Fall 2011 Western Algebraic Geometry Symposium

Codes, Non-associative Division Algebras, and Arithmetic Geometry

Space Time Codes

Suppose we want to send an encoded message from n_t transmit antennas to n_r receiver antennas. Because of errors in transmission, to do so reliably we need to add redundancy to our message. However, we would like to do so using as little redundancy as possible to guarantee correct decoding of the message. At each of T points in time, each transmit antenna sends a symbol(a complex number) so we can view the message as a matrix in $\mathcal{M}_{n_t \times T}(\mathbb{C})$. In fact, the codes of most interest will be linear subspaces $C \subset \mathcal{M}_{n_t \times T}(K)$, with K a number field. To minimize redundancy, the best codes will have the property that rank $A - B$ is maximal $\forall A \neq B \in C$, which we'll call the *rank condition*. Lastly, we are most interested in codes of maximal dimension satisfying the rank condition. As we will happily see in Lemma 1, when $n_t = T$, that the max dimension is T, and the study of classifying such space time codes corresponds to classifying non-associative division algebras over K.

Non-Associative Division Algebras, NADAs

- Let V be an n-dimensional K vector space with a bilinear operation $* : V \times V \to V$ that is not assumed to be associative. We call $A = (V, *)$ a non-associative algebra.
- For all $x, y \in A$, if the maps $L_x, R_y : A \to A$ with $L_x(a) = x * a$ and $R_y(a) = a * y$ are injective, then we say that A is a *division algebra*.
- Let β be a basis for V. If $a * b = c$, then we can define
$$[c]_\beta = (\sum_{i=1}^{n} a_i M_i)[b]_\beta$$
for some matrices M_i when a_i is the i^{th} entry of $[a]_\beta$. Now let x_i be indeterminants and form $M = \sum_{i=1}^{n} x_i M_i$. We call M the *left representation* of A with respect to β.
- Some examples of NADAs are jordan algebras, power associative algebras, and alternative algebras. One such class are the *twisted fields* introduced by Albert, generalizing the work of Dickson, in turn generalized by Menichetti, and most recently generalized by Deajim. Let L/K be a galois extension with $\alpha \in L$ and $N_{L/K}(\alpha) \neq 1$. Let $a, b \in L$ and define $*$ for twisted fields to be $a * b = ab - \alpha a^\sigma b^\tau$ with fixed $\sigma, \tau \in \mathrm{Gal}(L/K)$.

Main Lemmas

A form F over K is *K-anisotropic* is there are no non-trivial K-solutions to F.

Lemma 1. *Let k be a field and $z_1, \dots, z_n$ be indeterminants.*

(1) If V is an $n-$dimensional subspace of $\mathcal{M}_{n \times n}(k)$ with basis P_i, $1 \leq i \leq n$, then V is a maximal non-singular 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 $P_i \in \mathcal{M}_{n \times n}(k)$, $1 \leq i \leq n$, 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.

Thus, we see the central connection between space time codes, non-associative division algebras, and anisotropic forms of a certain degree.

Lemma 2. *(Room/Beauville) Let K be a field and $X = V(F)$ be a degree 4 surface in $\mathbb{P}^3(K)$. Then X is determinantal if and only if X contains a degree 6 arithmetic genus 3 curve which is defined over K.*

Main Question

Question. *Given a number field K. What are all 4-dimensional non-associative division algebras over K?*

Elliptic Curves and Divisors

- An *elliptic curve* E is an irreducible curve of genus one with a fixed base point $\mathcal{O}$. If both are defined over a field K, then we write E/K. Throughout we will assume K is perfect.
- Suppose $F \in K[x, y, z, w]$ is a form of degree 4 and F factors into 2 absolutely irreducible quadrics over $L = K(\sqrt{d})$. Let $\sigma_d : \sqrt{d} \to -\sqrt{d}$ generate $\mathrm{Gal}(L/K)$ so we have $F = aQQ^{\sigma_d}$ with $a \in K$. Let $\mathcal{H} = V(Q, Q^{\sigma_d}) \subset \mathbb{P}^3$. Note, $\mathcal{H}$ is defined over K. We can calculate the Hilbert polynomial of $I(\mathcal{H}) = (Q, Q^{\sigma_d})$ and we see that $\deg \mathcal{H} = 4$ and the arithmetic genus of the curve $\mathcal{H} = 1$.
- Thus, if $\mathcal{H}$ if geometrically irreducible, it has a jacobian $E = \mathrm{Jac}(\mathcal{H})$ which is an elliptic curve defined over K.
- Recall, a Weil divisor on a curve $\mathcal{H}$ is a formal sum $D = \sum_{P \in \mathcal{H}} n_P P$ over geometric points of $\mathcal{H}$, where $n_P \in \mathbb{Z}$ and $n_P = 0$ for all but finitely many P. The degree of $D = \sum n_P$. We write $D_1 \sim D_2$ if D_1 and D_2 are linearly equivalent.
- We say that a divisor D is defined over K and write $D \in \mathrm{Div}_K(\mathcal{H})$ if $D^\tau = D$ for all $\tau \in \mathrm{Gal}(\bar{K}/K)$. Let $\mathrm{Div}^n_K(\mathcal{H})$ be the set of degree n divisors defined over K on $\mathcal{H}$.
- There are two groups we need to consider related to the arithmetic of E/K. The *Weil-Chatelet* group $WC(E/K)$ consists of homogeneous spaces $\mathcal{H}$ of E(curves defined over K, isomorphic to E over $\bar{K}$) modulo a relations that comes from identifying $\mathcal{H}$ with a cocycle class in $H^1(\mathrm{Gal}(\bar{K}/K), E)$. The *Tate-Shafarevich* group $Ш(E/K)$ is the subgroup of $WC(E/K)$ which consists of curves which have points in every completion of K.
- We are interested in curves $\mathcal{H} \in WC(E/K)$ with no K-points, so either there is a completion $K_\mathfrak{p}$ of K with $\mathcal{H}(K_\mathfrak{p}) = \emptyset$(including $K_\infty = \mathbb{R}$), or $\mathcal{H}$ is a non-trivial element of $Ш(E/K)$.
- With $\mathcal{H}$ as above, we will find Q, Q^{σ_d} such that $I(\mathcal{H}) = (Q, Q^{\sigma_d})$ and there is a K-rational point on $Q \cup Q^{\sigma_d} \iff \mathcal{H}(K) \neq \emptyset$. If $\mathcal{H}$ has solutions in every completion of K, then theory says that such a Q, Q^σ exist if and only if $\mathcal{H}$ is of order 2 or 4 in $Ш(E/K)$.

Main Theorem

Theorem. *Let $F \in K[x, y, z, w]$ be a K-irreducible form of degree 4, and suppose that $F = QQ^{\sigma_d}$ over $K(\sqrt{d})$ for some $d \in K$, σ_d the non-trivial element in $\mathrm{Gal}(K(\sqrt{d})/K)$ and that Q, Q^{σ_d} are absolutely irreducible. Furthermore, let $\mathcal{H} = V(Q, Q^{\sigma_d})$, and suppose $\mathcal{H}$ is geometrically irreducible. Then F is determinantal if and only if there exists a divisor $D \in \mathrm{Div}^4_K(\mathcal{H})$ with $D = D_1 + D_1^\sigma$, $D_1, D_1^\sigma \in \mathrm{Div}^2_{K(\sqrt{d})}(\mathcal{H})$, $D_1 \not\sim D_1^\sigma$, and D is not a hyperplane section of $\mathcal{H}$.*

Building Examples of New Determinantal Anisotropic Quartics

One way to find $\mathcal{H}$ with the properties called for in the theorem is to start with an elliptic curve E/K with a K-rational 4-torsion point P. We let $E'' = E/ < 2P >$ and $E' = E/ < P >$. Note this means that the bottom rows of the diagrams are isogenies. We then seek $\mathcal{H} \in Ш(E/K)$ of order 2 or 4(so $\mathcal{H}(K) = \emptyset$). If $\mathcal{H}$ has order 2 in $Ш$ it is isomorphic to E over some $K(\sqrt{d})$ call it C_d, and then we proceed as follows(see diagram on left):

$$\begin{tikzcd} C_d \arrow[d] \arrow[dr] & & \\ E \arrow[r] & E'' \arrow[r] & E' \end{tikzcd} \qquad \begin{tikzcd} \mathcal{H} \arrow[r] \arrow[d] & C_{d,\tau} \arrow[d] \arrow[dr] & \\ E \arrow[r] & E'' \arrow[r] & E' \end{tikzcd}$$

(1) Find $D \in \mathrm{Div}^4_K(C_d)$ such that D is not a hyperplane section, $D = D_1 + D_1^\sigma$ and $D_1 \not\sim D_1^\sigma$. We do so by pulling back conjugate points on E'. Note such points exist when $E'(K(\sqrt{d})$ contains a non- K-rational point.

(2) Let L be the line through the two points in Supp D_1. Let $\mathfrak{C} = C_d \cup L \cup L^\sigma$. This is our degree 6 genus 3 curve defined over K.

(3) We want to find a basis for $H^0(V(F), I(\mathfrak{C}) \otimes \mathcal{O}(3))$. Note, this will be 4 quaternary cubic forms. We then do a free resolution on the ideal generated by these 4 forms. This gives us a 3×4 matrix $\tilde{M}$, whose entries are quaternary linear forms defined over K.

(4) The general theory tells us that we can adjoin a variable fourth row of linear forms to $\tilde{M}$ to form M, where $\det M = G$, and G is any quartic surface containing $\mathfrak{C}$. Thus we can solve for a fourth row such that we have $\det M = QQ^\sigma$, and M will be a NADA.

(5) We are currently working on the above algorithm for $\mathcal{H} \in Ш(E/K)$ of order 4 which, can be studied via the diagram on the right.

Example

With the setup above we have
$$E : y^2 = x^3 + 102x^2 + x$$
which has 4-torsion $(-1, 10)$. We then find $C_d \in Ш(E/K) - 0$ with
$C_2 : w^2 = 2 - 51Z^2 + 325Z^4 = (-1 + 13Z^2)(-2 + 25Z^2)$.
Note, it is non-trivial to show that C_2 is a non-trivial element of $Ш$. From this homogeneous space we build a new NADA

$$M = \begin{pmatrix} -y & x + 103/4y & 2574w - 103/2z & 26w \\ 1/2w - z & -1/2w & x & -10613/16x - 103/16y \\ -2w & 52w - z & y & -103/4x - 1/4y \\ \frac{16}{56843125}x + (\frac{416}{56843125} - \frac{1}{26})y & (\frac{-416}{56843125} + \frac{1}{26})x + (\frac{-10716}{56843125} + \frac{103}{104})y & (\frac{21432}{56843125} - \frac{103}{52})z + (\frac{-416}{22075} + 99)w & \frac{-2}{56843125}z + w \end{pmatrix}$$

Steve Limburg (University of Colorado at Boulder)