UPPSALA
UNIVERSITET

U.U.D.M. Project Report 2016:9

On division algebras of dimension 2^n admitting C_2^n as a subgroup of their automorphism group

Gustav Hammarhjelm

Examensarbete i matematik, 30 hp
Handledare: Ernst Dieterich
Examinator: Magnus Jacobsson
Juni 2016

Department of Mathematics
Uppsala University

On division algebras of dimension 2^n admitting C_2^n as a subgroup of their automorphism group

Gustav Hammarhjelm

June 7, 2016

Abstract

In this document we study division algebras, not assumed to be associative, whose dimension is 2^n and whose automorphism group admits a subgroup isomorphic to C_2^n. We call these algebras C_2^n-division algebras and we show that they are ubiquitous among all division algebras. Given a field k of characteristic not 2, we show that every C_2^n-division algebra is regular when viewed as a $k[C_2^n]$-module.

In [6], the groupoid structure of $\mathcal{D}_4^{1V}(k)$, the category of all unital C_2^2-division algebras whose right nucleus is non-trivial, is determined. Using these results, we investigate the full subcategories $\mathcal{F}_4^{1V}(l/\mathbb{Q})$, $\mathcal{S}_4^{1V}(l/\mathbb{Q})$, $\mathcal{N}_4^{1V}(l/\mathbb{Q})$ of $\mathcal{D}_4^{1V}(\mathbb{Q})$ formed by all fields, central skew fields and non-associative algebras, respectively, such that every object contains a subfield n isomorphic to l which is also a $k[C_2^2]$-submodule, where l ranges through a classifying list of the two-dimensional field extensions of $\mathbb{Q}$. For each l, we classify $\mathcal{F}_4^{1V}(l/\mathbb{Q})$, we find a list of central skew fields that exhausts $\mathcal{S}_4^{1V}(l/\mathbb{Q})$ and we construct a three-parameter family of non-associative algebras in $\mathcal{N}_4^{1V}(l/\mathbb{Q})$. We also classify $\mathcal{S}_4^{1V}(\mathbb{Q}(i)/\mathbb{Q})$ and we show that the central skew fields of $\mathcal{D}_4^{1V}(k)$ are the four-dimensional Hurwitz division algebras over k.

Contents

Notation and conventions

The following notation will be used throughout this document. The symbol $\mathbb{Z}$ denotes the set of integers and we set $\mathbb{N} = \{n \in \mathbb{Z} \mid n \geq 0\}$. For $n \in \mathbb{N} \setminus \{0\}$ we set $\underline{n} = \{m \in \mathbb{N} \mid 1 \leq m \leq n\}$. For any unital ring or algebra R we let R^* denote the set of invertible elements of R and $R_{\mathrm{sq}} = \{r^2 \mid r \in R\}$. For a category C we write $c \in C$ to express "c is an object of C".

1 Introduction

In this document we study a certain kind of division algebras, called C_2^n-division algebras and which are defined below. Division algebras are algebraic structures that admit an invertible multiplication which is compatible with addition, more precisely:

Definition 1.1. Let k be a field. A *k-algebra* A is a vector space over k equipped with a bilinear map $m : A \times A \longrightarrow A, (a, b) \mapsto ab$, called *multiplication*. The algebra A is said to be

(i) a *division algebra* if for all $a \in A \setminus \{0\}$ the linear maps $R_a : A \longrightarrow A,\ x \mapsto xa$ and $L_a : A \longrightarrow A,\ x \mapsto ax$ are *bijective*,

(ii) *unital* with *unity* e if there is $e \in A$ with $ea = a = ae$ for all $a \in A$,

(iii) *associative* if $a(bc) = (ab)c$ for all $a, b, c \in A$,

(iv) *commutative* if $ab = ba$ for all $a, b \in A$,

(v) *finite-dimensional* if A is finite-dimensional as a vector space over k.

Associative algebras are rings, whose ring structure is compatible with the structure of a vector space, but associativity is not assumed of an algebra in general! It is possible to carry out "division" in a division algebra A - for instance if $ab = ac$ where $a \in A \setminus \{0\}$ then $b = c$ since $ab = L_a(b) = L_a(c) = ac$ by applying the above definition, i.e. we may "divide through" by a.

Division algebras have been important in the history of mathematics. In trying to equip $\mathbb{R}^3$ with a "reasonable" multiplication Hamilton discovered the quaternions, which is a four-dimensional division algebra over the real numbers. Thereafter, people have been interested in understanding division algebras - more precisely, to find out more about their structural properties. A fascinating fact is that the only possible dimensions of a finite dimensional real division algebra are 1,2,4 and 8 [7]. But even division algebras of the same finite dimension over the same field may look structurally different, i.e. they might be *non-isomorphic*. To determine whether or not algebras are strucutrally different we need the notion of an algebra morphism.

Definition 1.2. Let k be a field and let A, B be k-algebras. A k-linear map $f : A \longrightarrow B$ is said to be an *algebra morphism* if $f(ab) = f(a)f(b)$ holds for all $a, b \in A$, i.e. f respects multiplication.

We say that a map $f : A \longrightarrow B$ is an *algebra isomorphism* if f is a bijective algebra morphism.

If A, B are k-algebras and there is an isomorphism $f : A \longrightarrow B$ we say that A, B are *isomorphic* and write $A \cong B$.

We let $\mathrm{Aut}_k(A) = \mathrm{Aut}(A) = \{f : A \longrightarrow A \mid f \text{ is an algebra isomorphism}\}$.

Now, given a family of algebras, in particular, a category of division algebras an interesting problem is to *classify the category up to isomorphism*:

Definition 1.3. Let $\mathcal{A}$ be a category and let $\mathcal{A}/\cong$ be the class of isoclasses of $\mathcal{A}$, i.e. any two objects $A, B \in \mathcal{A}$ belong to the same isoclass if and only if they are isomorphic as objects of $\mathcal{A}$. An *explicitly given* collection $\mathcal{L}$ of objects of $\mathcal{A}$ is said to

(i) be *irredundant* if for $L_1, L_2 \in \mathcal{L}$ with $L_1 \cong L_2$ implies $L_1 = L_2$,

(ii) *exhaust* $\mathcal{A}$ if for every $A \in \mathcal{A}$ there is $L \in \mathcal{L}$ with $A \cong L$,

(iii) be a *classification*, or a *classifying list*, if $\mathcal{L}$ is both irredundant and exhausts $\mathcal{A}$.

A classification of a category, in the above sense, gives very strong insight into the structure of the objects in the category. Namely, one has an explicitly given list such that any given object in the category is isomorphic to precisely one object in the list, so one could say that one knows precisely what an algebra in the category may look like.

In this document, the objects of all considered categories will be division algebras and morphisms will be non-zero algebra morphisms. In particular, given a field k and a positive integer n we let $\mathcal{D}_n(k)$ be the category whose objects are formed by all n-dimensional division algebras over k.

That $\mathcal{L}$ is explicitly given may for instance mean that its objects can be constructed by an explicit construction depending on parameters from some explicitly given set; examples will be given later.

In understanding a category a classification could be very desirable, as stated above. However, given a category of algebras, the classification problem is very difficult and far from being understood in full generality. As of yet, not even the finite-dimensional real division algebras have been fully classified (however, a classification has been obtained in case of two-dimensional real division algebras, see [5]). In order to make progress on the classification problem of categories of division algebras one has to attack subproblems which lend themselves to progress. In this document, categories formed by so called C_2^n-division algebras will be studied:

Definition 1.4. Let $n \in \mathbb{N}$ and let k be a field. A 2^n-dimensional k-division algebra A is said to be a *C_2^n-division algebra* (over k) if there is an injective group morphism

$$\iota : C_2^n \hookrightarrow \mathrm{Aut}_k(A),$$

where C_2 is the cyclic group of order two. Equivalently, A is a C_2^n-division algebra if $\mathrm{Aut}_k(A)$ contains a subgroup isomorphic to C_2^n.

We will, in this document, investigate the properties of C_2^n-division algebras. First we show that they are ubiquitous among the division algebras. We then show that they are regular when viewed as $k[C_2^n]$-modules in case $\mathrm{char}\, k \neq 2$. We will also, given a field k with $\mathrm{char}\, k \neq 2$, study the category $\mathcal{D}_4^{1V}(k)$ whose objects are unital C_2^2-division algebras with non-trivial right nucleus[1], show that the central skew fields of this category are the four-dimensional Hurwitz division algebras over k and attack the classification problem of $\mathcal{D}_4^{1V}(k)$ in case $k = \mathbb{Q}$.

2 Ubiquity of C_2^n-division algebras

In this section it will be demonstrated that C_2^n-division algebras are ubiquitous in the class of all division algebras by providing an array of examples of such algebras.

[1] See Definition 2.11 below.

2.1 $\mathbb{R}$,$\mathbb{C}$, $\mathbb{H}$, $\mathbb{O}$ are C_2^n-division algebras

First of all, one could wonder if the classical examples of real division algebras, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{H}$, $\mathbb{O}$, that is, the real numbers, the complex numbers, the quaternions and the octonions, are C_2^n-division algebras for $n = 0$, $n = 1$, $n = 2$ and $n = 3$ respectively. This is indeed the case.

We have, for any field k, that k itself is a C_2^0-division algebra, since $\mathrm{Aut}_k(k)$ contains $\{id\} \cong C_2^0$. Therefore, in particular, we have the following.

Proposition 2.1. *$\mathbb{R}$ is a real C_2^0-division algebra.*

The complex numbers is a finite Galois extension of $\mathbb{R}$ of degree 2, hence the field automorphisms of $\mathbb{C}$ leaving $\mathbb{R}$ fixed has order two. Indeed, $\mathrm{Aut}_{\mathbb{R}}(\mathbb{C}) = \{\mathrm{id}, \sigma\}$ where $\sigma(x)$ denotes the complex conjugate of x. Since complex multiplication in $\mathbb{C}$ makes $\mathbb{C}$ a 2-dimensional $\mathbb{R}$-algebra the algebra automorphisms of $\mathbb{C}$ as a real $\mathbb{R}$-algebra is $\{\mathrm{id}, \sigma\} \cong C_2$. Hence we conclude:

Proposition 2.2. *$\mathbb{C}$ is a real C_2^1-division algebra.*

Moving on to $\mathbb{H}$, we recall its definition. It may be described as the real vector space of dimension 4 with basis e, i, j, k endowed with a distributive and associative multiplication determined by the stipulations that e be the multiplicative identity of $\mathbb{H}$ and $i^2 = j^2 = k^2 = -e$, $ijk = -e$. This gives a multiplication table

	e	i	j	k
e	e	i	j	k
i	i	$-e$	k	$-j$
j	j	$-k$	$-e$	i
k	k	j	$-i$	$-e$

which determines the multiplication in $\mathbb{H}$. It can then be verified that (for instance by showing that $\mathbb{H}$ is isomorphic to a certain subring of $M_2(\mathbb{C})$, [7, see e.g. pp. 136]) $\mathbb{H}$ is an associative, unital four-dimensional real division algebra. Since, for instance, $ij = k \neq -k = ji$ the algebra $\mathbb{H}$ is non-commutative, hence a *proper skew field* (usually $\mathbb{H}$ is the standard example of a proper skew field).

Turning now to the group of automorphisms of $\mathbb{H}$ two ways to embed C_2^2 into $\mathrm{Aut}_{\mathbb{R}}(\mathbb{H})$ will be presented. The first one is the following.[2] Set $b_1 = i$, $b_2 = j$ and suppose that for $(c_1, c_2) \in C_2^2$ there is an algebra morphism $f_{c_1,c_2} : \mathbb{H} \longrightarrow \mathbb{H}$ with $f(b_m) = c_m b_m$ for $m \in \underline{2}$. Then $f(k) = f(ij) = f(i)f(j)$ is determined and hence f is uniquely determined. Then, we have that

$$\iota : C_2^2 \longrightarrow \mathrm{Aut}_{\mathbb{R}}(\mathbb{H}),\ (c_1, c_2) \mapsto f_{c_1,c_2}$$

is an injective group morphism. So it suffices to establish that f_{c_1,c_2} exists for each $(c_1, c_2) \in C_2^2$.

As shown in [7], for each $a \in \mathbb{H} \setminus \{0\}$ the map

$$\kappa_a : \mathbb{H} \longrightarrow \mathbb{H},\ x \mapsto axa^{-1}$$

[2] Ideas for this embedding, the embedding into $\mathbb{O}$ below and to consider isotopes of $\mathbb{O}$ from Seidon Alsaody, personal communication.

is an algebra automorphism of $\mathbb{H}$ and we have $\{\mathrm{id}, \kappa_i, \kappa_j, \kappa_k\} = \{f_{c_1,c_2} \mid (c_1, c_2) \in C_2^2\}$. The other way is to use the fact [11] that there is a group isomorphism $\mathrm{Aut}_{\mathbb{R}}(\mathbb{H}) \cong SO_3(\mathbb{R})$, where $SO_3(\mathbb{R}) = \{S \in M_3(\mathbb{R}) \mid S^T S = I_3, \det S = 1\}$. Then we have

$$C_2^2 \cong \left\{ \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} -1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{pmatrix}, \begin{pmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix} \right\} \leq SO_3(\mathbb{R})$$

and hence $C_2^2 \hookrightarrow \mathrm{Aut}_{\mathbb{R}}(\mathbb{H})$.

Summarizing, we have in two ways proved the following.

Proposition 2.3. *$\mathbb{H}$ is a real C_2^2-division algebra.*

We now turn to the last example from the classical ones, namely $\mathbb{O}$, the octonions. One way to look at $\mathbb{O}$ is to (as in [11, Chapter 1]) define $\mathbb{O} = \mathbb{H} \oplus \mathbb{H}$ and endow this eight-dimensional real vector space with an algebra multiplication as follows[3]

$$(a, b)(c, d) = (ac - \overline{d}b, da + b\overline{c}),$$

where for $x = a_1 e + a_2 i + a_3 j + a_4 k \in \mathbb{H}$ its conjugate $a_1 e - a_2 i - a_3 j - a_4 k$ is denoted $\overline{x}$. With this definition, $\mathbb{O}$ is in fact an eight-dimensional real division algebra with unity $E := (e, 0)$. The quaternion algebra $\mathbb{O}$ is neither associative nor commutative but it is quadratic and alternative.

Using the definition of conjugation of a quaternion we define the conjugate of an octonion $(a, b) \in \mathbb{O}$ by

$$\overline{(a, b)} = (\overline{a}, -b).$$

Then one can define the purely imaginary elements of $\mathbb{O}$ as $\mathfrak{I}(\mathbb{O}) = \{X \in \mathbb{O} \mid \overline{X} = -X\}$ and an inner product on $\mathbb{O}$ by $\langle X, Y \rangle = \overline{X}Y + \overline{Y}X$. A *Cayley triple* is a triple $(U, V, W) \in \mathfrak{I}(\mathbb{O})^3$ whose components satisfy the relations $U^2 = V^2 = W^2 = -(1, 0)$, $\langle U, V \rangle = 0$, $\langle U, W \rangle = 0$, $\langle V, W \rangle = 0$, $\langle UV, W \rangle = 0$. Denote the set of Cayley triples by $\mathbf{C}$. It can then be shown [11, 11.16] that for $(U, V, W) \in \mathbf{C}$ the elements

$$E, U, V, UV, W, UW, VW, (UV)W$$

constitute a basis of $\mathbb{O}$ as a real vector space and that for each pair $(U, V, W), (U', V', W') \in \mathbf{C}$ there is a unique algebra automorphism f of $\mathbb{O}$ with $f(U) = U'$, $f(V) = V'$, $f(W) = W'$. One often chooses the triple $(I_1, I_2, I_3) = ((i, 0), (j, 0), (0, 1)) \in \mathbf{C}$ to generate a basis of $\mathbb{O}$. Then, for each $(c_1, c_2, c_3) \in C_2^3$ we have $(c_1 I_1, c_2 I_2, c_3 I_3) \in \mathbf{C}$ and thus we can define f_{c_1,c_2,c_3} as the unique automorphism of $\mathbb{O}$ with $f(I_m) = c_m I_m$ for $m \in \underline{3}$. Then the map

$$\iota : C_2^3 \longrightarrow \mathrm{Aut}_{\mathbb{R}}(\mathbb{O}),\ (c_1, c_2, c_3) \mapsto f_{c_1,c_2,c_3}$$

is an injective group morphism. Thus we obtain:

Proposition 2.4. *$\mathbb{O}$ is a real C_2^3-division algebra.*

[3] Compare with multiplication of complex numbers by viewing a complex number $a + bi$ as a tuple (a, b) of real numbers. This construction is called the *Cayley-Dickson construction*, see e.g. [14].

2.2 Classification of real C_2-division algebras

In [5], the category $\mathcal{D}_2(\mathbb{R})$ of all two-dimensional real division algebras, is fully classified. In particular, it is shown that each $A \in \mathcal{D}_2(\mathbb{R})$ belongs to a subcategory equivalent to a groupoid arising from a group action of C_2 or D_3, which is shown to imply $\mathrm{Aut}(A) \in \{C_1, C_2, D_3\}$, where D_3 is the dihedral group with 6 elements, which of course contains C_2 as a subgroup.

We will here state the classification result of [5] and to do this we need the following definition, which gives the possibility to compare algebras by other means than algebra morphisms.

Definition 2.5. Let k be a field and A, B be k-algebras with $\dim_k A = \dim_k B$. A triple $(\alpha, \beta, \gamma) \in \mathrm{GL}(A, B)$ making the diagram

$$\begin{array}{ccc} A \times A & \longrightarrow & A \\ \downarrow{\scriptstyle \alpha\times\beta} & & \downarrow{\scriptstyle \gamma} \\ B \times B & \longrightarrow & B \end{array}$$

commute, where the horizontal arrows represent algebra multiplication in A and B, respectively, is said to be an *isotopy* of A and B and we say that B is an *isotope* of A.

Remark. Isotopy is a weaker notion than isomorphism in the sense that if $f : A \longrightarrow B$ is an isomorphism of k-algebras A, B, then (f, f, f) is an isotopy of A and B, i.e. isomorphic algebras are always isotopic.

If A is a division algebra over a field k and $\alpha, \beta \in \mathrm{GL}(A)$, then we can define an isotope $A_{\alpha,\beta}$ of A, which is equal to A as a vector space, but with multiplication $a \circ b := \alpha(a)\alpha(b)$.

The classification of $\mathcal{D}_2(\mathbb{R})$ is achieved through a study of isotopes of $\mathbb{C}$, namely, given $A, B \in \mathrm{GL}(\mathbb{R}^2)$ one defines a new division algebra $\mathbb{C}_{A,B} \in \mathcal{D}_2(\mathbb{R})$ with multiplication given by $x \circ y = (Ax)(By)$ where $x, y \in \mathbb{C}$ are viewed as columns of real numbers and complex multiplication accordingly.

For instance, it holds that $A \in \mathcal{D}_2(\mathbb{R})$ with $\mathrm{Aut}(A) = D_3$ implies $A \cong \mathbb{C}_{I,I}$ where $I = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$. To present the classification of objects of $\mathcal{D}_2(\mathbb{R})$ with automorphism group C_2 we reproduce notation from [5]. Let $\varphi : \mathbb{R}_{>0} \times \mathbb{R} \longrightarrow \mathcal{P} \subset M_2(\mathbb{R})$, $\binom{a}{b} \mapsto \begin{pmatrix} a & b \\ b & \frac{1+b^2}{a} \end{pmatrix}$ where $\mathcal{P}$ denotes the set of positive definite symmetric matrices with determinant 1. Let $\overline{\mathcal{U}}_0 = \{z \in \mathbb{C} \mid 0 < |z| \leq 1\}$. Define a map $\varrho : \overline{\mathcal{U}}_0 \longrightarrow \mathcal{P}$ by

$$\lambda e^{\alpha i} \mapsto \begin{pmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{pmatrix} \begin{pmatrix} \lambda & 0 \\ 0 & \lambda^{-1} \end{pmatrix} \begin{pmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{pmatrix}^T$$

for $0 < \lambda \leq 1$ and $0 \leq \alpha < 2\pi$. We now define the sets that will parametrize the objects of $\mathcal{D}_2(\mathbb{R})$ having automorphism group equal to C_2. Let $\mathcal{A}_2 = (\mathbb{R}_{>0} \times \mathbb{R}) \times (\mathbb{R}_{>0} \times \mathbb{R})$ and

$$\mathcal{B}_2 = (\{1\} \times (0,1)) \cup ((0,1) \times \{1\}) \cup ((0,1) \times (0,1)) \cup ((0,1) \times]0, i[)$$
$$\mathcal{B}_2' = (\{1\} \times]0, e^{\frac{\pi}{6}i}[) \cup (]0, e^{\frac{\pi}{6}i}[\times \{1\}) \cup (]0, e^{\frac{\pi}{6}i}[\times]0, e^{\frac{\pi}{6}i}[) \cup (]0, e^{\frac{\pi}{6}i}[\times]0, ie^{\frac{\pi}{6}i}[)$$

where, for a non-real number z we define $]0, z[= \{\lambda z \mid 0 < \lambda < 1\}$. With this notation we present the following result from [5].

Proposition 2.6. *The objects*

$$C := \{\mathbb{C}_{\varphi(\alpha)I^i,\varphi(\alpha)I^j} \mid \alpha \in \mathcal{A}, (i,j) \in \{(0,0),(0,1),(1,0)\} \cup \{\mathbb{C}_{I\varrho(\beta),I\varrho(\beta)} \mid \beta \in \mathcal{B}_2 \cup \mathcal{B}_2'\}$$

classify the objects of $\mathcal{D}_2(\mathbb{R})$ having automorphism group equal to C_2.

2.3 Isotopes of $\mathbb{O}$

We provide further examples of real C_2^3-division algebras as isotopes of $\mathbb{O}$. Set ${}^*\mathbb{O} = \mathbb{O}$ as vector spaces and define multiplication in ${}^*\mathbb{O}$ by $x \circ y = \overline{x}y$, where the right hand side is multiplication of octonions. Then, given $f \in \mathrm{Aut}_{\mathbb{R}}(\mathbb{O})$ one obtains an induced ${}^*f \in \mathrm{Aut}_{\mathbb{R}}({}^*\mathbb{O})$ by defining ${}^*f(x) = f(x)$. This is an automorphism since automorphisms of $\mathbb{O}$ satisfy $\overline{f(x)} = f(\overline{x})$ [11, Prop. 11.28]. Hence, $\mathrm{Aut}_{\mathbb{R}}(\mathbb{O}^*)$ contains a subgroup isomorphic to C_2^3, as $\mathrm{Aut}_{\mathbb{R}}(\mathbb{O})$ does. Similarly, one can proceed analogously by defining new algebras ${}^*\mathbb{O}^*$, $\mathbb{O}^*$ starting from $\mathbb{O}$ by defining $x \circ y = \overline{x}\,\overline{y}$, $x \circ y = x\overline{y}$ respectively and define f^*,${}^*f^*$ given $f \in \mathrm{Aut}_{\mathbb{R}}(\mathbb{O})$ accordingly.

2.4 Four-dimensional Hurwitz division algebras

In this section, we prove that certain Hurwitz algebras are C_2^2-division algebras. Hurwitz algebras are sometimes called unital composition algebras or, in dimension four, generalized quaternion algebras and have been studied extensively. To define a Hurwitz algebra, we need the notion of a quadratic form.

Definition 2.7. Let k be a field of characteristic not 2 and V a vector space over k. A map $n : V \longrightarrow k$ is said to be a *quadratic form* if

(i) $n(\alpha x) = \alpha^2 n(x)$ for all $\alpha \in k$ and $x \in H$,

(ii) $B(x,y) : V \times V \longrightarrow k$, $(x,y) \mapsto n(x+y) - n(x) - n(y)$ is a bilinear form.

(iii) A quadratic form q is said to be *non-degenerate* if its associated bilinear form B is non-degenerate.

Definition 2.8. Let k be a field of characteristic not 2. A *Hurwitz algebra over k* is a unital algebra H over k admitting a non-degenerate quadratic form $n : H \longrightarrow k$ such that $n(xy) = n(x)n(y)$ for all $x, y \in H$.

The following proposition shows that every four-dimensional Hurwitz algebra over fields of characteristic not 2 admits a basis similar to that of the real quaternions $\mathbb{H}$.

Proposition 2.9. *Let k be a field with* $\mathrm{char}\, k \neq 2$. *Let H be a four-dimensional Hurwitz algebra over k with identity element e. Then there is a k-basis $\{e, i, j, k\}$ of H and elements $\alpha, \beta \in k^*$ such that*

$$\begin{cases} i^2 = \alpha e, \\ j^2 = \beta e, \\ ij = k = -ji. \end{cases}$$

Proof. Let H be a four-dimensional Hurwitz algebra over k. By arguments on pp. 41 of [14] there is a basis $\{e, v_1, v_2, v_1v_2\}$ of H and elements $\mu, \nu \in k$ such that $1 + 4\mu \neq 0$ and $\nu \neq 0$ with $v_1^2 = v_1 + \mu e$ and $v_2^2 = \nu e$, $v_1v_2 = -v_2v_1$. Then $i := v_1 - 2^{-1}e$, $j := v_2$, $k := ij$, $\alpha := \mu + 4^{-1}$, $\beta := \nu$ satisfies the hypotheses of the proposition. □

Remark. Setting $k = \mathbb{R}$ and $\alpha = \beta = -1$ in $i^2 = \alpha e$, $j^2 = \beta e$, $ij = k = -ji$. gives the defining properties of the standard basis $\{e, i, j, k\}$ of $\mathbb{H}$, the quaternions. Furthermore, given a field k and $\alpha, \beta \in k^*$ one can define a four-dimensional unital associative algebra $A(\alpha, \beta)$ with basis $\{e, i, j, k\}$ satisfying $i^2 = \alpha e$, $j^2 = \beta e$, $ij = k = -ji$. These algebras generalize the quaternions. Since four-dimensional Hurwitz algebras over fields of characteristic not two admit bases satisfying the above they are sometimes called *generalized quaternion algebras*.

Proposition 2.9 allows us to conclude the following by generalizing arguments leading to 2.3.

Corollary 2.10. *Let k be a field with* $\operatorname{char} k \neq 2$. *Then every four-dimensional Hurwitz division algebra is a unital C_2^2-division algebra.*

Proof. Let H be a four-dimensional Hurwitz division algebra. By [14, Theorem 1], H is associative, and thus, for any $a \in H$ the map $\kappa_a : H \longrightarrow H,\ x \mapsto axa^{-1}$ is an algebra automorphism of H. Using Proposition 2.9, choose a basis $\{e, i, j, k\}$ and $\alpha, \beta \in k^*$ satisfying the conclusion of said proposition. We claim that then $V := \{\kappa_e, \kappa_i, \kappa_j, \kappa_k\} \subset \operatorname{Aut}(H)$ is a subgroup isomorphic to C_2^2.

First of all, we show that the automorphisms $\kappa_e, \kappa_i, \kappa_j, \kappa_k$ are all distinct. We have $\kappa_i(i) = -j, \kappa_j(i) = -i, \kappa_k(j) = -j$ and since $\operatorname{char} k \neq 2$ none of $\kappa_i, \kappa_j, \kappa_k$ equals the identity. Furthermore, $\kappa_i(i) = i, \kappa_j(i) = -i, \kappa_k(i) = -i$ show that $\kappa_i \neq \kappa_j$, $\kappa_i \neq \kappa_k$ and $\kappa_j(j) = j, \kappa_k(j) = -j$ show that $\kappa_j \neq \kappa_k$.

Since H is associative we have $k^2 = (ij)(ij) = i(ji)j = i(-ij)j = -i^2j^2 = -\alpha\beta$. Now, for $x \in H$

$$\kappa_k^2(x) = k(kxk^{-1})k^{-1} = k^2x(k^2)^{-1} = (-\alpha\beta e)x(\alpha\beta^{-1}e) = \alpha\beta\alpha\beta^{-1}x = x$$

so $\kappa_k^2 = \mathrm{id}$. Similarly, $\kappa_i^2 = \kappa_j^2 = \mathrm{id}$. It now suffices to show that $\kappa_i \circ \kappa_j = \kappa_j \circ \kappa_i \in V$. Indeed, for any $x \in H$ we have

$$\kappa_i(\kappa_j(x)) = i(jxj^{-1})i^{-1} = (ij)xj^{-1}i^{-1} = (ij)x(ij)^{-1} = kxk^{-1} = \kappa_k(x)$$

and

$$\kappa_j(\kappa_i(x)) = j(ixi^{-1})j^{-1} = (ji)x(ji)^{-1} = -(ij)x(-ij)^{-1} = kxk^{-1} = \kappa_k(x).$$

□

Remark. We could argue more generally as follows. Let A be an associative unital central k-algebra. For each $a \in A^*$ the map $\kappa_a : A \longrightarrow A,\ x \mapsto axa^{-1}$ is an automorphism, called an *inner automorphism*. The set $G_{A^*} := \{\kappa_a \mid a \in A^*\}$ is a subgroup of $\operatorname{Aut}(A)$ called the group of inner automorphisms of A. We have that $\iota : A^* \longrightarrow G_{A^*},\ a \mapsto \kappa_a$ is a surjective group morphism. We have $a \in \ker \iota$ if and only if $x = axa^{-1}$ for all $x \in A$ hence $a \in \ker \iota$ if and only if a is in the center of A, which is $\{\alpha e \mid \alpha \in k\}$. Hence $A^*/k^* \cong G_{A^*}$ where k^*, by abuse of notation, is the set $\{\alpha e \mid \alpha \in k^* = k \setminus \{0\}\}$.

If we now go back to the particular case of $A = H$ being a four-dimensional Hurwitz division algebra, which then is a central associative algebra, if we choose i, j as in Proposition 2.9 we have $e, i, j \in H^*$ and if E, I, J are the cosets of e, i, j in H^*/k^* respectively, we have $I^2 = J^2 = E$ and $IJ = JI$ so H^*/k^* contains a subgroup isomorphic to C_2^2 and hence, so does $\mathrm{Aut}(H)$.

2.5 The category $\mathcal{D}_4^{1V}(k)$

In this section, we introduce, given a field k with $\mathrm{char}\, k \neq 2$, a certain category $\mathcal{D}_4^{1V}(k)$ of C_2^2-division algebras, which have been studied extensively in [6]. To do this we need to introduce the following set, which measures associativity of an algebra.

Definition 2.11. Let k be a field and A a k-algebra. The set

$$N = N(A) = \{n \in A \mid (ab)n = a(bn)\}$$

is called *the right nucleus* of A.

Remark. Given an algebra A, not necessarily associative, N is an associative subalgebra of A. This justifies the interpretation of N as a measurement of associativity of A. The right nucleus of a unital algebra with unity e always contains $k \cdot e := \{\alpha e \mid \alpha \in k\} \cong k$ as a subalgebra. Therefore, we say that a unital algebra A has *non-trivial right nucleus* if $k \cdot e \subsetneq N$.

We are now ready to define the category $\mathcal{D}_4^{1V}(k)$.

Definition 2.12. Let k be a field with $\mathrm{char}\, k \neq 2$. We define $\mathcal{D}_4^{1V}(k)$ as the full subcategory of $\mathcal{D}_4(k)$ formed by the objects that are unital C_2^2-division algebras with non-trivial right nucleus.

The symbols $1, 4, \mathcal{D}, V$ in $\mathcal{D}_4^{1V}(k)$ illustrate the facts that the objects of the category are unital with non-trivial right nucleus, four-dimensional division algebras that admit Klein's four-group V as a subgroup of their automorphism group.

In [6], given a field k with $\mathrm{char}\, k \neq 2$, each object of $\mathcal{D}_4^{1V}(k)$ is *reduced* to a triple of elements in k^3. Conversely, given a triple from a set C in k^3 satisfying certain conditions, an algebra in $\mathcal{D}_4^{1V}(k)$ depending on the triple can be *constructed* such that this construction exhausts $\mathcal{D}_4^{1V}(k)$. In [6] the k-dependent, implicit conditions on C are presented as well as k-dependent conditions on when triples from C via the construction gives rise to isomorphic algebras. Given a field k, by understanding C, one can hope to arrive at classification results of $\mathcal{D}_4^{1V}(k)$.

The set C is well understood in case k is a finite field (see [2]) and in case k being an ordered field in which every positive element is a square (in particular $k = \mathbb{R}$, see [6]). In Section 5 of this document, we will attack the classification problem of $\mathcal{D}_4^{1V}(k)$ in case of $k = \mathbb{Q}$ and arrive at partial classification results. Since the paper [6] provides the foundations of this work we will give an overview of said document in Section 4, including details about the construction, reduction, the precise conditions on C as well as other important properties of the category $\mathcal{D}_4^{1V}(k)$.

3 Regularity of C_2^n-division algebras

In the previous section, we saw that there is an abundance of C_2^n-division algebras and we now proceed to present a property of such algebras.

Proposition 3.1. *Let n be a positive integer and k a field with* $\operatorname{char} k \neq 2$ *. Then any C_2^n-division algebra over k, viewed as a $k[C_2^n]$-module, is regular.*

Remark. Here $k[C_2^n]$ is the group algebra of C_2^n over k, which by definition, is the regular representation of C_2^n over k. Hence the statement of the proposition is that any C_2^n-division algebra satisfying the assumptions of the proposition is isomorphic to $k[C_2^n]$ when viewed as a $k[C_2^n]$-module. The proof uses representation theory and establishes a connection between representation theory and properties of division algebras.

This result is a generalization of Proposition 1.3 in [6], in which the case $n = 2$ is proved, with a proof similar to the one given below. A similar result is found in Lemma 2.4 (ii) of [1] in which the above proposition is proved for C_2^n-division algebras over finite fields of arbitrary characteristic and whence the idea of considering division algebras as modules over group algebras of subgroups of their automorphism group seems to originate.

Proof. We begin by investigating $k[C_2^n]$. Since $\operatorname{char} k \nmid 2^n = |C_2^n|$, Maschke's theorem [8] implies that $k[C_2^n]$ is semisimple as a $k[C_2^n]$-module, i.e. every submodule of $k[C_2^n]$ is a direct summand. Set $V = \mathbb{F}_2^n$. We will exhibit pairwise non-isomorphic one-dimensional submodules $S_v, v \in V$ of $k[C_2^n]$ so that we then must have $k[C_2^n] \cong \bigoplus_{v\in V} S_v$ since $|V| = |C_2^n|$.

To this end, let $B : V \times V \longrightarrow \mathbb{F}_2$ with $B(v, w) = v^T w$, so that B is a bilinear, non-degenerate and even symmetric bilinear form. Then, for each $v \in V$ the map $\sigma_v : V \to \mathbb{F}_2$, $\sigma_v(w) = B(v, w)$ is a group morphism. Take a group isomorphism $\varphi : V \longrightarrow C_2^n, w \mapsto \varphi_w$. Now, for $v \in V$ set $a_v := \sum_{u\in V}(-1)^{\sigma_v(u)}\varphi_u$ and $S_v := \operatorname{span}_k\{a_v\}$. Then S_v is a submodule of $k[C_2^n]$. Indeed, take any $\varphi_w \in C_2^n$, a basis element of $k[C_2^n]$, then

$$\varphi_w a_v = \sum_{u\in V}(-1)^{\sigma_v(u)}\varphi_{w+u} = \sum_{\tilde{u}\in V}(-1)^{\sigma_v(\tilde{u}+w)}\varphi_{\tilde{u}} = (-1)^{\sigma_v(w)}a_v$$

i.e. S_v is closed with respect to multiplication with any basis element of $k[C_2^n]$. We now consider each S_v as an irreducible representation of C_2^n by defining, for each $v \in V$ $\rho_v : C_2^n \longrightarrow \mathrm{GL}(S_v)$, $\varphi_w \mapsto \rho_v(\varphi_w)$ where $\rho_v(\varphi_w)(a_v) = \varphi_w a_v = (-1)^{\sigma_v(w)}a_v$. Thus, $\operatorname{Tr}\rho_v(\varphi_w) = (-1)^{\sigma_v(w)}$ and hence the character χ_v of S_v is $\chi_v(\varphi_w) = (-1)^{\sigma_v(w)}$. It now follows from injectivity of the map $v \mapsto \sigma_v$ and $\operatorname{char} k \neq 2$ that all characters χ_v, $v \in V$ are distinct. Since isomorphic representations have coinciding characters we deduce that all S_v are distinct and hence these submodules are the summands in the decomposition

$$k[C_2^n] = \bigoplus_{v\in V} S_v.$$

Let A be a C_2^n-division algebra over k and $\iota : C_2^n \hookrightarrow \mathrm{Aut}(A)$ an injective group morphism. Then, A has a $k[C_2^n]$-module structure induced by ι. By a corollary of Maschke's theorem [8, IX, Cor. 7.5] we have an isomorphism of $k[C_2^n]$-modules

$$A \cong \bigoplus_{v\in V} S_v^{n_v}$$

for uniquely determined integers $n_v \in \mathbb{N}$. The character of A is then $\chi_A = \sum_{v\in V} n_v\chi_v$ since the character of a direct sum is the sum of the characters. The aim is now to show that $\chi_A = \sum_{v\in V}\chi_v$ and that $\{\chi_v \mid v \in V\}$ forms a linearly independent set over k.

We have $\chi_A = \sum_{v\in V} n_v\chi_v$, but we can also calculate χ_A explicitly. Firstly, we have $\chi_A(\varphi_0) = 2^n = \dim_k A$. For $w \in V$, $w \neq 0$ we have $\mathrm{id} \neq \varphi_w \in C_2^n$. Set $\delta := \iota(\varphi_w)$. For $\lambda \in k$ define a subspace $E_\delta(\lambda) = \{x \in A \mid \delta(x) = \lambda x\}$. Since $x = \frac{1}{2}(x + \delta(x)) + \frac{1}{2}(x - \delta(x))$ with $\frac{1}{2}(x + \delta(x)) \in E_\delta(1)$, $\frac{1}{2}(x - \delta(x)) \in E_\delta(-1)$ we have the decomposition $A = E_\delta(1) \oplus E_\delta(-1)$ of A into k-subspaces. Since $\delta \neq \mathrm{id}$ there is $0 \neq a \in E_\delta(-1)$. We have $L_a(E_\delta(-1)) \subset E_\delta(1)$, $L_a(E_\delta(1)) \subset E_\delta(-1)$ and, since A is a division algebra, L_a is a bijective k-linear map and hence the spaces $E_\delta(1)$, $E_\delta(-1)$ have equal dimension. Thus, there is a basis of A such that the matrix of δ is diagonal with diagonal entries ± 1, equally many of each, and hence $\mathrm{Tr}[\delta] = 0$ in that basis, which implies $\chi_A(\varphi_w) = 0$. Thus $\chi_A(\varphi_w) = \begin{cases} 2^n \text{ if } w = 0, \\ 0 \text{ otherwise.} \end{cases}$

Now, since $k[C_2^n]$ is the regular representation of C_2^n we have $\sum_{v\in V}\chi_v(\varphi_w) = \begin{cases} 2^n \text{ if } w = 0, \\ 0 \text{ otherwise.} \end{cases}$ Therefore $\chi_A = \sum_{v\in V} n_v\chi_v = \sum_{v\in V}\chi_v$. Since all modules S_v are one-dimensional it follows from Theorem (30.12) of [3] that the set $\{\chi_v \mid v \in V\}$ is a linearly independent over k which implies that $n_v = 1$ in k for all $v \in V$. If $\mathrm{char}\, k = 0$ then this implies $n_v = 1$ for all $v \in V$ so we are done. If $\mathrm{char}\, k = p > 2$ then $n_v = 1 + a_v p$ where $a_v \in \mathbb{N}$. However, since $\sum_{v\in V} n_v = 2^n$ by dimension arguments we must have $a_v = 0$ for all $v \in V$ and the result follows. □

4 Overview of [6]

We will start by explaining the main goal of [6] which is to, given a field k with $\mathrm{char}\, k \neq 2$, describe the subcategory $\mathcal{D}_4^{1V}(k)$ of $\mathcal{D}_4(k)$ whose objects are the unital C_2^2-division algebras with non-trivial right nucleus.

The description relies on a *reduction* and a *construction* which are generalizations of procedures from [2], in which the setting is $k = \mathbb{F}_q$, a finite field with q elements, $2 \nmid q$. Through the reduction one associates to each object $A \in \mathcal{D}_4^{1V}(k)$ a triple $\underline{c} \in k^3$. Conversely, given a triple $\underline{c} \in C \subset k^3$ satisfying certain conditions, described thoroughly below, one can construct an object $A(\underline{c}) \in \mathcal{D}_4^{1V}(k)$. Proposition 3.1 is an important link in the chain of results resulting in the reduction and its importance will be accounted for in detail below.

Observe: Throughout the rest of this section, k will be a field with $\mathrm{char}\, k \neq 2$.

4.1 Reduction of objects in $\mathcal{D}_4^{1V}(k)$

We will begin by accounting for the reduction process in [6] starting with the following definition.

Definition 4.1. Let A be a unital k-algebra with unity 1. A *nuclear subfield* of A is a field l such that there is a filtration of subalgebras

$$1 \cdot k \subsetneq l \subset N \subset A,$$

of A, where N is the right nucleus of A. Henceforth, we will write k for $1 \cdot k \subset A$, since $k \cong 1 \cdot k$.

In [6] it is shown that any algebra $A \in \mathcal{D}_4^{1V}(k)$ possesses a *quadratic* nuclear subfield l i.e. a nuclear subfield of A whose dimension over k is 2. Then, since $\operatorname{char} k \neq 2$ the extension $k \subset l$ is Galois of degree 2. For a quadratic extension l of k and $x \in l$ we use $\overline{x}$ to denote the image of x under the non-trivial Galois automorphism of l over k. We can make A into a two-dimensional l-vector space by defining scalar multiplication via the given algebra multiplication in A, that is, $(a, x) \mapsto ax$ for $(a, x) \in A \times l$. Then, for any $v \in A \setminus l$ the set $\{1, v\}$ constitutes an l-basis of A.

Now, take $A \in \mathcal{D}_4^{1V}(k)$, choose a quadratic nuclear subfield l of A and take $v \in A \setminus l$ so that A is a two-dimensional l-vector space with basis $\{1, v\}$. Then define two functions $f_v, g_v : l^2 \longrightarrow l$ by $(x + vy)v = f_v(x, y) + vg_v(x, y)$ which are shown to be k-linear maps. If one knows f_v, g_v then one also knows the multiplication in A. Indeed, for $u = x + vy \in A$ the map L_u, left multiplication in A by u, is not only k-linear but even l-linear and the matrix of L_u in the basis $\{1, v\}$ is

$$\begin{pmatrix} x & f_v(x, y) \\ y & g_v(x, y) \end{pmatrix}.$$

By Artin's lemma, see [9, Lemma 2.33], there is an isomorphism of vector spaces $\varphi : l^4 \longrightarrow \operatorname{Hom}_k(l^2, l)$, $(a_1, a_2, a_3, a_4) \mapsto a_1x + a_2\overline{x} + a_3y + a_4\overline{y}$. In particular, since $f_v, g_v \in \operatorname{Hom}_k(l^2, l)$ these maps can be described using 8 constants from l. This is the first step in the reduction. The second step of the reduction needs an element $v \in A \setminus l$ satisfying the following.

Definition 4.2. Take $A \in \mathcal{D}_4^{1V}(k)$ and a quadratic nuclear subfield l of A. A vector $v \in A \setminus l$ is said to be *perfect* if there are $f_1, f_2 \in \operatorname{Aut}(A)$ such that

$$\begin{cases} f_1(x + yv) = x - vy \\ f_2(x + yv) = \overline{x} + v\overline{y} \end{cases}$$

for all $x, y \in l$.

With the existence of a perfect vector the 8 constants in l required to describe f_v, g_v reduce to 3 constants in k. This procedure is explained in detail in [6]. More precisely, it is shown that given a perfect vector v there exists a triple $\underline{c} = (c_1, c_2, c_3) \in k^3$ such that for $u = x + vy$ the matrix of L_u in the basis $\{1, v\}$ is

$$\begin{pmatrix} x & f_v(x, y) \\ y & g_v(x, y) \end{pmatrix} = \begin{pmatrix} x & c_2y + c_3\overline{y} \\ y & (1 - c_1)x + c_1\overline{x} \end{pmatrix}$$

and since A is a division algebra the associated map $q_{\underline{c}} : l^2 \longrightarrow l$, $q_{\underline{c}}(x, y) = \det(L_{x+vy}) = (1 - c_1)x^2 - c_2y^2 + c_1x\overline{x} - c_3y\overline{y}$ has no non-trivial zero.

The application that will be presented below proves the fact that for each $A \in \mathcal{D}_4^{1V}(k)$ there is a nuclear subfield l of A and a perfect vector $v \in A \setminus l$, which assures that the reduction always is successful. Pictorially, the reduction looks like

$$\begin{array}{ccc} k^3 & & \mathcal{D}_4^{1V}(k) \\ \cup & & \cup \\ \underline{c} & \leftsquigarrow & A \end{array}$$

where the squiggly arrow indicates that the reduction involves choices (of nuclear subfield and perfect vector).

4.2 Construction of objects in $\mathcal{D}_4^{1V}(k)$

We have seen the mechanics of the reduction of $A \in \mathcal{D}_4^{1V}(k)$ to a triple $\underline{c} \in k^3$ as carried out in [6]. We will now show how, in said paper, objects of $\mathcal{D}_4^{1V}(k)$ can be constructed from certain $\underline{c} \in k^3$.

Take a field k and a quadratic extension field l and set $\mathrm{Gal}(l : k) = \langle\sigma\rangle$, $\sigma(x) = \overline{x}$ for $x \in l$. For $\underline{c} \in k^3$ define $q_{\underline{c}} : l^2 \longrightarrow l$ by $(x, y) \mapsto (1 - c_1)x^2 - c_2y^2 + c_1x\overline{x} - c_3y\overline{y}$. Now set

$$C(l/k) = \{\underline{c} \in k^3 \mid q_{\underline{c}}^{-1}\{0\} = \{(0, 0)\}\}.$$

We call an element of $C(l/k)$ *an admissible triple with respect to* l. Then we define an algebra $A_l(\underline{c})$ which has underlying vector space l^2 and multiplication defined by

$$\begin{pmatrix} x \\ y \end{pmatrix}\begin{pmatrix} z \\ w \end{pmatrix} = \begin{pmatrix} x & c_2y + c_3\overline{y} \\ y & (1 - c_1)x + c_1\overline{x} \end{pmatrix}\begin{pmatrix} z \\ w \end{pmatrix}$$

for $x, y, z, w \in l$ (the right hand side is the usual product for l-matrices). It then holds that $\det(L_{\binom{x}{y}}) = q_{\underline{c}}(x, y) \neq 0$ unless $x = y = 0$ so $A_l(\underline{c})$ is a division algebra by construction.

Definition 4.3. Let k be a field with $\mathrm{char}\, k \neq 2$ and l a quadratic field extension of k. We define the full subcategory $\mathcal{D}_4^{1V}(l/k)$ of $\mathcal{D}_4^{1V}(k)$ by $A \in \mathcal{D}_4^{1V}(l/k)$ if and only if there is a subalgebra $n \subset N \subset A$ with $n \cong l$ and n is a $k[C_2^2]$-submodule of A.

In [6] it is shown that given a quadratic extension l of k the algebras $A_l(\underline{c})$, $\underline{c} \in C(l/k)$ exhausts $\mathcal{D}_4^{1V}(l/k)$. In a picture, we have

$$\begin{array}{ccc} C(l/k) & & \mathcal{D}_4^{1V}(l/k) \\ \cup & & \cup \\ \underline{c} & \longmapsto & A_l(\underline{c}) \end{array}$$

4.3 Decomposition and covering of $\mathcal{D}_4^{1V}(k)$

We now state two important results from [6] on the structure of the category $\mathcal{D}_4^{1V}(k)$.

Proposition 4.4. *The category $\mathcal{D}_4^{1V}(k)$ admits a decomposition*

$$\mathcal{D}_4^{1V}(k) = \mathcal{F}_4^{1V}(k) \amalg \mathcal{S}_4^{1V}(k) \amalg \mathcal{N}_4^{1V}(k)$$

into a coproduct of the full subcategories whose objects are formed by four-dimensional Galois extensions of k with Galois group C_2^2, skew fields with center k and non-associative algebras respectively.

Furtermore, given a classifying list $\mathcal{L}$ of the two-dimensional field extensions of k, we can cover the parts of the above decomposition according to

$$\mathcal{F}_4^{1V}(k) = \bigcup_{l \in \mathcal{L}} \mathcal{F}_4^{1V}(l/k),\ \mathcal{S}_4^{1V}(k) = \bigcup_{l \in \mathcal{L}} \mathcal{S}_4^{1V}(l/k),\ \mathcal{N}_4^{1V}(k) = \coprod_{l \in \mathcal{L}} \mathcal{N}_4^{1V}(l/k)$$

where, given $l \in \mathcal{L}$ we have $\mathcal{F}_4^{1V}(l/k) := \mathcal{D}_4^{1V}(l/k) \cap \mathcal{F}_4^{1V}(k)$, $\mathcal{S}_4^{1V}(l/k) := \mathcal{D}_4^{1V}(l/k) \cap \mathcal{S}_4^{1V}(k)$ and $\mathcal{N}_4^{1V}(l/k) := \mathcal{D}_4^{1V}(l/k) \cap \mathcal{N}_4^{1V}(k)$.

In particular, the proposition tells us that each object in $\mathcal{D}_4^{1V}(k)$ is either a Galois extension of k, a skew field with center k (a *central* skew field over k) or non-associative.

The following useful result [6] allows one to read off from an admissible triple in which of the three blocks of the above decomposition a constructed algebra will end up.

Proposition 4.5. *Let k be a field and l a two-dimensional field extension of k. Then, given $\underline{c} = (c_1, c_2, c_3) \in C(l/k)$ we have*

(i) $A_l(\underline{c}) \in \mathcal{F}_4^{1V}(l/k)$ *if and only if* $(c_1, c_3) = (0, 0)$.

(ii) $A_l(\underline{c}) \in \mathcal{S}_4^{1V}(l/k)$ *if and only if* $(c_1, c_2) = (1, 0)$.

In the previous section, we saw that given a quadratic field extension l of k, the family of algebras constructed from the admissible triples $C(l/k)$ with respect to l exhausts the category $\mathcal{D}_4^{1V}(l/k)$. From the covering in Proposition 4.4 we conclude that if $\mathcal{L}$ classifies the two-dimensional field extensions of k then $\bigcup_{l\in\mathcal{L}}\{A_l(\underline{c}) \mid \underline{c} \in C(l/k)\}$ exhausts $\mathcal{D}_4^{1V}(k)$ since $\{A_l(\underline{c}) \mid \underline{c} \in C(l/k)\}$ exhausts $\mathcal{D}_4^{1V}(l/k)$ as we saw in the previous section.

The challenge now is to, given a field k, find a classifying list $\mathcal{L}$ of quadratic field extensions of k and investigate the covering

$$\mathcal{D}_4^{1V}(k) = \left(\bigcup_{l\in\mathcal{L}} \mathcal{F}_4^{1V}(l/k)\right) \amalg \left(\bigcup_{l\in\mathcal{L}} \mathcal{S}_4^{1V}(l/k)\right) \amalg \left(\coprod_{l\in\mathcal{L}} \mathcal{N}_4^{1V}(l/k)\right)$$

with the aim of classification results. For instance, by finding $C(l/k)$ explicitly, one can construct $\mathcal{D}_4^{1V}(l/k)$ exhaustively, which is a step towards a classification of $\mathcal{D}_4^{1V}(l/k)$.

Example. Let $k = \mathbb{F}_q$ be the finite field of q elements, where q is the power of an odd prime. Since any two finite fields of a given order are isomorphic, the list $\mathcal{L} = \{\mathbb{F}_{q^2}\}$ classifies the two dimensional field extensions of $\mathbb{F}_q$. Since finite Galois extensions of a finite field have cyclic Galois groups and since finite skew fields are fields [9, Wedderburn's theorem] the decomposition in Proposition 4.4 becomes

$$\mathcal{D}_4^{1V}(\mathbb{F}_q) = \mathcal{N}_4^{1V}(\mathbb{F}_{q^2}/\mathbb{F}_q)$$

i.e. all unital C_2^2-division algebras over $\mathbb{F}_q$ with non-trivial right nucleus are non-associative. Now, the goal is to find $C(\mathbb{F}_{q^2}/\mathbb{F}_q)$ explicitly, which is done in [2].

In the above example, the classifying list $\mathcal{L}$ was as short as possible and some parts of the decomposition vanished. In general, the situation might be more complicated, for instance in case $k = \mathbb{Q}$ which we will investigate in Section 5 below.

4.4 General properties of $C(l/k)$

We reproduce the following result from [6].

Proposition 4.6. *Let k be a field with $\operatorname{char} k \neq 2$ and let l be a two-dimensional field extension. Then the following statements are true.*

(i) *For $c_2 \in k$ we have $(0, c_2, 0) \in C(l/k)$ if and only if $c_2 \notin l_{sq}$.*

(ii) *For $c_3 \in k$ we have $(1,0,c_3) \in C(l/k)$ if and only if $c_3 \notin \operatorname{im} n_{l/k}$ where $n_{l/k} : l \longrightarrow k,\ x \mapsto x\overline{x}$ is the norm of the field extension $k \subset l$.*

(iii) *Set $\underline{c} = (c_1,c_2,c_3), \underline{d} = (d_1,d_2,d_3)$. Then $A_l(\underline{c}) \cong A_l(\underline{d})$ if and only if there exists $x \in l$ such $(c_1,c_2,c_3) = (d_1, x^2d_2, n_{l/k}(x)d_3)$. If $A_l(\underline{c}) \cong A_l(\underline{d})$ we write $\underline{c} \sim \underline{d}$.*

For a group G let G° denote G with the identity element removed. If one can find an explicit transversal $\mathcal{T} \subset k^*$ of $(k^*/(l_{\mathrm{sq}} \cap k))^\circ$ (i.e. precisely one representative of each coset) then the family $A_l(0,t,0)$, $t \in \mathcal{T}$ is an irredundant list which exhausts $\mathcal{F}_4^{1V}(l/k)$, i.e. a classification is obtained.

Let $n_{l/k}(l^*)$ denote the image of l^* under $n_{l/k}$. This is a subgroup of k^* and if one finds an explicit transversal $\mathcal{T} \subset k^*$ of $(k^*/n_{l/k}(l^*))^\circ$ then the family $A_l(1,0,t)$, $t \in \mathcal{T}$ classifies $\mathcal{S}_4^{1V}(l/k)$.

4.5 An application of Proposition 3.1

The application appears as Lemma 2.4 in [6] and proves the required existence result of perfect vectors to allow the reduction process described in the previous subsection. The proposition below constitutes an elaborate version of the proof of this result and uses Proposition 3.1 in a crucial way.

Proposition 4.7 (Application)**.** *For every $A \in \mathcal{D}_4^{1V}(k)$ there exists a quadratic nuclear subfield $l \subset A$ and a perfect vector $v \in A \setminus l$.*

Proof. Take $A \in A \in \mathcal{D}_4^{1V}(k)$ and set $V = \mathbb{F}_2^2$. Find an isomorphism $\varphi : V \longrightarrow G,\ w \mapsto \varphi_w$ where G is a subgroup of A isomorphic to C_2^2. We show that A contains a quadratic nuclear subfield l which is at the same time a $k[C_2^2]$-submodule of A. For $w \in V$, $n \in N$, the right nucleus of A, and $a, b \in A$ we have

$$\varphi_w(\varphi_w(n)(ab)) = n\varphi_w(ab) = n(\varphi_w(a)\varphi_w(b)) = (n\varphi_w(a))\varphi_w(b) = \varphi_w((\varphi_w(n)a)b)$$

and since φ_w is an automorphism we get $\varphi_w(n)(ab) = (\varphi_w(n)a)b$ so $\varphi_w(n) \in N$, hence N is a $k[C_2^2]$-submodule of A. If A is non-associative then by Proposition 1.3 of [6] we have that N is two-dimensional and by [4, Theorem 1] even a field.

Now let $B : V \times V \longrightarrow \mathbb{F}_2,\ (v,w) \mapsto v^T w$ and define $\sigma_v : V \longrightarrow \mathbb{F}_2,\ \sigma_v(w) = B(v,w)$. Then, as in the proof of Proposition 3.1 we have $A \cong \bigoplus_{v \in V} S_v$ as $k[C_2^2]$-modules, where the character of S_v is given by $\chi_v(\varphi_w) = (-1)^{\sigma_v(w)}$. Let $A = \bigoplus_{v \in V} A_v$ where $S_v \cong A_v$. Now, $A_{(0,0)} \cong k$. Consider $l = A_{(0,0)} \oplus A_{(0,1)}$ which we claim to be a subfield of A if A is associative. We first show that l is a subalgebra. It suffices to show that for $x, y \in A_{(0,1)}$ we have $xy \in l$. We have that xy is fixed by all φ_w, $w \in V$ and hence $xy \in A_{(0,1)} \subset l$. If A is associative, then l is a two-dimensional associative division algebra hence a field by [4, Theorem 1].

Hence, in any case, there exists a quadratic nuclear subfield l of A which is a $k[C_2^2]$-submodule of A. The following table gives the action of φ_w on S_v, $v, w \in V$:

	$\varphi_{(0,0)}$	$\varphi_{(0,1)}$	$\varphi_{(1,0)}$	$\varphi_{(1,1)}$
$S_{(0,0)}$	1	1	1	1
$S_{(0,1)}$	1	−1	1	−1
$S_{(1,0)}$	1	1	−1	−1
$S_{(1,1)}$	1	−1	−1	1

If $l = A_{(0,0)} \oplus A_{(0,1)}$, as can be taken in the case of A being associative, then the restriction of $\varphi_{(0,1)}$ to l is the Galois automorphism of l over k. Furthermore, any non-zero $u \in A_{(1,1)}$ is a perfect vector since

$$\varphi_{(1,0)}(x + yu) = x - yu,$$
$$\varphi_{(1,1)}(x + yu) = \overline{x} + \overline{y}u$$

for all $x, y \in l$, where $\overline{x} = \varphi_{(0,1)}(x)$ (compare with Definition 4.2).

If A is non-associative then its right nucleus N is a two-dimensional subfield of A which is also a submodule of A. By [8, IX, Cor. 7.5] there is $v \in V\backslash\{0\}$ with $N = A_{(0,0)} \oplus A_v$. The case $v = (0, 1)$ was dealt with above, and the other cases can be treated by considering the above table in an analogous manner. □

5 Investigation of $\mathcal{D}_4^{1V}(\mathbb{Q})$

In this section we investigate the covering

$$\left(\bigcup_{l\in\mathcal{L}} \mathcal{F}_4^{1V}(l/k)\right) \amalg \left(\bigcup_{l\in\mathcal{L}} \mathcal{S}_4^{1V}(l/k)\right) \amalg \left(\coprod_{l\in\mathcal{L}} \mathcal{N}_4^{1V}(l/k)\right)$$

of $\mathcal{D}_4^{1V}(k)$ in case $k = \mathbb{Q}$, the rational numbers, where $\mathcal{L}$ is a classifying list of $\mathcal{F}_2(\mathbb{Q})$, the category of all two-dimensional field extensions of $\mathbb{Q}$ viewed as division algebras over $\mathbb{Q}$, to be found. The cases of k being an ordered field in which every positive elements is a square and k being a finite field with an odd number of elements have been studied in [6] but other instances of k have - until now - not been examined. The aim of the investigation in case $k = \mathbb{Q}$ is to understand as much as possible about the above covering of $\mathcal{D}_4^{1V}(\mathbb{Q})$ - with (partial) classification results in mind.

Throughout this section we let $\mathbb{P}$ denote the set of positive prime numbers and we set $\mathbb{P}_3 = \{p \in \mathbb{P} \mid p \equiv 3 \mod 4\}$. We will use that every non-zero rational number q admits a unique factorization, i.e. there is a unique function $n : \mathbb{P} \longrightarrow \mathbb{Z}$, $p \mapsto n_p$, with finite support such that $q = \pm \prod_{p\in\mathbb{P}} p^{n_p}$.

5.1 Classification of $\mathcal{F}_2(\mathbb{Q})$

Let $\mathcal{F}_2(\mathbb{Q})$ denote the category whose objects are two-dimensional field extensions of $\mathbb{Q}$ and whose morphisms are the following. Given $l, l' \in \mathcal{F}_2(\mathbb{Q})$ a morphism is a field morphism satisfying $f(x) = x$ for all $x \in \mathbb{Q}$. In particular, an automorphism in $\mathcal{F}_2(\mathbb{Q})$ is a Galois automorphism. We will in this section classify $\mathcal{F}_2(\mathbb{Q})$ by exhibiting a classifying list.

Lemma 5.1. *For every $l_1 \in \mathcal{F}_2(\mathbb{Q})$ there is $l_2 \in \mathcal{F}_2(\mathbb{Q})$ s.t. $l_1 \cong l_2$ and $l_2 \subset \mathbb{C}$.*

Proof. There is $a \in l_1$ s.t. $\mathbb{Q}(a) = l_1$. Let P_a be the minimal polynomial of a over $\mathbb{Q}$, i.e. P_a is an irreducible polynomial of degree 2. Let $b \in \mathbb{C}$ be a zero of P_a. Then we can take $l_2 = \mathbb{Q}(b)$ since both l_1, l_2 are isomorphic to $\mathbb{Q}[X]/(P_a)$ in $\mathcal{F}_2(\mathbb{Q})$. □

For an element $a \in \mathbb{Q}$ the symbol $\sqrt{a}$ denotes one of the roots of $X^2 - a$ in $\mathbb{C}$.

Lemma 5.2. *Take $a, b \in \mathbb{Q} \setminus \mathbb{Q}_{sq}$. Then $\mathbb{Q}(\sqrt{a}) \cong \mathbb{Q}(\sqrt{b})$ if and only if there exists $q \in \mathbb{Q}^*$ with $a = q^2 b$.*

Proof. Suppose there is $q \in \mathbb{Q}^*$ with $a = q^2 b$. Then $\mathbb{Q}(\sqrt{a}) = \mathbb{Q}(\sqrt{b})$ so the claim follows.

If $\mathbb{Q}(\sqrt{a}) \cong \mathbb{Q}(\sqrt{b})$, with an isomorphism φ, then $\varphi(\sqrt{a}) \in \mathbb{Q}(\sqrt{b})$ is a root of $X^2 - a$, hence $\sqrt{a} \in \mathbb{Q}(\sqrt{b})$. Similarly, $\sqrt{b} \in \mathbb{Q}(\sqrt{a})$ so $\mathbb{Q}(\sqrt{a}) = \mathbb{Q}(\sqrt{b})$. Hence, there exists $q_1, q_2 \in \mathbb{Q}$ with $q_2 \neq 0$ and $\sqrt{a} = q_1 + q_2\sqrt{b}$. If $q_1 \neq 0$, by squaring both sides, we get $\sqrt{b} \in \mathbb{Q}$, contradiction. Hence $\sqrt{a} = q_2\sqrt{b}$ which gives $a = q_2^2 b$. □

Proposition 5.3. *Let $Z = \{\pm \prod_{p\in F} p \mid \emptyset \neq F \subset \mathbb{P},\ |F| < \infty\} \cup \{-1\}$. Then the list*

$$\mathcal{L} := \{\mathbb{Q}(\sqrt{a}) \mid a \in Z\}$$

classifies $\mathcal{F}_2(\mathbb{Q})$.

Remark. Observe that $\mathbb{Q}^*_{\text{sq}} := \mathbb{Q}_{\text{sq}} \setminus \{0\}$ is a subgroup of $\mathbb{Q}^*$ and that Z is a transversal of the cosets in $(\mathbb{Q}^*/\mathbb{Q}^*_{\text{sq}})^\circ$. The symbol Z will be used to describe the set it describes in the above proposition for the remainder of this section.

Proof. By Lemma 5.1, it suffices to show that $\mathcal{L}$ is irredundant and exhausts the objects of $\mathcal{F}_2(\mathbb{Q})$ that are subsets of $\mathbb{C}$. That $\mathcal{L}$ is irredundant follows immediately from Lemma 5.2. By a modification of the primitive element theorem we can write $l = \mathbb{Q}(\sqrt{q})$ for some $q \in \mathbb{Q} \setminus \mathbb{Q}_{\text{sq}}$ for any $l \in \mathcal{F}_2(\mathbb{Q})$, where $l \subset \mathbb{C}$. Write $q = \pm \prod_{p\in\mathbb{P}} p^{n_p}$ and let $F = \{p \in \mathbb{P} \mid n_p \text{ odd}\}$. If $F = \emptyset$, then necessarily, $\mathbb{Q}(\sqrt{q}) = \mathbb{Q}(\sqrt{-1})$. Otherwise, set $a = \pm \prod_{p\in F} p$ so that $a \in Z$ and $\mathbb{Q}(\sqrt{q}) = \mathbb{Q}(\sqrt{a})$. □

Thus, the covering we are investigating can now be written as

$$\left(\bigcup_{a\in Z} \mathcal{F}_4^{1V}(\mathbb{Q}(\sqrt{a})/\mathbb{Q})\right) \amalg \left(\bigcup_{a\in Z} \mathcal{S}_4^{1V}(\mathbb{Q}(\sqrt{a})/\mathbb{Q})\right) \amalg \left(\coprod_{a\in Z} \mathcal{N}_4^{1V}(\mathbb{Q}(\sqrt{a})/\mathbb{Q})\right).$$

5.2 The set $C(\mathbb{Q}(\sqrt{a})/\mathbb{Q})$

We begin this section with a definition.

Definition 5.4. For $a \in Z$ set $C^a = C(\mathbb{Q}(\sqrt{a})/\mathbb{Q})$. Set $C^a_{1,0} = \{(c_1, c_2, c_3) \in C^a \mid (c_1, c_2) = (1, 0)\}$, $C^a_{0,0} = \{(c_1, c_2, c_3) \in C^a \mid (c_1, c_3) = (0, 0)\}$ and $C^a_* = C^a \setminus (C^a_{1,0} \cup C^a_{0,0})$.

Remark. By Proposition 4.5, for $\underline{c} = (c_1, c_2, c_3) \in \mathbb{Q}^3$, we have $A_{\mathbb{Q}(\sqrt{a})}(\underline{c}) \in \mathcal{S}_4^{1V}(\mathbb{Q}(\sqrt{a})/\mathbb{Q})$ if and only if $\underline{c} \in C^a_{1,0}$, $A_{\mathbb{Q}(\sqrt{a})}(\underline{c}) \in \mathcal{F}_4^{1V}(\mathbb{Q}(\sqrt{a})/\mathbb{Q})$ if and only if $\underline{c} \in C^a_{0,0}$ and $A_{\mathbb{Q}(\sqrt{a})}(\underline{c}) \in \mathcal{N}_4^{1V}(\mathbb{Q}(\sqrt{a})/\mathbb{Q})$ if and only if $\underline{c} \in C^a_*$.

5.3 On the category $\mathcal{F}_4^{1V}(\mathbb{Q}(\sqrt{a})/\mathbb{Q})$

The following proposition characterizes the elements of $C^a_{0,0}$.

Proposition 5.5. *Let $a \in Z$. For $c_2 \in \mathbb{Q}$ we have $(0, c_2, 0) \in C^a_{0,0}$ if and only if $c_2 \notin \mathbb{Q}_{sq} \cup a\mathbb{Q}_{sq}$.*

Proof. By Proposition 4.6 (i) we have $(0, c_2, 0) \in C^a_{0,0}$, where $c_2 \in \mathbb{Q}$, if and only if $c_2 \notin \mathbb{Q}(\sqrt{a})_{\mathrm{sq}}$. But $\mathbb{Q}(\sqrt{a})_{\mathrm{sq}} \cap \mathbb{Q} = \mathbb{Q}_{\mathrm{sq}} \cup a\mathbb{Q}_{\mathrm{sq}}$ whence the claim follows. □

If $\underline{c} = (0, c_2, 0) \in C^a_{0,0}$ then $A_{\mathbb{Q}(\sqrt{a})}(\underline{c})$ is a Galois extension of $\mathbb{Q}$ with Galois group C_2^2. Since C_2^2 has three subgroups of order two, $A_{\mathbb{Q}(\sqrt{a})}(\underline{c})$ will have three intermediate fields $\mathbb{Q} \subset l_i \leq A_{\mathbb{Q}(\sqrt{a})}(\underline{c})$, $i \in \underline{3}$, with $l_1 \cong \mathbb{Q}(\sqrt{a})$ by construction.

Recall that $A_{\mathbb{Q}(\sqrt{a})}(\underline{c})$ equals $\mathbb{Q}(\sqrt{a}) \times \mathbb{Q}(\sqrt{a})$ as vector space, with multiplication defined by

$$\begin{pmatrix} x \\ y \end{pmatrix}\begin{pmatrix} z \\ w \end{pmatrix} = \begin{pmatrix} x & c_2 y \\ y & x \end{pmatrix}\begin{pmatrix} z \\ w \end{pmatrix}$$

Considering the proof of Proposition 3.1 of [6] and taking into account that the only non-trivial automorphism of $\mathbb{Q}(\sqrt{a})$ fixing $\mathbb{Q}$ is determined by $\sqrt{a} \mapsto -\sqrt{a}$ we obtain the equalities of sets $l_2 = \mathbb{Q} \times \mathbb{Q}$, $l_3 = \mathbb{Q} \times \mathbb{Q}\sqrt{a}$.

In the next proposition we characterize l_2, l_3 up to isomorphism.

Proposition 5.6. *Take $a \in Z$ and $(0, c_2, 0) \in C^a_{0,0}$. Let l_2, l_3 be defined as in the previous paragraph. Then we have*

(i) $l_2 \cong \mathbb{Q}(\sqrt{c_2})$,

(ii) $l_3 \cong \mathbb{Q}(\sqrt{ac_2})$.

Proof. Using appropriate definitions one readily verifies:

(i) The map $l_2 = \mathbb{Q} \times \mathbb{Q} \longrightarrow \mathbb{Q}(\sqrt{c_2})$ given by $\begin{pmatrix} x \\ y \end{pmatrix} \mapsto x + y\sqrt{c_2}$ is an isomorphism.

(ii) The map $l_3 = \mathbb{Q} \times \mathbb{Q}\sqrt{a} \longrightarrow \mathbb{Q}(\sqrt{ac_2})$ given by $\begin{pmatrix} x \\ y\sqrt{a} \end{pmatrix} \mapsto x + y\sqrt{ac_2}$ is an isomorphism.

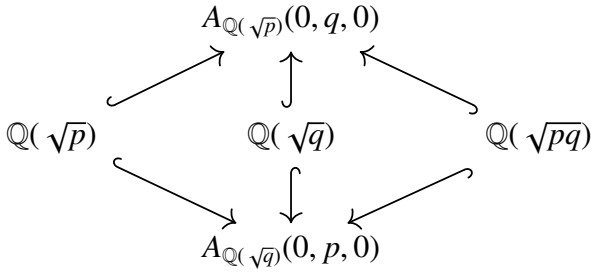
□

Remark. By Lemma 5.2 we infer that l_1, l_2, l_3 are pairwise non-isomorphic.

Furthermore, this result allows us to show examples of redundance in the covering

$$\mathcal{F}_4^{1V}(\mathbb{Q}) = \bigcup_{a \in Z} \mathcal{F}_4^{1V}(\mathbb{Q}(\sqrt{a})/\mathbb{Q}).$$

Namely, let $p, q \in Z$ be distinct prime numbers. Then we have $(0, q, 0) \in C^p_{0,0}$, $(0, p, 0) \in C^q_{0,0}$ and the following diagrams of fields and subfields



Thus, $A_{\mathbb{Q}(\sqrt{p})}(0, q, 0), A_{\mathbb{Q}(\sqrt{q})}(0, p, 0)$ are both four-dimensional field extensions of $\mathbb{Q}$ containing, up to isomorphism, the four-dimensional field extension $\mathbb{Q}(\sqrt{p}, \sqrt{q})$, hence they are isomorphic.

Proposition 5.7. *Set* $Z_{-1} = \{\prod_{p\in F} p \mid \emptyset \neq F \subset \mathbb{P}, |F| < \infty\}$. *Then, the fields* $A_{\mathbb{Q}(i)}(0, z, 0)$, $z \in Z_{-1}$ *classify* $\mathcal{F}_4^{1V}(\mathbb{Q}(i)/\mathbb{Q})$.

Proof. We first show that the list exhausts $\mathcal{F}_4^{1V}(\mathbb{Q}(i)/\mathbb{Q})$. Take $A \in \mathcal{F}_4^{1V}(\mathbb{Q}(i)/\mathbb{Q})$ and find $z \notin \pm\mathbb{Q}_{\text{sq}}$ such that $A \cong A_{\mathbb{Q}(i)}(0, z, 0)$. Write $z = \pm\prod_{p\in F_z} p^{n_p}$ where $F_z \subset \mathbb{P}$ is non-empty. Identify the set of primes $F_z' \subset F_z$ such that $p \in F_z'$ if and only if n_p is odd. Then, F_z' is non-empty since $z \notin \pm\mathbb{Q}_{\text{sq}}$. Then we have $(0, z, 0) \sim (0, \prod_{p\in F_z'} p, 0)$.

We now prove irredundance. Take F_1, F_2 non-empty, finite subsets of $\mathbb{P}$ and suppose $(0, z_1, 0) = (0, \prod_{p\in F_1} p, 0) \sim (0, \prod_{p\in F_2} p, 0) = (0, z_2, 0)$. If $F_1 \neq F_2$, then $z_1/z_2 = \prod_{p\in\mathbb{P}} p^{n_p}$ with some n_p odd. Thus we cannot have $z_1/z_2 \in \pm\mathbb{Q}_{\text{sq}}$, contradiction. □

Proposition 5.8. *Take* $a \in Z \setminus \{-1\}$. *Let* $D = \{d \mid (d \mid a) \wedge (|d| < \sqrt{|a|})\}$, $E = \{a' \in Z \mid \gcd(a', a) = 1\} \cup \{1\}$. *Then the fields* $A_{\mathbb{Q}(\sqrt{a})}(0, z, 0)$, $z \in Z_a := \{da' \mid d \in D, a' \in E\} \setminus \{1\}$ *classify* $\mathcal{F}_4^{1V}(\mathbb{Q}(\sqrt{a})/\mathbb{Q})$.

Proof. We first show that the list exhausts $\mathcal{F}_4^{1V}(\mathbb{Q}(\sqrt{a})/\mathbb{Q})$. Take $A \in \mathcal{F}_4^{1V}(\mathbb{Q}(\sqrt{a})/\mathbb{Q})$ and find $z \notin \mathbb{Q}_{\text{sq}} \cup a\mathbb{Q}_{\text{sq}}$ such that $A \cong A_{\mathbb{Q}(\sqrt{a})}(0, z, 0)$. Find $b \in Z \setminus \{a\}$ such that $z \in b\mathbb{Q}_{\text{sq}}$. Then $(0, z, 0) \sim (0, b, 0)$. Write $b = db'$ where $d \mid a$ and $\gcd(b', a) = 1$. Either, $|d| < \sqrt{|a|}$ and $b \in Z_a$ or $(0, z, 0) \sim (0, b, 0) = (0, db', 0) \sim (0, (a/d)b',)$ where $(a/d)b' \in Z_a$ since then $|a/d| < \sqrt{|a|}$.

We now prove irredundance. Suppose $(0, d_1a_1', 0) \sim (0, d_2a_2', 0)$ where $d_1, d_2 \in D$, $a_1', a_2' \in E$. Then, either $\frac{d_1a_1'}{d_2a_2'} \in \mathbb{Q}_{\text{sq}}$ or $\frac{d_1a_1'}{d_2a_2'} \in a\mathbb{Q}_{\text{sq}}$. In the first case, there are relatively prime integers r, s such that $d_1a_1's^2 = d_2a_2'r^2$. If there is a prime $p \mid d_1$ then $p \mid d_2$ since $\gcd(d_1, a_2') = 1$ and d_1, a_1', d_2, a_2' are not divisible by the square of any prime. Similarly, if $p \mid d_2$ then $p \mid d_1$, hence $d_1 = \pm d_2$. Hence $a_1's^2 = \pm a_2'r^2$. Now, by the same argument as above, $a_1' = \pm a_2'$. If $a_1' = -a_2'$ then we must have $d_1 = -d_2$ hence $d_1a_1' = d_2a_2'$, as desired.

Suppose $\frac{d_1a_1'}{d_2a_2'} \in a\mathbb{Q}_{\text{sq}}$. Then, there are relatively prime integers r, s with $d_1a_1's^2 = d_2a_2'ar^2$. We get, as above, $a_1' = \pm a_2'$. Hence $(s/r)^2 = \pm(a/d_1)d_2$ where $a/d_1, d_2$ are integers, not divisible by the square of any prime and s/r is an integer. Thus, $\pm a/d_1 = d_2$ and $\pm a = d_1d_2$. Thus, there is $i \in \underline{2}$ such that $|d_i| > \sqrt{|a|}$, contradiction. □

5.4 On the category $\mathcal{S}_4^{1V}(\mathbb{Q}(\sqrt{a})/\mathbb{Q})$

We begin by providing a connection to existing theory, by showing that the objects of the category $\mathcal{S}_4^{1V}(k)$ are Hurwitz algebras.

Proposition 5.9. *Let* k *be a field with* $\text{char}\, k \neq 2$. *Then every object of* $\mathcal{S}_4^{1V}(k)$ *is a Hurwitz division algebra.*

Proof. Take $A \in \mathcal{S}_4^{1V}(k)$, a quadratic nuclear subfield $l \subset A$ and a triple $\underline{c} = (1, 0, c_3) \in k^3$ such that $A \cong A_l(\underline{c})$. For $x \in l$, let $\overline{x}$ denote the action of the non-trivial Galois automorphism of l over k. Then, we claim that the mapping

$$n : A_l(\underline{c}) \longrightarrow k, \begin{pmatrix} x \\ y \end{pmatrix} \mapsto x\overline{x} - c_3y\overline{y} = q_{\underline{c}}\left(\begin{pmatrix} x \\ y \end{pmatrix}\right)$$

is a quadratic form which gives $A_l(\underline{c})$ the structure of a Hurwitz algebra according to Definition 2.8.

We have that $B : A_l(\underline{c}) \times A_l(\underline{c}),\ \left(\binom{x}{y}, \binom{z}{w}\right) \mapsto n\left(\binom{x}{y} + \binom{z}{w}\right) - n\left(\binom{x}{y}\right) - n\left(\binom{z}{w}\right)$ satisfies $B\left(\binom{x}{y}, \binom{z}{w}\right) = x\overline{z} + \overline{x}z - c_3(y\overline{w} + \overline{y}w)$ which is readily verified to be a non-degenerate bilinear form.

Recall that $n\left(\binom{x}{y}\right) = q_{\underline{c}}\left(\binom{x}{y}\right) = \det\begin{pmatrix} x & c_3\overline{y} \\ y & \overline{x} \end{pmatrix}$ from which it immeadiately follows that $n\left(\alpha\binom{x}{y}\right) = \alpha^2 n\left(\binom{x}{y}\right)$ for all $\alpha \in k$ by the properties of the determinant. Recall that multiplication in $A_l(\underline{c})$ is given by

$$\begin{pmatrix} x \\ y \end{pmatrix}\begin{pmatrix} z \\ w \end{pmatrix} = \begin{pmatrix} x & c_3\overline{y} \\ y & \overline{x} \end{pmatrix}\begin{pmatrix} z \\ w \end{pmatrix} = \begin{pmatrix} xz + c_3\overline{y}w \\ yz + \overline{x}w \end{pmatrix}.$$

Thus

$$n\left(\binom{x}{y}\right) n\left(\binom{z}{w}\right) = \det\begin{pmatrix} x & c_3\overline{y} \\ y & \overline{x} \end{pmatrix}\det\begin{pmatrix} z & c_3\overline{w} \\ w & \overline{z} \end{pmatrix} = \det\begin{pmatrix} xz + c_3\overline{y}w & c_3x\overline{w} + c_3\overline{yz} \\ yz + \overline{x}w & c_3y\overline{w} + \overline{xz} \end{pmatrix}$$

and

$$n\left(\begin{pmatrix} x \\ y \end{pmatrix}\begin{pmatrix} z \\ w \end{pmatrix}\right) = \det\begin{pmatrix} xz + c_3\overline{y}w & c_3\overline{(yz + \overline{x}w)} \\ yz + \overline{x}w & \overline{xz + c_3\overline{y}w} \end{pmatrix} = \det\begin{pmatrix} xz + c_3\overline{y}w & c_3x\overline{w} + c_3\overline{yz} \\ yz + \overline{x}w & c_3y\overline{w} + \overline{xz} \end{pmatrix}$$

so n is multiplicative.

□

Remark. Observe that the proposition is not confined to the case $k = \mathbb{Q}$.

By Proposition 2.10 and the fact that four-dimensional Hurwitz algebras are associative we get the following corollary.

Corollary 5.10. *Let k be a field of characteristic not equal to 2. Then the objects of $\mathcal{S}_4^{1V}(k)$ are the four-dimensional Hurwitz division algebras over k.*

Since there is, up to isomorphism, only one Hurwitz algebra in a given dimension which is not a division algebra [14], we can safely say that the objects of the category $\mathcal{S}_4^{1V}(k)$ constitute a large portion of the four-dimensional Hurwitz algebras.

In the literature, see for instance [14], there are exhaustive lists of Hurwitz algebras found by the Cayley-Dickson construction of algebras. Here, we approach the four-dimensional Hurwitz division algebras from a different angle and will obtain classification results, namely exhaustive lists and and even an exhaustive and irredundant list of four-dimensional Hurwitz algebras over $\mathbb{Q}$.

We now recall the norm of a field extension.

Definition 5.11. Let $k \subset l$ be a finite Galois extension with Galois group G. The *norm of l over k* is the map

$$n_{l/k} : l \longrightarrow k,\ x \mapsto \prod_{g \in G} g(x).$$

Remark. In particular, for $k = \mathbb{Q}, l = \mathbb{Q}(\sqrt{a})$, where $a \in Z$, we have $n_{\mathbb{Q}(\sqrt{a})/\mathbb{Q}}(q_1 + q_2\sqrt{a}) = q_1^2 - aq_2^2$. We define $n_a = n_{\mathbb{Q}(\sqrt{a})/\mathbb{Q}}$.

Proposition 5.12. *The set $C_{1,0}^a$ is non-empty for each $a \in Z$.*

Proof. By Proposition 4.6 (ii), the statement is equivalent with the statement that n_a is not surjective for any $a \in Z$. From [13, Theorem 1] it follows that for *every* finite Galois extension K of $\mathbb{Q}$, the map $n_{K/\mathbb{Q}}$ is not surjective, which implies our claim since the extensions $\mathbb{Q} \subset \mathbb{Q}(\sqrt{a})$ are finite Galois extensions. □

Remark. The above proposition implies that for each $a \in Z$ the category $\mathcal{S}_4^{1V}(\mathbb{Q}(\sqrt{a})/\mathbb{Q})$ is non-empty.

In the following proposition we provide more information about $C_{1,0}^a$ by presenting necessary and sufficient conditions allowing one to determine whether $(1, 0, c_3) \in C_{1,0}^a$. The test is derived using a classical result on ternary integral quadratic forms, originally due to Legendre.

Proposition 5.13. *Let $z \in \mathbb{Q} \setminus \mathbb{Q}_{sq}$, $a \in Z$. Choose $a_z \in Z$ such that $z \in a_z\mathbb{Q}_{sq}$ and set $d = \gcd(a, a_z) > 0$. Then $z \in \operatorname{im} n_a$ if and only if $\{a_z, a\} \cap \mathbb{N} \neq \emptyset$ and a_z is a square modulo $\frac{a}{d}$, a is a square module $\frac{a_z}{d}$ and $-\frac{a_z a}{d^2}$ is a square modulo d.*

Proof. Suppose $z \in \operatorname{im} n_a$. Then, there is a non-trivial pair $(x, y) \in \mathbb{Q}^2$ such that $z = x^2 - ay^2 = n_a(x + y\sqrt{a})$. We have $z = a_z q^2$ for some $q \in \mathbb{Q}^*$ and it holds that $z \in \operatorname{im} n_a$ if and only if $a_z \in \operatorname{im} n_a$ since $a_z = n_a(q^{-1}(x + y\sqrt{a}))$.

Now, we claim that the equation $a_z = X^2 - aY^2$, equation (1), has a non-trivial solution $(x, y) \in \mathbb{Q}^2$ if and only if the equation $X^2 - a_z Y^2 - aZ^2 = 0$, equation (2), has a non-trivial integral solution (x, y, z). Suppose first (1) has a non-trivial solution $x = \frac{x_1}{x_2}$, $y = \frac{y_1}{y_2}$. Then $(X, Y, Z) = (x_1 y_2, x_2 y_2, x_2 y_1)$ is a non-trivial integral solution of (2). Conversely, suppose (2) has a non-trivial solution (x, y, z). If $y = 0$ then $z \neq 0$ and $a = \left(\frac{x}{z}\right)^2$ which is a contradiction since $a \in Z$ is not a square. Hence $y \neq 0$ and $(X, Y) = (x/y, z/y) \in \mathbb{Q}^2$ is a non-trivial solution of (1) since at least one of x, z is non-zero.

Next, we claim that (2) has a non-trivial integral solution if and only if $dX^2 - \frac{a_z}{d}Y^2 - \frac{a}{d}Z^2 = 0$, equation (3), does. If (x, y, z) solves (3) then (dx, y, z) solves (2). If (x, y, z) solves (2), then $d \mid x^2$ and since d whose prime factors all occur with multiplicity at most one, i.e. d square-free, we have $d^2 \mid x^2$ and we can write $x = dx'$ for some integer x. Then (x', y, z) solves (3).

Summarizing, we have shown that $z \in \operatorname{im} n_a$ if and only if the equation $dX^2 - \frac{a_z}{d}Y^2 - \frac{a}{d}Z^2 = 0$ has a non-trivial integral solution. This equation is a ternary integral quadratic form. By a classic theorem of Legendre [10, Theorem 5.11] a ternary integral quadratic form $AX^2 + BY^2 + CZ^2 = 0$ with ABC square free has a non-trivial integral solution if and only if A, B, C do not all have the same sign and $-AB$ is a square modulo C, $-BC$ is a square modulo A and $-AC$ is a square modulo B.

Application of this result to the equation $dX^2 - \frac{a_z}{d}Y^2 - \frac{a}{d}Z^2 = 0$ yields the desired result. □

Proposition 5.14. *Set $\tilde{C}_{1,0}^a := \{(1, 0, a) \mid a \in Z\} \cap C_{1,0}^a \subset C_{1,0}^a$. Then the family $\{A_{\mathbb{Q}(\sqrt{a})}(\underline{c}) \mid \underline{c} \in \tilde{C}_{1,0}^a\}$ of central skew fields exhausts $\mathcal{S}_4^{1V}(\mathbb{Q}(\sqrt{a})/\mathbb{Q})$.*

Proof. Take $A \in \mathcal{S}_4^{1V}(\mathbb{Q}(\sqrt{a})/\mathbb{Q})$. Then by Proposition 4.5, there is $\underline{c} = (1, 0, z) \in C_{1,0}^a$ such that $A \cong A_{\mathbb{Q}(\sqrt{a})}(\underline{c})$. Find $a_z \in Z$ such that $z \in a_z\mathbb{Q}_{\mathrm{sq}}$, then also $(1, 0, a_z) \in C_{1,0}^a$ since $a_z \in \operatorname{im} n_a$ if and only if $z \in \operatorname{im} n_a$. But $a_z/z \in \mathbb{Q}_{\mathrm{sq}} \subset \operatorname{im} n_a$ so $(1, 0, z) \sim (1, 0, a_z)$ by Proposition 4.6 (iii) whence the claim follows. □

5.5 Classification of $\mathcal{S}_4^{1V}(\mathbb{Q}(i)/\mathbb{Q})$

Specializing to the case $a = -1$ we will in this section arrive at a classification of $\mathcal{S}_4^{1V}(\mathbb{Q}(i)/\mathbb{Q})$.

Definition 5.15. Let $N_2 = n_{\mathbb{Q}(i)/\mathbb{Q}}(\mathbb{Z}[i])$, $Q_2 = \operatorname{im} n_{\mathbb{Q}(i)/\mathbb{Q}}$ i.e. N_2 is the set of natural numbers expressible as the sum of two squares of natural numbers and Q_2 is the set of rational numbers expressible as the sum of two squares of rational numbers.

The following proposition allows identification of elements that belong to Q_2. Its statement can be found in [12, pp. 352].

Proposition 5.16. *Let $q \in \mathbb{Q}_{>0}$ and write $q = a/b$. Then $q \in Q_2$ if and only if $ab \in N_2$.*

Proof. Suppose $ab \in N_2$, so that have $ab = a_1^2 + a_2^2$ for some integers a_1, a_2, not both zero. Then, $q = a/b = (a_1/b)^2 + (a_2/b)^2 \in Q_2$.

Suppose now $a/b \in Q_2$. Write $a = ca', b = cb'$ for some integers a', b', c such that $\gcd(a', b') = 1$. If $a'b' \in N_2$ then also $c^2a'b' = ab \in N_2$ so it suffices to prove that $a'b' \in N_2$. Write $a'/b' = a/b = (p_1/q_1)^2 + (p_2/q_2)^2$ where $\gcd(p_i, q_i) = 1$ for $i \in \underline{2}$ and not both $p_i = 0$. Then

$$a'q_1^2q_2^2 = b'(p_1^2 + p_2^2). \tag{1}$$

Suppose $a'b' \notin N_2$. By a classical result of number theory [10, Theorem 2.15] there is a prime $q \in \mathbb{P}_3$ such that the maximal k with $q^k \mid a'b'$ is odd. If $q \mid a'$ then $q \mid p_1^2 + p_2^2$ hence $q \mid p_1, p_2$ since $q \in \mathbb{P}_3$ by another classical result [10, Lemma 2.14]. But then, the maximal power of q that divides the right hand side of (1) is even and the maximal power dividing the left hand side is odd, since $q \nmid q_1q_2$, contradiction.

If $q \mid b'$ then $q \mid (q_1q_2)^2$ and since $\gcd(p_i, q_i) = 1$, $i \in \underline{2}$, we have that the maximal power of q that divides the right hand side of (1) is odd, and the maximal power of q that divides the left hand side is even, contradiction. Consequently the claim follows. □

Corollary 5.17. *For $c_3 = \pm \prod_{p\in\mathbb{P}} p^{n_p} \in \mathbb{Q}$ we have $c_3 \notin \operatorname{im} n_{\mathbb{Q}(i)/\mathbb{Q}}$ if and only if $c_3 < 0$ or there exists $q \in \mathbb{P}_3$ such that n_q is odd.*

Proof. Since $Q_2 \subset \mathbb{Q}_{\geq 0}$ the claim about the case $c_3 < 0$ follows from Proposition 4.6 (ii) and $Q_2 = \operatorname{im} n_{\mathbb{Q}(i)/\mathbb{Q}}$. If $c_3 > 0$ then by Proposition 5.16 we get $\prod_{p\in\mathbb{P}} p^{|n_p|} \in N_2$ and hence by [10, Theorem 2.15] there is $q \in \mathbb{P}_3$ with n_q odd. □

Proposition 5.18. *Let $Z_i = \{\pm \prod_{p\in F} p \mid \emptyset \neq F \subset \mathbb{P}_3, |F| < \infty\} \cup \{-1\}$. Then, the skew fields $A_{\mathbb{Q}(i)}(1, 0, z)$, $z \in Z_i$ classify $\mathcal{S}_4^{1V}(\mathbb{Q}(i)/\mathbb{Q})$.*

Proof. Take $A \in \mathcal{S}_4^{1V}(\mathbb{Q}(i)/\mathbb{Q})$. Find $(1, 0, z) \in C_{1,0}^{-1}$ with $A \cong A_{\mathbb{Q}(i)}(1, 0, z)$ and write $z = \pm \prod_{p\in\mathbb{P}} p^{n_p}$. Set $F_z = \{p \in \mathbb{P}_3 \mid n_p \text{ is odd}\}$. If $F_z = \emptyset$ we must have $z = -1$ since $(1, 0, 1) \notin C_{1,0}^{-1}$ by Proposition 4.6 (ii). Otherwise, we have $(1, 0, z) \sim (1, 0, \operatorname{sgn}(z) \prod_{p\in F_z} p)$ where $\operatorname{sgn}(z) \prod_{p\in F_z} p \in Z_i$ since $z/\left(\operatorname{sgn}(z) \prod_{p\in F_z} p\right) \in \operatorname{im} n_{\mathbb{Q}(i)/\mathbb{Q}}$ by Corollary 5.17.

We now prove irredundance. For $z \in Z_i \setminus \{-1\}$ we have $(1, 0, z) \nsim (1, 0, -1)$ since if $z = \operatorname{sgn}(z) \prod_{p\in F} p$ for appropriate non-empty $F \subset \mathbb{P}_3$ then Corollary 5.17 shows that $z/(-1) \notin n_{\mathbb{Q}(i)/\mathbb{Q}}$.

Take now $z_1, z_2 \in Z_i \setminus \{-1\}$ and suppose $(1, 0, z_1) \sim (1, 0, z_2)$. Suppose $z_i = \prod_{p\in F_i}$ for appropriate $F_i \subset \mathbb{P}_3$, $i \in \underline{2}$. If $F_1 \neq F_2$ then we would have $z_1/z_2 \notin \operatorname{im} n_{\mathbb{Q}(i)/\mathbb{Q}}$ by Corollary 5.17 hence $(1, 0, z_1) \nsim (1, 0, z_2)$, contradiction. □

Remark. Note that this result gives a classification of the four-dimensional Hurwitz division algebras over $\mathbb{Q}$ in which $\mathbb{Q}(i)$ is a subfield as well as a $\mathbb{Q}[C_2^2]$-submodule.

5.6 On the category $\mathcal{N}_4^{1V}(\mathbb{Q}(\sqrt{a})/\mathbb{Q})$

We here present, for every $a \in Z$, a family of elements of C_*^a, showing in particular that the set is non-empty which implies that the category $\mathcal{N}_4^{1V}(\mathbb{Q}(\sqrt{a})/\mathbb{Q})$ is non-empty.

Proposition 5.19. *For each $a \in Z$, the category $\mathcal{N}_4^{1V}(\mathbb{Q}(\sqrt{a})/\mathbb{Q})$ is non-empty. More precisely, for each $a \in Z$ the set C_*^a contains a three-parameter family of triples given as follows.*

(i) *Take $a \in Z$ with $a > 0$. Then for $c_1 < \frac{1}{2}$, c_2 arbitrary and $c_3 > |c_2|$ we have $(c_1, c_2, c_3) \in C_*^a$.*

(ii) *Take $a \in Z$ with $a < 0$. Then for $c_1 > \frac{1}{2}$, c_2 arbitrary and $c_3 < -|c_2|$ such that $(c_1, c_2) \neq (1, 0)$ we have $(c_1, c_2, c_3) \in C_*^a$.*

Proof. The proofs of (i) and (ii) rely on the same mechanics so we prove (i). We recall that from the definition of C_*^a we have $(c_1, c_2, c_3) = \underline{c} \in C_*^a$ if and only if the function

$$q_{\underline{c}} : \mathbb{Q}(\sqrt{a}) \times \mathbb{Q}(\sqrt{a}),\ \begin{pmatrix} x \\ y \end{pmatrix} \mapsto (1 - c_1)x^2 + c_3 x\overline{x} - c_2 y^2 - c_3 y\overline{y}$$

only has the trivial zero (and $(c_1, c_2) \neq (1, 0)$, $(c_1, c_3) \neq (0, 0)$). Writing $x = x_1 + x_2 i, y = y_1 + y_2 i$ for $x_1, x_2, y_1, y_2 \in \mathbb{Q}$ we have $(c_1, c_2, c_3) \in C_*^a$ is equivalent with system

$$\begin{cases} 0 = X_1^2 + (1 - 2c_1)aX_2^2 - (c_2 + c_3)Y_1^2 + (c_3 - c_2)aY_2^2 \\ (1 - c_1)X_1X_2 = -c_2Y_1Y_2 \end{cases}$$

having only the trivial solution $(x_1, x_2, y_1, y_2) = (0, 0, 0, 0)$. The assumptions imply $(1 - 2c_1) > 0$, $-(c_2 + c_3) > 0$, $(c_3 - c_2)a > 0$ so the first equation has the trivial solution only which implies the desired result. □

Proposition 5.20. *Take $a \in Z$ such that there exists $p \in \mathbb{P}_3$ with $p \mid a$. Then if $\underline{c} = (c_1, c_2, c_3) \in \mathbb{Z}^3$ satisfies $(c_1, c_3) \neq (0, 0)$ and $1 - 2c_1 \equiv 1 \mod p$, $c_2 \equiv -1 \mod p$, $c_3 \equiv 0 \mod p$ we have $\underline{c} \in C_*^a$.*

Proof. Take $a \in Z$ as in the proposition and a corresponding $p \in \mathbb{P}_3$. Take $\underline{c} = (c_1, c_2, c_3) \in \mathbb{Z}^3$ satisfying the hypotheses of the proposition. Then, by the proof of the previous proposition $(c_1, c_2, c_3) \in C_*^a$ is equivalent with system

$$\begin{cases} 0 = X_1^2 + (1 - 2c_1)aX_2^2 - (c_2 + c_3)Y_1^2 + (c_3 - c_2)aY_2^2 \\ (1 - c_1)X_1X_2 = -c_2Y_1Y_2 \end{cases}$$

having only the trivial rational solution $(x_1, x_2, y_1, y_2) = (0, 0, 0, 0)$. But, since this system is homogenous, the existence of a non-trivial rational solution is equivalent with the existence of a non-trivial integral solution. So, suppose the system has a non-trivial integral solution (x_1, x_2, y_1, y_2). Again, since the system is homogenous, we may assume the existence of a non-trivial solution such that $\gcd(x_1, x_2, y_1, y_2) = 1$.

Considering the first equation modulo p we get $x_1^2 + y_1^2 \equiv 0 \mod p$. Since $p \equiv 3 \mod 4$ we get $p \mid x_1, y_1$. Thus $p^2 \mid x_1^2 - (c_2 + c_3)y_1^2 = a((c_2 - c_3)y_2^2 - (1 - 2c_1)x_2^2)$. Since $p^2 \nmid a$ we get $p \mid (c_2 - c_3)y_2^2 - (1 - 2c_1)x_2^2$. Therefore $(c_2 - c_3)y_2^2 - (1 - 2c_1)x_2^2 = -y_2^2 - x_2^2 \equiv 0 \mod p$ so $p \mid x_2, y_2$, contradiction. □

5.7 On the category $\mathcal{N}_4^{1V}(\mathbb{Q}(i)/\mathbb{Q})$

In this section we further investigate C_*^a in the special case $a = -1$ producing parametrized families of algebras in $\mathcal{N}_4^{1V}(\mathbb{Q}(i)/\mathbb{Q})$ using ad hoc number theoretic approaches. We first prove two results which will allow us to produce a one-parameter family of algebras in $\mathcal{N}_4^{1V}(\mathbb{Q}(i)/\mathbb{Q})$.

Proposition 5.21. *Let $m = p^{2k+1}m'$ where $p \in \mathbb{P}_3$, $k \in \mathbb{N}$ and $\gcd(m', p) = 1$. Then if $(x, y, z) \in \mathbb{Z}^3$ satisfies*

$$x^2 + y^2 = mz^2$$

we have $p \mid \gcd(x, y, z)$, i.e. x, y, z are not relatively prime.

Proof. We prove the claim by induction on k. Suppose first $k = 0$. Then we have $x^2 + y^2 = pm'z^2$ and hence $p \mid x^2 + y^2$ which implies $p \mid x$, $p \mid y$ as $p \in \mathbb{P}_3$. Hence $p^2 \mid x^2 + y^2 = pm'z^2$. Since $p \nmid m'$ we have $p \mid z$ and the claim follows.

Suppose now $k > 0$. Then again $p \mid x^2 + y^2$ so $p^2 \mid p^{2k+1}m'z^2$ and we have

$$(x/p)^2 + (y/p)^2 = p^{2(k-1)+1}m'z^2$$

from which we get $p \mid \gcd(x/p, y/p, z)$ by induction hypothesis and the claim follows. □

Corollary 5.22. *For $m \in \mathbb{N}$, $m \notin N_2$ the equation $X^2 + Y^2 = mZ^2$ has only the trivial solution in integers.*

Proof. Suppose towards a contradiction that there is a non-trivial solution $(x, y, z) \in \mathbb{Z}^3$ to $X^2 + Y^2 = mZ^2$ and set $d = \gcd(x, y, z)$. Then $(x/d, y/d, z/d)$ is also a non-trivial solution to the same equation so we may without loss of generality take (x, y, z) with $\gcd(x, y, z) = 1$. Since $m \notin N_2$ there is, by a classic result of number theory, $p \in \mathbb{P}_3$ and $k \in \mathbb{N}$ such that $m = p^{2k+1}m'$ and $p \nmid m'$. Hence we have

$$x^2 + y^2 = p^{2k+1}m'z^2$$

whence we get $p \mid \gcd(x, y, z)$ by Proposition 5.21, which is the desired contradiction. □

Proposition 5.23. *Take a positive integer $m \notin N_2$. Then $(c_1, c_2, c_3) = \left(\frac{1-m}{2}, 0, -1\right) \in C_*^{-1}$.*

Proof. Suppose $(x_1, x_2, y_1, y_2) \in \mathbb{Z}^4$ satisfies

$$\begin{cases} x_1^2 + (2c_1 - 1)x_2^2 + (-c_2 - c_3)y_1^2 + (c_2 - c_3)y_2^2 = 0 \\ (1 - c_1)x_1x_2 = c_2y_1y_2. \end{cases}$$

It suffices to show $x_1 = x_2 = y_1 = y_2 = 0$ to conclude $(c_1, c_2, c_3) \in C_*^{-1}$. Since $c_2 = 0$ and $1 - c_1 \neq 0$ we have two cases, namely $x_1 = 0$ or $x_2 = 0$.

If $x_2 = 0$ we must have $x_1^2 + y_1^2 + y_2^2 = 0$ which forces $x_1 = y_1 = y_2 = 0$ and if $x_1 = 0$ we must have

$$mx_2^2 = y_1^2 + y_2^2$$

which forces $x_2 = y_1 = y_2 = 0$ by Corollary 5.22. Hence $\left(\frac{1-m}{2}, 0, -1\right) \in C_*^{-1}$. □

Remark. From Proposition 4.6 (iii), it is immediate that for positive integers $m_1, m_2 \notin N_2$, we have $\left(\frac{1-m_1}{2}, 0, -1\right) \sim \left(\frac{1-m_2}{2}, 0, -1\right)$ if and only if $m_1 = m_2$. Therefore,

$$C_N := \{((1-m)/2, 0, -1) \mid m \in \mathbb{N}, m \notin N_2\}$$

is an irredundant subset of C_*^{-1}, i.e. no two algebras constructed from distinct triples of the set C_N are isomorphic.

The following result allows one to construct a three-parameter family of algebras in $\mathcal{N}_4^{1V}(\mathbb{Q}(i)/\mathbb{Q})$.

Proposition 5.24. *$(2m, 2n_1, 2n_2) \in C_*^{-1}$ for all $(m, n_1, n_2) \in \mathbb{Z}^3$ where $m \neq 0$, n_1 odd, n_2 even.*

Proof. We have $(2m, 2n_1, 2, n_2) \in C_*^{-1}$ if and only if

$$\begin{cases} 0 = x_1^2 + (4m-1)x_2^2 - (2n_1 + 2n_2)y_1^2 + (2n_1 - 2n_2)y_2^2 \\ (1-2m)x_1x_2 = 2n_1y_1y_2 \end{cases}$$

has only the trivial solution $(x_1, x_2, y_1, y_2) \in \mathbb{Z}^4$. Suppose there is a non-trivial solution. Set $d = \gcd(x_1, x_2, y_1, y_2)$ then $(x_1/d, x_2/d, y_1/d, y_2/d)$ is a non-trivial primitive solution. So suppose $(x_1, x_2, y_1, y_2) \in \mathbb{Z}^4$ is a non-trivial primitive solution to the above system. Since $1 - 2m$ is odd we have $2 \mid x_1$ or $2 \mid x_2$ by the second equation of the above system.

Suppose $2 \mid x_1$. Since $4m-1$ is odd, we have $2 \mid x_2^2$. Since n_1 odd, n_2 even the numbers $n_1 + n_2$, $n_1 - n_2$ are odd. Since $4 \mid x_1^2, x_2^2$ we have $2 \mid (n_1 - n_2)y_2^2 - (n_1 + n_2)y_1^2$ and thus y_1, y_2 must have the same parity. By the second equation, $2 \mid y_1y_2$ so both y_1, y_2 are even. Thus, x_1, x_2, y_1, y_2 are all even, contradiction.

If $2 \mid x_2$, we can proceed as above to obtain a contradiction. □

We conclude this section by a final parametrized subset of C_*^{-1}.

Proposition 5.25. *Take $c_2 = \pm \prod_{p \in \mathbb{P}} p^{n_p} \in \mathbb{Z}$ such that there exists $p \in \mathbb{P}_3$ with n_p odd. Then $(1, c_2, 0) \in C_*^{-1}$.*

Proof. We have $(1, c_2, 0) \in C_*^{-1}$ if and only if

$$\begin{cases} 0 = x_1^2 + x_2^2 - c_2y_1^2 + c_2y_2^2 \\ 0 = -c_2y_1y_2. \end{cases}$$

has the trivial solution $(x_1, x_2, y_1, y_2) \in \mathbb{Z}^4$ only. Suppose there is a non-trivial solution $(x_1, x_2, y_1, y_2) \in \mathbb{Z}^4$ to the above system. As always, we may assume the solution is primitive. The second equation implies that $y_1 = 0$ or $y_2 = 0$, assume first $y_1 = 0$ (the case $y_2 = 0$ is analogous). Fix $q \in \mathbb{P}_3$ s.t. $n_q > 0$ odd. Then, $q \mid x_1, x_2$ and hence the maximal power q dividing the right hand side of $-c_2y_2^2 = x_1^2 + x_2^2$ is even. However, the maximal power of q dividing the left hand side of $c_2y_2^2 = x_1^2 + x_2^2$ is odd, since for otherwise $q \mid y_2$ and $q \mid \gcd(x_1, x_2, y_1, y_2)$. □

It seems that by varying or refining the above approaches one could generate further parametrized families of algebras in $\mathcal{N}_4^{1V}(\mathbb{Q}(i)/\mathbb{Q})$ and get more insight into the structure of the category. However, exhaustively constructing the category $\mathcal{N}_4^{1V}(\mathbb{Q}(i)/\mathbb{Q})$ currently appears to be a distant goal.

5.8 Concluding remarks

In this final section, some concluding remarks and an overview of results obtained will be presented. In investigating the covering

$$\left(\bigcup_{a\in Z}\mathcal{F}_4^{1V}(\mathbb{Q}(\sqrt{a})/\mathbb{Q})\right)\amalg\left(\bigcup_{a\in Z}\mathcal{S}_4^{1V}(\mathbb{Q}(\sqrt{a})/\mathbb{Q})\right)\amalg\left(\coprod_{a\in Z}\mathcal{N}_4^{1V}(\mathbb{Q}(\sqrt{a})/\mathbb{Q})\right)$$

it turned out, as one might expect, that the complexity in investigating the different parts of the covering increased with decrease of structure. In saying this, we mean that the most satisfactory results were obtained in the investigation of the part of the covering consisting of fields whereas there is still a lot of work to be done in order to fully understand the non-associative part.

In Propositions 5.7 and 5.8 we classified the category $\mathcal{F}_4^{1V}(\mathbb{Q}(\sqrt{a})/\mathbb{Q})$ for each $a \in Z$. In Proposition 5.14 we found, for each $a \in Z$, a list of skew fields, indexed by a subset of Z, that exhausts $\mathcal{S}_4^{1V}(\mathbb{Q}(\sqrt{a})/\mathbb{Q})$ - which we also found to be a category coinciding with certain Hurwitz division algebras. In Proposition 5.18, we refined the exhausting list to a classifying list in the special case $a = -1$. In Section 5.6 we investigated the categories $\mathcal{N}_4^{1V}(\mathbb{Q}(\sqrt{a})/\mathbb{Q})$ for general $a \in Z$, finding a three-parameter family of algebras in each case, and thereafter obtained further families for particular values of a.

Throughout the course of this work, connections between, on one hand, fresh results about four-dimensional division algebras, and on the other, classical results of number theory have been found. We have also approached Hurwitz algebras from a different viewpoint than the classical one which resulted in partial classification results of four-dimensional Hurwitz algebras over $\mathbb{Q}$. The classical approach to Hurwitz involves the Cayley-Dickson construction, whereas we here instead use the construction (and reduction) in [6].

In the future, one could try to refine the above covering by further investigating redundance in the parts of the covering consisting of fields and skew fields. One could also continue the above work to explore the non-associative part of the covering which eventually might lead to an exhaustive list of non-associative algebras.

Acknowledgments

I would like to thank my supervisor Ernst Dieterich for his efforts in finding interesting problems for me to work with during my project. I am also grateful for all encouragement, inspirational discussions and for guidance in the right direction when I needed it. I would also like to express my gratitude towards my friend Johan Asplund for his support over the past couple of years and for fruitful collaborations. Finally, I would like to thank my family for all their care and support.

References

[1] M. I. Al-Ali, *Semifields as free modules*, The Quarterly Journal of Mathematics, 62 (2011), pp. 1–6.

[2] M. Bani-Ata, S. Aldhafeeri, F. Belgacem, and M. Laila, *On four-dimensional unital division algebras over finite fields*, Algebras and Representation Theory, 18 (2015), pp. 215–220.

[3] C. W. Curtis and I. Reiner, *Representation theory of finite groups and associative algebras*, John Wiley & Sons, Inc., 1962.

[4] O. Diankha, M. Traoré, M. Ramírez, and A. Rochdi, *Four-dimensional real third-power associative division algebras*, Communications in Algebra, 44 (2016), pp. 3397–3406.

[5] E. Dieterich, *Classification, automorphism groups and categorical structure of the two-dimensional real division algebras*, Journal of Algebra and its applications, 4 (2005), pp. 517–538.

[6] E. Dieterich, *On four-dimensional unital division algebras*, Manuscript, Uppsala. In preparation., (2016).

[7] H.-D. Ebbinghaus et al., *Zahlen*, Springer-Verlag Berlin Heidelberg, 1983.

[8] P. A. Grillet, *Abstract algebra*, vol. 242, Springer Science & Business Media, 2007.

[9] R. Lidl and H. Niederreiter, *Finite fields*, Cambridge university press, 2008.

[10] I. Niven, H. S. Zuckerman, and H. L. Montgomery, *An introduction to the theory of numbers*, John Wiley & Sons, 1991.

[11] H. Salzmann, D. Betten, T. Grundhöfer, H. Hähl, R. Löwen, and M. Stroppel, *Compact projective planes*, Walter de Gruyter & Co., Berlin, 1991.

[12] W. Sierpiński, *Elementary theory of numbers*, Państwowe Wydawnictwo Waukowe, Warszawa, 1964.

[13] L. Stern, *On the norm groups of global fields*, Journal of Number Theory, 32 (1989), pp. 203–219.

[14] K. A. Zhevlakov, I. P. Shestakov, A. Shirshov, and A. Slin'ko, *Rings that are nearly associative*, Academic Press, Inc., 1982.