A Matricial Perspective of
Wedderburn’s Little Theorem

Celino Miguel
Instituto de Telecomunicações
Pólo de Coimbra
Laboratório da Covilhã
celino@ubi.pt

Abstract

Wedderburn’s classic Little Theorem states that all finite division rings are commutative. This beautiful result was been proved by many people using a variant of different ideias. In this paper we give a simple proof based in Matrix Theory.

Mathematics Subject Classification: 12E15, 12E20, 15A21

Keywords: Division Ring, Finite Field, Eigenvalue

1 Some Historical Notes.

Up until the XIX century, the emergence of number systems was a natural process, mostly fostered by the solving of polynomial equations. For instance, the field of complex numbers \( \mathbb{C} \) results from the mathematicians attempts to establish a process for solving cubic equations (for the history of the complex numbers origin see [10] or [2]). The mathematicians showed then no major concern for the precise definition of the structure of these new numbers which were making their entry into the world of mathematics.

In 1843 Hamilton first discovers the Quaternions and shortly thereafter the Octonions are discovered independently by John T. Graves and Arthur Cayley. These new Hypercomplex Systems are no longer fields. The commutative law of multiplication is no longer applicable to quaternions and with octonions the associative law of multiplication must also be abandoned. But every non-zero element still has an inverse. Moreover, division by a non-zero element is still possible, a property which was regarded by the founders of the theory as crucial. In this case we speak of a division algebra [2], [6].
In the second half of the nineteenth century, many other hypercomplex systems were discovered and investigated. There arose the important question of how much freedom there really exists in this apparent profusion of examples, and work began with the classification of certain types of these systems. Frobenius and Peirce showed in 1880 that the real numbers, the complex numbers and the quaternions are the only finite-dimensional division algebras over the real numbers [4], [2]. It is the first remarkable theorem on the structure theory of rings.

In a famous paper [13] from the year 1905, Wedderburn first stated his theorem, now considered a classic, that any finite division ring is commutative, that is, a finite field. The theorem interrelates two seemingly unrelated things, namely the number of elements in a certain algebraic system and the multiplication of that system. Wedderburn gave three different proofs for this theorem. This beautiful theorem has been proved by many people using a variety of different ideas.

Ernst Witt [1] gave us the best known proof which is in fact a simplified version of the first proof offered by Wedderburn. In his proof, Witt makes use of group theory, complex numbers and some basic number theory.

In [3] Hernstein presents two proofs: one follows essentially Witt’s proof whereas the second is of a much more algebraic nature and becomes technically rather complex. There are, of course, numerous other proofs available in the literature. Some, such as those found in [7] or [4], obtained the theorem by an application of the theory of simple algebras and use the famous Skolem-Noether Theorem while one other, based almost entirely on group theory, can be found in [5].

In this paper we present a proof based only in linear algebra, finite field theory and the well known fact, from group theory, that in a finite group $G$ the conjugates of a proper subgroup do not exhaust $G$.

2 Proof of Wedderburn’s Little Theorem.

The proof will be preceded by a well known lemma. For the sake of integrity we present a proof

**Lemma- 1** If $G$ is a finite group and $H$ is a proper subgroup, then $\bigcup_{g \in G} g^{-1}Hg$ does not exhaust $G$.

**Proof.** If $h \in H$, then

$$(gh)H(gh)^{-1} = g(hHh^{-1})g^{-1} = gHg^{-1}.$$ 

Thus, in the union $\bigcup_{g \in G} g^{-1}Hg$, the terms corresponding to $g$ and to $gh$, for $h \in H$, are the same. In other words, the terms corresponding to two elements
in each coset $gH$ are the same. Then, the number of elements other than the identity in the union is

$$\leq |G : H|(|H| - 1) = |G : H||H| - |G : H| = |G| - |G : H| < |G| - 1,$$

and the lemma follows. □

**Theorem- 1 (Wedderburn)** Every finite division ring is commutative.

**Proof.** Let $D$ be a finite division ring. As $D$ is finite, the characteristic is positive and it is necessarily a prime number $p$, or otherwise $D$ would have zero divisors. The $p$ distinct elements

$$0, 1, 2, \ldots, p - 1,$$

form a subfield of $D$ isomorphic to the prime field $\mathbb{Z}_p$. We can regard $D$ as a vector space over the field $\mathbb{Z}_p$. Call the dimension $n$, so each element of $D$ is uniquely determined by $n$ coordinates in $\mathbb{Z}_p$. Then, $|D| = p^n$ and, concerning the addition, $D$ is the direct sum of $n$ copies of $\mathbb{Z}_p$. In other words, as an additive group

$$D \cong \mathbb{Z}_p \oplus \mathbb{Z}_p \oplus \cdots \oplus \mathbb{Z}_p. \quad (1)$$

Regarding the multiplicative structure of $D$, the main idea is to observe that every ring is isomorphic to a subring of the endomorphisms ring of its additive group $[4]$. The endomorphisms ring of the additive group defined in $(1)$ is isomorphic to the ring of the matrices of order $n$ whose elements belong to the ring of the residual classes modulo $p$, i.e. the field $\mathbb{Z}_p$ $[8]$. We obtain thus a matricial perspective of the problem which is now confined to proving that a division ring included in $M_n(\mathbb{Z}_p)$ is commutative. The advantage offered by this perspective is that we can make use of the matrix theory and linear algebra.

We assume then that the division ring $D$ is contained in the ring of all matrices of order $n$ with elements in the prime field $\mathbb{Z}_p$, that is $D \subset M_n(\mathbb{Z}_p)$. The set of matrices

$$\hat{\mathbb{Z}_p} = \left\{ \begin{bmatrix} 0 & 0 & \cdots & 0 \\ 0 & 0 & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & 1 \end{bmatrix}, \ldots, \begin{bmatrix} p - 1 & 0 & \cdots & 0 \\ 0 & p - 1 & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & p - 1 \end{bmatrix} \right\},$$
is a copy of the prime field $\mathbb{Z}_p$ in $M_n(\mathbb{Z}_p)$. Denote it by $\hat{\mathbb{Z}}_p$. Let $F \subset D$ be a matrix maximal subfield of $D$. $F$ is a simple extension of the prime field $\hat{\mathbb{Z}}_p$, that is, there exists a matrix $A \in D$, such that, $F = \hat{\mathbb{Z}}_p(A)$, where $A$ is a root of a monic irreducible polynomial $f \in \hat{\mathbb{Z}}_p[x]$ [11].

As to the properties that the matrix $A$ must necessarily possess, it must be noted that from the fact that the polynomial $f$ is irreducible, we conclude that $f$ is the minimal polynomial of the matrix $A$ over the field $\hat{\mathbb{Z}}_p$. Since a finite field is perfect [11] it follows that the roots of $f$ are distinct. Since the polynomial $f$ is a factor of the characteristic polynomial of the matrix $A$, its degree is less than or equal to $n$. Let $m$ be the degree of the polynomial $f$.

We have then $|\hat{\mathbb{Z}}_p(A)| = |F| = p^m = GF(p^m)$.

Let $\alpha \in F$ be a root of $f$. Since every finite extension of a finite field is normal [11], it follows that $f$ splits in $F$. Then, the matrix $A$ is diagonalizable, that is, there exists a regular matrix $S \in M_n(F)$ such that

$$S^{-1}AS = \begin{bmatrix} \lambda_1 & 0 & \ldots & 0 \\ 0 & \lambda_2 & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \ldots & 0 & \lambda_n \end{bmatrix},$$

(2)

where $\lambda_i$, $i = 1, \ldots, n$, are the eigenvalues of the matrix $A$. The function

$$\Phi : \hat{\mathbb{Z}}_p(A) \longrightarrow \hat{\mathbb{Z}}_p(S^{-1}AS),$$

defined by $\Phi([q(A)]) = q(S^{-1}AS)$, where $q \in \hat{\mathbb{Z}}_p[x]$, is an isomorphism. That is, the maximal matrix field $F$ can be diagonalized. Since,

$$0 = f(A) = f(S^{-1}AS) = \text{diag}(f(\lambda_1), \ldots, f(\lambda_n)),$$

then $\lambda_i$, $i = 1, \ldots, n$, are roots of $f$. Then, each $\lambda_i$, $i = 1, \ldots, n$, is a primitive element for the extension $F$ of $\mathbb{Z}_p$. That is

$$F \cong \mathbb{Z}_p(\lambda_1) = \ldots = \mathbb{Z}_p(\lambda_n).$$

(3)

If $\lambda_k$ is a fixed root of $f$, then

$$\lambda_k, \lambda_k^p, \lambda_k^{p^2}, \ldots, \lambda_k^{p^{m-1}},$$

(4)

are the $m$ distinct roots of $f$ [11]. Since $(S^{-1}AS)^{p^k} \in \mathbb{F}$, for $k = 1, \ldots, m - 1$, the set $\lambda_i$, $i = 1, \ldots, n$, includes all roots of $f$.

Let $G$ be another matrix subfield of $D$ with the same order of $F$. As in the case of $F$ we have $G = \hat{\mathbb{Z}}_p(B)$, where $B$ is a root of a monic irreducible polynomial $q \in \hat{\mathbb{Z}}_p[x]$. Two finite fields of the same order are isomorphic [11]. Let then $\Psi : F \longrightarrow G$ be an isomorphism. $\Psi$ is the identity in the prime field
A matricial perspective of Wedderburn’s Little theorem

\[ \hat{\mathbb{Z}}_p. \] Observe that, the image of the matrix \( A \) under the isomorphism \( \Psi \) is a primitive element for the field \( G \). That is,

\[ G = \hat{\mathbb{Z}}_p(B) = \hat{\mathbb{Z}}_p(\Psi(A)). \] (5)

Without loss of generality we can assume that \( \Psi(A) = B \). Let \( h \in \hat{\mathbb{Z}}_p[x] \) be a polynomial that annihilates the matrix \( A \), that is \( h(A) = 0 \). Then we have

\[ 0 = \Psi[h(A)] = h(\Psi(A)) = h(B). \] (6)

Thus, the matrices \( A \) and \( B \) have the same annihilating polynomials and thus they have the same minimum polynomial. Then, the matrices \( A \) and \( B \) are similar [9]. There exists then a regular matrix \( L \) such that

\[ LFL^{-1} = G. \] (7)

That is, any two matrix subfields of \( D \) with the same order are conjugates.

Next we use the maximality of the matrix field \( F \). If we regard \( D \) as a vector space over the maximal subfield \( F \), we can define the linear operator, on this space, \( L : D \to D \) by

\[ L(X) = XA, \] (8)

for \( X \in D \). The set of polynomials that annihilates the operator \( L \) is the same set that annihilates the matrix \( A \). Since the minimum polynomial of a matrix does not depend on the field under consideration, as long as it contains the entries [12], the minimum polynomial of the operator \( L \) is the same as the minimum polynomial of the matrix \( A \). Hence, \( L \) is diagonalizable. Then, there is a basis

\[ \{B_1, \ldots, B_k\} \]

of \( D \) over \( F \) consisting of eigenvalues of \( L \). Let \( \lambda \in F \) be an eigenvalue of the operator \( L \), that is

\[ L(X) = \lambda X, \] (9)

for some nonzero vector \( X \in D \). From (9) we have

\[ XA = \lambda X \iff XAX^{-1} = \lambda. \] (10)

So, the matrix \( A \) is similar to the matrix \( \lambda \), and both have therefore the same minimum polynomial. Thus, the fields generated by \( A \) and by \( \lambda \), over \( \hat{\mathbb{Z}}_p \), are the same, that is

\[ \hat{\mathbb{Z}}_p(\lambda) = \hat{\mathbb{Z}}_p(A) = F. \] (11)
Let $Y \in D$ be another eigenvector corresponding to $\lambda$. From (10) we conclude
\[
X^{-1}\lambda X = Y^{-1}\lambda Y \iff YX^{-1}\lambda = \lambda YX^{-1}.
\] (12)
That is, $YX^{-1}$ commutes with $\lambda$ and hence commutes with any element of $\hat{\mathbb{Z}}_p(\lambda) = F$. From the maximality of $F$ we conclude that $YX^{-1} \in F$. If we define $Z = YX^{-1}$, we have $Y = ZX$. That is, the vectors $X$ and $Y$ are linearly dependent. Then each eigenspace of $L$ has dimension one. Thus, the number of linearly independent eigenvectors of $L$ is the same as the number of zeros of the polynomial $f$. Hence, we have
\[
[D : \mathbb{Z}_p] = [D : F] [F : \mathbb{Z}_p] = m^2.
\] (13)
Since $[D : \mathbb{Z}_p]$ is independent of $F$, all maximal subfields of $D$ have the same order. Thus, they are conjugates. Since every element of $D$ is contained in a maximal subfield, by the lemma the theorem follows. □

References


Received: April, 2011