UNIVERSIDAD SAN FRANCISCO DE QUITO USFQ

Colegio de Ciencias e Ingenierías

Una demostración algebraica del teorema de Frobenius sobre las álgebras asociativas de división sobre los números reales

Artículo académico

.

Fernando Xavier Vinueza Fiallos

Licenciatura en matemáticas

Trabajo de titulación presentado como requisito
para la obtención del título de
Licenciado en matemáticas

Quito, 17 de mayo de 2017

UNIVERSIDAD SAN FRANCISCO DE QUITO USFQ

COLEGIO DE CIENCIAS E INGENIERÍAS

HOJA DE CALIFICACIÓN
DE TRABAJO DE TITULACIÓN

Una demostración algebraica del teorema de Frobenius sobre las álgebras asociativas de división sobre los números reales

Fernando Xavier Vinueza Fiallos

Calificación: ______________________________

Nombre del profesor, Título académico John R. Skukalek Ph.D

Firma del profesor ______________________________

Quito, 17 de mayo de 2017

Derechos de Autor

Por medio del presente documento certifico que he leído todas las Políticas y Manuales de la Universidad San Francisco de Quito USFQ, incluyendo la Política de Propiedad Intelectual USFQ, y estoy de acuerdo con su contenido, por lo que los derechos de propiedad intelectual del presente trabajo quedan sujetos a lo dispuesto en esas Políticas.

Asimismo, autorizo a la USFQ para que realice la digitalización y publicación de este trabajo en el repositorio virtual, de conformidad a lo dispuesto en el Art. 144 de la Ley Orgánica de Educación Superior.

Firma del estudiante:	_______________________________________
Nombres y apellidos:	Fernando Xavier Vinueza Fiallos
Código:	00128245
Cédula de Identidad:	0603066507
Lugar y fecha:	Quito, mayo de 2017

RESUMEN

En este artículo demostramos el Teorema de Frobenius sobre las álgebras asociativas de división sobre los números reales. Este teorema dice que ``cualquier álgebra asociativa de división de dimensión finita sobre los números reales es isomorfa a los números reales, los números complejos o los cuaterniones”. La demostración de este teorema se ha hecho para que sea fácil de entender para los estudiantes avanzados de matemáticas de pregrado. Consecuentemente, no usamos la teoría de módulos semisimples, el teorema centralizador y el radical de Jacobson como los libros de posgrado de matemática lo hacen; en vez de eso, nosotros nos limitamos a usar solamente la teoría de las álgebras centrales simples y la herramienta del producto tensorial de módulos y K-álgebras. Nosotros demostramos este teorema al trabajar en los casos no conmutativo y conmutativo. Adicionalmente, para determinar un isomorfismo a los cuaterniones, nosotros demostramos y usamos el clásico teorema de Skolem-Noether.

Palabras clave: Teorema de Frobenius, módulos, álgebras, álgebras de división, álgebras centrales simples, producto tensorial, K-álgebras, teorema de Skolem-Noether.

ABSTRACT

In this article we prove the Frobenius' theorem on associative division algebras over the Real Numbers which says that ``any finite dimensional associative division algebra of finite dimension over the real numbers is isomorphic to either the real numbers, complex numbers or quaternions". This proof of Frobenius' theorem is intended to be easy to understand for advanced undergraduate mathematics students. Thus we don't use the theory of semisimple modules, the centralizer theorem, and the Jacobson radical as graduate books do; instead, we limit ourselves to use only the theory of central simple algebras, and the machinery of tensor product of modules and K-algebras. We prove this theorem by working in the noncommutative and commutative case. Additionally, to determine an isomorphism to quaternions we prove and use the classical form of Skolem-Noether theorem.

Key words: Frobenius' theorem, modules, algebras, division algebras, central simple algebras, tensor product, K-algebras, Skolem-Noether theorem.

An Algebraic Proof of Frobenius' Theorem on Associative Division Algebras over the Real Numbers

Fernando X. Vinueza Fiallos

May 17, 2017

Abstract

In this article we prove the Frobenius' theorem on associative division algebras over the Real Numbers which says that "any finite dimensional associative division algebra of finite dimension over the real numbers is isomorphic to either the real numbers, complex numbers or quaternions". This proof of Frobenius' theorem is intended to be easy to understand for advanced undergraduate mathematics students. Thus we don't use the theory of semisimple modules, the centralizer theorem, and the Jacobson radical as graduate books do; instead, we limit ourselves to use only the theory of central simple algebras, and the machinery of tensor product of modules and K-algebras. We prove this theorem by working in the noncommutative and commutative case. Additionally, to determine an isomorphism to quaternions we prove and use the classical form of Skolem-Noether theorem.

Contents

List of Figures

1 Introduction

Every classification theorem is important in mathematics because it allows us to know exactly with what we are working. The example, which every undergraduate learns, is the classification of finite simple groups; a good review of this classification was done by Ron Solomon in the Notices of the AMS (Solomon, 1995). In this article we are going to classify the finite-dimensional associative division algebras over the field of real numbers. In the preliminaries section we will define the finite-dimensional associative division algebras over a field and later we will use as a field the real numbers.

The real numbers have been known in mathematics for centuries and many people were involved in their invention. The complex numbers were discovered by Cartan when he did research in solutions to cubic equations and later Gauss gave them the form we know today (the complex plane). The quaternions were invented by Sir William Rowan Hamilton, an Irish mathematician, who lived in the first half of the 19th century. Complex numbers can be used to represent rotations in the cartesian plane, something that Hamilton wanted to achieve with $\mathbb{R}^3$ in order to extend the complex numbers. During his research Hamilton first discovered what is now known as the quaternion group Q_8, which preceeded the discovery of the quaternions. He published the latter in his book "Lectures on Quaternions: containing a systematic treatment of A New Mathematical Method"(Hamilton, 1853), which was communicated to the Royal Irish Academy.

Throughout history there have been many proofs of Frobenius' Theorem. The first one was done by Frobenius himself in 1878 at the end of an algebraic paper that he published (Frobenius, 1878). Another proof was given by C.S. Pierson in 1881 of which there is a review and explanation by Thomas McLaughlin in his paper (McLaughlin, 2004). The shortest known proof was given by L.E. Dickson, who was an U.S. algebraist and number theorist, in his book(Dickson, 1914). After Dickson, other proofs appeared that used advanced mathematical machinery and were conceptual in nature.

Up until Dickson's proof in 1914, all proofs were mostly computational. This means that they relied more on the explicit construction of the algebras rather than on their inner structure. The most advanced computational proof was made by Dickson, where he used the fundamental theorem of algebra to build extensions of the real numbers isomorphic to the complex numbers, and then he built the quaternions. As part of his proof, Dickson concluded that 3-dimensional associative division algebras were not possible because of linear independence of imaginary units and the hypothesis of associativity and divisibility. Additionally, if one considers the algebras of dimension greater than 5 then a contradiction arises where any supposedly new imaginary unit outside the quaternions must in fact be in the quaternions.

After Dickson's proof appeared many new proofs that used tools of new algebraic theories, developed with the aim to generalize the quaternions. For example the developement of "the theory of semisimple artinian rings and central simple algebras" (Herstein, 1971). In the twentieth century "there were other approaches to this theorem but in different classification contexts"(Lam, 2001) because they used methods from analysis, algebraic topology and even algebraic geometry. For example we have: "Gel'fand Mazur theorem for commutative Banach division algebras"(Lam, 2001, p. 208), "Hopf's Theorem on commutative nonassociative real division algebras"(Lam, 2001, p. 208), "Kervaire-Milnor Theorem for nonassociative real division algebra"(Lam, 2001, p. 208), etc.

The proof of Frobenius' Theorem given in this article is purely algebraic, done in a classical setting because we limit ourselves to use only the theory of central simple algebras and the machinery of tensor product of modules and K-algebras. We do not use the theory of semisimple modules, the centralizer theorem and the Jacobson radical because they involve too much generalization of the mathematical theory we need. For more information on these theories see the books by Herstein, Farb and Dennis, and T.Y Lam on the bibliography. The theory of central simple algebras will help us understand why the quaternions are the only noncommutative algebra in Frobenius' Theorem.

2 Preliminaries

Before we begin the proof of our main theorem we should know what a module and an algebra are, since they are the main general structures we are going to use. After that, we are going to define finite-dimensional associative division algebras, which will help us understand the structure of the real numbers, complex numbers and quaternions as algebras. Finally, in this section we will present the algebra of octonions, which is an algebra containing the quaternions but it is not associative.

2.1 Standard terminology for homomorphisms of groups

We assume that the reader is already familiar with homomorphisms of groups. Here we give standard terminology for homomorphisms of groups, which the reader may have not seen before. The next list is taken from the book Abstract Algebra by Choudhary (Choudhary, 2008):

1. A **monomorphism** is an injective homomorphism.

2. An **epimorphism** is a surjective homomorphism.

3. An **isomorphism** is a bijective homomorphism.

4. An **endomorphism** is a homomorphism from a group to itself.

5. An **automorphism** is an isomorphism from a group to itself.

2.2 Ring

It is assumed that the reader is already familiar with rings, specifically with two-sided ideals (which we will just refer as ideals), left ideals and right ideals, quotient rings, and isomorphism theorems. However, we present here the definition of ring, ideal, left ideal, and right ideal.

Definition 2.1. A **ring** R is an additive abelian group $(R, +)$ with another binary operation called multiplication $(R, \cdot)$ satisfying the following conditions:

1. The multiplication is **associative**.

2. The multiplication has the **distributive property** with respect to addition. That is, for all $x, y, z \in A$ we have
   $(x + y) \cdot z = x \cdot z + y \cdot z$ and $x \cdot (y + z) = x \cdot y + x \cdot z$

Note that the multiplication operation is not assumed to be commutative nor have a multiplicative identity. Let R be a ring and let $1 \in R$ denote the multiplicative identity with the property $r \cdot 1 = 1 \cdot r = r$ for any $r \in R$. This multiplicative identity is unique. Also we denote the identity element of the additive group of the ring by 0. Many objects used in mathematics are rings. As examples we have:

1. The set of equivalence classes of integers modulo n. The sum is sum modulo n and multiplication is multiplication modulo n.

2. The integers themselves with usual sum and multiplication.

3. The set of nxn matrices with entries in the real numbers is a ring with operations of ordinary sum and multiplication of matrices.

For notation purposes we change the multiplication notation from $x \cdot y$ to xy. Let R be a ring. A **subring** B is a subset of the ring R that is also a ring with the same operations as the ring R. A **left ideal** I is a subgroup of the additive group of the ring R such that $ri \in I$ for all $r \in R$ and $i \in I$; a **right ideal** and a **two sided ideal** (which we refer to as an ideal) are defined in a similar way.

Let $X \subseteq R$ be a non-empty subset of R. The set $\langle X \rangle$ is the minimal ideal that contains X if $\langle X \rangle$ is defined as the set of all finite sums $RXR = \{\Sigma_{i=0}^{n} x_i t y_i | x_i, y_i \in R\}$. An ideal generated by a singleton set is called a **principal ideal**. The ring R is called a **commutative ring** if $rt = tr$ for all $r, t \in R$.

Later on, we will work exclusively with algebras that have the property of being associative with multiplicative identity, these algebras will be defined after the module subsection. Books of noncommutative algebra and noncommutative rings such as Farb and Dennis', and Lam's even define rings to have multiplicative identity, because the definition of associative algebras over a field requires them to also be rings with identity.

For the previous reasons we will also work on the same conditions of non-commutative algebra and non-commutative rings books. From now on in this article we always assume that rings have multiplicative identity 1 and are not necessarily commutative. This convention will also help us to not be redundant on this condition for rings throughout this article.

Let R be a ring. An element $a \in R$ is called a **unit** if it has a multiplicative inverse a^{-1} with the property $aa^{-1} = a^{-1}a = 1$. A **division ring** is a ring where all non-zero elements are units. A **field** is a commutative division ring.

Definition 2.2. A non-zero ring R is called a **simple ring** if R has no ideals except 0 and R.

Notice that simple rings could have non-trivial left ideals or right ideals. Here we present some examples that clarify this issue:

1. Any division ring is a simple ring and has no non-trivial left ideals or right ideals.
2. An *nxn* matrix ring over a division ring is a simple ring. It also has non-trivial left ideals containing all matrices with all columns equal to 0 except one column with entries of the division ring.

We assume the reader is already familiar with the definition of **ring isomorphism** between two rings R and W, we denote this ring isomorphism by $R \cong W$. We finish this section by giving the definition of the center of a ring.

Definition 2.3. Let R be a ring. The **center** of the ring R is the subset of R that contains all $x \in R$ such that $rx = xr$ for all $r \in R$.

We remind the reader the following definitions concerning fields, also we assume familiarity with an extension field of a field F. First we have an "algebraically closed or algebraically complete field"(Ames, 1969, p. 177)

Definition 2.4. Let F be a field. F is called **algebraically closed** or **algebraically complete** if every polynomial equation

$$a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0 = 0$$

where $a_i \in F$ and not all $a_i \neq 0$, has all its roots in F.

The following definitions can be found on pages 288-289 of Ames' book.

Definition 2.5. Let E be an extension field of a field F. An element $\beta \in E$ is said to be **algebraic over F** if β is a root of a polynomial with coefficients in F.

Definition 2.6. Let E be an extension field of a field F. E is called **algebraic over F** if every $\beta \in E$ is algebraic over F.

We also give the important definition of "an algebraic closure of a field"(Dummit & Foote, 2004, p. 543). In Dummit and Foote there is a proof that an algebraic closure of a field F is unique up to isomorphism.

Definition 2.7. The field $\overline{F}$ is called **an algebraic closure of the field F** if $\overline{F}$ is algebraic over F and $\overline{F}$ is algebraically closed.

2.3 Module

Another important structure is a module over a ring R. Modules are a generalization of vector spaces because vector spaces are modules over a field.

Definition 2.8. A left module M over a ring R or left R-module M is an abelian group, written additively, together with an operation of R on M such that for all $a, b \in R$ and $x, y \in M$ we have:

1. $a(x + y) = ax + ay$.
2. $(a + b)x = ax + bx$.
3. $(ab)x = a(bx)$.
4. $1x = x$.

Let M be a left R-module, let $a \in R$ and $m \in M$ arbitrary. We use for now the notation 0_R for the zero scalar and 0_M for the zero vector to show the relation that they have:

1. $0_R m = 0_M$.
2. $a0_M = 0_M$.
3. The following property can be proved just like with rings: $(-a)m = -(am) = a(-m)$.

We can now simply denote 0_R to 0 and 0_M to $\mathbf{0}$ and we will not use subscripts on the identity of the abelian group when it is clear by the context that we are using it. Next we have some examples of modules:

1. The real vector space $\mathbb{R}^n$ is a left $\mathbb{R}$-module.
2. Any left ideal of a ring R is a left R-module.
3. Any ring R is a $\mathbb{Z}$-module where the operation of $\mathbb{Z}$ is $nr = r+r+r+..+r$ the n^{th} sum of any element $r \in R$. Notice for $n < 0$ we have $(-n)r = -1(nr) = -r - r - r - ... - r$ and for $n = 0$ we have $0r = 0$.

Let R be a ring. If M is a left R-module we will denote this module by ${}_RM$; similarly, if M is a right R-module we will denote it by M_R. The ring R^{op} is called the **opposite ring of R** if it has the same elements and additive group structure as R but with multiplication defined by $a \cdot b = ba$ for all $a, b \in R$. From any left R-module we can define a right R^{op}-module where the action is given by $mr := rm$, and a similar situation happens for right R-modules.

Any ring R is a left module over itself, where the action of R is the same as multiplication in R, and R is called a **left regular module**. From now on **if we say modules then we refer to left modules unless otherwise specified**, without raising confusion.

> **Definition 2.9.** A subset T of an R-module M is called a **submodule** of M if it is a subgroup of the additive group of M and $rt \in T$ for all $r \in R$ and $t \in T$.

Let M be an R-module, then, we denote the **trivial submodule** of M by $\{0\}$. We notice that submodules are closed under scalar multiplication.

> **Definition 2.10.** Let M be an R-module. The set $Ann(M) = \{r \in R | rm = 0 \quad \forall m \in M\}$ is called the **annihilator** of M.

Examples of annihilators:

1. In the $\mathbb{R}$-module $\mathbb{R}^n$ the annhiliator is $Ann(\mathbb{R}^n) = \{0\}$.
2. For a matrix ring $M_n(D)$over a division ring D as a D module we have $Ann(M_n(D)) = 0$.
3. The $\mathbb{Z}$-module Z_{15} with the operation $m * [n] = [mn]$ has annhiliator $15\mathbb{Z}$. This operation is well-defined, which we will prove in the next subsection.

The annhiliator of an R-module M is an ideal of R. To show this, let $r \in Ann(M)$ and $b \in R$ arbitrary. We have that $Ann(M)$ is an additive subgroup of R;furthermore, for any $m \in M$ we have $(rb)m = r(bm) = 0$ and $(br)m = b(rm) = 0$ thus $Ann(M)$ is an ideal of R.

> **Definition 2.11.** Let M be a R-module. We say that M is a **simple module** if $M \neq \{0\}$ and the only submodules of M are the trivial submodule $\{0\}$ and M itself.

Let M be an R-module. M is called a **faithful module** if $Ann(M) = 0$. We can easily check that any non-zero module over a division ring be faithful.

2.3.1 Factor theorem and first isomorphism theorem

One way to form a new module from a given module and its submodules is the **quotient module**. Let M be a module over R and N any submodule of M. Since M is an abelian group then all its subgroups N are normal; consequently, we can form the quotient group M/N in the usual way.

We define the module operation on M/N by $r[y] = [ry]$ for all $r \in R$ and $[y] \in M/N$. We prove that the module operation is well defined by showing that it does not depend on the choice of the representative $[x] \in M/N$. Recall M and N are R-modules. Let $[x] \in M/N$ arbitrary and let $w, t \in [x]$ arbitrary, we have $w - t \in N$ thus $rw - rt \in N$. We have $[rw] = [rt]$, thus $r[w] = r[t]$ for any two representatives of $[x]$. Therefore the module operation on M/N is well-defined.

Now we are going to define homomorphisms of modules.

Definition 2.12. Let M and N be any two R-modules. An ***R*-module homomorphism** or an R-linear mapping from M into N is a mapping $f : M \longrightarrow N$ such that for all $m \in M$ and $r \in R$ we have:

1. $f(m_1 + m_2) = f(m_1) + f(m_2)$
2. $f(rm) = r\, f(m)$

Definition 2.13. Let M and N be any two R-modules and $f : M \longrightarrow N$ any R-module homomorphism. The R-module homomorphism f is called an **R-module isomorphism** if f is a bijective mapping. We denote an R-module isomorphism of M and N by $M \cong N$.

We also have the canonical map $\varphi : M \longrightarrow M/N$ which is an R-module homomorphism with kernel N. In this article we will only use two isomorphism theorems for modules: the factor theorem and the first isomorphism theorem. Details for the remaining two can be found in Choudhary's book (Choudhary, 2008). The proofs of the isomorphism theorems for modules are carried out the same way for groups, and thus we state them here without proof.

Theorem 2.14 (Factor Theorem)**.** Let M and W be modules over R. Let f be any R-module homomorphism $f : M \longrightarrow W$ with kernel N. For any submodule N' of the kernel N the module homomorphism f can be factored through M/N', that is, there is a unique module homomorphism $\overline{f} : M/N' \longrightarrow W$ such that $\overline{f} \circ \varphi = f$ where φ is the canonical map.

From the factor theorem we prove the first isomorphism theorem of modules simply by letting $N' = N$.

Corollary 2.15 (First isomorphism Theorem)**.** Let M and W be modules over R. Let f be any R-module homomorphism $f : M \longrightarrow W$ with kernel N. The module homomorphism f can be factored through M/N, that is, there is a unique module homomorphism $\overline{f} : M/N \longrightarrow W$ such that $\overline{f} \circ \varphi = f$ where φ is the canonical map.

2.3.2 Endomorphism ring of modules

In this subsection we will show that there is another way to understand these modules by using the endomorphism ring of their additive abelian structure. Let M and N be any two R-modules. The set of all R-module homomorphisms from M to N is an R-module and it is denoted by $Hom_R(M, N)$. If the homomorphism is from the module to itself, instead of writing $Hom_R(M, M)$ we write $End_R(M)$. Additionally, we note that $End_R(M)$ is also a ring with operation of sum, composition of endomorphisms, and multiplicative identity equal to the identity mapping. We notice that when R is a field we have the well known definition of an R-linear transformation between two vector spaces.

Definition 2.16. The **endomorphism ring** of an R-module M is the set of all R-module endomorphism of M, denoted $End_R(M)$, with ring operations of sum of endomorphisms, and multiplication defined as composition of endomorphisms.

We note that the identity mapping is the multiplicative identity of $End_R(M)$. We follow the same convention for composition of endomorphisms as noncommutative algebra books, that is, given arbitrary $f, g \in H = End_R(M)$ instead of writing $(f \circ g)(m)$ we write $(m)gf$ so M is naturally a right H-module; the same procedure is applied to right R-modules and their endomorphism ring. We follow this convention to avoid the formation of opposite rings. Now we give some examples of endomorphism rings:

1. Fixing a basis for a vector space V of dimension $\mathbf{n}$ over a field K, we have that $End_K(V) \cong M_n(K)$, which is easily proved using basic linear algebra.

2. We shall prove later that the endomorphism ring of a ring (with identity) over itself is isomorphic to the ring itself.

3. The endomorphism ring of any simple R-module M is a division ring.

Now we give another way to look at a left R-module M by using its endomorphism ring. Let $End(M)$ be the ring of endomorphisms of the additive group M with ring operations of sum of mappings and compositions using our convention. Given any $r \in R$ we have the endomorphism ${}_rT \in End(M)$ defined by

$$\begin{aligned} {}_rT : M &\longrightarrow M \\ x &\mapsto rx. \end{aligned}$$

The map

$$\begin{aligned} \phi : R &\longrightarrow End(M) \\ r &\mapsto {}_rT \end{aligned}$$

is a ring homomorphism. Hence, we may view an R-module as an additive abelian group together with the ring homomorphism ϕ.

Definition 2.17. An R-D **bimodule** M is a left R-module and a right D-module such that for any $m \in M$, $r \in R$ and $d \in D$ we have $(rm)d = r(md)$.

For bimodules we also have homomorphisms.

Definition 2.18. Let M and N be R-D bimodules. An **R-D bimodule homomorphism** is a mapping $f : M \longrightarrow N$ such that f is a left R-module homomorphism and a right D-module homomorphism. For all $m \in M$, $r \in R$ and $d \in D$ we have:

1. $f(m_1 + m_2) = f(m_1) + f(m_2)$.
2. $f(rmd) = r(f(m))d$.

Remark. Every ring R is a R-R bimodule, called a **regular bimodule**.

2.3.3 Direct product and direct sum

To define the direct product and direct sum of modules we need first their analogous definitions for groups because modules have the structure of abelian groups. We remind the reader that we are using definitions found in Lang's Algebra book (Lang, 2005).

Definition 2.19. Let G_1 and G_2 be groups. The **direct product** of G_1 and G_2 is the group $G_1 \times G_2$ consisting of all elements of the cartesian product of G_1 and G_2 , i.e all the pairs (x, y) where $x \in G_1$ and $y \in G_2$, with group operation defined component-wise by $(x_1, y_1)(x_2, y_2) = (x_1x_2, y_1y_2)$

We define the direct product of n groups similarly.

> Let A and I be two sets. By a **family** of elements of A, indexed by the set I, we mean a mapping $f : I \longrightarrow A$. Thus, for each $i \in I$ we are given an element $f(i) \in A$. Although a family does not differ from a mapping, we think of it as determining a collection of objects from A, and we write it often as
>
> $$\{f(i)\}_{i \in I}$$

or

$$\{a_i\}_{i\in I}$$

writing a_i instead of $f(i)$. We call I the indexing set (Lang, 2005, p. x).

Even more generally, for any indexing set I and any family of groups $\{G_i\}_{i\in I}$ we define the direct product $G = \prod G_i$ as the set consisting of all families $(x_i)_{i\in I}$ such that $x_i \in G_i$, where the group operation is component-wise, that is, if $(x_i)_{i\in I}$, $(y_i)_{i\in I} \in G$ then $(x_i y_i)_{i\in I} \in G$.

Definition 2.20. Let $(A_i)_{i\in I}$ be a family of abelian groups. The **direct sum** of $(A_i)_{i\in I}$ denoted $A = \bigoplus_{i\in I} A_i$ is the subset of $\prod A_i$ consisting of all families $(a_i)_{i\in I}$ with $x_i \in A_i$ such that $x_i = 0$ for all but a finite number of indices $i \in I$.

The direct sum of abelian groups has a very useful property called the **universal property of the direct sums**. It says that any group homomorphisms of the direct summands of a direct sum to another fixed group can be extended to a unique homomorphism of the whole direct sum to that fixed group. More precisely we have:

Let I be the indexing set of the direct sum $A = \bigoplus_{i\in I} A_i$ and let $\{\nu_i : A_i \longrightarrow A\}_{i\in I}$ be a family of homomorphisms of each direct summand A_i to the direct sum A such that ν_i maps $x \in A_i$ to the i^{th} component of the family $(x_i)_{i\in I}$ and having all other components equal to zero. Hence, each ν_i is an injective homomorphism and is called in the literature the **canonical injection of A_i into the direct product A** .

Proposition 2.21. Let $\{f_i : A_i \longrightarrow B\}_{i\in I}$ be a family of group homomorphisms into an abelian group B. Let $A = \bigoplus_{i\in I} A_i$ then there exists a unique group homomorphism

$$f : A \longrightarrow B$$

such that $f \circ \nu_i = f_i$ for all $i \in I$

Proof. Let

$$\begin{aligned} f : A &\longrightarrow B \\ (x_i)_{i\in I} &\longmapsto \sum_{i\in I} f_i(x_i) \end{aligned}$$

we notice that this sum is finite by definition of direct sum and that $f \circ \nu_i = f_i$ for all $i \in I$. Furthermore, f is uniquely determined because its values depend on the family of homomorphisms $f_i : A_i \longrightarrow B$ and any of these homomorphisms maps 0 in A_i to 0 in B. Suppose we have another homomorphism

$$\begin{aligned} h : A &\longrightarrow B \\ (x_i)_{i\in I} &\longmapsto \sum_{i\in I} f_i(x_i) \end{aligned}$$

then we have $f \circ \nu_i = h \circ \nu_i$. We make the sum over any element $(x_i)_{i\in I}$ of the direct sum $A = \bigoplus_{i\in I} A_i$ to obtain

$$\sum_{i\in I} f(\nu_i(x_i)) = \sum_{i\in I} h(\nu_i(x_i))$$

but we also have the following equations given by definition of the homomorphisms f and h

$$\begin{aligned} \sum_{i\in I} f(\nu_i(x_i)) &= \sum_{i\in I} f_i(x_i) \\ \sum_{i\in I} h(\nu_i(x_i)) &= \sum_{i\in I} h_i(x_i) \end{aligned}$$

which implies

$$\sum_{i\in I} f_i(x_i) = \sum_{i\in I} h_i(x_i)$$

Since $(x_i)_{i\in I} \in A$ is arbitrary we have $f = h$. Therefore f exists and is unique. □

Now we can define an R-module structure on $A = \bigoplus_{i\in I} A_i$ by setting the scalar multiplication component-wise. Let $r \in R$ and $(x_i)_{i\in I} \in A$ arbitrary, then

$$r(x_i)_{i\in I} = (rx_i)_{i\in I}$$

It is trivial to show that A is indeed an R-module. Also, the universal property of the direct sum of groups then becomes the universal property for the direct sum of modules. We also have the **canonical projection**, which is a homomorphism of a module onto its quotient by a submodule.

Definition 2.22. Let M be a module over R and N a submodule of M. The *canonical projection* of M by N is the homomorphism $\pi : M \longrightarrow M/N$ given by $x \mapsto x + N$

For example, we can project a direct sum of modules onto any module component of the direct sum by the R-module homomorphism

$$f : \bigoplus_{i \in I} A_i \longrightarrow \bigoplus_{i \in I} A_i$$
$$(x_1, x_2, ..., x_j, ..., x_n) \mapsto (0, 0, ..., x_j, ..., 0, 0)$$

or onto a direct sum of a subset of module components.

2.3.4 Descending chain condition (left artinian module)

Suppose M is a left module over R and let $N_1 \supseteq N_2 \supseteq N_3 \supseteq ...$ be a descending sequence of submodules of M. We say that the descending sequence **stabilizes** if for some n we have $M_n = M_{n+1} = M_{n+2} = M_{n+3} = ...$

Definition 2.23. A left module M over R is called **left artinian** if any descending sequence of modules stabilizes.

It is not hard to notice that any descending sequence has a minimal non-trivial submodule.

Definition 2.24. Let R be a ring. R is called left artinian if it is left artinian as a module over itself.

2.3.5 Generating set and linear independence

Let S be a subset of a module M over R. A linear combination of elements of S with coefficients in R is a sum

$$\sum_{y \in S} a_y y$$

where $\{a_y\}$ is a subset of R and **all but a finite number** of a_y are zero.

Definition 2.25. Let S be a subset of a module M over R. **S is a spanning or generating set for M over R**, similarly we say that S spans or generates M over R if each $y \in M$ can be written as a **linear combination** of elements of S with coefficients in R.

Let M be an R-module and T a generating set of M over R. The module M is said to be **finitely-generated**, **finite type** or **finite** over R if M has a finite number of generators, i.e T is a finite subset of M. Next we show some examples of modules over a ring that have no finite generating set and others that do.

1. Let M be the additive group of rational numbers. If we make M a $\mathbb{Z}$-module, then M has no finite generating set. Any finite set of rational numbers can be transformed to a finite set of integers which is not linearly dependent over $\mathbb{Z}$.

2. Consider the polynomial ring M in one indeterminate X with rational coefficients. M is a $\mathbb{Q}$-module. The set of all powers of the indeterminate X generates M as a $\mathbb{Q}$-module.

Definition 2.26. Let T be a subset of a module M over R. T is a **linearly independent** set of M over R if for any linear combination $\sum_{y \in T} a_y y = 0$ implies $a_y = 0$ for all $y \in T$.

We say that a subset T of an R-module M is **linearly dependent** if it is not linearly independent. Now we show some examples of linearly dependent sets and linearly independent sets.

1. Any subset of the $\mathbb{Z}$-module $\mathbb{Q}$ is linearly dependent because any linear combination in $\mathbb{Q}$ can be converted to a linear combination in $\mathbb{Z}$, which itself is linearly dependent because $\mathbb{Z}$ is generated by 1 as a $\mathbb{Z}$-module.

2. Let M be a faithful finitely generated R-module with m generators. The direct product of modules M^n is an R-module generated by mn elements.

Definition 2.27. Let W be a subset of an R-module M. W is a **basis** of M over R if W is a generating set of M over R and W is a linearly independent set.

A module M over a division ring or over a field with finite basis is called a **finite-dimensional** vector space over a division ring or over a field. Next we give examples of modules with a basis:

1. $\mathbb{R}^3$ has a basis.

2. Any polynomial ring over a field has a basis, e.g the set $\{x^0, x^1, x^2, ...\}$.

2.3.6 Free module

Definition 2.28. An R-module M is called **free module** if M admits a basis or is the zero module.

Let I be an indexing set, R a ring and let $\{R_i\}_{i \in I}$ be a family of R-modules which are all R-module isomorphic to the ring R viewed as a regular module. The direct sum

$$F = \bigoplus_{i \in I} R_i$$

admits a basis which consists of the elements e_i whose i^{th} coordinate is the unit of R_i (recall that it is isomorphic to the regular module R) and having all other components equal to zero.

Definition 2.29. Let M be an R-module. M is called a **cyclic module** if M is generated by some singleton subset of M.

Similarly, if $B = \{b_i\}_{i \in I}$ is a basis of an R-module M, then we can view M as the direct sum of cyclic modules $\{Rb_i\}_{i \in I}$ where we have the R-module isomorphism of Rb_i and R for all $i \in I$ because of the linear independence of the basis B. Thus we have a nice way of viewing a free module M as a direct sum of isomorphic copies of the regular module R.

Now we define a **free module** over a ring A **generated by a non-empty set** S, notice S is not necessarily a subset of A. This definition can be found in (Lang, 2005) on page 137.

> Let $A < S >$ be the set of all mappings $\varphi : S \longrightarrow A$ such that $\varphi(x) = 0$ for all but a finite number of x. Let $x \in S$ and $a \in A$, we denote by ax the map φ such that $\varphi(x) = a$ and $\varphi(y) = 0$ for $x \neq y$. Now given $\varphi \in A < S >$ there exists elements $x_i \in S$ and $a_i \in A$ such that
>
> $$\varphi = a_1x_1 + a_2x_2 + ... + a_nx_n$$
>
> The above expresion is unique because of the linear independence of the mappings ax. The set $A < S >$ is an additive abelian group by sum of mappings and is an A-module by the operation $a\varphi = aa_1x_1 + aa_2x_2 + ... + aa_nx_n$. It is immediately verified that the set of functions $\{\theta_x \mid x \in S\}$ such that $\theta_x(x) = 1$ and $\theta_x(y) = 0$ for $x \neq y$ is a basis for $A < S >$ as A-module (Lang, 2005).

Now let N be an A-module, let $g : S \longrightarrow N$ be a mapping of S into the A-module N and let the map $f : S \longrightarrow A < S >$ be such that $f(x) = 1x$. Observe that f is injective. We can define an A-module homomorphism

$$\begin{aligned} &g_* : A < S > \longrightarrow N \\ &g_*(\sum_{x \in S} a_x x) = \sum_{x \in S} a_x g(x) \end{aligned}$$

Furthermore we have $g_* \circ f = g$ and g_* is the only homomorphism with this property because we must have $g_*(1x) = 1g(x) = g(x)$.

2.3.7 Tensor product of modules

Before proceeding with the definition of tensor product of modules it will be useful to know the motivation for its definition. Tensor product of modules involves the notion of a multilinear mapping of modules and it is in there where the motivation of its definition comes from. Thus we should begin with the definition of a bilinear mapping of modules, which is a special case of a multilinear mapping of modules.

> **Definition 2.30.** Let R be a commutative ring. Let E, N, F be R-modules. Let $E \times N$ be the cartesian product of E and N. A **bilinear map** is a map $g : E \times N \longrightarrow F$ such that
>
> 1. For a fixed $x_o \in E$ the map $(x_o, y) \mapsto g(x_o, y)$ is R-linear in the indeterminate y.
> 2. For a fixed $y_o \in N$ the map $(x, y_o) \mapsto g(x, y_o)$ is R-linear in the indeterminate x.

A **multilinear mapping** extends the definition of bilinear mapping to the mapping of a cartesian product of any finite number of R-modules to one R-module. The requirement that the base ring be commutative in the definition of bilinear mapping lies in the following observation: Let E, N, F be R-modules and g a bilinear map $g : E \times N \longrightarrow F$ then for any $e \in E$, $n \in N$ and $a, b \in A$ we have

1. $g(ae, bn) = a(g(e, bn)) = a(bg(e, n)) = ab(g(e, n))$.
2. $g(ae, bn) = b(g(ae, n)) = b(ag(e, n)) = ba(g(e, n))$.

The definition of bilinear mapping lets us notice the following three properties: let $g : E \times N \longrightarrow F$ be a bilinear mapping of R-modules, then for any $e, z \in E$, $n, h \in N$ and $a, b \in R$ we have

1. $g(e + z, h) = g(e, h) + g(z, h)$
2. $g(e, n + h) = g(e, n) + g(e, h)$
3. $b(g(e, n)) = g(be, n) = g(e, bn)$

The definition of bilinear mapping is a special case of a multilinear mapping of any finite number of R-modules into an R-module.

> **Definition 2.31.** Let R be a commutative ring and I any finite indexing set, hence $|I| = n \in \mathbb{Z}^+$. Also, let $\{E_i\}_{i \in I}$ be any family of

R-modules indexed by I, F be any R-module, and $E_1 \times E_2 \times ... \times E_n$ be a cartesian product of the family. The map

$$f : E_1 \times E_2 \times ... \times E_n \longrightarrow F$$

is called a **R-multilinear mapping** or a multilinear mapping of the family of R-modules $\{E_i\}_{i \in I}$ if f is a map such that is R-linear in each component when the other components are fixed.

Let $f : E_1 \times E_2 \times ... \times E_n \longrightarrow F$ be a multilinear mapping of R-modules. For arbitrary $i \in I$, $j_i, t_i \in E_i$, and $a, b \in R$ we have the following properties:

1. $f(j_1, .., j_i + t_i, ..., j_n) = f(j_1, .., j_i, ..., j_n) + f(j_1, .., t_i, ..., j_n)$
2. $a(f(j_1, .., j_i, ..., j_n)) = f(j_1, .., aj_i, ..., j_n)$

The previous properties of a multilinear mapping of the family $\{E_i\}_{i \in I}$ of R-modules are the key to understand the construction of a tensor product for a given multilinear mapping.

Definition 2.32. Let $E_1, E_2, ..., E_n$ be modules over a commutative ring R. The **tensor product** of $E_1, E_2, ..., E_n$ is the pair (T, β) where T is an R-module and β is a R-multilinear mapping $\beta : E_1 \times E_2 \times ... \times E_n \longrightarrow T$ such that for any R-module X and any R-multilinear mapping $f : E_1 \times E_2 \times ... \times E_n \longrightarrow X$ there exists a unique R-module homomorphism $f_* : T \longrightarrow X$ for which $f_* \circ \beta = f$.

The pair (T, β) is "universal for multilinearity of the direct product $E_1 \times E_2 \times ... \times E_n$ where T is the tensor product and β is the tensor map"(Roman, 2008). The universality of the tensor product means that "the tensor product is unique up to a unique R-module isomorphism which is the universal property of tensor products"(Roman, 2008), thus we talk about **the** tensor product and not a tensor product. Hence, any tensor product T that we build will be unique in as mentioned, this universal property helps us solve many problems where there is a multilinear mapping of R-modules. The tensor product T is denoted by

$$E_1 \otimes_R E_2 \otimes_R ... \otimes_R E_n \quad \text{or} \quad \bigotimes_{j=1}^{n} E_j$$

The map β is the multilinear mapping

$$\beta : E_1 \times E_2 \times ... \times E_n \longrightarrow T$$
$$\beta(x_1, x_2, ..., x_n) = x_1 \otimes_R x_2 \otimes_R \cdots \otimes_R x_n$$

If the base commutative ring R is clearly understood from the context then we can simply write the tensor product as $E_1 \otimes E_2 \otimes ... \otimes E_n$. Also we have for each index $i \in \{1, 2, ..., n\}$

$$a(x_1 \otimes x_2 \otimes ... \otimes x_i \otimes ... \otimes x_n) = x_1 \otimes x_2 \otimes ... \otimes ax_i \otimes ... \otimes x_n$$

$$x_1 \otimes x_2 \otimes ... \otimes (x_i + x_i') \otimes ... \otimes x_n = (x_1 \otimes x_2 \otimes ... \otimes x_n) + (x_1 \otimes x_2 \otimes ... \otimes x_i' \otimes ... \otimes x_n)$$

for all $x_i, x_i' \in E_i$ and $a \in R$.

Remark: observe that $x_1 \otimes x_2 \otimes ... \otimes x_n$ is zero if and only if at least one $x_i = 0$. It can be proved that the tensor product is associative, a "theorem that is proved by using the universal property"(Lang, 2005, p. 622). Here we present that theorem without proof:

Theorem 2.33. Let M_1, M_2, M_3 be R-modules. Then there exists a unique isomorphism

$$M_1 \otimes (M_2 \otimes M_3) \longrightarrow (M_1 \otimes M_2) \otimes M_3$$

such that

$$(x \otimes y) \otimes z \mapsto x \otimes (y \otimes z)$$

for all $x \in M_1$, $y \in M_2$, $z \in M_3$

Now we will prove the existence and uniqueness of tensor products. First we prove uniqueness up to a unique R-module isomorphism because "it allows us to speak about **'the'** tensor product of two modules N and M"(Pierce, 1982). After that we prove existence "by constructing a specific tensor product in the isomorphism class of tensor products"(Lang, 2005).

Uniqueness of tensor products

For the R-modules $E_1, E_2, ..., E_n$ we suppose that the tensor product T together with the the multilinear mapping $\beta : E_1 \times E_2 \times ... \times E_n \longrightarrow T$ exist such that for any R-module X and any multilinear mapping $f : E_1 \times E_2 \times ... \times E_n \longrightarrow X$ **there exists a unique R-module homomorphism** $f_* : T \longrightarrow X$ for which $f_* \circ \beta = f$.

We are going to prove that the tensor product T is unique up to a unique isomorphism. We can represent these homomorphisms of the tensor product as a **commutative diagram** of mappings. A commutative diagram is a collection of mappings such that all mappings' composition starting from a fixed set A and finishing in another set B give the same result.

$$\begin{tikzcd}
E_1 \times E_2 \times ... \times E_n \arrow[r, "\beta"] \arrow[dr, "f"'] & T \arrow[d, "f_*"] \\
 & X
\end{tikzcd}$$

If we replace X by T itself then the unique R-module homomorphism is the identity, $f_* = id$ and consequently $f = \beta$

$$\begin{tikzcd}
E_1 \times E_2 \times ... \times E_n \arrow[r, "\beta"] \arrow[dr, "\beta"'] & T \arrow[d, "id"] \\
& T
\end{tikzcd}$$

Now we replace X by another arbitrary tensor product W with multilinear mapping $\eta : E_1 \times E_2 \times ... \times E_n \longrightarrow W$ of the modules $E_1, E_2, ..., E_n$; thus, we get two diagrams with unique homomorphism g and h respectively.

$$\begin{tikzcd}
E_1 \times E_2 \times ... \times E_n \arrow[r, "\beta"] \arrow[dr, "\eta"'] & T \arrow[d, "g"] \\
& W
\end{tikzcd}$$

$$\begin{tikzcd}
E_1 \times E_2 \times ... \times E_n \arrow[r, "\eta"] \arrow[dr, "\beta"'] & W \arrow[d, "h"] \\
& T
\end{tikzcd}$$

When we combine the previous two diagrams we obtain the diagram

$$\begin{tikzcd}
E_1 \times E_2 \times ... \times E_n \arrow[r, "\beta"] \arrow[drr, "\eta"] \arrow[ddr, "\beta"'] & T \arrow[dr, "g"] \arrow[dd, leftrightarrow, "id"] & \\
& & W \arrow[dl, "h"] \\
& T &
\end{tikzcd}$$

Since the homomorphisms g, h and id are unique we have that $g \circ h = id$ and $h \circ g = id$, which implies that g and h are isomorphisms and $g = h^{-1}$. Therefore the tensor products T and W are isomorphic and we can talk about **"the"** tensor product. This ends the proof.

Existence of tensor product

We are going to construct the tensor product of the R-modules $E_1, E_2, ..., E_n$ by using the construction of a free module over a commutative ring (see the Free Module subsection) and the factor theorem of modules (see the Factor Theorem and first Isomorphism theorem subsection). This construction was obtained from Serge Lang's book Algebra (Lang, 2005) on page 602. We will show this construction here because it is the most understandable.

Recall that $E_1 \times E_2 \times ... \times E_n$ is a cartesian product of the family of R-modules $\{E_1, E_2, ..., E_n\}$. Let M be the free R-module generated by the cartesian product set $E_1 \times E_2 \times ... \times E_n$ according to the section of free modules, that is, $M = R < E_1 \times E_2 \times ... \times E_n >$. Let N be the R-submodule of M generated by all the elements of $E_1 \times E_2 \times ... \times E_n$ of the type:

$$(x_1, ..., x_i + x_i', ..., x_n) - (x_1, ..., x_i, ..., x_n) - (x_1, ..., x_i + x_i', ..., x_n)$$
$$(x_1, ..., ax_i, ..., x_n) - a(x_1, ..., x_i, ..., x_n)$$

for all $x_i \in E_i$, $x_i' \in E_i$, $a \in R$. In the construction of the free module M we also obtained the mapping

$$g : E_1 \times E_2 \times ... \times E_n \longrightarrow M$$
$$(x_1, x_2, ..., x_n) \mapsto 1(x_1, x_2, ..., x_n)$$

We compose g with the canonical map $M \longrightarrow M/N$ to obtain the map

$$\varphi \ : E_1 \times E_2 \times ... \times E_n \longrightarrow M/N$$

We observe that φ is an R-multilinear map since its construction was adjusted to that purpose. Let

$$f : E_1 \times E_2 \times ... \times E_n \longrightarrow X$$

be an R-multilinear map. Recalling the definition of a free module generated by a set, we have an induced R-linear map $M \longrightarrow X$ which makes the following diagram commutative.

$$\begin{tikzcd}
E_1 \times E_2 \times ... \times E_n \arrow[r] \arrow[dr, "f"'] & M \arrow[d] \\
& X
\end{tikzcd}$$

We notice that since f is multilinear the induced map $M \longrightarrow X$ has value 0 on N, recalling the definition of a multilinear map and evaluating $M \longrightarrow X$ with any element in N. We observe then that N is a subset of the kernel of $M \longrightarrow X$, thus by the factor theorem of modules we obtain the diagram

$$\begin{tikzcd}
E_1 \times E_2 \times ... \times E_n \arrow[r, "\varphi"] \arrow[dr, "f"'] & M/N \arrow[d, "f_*"] \\
& X
\end{tikzcd}$$

where $f_* : M/N \longrightarrow X$ is unique for M/N and makes the previous diagram commutative. The module M/N is denoted by

$$E_1 \otimes_R E_2 \otimes_R ... \otimes_R E_n \quad \text{or} \quad \bigotimes_{j=1}^{n} E_j$$

and is called the tensor product T of any multilinear mapping of $E_1 \times E_2 \times ... \times E_n$. The subscript R in the tensor product simply indicates over which ring the tensor product is; if it is clear to which ring we refer then we can drop the subscript. The construction of the tensor product also gave us the mapping φ, if $x_i \in E_i$, we have

$$\varphi(x_1, x_2, ..., x_n) = x_1 \otimes_R x_2 \otimes_R ... \otimes_R x_n$$

By our construction of the tensor product, we notice that the mapping φ is in fact a multilinear mapping of $E_1 \times E_2 \times ... \times E_n$. Hence, the mapping φ is our tensor map. Note as well that the image of φ **generates the tensor product**. Recall the induced linear map of a free module over a set. Also we have for all index $i \in \{1, 2, ..., n\}$

$$a(x_1 \otimes x_2 \otimes ... \otimes x_i \otimes ... \otimes x_n) = x_1 \otimes x_2 \otimes ... \otimes ax_i \otimes ... \otimes x_n$$
$$x_1 \otimes x_2 \otimes ... \otimes (x_i + x_i') \otimes ... \otimes x_n = (x_1 \otimes x_2 \otimes ... \otimes x_n) + (x_1 \otimes x_2 \otimes ... \otimes x_i' \otimes ... \otimes x_n)$$

for all $x_i, x_i' \in E_i$ and $a \in R$. This ends the proof.

2.3.8 Module homomorphisms of tensor products

This definition was obtained from Serge Lang's book (Lang, 2005) on page 605. Suppose we have a collection of R-module homomorphisms

$$f_i : E_i' \longrightarrow E_i \quad \text{for all} \quad i = 1, 2, 3, .., n$$

We get an induced map on their product

$$\prod_{i=1}^{n} f_i : \prod_{i=1}^{n} E_i' \longrightarrow \prod_{i=1}^{n} E_i$$
$$(x_1, x_2, ..., x_n) \mapsto (f_1(x_1), f_2(x_2), ..., f_n(x_n))$$

Now we compose $\prod_{i=1}^{n} f_i$ with the canonical map to the tensor product of $E_1 \times E_2 \times ... \times E_n$. Thus we obtain an induced R-linear map between the tensor products $E_1' \otimes E_2' \otimes ... \otimes E_n'$ and $E_1 \otimes E_2 \otimes ... \otimes E_n$ denoted by $T(f_1, f_2, ..., f_n)$ which makes the following diagram commutative.

$$\begin{tikzcd}
E_1' \times E_2' \times ... \times E_n' \arrow[r] \arrow[d, "\prod_{i=1}^n f_i"'] & E_1' \otimes E_2' \otimes ... \otimes E_n' \arrow[d, "T(f_1, f_2, ..., f_n)"] \\
E_1 \times E_2 \times ... \times E_n \arrow[r] & E_1 \otimes E_2 \otimes ... \otimes E_n
\end{tikzcd}$$

Figure 1: Commutative diagram of induced linear map of tensor products (Lang, 2005)

Using the above diagram we can easily observe that the R-linear map $T(f_1, f_2, ..., f_n)$ has the property

$$T(f_1 \circ h_1, f_2 \circ h_2, ..., f_n \circ h_n) = T(f_1, f_2, ..., f_n) \circ T(h_1, h_2, ..., h_n)$$

and

$$T(id, id, ..., id) = id$$

We also notice that $T(f_1, f_2, ..., f_n)$ is the unique linear map whose effect on the generators of the tensor product is $x_1 \otimes x_2 \otimes ... \otimes x_n \mapsto f_1(x_1) \otimes f_2(x_2) \otimes ... \otimes f_n(x_n)$

2.3.9 Linear Algebra

Linear Algebra can also be done over division rings, not just fields, but one has to be careful about the formation of opposite rings. Here we give the following theorem on the existence of basis of division rings and fields without proof, details can be found for example in (Lang, 2005) and (Raya, Rider, & Rubio, 2007).

Theorem 2.34. Any module over a division ring has a basis.

2.4 Algebras

There is an even more general object than rings in mathematics. An algebra over a commutative ring A has the structure of an A-module and satisfies all the axioms of a ring with the exception of associativity and the existence of a multiplicative identity element.

Definition 2.35. An algebra H over a commutative ring A, also called an ***A*-algebra** H, is an A-module H together with a bilinear map $g : H \times H \longrightarrow H$.

We notice that the bilinear map in the algebra's definition is the multiplication operation of the algebra. Examples:

1. Any field extension of a field L is an L-algebra.
2. Any polynomial ring over a field K in one indeterminate is a K-algebra.
3. Any *nxn* matrix ring with entries in a field K is a K-algebra, then, it is called a matrix algebra over the field K.

In this article we consider only algebras that are associative and have multiplicative identity. This requirement allows us to view our A-algebras as rings with an A-bilinear mapping that is also the multiplication operation. Also in this article, when we mention an A-algebra H we mean the following:

> Let H be a ring and A a commutative ring. Let $f : A \longrightarrow H$ be a ring homomorphism such that $f(A)$ is a subset of the center of H, thus $f(a)$ commutes with every element of H. Hence, H is an A-module by defining the module operation as
>
> $$\begin{aligned} g : A \times H &\longrightarrow H \\ (a, b) &\mapsto f(a)h \end{aligned}$$
>
> Also the multiplication operation on the ring H given by $H \times H \longrightarrow H$ is clearly A-bilinear. This implies that the ring H with the ring homomorphism $f : A \longrightarrow H$ form an A-algebra (Lang, 2005, p. 121).

From now on, when we mention a K-algebra we consider the base commutative ring K to be a field unless otherwise specified. If H is a K-algebra and it is finitely generated over $f(K)$ as a K-module then we say that H is a **finite dimensional over the field $\boldsymbol{K}$** or H is a **finite-dimensional $\boldsymbol{K}$-algebra**.

Definition 2.36. A **subalgebra** W of the K-algebra H is a subset of H that is also a K-algebra. Consequently, every subalgebra of H contains the same multiplicative identity as H.

A **division algebra** is a K-algebra where all of its non-zero elements have a multiplicative inverse. Similarly, we define a **commutative algebra** as a K-algebra where the multiplication operation is commutative.

Definition 2.37. Let H be a K-algebra and $K[x]$ be the polynomial ring over K. An element $a \in H$ is said to be algebraic over K if there is a non-zero polynomial $g(x) \in K[x]$ such that $g(a) = 0$. The K-algebra H is called an **algebraic algebra** over K if every $a \in H$ is algebraic over K.

It is easily verified that any finite dimensional K-algebra H is algebraic over K because the set $\{a^n\}$ for each $a \in H$ and all $n \in \mathbb{N}$ is linearly dependent, hence there exists a minimal non-zero polynomial with a as a root for every $a \in H$.

2.4.1 Homomorphisms and ideals of algebras

The mapping preserving the structure of an algebra is called an algebra homomorphism. Notice that the definition preserves the structure of the algebra as a ring and as a module simultaneously.

Definition 2.38. Let A and B be K-algebras. A map $g : A \longrightarrow B$ is called a K-algebra homomorphism if it is a homomorphism of A and B as rings and as K-modules, that is, for all $a \in A$ and $k \in K$ we must have

1. $f(a_1 + a_2) = f(a_1) + f(a_2)$
2. $f(a_1 a_2) = f(a_1) f(a_2)$
3. $f(ka) = kf(a)$
4. $f(1_A) = 1_B$

If the K-algebra homomorphism is also a bijective map then we say a ***K*-algebra isomorphism**. A subset S of an algebra W is called a **left ideal of the algebra** W if it is a subgroup of the additive group of W and $ws \in S$ for all $w \in W$ and $s \in S$. We define similarly right ideals and ideals of a K-algebra.

2.4.2 Central simple algebras

A key observation in the proof of Frobenius' Theorem is that finite dimensional associative division algebras over the field of real numbers are central simple. Recall we consider only algebras over a field.

Definition 2.39. A **simple algebra** is a K-algebra that is also a simple ring, that is, the algebra does not have ideals except for the zero ideal and the algebra itself.

It is then easy to show that any division algebra is simple because any non-trivial left ideal must have 1. We give the definition of centralizer of a fixed subset of any algebra in general, see page 93 of Farb and Dennis.

Definition 2.40. Let B be an algebra and S any subset of B. The **centralizer of S in B** is the set $C_B(S) = \{b \in B| \quad sb = bs \quad \text{for all } s \in S\}$. One may check that $C_B(S)$ is a subalgebra of B for any subset S of B.

This allows us to define the center of a K-algebra.

Definition 2.41. Let H be an algebra over K. The **center** of H is the set $Z(H) = C_H(H) = \{x \in H \,|\, sx = xs \quad \text{for all}\, s \in H\}$. That is, $Z(H)$ is the center of H considered as a ring.

Definition 2.42. Let H be an algebra over K. The algebra H is called a **central algebra** if $Z(H)$ is ring isomorphic to the base field K.

A **central simple algebra** H over the field K is an algebra that is simple and whose center and base field is K.

2.4.3 Subfields of division algebras

Subfields are very important in our proof of Frobenius' Theorem, in particular "a powerful method for studying division rings is to study their maximal subfields"(Lam, 2001, p. 241). The definition of subfield we give here is general for any associative K-algebra and can be found for example in R.S. Pierce's book Algebra on page 234 (see references).

Definition 2.43. A **subfield** of a K-algebra H is a subalgebra A of H such that A is a field.

For division algebras we have a nice way of defining maximal subfields, see Farb and Dennis book on page 114.

Definition 2.44. Let R be a division ring. A subfield L of R is maximal if L is maximal with respect to set inclusion.

For division algebras we have another special way to characterize their maximal subfields. This happens because a subfield of a division algebra is a commuting subring. Here we give the following proposition which characterizes maximal subfields of division algebras, as presented in Lam's book on page 241.

Proposition 2.45. A subfield L of a division ring R is a **maximal subfield** if and only if $C_R(L) = L$. If this is the case then $Z(R) \subseteq L$.

Remark. For division algebras we use use definition 2.44 to prove proposition 2.45. However, for algebras that are not division algebras, the definition of a maximal subfield in the sense of definition 2.44 does not always coincide with maximal commuting subrings given by proposition 2.45. For more information and counterexamples on this issue, we recommend the reader Farb and Dennis' book on page 114.

2.4.4 Tensor product of algebras

The tensor product of algebras is another way to construct new algebras from previous ones, say W and T, over the same commutative ring R. We will make $W \otimes T$ into an R-algebra. This construction can be found in Serge Lang's book Algebra (Lang, 2005, p. 629), although we give here a more detailed explanation. Consider the bilinear map for a given $w, t \in W \times T$.

$$\begin{aligned} \beta_{w,t} : W \times T &\longrightarrow W \otimes T \\ (w', t') &\mapsto ww' \otimes tt' \end{aligned}$$

By the universal property of tensor products, we have the unique induced R-module homomorphism

$$\begin{aligned} \beta_{*(w,t)} : W \otimes T &\longrightarrow W \otimes T \\ \sum_{i=1}^{m} w_i \otimes t_i &\mapsto \sum_{i=1}^{m} ww_i \otimes tt_i \end{aligned}$$

We notice that $\beta_{*(w,t)}$ is bilinear for w and t. This leads us to consider the following bilinear map with a fixed $\sum_{i=1}^{m} w_i \otimes t_i \in W \otimes T$ in order that our map becomes well defined.

$$\begin{aligned} \alpha : W \times T &\longrightarrow W \otimes T \\ (w, t) &\mapsto \beta_{*(w,t)}(\sum_{i=1}^{m} w_i \otimes t_i) = \sum_{i=1}^{m} ww_i \otimes tt_i \end{aligned}$$

From this we get a unique induced R-module homomorphism for a fixed $\sum_{i=1}^{m} w_i \otimes t_i \in W \otimes T$.

$$\begin{aligned} \alpha_* : W \otimes T &\longrightarrow W \otimes T \\ \sum_{j=1}^{r} w_j \otimes t_j &\mapsto \sum_{j=1}^{r} \beta_{*(w_j,t_j)}(\sum_{i=1}^{m} w_i \otimes t_i) \end{aligned}$$

Similarly, we can obtain another linear map as α_* but with multiplication from the right. First we define the bilinear map

$$\begin{aligned} \beta_{w',t'} : W \times T &\longrightarrow W \otimes T \\ (w, t) &\mapsto ww' \otimes tt' \end{aligned}$$

Now, in a fashion similar to which we got α_*, now we obtain the R-module homomorphism σ_*.

$$\begin{aligned}\sigma_* : W \otimes T &\longrightarrow W \otimes T\\ \sum_{i=1}^{r} w_i \otimes t_i &\mapsto \sum_{i=1}^{r} \beta_{*(w_i,t_i)}(\sum_{j=1}^{m} w_j \otimes t_j)\end{aligned}$$

From the definition of bilinear map, we have that α_* and σ_* are the two R-linear maps in the bilinear map

$$(W \otimes T) \times (W \otimes T) \longrightarrow W \otimes T$$

such that $(w \otimes t)(w' \otimes t') = (ww' \otimes tt')$.

This map is associative, has multiplicative identity $1 \otimes 1$ and we have the natural ring homomorphism

$$\begin{aligned}\rho : R &\longrightarrow W \otimes T\\ r &\mapsto r \otimes 1 = 1 \otimes r\end{aligned}$$

Therefore $W \otimes T$ is an R-algebra, also called the **ordinary tensor product**.

2.4.5 The real numbers, complex numbers, quaternions and octonions

The set of **real numbers** $\mathbb{R}$ is a field and is trivially a finite dimensional associative division algebra over the real numbers. The set of **complex numbers** $\mathbb{C}$ is a field that has the real numbers as subfield; however, since $\mathbb{C}$ is a field it is not a central algebra over the real numbers. We note that the complex numbers are "finite dimensional over $\mathbb{R}$ with basis $\{1, i\}$ where i is the imaginary unit of $\mathbb{C}$ with the property $i^2 = -1$" (Conway & Smith, 2003, p. 1).

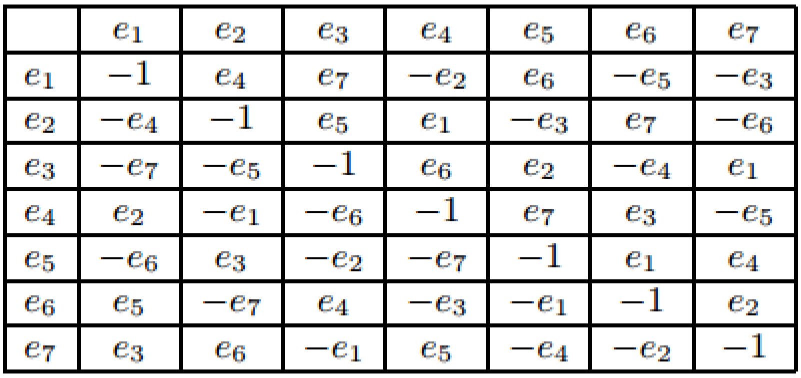
The set of **quaternions** $\mathbb{H}$ is a 4-dimensional associative division algebra over the real numbers. They are "formal expressions $x_0 + x_1 i + x_2 j + x_3 k$ where $x_0, x_1, x_2, x_3 \in \mathbb{R}$. Furthermore, we have that 1, i, j, k are the basis of the quaternions and satisfy Hamilton's celebrated equations

$$\begin{aligned}ijk &= -1\\ i^2 = j^2 = k^2 &= -1\end{aligned}$$

We use Hamilton's equations to multiply any two quaternions and note that they are not commutative but associative"(Conway & Smith, 2003, p. 11). We have also that given a quaternion $x_0 + x_1 i + x_2 j + x_3 k$ then its inverse is

$\frac{x_0 - x_1 i - x_2 j - x_3 k}{x_0^2 + x_1^2 + x_2^2 + x_3^2}$.

The set of **octonions** $\mathbb{O}$ is an 8-dimensional division algebra over the real numbers but "they are not associative"(Baez, 2001, p. 145). Baez(2001) in his article on the octonions mentions that "the unit quaternions $e_i \in \mathbb{O}$ for $i = 1, ..., 7$ including 1 are the basis elements of the octonions and their multiplication with the exception of 1 is given in the following multiplication table:"



	e_1	e_2	e_3	e_4	e_5	e_6	e_7
e_1	-1	e_4	e_7	$-e_2$	e_6	$-e_5$	$-e_3$
e_2	$-e_4$	-1	e_5	e_1	$-e_3$	e_7	$-e_6$
e_3	$-e_7$	$-e_5$	-1	e_6	e_2	$-e_4$	e_1
e_4	e_2	$-e_1$	$-e_6$	-1	e_7	e_3	$-e_5$
e_5	$-e_6$	e_3	$-e_2$	$-e_7$	-1	e_1	e_4
e_6	e_5	$-e_7$	e_4	$-e_3$	$-e_1$	-1	e_2
e_7	e_3	e_6	$-e_1$	e_5	$-e_4$	$-e_2$	-1

Figure 2: Unit octonion multiplication table (Baez, 2001, p. 150)

Notice that the above multiplication table is non associative, for example take the units e_3, e_4, and e_5; then, we have for one part $(e_3e_4)e_5 = e_6e_5 = -e_1$ and for other part $e_3(e_4e_5) = e_3e_7 = e_1$. Thus the octonions are clearly non associative. Furthermore "for any octonion $x_0 + \sum_{i=1}^{7} x_i e_i$ we have its inverse

$$\frac{x_0 - \sum_{i=1}^{7} x_i e_i}{x_0^2 + \sum_{i=1}^{7} x_i^2}$$

where the denominator of the inverse is the square of the norm of the octonion"(Baez, 2001, p. 154). The norm of an octonion is the sum of the square of its coefficients. The reader can verify that the octonions contain a subalgebra isomorphic to the quaternions and another algebra isomorphic to the complex numbers.

We have only mentioned the octonions for the sake of completeness, to know that there exists an algebra that is a finite dimensional division algebra over the real numbers but not associative that contains the quaternions and complex numbers. For a lot more information about all the algebras covered in this chapter including applications, the reader can study the article "The octonions" by Baez(2001) and the book "On Quaternions and Octonions: Their Geometry, Arithmetic and Symmetry" by Conway and Smith(2003).

3 Preliminary results

The preliminary results are the theorems, propositions, lemmas, etc which will help us prove our main theorem. Before that, we remind the reader a convention we adopted when dealing with endomorphism rings of modules. Our convention for endomorphism rings says the following: Let M be a left R-module and $W = End_R(M)$, then M is naturally a right W-module and given arbitrary $f, g \in End_R(M)$ instead of writing $(f \circ g)(m)$ we write $(m)gf$ for the composition of endomorphisms. Similarly, if we begin with a right R-module M, then M is naturally left W-module where W is the endomorphism ring of M. These conventions help us avoid the formation of opposite rings.

Let E be a ring and consider it a left regular module ${}_EE$. It turns out that we can obtain explicitly End_EE which is equal to the set of endomorphisms of multiplication by the right by any $e \in E$.

Proposition 3.1. Let E be a ring and ${}_EE$ the left regular module of E. Then, $End_EE = \{T_e|\, e \in E\}$ where

$$\begin{aligned} T_e : E &\longrightarrow E \\ x &\mapsto xe \end{aligned}$$

Proof. First we show that $\{T_e|\, e \in E\}$ is indeed an endomorphism of ${}_EE$. Let T_e and $e' \in E$ be arbitrary, then we have

$$T_e(x+y) = (x+y)e = xe + ye \quad \text{which implies} \quad T_e(x+y) = T_e(x) + T_e(y)$$
$$T_e(e'x) = (e'x)e = e'(xe) \quad \text{which implies} \quad T_e(e'x) = e'\,T_e(x)$$

Thus $\{T_e\} \subseteq End_EE$. Now let $f \in End_EE$ be arbitrary, the endomorphism f is determined according to where f sends the identity of E. We have $f(1) = e$ thus for any $x \in E$ we have $xf(1) = xe$ and consequently $f(x) = xe$, then $f = T_e$. We then get $End_EE \subseteq \{T_e\}$, therefore $End_EE = \{T_e\}$. □

To see the usefulness of considering the composition of endomorphisms f, g of an R-module M as $(m)gf$ instead of $(f \circ g)(m)$ we show the ring homomorphism of E and End_EE. Example:
The map $g : E \longrightarrow End_EE$ given by $e \mapsto T_e$ is an homomorphism, indeed we have

1. $g(x+y) = T_{x+y} = T_x + T_y$ then $g(x+y) = g(x) + g(y)$.
2. $g(xy) = T_{xy}$, but T_{xy} is the map $w \mapsto wxy$ where $w \in E$. Notice we have $wxy = ((wx)y)$, thus we get $T_{xy}(w) = T_y(T_x(w)) = (T_y \circ T_x)(w)$. By our convention on composition of endomorphisms we have $(T_y \circ T_x)(w) = (m)T_xT_y$ then $g(xy) = g(x)g(y)$.

Notice again that for the endomorphism composition we have used our convention. If we had not used it, we would have obtained a ring homomorphism of R^{op} and $End_E E$ which is exactly what we want to avoid.

We now prove the following proposition, important for left artinian modules:

Proposition 3.2. Let M be a left R-module. M is left artinian if and only if for any submodule N, implies N is left artinian and M/N is left artinian.

Proof. Let M be a left R-module.
$\Rightarrow$ Suppose M is left artinian. Let N be an arbitrary submodule of M, then any descending sequence of submodules of N is also a descending sequence of submodules of M, hence it must stabilize, and thus N is left artinian. Let

$$W_1 \supseteq W_2 \supseteq W_3 \supseteq \cdots \tag{1}$$

be any descending sequence of left modules of M/N. We use the canonical projection $\pi : M \longrightarrow M/N$ to get a descending sequence of submodules of M given by

$$\pi^{-1}(W_1) \supseteq \pi^{-1}(W_2) \supseteq \pi^{-1}(W_3) \supseteq \cdots$$

which must stabilize, and thus the descending sequence 1 must stabilize as well. Hence, M/N is left artinian.
$\Leftarrow$ Suppose any submodule N of M is left artinian and M/N is left artinian. Let $N = \{0\}$, the trivial group, so $M/\{0\}$ is left artinian by hypothesis. We notice $M \cong M/\{0\}$ as R-modules. Thus, M is left artinian. □

3.1 Endomorphism ring of infinite dimensional vector spaces over division rings is not simple

We obtain the endomorphism ring of any finite direct sum of R-modules $E_1, E_2, ..., E_n$.

Proposition 3.3. Let $\{E_i\}_{i\in I}$ be any finite family of R-modules, denote $|I| = n \in \mathbb{Z}^+$, and let $\bigoplus_{i=1}^n E_i$ be their direct sum. Then, for any $f \in End_R(\bigoplus_{i=1}^n E_i)$ exists R-module homomorphisms $f_{ji} \in Hom_R(E_i, E_j)$ where $i, j \in I$ such that f is the map multiplication by a matrix given by

$$f : \bigoplus_{i=1}^{n} E_i \longrightarrow \bigoplus_{j=1}^{n} E_j$$

$$(x_1, x_2, ..., x_n) \mapsto \begin{bmatrix} f_{11} & f_{12} & \cdots & f_{1n} \\ f_{21} & f_{22} & \cdots & f_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ f_{n1} & f_{n2} & \cdots & f_{nn} \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix}$$

Proof. Let $\{E_i\}_{i\in I}$ be any finite family of R-modules, denote $|I| = n \in \mathbb{Z}^+$, and let $E = \bigoplus_{i=1}^n E_i$ be their direct sum. Let $f \in End_R(\bigoplus_{i=1}^n E_i)$ arbitrary

$$f : \bigoplus_{i=1}^{n} E_i \longrightarrow \bigoplus_{j=1}^{n} E_j$$

Let $\{\nu_i : A_i \longrightarrow A\}_{i\in I}$ be the family of canonical injections from E_i into E (see the direct sum subsection). By the universal property of direct sum of modules we have the family of R-module homomorphisms: for all $i = 1, 2, 3, ..., n$

$$f_i : E_i \longrightarrow \bigoplus_{j=1}^{n} E_j$$

$$x_i \longrightarrow f(\nu_i(x_i))$$

which induces a unique R-module homomorphism

$$f : \bigoplus_{i=1}^{n} E_i \longrightarrow \bigoplus_{j=1}^{n} E_j$$

$$(x_1, x_2, ..., x_n) \longrightarrow \sum_{i=1}^{n} (f_i(x_i))$$

Define for any $j \in I$ the submodule of E given by $W_j = \{x \in E \mid$ j^{th} *component of* x *equal 0*$\}$. Define for any $j \in I$ the quotient R-module E/W_j, the mapping

$$\begin{aligned} \rho_j : E/W_j &\longrightarrow E_j \\ [(x_1, x_2, \cdots, x_j, \cdots, x_n)] &\mapsto x_j \end{aligned}$$

is well defined and is an R-module isomorphism for any $j \in I$. Additionally, we have the canonical map $\pi_j : E \longrightarrow E/W_j$ for any $j \in I$. Define $f_{ji} = \rho_j \circ \pi_j \circ f_i$ for all $i, j \in I$, thus $f_{ij} \in Hom_R(E_i, E_j)$ for any $i, j \in I$.

Notice that for any $i \in I$ and any $x_i \in E_i$ we have

$$f_i(x_i) = (f_{1i}(x_i), f_{2i}(x_i), \cdots, f_{ji}(x_i), \cdots, f_{ni}(x_i))$$

We then have

$$\begin{aligned} f : \bigoplus_{i=1}^{n} E_i &\longrightarrow \bigoplus_{j=1}^{n} E_j \\ (x_1, x_2, ..., x_n) &\longrightarrow \sum_{i=1}^{n} (f_{1i}(x_i), f_{2i}(x_i), \cdots, f_{ji}(x_i), \cdots, f_{ni}(x_i)) \end{aligned}$$

Therefore we can represent $f \in End_R(\bigoplus_{i=1}^{n} E_i)$ by a map multiplication by a matrix given by

$$\begin{aligned} f : \bigoplus_{i=1}^{n} E_i &\longrightarrow \bigoplus_{j=1}^{n} E_j \\ (x_1, x_2, ..., x_n) &\mapsto \begin{bmatrix} f_{11} & f_{12} & \cdots & f_{1n} \\ f_{21} & f_{22} & \cdots & f_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ f_{n1} & f_{n2} & \cdots & f_{nn} \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix} \end{aligned}$$

Since $f \in End_R(\bigoplus_{i=1}^{n} E_i)$ is arbitrary, the proposition is proved.

□

Now we will consider endomorphism rings of infinite dimensional vector spaces over a division ring, however we are only interested in them because they are not simple rings. More information about these endomorphism rings can be found on pages 415 and 424 from the book Algebra by Hungerford (Hungerford, 1974). The following proposition is actually an exercise on page 424 from Hungerford's book.

Proposition 3.4. Let V be an infinite dimensional vector space over a division ring D. If H is the set of all $\alpha \in End_D(V)$ such that $\alpha(V)$ is finite-dimensional, then H is a proper ideal of $End_D(V)$. Therefore $End_D(V)$ is not simple.

Proof. Let V be an infinite dimensional vector space over a division ring D. Let H be the set of all $\alpha \in End_D(V)$ such that i$\alpha(V)$ is finite-dimensional. Clearly, we have $H \subset End_D(V)$, it is a proper subset because the identity homomorphism of V does not have a finite dimensional image. Now we show that H is an ideal of $End_D(V)$. Let $h, w \in H$, $\alpha \in End_D(V)$ arbitrary

1. The zero map is element of H since its image is generated by 0. We also have $(h+w)(V) = h(V)+w(V)$ which is finite dimensional. Thus, H is a subgroup of the additive group of $End_D(V)$.

2. Now for any $\alpha \in End_D(V)$ and $h \in H$ we have that $(h \circ \alpha)(V)$ is finite dimensional because $(h \circ \alpha)(V) \subseteq h(V)$. Now we consider $(\alpha \circ h)(V)$, let $\{\nu_1, \nu_2, ..., \nu_n\}$ be the basis for $h(V)$, then the homomorphism $(\alpha \circ h)(V)$ is determined by the image of the basis vectors under α. We have that $(\alpha \circ h)(V)$ has basis of some subset of $\{\alpha(\nu_1), \alpha(\nu_1), ..., \alpha(\nu_n)\}$; consequently $(\alpha \circ h)(V)$ is a finite dimensional vector space.

Thus, H is a proper ideal of $End_D(V)$. We conclude that $End_D(V)$ is not a simple ring. □

3.2 Classification theorem of simple left artinian rings

This theorem was discovered by Wedderburn and Artin first for finite dimensional simple algebras and then for simple left artinian rings. Books on noncommutative rings study these theorems and their applications extensively, such as (Lam, 2001) and (Farb & Dennis, 1993). In this subsection we are going to prove the classification theorem of simple left artinian rings by using the **double centralizer property**. After that, we prove propositions that use this classification theorem and are important for the proof of our main theorem.

Theorem 3.5 (Double centralizer property)**.** Let R be a simple ring and I a non-zero left ideal. Let $D = End_R(I)$, so I is right D-module. Then the natural map

$$\begin{aligned} f : R &\longrightarrow End(I_D) \\ r &\mapsto {}_rT \end{aligned}$$

where ${}_rT$ is defined by

$$\begin{aligned} {}_rT : N &\longrightarrow N \\ x &\mapsto rx \end{aligned}$$

is a ring isomorphism.

Proof. Let R be any simple ring and I a non-zero left ideal. Let $D = End_R(I)$, so I is right D-module, and denote $H = End(I_D)$. Let ${}_rT \in End(I_D)$ where $r \in R$, which is left multiplication by r. Define the natural map

$$\begin{aligned} f : R &\longrightarrow End(I_D) \\ r &\mapsto {}_rT \end{aligned}$$

we check that it is a ring homomorphism

1. $f(x+y) = {}_{x+y}T$ but ${}_{x+y}T$ is $n \mapsto (x+y)n = xn + yn$ which implies $f(x+y) = {}_xT + {}_yT$ so $f(x+y) = f(x) + f(y)$.
2. $f(xy) = {}_{xy}T$ but ${}_{xy}T$ is given by $n \mapsto (xy)n = x(yn)$ thus ${}_{xy}T = {}_xT \circ {}_yT$. From this we have $f(xy) = {}_xT \circ {}_yT$ so $f(xy) = f(x)f(y)$.

Hence, f is a ring homomorphism. The kernel of f is the set of annhiliators of the module ${}_RI$ which is an ideal of R. Since R is simple and I is non-zero, we have that $ker(f) = Ann({}_RI) = 0$. Thus, f is injective. To show that f is onto we use the fact that I is a non-zero left ideal. First, we note that for any $a \in I$ the map

$$\begin{aligned} g_a : I &\longrightarrow I \\ y &\mapsto ya \end{aligned}$$

is R-linear thus $\{g_a \ |a \in I\} \subseteq End({}_RI)$. We showed $f(R) \subseteq End(I_D)$. We must show $f(R)$ contains $End(I_D)$. Now for any $n' \in I$ and $h \in H = End(I_D)$ we have

$$\begin{aligned} (h \circ (f(n')))(n) &= h(n'n) \\ &= h(g_n(n')) \\ &= g_n(h(n')) \\ &= h(n')n \\ &= f(h(n')) \end{aligned}$$

In this way $H \circ f(I) \subseteq f(I)$. We notice that I being a left ideal and R having a multiplicative identity, i.e $RI = I$, allow us to have the equation

$$f(R) \circ f(I) = f(I)$$

Also we have $f(I) \circ f(R) = f(R)$, observe $IR = \{\sum_{i=1}^{n} a_i r_i \; | a_i \in I \text{ and } r_i \in R\}$ is a two sided ideal of R, which equals R because I is non-zero. From this we obtain

$$\begin{aligned} H \circ f(I) \subseteq& f(I) \\ H \circ f(I) \circ f(R) \subseteq& f(I) \circ f(R) = f(R) \\ H \circ f(R) \subseteq& \; f(R) \end{aligned}$$

Now we also have that $f(R)$ is an additive subgroup of H, hence $f(R)$ is a left ideal in $H = End(I_D)$. We notice that the identity of H is $f(1) = {}_1T$, but $f(1) \in f(R)$ which implies $End(I_D) \subseteq f(R)$. We get $End(I_D) = f(R)$, therefore f is a ring isomorphism. □

The classification theorem for simple left artinian rings says that any such ring is isomorphic to a matrix ring with entries in a division ring. We now prove this theorem.

Theorem 3.6. Let R be any simple left artinian ring. Then $R \cong M_n(D)$ for some n and some division ring D, with n unique and D unique up to isomorphism.

Proof. Let R be a simple left artinian ring. Consider a descending sequence of left ideals of R, which do not contain the identity. Since R is left artinian, this sequence has a minimal non-zero submodule which is a minimal non-zero left ideal I of R. We apply to R and I the previous theorem (double centralizer property), then

$$R \cong End_D(I)$$

where $D = End_R(I)$, and I is naturally a right D-module.

Since I is a simple R-module, then it is a cyclic module and every element of I generates I as a cyclic module. Notice that any non-zero mapping $d \in D$ must have trivial kernel (0) because the kernel of d must be either I or (0) in I; additionally, we have $d(I) = I$ because the image is a non-zero submodule of I, thus d is an isomorphism and consequently has an inverse in D. Hence, D is a division ring.

We have that I_D is a vector space space over the division ring D so I has a basis over D. This basis is finite because otherwise if I is infinite dimensional over D then $End(I_D)$ has a non-trivial proper ideal by proposition 3.4 which contradicts the fact that it is a simple ring because $R \cong End(I_D)$. From this we have $End(I_D) \cong M_n(D)$. Consequently we get

$$R \cong M_n(D).$$

We have that $M_n(D)$ has minimal left ideals. A minimal left ideal of $M_n(D)$ consists of the set of matrices whose columns are zero except for one column. From this we have that $M_n(D)$ has n minimal left ideals V_i for $i = 1, 2, ..., n$, all of them isomorphic as left R-modules and also $V_i \cap V_j = 0$ when $i \neq j$. Consequently, we have an R-module isomorphism $M_n(D) \cong \bigoplus_{i=1} V_i$ so R has also this direct sum decomposition as a regular module into simple R-modules, thus n is uniquely determined (this sum cannot be further decomposed into simple modules).

Now, for a given minimal left ideal I of R we got $D = End_R(I)$. We claim that the ring D is unique up to isomorphism. Let I' be any other minimal left ideal of R and recall that we have an R-module isomorphism $I \cong I'$. Consider the map

$$g : End_R(I) \longrightarrow End_R(I')$$
$$d \mapsto h \circ d \circ h^{-1}$$
$$\text{where h is the module isomorphism } I \cong I'$$

We claim g is a ring isomorphism. Recall both endomorphism rings are division rings.

1. $g(d_1+d_2) = h\circ(d_1+d_2)\circ h^{-1} = h\circ d_1\circ h^{-1}+h\circ d_2\circ h^{-1} = g(d_1)+g(d_2)$
2. $g(d_1\circ d_2) = h\circ d_1\circ d_2\circ h^{-1} = (h\circ d_1\circ h^{-1})\circ(h\circ d_2\circ h^{-1}) = g(d_1)\circ g(d_2)$
3. Let $y = h \circ d \circ h^{-1} \in End({}_RI')$ arbitrary then $d = h^{-1} \circ y \circ h$ maps to y; hence, g is onto.
4. The map g is non-zero, also $End({}_RI)$ is a simple ring because it is a division ring. Since the kernel is an ideal of $End({}_RI)$ we have $ker(g) = (0)$ because $End({}_RI)$ is a simple ring.

From this we have that $D = End({}_RI) \cong End({}_RI') = D'$; thus, the division ring D is unique up to isomorphism. □

The following proposition gives a "nice characterization of simple left artinian rings"(Auslander & Buchsbaum, 2014). However, we prove it here in a different fashion.

Proposition 3.7. Let R be a left artinian ring. R is a simple ring if and only if R has a faithful simple submodule.

Proof. Let R be a left artinian ring.

$\Rightarrow$ Suppose R is a simple ring, then it is isomorphic to a matrix ring over a division ring by the classification theorem of simple left artinian rings (theorem 3.6). Thus, R contains a faithful simple submodule.

$\Leftarrow$ Suppose R has a faithful simple submodule N. Since N is a faithful simple submodule of R, we have that N is a unique simple R-module up to isomorphism. Observe that isomorphic modules have the same annhiliator. Hence, each minimal left ideal of R obtained from any descending sequence of modules without identity of the left regular module R is a simple R-module isomorphic to N. Therefore, the left regular module R has only one isomorphism class of simple left ideals, which are isomorphic to N. Let $\{L_i\}_{i\in I}$ be the family of all simple left ideals of R, recall that all of them are isomorphic to N as R-modules, indexed by some indexing set I. Let

$$W = \bigoplus_{i\in I} L_i \tag{2}$$

be the direct sum of all simple left ideals of R. Notice that there is an embedding of $\bigoplus_{i\in I\setminus\{i_1,i_2,i_3,\ldots,i_m\}} L_i$ for each $m = 1, 2, 3, ...$ into the direct sum W given by the universal property of direct sum of modules with the family of homomorphisms $\{\beta_i\}_{i\in I\setminus\{i_1,i_2,i_3,\ldots,i_m\}}$ where β_i maps each direct summand L_i in $\bigoplus_{i\in I\setminus\{i_1,i_2,i_3,\ldots,i_m\}} L_i$ into the direct sum W such that β_i maps $x \in L_i$ to the i^{th} component of the family $(x_i)_{i\in I} \in W$ and having all other components equal to zero.

Since R is left artinian then the descending sequence of W in equation 2 given by

$$W \supseteq \bigoplus_{i\in I\setminus\{i_1\}} L_i \supseteq \bigoplus_{i\in I\setminus\{i_1,i_2\}} L_i \supseteq \bigoplus_{i\in I\setminus\{i_1,i_2,i_3\}} L_i \supseteq \ldots \supseteq \bigoplus_{i\in I\setminus\{i_1,i_2,i_3,\ldots,i_m\}} L_i \supseteq \ldots$$

stabilizes for some $k \in \mathbb{Z}^+$ and $\bigoplus_{i\in I\setminus\{i_1,i_2,i_3,\ldots,i_k\}} L_i \cong L_j$ for some $j \in I$. We observe that $I \setminus \{i_1, i_2, i_3, ..., i_k\} = \{j\}$, thus we rename $j = i_{k+1} = i_t$, $t \in \mathbb{Z}^+$, with $k + 1 = t$ and we get $I = \{i_1, i_2, i_3, ..., i_t\}$. Consequently, the indexing set $J = \{1, 2, 3, \ldots, t\}$ is the indexing set of the family of all simple left ideals of R.

Hence, we have

$$W = \bigoplus_{i\in J} L_i = \bigoplus_{i=1}^{t} L_i \tag{3}$$

Given the family of R-module homomorphisms $\{f_i\}_{i\in J}$ where

$$\begin{aligned} f_i : L_i &\longrightarrow R \\ x &\mapsto x \end{aligned}$$

by the universal property of the direct sum of modules we obtain the unique induced R-module homomorphism

$$\begin{aligned} f : W &\longrightarrow R \\ (x_i)_{i\in J} &\longmapsto \sum_{i\in J} f_i(x_i) \end{aligned}$$

We claim that f is a R-module isomorphism. To show f is onto, suppose that the quotient R-module $R/f(W)$ is not isomorphic to the trivial module. By proposition 3.2 we have that $R/f(W)$ is left artinian, thus $R/f(W)$ has a simple R-module which we denote ϑ and is generated by any non-zero element $[v] \in \vartheta$, so for any $r \in R$ and representatives $[v_1] = [v_2]$ we have $rv_1 - rv_2 \in f(W)$. However, since $[v_2]$ also generates ϑ, without loss of generality we conclude that the set $\{rv_2 | r \in R\}$ is a simple left ideal in R which is not in the family of all simple left ideals $\{L_i\}_{i\in J}$, hence a contradiction. Thus, we have the R-module isomorphism $R/f(W) \cong \{0\}$ which implies that for any $r \in R$ we get $r - 0 = r \in f(W)$. As a result, $R = f(W)$ so f is onto.

To show that f is one to one we notice that $L_i \cap L_j = \emptyset$ for any two $i, j \in J$. This shows that $f((x_i)_{i\in J})$ can only be zero when all components in $(x_i)_{i\in J}$ are zero which implies $ker f = \emptyset$. Therefore, f is one to one. We proved that f is a R-module isomorphism.

Finally, we show that R is simple by proving that R is isomorphic to a matrix ring over a division ring. Recall that we let N be the unique faithful simple module of R up to isomorphism, so we have the R-module isomorphism

$$\sigma : \bigoplus_{i\in J} N \longrightarrow W$$

Let $\psi = f \circ \sigma$. Define the ring homomorphism map

$$\begin{aligned} \phi : End_R(R) &\longrightarrow End_R(\bigoplus_{i\in J} N) \\ h &\mapsto \psi^{-1} \circ h \circ \psi \end{aligned}$$

It is easy to verify that ϕ is a ring isomorphism. Recall that we have the ring isomorphisms $R \cong End_R(R)$ by our convention on endomorphism rings and $End_R(\bigoplus_{i\in J} N) \cong M_t(D)$ where $t = |J|$ and $D = End_R(N)$ by proposition 3.3. Since $M_t(D)$ is a simple ring then R is a simple ring. □

> **Corollary 3.8.** Let R be a simple ring and M a left R-module. If M is left artinian then there exists an R-module isomorphism $M \cong \bigoplus_{i=1}^{n} W$, where W is a unique up to isomorphism faithful simple R-submodule of M and n is the number of faithful simple submodules of M isomorphic to W.

Proof. Let R be a simple ring and M a left R-module. Suppose M is left artinian. Then M has a non-trivial simple R-submodule H, furthermore H is a faithful simple R-module because it is non-trivial and R is a simple ring. In the proof of proposition 3.7, replace the left artinian R-module R with our left artinian R-module M and the replace the faithful simple module P of R with our H. Next, employ the same reasoning that was used to show that if R has a faithful simple R-submodule then R is simple but only until we proved the R-module isomorphism $R \cong \bigoplus_{i=1}^{n} P$ where n is the number of faithful simple submodules of R. Instead, we obtain the R-module isomorphism $M \cong \bigoplus_{i=1}^{n} H$ where n is the number of faithful simple R-submodules of M and H is unique up isomorphism. □

We also prove here "Burnside's proposition" (Farb & Dennis, 1993, p. 45) by using the first isomorphism theorem of rings and proposition 3.7.

> **Proposition 3.9** (Burnside)**.** Let R be a an algebra over the field K and M a simple left R-module with $dim_K(M)$ finite. If $End_R(M) \cong K$ then the map
>
> $$f : R \longrightarrow End_K(M)$$
> $$r \longrightarrow {}_rT$$
>
> where $End_K(M)$ is the endomorphism ring of M as a right K-module and ${}_rT$ is multiplication on the left by $r \in R$, is onto.

Proof. Let R be a an algebra over the field K and M a simple R-module with $dim_k(M)$ finite. Suppose $End_R(M) \cong K$, then M is naturally a right K-module. Define the map

$$f : R \longrightarrow End_K(M)$$
$$r \longrightarrow {}_rT$$

of R into the endomorphism ring of M as a right K-module, where ${}_rT$ is multiplication on the left by $r \in R$. We use the first isomorphism theorem of rings to get the ring isomorphism

$$\eta : R/Ann(M) \longrightarrow f(R) \tag{4}$$

The ring $f(R)$ is a subring of the ring $End_K(M)$ which is finite dimensional over K, thus $f(R)$ is also finite dimensional over K and hence left artinian. Since the ring $R/Ann(M)$ is isomorphic to $f(R)$ it follows that $R/Ann(M)$ is left artinian. Furthermore, we notice that M is a faithful simple $R/Ann(M)$-module.

We use proposition 3.7 on the ring $R/Ann(M)$ to conclude that $R/Ann(M)$ is a simple left artinian ring. Now by theorem 3.6 applied to the ring $R/Ann(M)$ together with $End_R(M) \cong K$, by hypothesis, we conclude that $R/Ann(M)$ is ring isomorphic to $End_K(M)$. It follows that $f(R) = End_K(M)$ which implies that f is onto. □

3.3 Tensor product distributes over finite direct sum of modules

This following proposition is very useful when dealing with tensor products and finite direct sums.

Lemma 3.10. Let E_i and Z be modules over R for $i = 1, 2, ..., n$. If $E = \bigoplus_{i=1}^{n} E_i$ then we have the R-module isomorphism

$$Z \otimes E \cong \bigoplus_{i=1}^{n} (Z \otimes E_i)$$

Proof. For E and each $i = 1, 2, 3, ..., n$ we have the canonical projections to a single component of the direct sum

$$\begin{gathered} \rho_i : E \longrightarrow E \\ (x_1, x_2, ..., x_i, ..., x_n) \mapsto (0, ..., x_i, ..., 0) \end{gathered}$$

We notice that $\rho_i \circ \rho_j = 0$ when $i \neq j$. R-module homomorphism between tensors are done component wise by definition, from this we define the R-module homomorphism for each $i = 1, 2, 3, ..., n$

$$\begin{gathered} T_i(id_Z, \rho_i) : Z \otimes E \longrightarrow \bigoplus_{i=1}^{n} (Z \otimes \rho_i(E)) \\ \sum_{j=1}^{m} z_j \otimes x_j \mapsto (0, \cdots, 0, \sum_{j=1}^{m} z_j \otimes \rho_i(x_j), 0, \cdots, 0) \end{gathered}$$

We notice that $T_i(id_Z, \rho_i) \circ T_j(id_Z, \rho_j) = T(id_Z \circ id_Z, \rho_i \circ \rho_j)$ thus $T_i(id_Z, \rho_i) \circ T_j(id_Z, \rho_j) = T(id_Z, 0) = 0$ for $i \neq j$ and 0 is the zero homomorphism.

We observe then that each T_i is a canonical injections on $\bigoplus_{i=1}^n (Z \otimes \rho_i(E))$. Therefore their sum $\sum_{i=1}^n T_i$ is an isomorphism of $Z \otimes E$ and $\bigoplus_{i=1}^n (Z \otimes \rho_i(E))$.

Observe that for all $i = 1, 2, \ldots, n$ we have R-module isomorphisms $Z \otimes \rho_i(E) \cong Z \otimes E_i$. By the universal property of direct sum of modules and the R-module isomorphisms $Z \otimes \rho_i(E) \cong Z \otimes E_i$ for all $i = 1, 2, 3, \ldots, n$ we obtain the unique R-module isomorphism $\bigoplus_{i=1}^n (Z \otimes \rho_i(E)) \cong \bigoplus_{i=1}^n (Z \otimes E_i)$. Therefore we have shown the R-module isomorphism $Z \otimes E \cong \bigoplus_{i=1}^n (Z \otimes E_i)$. □

3.4 Properties of *K*-algebra tensor products

As we said earlier, we consider only algebras over a field that are associative and have multiplicative identity. Let A and B be K-algebras and form the tensor product of algebras $A \otimes_K B$, we have the K-algebra maps

$$\begin{aligned} \rho : A &\longrightarrow A \otimes_K B \\ a &\mapsto a \otimes 1 \end{aligned}$$

$$\begin{aligned} \eta : B &\longrightarrow A \otimes_K B \\ b &\mapsto 1 \otimes b \end{aligned}$$

We can view the algebra $A \otimes_K B$ as a free A-module by using the map ρ and observing that B itself is a free K-module, i.e $B = \bigoplus_{j \in J} K$ with the isomorphism

$$A \otimes_K B = A \otimes_K \bigoplus_{j \in J} K \cong \bigoplus_{j \in J} A \otimes_K K$$

thus if $\{e_j\}$ is a basis for B then $\{1 \otimes e_j\}$ is a basis for $A \otimes_K B$ as an A-module. We can view in the same way the algebra $A \otimes_K B$ as a free B-module by using the η map. Any element of a free module is zero only when all coefficients are zero, this implies that the maps ρ and η are injective so they are canonical inclusions; hence, there is a K-algebra isomorphism of A and B in $A \otimes_k B$.

We also note that $(a \otimes 1)(1 \otimes b) = (1 \otimes b)(a \otimes 1)$ for any $a \in A$ and $b \in B$. Thus A and B are commuting subalgebras of $A \otimes_K B$. Now we will prove a universal mapping property of $A \otimes_K B$ as a K-algebra.

Theorem 3.11. Given any K-algebra T, and any pair of K-algebra homomorphisms $f : R \longrightarrow T$ and $g : S \longrightarrow T$ such that $f(R)$ and $g(S)$ commute and $f|_K = g|_K$, then there exists a unique K-algebra homomorphism $h : R \otimes S \longrightarrow T$ such that $h \circ \tau = f$ and $h \circ \theta = g$ where τ is the canonical injection of R in $R \otimes S$ and θ is the canonical injection of S in $R \otimes S$.

Proof. Let T be an arbitrary K-algebra, and any pair of K-algebra homomorphisms $f : R \longrightarrow T$ and $g : S \longrightarrow T$ such that $f(R)$ and $g(S)$ commute and $f|_k = g|_k$. Since $f(R)$ and $g(S)$ commute and $f|_K = g|_K$ we can define the K-bilinear map

$$\begin{aligned} \Psi : R \times S &\longrightarrow T \\ (r, s) &\mapsto f(r)g(s) \end{aligned}$$

Indeed we have that $(kr, t) = (r, kt)$ for any $k \in K$ and Ψ is K-linear when r or t are fixed. However, since f and g are K-algebra homomorphism, we actually have K-algebra homomorphisms when r and t are fixed. Thus by the universal property of tensor products we have a unique induced R-linear map

$$\begin{aligned} h : R \otimes S &\longrightarrow T \\ \sum_{i=1}^{m} r_i \otimes s_i &\mapsto \sum_{i=1}^{m} f(r_i)g(s_i) \end{aligned}$$

we show that is also a K-algebra homomorphism

$$\begin{aligned} h((\sum_{i=1}^{m} r_i \otimes s_i)(\sum_{j=1}^{n} r_j \otimes s_j)) &= h(\sum_{i=1}^{m}\sum_{j=1}^{n} r_i r_j \otimes s_i s_j) \\ &= \sum_{i=1}^{m}\sum_{j=1}^{n} f(r_i r_j)g(s_i s_j) \\ &= \sum_{i=1}^{m}\sum_{j=1}^{n} f(r_i)f(r_j)g(s_i)g(s_j) \\ &= \sum_{i=1}^{m}\sum_{j=1}^{n} f(r_i)g(s_i)f(r_j)g(s_j) \\ &= \sum_{i=1}^{m} f(r_i)g(s_i)(\sum_{j=1}^{n} f(r_j)g(s_j)) \\ &= (\sum_{i=1}^{m} f(r_i)g(s_i))(\sum_{j=1}^{n} f(r_j)g(s_j)) \\ &= h((\sum_{i=1}^{m} r_i \otimes s_i))h((\sum_{j=1}^{n} r_j \otimes s_j)) \end{aligned}$$

we also show that h maps the multiplicative identity in $R \otimes S$ to the multiplicative identity in T, we have

$$h(1 \otimes 1) = f(1)g(1) = 1$$

Thus h is indeed a K-algebra homomorphism. We also have the tensor map

$$\begin{aligned} \varphi : R \times S &\longrightarrow R \otimes S \\ (r, s) &\mapsto r \otimes s. \end{aligned}$$

We can identify R with $(R, 1)$ and S with $(1, S)$. We have the canonical inclusions $\eta_1 : R \longrightarrow R \times S$ and $\eta_2 : S \longrightarrow R \times S$. Now we compose the previous canonical inclusions with the tensor map to get $\tau = \varphi \circ \eta_1$, which is the canonical inclusion of R in $R \otimes S$, and $\theta = \varphi \circ \eta_2$, which is the canonical inclusion of S in $R \otimes S$. Therefore h is the unique K-algebra homomorphism such that $h \circ \tau = f$ and $h \circ \theta = g$. □

3.5 Tensor product of a simple algebra and a central simple algebra is a simple algebra

The following theorem will be an important technical step in proving a theorem involving maximal subfields of finite dimensional associative division algebras. This theorem can be found in Herstein's book Noncommutative Rings (Herstein, 1971) on page 90.

From there we will use the key idea that there exist elements in the tensor product of a simple algebra B and a central simple algebra A over the same base field K with the least number of non-zero summands in their linear combination. We mean if n is such number of non-zero summands then any element x of the tensor product with number of non-zero summands less than n imply $x = 0$. Now we give the proof of the theorem.

Theorem 3.12. If A is a central simple algebra over K and B is a simple algebra containing K in its center then $A \otimes_K B$ is a simple algebra.

Proof. Let A be a central simple algebra over K and B a simple algebra containing K in its center. Let I be a non zero ideal of $A \otimes_K B$, clearly $I \subseteq A \otimes_K B$. Pick $x \in I$ with the least number of non-zero summands of its linear combination, say $x = \sum_{i=1}^{r} a_i \otimes b_i$; thus, if x' has a number of non-zero summands $n \leq r$ then $x' = 0$.

We have that $A \otimes 1 = \{a \otimes 1 \mid \forall \in A\}$ is a subalgebra of $A \otimes_K B$. From the element x in $A \otimes_K B$ that we picked before, we have that $(A \otimes 1)x(A \otimes 1) \in I$. Thus $\sum_{i=1}^{r} ha_it \otimes b_i$ with $h, t \in A$ arbitrary is element of I.

We recall that A is a simple algebra, thus $AaA = A$ for any $a \in A$, from this we can write the multiplicative identity of A as $1 = \sum_{i=1}^{n} s_iat_i$. Next, we choose elements in the set $\{\sum_{i=1}^{r} ha_it \otimes b_i \mid h, t \in A\} \subset I$ and sum them such that we obtain $y = 1 \otimes b_1 + a'_2 \otimes b_2 + ... + a'_r \otimes b_r \in I$ and note that y has same number of non-zero summands has our picked x.

Now we notice that $(a \otimes 1)y - y(a \otimes 1) \in I$ for arbitrary $a \otimes 1 \in A \otimes 1$, consequently $y' = (a-a) \otimes b_1 + (aa'_2 - a'_2 a) \otimes b_2 + ... + (aa'_r - a'_r a) \otimes b_2 \in I$. We observe that the first term of y' is zero, thus y' has less number of non-zero summands than x, which implies $y = 0$. We know that B has a basis $\{e_j\}$ over K, with j an element of some index set J, and we can make $A \otimes_K B$ an A module by the ring homomorphism

$$\eta : A \longrightarrow A \otimes_K B$$
$$a \mapsto a \otimes 1$$

From this we have that $A \otimes_K B$ is free over A with basis $\{1 \otimes e_j \mid j \in J\}$. Since $y' = 0$ this implies $aa'_2 - a'_2 a = 0$ which can only happen if $a'_2 \in C(A) = K$ (recall A is central, thus its center is its base field). We observe also that since K is in the center of B, we have that y can be written in the following way

$$1 \otimes b_1 + a'_2 \otimes b_2 + ... + a'_r \otimes b_r = 1 \otimes b'_1 + 1 \otimes b'_2 + ... + 1 \otimes b'_r$$

From this we have that $1 \otimes (b'_1 + b'_2 + ... + b'_r) = 1 \otimes b' \in I$. Consequently, $(1 \otimes B)(1 \otimes b')(1 \otimes B) = 1 \otimes B \in I$. Since $1 \otimes B \in I$, then $(A \otimes 1)(1 \otimes B) \in I$. We have $A \otimes B \subseteq I$, thus $A \otimes B = I$. Therefore, $A \otimes_K B$ is a simple algebra. □

We also give the following proposition that says that the tensor product of two central simple algebras (CSA) is a central simple algebra. This proposition will help us define later the Brauer group of a field in the applications section.

Proposition 3.13. Let K be a field. If A and B are CSA over K then $A \otimes_K B$ is a CSA over K.

Proof. Suppose K is a field. Let A and B be any CSA over K. We form the algebra $A \otimes_K B$ (which we know is simple by Theorem 3.12) thus, we just have to prove that the center of $A \otimes_K B$ is K. Let $x = \sum_{i=1}^m a_i \otimes b_i \in Z(A \otimes_K B)$ be arbitrary (recall Z(S) is the center of an algebra S). We have for any $y = \sum_{j=1}^n a_j \otimes b_j \in A \otimes_K B$ the property

$$\begin{aligned} xy =& yx \\ \sum_{j=1}^{n}\sum_{i=1}^{m} a_i a_j \otimes b_i b_j =& \sum_{j=1}^{n}\sum_{i=1}^{m} a_j a_i \otimes b_j b_i \end{aligned}$$

We observe that $a_i a_j = a_j a_i$ and $b_i b_j = b_j b_i$ for any $i = 1, 2, ..., n$ and $j = 1, 2, ..., m$, thus $a_i, b_i \in K$; from this, it follows $x \in K \otimes_K K \cong K$. Consequently $Z(A \otimes_K B) \subseteq K \otimes_K K$. Now if $z \in K \otimes_K K$ is arbitrary then clearly $z \in Z(A \otimes_K B)$. From this we have $K \otimes_K K \subseteq Z(A \otimes_K B)$. Therefore $Z(A \otimes_K B) = Z(A) \otimes_K Z(B) \cong K$. We have shown that the center of $A \otimes_K B$ is K, thus is a CSA over K. □

4 Proof of main theorem

The main theorem states that "any finite dimensional associative division algebra of finite dimension over the real numbers is isomorphic to either the real numbers, complex numbers or quaternions" (Palais, 1968). We are going to see the fundamental role that maximal subfields play in this classification theorem. They are the reason that there are not associative division algebras of dimension 3 over the real numbers, and also that quaternions are the only noncommutative associative division algebra of dimension 4 over the real numbers.

Let D be any finite-dimensional associative division algebra over the real numbers. This proof will be done by cases considering D as either noncommutative or commutative. First, we consider the noncommutative case to deduce the properties and dimension of D as $\mathbb{R}$-algebra, and after that the commutative case, which is basically to consider the field extensions of $\mathbb{R}$. The classical form of Noether-Skolem theorem is the key to prove an isomorphism to quaternions in the noncommutative case.

4.1 Dimension over center is a perfect square

An algebra can be either commutative or noncommutative. We work in this subsection in the noncommutative case. Let D be a noncommutative finite-dimensional associative division algebra over $\mathbb{R}$. We observe that for the noncommutative case we get $C_D(D) = \mathbb{R}$, thus $Z(D) = \mathbb{R}$. Consequently, D is finite dimensional over its center.

We prove the following theorem that gives us the surprising result that "the dimension of D over its center is a perfect square"(Herstein, 1971, p. 91). We give here a more detailed proof of this theorem.

The following proposition (Herstein, 1971, p. 50) is a key step to prove the mentioned theorem.

Proposition 4.1. Let F be an algebraically closed field. If B is a division algebra that is also algebraic over F then $B = F$.

Proof. Let F be an algebraically closed field and B a division algebra algebraic over F. First, we have by definition of algebra that $F \subseteq B$. Furthermore, we have that F splits every polynomial in $f(x) \in F[x]$ because F is algebraically closed. Let $h \in B$ arbitrary, since B is algebraic over F then there exists a polynomial $g(x) \in F[x]$ such that $g(h) = 0$. Since g(x) splits in F we have that

$$0 = g(h) = (h - f_1)\ (h - f_2)\ ...(h - f_n)$$

However B is a division algebra, thus it does not have zero divisors, which implies that at least one $(h-f_i)$ is zero. Hence, $h = f_i$ for some $i = 1, 2, ..., n$. Since $h \in B$ was arbitrary we have $B \subseteq F$. Therefore $B = F$. □

Theorem 4.2. If D is a finite-dimensional division algebra over its center K, then the dimension of D over K is a perfect square.

Proof. Let $\overline{K}$ be an algebraic closure of K and D be a finite-dimensional division algebra over its center K. We have that D and $\overline{K}$ are K-algebras. We form the K-algebra $\overline{D} = \overline{K} \otimes_K D$. We have that D is finite dimensional over its center K, and consequently a finite free K-module, thus we get the following K-module isomorphism

$$\overline{D} = \overline{K} \otimes_K D = \overline{K} \otimes_K \bigoplus_{i=1}^{n} K_j \cong \bigoplus_{i=1}^{n} \overline{K} \otimes_K K \cong \bigoplus_{i=1}^{n} \overline{K}$$

where we have used the following K-module isomorphism

$$\begin{aligned} g : \overline{K} &\longrightarrow \overline{K} \otimes_K K \\ r &\mapsto r \otimes_K 1 \end{aligned}$$

because for any $a_1, a_2 \in \overline{K}$ and any $k \in K$ we have

1. $g(a_1 + a_2) = (a_1 + a_2) \otimes 1 = a_1 \otimes +a_2 \otimes 1 = g(a_1) + g(a_2)$
2. $g(ka) = (ka) \otimes 1 = k(a \otimes 1) = k\, g(a)$
3. g is injective because $a \otimes 1 = 0 \Leftrightarrow a = 0$
4. We have obviously $g(\overline{K}) \subseteq \overline{K} \otimes_K K$. Let $x \in \overline{K} \otimes_K K$ arbitrary, we observe $x = \sum_{i=1}^{m} a_i \otimes k_i = \sum_{i=1}^{m} k_i a_i \otimes 1 = \sum_{i=1}^{m} a_i' \otimes 1$; hence, we get $x = a'' \otimes 1$. Consequently $x \in g(\overline{K})$ and $g(\overline{K}) = \overline{K} \otimes_K K$. Therefore, g is surjective.

From the previous K-module isomorphism and by recalling that $\overline{D}$ as an algebra is a free $\overline{K}$-module with basis $\{1 \otimes e_j\}$ where $\{e_j\}$ is a basis of D we have

$$\overline{D} = \overline{K} \otimes_K D \cong \bigoplus_{i=1}^{n} \overline{K} \tag{5}$$

Therefore, we conclude that $[\overline{D} : \overline{K}] = [D : K]$.

Now by Theorem 3.12 we have that $\overline{D} = \overline{K} \otimes_K D$ is a simple algebra and is also left artinian by the previous isomorphism; hence, by Theorem 3.6 of the classification of left artinian rings we have the isomorphism

$$\overline{D} \cong M_m(D')$$

for a unique m and some division ring D' up to isomorphism. Furthermore, we observe that D' is a finite dimensional algebra over $\overline{K}$ because of isomorphism 5 and we recall that $D' = End(V)$ where V is a unique up to isomorphism simple module of $\overline{D}$ and $\overline{D}$ is a finite free $\overline{K}$-module. We apply proposition 4.1 to D'.

We know that D' is finite dimensional over $\overline{K}$, thus D' is algebraic over $\overline{K}$. Since $\overline{K}$ is algebraically closed and D' is algebraic over $\overline{K}$, then by Proposition 4.1 we obtain $D' = \overline{K}$. From this we have

$$\overline{D} \cong M_m(\overline{K}) \tag{6}$$

Recall that $\overline{D}$ is a finite free $\overline{K}$-module, thus by isomorphism 6 we have $[\overline{D} : \overline{K}] = m^2$, but we also have $[\overline{D} : \overline{K}] = [D : K]$. Therefore $[D : K] = m^2$, the dimension of D over its center is a perfect square. □

We apply theorem 4.2 to our noncommutative D, recall if D is noncommutative then D is an associative division algebra that is finite dimensional over its center $\mathbb{R}$. Therefore, we have that $[D : \mathbb{R}] = m^2$ for some non-zero integer m.

4.2 Maximal subfields and the commutative case

The following theorem elucidates the great impact of maximal subfields to our noncommutative D. Recall that D always has maximal subfields; we discussed about this fact in the Algebras subsection "Subfields of division algebras". The following theorem can be found on page 96 of Farb and Dennis' book Noncommutative Algebra(see references), we also give here a more detailed explanation without using the theory leading to the Centralizer Theorem (see page 93 of the same book) but instead Burnside's proposition which we proved in the section of the classification theorem of simple left artinian rings.

Theorem 4.3. Let B be a central division algebra over the field K and $[B : K] = n^2$. If L is any maximal subfield of B then $[L : K] = n$.

Proof. Let B be a central division algebra over the field K and $[B : K] = n^2$. We have that B itself is a simple regular module, which is the key to our proof. Let L be an arbitrary maximal subfield of B. We notice that B is naturally a ${}_BB_L$ bimodule, thus, we have the following K-algebra homomorphisms from B and L to the endomorphism ring $End_K(B)$(observe it does not matter if we consider B as a right or left K-module because K is in the center of B):

$$f : B \longrightarrow End_K(B)$$
$$b \mapsto {}_bT$$

and

$$\begin{aligned} g : L &\longrightarrow End_K(B) \\ l &\mapsto T_l \end{aligned}$$

Where ${}_bT$ is ring multiplication by the left by $b \in B$, and similarly T_l is multiplication by the right by $l \in L$. We observe that since B is a ${}_BB_L$ regular bimodule then $f(B) \circ g(L) = g(L) \circ f(B)$, and furthermore, when both f and g are evaluated in K, we get $f(K) = g(K)$. This allows us to apply Theorem 3.11 to obtain a unique K-algebra homomorphism

$$h : B \otimes_K L \longrightarrow End_K(B)$$

Thus, we view the bimodule ${}_BB_L$ as a left $B \otimes_K L$-module B. Notice that B is a simple $B \otimes_K L$-module B, also by Theorem 3.12 we have that $B \otimes_K L$ is a simple K-algebra. Therefore, B is a faithful simple left $B \otimes_K L$-module.

Now we obtain $End_{B \otimes_K L}(B)$, first we observe that $End_{B \otimes_K L}(B) \subset End_B(B)$ thus, if $g \in End_{B \otimes L}(B)$ then $g = g_b$, i.e ring multiplication by the right for some $b \in B$

$$\begin{aligned} g_b : B &\longrightarrow B \\ x &\mapsto xb \end{aligned}$$

Furthermore, we must have $g_b(xl) = g_b(x)l$ for every $l \in L$. Consequently, we have

$$\begin{aligned} g_b(xl) &= (xl)b \\ &= g_b(x)l \\ &= (xb)l \end{aligned}$$

We notice that $bl = lb$ thus $b \in C_B(L) = L$, so $b = l' \in L$. As a result,

$$L \cong End_{B \otimes_K L}(B) \tag{7}$$

Recall that B is a simple $B \otimes_K L$-module. B is finite-dimensional over L because B is finite-dimensional over K by hypothesis (note any descending sequence of L-modules of B is also a descending sequence of K-modules of B), and $B \otimes_K L$ is also a L-algebra. Also recall $L \cong End_{B \otimes_K L}(B)$, thus B is a right L-module. We can apply Burnside's proposition 3.9 to the L-algebra $B \otimes_K L$ and the simple $B \otimes_K L$-module B to obtain the onto ring homomorphism

$$\begin{aligned} \theta : B \otimes L &\longrightarrow End_L(B) \\ \sum_{i=1}^{t} b \otimes l &\mapsto \sum_{i=1}^{t} {}_bT \circ T_l \end{aligned}$$

We claim that θ is one to one. Since B is a division algebra, then B has no zero divisors which implies that either $b = 0$ or $l = 0$ in the θ map. We know by the properties of the tensor product that $0 \otimes l = b \otimes 0 = 0 \otimes 0$ for any $b \in B$, $l \in L$. Hence, $ker\theta = \{0 \otimes 0\}$. Another way to prove θ is one to one is to notice that $B \otimes_K L$ is a simple K-algebra (as a result a simple ring) and θ is a non-zero homomorphism. Consequently, θ is one to one. We conclude that θ is a ring isomorphism.

Since the dimension of B over L is finite, we let $[B : L] = m$. From this we obtain the isomorphism

$$B \otimes L \cong \mathbf{M}_m(L) \tag{8}$$

From isomorphism 8 we have $[B \otimes_K L : L] = m^2$, and also since B is central finite over its center K we have $[B : K] = [B \otimes_K L : L]$. Consequently, we have $[B : K] = m^2$. Furthermore, by hypothesis the dimension of B over its center K is a perfect square, thus, we have $[B : K] = n^2 = m^2$ so $m = n$. But we had $[B : L] = m$ and we also note that $[B : L][L : K] = m^2$, this implies $[L : K] = n$. □

We apply theorem 4.3 to our noncommutative D by noticing that any maximal subfield L of D must be isomorphic to $\mathbb{C}$ because L is an algebraic closure of $\mathbb{R}$ and it is unique up to isomorphism. Hence, $[L : \mathbb{R}] = 2$, by Theorem 4.3 (which we just proved) we conclude that $[D : \mathbb{R}] = 4$. This property of the maximal subfields of the noncommutative D is the reason that there is not associative division algebras of dimension 3 over $\mathbb{R}$.

Commutative case: Suppose that D is commutative. Hence, we have that D is a field which contains $\mathbb{R}$, also $[D : L] = 1$ and has the property $[D : \mathbb{R}] = [L : \mathbb{R}]$. It follows that either $D \cong \mathbb{C}$ or $D \cong \mathbb{R}$.

4.3 Isomorphism to quaternions $\mathbb{H}$

We prove in this subsection that the noncommutative D is isomorphic to the quaternions $\mathbb{H}$. To do this, we use our previous result that $[D : \mathbb{R}] = 4$ and the classical form of Noether-Skolem theorem which involves only a central simple K-algebra and its simple K-subalgebras. The general form of Noether-Skolem theorem can be found for example in Herstein's book on page 99 and Farb and Dennis' book on page 93. We need the following lemma, found on page 45 of Farb and Dennis' book.

Lemma 4.4. *Let A be any central simple K-algebra which is finite-dimensional over the base field K and A^{op} the opposite ring of A. Then, there exists a K-algebra isomorphism $A \otimes_K A^{op} \cong End_K(A)$.*

Proof. Let A be any central simple K-algebra which is finite dimensional over the base field K and A^{op} the opposite ring of A. Notice that A is an A-A-module, that is, a regular bimodule over A itself. Recall that $End_K(A)$ is the ring of endomorphisms of A as K-module, ${}_aT \in End_K(A)$ is ring multiplication on the left by $a \in A$ and similarly, $T_a \in End_K(A)$ is ring multiplication on the right by $a \in A$. Define the K-algebra homomorphisms

$$\begin{aligned} h : A &\longrightarrow End_K(A) \\ a &\mapsto {}_aT \end{aligned}$$

and

$$\begin{aligned} f : A^{op} &\longrightarrow End_K(A) \\ a' &\mapsto T_{a'} \end{aligned}$$

We note that $h(a) \circ f(a') = f(a') \circ h(a) \in End(A)$ for all $a, a' \in A$ and $h(k) = f(k)$ for all $k \in K$. We use the K-algebra homomorphisms h and f with theorem 3.11 to deduce that A has the structure of a left $A \otimes A^{op}$-module. Our previous application of theorem 3.11 also gives us the unique induced K-algebra homomorphism

$$\begin{aligned} g : A \otimes_K A^{op} &\longrightarrow End_K(A) \\ \sum_{i=1}^{n}(a_i \otimes a_i') &\mapsto \sum_{i=1}^{n} {}_{a_i}T \circ T_{a_i'} \end{aligned}$$

We claim that g is a K-algebra isomorphism. We use Burnside's proposition (proposition 3.9) to prove that g is onto. We first notice that $End_{A \otimes_K A^{op}}(A) = \{T_k | \ k \in K\}$, thus, we have the ring isomorphism $End_{A \otimes_K A^{op}}(A) \cong K$ and this implies that A is naturally a right K-module. Since ${}_kT = T_k$ for all $k \in K$ the structures of A as a left K-module and a right K-module are the same, hence, $End_K(A)$ is the same ring for both structures.

Now for any non-zero $a'' \in A$, consider the cyclic left $A \otimes_K A^{op}$-submodule $\{xa'' | \ \ x \in A \otimes_K A^{op}\}$ of the left $A \otimes_K A^{op}$-module A and observe that $\{xa'' | \ \ x \in A \otimes_K A^{op}\}$ is a non-trivial ideal of A, but A is a simple algebra. Thus, $\{xa'' | \ \ x \in A \otimes A^{op}\} = A$, since a'' is arbitrary we conclude that A is a simple left $A \otimes_K A^{op}$-module A.

In summary, we have the K-algebra $A \otimes_K A^{op}$, A is a simple left $A \otimes_K A^{op}$-module, also A is finite-dimensional over K by hypothesis, and $End_{A \otimes_K A^{op}}(A) \cong K$. Thus by Burnside's proposition the K-algebra homomorphism g is onto.

Finally, we show that g is one to one by recalling that the tensor product of a central simple K-algebra and a simple algebra which has K in its center is a simple K-algebra by theorem 3.12. We have by hypothesis that A is a central simple K-algebra, A^{op} is simple because any ideal of A is an ideal of A^{op} and any ideal of A^{op} is an ideal of A, and A^{op} has K in its center. Consequently, $A \otimes_K A^{op}$ is a simple K-algebra. Since g is a non-zero K-algebra homomorphism and $A \otimes_K A^{op}$ is simple, then the kernel of g is trivial, then g is one to one. Therefore, g is a K-algebra isomorphism of $A \otimes_K A^{op}$ and $End_K(A)$. □

Theorem 4.5 (Noether-Skolem)**.** Let A be any central simple K-algebra which is finite-dimensional over K and let B be any simple K-subalgebra of A. If $f : B \longrightarrow A$ is any non-zero K-algebra homomorphism of B into A, then there exists an invertible element $t \in A$ such that $f(b) = tbt^{-1}$ for all $b \in B$.

Proof. Let A be any central simple K-algebra which is finite-dimensional over K and let B be any simple K-subalgebra of A. Suppose $f : B \longrightarrow A$ is any non-zero K-algebra homomorphism of B into A. This proof of Noether-Skolem theorem uses Herstein's idea to consider the use of the K-algebras $B \otimes_K A$ and $f(B) \otimes_K A$.

First we use lemma 4.4 on A to get the K-algebra isomorphism

$$g : A \otimes_K A^{op} \longrightarrow End_K(A)$$

$$\sum_{i=1}^{n}(a_i \otimes a_i') \mapsto \sum_{i=1}^{n} {}_{a_i}T \circ T_{a_i'}$$

In lemma 4.4 we also showed that A is a left $A \otimes_K A^{op}$-module. Now we consider the left $B \otimes_K A^{op}$-module A and the left $f(B) \otimes_K A^{op}$-module A. Since $f : B \longrightarrow A$ is one to one, notice the K-algebra isomorphism

$$\psi : B \otimes_K A^{op} \longrightarrow f(B) \otimes_K A^{op}$$

$$\sum_{i=1}^{n}(b_i \otimes a_i') \mapsto \sum_{i=1}^{n}(f(b_i) \otimes a_i')$$

Since $B \otimes_K A^{op}$ is a simple K-algebra (notice A^{op} is a central simple K-algebra) and A is a left artinian $B \otimes_K A^{op}$-module because A is finite dimensional over K, we use corollary 3.8 to get the $B \otimes_K A^{op}$-module isomorphism $A \cong \bigoplus_{i=1}^{n} W$ where W is a unique up to isomorphism faithful simple $B \otimes_K A^{op}$-submodule of A and n is the number of faithful simple $B \otimes_K A^{op}$-submodules of A.

Notice that both A and W are also left $f(B) \otimes_K A^{op}$-modules by the K-algebra isomorphism ψ. Again, by corollary 3.8 we have the $f(B) \otimes_K A^{op}$-module isomorphism $A \cong \bigoplus_{i=1}^{n} V$ where V is a unique up to isomorphism faithful simple $f(B) \otimes_K A^{op}$-submodule of A and n is the number of faithful simple $f(B) \otimes_K A^{op}$-submodules of A. Notice that n is the same number as faithful simple $B \otimes_K A^{op}$-submodules of A. Thus, we have a $B \otimes_K A^{op}$-module isomorphism

$$\varphi : \bigoplus_{i=1}^{n} W \longrightarrow \bigoplus_{i=1}^{n} V$$

which has the property $\varphi((b \otimes a)x) = (f(b) \otimes a)\varphi(x)$ for arbitrary $(b \otimes a) \in B \otimes_K A^{op}$ and for all $x \in \bigoplus_{i=1}^{n} W$. Observe that φ is also a $B \otimes_K A^{op}$-module endomorphism of A and a K-module endomorphism of A. By the K-algebra isomorphism g we have $\varphi = \sum_{i=1}^{n} {}_{a_i}T \circ T_{a'_i}$.

Since φ is an isomorphism, the sum $\sum_{i=1}^{n} {}_{a_i}T \circ T_{a'_i}$ must be invertible in $End_K(A)$. Observe that by the property of φ the invertible sum has the form $\sum_{i=1}^{n} {}_{a_i}T \circ T_{k'_i}$ where $k'_i \in K$ for $i = 1, 2, ..., n$. Thus, by a property of the tensor product we must have $\varphi = {}_tT$ for some invertible $t \in A$.

Recall we had the property $\varphi((b \otimes a)x) = (f(b) \otimes a)\varphi(x)$. We then have ${}_tT((b \otimes a)x) = (f(b) \otimes a)_tT(x)$ which can be written as $tbxa = f(b)txa$. Therefore, for arbitrary $b \in B$ we have $f(b)t = tb$, which implies $f(b) = tbt^{-1}$. □

We apply the classical Noether-Skolem theorem to our noncommutative D by setting a maximal subfield $L \subset D$ as our simple K-subalgebra, and using the K-algebra homomorphism

$$\begin{gathered} f : L \longrightarrow D \\ a + bi \mapsto a - bi \end{gathered}$$

where $i^2 = -1$ and $a, b \in \mathbb{R}$, thus $t \in D$ exists such that $a - bi = t(a + bi)t^{-1}$.

Observe that $t \notin L$ because otherwise it would commute with $a + bi$ and f would be the identity mapping. Also observe $a + bi = t^2(a + bi)t^{-2}$ which implies $t^2 \in C_D(L) = L$ or $t^2 \in C_D(D) = \mathbb{R}$. Suppose $t^2 \in C_D(L) = L$, consequently there exists $x \in L$ such that $t^2 + x = 0$. In this case $t^2 + x = 0$ has solutions in L, hence $t \in L$. However, recall $t \notin L$, we have a contradiction. Hence, we must have $t^2 \in \mathbb{R}$. As a result, $t^2 + r = 0$ for some $r \in \mathbb{R}$. If $r < 0$ then $t \in \mathbb{R}$ which is a contradiction because we observed that $t \notin L$. Hence, $r > 0$ which implies $t^2 = -r$. Since $r > 0$ then there exists a positive number $u \in \mathbb{R}$ such that $r = u^2$. So we have $t^2 = -u^2$.

Since $\left(tu^{-1}\right)^2 = -1$ we define $j = tu^{-1}$. Observe that we also have $\left(t^{-1}u\right)^2 = -1$ and define $j^{-1} = t^{-1}u = -j$. We showed that there is an element $j \in D \setminus L$ with the property $j^2 = -1$.

Next define $k = ij \in D$. From this we have

$$\begin{aligned} k\{-k\} &= (ij)\{-(ij)\} \\ -k^2 &= i\{ji(-j)\} \\ -k^2 &= i(-i) \\ k^2 &= -1 \end{aligned}$$

The inverse of k is $k^{-1} = -k$. We notice that $1,\ i,\ j,\ k$ are four linearly independent elements in the noncommutative D and we recall that we got $[D : \mathbb{R}] = 4$. Also we have $i^2 = j^2 = k^2 = -1$ and $ijk = -1$ which are the multiplication rules for quaternions. Therefore, the noncommutative D is isomorphic as an $\mathbb{R}$-algebra to the quaternions $\mathbb{H}$. This finishes the proof of our main theorem.

5 Application

Before we begin this chapter we make this **important assumption**: all the **CSA (central simple algebras)** and algebras that we work in this chapter are finite dimensional over their base field K. We use this assumption simply to avoid the overuse of the phrase "finite dimensional over the base field", so that the text is easier to understand. In this chapter we will learn one application of Frobenius' Theorem.

5.1 Brauer group

First, we show some history of the Brauer group, after that we will learn its relation to this article, then we show that the Brauer group is indeed a group, finally we apply Frobenius' Theorem to the Brauer group of the real numbers. It is important to indicate that in this subsection we will only give the statements of the theorems without proof but we will be giving references to them in the literature, which the reader can understand with the knowledge acquired in this article.

5.1.1 Definition

The Brauer group of a field K "was defined by R. Brauer in 1929"(Farb & Dennis, 1993, p. 109). Farb and Dennis (1993) mention that "computing the Brauer group of a field is a classical problem which has strong ties with number theory and algebraic geometry". In essence, we use the Brauer group of a field K to classify all finite dimensional central division algebras over K. Recall that all our algebras are associative and have a multiplicative identity. Recall that by proposition 3.13 we have that the algebra tensor product, also called ordinary tensor product, of CSA over K is another CSA over K. The ordinary tensor product of CSA over K is important because it is the group operation in the Brauer group of K.

The set of all CSA over K is a group under the operation of ordinary tensor product of CSA over K. The Brauer group of K is the group of equivalence classes of CSA over K by the similarity relation (which we define later). Each finite dimensional central division algebra over K belongs exactly to one of those equivalence classes of the CSA over K. The following definitions, lemmas and propositions used to define the Brauer group of a field K appear on the book Noncommutative Algebra by Farb and Dennis on the Brauer chapter.

Definition 5.1 (Similarity relation)**.** Let H and W be finite dimensional central simple algebras over the field K. We say that H and W are **similar**, written $H \backsim W$, if any of the following conditions hold:

1. If $H \cong M_n(D)$ and $W \cong M_n(E)$ then $D \cong E$.
2. There exists integers $m,\ n$ such that $H \otimes M_m(K) \cong W \otimes M_n(K)$.
3. There exists integers $m,\ n$ such that $M_m(H) \cong M_n(W)$.
4. If M is a unique simple H-module up to isomorphism and N is a unique simple W-module up to isomorphism then $End_H(M) \cong End_W(M)$.

It is easy to show that the similarity relation is an equivalence relation on the group of CSA over K with the group operation of ordinary tensor product of CSA over K.

Definition 5.2 (Brauer group of a field K)**.** The **Brauer group** of a field K, denoted **Br(K)**, is the set of equivalence classes of CSA over K under the equivalence relation of similarity. The operation in this group is the ordinary tensor product of CSA over K. The identity element is the equivalence class of K. We denote the equivalence class of an arbitrary H, a CSA over K, by $[\mathbf{H}]$.

5.1.2 Brauer group is abelian

We have to show that the Brauer group is well defined and is a group. On pages 111-112 of Farb and Dennis' book there are the following lemmas to prove it

Lemma 5.3. Let $M_n(K)$ be any full matrix K-algebra and A any K-algebra. We have the following K-algebra isomorphisms

1. $M_n(A) \cong A \otimes_K M_n(K)$.
2. $M_n(K) \otimes_K M_m(K) \cong M_{nm}(K)$

The previous lemma is used to prove the following lemma. It shows that multiplication in the Brauer group of a field K is well-defined.

Lemma 5.4. Let W_1, W_2, H_1, H_2 be CSA over K. If $W_1 \backsim W_2$ and $H_1 \backsim H_2$ then $W_1 \otimes_K H_1 \backsim W_2 \otimes_K H_2$.

The previous two lemmas are used to show that $\mathrm{Br}(K)$ is a well-defined abelian group.

Proposition 5.5. The set of equivalence classes in $\mathrm{Br}(K)$ with the operation $[H] * [W] = [H \otimes_K W]$ for any two $[H], [W] \in Br(K)$ is a well-defined abelian group.

5.1.3 Brauer group of the real numbers

Here we obtain the Brauer group of the real numbers. An easy proof of it requires the use of Frobenius' Theorem.

Proposition 5.6. The Brauer group of the real numbers $\mathrm{Br}(\mathbb{R})$ is isomorphic to $\mathbb{Z}_2$.

Proof. Let $\mathrm{Br}(\mathbb{R})$ be the Brauer group of the real numbers. By definition of the Brauer group we know that each equivalence class $[W] \in$Br$(\mathbb{R})$ has a unique up to isomorphism central division algebra finite-dimensional over $\mathbb{R}$. By Frobenius' Theorem on associative division algebras over $\mathbb{R}$ we have that the only such algebras that are central over $\mathbb{R}$ are $\mathbb{R}$ and the quaternions $\mathbb{H}$ up to isomorphism.

We conclude that $\mathrm{Br}(\mathbb{R})$ has only two equivalence classes, namely $[\mathbb{H}]$ and $[\mathbb{R}]$. Furthermore, we have $[\mathbb{H}] * [\mathbb{H}] = [\mathbb{H} \otimes \mathbb{H}] = [\mathbb{R}]$ by lemma 4.4 and we notice the $\mathbb{R}$-algebra isomorphism $\mathbb{H} \cong \mathbb{H}^{op}$. Thus, $[\mathbb{H}]$ generates $\mathrm{Br}(\mathbb{R})$. Therefore, we have the group isomorphism $\mathrm{Br}(\mathbb{R}) \cong \mathbb{Z}_2$. □

References

Ames, D. B. (1969). *An introduction to abstract algebra.* Pennsylvania, USA: INTERNATIONAL TEXTBOOK COMPANY.

Auslander, M., & Buchsbaum, D. (2014). Groups, rings, modules. In *Dover Books on Mathematics* (Dover ed., p. 295). New York, USA: Dover Publications, Inc.

Baez, J. C. (2001). The octonions. *Bulletin(New Series)of the American Mathematical Society*, *39*(2), 145-205. Retrieved from `http://www.ams.org/journals/bull/2002-39-02/S0273-0979-01-00934-X/` doi: 10.1090/S0273-0979-01-00934-X

Choudhary, P. (2008). *Abstract Algebra.* New York, USA: Oxford Book CO.

Conway, J. H., & Smith, D. A. (2003). *On Quaternions and Octonions: Their Geometry, Arithmetic and Symmetry* (1st ed.). Massachusetts, USA: A.K Peters, Ltd.

Dickson, L. E. (1914). LINEAR ALGEBRAS. In J. Leathem & G. Hardy (Eds.), *Cambridge Tracts in Mathematics and Mathematical Physics* (Vol. 16, p. 10-12). Cambridge, England: Cambridge University Press.

Dummit, D. S., & Foote, R. M. (2004). Field theory. In K. Santor & J. Battista (Eds.), *Abstract Algebra* (3rd ed., p. 543-544). New Jersey, USA: John Wiley and Sons, Inc.

Farb, B., & Dennis, R. K. (1993). Noncommutative Algebra. In *Graduate Texts in Mathematics* (1st ed., Vol. 144). New York, USA: Springer-Verlag.

Frobenius, F. G. (1878). Ueber lineare Substitutionen und bilineare Formen. *Journal fuer die reine und angewandte Mathematik*, *84*, 1-63.

Hamilton, W. R. (1853). Lectures on Quaternions: containing a systematic treatment of A New Mathematical Method. In *Lectures on Quaternions* (Vol. 1). Dublin, Ireland: Hodges and Smith.

Herstein, I. (1971, March). NONCOMMUTATIVE RINGS. In *The Carus Mathematical Monographs* (2nd ed., Vol. 15). USA: THE MATHEMATICAL ASSOCIATION OF AMERICA.

Hungerford, T. W. (1974). Algebra. In S. Axler, F. Gehring, & K. Ribet (Eds.), *Graduate Texts in Mathematics* (1st ed., Vol. 512). New York: Springer-Verlag.

Lam, T. Y. (2001). A first course in noncommutative rings. In *Graduate Texts in Mathematics* (2nd ed., Vol. 31, chap. 1, 3, 5). New York, USA: Springer-Verlag.

Lang, S. (2005). Algebra. In *Graduate Texts in Mathematics* (Revised 3rd ed., Vol. 211). New York, USA: Springer-Verlag.

McLaughlin, T. G. (2004). C.S.Peirce's Proof of Frobenius' Theorem on Finite-Dimensional Real Associative Division Algebras. *Transactions of the Charles S. Peirce Society*, *40*(4), 701-710. Retrieved from http://www.jstor.org/stable/40321024

Palais, R. (1968). The Classification of Real Division Algebras. *The American Mathematical Monthly,75(4), 366-368.* Retrieved from http://www.jstor.org/stable/2313414 doi: 10.2307/2313414

Pierce, R. (1982). Associative algebras. In F. Hearing, P. Halmos, & C. Moore (Eds.), *Graduate Texts in Mathematics* (1st ed., Vol. 88, chap. 1, 9, 12, 13). New York, USA: Springer-Verlag.

Raya, A., Rider, A., & Rubio, R. (2007). Sistemas generadores. In *Algebra y Geometria lineal* (p. 74-84). Barcelona, Spain: Editorial Reverte.

Roman, S. (2008). Advanced linear algebra. In S.Axler & K.A.Ribet (Eds.), *Graduate Texts in Mathematics* (3rd ed., Vol. 135, p. 382-383). New York,USA: Springer.

Solomon, R. (1995). On Finite Simple Groups an their Classification. *Notices of the AMS*, *42*(2), 231-239. Retrieved from http://www.ams.org/notices/199502/solomon.pdf