:

$$1 \to \mu_2 \to \mathbb{G}_m \to \mathbb{G}_m \to 1. \tag{3.2.2}$$

We have in particular an exact sequence (a part of the Galois cohomology sequence for the Kummer sequence):

$$1 \to \mu(F) \to F^* \to F^* \to F^*/F^{*2}. \tag{3.2.3}$$

The connecting homomorphism $F^* \to F^*/F^{*2}$ is the Spinor norm homomorphism $SO(2)(F) \to F^*/F^{*2}$.

3.3. The group GSpin**.** We now want to describe a similar story for $\mathrm{GO}^+(B,\sigma)$ when B is a quaternion algebra over F. For notational simplicity, let $K = C^+(B,\sigma)$ be the Clifford algebra associated to the twisted quadratic space (B,σ). Then $\dim_F(K) = 2$. We have a canonical exact sequence of algebraic groups (obtained by restriction of scalars):

$$1 \to R_{K/F}\mu_2 \to R_{K/F}\mathbb{G}_m \to R_{K/F}\mathbb{G}_m \to 1. \tag{3.3.1}$$

Let (B,σ) be a twisted quadratic space with B a quaternion algebra. We define $\mathrm{GSpin}(B,\sigma)$ as follows

$$\mathrm{GSpin}(B,\sigma) = R_{K/F}\mathbb{G}_m. \tag{3.3.2}$$

And we define the spin group $\mathrm{Spin}(B,\sigma)$ by

$$\mathrm{Spin}(B,\sigma) = \mathbb{G}^1_{m\,K/F}. \tag{3.3.3}$$

Thus we have the commutative diagram:

$$\begin{array}{ccccccccc} 1 & \longrightarrow & R_{K/F}\mu_2 & \longrightarrow & R_{K/F}\mathbb{G}_m & \longrightarrow & R_{K/F}\mathbb{G}_m & \longrightarrow & 1 \\ & & \| & & \| & & \| & & \\ 1 & \longrightarrow & R_{K/F}\mu_2 & \longrightarrow & \mathrm{GSpin}(B,\sigma) & \longrightarrow & \mathrm{GO}^+(B,\sigma) & \longrightarrow & 1 \end{array} \tag{3.3.4}$$

And we have a commutative diagram of groups

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \mu^1_{2\,K/F} & \longrightarrow & \mathrm{Spin}(B,\sigma) & \longrightarrow & \mathrm{O}^+(B,\sigma) & \longrightarrow & 1 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 1 & \longrightarrow & R_{K/F}\mu_2 & \longrightarrow & \mathrm{GSpin}(B,\sigma) & \longrightarrow & \mathrm{GO}^+(B,\sigma) & \longrightarrow & 1 \end{array} \tag{3.3.5}$$

Thus we have proved that

Proposition 3.3.6. *Let F be a field and (B,σ) be a twisted quadratic space over F with B a quaternion algebra over F. Let $K = C^+(B,\sigma)$ be the (even) Clifford algebra of (B,σ). Then there is a canonical isogeny $\mathrm{GSpin}(B,\sigma) \to \mathrm{GO}^+(B,\sigma)$ with kernel $R_{K/F}\mu_2$. We have a commutative diagram of algebraic groups:*

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \mu^1_{2\,K/F} & \longrightarrow & \mathrm{Spin}(B,\sigma) & \longrightarrow & \mathrm{O}^+(B,\sigma) & \longrightarrow & 1 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 1 & \longrightarrow & R_{K/F}\mu_2 & \longrightarrow & \mathrm{GSpin}(B,\sigma) & \longrightarrow & \mathrm{GO}^+(B,\sigma) & \longrightarrow & 1 \end{array} \tag{3.3.7}$$

4. Spin structures on an elliptic curve

4.1. Elliptic curves of spinorial type. Let k be a field and let $\bar{k}$ be its algebraic closure. Let E/k be an elliptic curve. We will write $\mathrm{End(E)} = \mathrm{Hom_k(E,E)}$ for the $\mathbb{Q}$-algebra endomorphisms of E defined over k. We will say that E is of *spinorial type* if the $\mathbb{Q}$-algebra $\mathrm{End_k(E)}$ admits a non-trivial involution of the first kind.

Proposition 4.1.1. *Let E/k be an elliptic curve over a field k. Consider the following assertions:*

(1) *E is of spinorial type.*
(2) $\mathrm{End_k(E)} = \mathrm{End_{\bar{k}}(E)}$ *is a quaternion algebra.*
(3) *E is supersingular.*
(4) *The characteristic of k is $p > 0$.*

Then we have (1) $\Leftrightarrow$ (2) $\Rightarrow$ (3) $\Rightarrow$ (4).

Proof. Clearly the assertions (2) $\Rightarrow$ (3) $\Rightarrow$ (4) are well-known. So we need to prove the equivalence (1) $\Leftrightarrow$ (2).

Let $B = \mathrm{End_k(E)}$. We prove (1) $\Rightarrow$ (2). By the classification of the endomorphism algebras of E there are three possibilities: B is either (a) the field of rational numbers (b) an imaginary quadratic field or (c) a quaternion algebra. If $B = \mathbb{Q}$, then B does not admit any non-trivial involutions. Similarly if B is an imaginary quadratic field then B does not admit any non-trivial involutions of the first kind (*i.e.*, involutions trivial on its center). Hence B cannot be the field of rational numbers or an imaginary quadratic field. So the hypothesis (1) implies that B is a quaternion algebra.

Now to prove (2) $\Rightarrow$ (1) we use [7, Corollary 2.8 (page 18) and Proposition 2.21 (page 26)] which says that any quaternion algebra $B/\mathbb{Q}$ admits non-trivial involutions of the first kind. So E is of spinorial type. This completes the proof. □

4.2. Elliptic curves of spinorial type over finite fields. From now on we will study elliptic curves of spinorial type over a finite field $\mathbb{F}_q$ with $q = p^n$ elements. Before proceeding further we recall the classification up to isogeny of elliptic curves over a finite field $\mathbb{F}_q$ (see [6] or [12, Theorem 4.1]).

Theorem 4.2.1. *Let $\mathbb{F}_q$ be a field with $q = p^a$ elements. The set of isogeny classes of elliptic curves over $\mathbb{F}_q$ are in bijection with a certain set of integers, denoted I_q, contained in the interval $[-2\sqrt{q}, 2\sqrt{q}]$. An integer $\beta \in [-2\sqrt{q}, 2\sqrt{q}]$ is in I_q if and only if:*

(1) $(\beta, p) = 1$*; or*
(2) $p|\beta$ *and we are in any of the following subcases:*
  (a) *a is even and $\beta = \pm 2\sqrt{q}$;*
  (b) *a is even and $p \not\equiv 1 \mod 3$ and $\beta = \pm\sqrt{q}$;*
  (c) *a is odd and $p = 2, 3$ and $\beta = \pm p^{\frac{a+1}{2}}$;*
  (d) *a is odd and $\beta = 0$;*
  (e) *a is even and $p \not\equiv 1 \mod 4$ and $\beta = 0$.*

In case (1) *the associated isogeny class consists of ordinary elliptic curves. Otherwise the associated isogeny class consists of supersingular elliptic curves. In all cases, except in the case* 2(*a*)*, the endomorphism algebra* $\mathrm{End_{\mathbb{F}_q}(E)}$ *of any elliptic curve E in the isogeny class associated to β is an imaginary quadratic field. If we are in the exceptional case* 2(*a*) *then the endomorphism algebra is the unique quaternion algebra over $\mathbb{Q}$ which is ramified at p and ∞.*

Proposition 4.2.2. *Let $E/\mathbb{F}_q$ be a supersingular elliptic curve. Then $E \times_{\mathbb{F}_q} \mathbb{F}_{q^2}$ is of spinorial type.*

Proof. If E is a supersingular elliptic curve defined over $\mathbb{F}_q$ then $E' = E \times_{\mathbb{F}_q} \mathbb{F}_{q^2}$ is a supersingular elliptic curve over $\mathbb{F}_{q^2}$ with all its endomorphisms defined over $\mathbb{F}_{q^2}$. Hence E' is of spinorial type by the previous proposition. □

We end the subsection with the following consequence of Proposition 4.2.1 and Proposition 4.1.1.

Proposition 4.2.3. *Let $E/\mathbb{F}_q$ be an elliptic curve of spinorial type. Then*

(1) *E is supersingular,*
(2) *The two eigenvalues of the Frobenius endomorphism of E are equal;*
(3) *Frobenius endomorphism $\tau_E : E \to E$ is in the center of $B = \mathrm{End}_{\mathbb{F}_q}(\mathrm{E})$.*

Proof. This is immediate from Deuring's classification of supersingular elliptic curves (see Theorem 4.2.1). □

4.3. Spin structures on an elliptic curve. Let $E/\mathbb{F}_q$ be an elliptic curve over a finite field $\mathbb{F}_q$. Assume that E is an elliptic curve of spinorial type. Let $B = \mathrm{End(E)}$ be the endomorphism algebra of E. A *spin structure* on E is a choice of an involution $\sigma : B \to B$ of first kind and orthogonal type. Equivalently, a spin structure on an elliptic curve is a choice of twisted quadratic space structure (B, σ) on B where $B = \mathrm{End(E)}$ and $\sigma : B \to B$ is an involution of the first kind and orthogonal type.

Proposition 4.3.1. *Let $E/\mathbb{F}_q$ be an elliptic curve and suppose E is an elliptic curve with a spin structure (B, σ). Then the Frobenius endomorphism $\tau_E : E \to E$ induces a similitude of (B, σ).*

Proof. Let E be an elliptic curve with a spin structure (B, σ). Then the Frobenius endomorphism $\tau_E : E \to E$ is in the center of B. The center of B is $\mathbb{Q}$. We have to prove that $\sigma(\tau)\tau \in \mathbb{Q}$. But τ is in the center of B, so $\sigma(\tau) = \tau$ and so $\sigma(\tau)\tau = \tau^2 \in \mathbb{Q}$ as $\tau \in \mathbb{Q}$. So τ is a similitude of (B, σ). To prove that τ is a proper similitude we have to prove that the multiplier $\mu(\tau) = \sigma(\tau)\tau$ of the similitude τ satisfies,

$$\mu(\tau) = \sigma(\tau)\tau = \mathrm{Nrd}(\tau) = q.$$

The last equality follows from the fact that τ operates by $\pm\sqrt{q}$ (or by the following proposition, see [10, Page 82]). This proves the assertion. □

Proposition 4.3.2. *Let $E/\mathbb{F}_q$ be an elliptic curve of spinorial type. Let $\tau \in \mathrm{End(E)}$ be the Frobenius endomorphism of E. Then we have*

(1) *The reduced trace of τ is $\pm 2\sqrt{q}$,*
(2) *the reduced norm of τ is q.*

In particular, the reduced norm is a square.

Proposition 4.3.3. *Let $(B, \sigma)/\mathbb{Q}$ be a twisted quadratic space with B a quaternion algebra over $\mathbb{Q}$ which is ramified at ∞. Let $K = C^+(B, \sigma)$ be the associated even Clifford algebra. Then $K/\mathbb{Q}$ is an imaginary quadratic extension of $\mathbb{Q}$.*

Proof. The algebra B is given by its symbol $B = \left(\frac{a,b}{\mathbb{Q}}\right)$. Since B is ramified at ∞, we see that the Hilbert symbol $(a, b)_\infty = -1$ and this means that $a < 0$ and $b < 0$. Now let σ be an orthogonal involution on B and let γ be the canonical symplectic involution of B. Then σ is of the form $\sigma = \mathrm{int}(u) \circ \gamma$ for some $u \in B$ with $\gamma(u) = -u$. Thus u is a pure quaternion and $\mathrm{disc}(\sigma) = -\mathrm{Nrd}(u)$. But a simple calculation shows that

$$\mathrm{Nrd}(u) = -au_1^2 - bu_2^2 + abu_3^2,$$

where $u = iu_1 + ju_2 + ku_3$ and $i^2 = a, j^2 = b, ij = -ji = k$. Since $a < 0$ and $b < 0$, we see that the quadratic form $(-a, -b, ab)$ is positive definite. Hence $\mathrm{Nrd}(u) > 0$ and in particular $\mathrm{disc}(\sigma) = -\mathrm{Nrd}(u) < 0$. By Theorem 2.11.2 we know that in this case $K = C^+(B, \sigma) = \mathbb{Q}[x]/(x^2 - \mathrm{disc}(\sigma))$ and as $\mathrm{disc}(\sigma) < 0$, K is an imaginary quadratic extension of $\mathbb{Q}$. This completes the proof. □

5. Spinorial representation of the Weil group

5.1. Weil groups. Let $E/\mathbb{F}_q$ be an elliptic curve. Let $W(\bar{\mathbb{F}}_q/\mathbb{F}_q) \subset \mathrm{Gal}(\bar{\mathbb{F}}_q/\mathbb{F}_q)$ be the Weil group of $\mathbb{F}_q$. It is standard that $\mathbb{Z} \simeq W(\bar{\mathbb{F}}_q/\mathbb{F}_q)$ and we choose the isomorphism given by $1 \mapsto \mathrm{Frob}_{geom}$, where $\mathrm{Frob}_{geom} \in \mathrm{Gal}(\bar{\mathbb{F}}_q/\mathbb{F}_q)$ is the geometric Frobenius of $\mathbb{F}_q$. Proposition 4.3.1 provides a canonical representation of the Weil group arising from $(E, (B, \sigma))$:

Proposition 5.1.1. *Let E be an elliptic curve with a spin structure (B, σ). Then there is a canonical similitude representation*

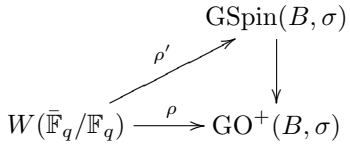
$$\rho_{E,\sigma} : W(\bar{\mathbb{F}}_q/\mathbb{F}_q) \to \mathrm{GO}^+(B, \sigma), \tag{5.1.2}$$

which is given by

$$\rho_{E,\sigma}(\mathrm{Frob}_{geom}) = (\tau, \tau) \in \mathrm{GO}^+(B, \sigma)(K) = R_{K/\mathbb{Q}}\mathbb{G}_m(K) = K^* \times K^*.$$

5.2. Spinorial liftings. Let $\rho : W(\bar{\mathbb{F}}_q/\mathbb{F}_q) \to \mathrm{GO}^+(B, \sigma)$ be a homomorphism of groups. We say that ρ admits a spinorial lifting if there exists a representation $\rho' : W(\bar{\mathbb{F}}_q/\mathbb{F}_q) \to \mathrm{GSpin}(B, \sigma)$ which makes the following diagram commutative:

(5.2.1)



5.3. A criterion for existence of Spinorial liftings.

Theorem 5.3.1. *Let $E/\mathbb{F}_q$ be an elliptic curve with a spin structure (B, σ). Let $K = C^+(B, \sigma)$ be the associated even Clifford algebra. Let $\tau_E = \tau \in \mathrm{End(E)}$ be the Frobenius endomorphism of E. Then a lift $\rho_E^{spin} : W(\bar{\mathbb{F}}_q/\mathbb{F}_q) \to \mathrm{GSpin}(B, \sigma)$ exists if and only if the Clifford algebra $K = K(B, \sigma)$ satisfies $K = F(\sqrt{\tau})$.*

Proof. The endomorphism $\tau \in \mathrm{End(E)} = \mathrm{B}$ is a central element in B with reduced norm $\mathrm{Nrd}(\tau) = q$. So by Theorem 4.2.1 $\tau = \pm\sqrt{q}$. We have an exact sequence of groups obtained by taking Galois cohomology of (3.3.1) with $G_{\mathbb{Q}} = \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$, we get (for the Galois cohomology computations, which are easy, the unfamiliar reader may use [7, Lemma 29.6, page 394]):

$$1 \to \mu_2(K) \to K^* \to K^* \to K^*/K^{*2} = H^1(G_{\mathbb{Q}}, R_{K/\mathbb{Q}}(\mu_2)). \tag{5.3.2}$$

Then $\tau \in \mathrm{GO}^+(B, \sigma)$ lifts to $\mathrm{GSpin}(B, \sigma)$ if and only if its image in K^*/K^{*2} is 1. Equivalently a lifting exists if and only if $\sqrt{\tau} \in K$. When this happens, we have a lift

$$\rho^{spin} : W(\bar{\mathbb{F}}_q/\bar{\mathbb{F}}_q) \to \mathrm{GSpin}(B, \sigma),$$

given by

$$\rho^{spin}(\mathrm{Frob}_{geom}) = (\sqrt{\tau}, -\sqrt{\tau}) \in \mathrm{GSpin}(B, \sigma)(K) = K^* \times K^*.$$

This prove the proposition. □

6. Arithmetic spin structures

6.1. Definition of Arithmetic spin structures. Let $E/\mathbb{F}_q$ be an elliptic curve with a spin structure (B,σ). We say that the spin structure (B,σ) is an *arithmetic spin structure* if the canonical similitude representation $\rho_{E,\sigma} : W(\bar{\mathbb{F}}_q/\mathbb{F}_q) \to \mathrm{GO}^+(B,\sigma)$ admits a spinorial lifting.

6.2. Existence of an arithmetic spin structure. We now show that arithmetic spin structures exists on an elliptic curve under suitable circumstances.

Theorem 6.2.1. *Let $E/\mathbb{F}_q$ be an elliptic curve of spinorial type with $q = p^{2n}$. Let $B = \mathrm{End(E)}$ and let $\tau \in B$ be the Frobenius endomorphism of E. Then we have the following:*

1. *if n is odd then there exists a unique arithmetic spin structure of discriminant $-p^n$ on $E/\mathbb{F}_q$ if and only if $\tau \in \mathrm{End(E)}$ is given by multiplication by $-p^n$.*
2. *if n is even, then there exists an arithmetic spin structure of E if and only if B contains a pure quaternion with reduced norm 1.*

Proof. We prove (1). If E carries an arithmetic spin structure σ of discriminant $-p^n$, then by Theorem 5.3.1 we see that $\tau^2 \in C^+(B,\sigma)$ and $\mathbb{Q}(\sqrt{\tau}) = C^+(B,\sigma) = \mathbb{Q}[x]/(x^2+p^n)$ thus $\tau = -p^n$. So we have to prove the converse.

To produce an arithmetic spin structure we have to prove the existence of a spin structure (B,σ) on $E/\mathbb{F}_q$ such that the canonical similitude representation

$$\rho_{E,\sigma} : W(\bar{\mathbb{F}}_q/\mathbb{F}_q) \to \mathrm{GO}^+(B,\sigma)$$

lifts to a spin representation. By Theorem 5.3.1, this happens if and only if $\tau = \pm p^n \in K^{*2}$. By Proposition 4.3.3 we know that the discriminants of involutions which can occur as spin structures are all negative. So we see that there is no orthogonal involution on B whose discriminant can be $+p^n$. So it remains to show that there is an involution σ whose discriminant is $-p^n$. To construct an involution of the first kind and of orthogonal type on B with discriminant $-p^n$ it suffices to construct a pure quaternion $u \in B$ (i.e. a quaternion with reduced trace zero) with reduced norm $\mathrm{Nrd}(u) = p^n$. Indeed given such a u, the discriminant of the involution $\sigma = \mathrm{int}(u) \circ \gamma$ is given by (see 2.9)

$$\mathrm{disc}(\sigma) = -\mathrm{Nrd}(u) = -p^n.$$

Thus we see that the even Clifford algebra $C^+(B,\sigma)$ is $C^+(B,\sigma) = K = \mathbb{Q}[x]/(x^2+p^n)$. Further orthogonal involutions on B are classified, up to isomorphism, by their discriminants (by [7, 7.4, Page 82] any two orthogonal involutions differ by an inner conjugation by a non-zero quaternion). So the spin structure (B,σ) is unique up to isomorphism and is arithmetic.

So let us construct the required u. We claim now that there exists a quaternion $u \in B$ of trace zero, with reduced norm p^n, for any odd value of n. Indeed it is easy to see that B can be given by symbols $\left(\frac{-a,-p}{\mathbb{Q}}\right)$ for a suitable choice of a and so B contains a trace zero quaternion v such that $v^2 = -p$. The reduced norm of v is

$\mathrm{Nrd}(v) = p$ and hence the quaternion $u = p^{(n-1)/2}v$ has reduced norm p^n. Thus the involution $\sigma = \mathrm{int}(u) \circ \gamma$ has discriminant

$$\mathrm{disc}(\sigma) = -\mathrm{Nrd}(u) = -p^n$$

as claimed. Thus the Clifford algebra $K = \mathbb{Q}[x]/(x^2 + p^n)$, and so $\sqrt{-p^n} \in K$ and so we see that if E is such that $\tau = -p^n$, then τ has a square root in K and so we have a lifting

$$\rho^{spin}_{E,\sigma} : W(\bar{\mathbb{F}}_q/\mathbb{F}_q) \to \mathrm{GSpin}(B, \sigma) \tag{6.2.2}$$

given by

$$\rho^{spin}_{E,\sigma}(\mathrm{Frob}) = (\sqrt{\tau}, -\sqrt{\tau}) \in \mathrm{GO}^+(B, \sigma)(K) = K^* \times K^*.$$

Now we prove (2). If n is even, then $\tau = -p^n$ has a square root in K if and only if $\sqrt{-1} \in K$. So the existence of an involution with this property is tantamount to finding a pure quaternion v whose reduced norm is 1. If we can find such a v, then we can take $u = p^{n/2}v$ and observe that u has reduced norm $\mathrm{Nrd}(u) = p^n$. Hence $\sigma = \mathrm{int}(u) \circ \gamma$ is an orthogonal involution of the first kind with discriminant $\mathrm{disc}(\sigma) = -p^n$ and $\tau = -p^n$ has a square root in $K = \mathbb{Q}[x]/(x^2 + p^n) = \mathbb{Q}(i)$. □

Corollary 6.2.3. *Let $E/\mathbb{F}_{p^2}$ of spinorial type. Then E carries an arithmetic spin structure if and only if the Frobenius endomorphism of E operates by multiplication by $-p$. If E has an arithmetic spin structure, then it is unique up to isomorphism.*

7. A candidate for $\mathbb{Q}(1/4)$

7.1. Definition of $\mathbb{Q}(1/4)$. Let $E/\mathbb{F}_{p^2}$ be an elliptic curve with an arithmetic spin structure. We will define $\mathbb{Q}(1/4)$ to be the triple $(E, (B, \sigma))$ where E is our elliptic curve and $B = \mathrm{End(E)}$ and (B, σ) is the arithmetic spin structure on E. We show now that $\mathbb{Q}(1/4)$ is equipped with an ℓ-adic (for $\ell \neq p$) and a crystalline realization at p.

7.2. The ℓ-adic realization of $\mathbb{Q}(1/4)$. The object $\mathbb{Q}(1/4)$ comes equipped with an ℓ-adic realization, denoted $\mathbb{Q}(1/4)_\ell$. We define the ℓ-adic realization $\mathbb{Q}(1/4)_\ell$ of $\mathbb{Q}(1/4)$ to be the representation obtained by extension of scalars of the canonical spin representation $\rho^{spin}_{E,\sigma} \to \mathrm{GSpin}(B, \sigma)$. This gives us a Weil sheaf (by [4] such a sheaf is specified by specifying a representation of the Weil group) on the point $\mathrm{Spec}(\mathbb{F}_{p^2})$:

$$\rho^{spin}_{E,\sigma,\ell} : W(\bar{\mathbb{F}}_{p^2}/\mathbb{F}_{p^2}) \to R_{K/\mathbb{Q}}\mathbb{G}_m(\mathbb{Q}_\ell) = \mathrm{GSpin}(B, \sigma)(\mathbb{Q}_\ell). \tag{7.2.1}$$

7.3. The crystalline realization of $\mathbb{Q}(1/4)$. Let $(E, (B, \sigma))$ be an elliptic curve over $\mathbb{F}_{p^{2n}}$ with an arithmetic spin structure (B, σ). Let $W = W(\mathbb{F}_{p^{2n}})$ be the ring of Witt vectors of $\mathbb{F}_{p^{2n}}$. Let $F : W \to W$ be the Frobenius morphism of W. Let $K_0 = W \otimes \mathbb{Q}_p$ be the quotient field of W and let $F : K_0 \to K_0$ be the extension of F to K_0. Let $H^1_{cris}(E/W)$ be the crystalline cohomology of E; we have an F-linear map $\phi : H^1_{cris}(E/W) \to H^1_{cris}(E/W)$. The data $(H^1_{cris}(E/W), \phi)$ is the data of an F-crystal associated to $E/\mathbb{F}_{p^{2n}}$. Let (M, ϕ) denote the extension of the F-crystal $(H^1_{cris}(E/W), \phi)$ to an F-isocrystal over K_0; since E has an arithmetic spin structure, the F-linear map $\phi : M \to M$ is simply the map $\phi = -p^n F$. We want to construct a crystal (M^{spin}, ϕ^{spin}) which we would like to call the crystalline realization of $\mathbb{Q}(1/4)$. The endomorphism algebra of (M, ϕ) is the unique quaternion algebra $B \otimes \mathbb{Q}_p$ over

$\mathbb{Q}_p$. The orthogonal involution $\sigma : B \to B$ extends to an orthogonal involution $\sigma_p : B \otimes \mathbb{Q}_p \to B \otimes \mathbb{Q}_p$. The data (M, ϕ, σ_p) is an F-isocrystal equipped with a spin structure (in the obvious sense). The Clifford algebra $C^+(M, \phi, \sigma_p)$ is a $\mathbb{Q}_p$ vector space isomorphic to $\mathbb{Q}_p[x]/(x^2 + p^n)$. Define $M^{spin} = C^+(M, \phi, \sigma_p)$, and define ϕ^{spin} to be multiplication by $x \in \mathbb{Q}_p[x]/(x^2 + p^n)$ thought of as an F-linear endomorphism of M^{spin}. This gives us a Dieudonne isocrystal (M^{spin}, ϕ^{spin}) over $\mathbb{Q}_p$ which we call the crystalline realization of $\mathbb{Q}(1/4)$ and denote it by $\mathbb{Q}(1/4)_p$.

7.4. The L-function of $\rho^{spin}_{E,\sigma}$. Let $E/\mathbb{F}_q$ be an elliptic curve with an arithmetic spin structure (B, σ). Then $q = p^{2n}$ and the Frobenius endomorphism of E operates by $-p^n = -\sqrt{q}$; the eigenvalues of Frobenius under the spin representation $\rho^{spin}_{E,\sigma}$ are $\pm\sqrt{-p^n} = \pm\sqrt{-\sqrt{q}}$. Thus the Hasse-Weil zeta function of $\rho^{spin}_{E,\sigma}$ is given by

$$Z(\rho^{spin}_{E,\sigma}, T) = \frac{1}{(1 - \sqrt{-p^n}T)\,(1 + \sqrt{-p^n}T)}. \tag{7.4.1}$$

We will write

$$L(\rho^{spin}_{E,\sigma}, s) = Z(\rho^{spin}_{E,\sigma}, q^{-s}). \tag{7.4.2}$$

And this is

$$L(\rho^{spin}_{E,\sigma}, s) = \frac{1}{\left(1 + q^{\frac{1}{2}-2s}\right)}. \tag{7.4.3}$$

We note that (7.4.3) can also be written more suggestively as

$$L(\rho^{spin}_{E,\sigma}, s) = \frac{1}{\left(1 + q^{\frac{1}{2}-2s}\right)} \tag{7.4.4}$$

$$= \frac{1}{\left(1 + q^{2\left(\frac{1}{4}-s\right)}\right)} \tag{7.4.5}$$

$$= \frac{1}{\left(1 + \sqrt{-1}q^{\frac{1}{4}-s}\right)\left(1 - \sqrt{-1}q^{\frac{1}{4}-s}\right)}, \tag{7.4.6}$$

especially the last equality which makes the 1/4-twisting more transparent. Note that the presence of the two factors in the last equality should be seen as a manifestation of the fact that the Clifford algebra $C^+(B, \sigma)$ is a quadratic extension of $\mathbb{Q}$.

7.5. The L-function of $H^1(E)$. Since the Frobenius endomorphism of E operates by $-\sqrt{q}$, we can also calculate the L-function E, that is the reciprocal of the characteristic polynomial of Frobenius on $H^1(E, \mathbb{Q}_\ell)$. The characteristic polynomial is given by

$$Z(H^1(E), T) = (1 + \sqrt{q}T)^2. \tag{7.5.1}$$

The L-function of E is defined as

$$L(E, s) = Z(H^1(E), q^{-s})^{-1} = \frac{1}{\left(1 + q^{\frac{1}{2}-s}\right)^2} \tag{7.5.2}$$

7.6. A relation between $L(\rho^{spin}_{E,\sigma}, s)$ and $L(H^1(E), s)$. From (7.4.3) and (7.5.1) we have the relation:

Theorem 7.6.1. *For an elliptic curve $E/\mathbb{F}_q$ with an arithmetic spin structure (B, σ) and spinorial representation $\rho^{spin}_{E,\sigma} : W(\bar{\mathbb{F}}_q/\mathbb{F}_q) \to \mathrm{GSpin}(B, \sigma)$, we have*

$$L(E, s) = L\left(\rho^{spin}_{E,\sigma}, \frac{s}{2}\right)^2.$$

In particular we have

$$L(E, 1) = L\left(\rho^{spin}_{E,\sigma}, \frac{1}{2}\right)^2.$$

References

[1] G. W. Anderson, *Cyclotomy and an extension of the Taniyama group*, Compositio Math. **57** (1986), no. 2, 153–217.

[2] C. C. Chevalley, The algebraic theory of spinors, Columbia University Press, New York (1954).

[3] P. Deligne, *La conjecture de Weil pour les surfaces $K3$*, Invent. Math. **15** (1972) 206–226.

[4] ———, *La conjecture de Weil. II*, Inst. Hautes Études Sci. Publ. Math. (1980), no. 52, 137–252.

[5] C. Deninger, *Motivic L-functions and regularized determinants. II*, in Arithmetic geometry (Cortona, 1994), Sympos. Math., XXXVII, 138–156, Cambridge Univ. Press, Cambridge (1997).

[6] M. Deuring, *Die Typen der Multiplikatorenringe elliptischer Funktionenkörper*, Abh. Math. Sem. Hansischen Univ. **14** (1941) 197–272.

[7] M.-A. Knus, A. Merkurjev, M. Rost, and J.-P. Tignol, The book of involutions, Vol. 44 of *American Mathematical Society Colloquium Publications*, American Mathematical Society, Providence, RI (1998). With a preface in French by J. Tits.

[8] M. Kuga and I. Satake, *Abelian varieties attached to polarized K_3-surfaces*, Math. Ann. **169** (1967) 239–242.

[9] Y. Manin, *Lectures on zeta functions and motives (according to Deninger and Kurokawa)*, Astérisque (1995), no. 228, 4, 121–163. Columbia University Number Theory Seminar (New York, 1992).

[10] D. Mumford, Abelian varieties, Tata Institute of Fundamental Research Studies in Mathematics, No. 5, Published for the Tata Institute of Fundamental Research, Bombay (1970).

[11] N. Ramachandran, *Values of zeta functions at $s = 1/2$*, Int. Math. Res. Not. (2005), no. 25, 1519–1541.

[12] W. C. Waterhouse, *Abelian varieties over finite fields*, Ann. Sci. École Norm. Sup. (4) **2** (1969) 521–560.

Math. department, University of Arizona, 617 N Santa Rita, Tucson 85721-0089, USA.
E-mail address: kirti@math.arizona.edu