Mathematical
Surveys
and
Monographs

Volume 191

An Introduction to Central Simple Algebras and Their Applications to Wireless Communication

Grégory Berhuy
Frédérique Oggier

American Mathematical Society

Mathematical
Surveys
and
Monographs

Volume 191

An Introduction to Central Simple Algebras and Their Applications to Wireless Communication

Grégory Berhuy
Frédérique Oggier

American Mathematical Society
Providence, Rhode Island

2010 *Mathematics Subject Classification.* Primary 12E15; Secondary 11T71, 16W10.

For additional information and updates on this book, visit
www.ams.org/bookpages/surv-191

Library of Congress Cataloging-in-Publication Data

Berhuy, Grégory.
An introduction to central simple algebras and their applications to wireless communications / Grégory Berhuy, Frédérique Oggier.
pages cm. – (Mathematical surveys and monographs ; volume 191)
Includes bibliographical references and index.
ISBN 978-0-8218-4937-8 (alk. paper)
1. Division algebras. 2. Skew fields. I. Oggier, Frédérique. II. Title.

QA247.45.B47 2013
512′.3–dc23 2013009629

∞ The paper used in this book is acid-free and falls within the guidelines
established to ensure permanence and durability.
Visit the AMS home page at http://www.ams.org/

10 9 8 7 6 5 4 3 2 1 18 17 16 15 14 13

An Introduction to Central Simple Algebras and Their Applications to Wireless Communication

Foreword

Mathematics continually surprises and delights us with how useful its most abstract branches turn out to be in the real world. Indeed, physicist Eugene Wigner's memorable phrase[1] "The unreasonable effectiveness of mathematics" captures a critical aspect of this utility. Abstract mathematical ideas often prove to be useful in rather "unreasonable" situations: places where one, a priori, would not expect them at all! For instance, no one who was not actually following the theoretical explorations in multi-antenna wireless communication of the late 1990s would have predicted that division algebras would turn out to be vital in the deployment of multi-antenna communication. Yet, once performance criteria for space-time codes (as coding schemes for multi-antenna environments are called) were developed and phrased as a problem of design of matrices, it was completely natural that division algebras should arise as a solution of the design problem. The fundamental performance criterion ask for $n \times n$ matrices M_i such that the difference of any two of the M_i is of full rank. To anyone who has worked with division algebras, the solution simply leaps out: any division algebra of index n embeds into the $n \times n$ matrices over a suitable field, and the matrices arising from the embedding naturally satisfy this criterion.

But there is more. Not only did division algebras turn out to be the most natural context in which to solve the fundamental design problem above, they also proved to be the correct objects to satisfy various other performance criteria that were developed. For instance, a second, and critical, performance criterion called the coding gain criterion turned out to be naturally satisfied by considering division algebras over number fields and using natural $\mathbb{Z}$-orders within them that arise from rings of integers of maximal subfields. Other criteria (for instance "DMG optimality," "good shaping," "information-losslessness" to name just a few) all turned out to be satisfied by considering suitable orders inside suitable division algebras over number fields. Indeed, this exemplifies another phenomenon Wigner describes: after saying that "mathematical concepts turn up in entirely unexpected connections," he goes on to say that "they often permit an unexpectedly close and accurate description of the phenomena in these connections." The match between division algebras and the requirement of space-time codes is simply uncanny.

The subject of multi-antenna communication has several unsolved mathematical problems still, for instance, in the area of decoding for large numbers of antennas. Nevertheless, division algebras are already being deployed for practical two-antenna

[1] Eugene P. Wigner, The unreasonable effectiveness of mathematics in the natural sciences, Comm. Pure Appl. Math., **13** Feb. 1960, 1–14

systems, and codes based on them are now part of various standards of the Institute of Electrical and Electronics Engineers (IEEE). It would behoove a student of mathematics, therefore, to know something about the applicability of division algebras while studying their theory; in parallel, it is vital for a communications engineer working in coding for multiple-antenna wireless to know something about division algebras.

Berhuy and Oggier have written a *charming* text on division algebras and their application to multiple-antenna wireless communication. There is a wealth of examples here, particularly over number fields and local fields, with explicit calculations, that one does not see in other texts on the subject. By pairing almost every chapter with a discussion of issues from wireless communication, the authors have given a very concrete flavor to the subject of division algebras. The book can be studied profitably not just by a graduate student in mathematics, but also by a mathematically sophisticated coding theorist. I suspect therefore that this book will find wide acceptability in both the mathematics and the space-time coding community and will help cross-communication between the two. I applaud the authors' efforts behind this very enjoyable book.

B.A. Sethuraman

Northridge, California

Contents

Introduction

A central simple algebra over a field k is a finite dimensional k-algebra with center k which does not have any proper two-sided ideals. The most elementary example is the Hamilton quaternion algebra. More generally, a division ring with center k can be viewed as a central simple k-algebra, where the algebra structure is induced by the multiplication law. Central simple algebras and division rings have been extensively studied, and have appeared in many other areas of mathematics, such as ring theory, number theory, representation theory of finite groups, algebraic geometry or classification theory of quadratic forms. Surprisingly, they have recently been proven useful in coding theory.

The ambition of this book is to provide an introduction to the theory of central simple algebras accessible at a graduate level, starting from scratch and including fundamental concepts such as splitting fields, Brauer group, crossed product algebras, index and exponent, as well as algebras with involution. Even though most of our exposition is rather classical, we have tried to focus on explicit techniques and examples, most of them coming from coding theory. The codes presented in this book are there to illustrate the theory of central simple algebras, and do not give an exhaustive view of the work done on the theory of algebraic space-time coding.

The use of division algebras for space-time coding is usually attributed to the seminal work by B. A. Sethuraman et al. [**48**]. Number fields and cyclic algebras were discussed, which have been a favourite tool for space-time design (see for example [**12, 6, 40, 13, 32, 55**]). Other algebras have been explored, such as Clifford algebras [**27**], or crossed product algebras (e.g. [**57**]).

Alternative studies considered the use of maximal orders (e.g. [**56**]) or non-associative algebras (e.g. [**42**]).

Some surveys on coherent space-time coding [**36, 45**] and one survey on non-coherent space-time coding [**35**] are now available. These works are just representing a few of the different approaches studied so far in the area of space-time coding, which is still an active field of research. These are just pointers for the interested reader, and by no mean provide a complete list.

In Chapter I, we introduce the concept of a central simple k-algebra and give the first examples of such algebras, including quaternion algebras. We then explain how they can be embedded into matrix algebras, and how this result may be used in coding theory. In Chapter II, we have a closer look at the properties of quaternion algebras. We also prove that the only finite dimensional division $\mathbb{R}$-algebras are, up to isomorphism, $\mathbb{R}, \mathbb{C}$ or the Hamilton quaternion algebra $\mathbb{H}$. We then provide examples of quaternion based codes. The results presented in Chapter III are the core of the theory. We first study the stability of central simple k-algebras under algebraic operations such as tensor product or base field extension. We then prove that any central simple k-algebra is isomorphic to a matrix algebra over a central division k-algebra, and establish that every k-automorphism of such an algebra is inner. We also focus on the structure of the centralizer of a simple subalgebra, which is a crucial tool in the study of maximal subfields and splitting fields of central simple algebras, which will be developed in Chapter IV. As an application of this theory, we define the reduced characteristic polynomial of an element of a central simple algebra, and introduce the concept of the reduced norm, which generalizes the determinant of a matrix. The latter can in turn be used to reinterpret code parameters. In Chapter V, we define the Brauer group $\mathrm{Br}(k)$ of a field k, which allows us to study globally all central simple k-algebras. We show that this group is an abelian torsion group, and use this result to define the exponent of a central simple k-algebra. We end this chapter by establishing the existence of a primary decomposition of a central simple k-algebra. In Chapter VI, we characterize central simple algebras which have a Galois maximal subfield. This leads to the notion of a crossed product algebra. We then present the standard results on these particular algebras. At the end of this chapter, crossed product algebras are used to construct families of codes. Chapter VII is devoted to cyclic algebras, that is, the case where the Galois maximal subfield is cyclic. At this occasion, an overview of the theory of central simple algebras over local and number fields is given without proofs. Explicit criteria to decide whether a given central simple algebra over a global field is division are established. Finally, these criteria are used to design codes based on cyclic division algebras. Chapter VIII focuses on central simple k-algebras of degree 4. We show that these algebras are crossed products over a biquadratic extension L/k, and a full description by generators and relations is given. We also provide a criterion to check if such an algebra is division in terms of the parameters defining the algebra when k is a number field, and applications to code constructions are given. In Chapter IX, the concept of a unitary involution on a central simple algebra is defined. The existence of unitary involutions is then investigated. We particularly focus on the case of crossed product algebras. We then explain how central simple algebras with a unitary involution may be used in coding theory via the construction of unitary codes, and we give various examples.

We would like to sincerely thank N. Markyn, S. Pumpluen, A. Quéguiner-Mathieu, B.A. Sethuraman, J.-P. Tignol, T. Unger and R. Vehkalahti for their careful reading of substantial parts of this book. Their pertinent comments enabled us to dramatically improve the quality of the exposition.

CHAPTER I

Central simple algebras

This chapter contains the necessary definitions and background on central simple algebras. After some preliminaries on k-algebras and tensor products, we introduce central simple algebras and give some examples. We then show how to identify central simple algebras with matrix subalgebras. As a first illustration, we explain how central simple algebras may be used in coding theory, and examples of code constructions are presented.

I.1. Preliminaries on k-algebras

In the sequel, k will denote an arbitrary field.

DEFINITION I.1.1. A **k-algebra** is a pair (A, μ), where A is a k-vector space and $\mu : A \times A \longrightarrow A$ is a k-bilinear map, called the **product law** of A. We write aa' for $\mu(a, a')$, and call it the **product** of the elements a and a'.

A k-algebra A is called **associative** (resp. **commutative**, resp. **unital**) if the product law is associative (resp. commutative, resp. has a unit element 1_A).

EXAMPLES I.1.2.

(1) The ring of polynomials $k[X]$ is a commutative, associative and unital k-algebra.

(2) If L/k is a field extension, then L is a commutative, associative and unital k-algebra.

□

DEFINITION I.1.3. A **k-algebra morphism** is a k-linear map
$f : A \longrightarrow B$ satisfying

$$f(aa') = f(a)f(a') \text{ for all } a, a' \in A.$$

If A and B are unital, we require in addition that $f(1_A) = 1_B$. A **k-algebra isomorphism** is a k-algebra morphism which is bijective. In this case, the inverse map f^{-1} is also a k-algebra morphism.

DEFINITION I.1.4. A **subalgebra** of a k-algebra A is a linear subspace B of A which is closed under the product. If A is unital, we require in addition that $1_A \in B$. It is unital, (resp. associative, resp. commutative) whenever A is.

EXAMPLES I.1.5.

(1) The intersection of an arbitrary family of subalgebras of a k-algebra A is again a subalgebra of A.

(2) The image of any k-algebra morphism $f : A \longrightarrow B$ is a subalgebra of B.

□

Definition I.1.6. The **center** of a k-algebra A is by definition the set

$$Z(A) = \{z \in A \mid az = za \text{ for all } a \in A\}.$$

It is a commutative subalgebra of A whenever A is associative.

Example I.1.7. The matrix algebra $\mathrm{M}_n(k)$, consisting of $n \times n$ matrices with entries from k, is a unital k-algebra with center k (we identify k with the set of scalar matrices). □

Remark I.1.8. If A is an associative unital k-algebra, then addition and product naturally endow A with a ring structure. In particular, every subalgebra of A is also a subring, and every k-algebra morphism is also a ring morphism. Moreover if $1_A \neq 0_A$ (i.e. A is not zero), k identifies with a subalgebra of $Z(A)$ (hence a subalgebra of A).

Indeed the k-bilinearity of the product law and the properties of 1_A imply that we have

$$(\lambda{\cdot}1_A)a = 1_A(\lambda{\cdot}a) = (\lambda{\cdot}a)1_A = a(\lambda{\cdot}1_A)$$

for all $a \in A$ and $\lambda \in k$, so $k{\cdot}1_A \subset Z(A)$. One may verify that $k{\cdot}1_A$ is a k-subalgebra of $Z(A)$. Hence the map

$$\begin{aligned} k &\longrightarrow Z(A) \\ \lambda &\longmapsto \lambda{\cdot}1_A \end{aligned}$$

is a non-trivial k-algebra morphism, which is injective since k is a field. □

In this book, all k-algebras will implicitly be assumed to be unital, associative, and finite-dimensional over k. Moreover, we will systematically identify k and $k{\cdot}1_A$.

Definition I.1.9. A **division** k-algebra is a k-algebra which is also a division ring (that is, every non-zero element is invertible).

At this stage, it may be worth making a few remarks on subalgebras of finite dimensional division algebras generated by a single element.

Let D be a finite dimensional division k-algebra, and let $d \in D$. We denote by $k[d]$ the smallest subalgebra of D containing d, and by $k(d)$ the smallest division subalgebra of D containing d. Clearly, we have

$$k[d] = \{P(d) \mid P \in k[X]\}.$$

Since D is finite dimensional over k, so is $k[d]$. Therefore, the successive powers of d cannot be linearly independent, and the evaluation morphism

$$ev_d : \begin{aligned} k[X] &\longrightarrow D \\ P &\longmapsto P(d) \end{aligned}$$

cannot be injective. Hence, its kernel is generated by a unique monic polynomial $\mu_{d,k} \in k[X]$, and we have an isomorphism of k-algebras

$$k[X]/(\mu_{d,k}) \cong_k k[d].$$

Since D has no zero divisors, $k[d]$ is an integral domain and $(\mu_{d,k})$ is a prime ideal, hence maximal. Thus $k[d]$ is a field, $k[d] = k(d)$ and we have

$$[k(d) : k] = \deg(\mu_{d,k}).$$

Moreover, $\mu_{d,k}$ is irreducible since it generates a maximal ideal of $k[X]$, and $\mu_{d,k}(d) = 0$.

We will use these facts without further reference from now on.

Definition I.1.10. Let D be a division k-algebra, and let $d \in D$. The polynomial $\mu_{d,k}$ is called **the minimal polynomial** of $d \in D$ over k.

We now recall the main properties of the tensor product of k-algebras.

If A and B are k-algebras, their **tensor product** $A \otimes_k B$ may be viewed as the k-vector space spanned by the symbols $a \otimes b, a \in A, b \in B$ subject to the relations:

$$(a + a') \otimes b = a \otimes b + a' \otimes b$$
$$a \otimes (b + b') = a \otimes b + a \otimes b'$$
$$(\lambda a) \otimes b = a \otimes (\lambda b) = \lambda(a \otimes b)$$

for all $a, a' \in A, b, b' \in B, \lambda \in k$. The symbols $a \otimes b$ are called **elementary tensors**.

The product on $A \otimes_k B$ is the unique product law satisfying

$$(a \otimes b)(a' \otimes b') = aa' \otimes bb' \text{ for all } a, a' \in A, b, b' \in B.$$

If $(e_i)_{i \in I}$ and $(e'_j)_{j \in J}$ are k-bases of A and B as k-vector spaces, then $(e_i \otimes e'_j)_{(i,j) \in I \times J}$ is a k-basis of $A \otimes_k B$. In particular $A \otimes_k B$ is finite-dimensional as a k-vector space if and only A and B are, and in this case we have

$$\dim_k(A \otimes_k B) = \dim_k(A) \dim_k(B).$$

Moreover, if $\varphi : A \longrightarrow C$ and $\psi : B \longrightarrow C$ are two morphisms of unital k-algebras satisfying

$$\varphi(a)\psi(b) = \psi(b)\varphi(a) \text{ for all } a \in A, b \in B,$$

there exists a unique morphism $h : A \otimes_k B \longrightarrow C$ of unital k-algebras satisfying

$$h(a \otimes 1_B) = \varphi(a) \text{ and } h(1_A \otimes b) = \psi(b) \text{ for all } a \in A, b \in B.$$

In particular, if $f : A \longrightarrow A'$ and $g : B \longrightarrow B'$ are two morphisms of unital k-algebras, there exists a unique k-algebra morphism

$$f \otimes g : A \otimes_k B \longrightarrow A' \otimes_k B'$$

satisfying

$$(f \otimes g)(a \otimes b) = f(a) \otimes g(b) \text{ for all } a \in A, b \in B.$$

If f and g are isomorphisms, so is $f \otimes g$.

Finally, if A and B are unital, the k-algebra morphisms

$$\begin{array}{c} A \longrightarrow A \otimes_k B \\ a \longmapsto a \otimes 1_B \end{array} \quad \text{and} \quad \begin{array}{c} B \longrightarrow A \otimes_k B \\ b \longmapsto 1_A \otimes b \end{array}$$

are injective.

Now let L/k be an arbitrary field extension. If A is a k-algebra and B is an L-algebra, then $A \otimes_k B$ has a natural structure of L-algebra, where the structure of L-vector space is defined on elementary tensors by

$$\lambda\cdot(a \otimes b) = a \otimes \lambda b \text{ for all } \lambda \in L, a \in A, b \in B.$$

In particular, $A \otimes_k L$ has a natural structure of an L-algebra. Moreover, $A \otimes_k L$ is finite dimensional over L if and only if A is finite dimensional over k. In this case, we have

$$\dim_L(A \otimes_k L) = \dim_k(A).$$

If A and B are unital, we have a natural isomorphism of L-algebras

$$(A \otimes_k L) \otimes_L B \cong_L A \otimes_k B.$$

Similarly, $B \otimes_k A$ and $L \otimes_k A$ have a natural structure of L-algebras, and we have an isomorphism of L-algebras

$$B \otimes_L (L \otimes_k A) \cong_L B \otimes_k A.$$

If now A and B are two unital k-algebras, we have a natural L-algebra isomorphism

$$(A \otimes_k B) \otimes_k L \cong_L (A \otimes_k L) \otimes_L (B \otimes_k L).$$

Finally, if $k \subset K \subset L$ is a tower of field extensions, we have

$$(A \otimes_k K) \otimes_K L \cong_L A \otimes_k L.$$

The justification of the tensor product properties described above is quite lengthy, so we leave the details for now. For the sake of completeness, the reader may find full constructions and proofs in Appendix A.

We end this section with an elementary lemma.

Lemma I.1.11. *Let A be a k-algebra, let $n \geq 1$ be an integer and let L/k be a field extension. Then the following properties hold:*

(1) *we have a natural k-algebra isomorphism $\mathrm{M}_n(k) \otimes_k A \cong_k \mathrm{M}_n(A)$;*
(2) *we have a natural L-algebra isomorphism $\mathrm{M}_n(k) \otimes_k L \cong_L \mathrm{M}_n(L)$.*

Proof.

(1) The k-algebra morphisms

$$\begin{aligned} \mathrm{M}_n(k) &\longrightarrow \mathrm{M}_n(A) \\ M &\longmapsto M \end{aligned} \quad \text{and} \quad \begin{aligned} A &\longrightarrow \mathrm{M}_n(A) \\ a &\longmapsto aI_n \end{aligned}$$

have commuting images, and therefore there is a unique k-algebra morphism $\varphi : \mathrm{M}_n(k) \otimes_k A \longrightarrow \mathrm{M}_n(A)$ satisfying

$$\varphi(M \otimes a) = aM, \text{ for all } M \in \mathrm{M}_n(k), a \in A.$$

Since $\mathrm{M}_n(k) \otimes_k A$ and $\mathrm{M}_n(A)$ have the same dimension over k, it suffices to prove that φ is surjective. Let E_{ij} be the matrix with coefficient 1 at row i and column j and coefficients 0 elsewhere. For any matrix $M' = (m'_{ij}) \in \mathrm{M}_n(A)$, we have

$$\varphi(\sum_{i,j} E_{ij} \otimes m'_{ij}) = M',$$

which proves the surjectivity of φ.

(2) By (1), we have an isomorphism of k-algebras $\mathrm{M}_n(k)\otimes_k L \cong_k \mathrm{M}_n(L)$. One may check that this isomorphism is also L-linear. □

REMARK I.1.12. In particular, we have a natural isomorphism

$$\mathrm{M}_m(k)\otimes_k \mathrm{M}_n(k)\cong_k \mathrm{M}_{mn}(k)$$

which maps $M\otimes N$ onto the Kronecker product of M and N. □

I.2. Central simple algebras: the basics

We now define the main object of this book.

DEFINITION I.2.1. Let k be a field. A k-algebra A is **simple** if it has no non-trivial two-sided ideals.

The next lemma gives an elementary but very useful property of simple algebras.

LEMMA I.2.2. *Let k be a field, and let $\phi : A \longrightarrow B$ be a k-algebra morphism. If A is simple, then ϕ is injective. If moreover A and B are finite dimensional over k and $\dim_k(A)=\dim_k(B)$, then ϕ is an isomorphism.*

Proof. Assume that A is simple. Since $\ker(\phi)$ is a two-sided ideal of A, we have $\ker(\phi)=(0)$ or A. The latter case cannot happen since $\phi(1)=1$. Hence ϕ is injective; the last part is clear. □

We now give examples of simple algebras.

EXAMPLES I.2.3.

(1) Any division ring D is a simple $Z(D)$-algebra.

(2) Let k be an arbitrary field. Then $\mathrm{M}_n(k)$ is a simple k-algebra.

Indeed, let J be a non-zero ideal of $\mathrm{M}_n(k)$, and let $M=(m_{ij})_{i,j}$ be a non-zero element of J. Fix two integers r,s such that $m_{rs}\neq 0$. For all $i=1,\dots,n$, we have

$$m_{rs}^{-1}E_{ir}ME_{si}=E_{ii},$$

and therefore,

$$I_n=\sum_i E_{ii}=\sum_i m_{rs}^{-1}E_{ir}ME_{si}\in J$$

since J is a two-sided ideal. Hence J contains a unit, so $J=\mathrm{M}_n(k)$.

(3) Similar arguments show that if D is a division k-algebra, then $\mathrm{M}_r(D)$ is a simple k-algebra for all $r\geq 1$.

□

We now give our first concrete example of a simple k-algebra. Let k be a field of characteristic different from 2.

Let $a,b\in k^\times$, and consider the k-linear subspace $(a,b)_k$ of $\mathrm{M}_4(k)$ generated by the matrices

$$I_4=\begin{pmatrix}1&0&0&0\\0&1&0&0\\0&0&1&0\\0&0&0&1\end{pmatrix}, i=\begin{pmatrix}0&a&0&0\\1&0&0&0\\0&0&0&a\\0&0&1&0\end{pmatrix},$$

$$j = \begin{pmatrix} 0 & 0 & b & 0 \\ 0 & 0 & 0 & -b \\ 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \end{pmatrix}, ij = \begin{pmatrix} 0 & 0 & 0 & -ab \\ 0 & 0 & b & 0 \\ 0 & -a & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}.$$

Straightforward computations show that these matrices are linearly independent over k, and that we have

$$i^2 = a, j^2 = b, (ij)^2 = -ab \text{ and } ji = -ij.$$

It easily follows that $(a,b)_k$ is a k-subalgebra of $\mathrm{M}_4(k)$ of dimension 4 over k.

DEFINITION I.2.4. Let k be a field of characteristic different from 2. The k-algebra $(a,b)_k$ is called a **quaternion k-algebra**.

PROPOSITION I.2.5. *Let k be a field of characteristic different from 2. For every $a, b \in k^\times$, the k-algebra $(a,b)_k$ is a simple k-algebra, with center isomorphic to k.*

Proof. Let us first determine the center of $(a,b)_k$.

Let $q_1 = x + yi + zj + tij \in (a,b)_k$ and assume that $q_1 \in Z((a,b)_k)$. Then we have

$$iq_1 = i(x + yi + zj + tij) = xi + ay + zij + taj$$

and

$$q_1 i = (x + yi + zj + tij)i = xi + ay - zij - taj.$$

Since by assumption $iq_1 = q_1 i$, we have therefore $z = t = 0$ and thus $q_1 = x + yi$. Since we have $jq_1 = q_1 j$, we get $xj - yij = xj + yij$ in a similar way, so $y = 0$ and $q_1 = x \in k$. Hence $Z((a,b)_k) = k$.

Let us prove now that $(a,b)_k$ is simple. For, let I be a non-zero two-sided ideal of $(a,b)_k$, and let $q_1 = x + yi + zj + tij \in I, q_1 \neq 0$. We then have

$$\frac{1}{2}(iq_1 - q_1 i) = zij + taj \in I \text{ and } \frac{1}{2}(iq_1 + q_1 i) = xi + ay \in I.$$

Since by assumption x, y, z or t is non-zero, it follows that $zij + taj$ or $xi + ay$ is non-zero. Assume for example that $q_2 = zij + taj$ is not zero, that is $z \neq 0$ or $t \neq 0$. We have

$$\frac{1}{2}(jq_2 - q_2 j) = -bzi \in I \text{ and } \frac{1}{2}(jq_2 + q_2 j) = tab \in I.$$

If $t \neq 0$, then $tab \in k^\times$ is a unit of $(a,b)_k$; if $z \neq 0$, then $-bzi \in k^\times$ is a unit of $(a,b)_k$ (with inverse $-(abz)^{-1}i$). In both cases, I contains a unit, so $I = (a,b)_k$. The case $xi + ay \neq 0$ may be dealt with in a similar way and is left to the reader. □

REMARK I.2.6. Later on, we will see a criterion to decide whether or not $(a,b)_k$ is a division algebra. For the moment, let us just point out that it can actually be a division algebra for some well-chosen values of a and b. For example, if $k = \mathbb{R}$ and $a = b = -1$, we obtain the Hamilton quaternion algebra $\mathbb{H}$, which is known to be a division ring. We will recover this fact in the next chapter. □

DEFINITION I.2.7. A k-algebra A is called **central** if $Z(A) = k$. A **central simple** k-algebra is a k-algebra which is central and simple.