Gulf Journal of Mathematics
Vol 16, Issue 1 (2024) 68-78

ISSN: 2309-4966
https://doi.org/10.56947/gjom.v16i1.1419

A NOTE ON WEDDERBURN AND HASSE THEOREMS

ILIAS ELMOUKI[1]* AND SEDDIK ABDELALIM[2]

Abstract. Wedderburn and Hasse theorems have always fascinated many algebraists as there have been just very few proofs not bringing together a unified version because of their various considerations. In this note, we aim to look at these problems again but now with more simplified versions that include other details in order to let them be understandable for most readers in the subjects of finite fields and elliptic curves. In the proof of Wedderburn's theorem, we succeed to show how it is equivalent to define either a centralizer of non-central elements or stabilizer, allowing to use interchangeably the index of the centralizer or the order of the orbit via the stabilizer as this is true when we consider the group acting on itself by conjugation. As for Hasse's theorem, and in order to shorten the maze to other concepts of algebraic curves, we provide here in just two paragraphs, a direct version of the isogeny-based proof whose methods have the advantage to be applicable to other situations, and then, we state three of this result with an explanation of how this all leads in the end to the need of an algorithm like the one of René Schoof in 1985.

1. Simplified proof version of Wedderburn's Theorem

1.1. **History on Wedderburn's Theorem.** In Wedderburn's little theorem [12, 14], we have the statement that every finite division ring or finite skew field is a field. In order to not get confused by the expression, it is important to note that for example in French language, a skew field is called "corps gauche" and if a field is commutative, we add the qualificative so we get "corps commutatif". This is why we choose here to state the Wedderburn's theorem in the simple way that could be acceptable for all as follows.

Theorem 1.1. *Every finite field is necessarily commutative.*

Before going to the proof, we note that the Artin–Zorn theorem has generalized the theorem to alternative rings by restating that every finite alternative division ring is a field [19]. In Parshall's opinion [16], the first correct proof is due to Leonard Eugene Dickson. Then, a simplified version was later given by Ernst Witt in 1931 [21, 11] and which came later after the attempt of Artin in 1927 [4] who did not use any divisibility argument. The result can also be seen as a consequence of the Skolem–Noether theorem [15] and which states that if K

Date: Received: Sep 4, 2023; Accepted: Dec 25, 2023.

* Corresponding author.

2020 *Mathematics Subject Classification.* Primary 12E20,20K01,14H52; Secondary 11T06,14K02.

Key words and phrases. finite field, finite Abelian group, elliptic curve, Galois theory, isogeny.

is a finite division algebra with center Z, while having $[K : Z] = n^2$ and m the cardinality of Z, then every maximal subfield of K has m^n elements, isomorphic and then conjugate. However, in case of a multiplicative group G^* of K, it can not be a union of conjugates of a proper subgroup, thus, we can only have $n = 1$.

A well-known proof was given by Ted Kaczynski in 1964 [9] and where the author acknowledged the earlier historical proofs. Since we are more interested in our team to rely on Abelian group-theoretic proofs for many problems as in [23, 5, 1, 24, 2], we also suggest to read the non-detailed but interesting proof done by Hans Zassenhaus in 1953 [22]. Following this same way of reasoning while combining some elements of the proof approaches in [6] as well as the one in [17], we succeed here to show how is it possible to introduce interchangeably the index of the subgroup or the order of the orbit by either defining a stabilizer or centralizer.

1.2. **A Simple Detailed Proof.** We note that in the introductory part of the proof, our contribution is summarized in showing how it is sufficient to prove that $gcd\left(\frac{|G^*|}{|Z_{G^*}(k)|}\right)|gcd(X)$ and use it in the end of the proof to get a contradiction with the introduction of the cyclotomic polynomials, then we show in the middle part of the proof, how it is equivalently possible to meet the same equation on the order of G^* by considering either $Z_{G^*}(k)$ or G^*_k.

In order to understand all these notations, let us go now directly in presenting our simplified proof version.

Proof. Let us consider a multiplicative group G^* of a finite field K.

- Being a finite group, there is a theorem [6] which states that G^* is Abelian if and only if there exists a nonzero natural number $n(k)$ for each element $k \in G^*$ such that $|Z_{G^*}(k)| = m^{n(k)} - 1$ with $m = |Z| + 1$, $k \in G^* \setminus Z$ and where Z is the center of G^*, and $|Z_{G^*}(k)|$ is the order of centralizers of non-central elements in G^*.
- As a remark, since we are interested in Abelian groups, one would take $m = |G^*| + 1$ and all $n(k) = 1$. But until now, we consider that the dimension of K is some $n \neq 1$, then we take $|G^*| = m^n - 1$. This is important as we will see that the equation we get from the formula of $|G^*|$ in function of $|Z|$ and $|Z_{G^*}(k)|$, will lead us to the idea that for having K as a commutative field or G^* as an Abelian group, we should have $n = 1$.
- In fact, we could wonder about an equivalence here, as from the implication that G^* is Abelian, it will be the same as saying G^* coinciding with its center Z or with each centralizer Z_{G^*}, and then, we can directly deduce that $|Z_{G^*}(k)| = (|Z| + 1)^{n(k)} - 1 = (|G^*| + 1)^n - 1$, $n(k) = n = 1$, but the question remains, is the other sense of implication true?
- The implication, namely starting from the fact that $|Z_{G^*}(k)| = m^{n(k)} - 1$, $m = |Z| + 1$, and prove that G^* is Abelian, is not that easy. Let us then

verify if this is true. For this, we will need to denote hereafter the set $\{|Z_{G^*}(k)|, k \in G^* \setminus Z\}$ by X.

The main idea from this part of proof is to show that $gcd\left(\frac{|G^*|}{|Z_{G^*}(k)|}\right)$ divides $gcd(X)$ for every $k \in G^* \setminus Z$, then use it with the introduction of cyclotomic polynomials in order to get a contradiction that will serve to state that by using the previous assumptions, G^* can not be different to its center, then it is Abelian.

Saying that we want to prove that $gcd\left(\frac{|G^*|}{|Z_{G^*}(k)|}\right)|gcd(X)$ can be simplified to $\frac{|G^*|}{lcm(|Z_{G^*}(k)|)}|gcd(X)$ as we can deduce from [14] but we prefer to continue with the similar and direct argument as in [6].

Since this should be checked for every $k \in G^* \setminus Z$, we try to show that $\frac{|G^*|}{lcm(X)}|gcd(X)$, by following these first proof part steps.

- Since Z is a subgroup of G^*, then we have,

$$|G^*| = |Z| + \sum_i \frac{|G^*|}{|Z_{G^*}(k_i)|}.$$

- Since $\frac{|G^*|}{lcm(X)}\Big||G^*|$ and in addition to having $\frac{|G^*|}{lcm(X)}\Big|\frac{|G^*|}{|Z_{G^*}(k_i)|}$, then based on the equation above, we deduce that $\frac{|G^*|}{lcm(X)}\Big||Z|$ and which gives $|G^*|\Big||Z|.lcm(X)$.
- Since Z is a subgroup of each $Z_{G^*}(k_i)$, $k_i \in G^* \setminus Z$, then $|Z|\Big||Z_{G^*}(k_i)|$ and which gives $|Z|\Big|gcd(X)$.

We have just shown that,

- $|G^*|\Big||Z|.lcm(X)$,
- $|Z|\Big|gcd(X)$.

Then, we finally have $\frac{|G^*|}{lcm(X)}|gcd(X)$.

- By the definition we have given to X, we can see that

$$gcd(X) = m^{gcd(\{n(k), k \in G^*\})} - 1$$

and assuming that $gcd(\{n(k), k \in G^*\})$ can be replaced by e which is also the same as $gcd(\{n(k), k \in G^* \setminus Z\})$ and that is equal to 1, then we have $gcd(X) = m - 1$.

Since we just obtained $\frac{|G^*|}{lcm(X)}|gcd(X)$.
Then, as noted in the introduction of this proof, we have $|G^*| = m^n - 1$ which gives now $\frac{m^n-1}{lcm(X)}|m-1$.

By introducing now the cyclotomic polynomials in $\mathbb{Z}$, the expression of $m^n - 1$ can be expressed as

$$m^n - 1 = \prod_{q|n} \Phi_q(m)$$

where Φ_q the q-th complex cyclotomic polynomial. and we also have

$$m^{n(k)} - 1 = \prod_{q|n(k)} \Phi_q(m)$$

We know that for every $k \in G^* \setminus Z$, $m^{n(k)} - 1 | m^n - 1$ then, $n(k)|n$. Now, we have,

$$\frac{m^n - 1}{m^{n(k)} - 1} = \prod_{q|n, q\nmid n(k)} \Phi_q(m)$$

- This is due to the fact that since $n(k)|n$, then the set of divisors of n is the disjoint union of the set of divisors of $n(k)$ and the set of divisors of n that do not divide $n(k)$, and this gives $\prod_{q|n} \Phi_q(m) = \prod_{q|n(k)} \Phi_q(m). \prod_{q\nmid n(k)} \Phi_q(m)$.

For one who would want to prove this otherwise by introducing a stabilizer through an orbit instead of talking about a centralizer of non-central elements, the following remark would be very useful.
Or in other words, instead of having the equation,

$$|G^*| = |Z| + \sum_i |G^* : Z_{G^*}(k_i)|, \ k_i \in G^* \setminus Z$$

where $|G^* : Z_{G^*}(k_i)|$ is the index of the subgroup $Z_{G^*}(k_i)$ on G^* as defined before as $\frac{|G^*|}{|Z_{G^*}(k_i)|}$.
One can have otherwise, the equation,

$$|G^*| = |Z| + \sum_i |O_{k_i}|, \ k_i \in G^* \setminus Z$$

where $O_k = \{kxk^{-1}, x \in G\}$ is the orbit of k.

- In fact, since we have supposed K as non-commutative field $n \neq 1$, then G^* operates on itself by conjugation or interior automorphism,

$$\begin{aligned} i_k \ : \ & G^* \to G^* \\ & x \to kxk^{-1} \end{aligned}$$

Consider then the following action.

- We define for every $k \in G^*$, the set $G_k^* = \{x \in G^*, kx = xk\}$ as the stabilizer of k. In this case, we can say that the centralizer $Z_{G^*}(k)$ which we have defined earlier, coincides with the stabilizer G_k^* as an initiative to let the reader understands how one could use them interchangeably in this theorem's proof based on properties of each one of them.

We have $|G_k| = m^{n(k)}$ and G_k^* is a subgroup of G^*, then by using the Lagrange's theorem, we finally have $m^{n(k)} - 1 | m^n - 1$ for every $m \in \mathbb{N}, m \geq 2$, and then, $n(k)|n$.
We also have,

$$|O_k| = \frac{|G^*|}{|G_k^*|} = \frac{m^n - 1}{m^{n(k)} - 1}$$

Then, the equation above becomes,

$$|G^*| = |Z| + \sum_i \frac{|G^*|}{|G_{k_i}^*|} = |Z| + \sum_i \frac{m^n - 1}{m^{n(k_i)} - 1},\ k_i \in G^* \setminus Z$$

One can observe the proof of the formula on the order of the orbit this way.

- In fact, given Z as the center of K with $|Z| = m$, we have Z is a subfield of K, then $|K| = m^n$. Just as remark, since we are still supposing K as a noncummutative field, then $Z \neq K$, and then $n \geq 2$. Let Z_k denotes the set of elements of K that commutes with k, an extension of Z. We have Z is a subfield of Z_k, then similarly, we get $|Z_k| = m^{n(k)}$. In addition, Z_k is a subfield of K, then $|K| = |Z_k|^{n'},\ n' \in \mathbb{N}^*$, which gives $|K| = (m^{n(k)})^{n'}$. Then, $n = n'.n(k)$, hence, $n(k)|n$ for every element of K. Let $stab(k)$ denotes the stabilizer of k in the multiplicative group of K, namely G^*, we have $Z_k = stab(k) \cup \{0\}$ which gives $|stab(k)| = m^{n(k)} - 1$. Let $orb(k)$ denotes the orbit of k, we have,

  $$|orb(k)| = \frac{|G^*|}{|stab(k)|} = \frac{m^n - 1}{m^{n(k)} - 1}$$

  Thus,

  $$|G^*| = |Z| + \sum_i |O_{k_i}|,\ k_i \in G^* \setminus Z$$

  becomes

  $$|G^*| == |Z| + \sum_i \frac{m^n - 1}{m^{n(k_i)} - 1},\ k_i \in G^* \setminus Z$$

Going back to our proof, we have seen that,

$$\frac{m^n - 1}{m^{n(k)} - 1} = \prod_{q|n, q\nmid n(k)} \Phi_q(m)$$

and in particular we have, $\Phi_n(m) | \frac{m^n - 1}{m^{n(k_i)} - 1}$, and we have $k_i \in G^* \setminus Z$ if and only if $n(k) \neq n$ in a way that we have,

$$m^n - 1 = m - 1 + \sum \frac{m^n - 1}{m^{n(k)} - 1}$$

Thus, $\Phi_n(m)$ divides $m-1$.
If we go back to what we have shown before without using any action on the group G^*, we have reached the result that $\frac{m^n-1}{lcm(X)}|m-1$ and which also leads to the same conclusion that $\Phi_n(m)$ divides $m-1$.
This is to say that in order to help the readers to not get confused by the different versions of the proof in literature, we have proceeded in this last part by two methods. This means that now one could simply work either by defining the stabilizer G_k^* or taking the centralizer $Z_{G^*}(k)$, $k \in G^* \setminus Z$.

In particular, we have $|\Phi_n(m)| \leq m-1$.

- In fact, from the formula above, we get,

$$m-1 = m^n - 1 - \sum \frac{m^n-1}{m^{n(k)}-1}$$

and since $n(k)|n$, then the rational fraction $m^n - 1 - \sum \frac{m^n-1}{m^{n(k)}-1}$ is in $\mathbb{Z}[X]$ and this is due to the following points.

  - We have seen before that $\frac{m^n-1}{m^{n(k)}-1} = \prod_{q|n, q\nmid n(k)} \Phi_q(m)$ which implies that $m^n - 1 = (m^{n(k)}-1).\Big(\prod_{q|n, q\nmid n(k)} \Phi_q(m)\Big)$ and then $\prod_{q|n, q\nmid n(k)} \Phi_q(m) \in \mathbb{Z}[X]$ as we have the property that if there exists an unitary polynomial $Q \in A[X]$, $A \subset K$ a subfield of K and $\Phi \in K[X]$ such that $\Phi.Q \in A[X]$, then $\Phi \in A[X]$.
  - Now, we note that $n(k_i)|n$ but $n(k_i) < n$ because if we have $n(k_i) = n$, the orbit $orb(k_i)$ as we have defined before, will coincide with G^* and k_i will be in Z, and this is not true based on our assumption. $n(k) < n$ also implies that n is in the set D of its divisors and that do not divide $n(k)$, and then $\frac{m^n-1}{m^{n(k)}-1} = \Phi_n(m).\Big(\prod_{q\in D-\{n\}} \Phi_q(m)\Big)$ and similarly from the property as we have just stated, this gives $\prod_{q\in D-\{n\}} \Phi_q(m) \in \mathbb{Z}[X]$ and thus Φ_n divides $\frac{m^n-1}{m^{n(k)}-1}$ in $\mathbb{Z}[X]$.
    Since Φ_n also divides m^n-1 then it divides $m^n - 1 - \sum \frac{m^n-1}{m^{n(k)}-1}$, which means there exists a polynomial $Q \in \mathbb{Z}[X]$ such that

$$m^n - 1 - \sum \frac{m^n-1}{m^{n(k)}-1} = Q(m).\Phi_n(m)$$

.
    Since $m-1 = m^n - 1 - \sum \frac{m^n-1}{m^{n(k)}-1}$, then $m-1 = Q(m).\Phi_n(m)$, $Q \in \mathbb{Z}[X]$, $m \neq 1$, hence $|\Phi_n(m)| \leq m-1$.

On the other hand, considering the primitive roots $r_1, ...r_l$ of complex unity and with $r_i \neq 1$ since $n \neq 1$.

We have,

$$\Phi_n(m) = (m - r_1)(m - r_2)...(m - r_l)$$

For every i, we have $|m - r_i| > m - 1$.
Thus, $|\Phi_n(m)| > (m - 1)^l \geq m - 1$ which is absurd.
Finally n is necessarily equal to 1, which implies $G^* = Z$, then it is an Abelian group. □

2. Simplified proof version of Hasse's Theorem

For Hasse's theorem, we should note that the problem was originally been conjectured by Artin's thesis in 1924 [3], then Hasse proved it later in a series of papers in 1936 [8]. Here, we only use two small paragraphs for the proof but by preserving the fact that an isogeny Ψ is separable if and only if $\Psi^*\omega \neq 0$ and which is not that easy to prove as Silverman showed in this book this result by considering the context of general agebraic curves [20] and using results from book of Hartshorne [7], thus, we accept this proposition as it is.

We also report that in his book [10], Knapp added Cassel's corrections to the Manin's incomplete polynomial-arithmetic-based proof [13], but in his chapter X's last notes, he concluded that with the isogeny-based proof, despite its length and complications, it remains the most preferable one as its methods have the advantage to be applicable to other situations.

Let us now state the Hasse's theorem as follows.

Theorem 2.1. *s If E is an elliptic curve defined over $K = \mathbb{F}_q$ (a finite field with q elements), then we have,*

$$|card(E(K) - q - 1| \leq 2\sqrt{q}$$

Let us go to the proof but with we note that the following four points are important introductory elements before providing any direct evidence about the result.

2.1. A Simplified Direct Proof.

- Suppose that our elliptic curve E is defined by a Weierstrass' equation *(cubic with coefficients in K)* and that is,

$$E: \ y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_5$$

and consider $\Phi : E \to E$ an isogeny between E and itself.
In order to go directly in advance in the proof, we will take Φ defined as the Frobenius morphism also called the q-th power Frobenius isogneny, and that is,

$$\begin{aligned} \Phi \ &: \ E \to E \\ &\quad (x, y) \to (x^q, y^q) \end{aligned}$$

which is the topological generator of the absolute Galois group $Gal(\bar{K}/K)$.

- Φ being a Frobenius morphism is the same as saying it is an endomorphism over K such that $\Phi : \ K \to K$ is defined by $\Phi(x) = x^p$ with p a prime number being the characteristic of K (the smallest such that $p1_K = \underbrace{1_K + ... + 1_K}_{\text{p summands}} = 0_K$).
- Φ being the topological generator of the absolute Galois group $Gal(\bar{K}/K)$ is the same as saying that the closure of the subgroup generated by Φ is the full Galois group, and we have $P \in E(K) \Longleftrightarrow \Phi(P) = P$.
- We also note that K is a perfect field since Φ is even an automorphism here. Then, the algebraic closure $\bar{K}$ is the same as the separable closure and this can generally holds directly from the fact that we have K as a finite field, and this is enough to define $Gal(\bar{K}/K)$ as an absolute Galois group.

Now, we prove the result in just these two following paragraphs.

Proof. Since we have defined Φ as a Frobenius isogeny then by definition Φ is inseparable and $deg(\Phi) = q$. Then, we have $\Phi^*\omega = 0$ for every $\omega \in \Omega_E$ with Ω_E being the space of differential forms on E and $\Phi^* : \bar{K}(E) \to \bar{K}(E)$ being the usual injection of function fields with $\bar{K}(E)$ the function field of E over $\bar{K}$. In fact, this is due to a proposition which states that an isogeny Ψ is separable if and only if $\Psi^*\omega \neq 0$ [20]. It follows from the inseparability of Φ above that $(id - \Phi)^*\omega = \omega$ and which in turn implies that $id - \Phi$ is a separable isogeny.

We have just stated before the proof that $P \in E(K) \Longleftrightarrow \Phi(P) = P$ which gives $E(K) = ker(id - \Phi)$. Having the statement of a theorem in [7] whose result implies that if some Ψ is a separable isogeny then $card(ker(\Psi)) = deg(\Psi)$, therefore since also we have just found that $id - \Phi$ is a separable isogeny, then we have $card(ker(id - \Phi)) = deg(id - \Phi)$.
In addition to knowing that $deg(\Phi)$ is a positive definite quadratic form, then, we can now use the Cauchy–Schwarz Lemma to get the following inequality,

$$|deg(id - \Phi) - deg(id) - deq(\Phi)| \leq 2\sqrt{deg(id)deg(\Phi)}$$

which is the same as saying,

$$|card(E(K)) - 1 - q| \leq 2\sqrt{q}$$

□

Now, after proving the Hasse's theorem, we look at some of its consequences.

2.2. **Consequences and the Need to Schoof's Algorithm.** First, we note that the quantity $c = 1 + q - card(E)$ is called the trace of the q-th power Frobenius isogeny, and we have Φ verifying $\Phi^2 - c\Phi + q = 0$.
Since, we have $card(E) = 1 + q - c$, then in order to benefit from the result of Hasse's theorem, one would seek some c such that $|c| \leq 2\sqrt{q}$. But before going further in this, if we put $m = -c$, then let us say that we can now state the Hasse's theorem otherwise as in the following.

Theorem 2.2. *If E is an elliptic curve defined over $K = \mathbb{F}_q$ (a finite field with q elements), then we have,*

$$card(E(K)) = q + 1 + m$$

where $|m| \leq 2\sqrt{q}$.

Note that m can either be positive or negative, which means the number of points in E is essentially $p + 1$ but with some error r.
In fact, we can even state the Hasse's theorem as in the following.

Theorem 2.3. *If E is an elliptic curve defined over $K = \mathbb{F}_p$ (a finite field with prime p elements), then we have,*

$$p + 1 - 2\sqrt{p} \leq card(E(K)) \leq p + 1 + 2\sqrt{p}$$

Example 2.4. Let us take the following example.
We consider an elliptic curve E over $\mathbb{F}_p$ with $p = 127$.
We have $2\sqrt{127} \approx 22.53$, then $p + 1 - 2\sqrt{p} \approx 105.47$ and $p + 1 + 2\sqrt{p} \approx 150.53$.
What does this mean?
It means for every integer number $i \in \{105, ..., 151\}$, there exist $s, t \in \mathbb{F}_{127}$ such that $card(E(\mathbb{F}_p)) = i$.

Hasse's theorem shows to be beneficial in giving an upper bound for the number of points in E or even two bounds as we have just seen in the example for the last version with a prime number, however, this does not provide an algorithm in order to solve the finite field point counting problem. The Schoof's algorithm [18] comes for this reason in order to provide a practical solution by using that upper bound in order to compute $card(E)$.

Generally, we need to follow the following rules,

- In order to compute c, namely the trace that we have defined above, we will need to compute $c \mod N$ for $N > 4\sqrt{q}$.
- In order to compute $c \mod N$, we will need first to do a prime factorization of N as $N = \prod n_i$.
- For that, we will need to compute $c \mod n_i$ for each i.
- For that, we will need to use the Chinese remainder theorem in order to finally find $c \mod n_i$.

From the equation verified by the q-th power Frobenius isogeny Φ, we can say that for every n and any point $P = (x, y) \in E(K)[n]$, we have

$$\Phi^2(P) - [c]\Phi(P) + [q](P) = 0$$

which is the same as saying,

$$(x^{q^2}, y^{q^2}) - [c](x^q, y^q) + [q](x, y) = 0$$

Then, in particular, we will proceed as follows,

- We will need to set a unique positive integer $d \leq n$ such that $d \equiv c \mod n$

Now, the equation becomes,

$$(x^{q^2}, y^{q^2}) + [q_d](x, y) = [d](x^q, y^q)$$

- In order to finally find $c \mod n$, we will need to compute d for each n along with the use of Chinese remainder theorem.

3. Conclusion

By the essential background added in this note along with the simplified proof versions provided here in the context of Wedderburn and Hasse theorems, we can conclude that the usual arguments used to show these results, will become now easier to introduce in research and lectures around this topic.

The proof of the first theorem has shown the possibility of an interchangeable introduction between stabilizers and centralizers as well as between the index of the subgroup and the order of the orbit. As for the second theorem, the readers can get now a direct and short evidence about this result without having recourse to any complicated proof while having an idea about its limitation that led to the creation of the Schoof's algorithm and which is rarely analyzed because of its introduction complications.

Acknowledgement. A special thanks to the editors Professor Dr. Firuz Kamalov and our Professor Dr. Najib Mahdou. We would also like to thank the anonymous referee for the nice report which really helped us to improve the content of this note.

References

1. Abdelalim, S. (2015). Characterization the strongly co-Hopfian Abelian groups in the category of Abelian torsion groups. Journal of Mathematical analysis, 6(4), 1-10. https://ilirias.com/jma/repository/docs/JMA6-4-1.pdf
2. Abdelalim S., Chillali, A., Essanouni, H., Zeriouh, M., & Ziane, M. H. (2014). Construction of the α_2-Automorphism. International Journal of Algebra, 8(5), 247-251. https://dx.doi.org/10.12988/ija.2014.4219
3. Artin, E. (1924). Quadratische Körper im Gebiete der höheren Kongruenzen. II. Analytischer Teil, Mathematische Zeitschrift, 19 (1): 207–246, ISSN:0025-5874, JFM.51.0144.05, MR.1544652, S2CID.117936362. https://doi.org/10.1007/BF01181075
4. Artin, E. (1927). Über einen Satz von Herrn J. H. MacLaglan Wedderburn, Abh. Math. Sem. Univ. Hamburg, vol. 5, 1927, pp. 245-250. https://doi.org/10.1007/BF02952525
5. Chillali, A., Abdelalim, S., & Essanouni, H. (2015). The strongly Hopfian abelian groups. Gulf Journal of Mathematics, 3(2). https://doi.org/10.56947/gjom.v3i2.164
6. Grundhöfer, T. (1998). Commutativity of finite groups according to Wedderburn and Witt. Archiv der Mathematik, 70(6). https://doi.org/10.1007/s000130050214
7. Hartshorne, R. (1977). Algebraic geometry. Graduate Texts in Mathematics, 52. https://doi.org/10.1007/978-1-4757-3849-0
8. Hasse, H. (1936). Zur Theorie der abstrakten elliptischen Funktionenkörper. I, II & III, Crelle's Journal, 1936 (175), ISSN:0075-4102, S2CID.118733025, Zbl.0014.14903. https://doi:10.1515/crll.1936.175.193
9. Kaczynski, T.J. (June–July 1964). "Another Proof of Wedderburn's Theorem". American Mathematical Monthly. 71 (6): 652–653. https://doi.org/10.2307/2312328
10. Knapp, A. W. (1992). Elliptic curves (Vol. 40). Princeton University Press. https://lccn.loc.gov/92022183

11. Lam, Tsit-Yuen (2001). A first course in noncommutative rings. Graduate Texts in Mathematics. Vol. 131 (2 ed.). Springer. ISBN:0-387-95183-0. https://doi.org/10.1007/978-1-4419-8616-0
12. Maclagan-Wedderburn, J. H. (1905). A theorem on finite algebras. Trans. Amer. Math. Soc. 6, 349-352. https://ams.org/journals/tran/1905-006-03/S0002-9947-1905-1500717-7
13. Manin, Y. I. (1956). On cubic congruences to a prime modulus. Izvestiya Rossiiskoi Akademii Nauk. Seriya Matematicheskaya, 20(5), 673-678. https://mathnet.ru/eng/im3844
14. Michael, A. & Mutschler, B. J. (2003). On Wedderburn's theorem about finite division algebras. https://uni-math.gwdg.de/mad/Wedderburn/Wedderburn.pdf
15. Milne, J.S. (1997). Class field theory. Theorem 4.1 in Ch. IV of Milne. https://jmilne.org/math/CourseNotes/cft.html.
16. Parshall, K. H. (1983). In pursuit of the finite division algebra theorem and beyond: Joseph H M Wedderburn, Leonard Dickson, and Oswald Veblen. Archives of International History of Science. 33: 274-99. https://pascal-francis.inist.fr/vibad/index.php?action=getRecordDetail&idt=12127068
17. Perrin, D., Cabanes, M., & Duchene, M. (1996). Cours d'algèbre (Vol. 4). Paris: Ellipses. https://www.editions-ellipses.fr/accueil/7778-cours-d-algebre-agregation-9782729855529.html
18. Schoof, R. (1985). Elliptic Curves over Finite Fields and the Computation of Square Roots mod p. Math. Comp., 44(170):483–494, 1985. https://doi.org/10.1090/S0025-5718-1985-0777280-6
19. Shult, E.E. (2011). Points and lines. Characterizing the classical geometries. Universitext. Berlin: Springer-Verlag. p. 123. ISBN:978-3-642-15626-7. Zbl:1213.51001. https://doi.org/10.1007/978-3-642-15627-4
20. Silverman, J. H. (2009). The arithmetic of elliptic curves (Vol. 106, pp. xx+-513). New York: Springer. https://doi.org/10.1007/978-0-387-09494-6
21. Witt, E. (1931). Über die Kommutativität endlicher Schiefkörper. Abh. Math. Sem. Univ. Hamburg 8, 413. https://doi.org/10.1007/BF02941019
22. Zassenhaus, H. J. (1952). A group-theoretic proof of a theorem of Maclagan-Wedderburn. Glasgow Mathematical Journal, 1(2), 53-63. https://doi.org/10.1017/S2040618500035474
23. Zeriouh, M., Abdelalim, S., & Ziane, M. (2016). Coonstruction of an automorphism of an abelian group that satisfies the property of the weak extension without satisfying the property of the extension. Gulf Journal of Mathematics, 4(4). https://doi.org/10.56947/gjom.v4i4.261
24. Zeriouh, M., Ziane, M. H., Abdelalim, S., & Essanouni, H. (2015). Characterization of the automorphisms of an abelian torsion group having the weakly extension property. Journal of Taibah University for Science, 9(3), 357-360. https://doi.org/10.1016/j.jtusci.2015.02.009

[1] Team of Algebra and Discrete Mathematics, Laboratory of Fundamental and Applied Mathematics (LMFA), Department of Mathematics and Computer Science, Faculty of Sciences Ain Chock (FSAC), University Hassan II of Casablanca (UNIVH2C), Morocco.

Email address: i.elmouki@gmail.com

[2] Team of Algebra and Discrete Mathematics, Laboratory of Fundamental and Applied Mathematics (LMFA), Department of Mathematics and Computer Science, Faculty of Sciences Ain Chock (FSAC), University Hassan II of Casablanca (UNIVH2C), Morocco.

Email address: seddikabd@hotmail.com