Space-Time Codes and Non-Associative Division Algebras Arising from Elliptic Curves

Abdulaziz Deajim and David Grant

Abstract. Space-time codes are sets of complex $M \times T$ matrices used to describe the amplitude-phase modulation of a radio signal transmitted over T time slots from each of M transmit antennas. Under certain assumptions on the transmission channel, useful examples when $M = T$ have been built by taking as codes M-dimensional vector spaces V of $M \times M$ matrices over number fields with every non-zero element of V nonsingular. All such spaces arise as representations of M-dimensional non-associative division algebras over number fields. We introduce new 3-dimensional non-associative division algebras over any perfect field k associated to elliptic curves E over k, which allows us to classify all such algebras over k. We give a finer classification over number fields in terms of the Tate-Shafarevich group of E.

Introduction

In this paper we introduce a new family of 3-dimensional non-associative division algebras over a perfect field k, arising from the arithmetic of elliptic curves over k. This allows us to completely classify 3-dimensional non-associative division algebras over k. We also give a finer classification over number fields in terms of the Tate-Shafarevich group of elliptic curves.

Non-associative division algebras have quite a pedigree, and those of dimension 3 have long been of interest. However, our motivation for studying such algebras comes from a recent development in communications theory: the advent of space-time codes, which are sets of complex matrices used to describe the amplitude-phase modulation of radio signals transmitted over multiple antennas.

In section 1 we recall (and give references for) what we need of the theory of space-time codes, and describe how the search for desirable codes leads to the study of non-associative division algebras over number fields. We recount what we need of the history and theory of non-associative division algebras in section 2. In section 3, we describe our new family of 3-dimensional non-associative division algebras over a perfect field k: each such algebra A is associated via its representations to a homogeneous space C of an elliptic curve over k, where C has index 3 as a

2000 *Mathematics Subject Classification.* Primary 17A35, 94B27; Secondary 11G05.

The second author was partially supported by NSF grant CCF 0434410 and was enjoying the hospitality of the Mathematical Sciences Research Institute as this work was being completed.

homogeneous space over k, and where C has a k-rational divisor D of degree 0 which is not linearly equivalent to 0. We also describe how this classifies all such algebras. We give in section 4 a constructive procedure for reproducing A in terms of the associated C and D.

In section 5 we present a finer classification of the new 3-dimensional non-associative division algebras over number fields K: we relate such algebras A which are not division algebras over any localization of K to elements of order 3 in the Tate-Shafarevich group of elliptic curves E over K with non-trivial Mordell-Weil group over K. In the final section 6 we compute an example of such an A from a specific E over $\mathbb{Q}$.

The results in this paper were obtained by the first author in his Ph. D. thesis [**17**] written under the direction of the second author.

We thank Mahesh Varanasi for introducing us to space-time codes and for helpful comments on this paper. Also, after we gave the talk at the AMS meeting in San Francisco that grew into this paper, several conference participants told us that Catherine O'Neil and Manjul Bhargava had independently proved Proposition 4 and Theorems 1 and 2. Interestingly, they were led to these results from considerations having nothing to do with codes or algebras. We thank them for describing their unpublished results to us so appropriate attribution could be made.

1. Space-Time codes

Before embarking on a discussion of space-time codes, perhaps it makes sense first to recall aspects of the theory of classical codes for single transmit antennas systems. "Classical codes" is a retronym for what were just called "codes" before the introduction of space-time codes.

Classical codes are designed to allow for more reliable transmission of information over a noisy channel. Given a finite alphabet $\mathcal{A}$ of symbols, a code is a subset $\mathcal{C}$ of $\mathcal{A}^n$ whose elements are called codewords, the entries of which are transmitted over the channel during n time slots. Because of noise in the channel, if $x \in \mathcal{C}$ is transmitted, some potentially different vector $y \in \mathcal{A}^n$ is received. If the channel is discrete, symmetric, and memoryless, the maximum likely estimate for x given y is the codeword c of minimal Hamming distance to y. The Hamming distance $d_H(y, c)$, which is the number of coordinates in which y and c differ, is a metric. Hence to maximize the error-correcting capabilities of the code we want its minimal distance $d_{\mathcal{C}} = \min_{c,c' \in \mathcal{C}, c \neq c'} d_H(c, c')$ to be as large as possible. For more on the theory of classical codes, see e.g., [**39**].

Space-time codes are designed for reliable transmission over a noisy channel for radio frequency carrier signals from $M > 1$ antennas (like cell towers) over T time slots. A complex number is used to describe the amplitude and phase of such a signal, so codewords in a space-time code are $M \times T$ complex matrices (one row of length T per transmit antenna). Specifically, let $\mathcal{A}$ be a finite subset of $\mathbb{C}$. A *space-time code* is a subset $\mathcal{C}$ of $\mathrm{Mat}_{M \times T}(\mathcal{A})$, the set of $M \times T$ matrices with entries in $\mathcal{A}$. The elements of $\mathcal{C}$ are the *codewords* of the code and $\mathcal{A}$ is its *alphabet*. We assume our system also has $U \geq 1$ receive antennas. If one transmits $x \in \mathcal{C}$ over a noisy channel, a $U \times T$ matrix y is received (one row from every receive antenna).

We make a technical assumption, as explained in [**38**], that the channel has a $U \times M$ matrix of "fading coefficients" H, whose entries are independent and identically distributed complex normal random variables, and has additive white

Gaussian noise. Then in [**38**] it is shown that the maximum likely estimate for x given y is the $c \in \mathcal{C}$ such that the euclidean distance between y and Hc is minimal. Further, in [**38**] it is shown that the probability of error (averaged over H) that a transmitted codeword x is mistaken for another codeword c is proportional to the d^{th}-power of the reciprocal of the signal-to-noise ratio, where $d = \text{rk}(y-c)$, the rank of $y-c$. So the larger the $\text{rk}(y-c)$, the smaller the probability of this error. The rank distance $d_{\text{rk}}(y,c) = \text{rk}(y-c)$ is a metric. Hence to maximize the error-correcting capabilities of the code, we want its minimal distance $d_{\mathcal{C}} = \min_{c,c' \in \mathcal{C}, c \neq c'} d_{\text{rk}}(c,c')$ to be as large as possible.

There are a variety of other engineering constraints that affect the design of space-time codes: we mention them briefly to motivate our choice of investigation. In [**22**] it is shown that $\mathcal{A}$ can be perturbed by an arbitrarily small amount so that it lies in the algebraic closure $\bar{\mathbb{Q}}$ of $\mathbb{Q}$ without changing the ranks of differences of any codewords. So there is no loss in generality in assuming that $\mathcal{A}$ lies in a number field K. Also, the better the channel, the more codewords one can use and still transmit reliably. Since the quality of a channel is not known ahead of time, it is advantageous to have an infinite nested sequence of codes

$$\mathcal{C}_1 \subset \cdots \subset \mathcal{C}_n \subset \cdots,$$

where a code in the sequence with more codewords is employed when the channel improves. Taking the union $\mathcal{C} = \cup_n \mathcal{C}_n$, one gets an infinite space-time code $\mathcal{C}$ on an infinite alphabet $\mathcal{A}$ in K. To make decoding tractable, one wants $\mathcal{C}$ to be a lattice in $\text{Mat}_{M\times T}(K)$ (see [**23**] for details). Hence $\mathcal{C} \otimes \mathbb{Q}$ is a vector space over $\mathbb{Q}$. For simplicity, we will only consider the case that $T = M$. Then the codes with the best error correcting capability will have minimal distance $d_{\mathcal{C}} = M$. Also in this case, if we have a system with only one receiving antenna, so $U = 1$ (a so-called MISO channel: multiple input with single output) then, as explained in [**23**], it is a reasonable simplifying assumption to restrict to the case that $\mathcal{C} \otimes \mathbb{Q}$ is a vector space over K.

With all these assumptions, what we seek are K-subspaces $V \subset \text{Mat}_{M\times M}(K)$, such that every non-zero $v \in V$ is nonsingular. Since, say, the top row of a non-zero matrix in such a space cannot vanish, the maximal dimension of such a V is M.

DEFINITION 1. Let k be a field. An M-dimensional k-vector space $V \subset \text{Mat}_{M\times M}(k)$ is called a maximal nonsingular space if every non-zero $v \in V$ is nonsingular.

Examples of maximal nonsingular spaces over k have been built by representing division algebras over k. The first well-known space-time code was the Alamouti Code [**1**] which is a 2-dimensional complex representation of the quaternions over $\mathbb{R}$. This idea was generalized in [**34**], where codes were built by representing the octonians over $\mathbb{R}$. The most far-reaching ideas in [**34**] were to build codes by representing field extensions over a number field (also done in [**13**] and [**14**]), and to build codes by representing cyclic division algebras over number fields. Independently, Belfiore and Rekaya proposed building codes by representing quaternion algebras over number fields [**7**]. The most famous example of this is the so-called Golden Code, which represents a quaternion algebra over the Gaussian integers. This code was obtained by Dayal and Varanasi [**15**], [**16**], and later independently by Belfiore et. al. in [**8**]. Further work on representing cyclic division algebras is e.g., in [**9**],

[21], [30], [31], [32], [35], [37]. Codes have also been built by representing cross product algebras [33].

We are indebted to Eric Moorehouse for pointing out to us the well-known fact that maximal nonsingular spaces *always* come from representing division algebras — albeit non-associative ones. In the next section we will define and discuss non-associative division algebras and recall this fact as Lemma 1.

2. Non-associative division algebras

We first recall some facts about algebras.

DEFINITION 2. Let A be an n-dimensional vector space over a field k. If there is a product

$$\circ : A \times A \to A$$

which is k-bilinear, then we call $A = (A, \circ)$ an n-dimensional non-associative k-algebra.

If in addition $a \circ b = 0$ implies that $a = 0$ or $b = 0$, we call A a non-associative k-division algebra.

If the product is associative, we call A an *associative algebra*. Hence we are considering associative algebras as a special case of non-associative algebras.

DEFINITION 3. Let f, f_1, f_2 be any k-isomorphisms from a k-vector space A to a k-vector space B. If $(A, \circ)$ and $(B, *)$ are k-algebras such that for every $b_1, b_2 \in B$,

$$b_1 * b_2 = f(f_1^{-1}(b_1) \circ f_2^{-1}(b_2)),$$

then we call (f, f_1, f_2) a k-isotopism from $(A, \circ)$ to $(B, *)$. Isotopism is an equivalence relation, so if there is a k-isotopism from $(A, \circ)$ to $(B, *)$, we will say that the algebras are k-isotopic.

Let A be a non-associative algebra of dimension n over a field k, and suppose that $\mathcal{B}$ is a basis for A. For $a \in A$, let $[a]_{\mathcal{B}}$ denote the column vector of its coordinates with respect to this basis.

DEFINITION 4. Let $(A, \circ)$ be an n-dimensional non-associative algebra over a field k, and $\mathcal{B}$ a basis for A as a k-vector space. Then by the bilinearity of $\circ$, there are matrices $M_i, N_i \in \mathrm{Mat}_{n\times n}(k)$, $1 \leq i \leq n$, such that for every $p, q \in A$, setting $r = p \circ q$ we have

$$[r]_{\mathcal{B}} = (\sum_{i=1}^{n} p_i M_i)[q]_{\mathcal{B}} = {}^t[p]_{\mathcal{B}}(\sum_{i=1}^{n} q_i N_i),$$

where $(p_i) = [p]_{\mathcal{B}}, (q_i) = [q]_{\mathcal{B}}$, and ^{t} denotes taking the transpose.

Let x_i and y_i, $1 \leq i \leq n$, be indeterminates, and x, y the column vectors whose entries are x_i and y_i. We call

$$\Lambda = \sum_{i=1}^{n} x_i M_i \text{ and } \Gamma = \sum_{i=1}^{n} y_i N_i, \tag{1}$$

the left and right representations of A with respect to $\mathcal{B}$, so $\Lambda y = {}^t x \Gamma$.

Let $f_\Lambda(x_1, ..., x_n)$, $f_\Gamma(y_1, ..., y_n)$ be the determinants of Λ and Γ. We call them the left and right determinants of A, and they are independent of the choice of $\mathcal{B}$.

Note that if A is isotopic to B, then there is an invertible linear change of variables taking the left (respectively right) determinant of A to the left (respectively right) determinant of B.

DEFINITION 5. If f is a form over a field k which has no non-trivial solutions over k, then we call f a k-anisotropic form.

DEFINITION 6. For any indeterminates $z_1, ..., z_n$ and $P_i \in \mathrm{Mat}_{n\times n}(k)$, $1 \leq i \leq n$, we call $\sum_{i=1}^n z_i P_i$ a linear matrix over k.

The left and right representations of a division algebra A over k are linear matrices whose determinants are k-anisotropic.

We can now demonstrate the claim from the end of the last section.

LEMMA 1. *Let k be a field, and $z_1, ..., z_n$ be indeterminates.*

1) If V is an n-dimensional subspace of $\mathrm{Mat}_{n\times n}(k)$ with basis P_i, $1 \leq i \leq n$, then V is a maximal nonsingular space if and only if the determinant of the linear matrix $P = \sum_{i=1}^n z_i P_i$ is k-anisotropic.

2) Let $P_i \in \mathrm{Mat}_{n\times n}(k)$, $1 \leq i \leq n$, be such that the determinant of the linear matrix $P = \sum_{i=1}^n z_i P_i$ is k-anisotropic. Then P is the left-representation of an n-dimensional non-associative division algebra over k.

PROOF. (1) is clear. As for (2), if A is k^n with the product $u \circ v = (\sum_{i=1}^n u_i P_i)v$, where $u = {}^t(u_1, ..., u_n)$, then the left representation of A with respect to the standard basis is P. □

COROLLARY 1. *Let k be a field. To find all n-dimensional non-associative division algebras over k (up to isotopy), it suffices to:*

1) Find all degree-n anisotropic forms f in n variables over k (up to invertible linear change of variables).

2) Determine which such f are the determinants of linear matrices.

3) Given such an f, find all linear matrices whose determinant is f.

An early construction of non-associative division algebras was due to Dickson, who for any field k of characteristic not 2, attached a (commutative) 3-dimensional non-associative division algebra $(A, \circ)$ over k to any irreducible cubic

$$g = x^3 - ax^2 - bx - c$$

over k. (He also showed that these were the only commutative ones when k is a finite field: see [**20**]. Also see [**24**] and [**40**] for more recent work.) Suppose that R is the set of roots of g in a splitting field of g. Dickson took A be a 3-dimensional vector space over k with basis $1, i, j$, and $\circ$ to be a k-bilinear product satisfying $j = i \circ i, i \circ j = j \circ i = c + bi + aj, j \circ j = 4ac - b^2 - 8ci - 2bj$, with 1 being a 2-sided identity for $\circ$. Then the left determinant and right determinant of $(A, \circ)$ are both

$$\prod_{r\in R}(x - ry - (b + 2cr - 2r^2)z),$$

which is an anisotropic form over k.

This was generalized by Albert to the construction of *twisted fields* over a field k [**3**], which was further generalized by him to the construction (naturally enough) of *generalized twisted fields* over k [**4**]. This was all done for k a finite field, but Menichetti gave a definition over any field [**27**], which we state more generally here.

DEFINITION 7. Let F be a degree-n galois extension of a field k. Fix σ, τ in $\mathrm{Gal}(F/k)$, and $\alpha \in F$, an element whose norm to k is not 1. Let $\circ : F \times F \to F$ be defined by

$$x \circ y = xy - \alpha x^{\sigma} y^{\tau}.$$

Then $(F, \circ)$ is an n-dimensional non-associative division algebra over k called a generalized twisted field over k split by F.

When $n = 2$, all non-associative division algebras over k are isotopic to representations of quadratic field extensions over k. Indeed, it is shown in [**2**] that any such algebra is isotopic to a non-associative division algebra $(A, \circ)$ with a multiplicative identity e. Then embedding k into A by sending $a \mapsto a \circ e$, we can assume that k is in the center of A. Remark 11.4.3 of [**10**] then shows that $(A, \circ)$ is a field (see also [**19**]).

From now on we will concentrate on the case $n = 3$.

3. Classifying 3-dimensional non-associative division algebras over a perfect field

By Corollary 1, to classify 3-dimensional non-associative division algebras, our first task is to classify anisotropic ternary cubic forms. We do this now for forms over a perfect field k. Let G_k denote the absolute galois group of k.

LEMMA 2. *Let $f(x_1, x_2, x_3)$ be an anisotropic cubic form over a perfect field k, and $C = Z(f)$, the projective algebraic set defined by f over an algebraic closure $\bar{k}$ of k. Then either:*

1) C is the union of 3 lines conjugate under G_k, or,

2) C is absolutely irreducible, is nonsingular, and is a curve of genus 1.

PROOF. The group G_k acts on the components of C. Since f is k-anisotropic, C cannot contain a k-rational line. Hence if C is not absolutely irreducible, it must be the union of three conjugate lines.

If C is absolutely irreducible, then since it is a plane cubic, it has at most 1 singular point. Such a singular point would then be k-rational, so C must be nonsingular. Hence C is a curve of genus 1. □

If A is a 3-dimensional generalized twisted field over k split by a cyclic cubic extension F of k, then its left and right determinants are products of three conjugate lines. Menichetti [**27**] has shown the converse:

PROPOSITION 1. [**27**] *If k is a perfect field with a cyclic cubic extension field F, and A is a non-associative division algebra of dimension 3 over k, for which f_Λ and f_Γ factor into linear factors over F, then A is isotopic to a generalized twisted field over k split by F.*

REMARK 1. In fact, f_Γ factors over F if and only if f_Λ does. That this is true over the algebraic closure of F is a special case of Proposition 1 (iii) of [**29**]. We now proceed along similar lines to show that it is also true over F.

As in (1), let $\Lambda = \sum_{i=1}^{3} x_i M_i$ be the left representation of A. Since A is a division algebra, M_1 is invertible. Multiplying Λ by M_1^{-1} gives a representation of an isotopic algebra, so we can take $M_1 = I$, the 3×3 identity. Suppose $x_1 + \alpha x_2 + \beta x_3$ is a factor of f_Λ over F. Then $-\alpha x_2 - \beta x_3$ is an eigenvalue of $x_2 M_2 + x_3 M_3$, and $-(\alpha x_2 + \beta x_3) I + x_2 M_2 + x_3 M_3$ is a singular matrix, with a non-zero

vector v with entries in $F(x_2, x_3)$ in its nullspace. Clearing denominators and taking homogeneous parts, we can assume that the entries of v are homogeneous polynomials in $F[x_2, x_3]$ of some minimal degree d. If d is 0, then v is a common eigenvector of M_2 and M_3, and the same is true of its conjugates over k. Since f_Λ has three distinct conjugate linear factors, v has three distinct conjugates corresponding to three distinct eigenvalues. Hence all M_i commute with each other and A is a field isomorphic to F, so f_Γ factors over F as well. So we can take $d > 0$. Again as in (1), we have $\Lambda y = {}^t x\Gamma$, where $\Gamma = \sum_{i=1}^{3} y_i N_i$. We deduce that when $x_1 = -\alpha x_2 - \beta x_3$, ${}^t x\Gamma = 0$ when $y_i = v_i$. Hence the map $y_i = v_i$ is a non-constant rational map from $\mathbb{P}^1$ to $Z(f_\Gamma) = Z(\det(\Gamma))$. Hence $Z(f_\Gamma)$ cannot be a curve of genus 1, so f_Γ must factor into conjugate linear factors over an extension field of k. Since v is defined over $F(x_2, x_3)$, and a curve can be contained in at most one line in $\mathbb{P}^2$, f_Γ must factor over F.

Note that a k-anisotropic ternary cubic form f remains anisotropic over any quadratic extension M of k: the k-rational line though an M-rational point of $Z(f)$ and its conjugate would have a third point of intersection with $Z(f)$ that is k-rational. From Proposition 1, we get the following:

PROPOSITION 2. *Let A be a 3-dimensional non-associative division algebra over k, and f_Λ its left determinant. Suppose that f_Λ factors over a cubic extension field F of k.*

1) If F is a cyclic extension of k, A is isotopic to a generalized twisted field over k split by F.

2) If F is a radical cubic extension of k whose galois closure N over k contains the quadratic extension M of k, then $A \otimes M$ is a generalized twisted field over M split by N.

REMARK 2. Dickson's construction (see §2) gives examples of algebras that fall into case (2). Indeed, the algebra attached to an irreducible cubic g over k becomes a twisted field over k adjoined with the square root of the discriminant of g.

Therefore we can concentrate on classifying non-associative 3-dimensional division algebras A over k whose left representations have determinants which are absolutely irreducible ternary cubic forms.

REMARK 3. Menichetti settled a conjecture of Kaplansky [**25**] by showing that when k is a finite field, every 3-dimensional non-associative division algebra over k is isotopic to a generalized twisted field [**26**]. He gave a more recent proof based on Proposition 1, by noting that the Hasse-Weil bound on absolutely irreducible ternary cubics over k prohibits them from being k-anisotropic.

PROPOSITION 3. *Let k be a perfect field, f an absolutely irreducible anisotropic ternary cubic form over k, and $C = Z(f)$, which is a curve of genus 1.*

Let E be the elliptic curve which is the jacobian of C. Then C is a homogeneous space for E over k (i.e., it is in the Weil-Châtelet group $WC(E/k)$), and has index 3 as a homogeneous space over k.

PROOF. A cubic curve over k must have index over k dividing 3, so since C is k-anisotropic, it must have index 3. □

Note that every C in $WC(E/k)$ which has index 3 over k has a model as a plane cubic over k, so is $Z(f)$ for some absolutely irreducible ternary cubic over k

[**5**]. So to carry out the second step in Corollary 1 for $n = 3$, we need now only find which elliptic curves E over k have elements of $WC(E/k)$ which have index 3 over k and which are determinants of linear matrices over k. This is answered by a result of Beauville [**6**].

PROPOSITION 4. *Let f be an absolutely irreducible nonsingular ternary cubic form over a perfect field k, and $C = Z(f)$. Then f is the determinant of a linear matrix over k if and only if there is a k-rational divisor D on C of degree 0 which is not linearly equivalent to* 0.

PROOF. Corollary 1.12 of [**6**] applied to plane cubic forms shows that f is the determinant of a linear matrix over k if and only if there is a k-rational divisor D of degree 0 such that $H^0(C, D) = 0$. By the Riemann-Roch theorem, since C has genus 1 and D has degree 0, $H^0(C, D) = H^0(C, -D)$. Lemma 5.4 of [**28**] shows that on a complete variety, a divisor D or its negative have no non-trivial global sections precisely when D is not linearly equivalent to 0. Hence f is the determinant of a linear matrix over k if and only if there exists a k-rational divisor D of degree 0 on C which is not linearly equivalent to 0. □

For a nonsingular variety V over k, we will let $\mathrm{Div}_k^0(V)$ denote its group of k-rational divisors of degree 0, and $\mathrm{Pic}_k^0(V)$ denote its group of k-rational divisor classes of degree 0. For $D \in \mathrm{Div}_k^0(V)$, we will let $[D]$ denote its corresponding divisor class in $\mathrm{Pic}_k^0(V)$. We will write $D_1 \sim D_2$ if the divisors D_1, D_2 on V are linearly equivalent.

In light of Propositions 2, 3, and 4, we can now update Corollary 1.

COROLLARY 2. *To find all non-associative 3-dimensional division algebras over a perfect field k which are not isotopic to generalized twisted fields over k or a quadratic extension of k, one needs only to find all elliptic curves E over k such that:*

1) There are elements C in $WC(E/k)$ which have index 3 over k and for which there exist $D \in \mathrm{Div}_k^0(C)$ with $[D] \neq 0$.

2) Writing $C = Z(f)$, f a ternary cubic, find all ways to write f as the determinant of a linear matrix over k.

REMARK 4. So far as we know, the algebras arising from genus 1 curves as in (1) form a new class of 3-dimensional non-associative division algebras.

We will show how to carry out (2) in the next section.

4. Constructive proof of Proposition 4 for anisotropic cubic forms

The proof of Proposition 4 is not constructive (at least not to our tastes). In what follows we give a constructive proof in the case of anisotropic cubic forms. We prove the two implications of Proposition 4 separately.

THEOREM 1. *Let $f(x_1, x_2, x_3)$ be an absolutely irreducible anisotropic cubic form over a perfect field k, $C = Z(f)$, and D a k-rational divisor on C of degree 0 which is not linearly equivalent to* 0. *Let $\{Q_1, Q_2, Q_3\}$ be the intersection of C with $Z(\ell)$ for any linear form $\ell(x_1, x_2, x_3)$ with coefficients in k, and $Q = Q_1 + Q_2 + Q_3$ the resulting k-rational divisor. Set $D' = Q + D$, $D'' = Q - D$. By the Riemann-Roch Theorem, $\mathcal{L}(D')$ and $\mathcal{L}(D'')$ are 3-dimensional: let $\{g_1, g_2, g_3\}$ and $\{h_1, h_2, h_3\}$*

be respective k-bases for them. Then there are points P_{ij}, R_{ij}, $1 \le i,j \le 3$ on C such that

$$(g_i) = \sum_{j=1}^{3} P_{ij} - D', \ 1 \le i \le 3, \ (h_j) = \sum_{i=1}^{3} R_{ij} - D'', \ 1 \le j \le 3.$$

We claim that

1) For every $1 \le i,j \le 3$ there is a non-zero ternary quadratic form q_{ij} over k that passes through the six points

$$S_{ij} = \{P_{i1}, P_{i2}, P_{i3}, R_{1j}, R_{2j}, R_{3j}\},$$

taken with multiplicity, that is unique up to constant multiples.

2) The q_{ij} can be chosen such that every 2×2 minor of $N = [q_{ij}]_{1 \le i,j \le 3}$ is divisible by f.

3) With N chosen as in (2), $\det N \neq 0$.

4) Let L be the linear matrix over k such that the classical adjoint of N, $N^{adj} = fL$. Then there is a non-zero constant $\beta \in k$ such that $\det L = \beta f$. Dividing any row or column of L by β gives a linear matrix M over k with $\det M = f$.

PROOF. 1) The functions $f_{ij} = x_i x_j / \ell^2$, $1 \le i \le j \le 3$ are in $\mathcal{L}(2Q)$, and are linearly independent since f is an absolutely irreducible cubic. Since C has genus 1, the dimension of $\mathcal{L}(2Q)$ is 6, and the f_{ij} are a basis for $\mathcal{L}(2Q)$. It follows that since the divisor of $g_i h_j$ is

$$P_{i1} + P_{i2} + P_{i3} + R_{1j} + R_{2j} + R_{3j} - 2Q,$$

$g_i h_j \in \mathcal{L}(2Q)$, and such a q_{ij} exists over $\bar{k}$. If q'_{ij} is another such quadratic, then q'_{ij}/q_{ij} is a constant c in the function field $k(C)$ of C, and hence $q'_{ij} \equiv c q_{ij} \mod f$. Again, since f is an absolutely irreducible cubic, we have $q'_{ij} = c q_{ij}$. Finally, since G_k fixes S_{ij}, it acts on q_{ij} via multiplication by constants, so by Hilbert's Theorem 90 there is a multiple of q_{ij} defined over k.

2) Any 2×2 minor of N is of the form $q_{ij}q_{i'j'} - q_{ij'}q_{i'j}$, for some $1 \le i \neq i', j \neq j' \le 3$. Both $q_{ij}q_{i'j'}$ and $q_{ij'}q_{i'j}$ are quartics which vanish on the 12 points $P_{i\ell}, P_{i'\ell}, R_{\ell j}, R_{\ell j'}$, $1 \le \ell \le 3$, taken with multiplicity. Hence $q_{ij}q_{i'j'}/q_{ij'}q_{i'j}$ represents a constant function $c \in k$ in $k(C)$. Again it follows that $q_{ij}q_{i'j'} \equiv c q_{ij'}q_{i'j} \mod f$. Note that $c \neq 0$, for otherwise f divides $q_{ij}q_{i'j'}$, and since f is irreducible it would divide one of the quadratics q_{ij} or $q_{i'j'}$, which is impossible. Hence we can multiply q_{12}, q_{13}, q_{22}, and q_{23} by constants such that the minors $N_{13}, N_{23}, N_{12}, N_{22}$ all vanish mod f. By the Laplace expansion, $N_{13}(q_{12}/q_{32}) + N_{23}(q_{22}/q_{32}) + N_{33} = 0$ in $k(C)$, so $N_{33} \equiv 0 \mod f$. Likewise $N_{32} \equiv 0 \mod f$. By a similar argument, we get in turn that $N_{11} \equiv N_{21} \equiv N_{31} \equiv 0 \mod f$.

3) First we claim that each q_{ij} is absolutely irreducible. If not, it factors into 2 lines $\ell_1 \ell_2$, with the three zeros of each line intersected with C defined over some quadratic extension F of k. Without loss of generality, say ℓ_1 vanishes at P_{i1}. Then since C has index 3 over k, P_{i1} has three conjugates over k and hence over the quadratic extension F. Since g_i is defined over k, the other conjugates must be P_{i2} and P_{i3}, so we would have that P_{i1}, P_{i2}, and P_{i3} are collinear, violating the assumption that D is not linearly equivalent to 0, and establishing the claim.

Next we claim that each minor $N_{ij} = \pm(q_{i'j'}q_{i''j''} - q_{i'j''}q_{i''j'})$ does not vanish, where $\{i, i', i''\} = \{j, j', j''\} = \{1, 2, 3\}$. If it did, $q_{i'j'}$ would divide $q_{i'j''}q_{i''j'}$ and hence either $q_{i'j''}$ or $q_{i''j'}$. The latter would imply that $\{P_{i'1}, P_{i'2}, P_{i'3}\} =$

$\{P_{i''1}, P_{i''2}, P_{i''3}\}$, and the former that $\{R_{1j'}, R_{2j'}, R_{3j'}\} = \{R_{1j''}, R_{2j''}, R_{3j''}\}$. This violates either the assumption that the g_i or h_j are linearly independent, and establishes the claim.

From the above and (2) we conclude that $N^{adj} = fL$, where L is a linear matrix whose entries are all non-zero.

Now assume that $\det N = 0$. Since its 2×2 minors do not vanish, N must have rank 2. Since every column of N^{adj} is in the 1-dimensional nullspace of N, N^{adj} has rank 1.

It is easy to see that every rank-1 linear matrix L whose entries are all non-zero is either a product $D\kappa$ or κD where D is a nonsingular diagonal linear matrix and κ is a rank-1 matrix of constants. From $0 = N^{adj}N = NN^{adj}$ we conclude that either $\kappa N = 0$ or $N\kappa = 0$. The former violates the linear independence of the g_i and the latter violates the linear independence of the h_j. Hence $\det N \neq 0$.

4) From $N^{adj} = fL$ and $NN^{adj} = \det N I$, we get

$$f^3 \det L = \det N^{adj} = (\det N)^2.$$

Since f is absolutely irreducible, f^2 divides $\det N$, and since they have the same degree, $\det N = \alpha f^2$ for some $\alpha \in k$. By (3), $\alpha \neq 0$. Hence $\det(L) = \beta f$, where $\beta = \alpha^2 \neq 0$. Dividing any row or column of L by β gives a matrix M over k with $\det M = f$. □

REMARK 5. Given f and D, instead of first computing g_i and h_j for $1 \leq i, j \leq 3$, it may be easier to first find six k-rational divisors $E_i = P_{i1} + P_{i2} + P_{i3}$, and $F_j = R_{1j} + R_{2j} + R_{3j}$, $1 \leq i, j \leq 3$, on C such that

$$D = E_1 - Q \sim E_2 - Q \sim E_3 - Q \sim -F_1 + Q \sim -F_2 + Q \sim -F_3 + Q,$$

and then find quadratics q_{ij} over k such that the intersection divisor of $Z(q_{ij})$ with C is $E_i + F_j$, and such that if $N = [q_{ij}]$, then $f | N^{adj}$ (see, e.g., section 6). Then if $\det(N) \neq 0$, necessarily the functions g_i and h_j whose divisors are $E_i - D'$ and $F_j - D''$, $1 \leq i, j \leq 3$, are bases for $\mathcal{L}(D')$ and $\mathcal{L}(D'')$ respectively, with $D' = Q + D$ and $D'' = Q - D$. With this the hypotheses of the theorem are met, so if L is the linear matrix such that $N^{adj} = fL$, then dividing any row or column of L by a non-zero constant gives a matrix M with $\det M = f$.

The following is a converse to Theorem 1, and the other half of a constructive proof of Proposition 4 for anisotropic cubic forms.

THEOREM 2. *Let $f(x_1, x_2, x_3)$ be an absolutely irreducible anisotropic cubic form over a perfect field k. Then every linear matrix L over k whose determinant is f arises from the construction given in Theorem 1.*

Specifically, let $C = Z(f)$, $\{Q_1, Q_2, Q_3\}$ be the intersection of C with a k-rational line $Z(\ell)$, and $Q = Q_1 + Q_2 + Q_3$. Let $N = L^{adj}$, and q_{ij} the quadratic form which is the ij^{th} entry of N. Then:

1) There are points P_{ij} and R_{ij}, $1 \leq i, j \leq 3$ on C such that:

i) q_{ij} vanishes on the points

$$S_{ij} = \{P_{i1}, P_{i2}, P_{i3}, R_{1j}, R_{2j}, R_{3j}\},$$

taken with multiplicity.

ii) For all $1 \leq i, j \leq 3$, $E_i = P_{i1} + P_{i2} + P_{i3}$ and $F_j = R_{1j} + R_{2j} + R_{3j}$ are k-rational.

iii) If $D' = E_1$, $D'' = 2Q - D'$, *then*

$$E_1 \sim E_2 \sim E_3 \sim D', \text{ and } F_1 \sim F_2 \sim F_3 \sim D''.$$

iv) If $D = D' - Q$, *(so* $D' = Q + D$ *and* $D'' = Q - D$*), then* D *is* k*-rational of degree* 0 *and* $[D] \neq 0$.

2) Let g_i *and* h_j *be* k*-rational functions whose divisors are respectively* $E_i - D'$ *and* $F_j - D''$. *Then* g_i *and* h_j *are bases for* $\mathcal{L}(D')$ *and* $\mathcal{L}(D'')$, *respectively.*

3) $L = N^{adj}/f$.

PROOF. 1) Let L be a linear matrix over k whose determinant is an absolutely irreducible anisotropic cubic form $f(x_1, x_2, x_3)$. Note that every 2×2 minor of L is a non-zero quadratic form, since otherwise there is a k-linear combination of 2 rows or columns of L that has only one non-zero entry, violating the irreducibility of f. Therefore each 2×2 minor cannot vanish mod f. Hence in the function field $k(C)$ of C, L/ℓ has rank 2. So if $N = L^{adj}$, as in the proof of (3) in the previous theorem, N/ℓ^2 has rank 1 in $k(C)$.

For any $1 \leq j \leq 3$, let $R_j = Z(q_{1j}, q_{2j}, q_{3j})$ be the common intersection of the quadratics q_{1j}, q_{2j}, q_{3j}, which is a k-rational set. Since the determinant of N is f^2, C must vanish at the points of R_j. Since f is absolutely irreducible, q_{1j}, q_{2j}, q_{3j} cannot have a component in common, so no 3 points of R_j are collinear and $|R_j| \leq 4$. Since C has no points over k or any quadratic extension of k, $|R_j|$ is 0 or 3. Take $1 \leq j' \leq 3$, $j' \neq j$. Since N/ℓ^2 has rank 1 in $k(C)$, $q_{1j}/q_{1j'}, q_{2j}/q_{2j'}, q_{3j}/q_{3j'}$ are representatives for a function $w_{jj'} \in k(C)$ whose divisor of zeros is $\leq \sum_{P \in R_j} P$ and whose divisor of poles is $\leq \sum_{P \in R_{j'}} P$. If R_j were empty, then $w_{jj'}$ would be a function with no zeros, so would be a non-zero constant $c_{jj'}$. Hence $q_{ij} \equiv c_{jj'} q_{ij'}$ mod f, so since the q_{ij} are quadratics, $q_{ij} = c_{jj'} q_{ij'}$, for $1 \leq i \leq 3$. This would mean $\det N = 0$, a contradiction. Therefore R_j is a k-rational set of 3 non-collinear distinct points on C for every $1 \leq j \leq 3$. Likewise, we must have $R_j \neq R_{j'}$ since $w_{jj'}$ is not a constant. Hence the F_j are all k-rational, distinct, linearly equivalent to each other, and not linearly equivalent to Q. Applying the same argument to ${}^tL$ replaces N by ${}^tN$, so we get distinct k-rational sets $P_i = \{P_{i1}, P_{i2}, P_{i3}\}$, of non-collinear points at which all entries of the i^{th} row of N vanish, for $1 \leq i \leq 3$. Hence the E_i are all k-rational, distinct, and linearly equivalent to each other. Hence D is k-rational of degree 0 and $[D] \neq 0$.

If $P_i \neq R_j$, for some $1 \leq i, j \leq 3$, then since the q_{ij} are quadratics and f is absolutely irreducible, we know that the intersection of $Z(q_{ij})$ and C is precisely S_{ij}. Since for some i and j, $P_i \neq R_j$, we have that $E_i + F_j \sim 2Q$, which gives $F_j \sim D''$. We note that even if $P_i = R_j$ for some i, j, then still q_{ij} vanishes at S_{ij}, accounting for multiplicities. Indeed, in this case, there are $1 \leq i', j' \leq 3$ such that $P_i \neq R_{j'}$, $P_{i'} \neq R_j$ and $P_{i'} \neq R_{j'}$. Since $f | q_{ij} q_{i'j'} - q_{ij'} q_{i'j}$, $Z(q_{ij} q_{i'j'})$ has the same intersection with C as does $Z(q_{i'j} q_{ij'})$. The latter intersection consists of $P_i, P_{i'}, R_j$ and $R_{j'}$ counted with multiplicities, so the former must, too. Since the intersection of $Z(q_{i'j'})$ with C is $S_{i'j'}$, we have the result.

2) If g_i and h_j did not form bases, we would have $\det N = 0$.

3) This is just $(L^{adj})^{adj} = (\det L)L$, which follows since L is a 3×3 matrix. □

COROLLARY 3. *Let* A *be a 3-dimensional non-associative division algebra over a perfect field* k *which is not isotopic to a generalized twisted field over* k *or over any quadratic extension of* k. *Let* f *be the left determinant of* A *which is an anisotropic absolutely irreducible ternary cubic over* k. *Let* $C = Z(f)$.

Theorem 2 gives a method for finding a k-rational divisor D on C of degree 0 such that $[D] \neq 0$ in $\mathrm{Pic}_0^k(C/k)$. Theorem 1 gives a method for recovering A up to isotopy from C and D.

Indeed, Theorem 2 gives that $D = Z(q_{11}, q_{12}, q_{13}) - Z(f, \ell)$.

5. Classifying 3-dimensional non-associative division algebras over number fields

Let K be a number field and $\mathcal{O}_K$ be its ring of integers. Let $\wp$ be a non-zero prime ideal in $\mathcal{O}_K$, and $K_\wp$ the completion of K at $\wp$. Let E be an elliptic curve over $K_\wp$ and $C \in WC(E/K_\wp)$ have index 3 over $K_\wp$. One can show [**18**] that there is always a divisor $D \in \mathrm{Div}^0_{K_\wp}(C)$ with $[D] \neq 0$. Therefore by Corollary 2 and the results of section 4, the problem of finding all non-associative 3-dimensional division algebras over $K_\wp$ comes down to the problem of finding all $K_\wp$-anisotropic ternary cubic forms, which we do in [**18**].

One class of division algebras over a number field K consists of algebras A where $A \otimes K_\wp$ is a division algebra for some prime $\wp \subset \mathcal{O}_K$. Our remaining interest therefore is in division algebras A such that $A \otimes K_\wp$ is *not* a division algebra for any localization $K_\wp$ of K.

For an elliptic curve E/K, let $Ш(E)$ denote its Tate-Shafarevich group over K. We get the following classification:

THEOREM 3. *Let K be a number field. Then every non-associative division algebra A of dimension 3 over K is one of the following types:*

1) A is a generalized twisted field.

2) $A \otimes M$ is a generalized twisted field over M, for some quadratic extension M of K.

3) $A \otimes K_\wp$ is a non-associative division algebra over $K_\wp$ for some prime $\wp \subset \mathcal{O}_K$.

4) A has a left representation whose determinant is in $Ш(E)[3] - \{0\}$ for some elliptic curve E/K with $E(K) \neq 0$.

PROOF. Suppose that A does not lie in the classes of algebras described in (1), (2), and (3). Then by Corollary 2, if f is the left determinant of A, then $C = Z(f)$ is an element of $WC(E/K)$ — where E/K is the jacobian of C — which has index 3 over K. Since $A \otimes K_\wp$ is not a division algebra for any $\wp$, f has a non-trivial solution in $K_\wp$ for every $\wp$. Since cubic forms always have real and complex points, C is everywhere locally trivial, so $C \in Ш(E/K)$. Recall [**36**] that for $C \in Ш(E/K)$, the index of C over K is equal to its period in $Ш(E/K)$, and that a non-trivial K-rational D of degree 0 on C exists if and only if $E(K) \neq 0$. □

6. An example

Part (4) of Theorem 2 and the results of section 4 give a recipe for constructing new non-associative division algebras over a number field K. We now present the one example we have computed, where $K = \mathbb{Q}$ and E is the elliptic curve 9747G1 in Cremona's tables [**12**]. There it is shown that E has bad reduction only at 3 and 19, that $E(\mathbb{Q}) = \mathbb{Z}/3\mathbb{Z}$, and assuming the Birch-Swinnerton-Dyer Conjecture holds for E, that $Ш(E/\mathbb{Q}) = (\mathbb{Z}/3\mathbb{Z})^2$. Our first task is to produce a homogeneous space C that we can verify lies in $Ш(E/\mathbb{Q})[3] - \{0\}$.

A linear change of variables of 9747G1 gives us the model

$$y^2z + 361yz^2 = x^3 \tag{2}$$

for E, upon which P defined by $(x, y, z) = (0, 0, 1)$ is a $\mathbb{Q}$-rational point of order 3. Let $\phi : E \to E' = E/ < P >$ be the resulting isogeny of degree 3. We will search for C in $Ш(E/\mathbb{Q})[\phi] \subseteq Ш(E/\mathbb{Q})[3]$.

Let G denote the absolute galois group of $\mathbb{Q}$. As G-modules, $< P >= \mathbb{Z}/3\mathbb{Z}$, and $H^1(G, \mathbb{Z}/3\mathbb{Z})$ parameterizes cyclic cubic extensions of $\mathbb{Q}$. Hence any $C \in H^1(G, E[\phi]) = H^1(G, \mathbb{Z}/3\mathbb{Z})$ is a twist of E over a cyclic cubic extension of $\mathbb{Q}$.

Recall that every cyclic cubic extension of $\mathbb{Q}$ is $\mathbb{Q}(r)$ for r a root of

$$t^3 - 3jt^2 + 3(j-1)t + 1$$

for some $j \in \mathbb{Q}$. In section 4 of [**11**] it is shown that for any such j, the twist of (2) corresponding to $\mathbb{Q}(r)$ as an element of $H^1(G, \mathbb{Z}/3\mathbb{Z})$ is

$$C : (27)(361)X^3 = 9(j^2 - j + 1)(Z^3 - 3jZ^2Y + 3(j-1)ZY^2 + Y^3),$$

coming from an isomorphism $\theta : C \to E$ over $\mathbb{Q}(r)$ given by

$$x = 3(361)X, y = (361)(((2-3j)Y + 2Z) + r((3j+1)Y + (3j-2)Z) - r^2(Y+Z)),$$

$$z = 2Y + (3j-4)Z + r((3j-2)Y + (1-6j)Z) - r^2(Y - 2Z).$$

It is also shown there that E' has a model

$$v^2w + 9(361)vw^2 = u^3 - 27(361)^2w^3$$

and that the composite morphism $\psi = \phi \circ \theta$ is defined over $\mathbb{Q}$.

We will now consider C for $j = 0$, in which case $r = \zeta_9 + \zeta_9^{-1}$ where ζ_9 is a primitive ninth-root of unity. Then C is given by $f(X, Y, Z) = 0$, where

$$f(X, Y, Z) = 1083X^3 - Y^3 - Z^3 + 3Y^2Z,$$

and ψ is the morphism

$$u = (27)(361)^3(XY^2 - XYZ + XZ^2), v = (27)(361)^3(-2Y^3 + 3Y^2Z + 3YZ^2 - 2Z^3),$$

$$w = (9)(361)^2(Y^3 - 3Y^2Z + Z^3).$$

We now want to verify that C is of order 3 in $Ш(E/\mathbb{Q})$. First of all, C is automatically trivial over $\mathbb{Q}_p$ for any prime $p \neq 3, 19$. Hensel's Lemma shows that the point $(0, 1, 9)$ over $\mathbb{Z}/19\mathbb{Z}$ lifts to a $\mathbb{Z}_{19}$-point. Changing models for C by substituting $X + 3Y$ for Y and $-X + 3Z$ for Z yields

$$C' : 40X^3 - X^2Y - 2XY^2 - Y^3 + 2XYZ + 3Y^2Z + XZ^2 - Z^3 = 0$$

after dividing by 27. Hensel's Lemma shows that the $\mathbb{Z}/3\mathbb{Z}$-point $(X, Y, Z) = (1, 1, 0)$ on C' lifts to a $\mathbb{Z}_3$-point. Since cubics always have real points, C is everywhere locally trivial.

Note that E' is curve 9747G2 in [**12**], which shows that $E'(\mathbb{Q}) = 0$. Hence $(\ell, m, n) \in C(\mathbb{Q})$ for relatively prime integers ℓ, m, n only if $\psi(\ell, m, n) = (u, v, w) = (0, 1, 0)$. This implies $m^3 - 3m^2n + n^3 = 0$, which only has the integer solution $m = n = 0$. But $(1, 0, 0)$ does not lie on C, so $C(\mathbb{Q}) = \emptyset$. This shows that C is non-trivial in $Ш(E/\mathbb{Q})$, so as an irreducible cubic is a homogeneous space of index 3 over $\mathbb{Q}$, hence must be of order 3 in $Ш(E/\mathbb{Q})$.

To apply Theorem 1, we need a rational divisor D of degree 0 on C that is not linearly equivalent to 0.

Let P_0 be the origin on E, $P_1 = P$ and $P_2 = -P$, which are inflection points. Then if we set $Q_i = \theta^{-1}(P_i)$, then $Q_0 = (0, 1, r)$, $Q_1 = (0, 1, 1/(1-r))$, $Q_2 = (0, 1, (r-1)/r)$ and there is a generator σ in $\mathrm{Gal}(\mathbb{Q}(r)/\mathbb{Q})$ that sequentially maps r into $1/(1-r)$ into $(r-1)/r$. Hence $\{Q_0, Q_1, Q_2\}$ is a $\mathbb{Q}$-rational set which is the locus of $X = 0$ on C. Let ℓ be the line which is tangent to C at Q_0, so has divisor $3Q_0$. Then $2Q_0 \sim Q_1 + Q_2$, so if we set $D = Q_0 - Q_2$, $D \sim D^\sigma$, so the divisor class $[D]$ is $\mathbb{Q}$-rational and is non-trivial in $\mathrm{Pic}^0_{\mathbb{Q}}(C)$. Since $C \in Ш(E/\mathbb{Q})$, the class $[D]$ must contain a rational divisor. To find one, note that the divisor of $(\ell/X)(\ell^\sigma/X)(\ell^{\sigma^2}/X)$ vanishes, so the norm of ℓ/X is a constant in $\mathbb{Q}(C)$. We can take $\ell = rY - Z$, and we find $\ell\ell^\sigma\ell^{\sigma^2} = -Y^3 - Z^3 + 3Y^2Z = -1083X^3 + f(X, Y, Z)$. Let $\mathcal{N}$ denote the norm from $\mathbb{Q}(r)(C)/\mathbb{Q}(C)$ which restricts to the norm from $\mathbb{Q}(r)$ to $\mathbb{Q}$ on constants. Suppose we have an $\alpha \in \mathbb{Q}(r)$ with $\mathcal{N}(\alpha) = -1083$. Then $\mathcal{N}(\ell/\alpha X) = 1$, so by Hilbert's Theorem 90, there is a $g_\alpha \in \mathbb{Q}(r)(C)$ such that $\ell/\alpha X = g_\alpha^\sigma/g_\alpha$. Since the divisor of $\ell/\alpha X$ is $D - D^\sigma$, it follows that $D_\alpha = D + (g_\alpha)$ is a $\mathbb{Q}$-rational divisor in $[D]$. A standard argument shows that we can take

$$g_\alpha = 1 + (\ell/\alpha X)^{\sigma^2} + (\ell/\alpha X)^\sigma(\ell/\alpha X)^{\sigma^2} = W_\alpha/\alpha^\sigma\alpha^{\sigma^2}X^2,$$

where W_α is the quadratic $\alpha^\sigma\alpha^{\sigma^2}X^2 + \alpha^\sigma X\ell^{\sigma^2} + \ell^\sigma\ell^{\sigma^2}$. The intersection of $Z(W_\alpha)$ with C consists of 6 points including Q_1 and twice Q_2. Let $P_{\alpha 1}$, $P_{\alpha 2}$, $P_{\alpha 3}$ be the residual points of intersection. Then

$$D_\alpha = P_{\alpha 1} + P_{\alpha 2} + P_{\alpha 3} - Q_0 - Q_1 - Q_2.$$

If $\alpha_1 = 8 + 6r - 5r^2$, then $N(\alpha_1) = -1083$. Since $\mathcal{N}(-r) = 1$, if $\alpha_2 = -r\alpha_1$, $\alpha_3 = r^2\alpha_1$, then also $\mathcal{N}(\alpha_i) = -1083$ for $i = 2, 3$. Let $P_{ij} = P_{\alpha_i j}$ for $1 \le i, j \le 3$.

Let $q_{11} = 3(-86X^2 + 3XY + 8XZ + Z^2)$. It is shown in [**17**] that taking the resultant of f and W_{α_1} shows that q_{11} vanishes on P_{11}, P_{12}, and P_{13}. Let R_{11}, R_{21}, R_{31} be the other 3 points of intersection of $Z(W_{\alpha_1})$ and C. Likewise, $q_{22} = 73X^2 - 11XY + 24XZ + Z^2$ and $q_{33} = 3(X^2 - 13XY + 43XZ + Z^2)$ vanish respectively on P_{21}, P_{22}, P_{23} and P_{31}, P_{32}, P_{33}. Define R_{1i}, R_{2i}, R_{3i} as the other points of intersection of C and $Z(W_{\alpha_i})$ for $i = 2, 3$. Then following the process outlined in Remark 5, we can take

$$\begin{aligned}
q_{12} &= -246X^2 - 3XY + 21XZ + YZ - Y^2 + 2Z^2,\\
q_{13} &= 3(-159X^2 - 2XY + 19XZ + YZ + Z^2),\\
q_{21} &= 147X^2 - 16XY + 35XZ - YZ + 2Z^2,\\
q_{23} &= 234X^2 - 18XY + 54XZ + YZ - Y^2 + 2Z^2,\\
q_{31} &= -12X^2 - 21XY + 75XZ - 4YZ + Y^2 + 4Z^2,\\
q_{32} &= -87X^2 - 19XY + 56XZ - YZ + 2Z^2,
\end{aligned}$$

which were multiplied by constants so that $N = [q_{ij}]$ has the property that $N^{adj} = fL$ for a linear matrix L. For details on the construction of the q_{ij}, see [**17**]. We get that L is

$$\begin{pmatrix} 19X + Z & 39X & -21X - Y - Z \\ -3X + Y - 2Z & -6X + 3Z & -9X \\ -11X & -18X + Y - 2Z & 16X + Z \end{pmatrix},$$

whose determinant is precisely f. Hence L is the left representation of a new 3-dimensional non-associative division algebra over $\mathbb{Q}$.

References

[1] S. Alamouti. *A simple transmit diversity technique for wireless communications.* IEEE Journal on Select Areas in Communications **16**, No. 8 (1998), 1451–1458.

[2] A. A. Albert. *Non-associative algebras I: Fundamental concepts and Isotopy*, Ann. of Math. **43** (1942), 685–707.

[3] A. A. Albert. *On nonassociative division algebras*, Trans. Amer. Math. Soc. **72** (1952), 296–309.

[4] A. A. Albert. *Generalized twisted fields*, Pac. J. Math. **11** (1961), 1–8.

[5] S. An, S. Kim, D. Marshall, S. Marshall, W. McCallum, A. Perlis. *Jacobians of genus one curves*, J. Number Theory **90** (2001), 304–315.

[6] A. Beauville. *Determinental hypersurfaces*, Mich. Math. J. **48** (2000), 39–64.

[7] J.-C. Belfiore, G. Rekaya. *Quaternionic lattices for space-time coding.* ITW Proceedings (2003), 267–270.

[8] J.-C. Belfiore, G. Rekaya, E. Viterbo. *The Golden Code: A* 2×2 *full-rate space-time code with nonvanishing determinants.* IEEE Trans. Inform. Theory **51**, No. 4 (2005), 1432–1436.

[9] G. Berhuy, F. Oggier. *On the Existence of Perfect Space-Time Codes*, preprint.

[10] M. Bilioti, V. Jha, N. L. Larson. "Foundations of Translation Planes," Marcel Dekker, New York, 2001.

[11] K. R. Coombes and D. R. Grant. *On heterogeneous spaces.* J. London. Math. Soc. **40** (1989), 385–397.

[12] J. E. Cremona. "Elliptic curve Data." http://www.maths.nott.ac.uk/personal/jec/ftp/data/INDEX.html.

[13] M. O. Damen, K. Abed-Meraim, J. C. Belfiore. *Diagonal algebraic space-time block codes.* IEEE Trans. Inform. Theory **48** (2002), 628–636.

[14] P. Dayal, M. K. Varanasi. *Maximal diversity algebraic space-time codes with low peak-to-mean power ratio.* IEEE Trans. Inf. Theory **51** No. 5 (2005), 1691–1708.

[15] P. Dayal, M. K. Varanasi. *An Optimal Two Transmit Antenna Space-Time Code and its Stacked Extensions.* Proc. Asilomar Conf. on Signals, Systems and Computers, Monterey, CA, Nov. 2003.

[16] P. Dayal, M. K. Varanasi. *An optimal two transmit antenna space-time code and its stacked extensions.* IEEE Trans. Inform. Theory **51**, No. 12 (2005), 4348–4355.

[17] A. Deajim. "On nonassociative division algebras arising from elliptic curves," Ph. D. thesis, University of Colorado at Boulder, 2006.

[18] A. Deajim, D. Grant. *On the classification of 3-dimensional non-associative division algebras over local fields*, in preparation.

[19] L. E. Dickson. *Linear algebras in which division is always uniquely possible.* Trans. Amer. Math. Soc. **7** (1906), 370–390.

[20] L. E. Dickson. *On triple algebras and ternary cubic forms.* Bull. Amer. Math. Soc. **14** (1908), 160–168.

[21] P. Elia, B. A. Sethuraman, P. V. Kumar. *Perfect space-time codes with minimum and non-minimum delay for any number of antennas.* International Conference on Wireless Networks, Communications and Mobile Computing, (2005), 722–727.

[22] D. Grant, M. K. Varanasi. *The Equivalence of Space-Time Codes and Codes defined over Finite Fields and Galois Rings,* preprint.

[23] D. Grant, M. K. Varanasi. *Space-time codes constructed from non-associative division algebras,* in preparation.

[24] I. Kaplansky. *Three-dimensional division algebras.* J. Algebra **40** (1976), 384–391.

[25] I. Kaplansky. *Three-dimensional division algebras. II.* Houston J. Math. **1**, No. 1 (1975), 63–79.

[26] G. Menichetti. *On a Kaplansky conjecture concerning three-dimensional division algebras over a finite field.* J. Algebra **47**, No. 2 (1977), 400–410.

[27] G. Menichetti. *n-dimensional algebras over a field with a cyclic extension of degree n.* Geometrica Dedicata **63** (1996), 69–94.

[28] J. S. Milne. *Abelian varieties,* in "Arithmetic Geometry," G. Cornell and J. Silverman, eds., Springer-Verlag, New York, 1986.

[29] K. Ng. *The classification of* $(3,3,3)$ *trilinear forms.* J. Reine Angew. Math. **468** (1995), 49–75.

[30] F. Oggier, G. Rekaya, J.-C. Belfiore, E. Viterbo. *Perfect Space Time Block Codes.* IEEE Trans. Inf. Theory. **52** (2006), 3885–3902.

[31] F. Oggier, E. Viterbo. *Algebraic number theory and code design for Rayleigh fading channels.* Foundations and Trends in Communications and Information Theory, vol. 1 (2004), 333-415.

[32] G. Rekaya, J.-C. Belfiore, E. Viterbo. *Algebraic* $3 \times 3, 4 \times 4$ *and* 6×6 *Space-Time Codes with Non-Vanishing Determinants.* Proc. of Intern. Symp. on Inform. Theory and its Applications, ISITA (2004), 325–329.

[33] V. Shashidhar, B. Sundar Rajan, A. Sethuraman. *Information-Lossless STBCs from Crossed-Product Algebras* Proc. ISIT (2004), 126–126.

[34] A. Sethuraman, V. Shashidhar, B. Sundar Rajan. *Full-diversity, high-rate space-time block codes from division algebras.* IEEE Trans. Inf. Theory. **49** (2003), 2596–2616.

[35] A. Shokrollahi, B. Hassibi, B. M. Hochwald, W. Sweldens. *Representation theory for high-rate multiple-antenna code design.* IEEE Trans. Inf. Theory, **47**, No.6. (2001), 2335–2367.

[36] J. H. Silverman. "The arithmetic of elliptic curves," Grad. Texts in Math., Springer-Verlag, New York, 1986.

[37] T. Kiran, B. Sundar Rajan. *High-rate Full-rank Space-Time Block Codes from Cayley Algebra.* Proc. of Int. Conf. on Signal Processing and Comm. (SPCOM 2004).

[38] V. Tarokh, N. Seshadri, A. R. Calderbank. *Space-time block codes for high data rate wireless communications.* IEEE Trans. Inf. Theory, **44**, No. 2 (1998) 744–765.

[39] J. H. van Lindt. "Introduction to coding theory," 2nd. ed., Grad. Texts in Math., Springer-Verlag, Berlin, 1999.

[40] G. P. Wene. *Division algebras three-dimensional over algebraic number fields.* Lecture notes in pure and applied math. **190**, 413–420, Dekker, New York, 1997.

Department of Mathematics, College of Sciences, King Khalid University, P.O. Box 9004, Abha, Saudi Arabia

E-mail address: deajim@kku.edu.sa

Department of Mathematics, University of Colorado at Boulder, Boulder, Colorado 80309-0395 USA

E-mail address: grant@colorado.edu