Proving Wedderburn's little theorem

Emil August Hovd Olaisen

May 2020

1 Introduction

The goal of this text is to prove Wedderburn's little theorem. The theorem states that all finite integral domains are finite fields, also called galois fields. The outline of this text is as follows. We start by stating some of the basic definitions from algebra. Then we will prove that finite integral domains are division rings. After that we break down the important theorems about finite fields. We also look at two different types of functions on finite fields called automorphisms and norms. From there we can prove that finite division rings are fields.

This text assumes that you are familiar with basic group theory. This would include the study of groups, cyclic groups, subgroups and factor groups. As well as Cauchy's theorem, the fundamental theorem of group homomorpisms and the fundamental theorem of ring homomorphisms. You should also be familiar with polynomial rings, snd what their ideals are. [1]

Our definitions and theorems mentioned above are from the textbook Basic Abstract Algebra. This is why some of the definitions here are different than what you may be used to. For instance a ring does not need unity, and integral domains need not be commutative. Many of the proofs are based in the article "A Group-Theoretic Proof of a Theorem of Maclagan-Wedderburn" by Hans J. Zassenhaus. [2]

I would like to thank Steffen Oppermann for giving me valuable feedback.

2 Definitions in Algebra

We will start this text by giving the definitions of *groups*, *rings*, *integral domains* and *fields*.

Definition 1. *A set G equipped with a binary operation $*$ is called a* ***group****, if $\forall x, y, z \in G$ the following properties hold:*

1. $(x * y) * z = x * (y * z)$
2. $\exists e \in G$ *s.t.* $e * x = x = x * e$
3. $\forall x \in G$ *there exists a corresponding* x^{-1} *s.t.* $x * x^{-1} = x^{-1} * x = e$

e is called the identity of G, and x^{-1} is called the inverse of x. If we also have the additional property $x * y = y * x$, then we say that G is an ***abelian group****. We often call the group $(G, *)$.*

Definition 2. *A set R equipped with the two binary operations $+$ and $\cdot$ is called a* ***ring*** *if $(R, +)$ is an abelian group, and if $\forall x, y, z \in R$ the following properties hold:*

1. $(x \cdot y) \cdot z = x \cdot (y \cdot z)$
2. $x \cdot (y + z) = (x \cdot y) + (x \cdot z)$
3. $(x + y) \cdot z = (x \cdot z) + (y \cdot z)$

If $\exists 1 \in R$ s.t. $1 \cdot x = x = x \cdot 1$, then R is called a ***ring with unity****. If $x \cdot y = y \cdot x$, then R is called a* ***commutative ring****. The additive identity in R is called 0, and the additive inverse of x is denoted $-x$.*

Definition 3. *A ring R is called an* ***integral domain*** *if for all $x, y \in R, x \cdot y = 0 \implies$ either $x = 0$ or $y = 0$.*

Definition 4. *A ring R is called a* ***division ring*** *if $(R \backslash \{0\}, \cdot)$ is a group. Furthermore, if it is an abelian group, then R is also a* ***field****.*

It follows immediately from the definition of a field that every field is a division ring. The converse is not the case. The quaternions are an example of a division ring that is not a field. We will finish this section by showing that all division rings are integral domains.

Theorem 1. *Every division ring R is an integral domain.*

Proof. If we assume that $x \cdot y = 0$ for some $x, y \in R$. We want to show that either $x = 0$ or $y = 0$. We have that either $x = 0$ or $x \neq 0$. The first case immediately proves our assertion. If $x \neq 0$, then x has a multiplicative inverse, since R is a division ring. If we multiply with the inverse from the left we obtain $y = 0$, which is what we wanted to show. □

The converse of this theorem is not true. The set of integers $(\mathbb{Z}, +, \cdot)$ is an example of an integral domain that is not a division ring.

3 Integral Domains

In the last section we discussed the relationship between integral domains, division rings and fields. We showed that R is a field $\implies$ R is a division ring $\implies$ R is an integral domain. We also found examples that demonstrate that the converse is not always the case.

One can easily see the relation between division rings and fields. Fields are simply division rings where multiplication is commutative. The relation between integral domains and division rings is not as obvious, but nonetheless very important. The cancellation law applies to integral domains, which is a property often used in elementary algebra.

Theorem 2. *Let R be an integral domain. For $x, y, z \in R$ where $x \neq 0$ and $x \cdot y = x \cdot z$, we have that $y = z$.*

Proof. The equation $x \cdot y = x \cdot z$ can be changed to $x \cdot (y - z) = 0$. Since R is an integral domain $y - z = 0$, which means that $y = z$. □

The proof that $y \cdot x = z \cdot x$ implies $z = y$ the same.

The contra-positive of the cancellation laws is that if $x \neq 0$, then $y \neq z \implies x \cdot y \neq x \cdot z$ and $y \cdot x \neq z \cdot x$. This way of writing the cancellation laws is useful for proving that finite integral domains are division rings.

Theorem 3. *Every finite integral domain is a division ring.*

Proof. Let R be a finite integral domain. What we want to show is that $\exists 1 \in R$ s.t. $1 \cdot x = x = x \cdot 1, \forall x \in R$, and that $\forall x \in R, \exists x^{-1}$ s.t. $x^{-1} \cdot x = x \cdot x^{-1} = 1$.

Let $|R| = n$. R can be rewritten as $\{r_1, r_2, \ldots, r_n\}$, where $r_i \neq r_j$ if $i \neq j$. Let $x \in R$, then by the cancellation law (or rather the contrapositive) $\{x \cdot r_1, x \cdot r_2, \ldots, x \cdot r_n\}$ and $\{r_1 \cdot x, r_2 \cdot x, \ldots, r_n \cdot x\}$ are equal to R, since both sets have n different elements from R. This means that for some r_i, r_j we have that $r_i \cdot x = x = x \cdot r_j$. $\forall y \in R, \exists r_k$ s.t. $y = x \cdot r_k$. This means that $r_i \cdot y = r_i \cdot x \cdot r_k = x \cdot r_k = y$. A similar argument shows that $\forall z \in R, z \cdot r_j = z$. r_i fixes all elements from the left, and r_j fixes all elements from the right. If we apply this to $r_i \cdot r_j$, we see that $r_i = r_i \cdot r_j = r_j$, which means that $r_i = 1$.

Now we are going to prove the existence of an inverse for any nonzero $x \in R$. We are going to look at R the same way as the first part of the proof. R is the same as $\{x \cdot r_1, x \cdot r_2, \ldots, x \cdot r_n\}$ and $\{r_1 \cdot x, r_2 \cdot x, \ldots, r_n \cdot x\}$. For some r_l and r_m, $r_l \cdot x = 1 = x \cdot r_m$. These are respectively left and right inverses of x. However, $r_l = r_l \cdot 1 = r_l \cdot x \cdot r_m = 1 \cdot r_m = r_m$, meaning that $r_l = x^{-1}$. □

Since division rings and and fields seem more similar than integral domains and division rings, one may assume that proving that finite division rings are fields should be easy. But as we are about to see, the second part of Wedderburn's little theorem is far more involved.

4 Finite Fields

In this section we are going to look at the structure of finite division rings and finite fields. We are going to look at finite division rings in general to demonstrate that much of what applies to finite fields apply to finite division rings. In fact, they have very similar structures.

The first thing we are going to look at is the characteristic of such rings.

Definition 5. *Let R be a ring. The* ***characteristic*** *of R is the smallest positive integer n such that $n \cdot r = 0$ for all $r \in R$.*

If no such n exists, we say that R has characteristic 0.

Obviously the ring $\mathbb{Z}$ has characteristic 0, and the field of integers modulo a prime p; $\mathbb{Z}_p$ has characteristic p. The set $\mathbb{Z}_p$ is a set of great interest to us. We are going to use this set as a basis for the finite division rings. Also keep in mind that it is impossible for a ring to have characteristic 1, unless it is the trivial ring 0, which is not a field. Another thing to note is that the characteristic is unique.

It should be noted, that we are denoting the unity of a ring as 1. The notation $n \cdot r$ can be used in rings that do not have unity, in those instances it means adding r with itself n times. in rings that have unity an integer n simply means the sum of the unity with itself n times, which is an element of the ring. Multiplying an r with this n gives an identical result adding r with itself n times. In a ring with unity, a characteristic is a zero of the ring, since it has identical properties, and smaller numbers are non-zero, since there are elements that they can be multiplied with to produce a non-zero element.

Theorem 4. *Any division ring F has either characteristic 0 or characteristic p, Where p is some prime. Furthermore, if F is finite, then it is of characteristic p.*

Proof. We know that F has characteristic 0, a prime or a composite number. We are going to demonstrate that it is not a composite. Let us assume that F has characteristic $n = a \cdot b$ where $a, b \neq 1$. $\forall x \in F$, $a \cdot b \cdot x = 0$. Since n is the characteristic $a \neq 0$, and therefore has an inverse. We multiply with the inverse from the left and obtain $b \cdot x = 0$. This means that b also has the same property as n. If a composite has the same property of a characteristic, then some non-unit factor of that composite has that property. Meaning that it is impossible for a division ring to have a composite characteristic, proving the first part of the theorem.

If we assume that F is finite, then $(F, +)$ is a finite group. By Fermat's theorem on groups $|F| \cdot x = 0$. This means that it has a non-zero characteristic. Finite division rings have a prime characteristic. □

Theorem 5. *A finite division ring F is of order p^r, where p is it's characteristic and r is some positive integer.*

Proof. In order to prove this, we are going to demonstrate that no prime outside of p divides the order of F. Let $q \neq p$ be a prime that divides $|F|$. If we apply Cauchy's theorem to $(F,+)$, then for some non-zero $x \in F, q \cdot x = 0$. From number theory we know that $gcd(p,q) = 1$, and therefore some linear combination of these over $\mathbb{Z}$ can produce 1. That is for some $a, b \in \mathbb{Z}, a \cdot p + b \cdot q = 1$. We can use this to show that $0 = p \cdot x = q \cdot x = a \cdot p \cdot x + b \cdot q \cdot x = (a \cdot p + b \cdot q) \cdot x = 1 \cdot x = x$. Which means that for no non-zero x does $q \cdot x = 0$. $q \mid |F|$ gives us a contradiction. This means that p is the only prime that divides F. r is positive, since if it were zero then F would be the trivial ring, which it is not. $|F| = p^r$ □

What this theorem shows is that for a non-zero $x \in F, \{x, 2 \cdot x, \ldots, p \cdot x\}$ are distinct elements, $p \cdot x$ of course being 0. Any integer n multiplied with x is one of those elements. If we choose $x = 1$, then we get $\{1, 2, \ldots, p\}$. This set is closed under multiplication. This set is isomorphic $\mathbb{Z}_p$ and is a field contained in F. For simplicity we will say that $\mathbb{Z}_p$ is a subfield of F instead of saying that it has a subfield isomorphic to $\mathbb{Z}_p$.

Definition 6. *Let E and F be fields. If F is contained in E then F is called a* ***subfield*** *of E, and E is called an* ***extension field*** *of F.*

We are now going to look at one final theorem to illustrate the structure of finite division rings.

Theorem 6. *Let F be a division ring of order p^r, where p is its characteristic. F is a vector space over $\mathbb{Z}_p$ of dimension r. One consequence of this is; $(F,+) \simeq \mathbb{Z}_p^r$.*

Proof. To prove this, we are going to find a basis for F. We find this basis via induction. Set $b_1 = 1$. Let us then assume we have a set of linearly independent elements $\{b_1, b_2, \ldots, b_k\}$ over $\mathbb{Z}_p$. Since they are linearly independent each element in the span of this basis is a unique combination. $|Span\{b_1, b_2, \ldots, b_k\}| = p^k$. This includes 0, meaning that 0 can only be expressed if all the terms are 0. If $k < r$ we can choose a b_{k+1} not in the span. The set $\{b_1, b_2, \ldots, b_k, b_{k+1}\}$ is linearly independent. This is the case because if $z_1 \cdot b_1 + z_2 \cdot b_2 + \cdots + z_{k+1} \cdot b_{k+1} = 0$ then $z_{k+1} = 0$, if it does not, then

$$b_{k+1} = -z_{k+1}^{-1} \cdot z_1 \cdot b_1 - z_{k+1}^{-1} \cdot z_2 \cdot b_2 - \cdots - z_{k+1}^{-1} \cdot z_k \cdot b_k,$$

which is a contradiction since b_{k+1} is not in the span of the k first basis elements. This means that

$$z_1 \cdot b_1 + z_2 \cdot b_2 + \cdots + z_k \cdot b_k = 0,$$

implying that $z_1 = z_2 = \cdots = z_k = x_{k+1} = 0$. The set $\{b_1, b_2, \ldots, b_k, b_{k+1}\}$ is linearly independent.

If we repeat this process up to r we have a basis which spans p^r elements from F. $Span\{b_1, b_2, \ldots, b_r\} = F$. □

From this point on we are going to be analysing finite fields in particular. We are going to assume that multiplication is commutative. Previously we stated that if $|F| = p^r$ then $\mathbb{Z}_p$ is a subfield of F, and F is an extension field of $\mathbb{Z}_p$. We are going to introduce a particular type of extension field called a splitting field.

Definition 7. *Let F be a field, and E an extension field of F. E is called a* ***splitting field*** *of a polynomial $f(x) \in F[x]$ over F if $f(x) = (x - a_1)(x - a_2) \cdots (x - a_n)$, where $a_1, a_2, \dots, a_n \in E$, and E is the field generated by F and $a_1, a_2, \dots, a_n$.*

$\mathbb{C}$ is a splitting field of $x^2 + 1$ over $\mathbb{R}$. And $\{a + b\sqrt{3} \mid a, b \in \mathbb{Q}\}$ is a splitting field of $x^2 - 3$ over $\mathbb{Q}$.

If R is a ring, we denote R^* as the group of invertible elements in R using multiplication. By the definition of a field $F^* = (F\backslash\{0\}, \cdot)$ and is an abelian group. From now on we denote $|F| = p^r = q$. Fermat's theorem on groups show us that for any $x \in F^*, x^{q-1} = 1$. Multiplying with x we obtain $x^q = x$. This equation also holds true for 0. The polynomial $x^q - x$ has q distinct zeros in F. Therefore $x^q - x = (x - a_1)(x - a_2) \cdots (x - a_q)$ where $F = \{a_1, a_2, \dots, a_q\}$. F is then a splitting field of $x^q - x$ over $\mathbb{Z}_p$.

Any factorization of $x^q - x = (x - b_1)(x - b_2) \cdots (x - b_q)$ where each $b_i \in F$ is in fact the same factorization as the one using each element in F.

To show this we want to use a famous formula from algebra.

Theorem 7. *Let R be a commutative ring of characteristic c. For any number of elements in R. $(\sum_{i=1}^{n} r_i)^c = \sum_{i=1}^{n} r_i^c$. This equation is sometimes called the freshman's dream.*

Proof. Since R is commutative, we can use the binomial formula on $(r_1 + \sum_{i=2}^{n} r_i)^c$. We obtain

$$(r_1 + \sum_{i=2}^{n} r_i)^c = \sum_{j=0}^{c} \binom{c}{j} r_1^{c-j} (\sum_{i=2}^{n} r_i)^c$$

Looking at $\binom{c}{j} = \frac{c!}{j!(c-j)!}$, one can see that $c \mid \binom{c}{j}$ when $0 < j < c$. When this is the case $\binom{c}{j} r = 0$ for all r in R. When $j = c$ or $j = 0$, $\binom{c}{j} = 1$.

$$(r_1 + \sum_{i=2}^{n} r_i)^c = \sum_{j=0}^{c} \binom{c}{j} r_1^{c-j} (\sum_{i=2}^{n} r_i)^c = r_1^c + (\sum_{i=2}^{n} r_i)^c$$

If you apply the binomial formula n times you get

$$(\sum_{i=1}^{n} r_i)^c = \sum_{i=1}^{n} r_i^c$$

□

This formula can be expanded to saying that

$$(\sum_{i=1}^{n} r_i)^{(c^d)} = \sum_{i=1}^{n} r_i^{(c^d)}$$

by applying the freshman's dream d times. This expansion of the freshman's dream is going to be used to proving:

Theorem 8. *$q = p^r$. Let F be a field of characteristic p and let F split over the polynomial $x^q - x$ such that $(x - a_1)(x - a_2)\cdots(x - a_q) = x^q - x \in \mathbb{Z}_p$ where each $a_i \in F$. Then $\{a_1, a_2, \dots, a_q\}$ is a subfield of F of order q.*

Proof. Firstly we want to show that the sum and product of zeros of $x^q - x$ are also zeros. let a and b be two zeros. $(a + b)^q - (a + b) = a^q + b^q - a - b = 0$ and $(ab)^q - ab = a^q b^q - ab = ab - ab = 0$. The identity in F is also a zero, and if $a^q = a$, then by multiplying with a^{-1} $q+1$ times we obtain $a^{-1} = a^{-q} = (a^{-1})^q$. The inverse of zeros are also zeros. The zeros of $x^q - x$ are therefore a subfield of F.

We are going to show that $(x - a_i)^2$ does not divide $x^q - x$. $a_i^q = a_i$. By the freshman's dream means that $x^q - x = x^q - x - a_i^q + a_i = (x^q - a_i^q) - (x - a_i) = (x - a_i)^q - (x - a_i) = (x - a_i)((x - a_i)^{q-1} - 1)$. Obviously a_i is not a zero in $(x - a_i)^{q-1} - 1$. a_i is a zero of multiplicity 1. This means that all of the zeros are unique, that is $|\{a_1, a_2, \dots, a_q\}| = q$. □

This theorem only states that if a field of characteristic p has q zeros over $x^q - x$, that the zeros are a field. The theorem does not state that the ploynomial has zeros. What the theorem does tell us however is that the splitting field of $x^q - x \in \mathbb{Z}_p[x]$ is a field of q elements, and that a field of q elements is the splitting field of $x^q - x$. That is $|\mathbb{Z}_p(a_1, a_2, \dots, a_q)| = q$. Our next theorem tells us that any irreducible polynomial ofer a field has an extension such that the polynomial has a zero.

Theorem 9. *Let F be a field for any irreducible polynomial $p(x) \in F[x]$ there exists some extension of F such that it has a zero in $p(x)$.*

Proof. If $p(x)$ is irreducible then $(p(x))$ is a maximal ideal in $F[x]$. Which means that $F[x]/(p(x))$ is a field. It can be regarded as an extension field of F as elements of F are the constant polynomials.

We want to show that $\overline{x}$ is a zero of $p(x)$. Remember that $\overline{x}$ is the coset of x, that is two elements x and y are in the same coset if and only if $x - y \in (p(x))$. What this means is that $\bar{(}x) = x + \langle p(x) \rangle$. Where $\langle p(x) \rangle$ denotes an element of

$(p(x))$.

$$\begin{aligned}
&p(\overline{x}) = \sum_{i=0}^{n} a_i \overline{x}^i = \sum_{i=0}^{n} a_i (x + \langle p(x) \rangle)^i = \\
&\sum_{i=0}^{n} (a_i x + \langle p(x) \rangle)(x + \langle p(x) \rangle)^{i-1} = \sum_{i=1}^{n} (\overline{a_i x})(\overline{x})^{i-1} = \\
&\sum_{i=0}^{n} (\overline{a_i x})^i = \sum_{i=0}^{n} \overline{(a_i x)^i} = \overline{\sum_{i=0}^{n} (a_i x)^i} = \overline{p(x)} = 0
\end{aligned}$$

□

Thus we have an extension field where $p(x)$ has a zero. This can be used tho show that for every field F and all $p(x) \in F[x]$ there is some extension of F where $p(x)$ factors into elements $(x - a)$. $p(x) = \prod_{i=1}^{n} p_i(x)$, where $p_i(x)$ are irreducible polynomials. Using the algorithm described in theorem 9 you can find an find an irreducible polynomial of degree two or greater. Find the quotient ring of the ideal generated by that polynomial. If you then factor again you get $p(x) = \prod_{i=1}^{m} r_i(x)$ a different set of irreducible polynomials, but this time $m > n$ as you have at least one more zero. You can do this until $p(x) = \prod_{i=1}^{q} (x - a_i)$ where all a_i are contained in some extension of F. Let us call this extenison E. If F has characteristic p then for any $a \in E$, $pa = (p \cdot 1)a = 0$. Meaning that any extension preserves the characteristic.

If we extend $\mathbb{Z}_p$ so that we can factor $x^{(p^r)} - x$ into p^r zeros, we get a field of p^r elements by one of our theorems. This means that for any prime p and positive integer r there is a field of p^r elements.

Definition 8. *A **monic polynomial** is a ploynomal of the form $x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$. Let E be an extension field of the field F. The monic polynomial of smallest degree such that a is a zero of that polynomial is called the **minimal polynomial** of a.*

What we want to demonstrate now is that two different splitting fields of a polynomial in $F[x]$ are isomorphic to each other. We are going to use that if a and b are zeros of an irreducible polynomial $p(x) \in F[x]$, then $F(a) \simeq F(b)$.

Let $\phi_a : F[x] \to F(a)$ be the evaluation homomorphism $\phi_a(f(x)) = f(a)$. Since $ker(\phi_a) = (g(x))$ for some polynomial, we have that $p(x) = g(x)h(x)$ since $p(x) \in (g(x))$. However, $p(x)$ is irreducible, therefore $(p(x)) = (g(x)) = ker(\phi_a)$. This means that any polynomial of which a is a zero, it is contained in $(p(x))$. By the fundamental theorem of ring homomorphisms $F[x]/(p(x)) \simeq \phi_a[F[x]]$. Obviously $F(a) \subseteq \phi_a[F[x]]$, also $\phi_a(x) = a$ and $\phi_a[F] = F$. Which means that

$\phi_a[F[x]] = F(a)$. One can apply ϕ_b on $F[x]$ to get that

$$F(b) \simeq \phi_b[F[x]] \simeq F[x]/(p(x)) \simeq \phi_a[F[x]] = F(a)$$

It should also be noted that the isomorphism represented here leaves F invariant, since ϕ_a and ϕ_b map elements of F to the same element. In general we know that if there exists some onto isomorphism $\phi : E_1 \to E_2$ where E_1 and E_2 are extension fields that leave F invariant. Then a polynomial in $F[x]$ is irrducible in E_1 if and only if it is irreducible in E_2. If $g(x) \in F[x]$ has a zero in E_2, say a, we know that

$$\begin{aligned} g(\phi(a)) &= a_n\phi(a)^n + \cdots + a_1\phi(a) + a_0 \\ &= \phi(a_na^n) + \cdots + \phi(a_1a) + \phi(a_0) \\ &= \phi(a_na^n + \cdots + a_1a + a_0) \\ &= \phi(g(a)) \\ &= 0 \end{aligned}$$

With this out of the way we are ready to show that splitting fields are unique up to isomorphism.

Theorem 10. *Let $F(a_1, a_2, \ldots, a_n)$ and $F(b_1, b_2, \ldots, b_n)$ be two diferent splitting fields of a polynomial $p(x) \in F[x]$ of degree n, then $F(a_1, a_2, \ldots, a_n) \simeq F(b_1, b_2, \ldots, b_n)$.*

Proof. Recall that $(x - a_1)(x - a_2), \cdots (x - a_n)$ and $(x - b_1)(x - b_2), \cdots (x - b_n)$ are two different ways to factorize $p(x)$. Let $p(x)$ be the minimal polynomial of a_1. Let $b_{i_1} \in F(b_1, b_2, \ldots, b_n)$ be one of the zeros of $p(x)$. We get that

$$F(a_1) \simeq F(b_{i_1})$$

We choose the lowest j such that a_j is not in $F(a_1) = F(a_1, \ldots a_{j-1})$. Let $b_{i_2} \in F(b_1, b_2, \ldots, b_n)$ be a zero of the minimal polynomial of a_j, this can be used to show that

$$F(a_1, \ldots a_{j-1})(a_j) = F(a_1, \ldots, a_j) \simeq F(b_{i_1})(b_{i_2}) = F(b_{i_1}, b_{i_2})$$

We can repeat this process until we get that

$$F(a_1, a_2, \ldots, a_n) \simeq F(F(b_{i_1}, b_{i_2}, \ldots, b_{i_k}) \subseteq F(b_1, b_2, \ldots, b_n)$$

We have an isomorphism $\phi : F(a_1, a_2, \ldots, a_n) \to F(b_{i_1}, b_{i_2}, \ldots, b_{i_k})$ that leaves F invariant. This means that $p(x)$ cannot be factored into irreducible polynomials of degree two or higher in $F(b_{i_1}, b_{i_2}, \ldots, b_{i_k})$ since it can not be factored like that in $F(a_1, a_2, \ldots, a_n)$. This means that $F(b_{i_1}, b_{i_2}, \ldots, b_{i_k}) \subseteq F(b_1, b_2, \ldots, b_n)$ is a splitting field of $p(x)$ over F. We can therefore conclude that $F(b_{i_1}, b_{i_2}, \ldots, b_{i_k}) = F(b_1, b_2, \ldots, b_n)$. Which proves our theorem. □

The next thing we want to show about finite fields is that they are cyclical, that is $F^* = \{a^1, a^2, \ldots, a^{|F^*|}\}$ for some $a \in F^*$. We write this as $F^* = \langle a \rangle$. To prove this, we want to use a theorem from group theory.

Theorem 11. *Let G be an abelian group. Let $a, b \in G$ be elements of order m and n respectively. Then there exists some $x \in G$ such that the order of x is $lcm(m, n)$.*

Proof. Let us assume that m and n are relatively prime. We want to show that the order of $x = a \cdot b$ is $lcm(m, n) = l$. Since $m \mid l$ and $n \mid l$, $x^l = a^l b^l = e$. Let k be the order of x, which means that $k \mid l$. Let $b^{-1} = c$.

$$\begin{aligned} a^k b^k &= e \\ a^k &= b^{-k} \\ a^k &= (b^{-1})^k \\ a^k &= c^k \end{aligned}$$

c is also of order n. l is the smallest positive integer such that $a^l = e = c^l$. This is the case since $a^i = e \Leftrightarrow m \mid i$ and $b^j = e \Leftrightarrow n \mid j$, and $lcm(m, n)$ is defined as the smallest number such that both m and n divide. If some power of (a^k) is the identity, then the same power of c^k is the identity. The same is true the other way around. The order of a^k is therefore the same as the order of c^k. We call this number o. $(a^k)^m = a^{km} = (a^m)^k = e$, you can do the same using b and n, which means that $o \mid m$ as well as $o \mid n$. $o \mid gcd(m, n) = 1$, then $o = 1$, which means that $k = l$. Which means that l is the smallest number such that $(ab)^l = e$.

We can write

$$lcm(m, n) = \prod_{i=1}^{t} p_i^{r_i},$$

where p_i are distinct primes and r_i are positive integers. In the case where m and n are not relatively prime, we need only find t elements whose order are $p_i^{r_i} = q_i$. This can be done since either m or n are divided by q_i. If it is m then $a^{\frac{m}{q_i}}$ is an element of order q_i, if it is n then $b^{\frac{n}{q_i}}$ has order q_i. We can therefore find elements whose order are $\{q_1, q_2, \ldots, q_t\}$ all of which are relatively prime. Thus there exists an element of order $lcm(m, n)$. □

With this fact established we can now prove that finite fields are cyclic.

Theorem 12. *If F is a finite field, then for some $a \in F^*$, $F^* = \langle a \rangle$. F^* is cyclic.*

This theorem is proved by finding that some polynomial of order n has at least n zeros by some result in group theory. n is thus both an upper and a lower bound. This technique is used in several proofs moving forward.

Proof. $|F^*| = q$ Let r be the $lcm(o(a_1), o(a_2), \ldots, o(a_q)) = l$ where a_i are distinct elements of F^*. $l \mid q$ means that $l \leq q$. By theorem 11 we can find an element $a \in F*$ where $o(a) = l$. Obviously each element of F^* satisfies the equation $x^l - 1 = 0$. The polynomial $x^l - 1$ has at most l zeros. Since each element of F^* is a zero $q \leq l$. Combining this with $l \leq q$. We get that $l \leq q \leq l$ meaning that $l = q$. a is of order q, meaning that $\langle a \rangle = F^*$, and is cyclic. □

One consequence of this theorem is that $F^* \simeq (\mathbb{Z}_{q-1}, +)$.

This theorem is also useful to find the subfields of F. As all finite fields have order p^r, a subfield of F is one of order p^s where $s \leq r$. The next theorem demonstrates what the subfields of F are.

Theorem 13. *Let F be a field of order p^r. S is a subfield of F if and only if it is the set of zeros of a polynomial $x^{(p^s)} - x$, where s divides r. This subfield has order p^s. This subfield exists for all divisors of r.*

Proof. Firstly we want to show that F has no subfields S of order p^s if $r = as+b$ where $1 \leq b < s$. If this is the case then for all $x \in S$ we have $x = x^{(p^r)} = x^{(p^{as+b})} = (x^{(p^{as})})^{(p^b)} = x^{(p^b)}$, then the polynomial $x^{(p^b)} - x$ has $p^s > p^b$ zeros, which is impossible. We can conclude that $s \mid r$. If we have a subfield S of order p^s. Then all elements of S are the zeros of $x^{(p^s)} - x$.

Let us then assume we fave a divisor s of r such that $r = ds$. Let g be a generator of F^*. Obviously $p^s \equiv 1 \pmod{p^s - 1}$. Exponentiating each side d times we obtain $p^r \equiv 1 \pmod{p^s - 1}$. This means that there exists some element h of order $p^s - 1$, i.e. the set $\{h, h^2, \ldots, h^{(p^{s-1})}, 0\}$ contains p^s distinct elements, all of which are zeros in $x^{(p^s)} - x$. h therefore generates a subfield of F of order p^s. □

We want to summarise all of our results. For any prime p and positive integer r there exist some field of order p^r. This field is the splitting field of $x^{(p^r)} - x$ over $\mathbb{Z}_p$, and is thus unique up to isomorphism. For any s which is a divisor of r we have a unique subfield of order p^s. Also all subfields of a this field are of order p^s where $s|r$. Since finite fields of a given order are unique up to isomorphism we denote a field of order p^r as $GF(p^r)$. It is called the galois field of order p^r. $GF(p^r)$ is a vector space over $\mathbb{Z}_p$ of dimension r, and $GF(p^r)^*$ is cyclic. Therefore $(GF(p^r), +) \simeq \mathbb{Z}_p^r$ and $GF(p^r)^* \simeq \mathbb{Z}_{p^r-1}$.

5 Automorphisms on Galois fields

We are going to categorize all automorphisms on any galois field, then we are going to use this knowledge to define and discuss norms on galois fields.

Our next theorem shows that the transformation $x \to x^{(p^k)}$ is an isomorphism (also called an endomorphism) on any field of characteristic p.

Theorem 14. *Let F be a field of characteristic p. The transformation $\pi_k : F \to F$, $\pi_k(x) = x^{(p^k)}$ is an embedding from F into itself. If F is finite it is an embedding onto itself, making it an automorphism.*

Proof. Using the freshmsn's dream clearly

$$\pi_k(x+y) = (x+y)^{(p^k)} = x^{(p^k)} + y^{(p^k)} = \pi_k(x) + \pi_k(y)$$

Also

$$\pi_k(xy) = (xy)^{(p^k)} = x^{(p^k)} y^{(p^k)} = \pi_k(x)\pi_k(y)$$

Meaning that π_k is a homomorphism on F. Since $x^{(p^k)} = 0 \Leftrightarrow x = 0$, π_k is also an isomorphism.

For the last part, assume that $|F| = q$, where q is an integer. Because π_k is a bijection, $|\pi_k[F]| = |F| = q$. If we have q distinct elements from F, we have the entire set. $\pi_k[F] = F$, making π_k an automorphism. □

If we look at these automorphisms in regard to $GF(p^r) = F$, we see that $\pi_r(x) = x^{(p^r)} = x$. Meaning that π_r is the identity on F. Here you can also use the fact that F^* is cyclic to demonstrate that for all $k, 1 \leq k < r$, π_k is not the identity. This is the case since for some $x \in F$ r is the smallest integer such that $\pi_r(x) = x$. This means that $\pi_k(x) = x^{(p^k)} \neq x$, π_k is not the identity.

It seems intuitive that for integers greater than r, we would get that $\pi_k = \pi_{k \ mod \ r}$. Let $k = ar + b$, where a is a is a non-negative integer and b is a non-negative integer smaller than p. If we assume $b > 0$

$$\pi_k(x) = x^{(p^k)} = x^{(p^{ar+b})} = x^{(p^{ar}p^b)} = (x^{(p^{ar})})^{(p^b)} = x^{(p^b)} = \pi_b(x)$$

In the case where $b = 0$, $\pi_k = \pi_r$, which is the identity. This means that the set $\{\pi_k \mid k \text{ is a positive integer}\} = \{\pi_k \mid 1 \leq k \leq r\}$. We denote this set (π_1).

With this being the case, we should be able to find an inverse. Let j, k be positive integers,

$$\pi_j(\pi_k(x)) = (x^{(p^k)})^{(p^j)} = x^{(p^k)(p^j)} = x^{(p^{k+j})} = \pi_{k+j}(x).$$

If $1 \leq k < r$, then there is a an j, such that $1 \leq j < r$ and $j + k = r$. $\pi_j(\pi_k) = \pi_{k+j} = \pi_r$ for the non-identity elements in (π_1). π_j is the inverse of π_k. This combined with the existence of an identity and exponentiation being associative means that this set of automorphims is an abelian group (π_1). The mapping $\pi_k \to k \ mod \ r$ is clearly an isomorphism from (π_i) onto $(\mathbb{Z}_r, +)$.

Let us look at how these automorphisms map elements of subfields of F. Let $GF(p^s)$ be a subfield of F. As we established in the last section $r = d \cdot s$ for some positive integer d. π_s leaves each element of $GF(p^s)$ invariant, meaning that $\pi_s(x) = x$ for all $x \in GF(p^s)$. The same is also the case for all π_{as} when a is a positive integer. s is also the smallest integer such that π_s leaves each element of $GF(p^s)$ invariant as previously discussed. Let $k = as + b$ where b is an integer and $0 \leq b < s$. $x = \pi_k(x) = \pi_b(x) = x^{(p^b)}$. If this were the case, the the polynomial $x^{(p^b)} - x$ would have at least $p^s > p^b$ zeros, which is impossible. $\langle \pi_s \rangle$ is a subgroup of (π_1) of order d. Using the same isomprphism described earlier, it is isomorphic to the subgroup $\langle s \rangle$ of $(\mathbb{Z}, +)$.

The next theorem shows that this is the complete picture in regards to automorphisms on F.

Theorem 15. *Let ϕ be an automorphism on a galois field $GF(p^r)$, then $\phi \in (\pi_1)$.*

Proof. If $\phi(x) = x$ and $\phi(y) = y$, then $\phi(xy) = \phi(x)\phi(y) = xy$ and $\phi(x + y) = \phi(x) + \phi(y) = x + y$. Any automorphism preserves zero and unity, meaning that it is left invariant, also $\phi(e) = \phi(xx^{-1}) = \phi(x)\phi(x^{-1}) = x\phi(x^{-1})$, multiplying both sides with x^{-1} we get $\phi(x^{-1}) = x^{-1}$. Also $0 = \phi(0) = \phi(x - x) = \phi(x) + \phi(-x)$, if we subtract with $\phi(x)$, it is clear that $\phi(-x) = -\phi(x) = -x$. The set of elements left invariant by ϕ is thus a subfield of $GF(p^r)$. It can therefore be written as $GF(p^s)$, for some s where $r = ds$.

If ϕ is the identity of $GF(p^r)$, then $\phi = \pi_r$, which would be an exponentiation. We assume there exists some a that is not left invariant ϕ. Let us look at the polynomial

$$f(x) = \prod_{i=1}^{d} (x - \pi_{is}(a))$$

If we apply π_s to each of the coefficients in $f(x)$, then

$$\prod_{i=1}^{d} (x - \pi_s(\pi_{is}(a))) = \prod_{i=1}^{d} (x - \pi_{(i+1)s}(a)) =$$

$$(x - \pi_{r+s}) \prod_{i=2}^{d} (x - \pi_{is}(a)) = \prod_{i=1}^{d} (x - \pi_{is}(a)) = f(x)$$

This means that all of the coefficients of $f(x)$ lie in $GF(p^s)$. If we apply ϕ to all of the coefficients of $f(x)$ we get

$$\prod_{i=1}^{d} (x - \phi(\pi_{is}(a))) = f(x)$$

since all of the coefficients lie in $GF(p^s)$, and are thus left invariant by ϕ. The last of the terms is $(x - \phi(\pi_r(a)) = (x - \phi(a))$. This term must equal another of the terms in $f(x)$. Let us say that it is the jth term, i.e. $(x-\phi(a)) = (x-\pi_{js}(a))$, meaning $\phi(a) = \pi_{js}(a)$. Applying the inverse of π_{js} we get $\pi_{js}^{-1}(\phi(a)) = a$. Thus the function $\pi_{js}^{-1}(\phi)$ leaves a invariant. It also leaves $GF(p^s)$ invariant, as it is the composite of two functions that leave it invariant. If $\pi_{js}^{-1}(\phi)$ does not leave $GF(p^r)$ invariant, then we set $\pi_{js} = \pi_{k_1}$ and repeat this same process by finding a b that $\pi_{k_1}(\phi)$ does not leave invariant. We repeat this process $n-1$ times until we get a function

$$\pi_{k_n}^{-1}(\pi_{k_{n-1}}^{-1}(\dots \pi_{k_1}^{-1}(\phi)\dots))$$

that leaves $GF(p^r)$ invariant. Then for any $x \in GF(p^r)$

$$\begin{aligned}\pi_{k_n}^{-1}(\pi_{k_{n-1}}^{-1}(\dots \pi_{k_1}^{-1}(\phi(x))\dots)) &= x\\ \phi(x) &= \pi_1(\pi_{k_2}(\dots \pi_{k_n}(x)\dots))\end{aligned}$$

This means that ϕ is a composite of automorphisms from (π_1), and thus $\phi \in (\pi_1)$. □

What we have now demonstrated is that the group of automorphisms of F is isomorphic to $(\mathbb{Z}_r, +)$. Generally, for a field F and a subfield S, the group of automorphisms of F that leave S invariant is denoted $G(F/S)$.

Theorem 16. *Let $F = GF(p^r)$, then there exists a $1-1$ correspondence between the subfields of F and the subgroups of the group of automorphism of F (π_1). The correspondence is given by $GF(p^s) \to (\pi_s)$.*

Proof. Let $GF(p^s) = S$ be a subfield of F, we know that each automorphism that leaves S fixed is of the form π_{si}. These automorphisms are genreated by π_s, and the thus the subgroup (π_s) is the group of automorphisms that leave S fixed.

Since $(\pi_1) \simeq (\mathbb{Z}_r, +)$ any subgroup of (π_1) is of the form (π_j). It can be instead be generated by $\pi_{lcm(j,r)}$, and is thus mapped the subgroup of automorphims leaving $GF(p^{lcm(j,r)})$ invariant. □

This can in fact be shown to be true for many types of field extensions. It is a special case of the fundamental theorem of galois theory.

6 Norms of Galois fields

In this section we are going to look at one type of function on a galois field; a norm.

Definition 9. *Let $F = GF(p^r)$ be a galois field, and let $S = GF(p^s)$ be one of it's subfields such that $r = ds$. For $x \in F$ it's **conjugates over** S are the elements $\pi_{is}(x)$, where π_{is} are automorphisms in $G(F/S)$. The **norm of** x **over** S is the product of the d conjugates over (these need not be unique). We denote the norm like this like this*

$$N_{F/S}(x) = \prod_{i=1}^{d} \pi_{is}(x)$$

We can also write the norm like this

$$N_{F/S}(x) = \prod_{i=1}^{d} \pi_{is}(x) = x^{(\sum_{i=1}^{d} p^{is})} = x^{(\sum_{i=1}^{d} q^{i})} = x^{((q^d-1)/(q-1))} \qquad (1)$$

If we apply an automorphism in $G(F/S)$ we get

$$\pi_{js}(N_{F/S}(x)) = \pi_{js}(\prod_{i=1}^{d} \pi_{is}(x)) = \prod_{i=1}^{d} \pi_{js}(\pi_{is}(x)) = \prod_{i=1}^{d} \pi_{(j+i)s}(x) = N_{F/S}(x)$$

This means that any automorphism in $G(F/S)$ leaves $N_{F/S}(x)$ invariant, thus $N_{F/S}(x) \in S$. Since a norm is a product of functions that preserve multiplication, it itself preserves multiplication. For $x, y \in F$

$$N_{F/S}(xy) = N_{F/S}(x)N_{F/S}(y)$$

It should also be noted that the conjugates of $z \in S$ are z, meaning

$$N_{F/S}(z) = z^d$$

What this means is that the norm $N_{F/S}$ is a homomorphism from F^* into S^*, we now show that it is onto.

Theorem 17. *Let $F = GF(p^r)$ be a galois field, and let $S = (GF(p^s)$ be a subfield of F. Let $N_{F/S}(x)$ be the norm over S. Then $\forall z \in S$, $\exists x \in F$ such that $N_{F/S}(x) = z$.*

Proof. Set $q = p^s$ and $r = ds$. As established earlier, $N_{F/S}$, $F^* \to F^*$ is a homomorphism. $ker(N_{F/S})$ is a normal subgroup of F^*. By the fundamental theorem of homomorphisms $F^*/ker(N_{F/S}) \simeq N_{F/S}[F^*]$. The polynomial $x^{((q^d-1)/(q-1))} - 1$ has at most $(q^d - 1)/(q - 1)$ zeros. We are thus presented with an inequality

$$\begin{aligned}
|ker(N_{F/S})| &\leq (q^d - 1)/(q - 1) \\
|ker(N_{F/S})| &\leq |F^*|/|S^*| \\
|S^*| &\leq |F^*|/|ker(N_{F/S})| \\
|S^*| &\leq |N_{F/S}[F^*]| \leq |S^*|
\end{aligned}$$

Thus $|S^*| = |N_{F/S}[F^*]|$, implying that $S^* = N_{F/S}[F^*]$. The norm of F over S is an onto mapping. □

The last theorem of this section describe what elements in F have 1 as their norm. It describes the subgroup of F^* $ker(N_{F/S})$.

Theorem 18. *Let F be a field of q^d elements, and let S be a subfield of q elements. An element $x \in F$ fulfills*

$$x^{(q^d-1)/(q-1)} = 1$$

if and only if

$$x = y^{q-1}$$

for some $y \in F^*$.

Proof. Let $x = y^{q-1}$ for some $x, y \in F$. Then $x^{(q^d-1)/(q-1)} = y^{(q^d-1)} = 1$.

Let us prove the other way. The mapping $\phi, F^* \to F^*$, $\phi(y) = y^{q-1}$ is a homomorphism. We can restate the theorem to $\phi[F^*] = ker(N_{F/S})$. By the fundamental theorem of homomorphisms $F^*/ker(\phi) \simeq \phi[F^*]$. $ker(\phi)$ has at most $q-1$ elements, since the polnomial $x^{q-1} - 1$ has at most $q-1$ zeros.

$$|ker(\phi)| \leq q - 1$$
$$(q^d - 1)/(q-1) \leq |F^*|/|(ker(\phi)| = |\phi[F^*]|$$

The image of ϕ are all zeros of $x^{(q^d-1)/(q-1)} = 1$, this polynomial has at most $(q^d-1)/(q-1)$ zeros. This means that $(q^d-1)/(q-1) \leq |\phi[F^*]| \leq (q^d-1)/(q-1)$. As $\phi(F^*)$ is a subset of $ker(N_{F/S})$ we get $\phi[F^*] = ker(N_{F/S})$. □

With this theorem established, we are ready to prove Wedderburn's little theorem.

7 Proving Wedderburn's little theorem

In this section we are going to use group theory to prove Wedderburn's little theorem. Let D be a finite division ring. The first part of the proof is going to be to demonstrate that the centralizer of an abelian subgroup of D^* is the same as the normalizer of the same subgroup. Then we are going to show that any finite group with this property is abelian itself. Meaning that D^* is abelian, and hence D is a field.

Let us first repeat what we mean by normalizer and centralizer. Let G be a group and N a subgroup. We say that N is a normal subgroup if for any $x \in G$, $xNx^{-1} = N$. This means that for any $a_1 \in N$, there exists some $a_2 \in N$ such that $xa_1x^{-1} = a_2$.

The normalizer of a subgroup S on G, is the largest subgroup of G which S is a normal subgroup of. We write it like this $N_G(S) = \{x \in G \mid xSx^{-1} = S\}$. It is easily verified that $N_G(S)$ is a group. If $x, y \in N_G(S)$, then $xyS(xy)^{-1} = xySy^{-1}x^{-1} = xSx^{-1} = S$, $xy \in N_G(S)$. Also $xSx^{-1} = S$ means that $S = x^{-1}Sx$. Therefore $x^{-1} \in N_G(S)$. Since S is contained in $N_G(S)$, it is a normal subgroup of the normalizer.

The centralizer is a similar concept. It is the set of all elements in G that commute with all the elements of S. We denote it like this $C_G(S) = \{x \in G \mid xs = sx, \text{ for all } s \in S\}$. The identity obviously commutes with S. If we have that $x, y \in G$ then $xys = xsy = sxy$. We also have that $x^{-1}s = (s^{-1}x)^{-1} = (xs^{-1})^{-1} = sx^{-1}$. The centralizer is a group.

If $sx = xs$ we have that $xsx^{-1} = s$ and therefore $xSx^{-1} = S$. This means that $C_G(S)$ is a subgroup of $N_G(S)$. If we wanted to show that these two groups were equal, we would only need to show that $N_G(S)$ is a subgroup of $C_G(S)$. This leads us to our next theorem.

Theorem 19. *If D is a finite division ring. Then for any abelian subgroup G of D^*, we have that $N_{D^*}(G) = C_{D^*}(G)$.*

Outline of the proof: The overall goal is to show that for any element $x \in N_{D^*}(G)$ we also have that $x \in C_{D^*}(G)$. We know that since $x^{|D^*|} = 1 \in C_{D^*}(G)$ we can find the smallest integer m such that $x^m \in C_{D^*}(G)$. We create a field F that contains both G and x^m. Since it is a field $F^* \subseteq C_{D^*}(G)$. This means that if we show that if $x \in F$, then $x \in C_{D^*}(G)$. We note that the mapping $a \to xax^{-1}$ is an automorphism on F. We denote it as σ. We set S as the subfield F left invariant by σ, and y as an element such that $N_{F/S}(y) = x^m$. We show that the expression

$$(x-y)(1+\sum_{i=1}^{m-1}(\prod_{j=1}^{i}\sigma^{j-1}(y^{-1}))x^i) - y = 0$$

By demonstrating that the latter factor cannot be equal to zero we get that $x = y \in C_{D^*}(G)$.

Proof. Let $x \in N_{D^*}(G)$, we want to show that $xa = ax$ for all $a \in G$. We know that $x^{|D^*|} = 1$. Since $1 \in C_{D^*}(G)$ there exists an integer m that is the smallest integer where $x^m \in C_{D^*}(G)$. If $m = 1$ we are done, since then $xa = ax$. We will from now on assume that $1 < m$.

We now want to find a field that contains G and x^m. Let H be the subgroup of D^* generated by G and x^m. Since x^m commutes with G the group H is abelian. Let F be the set of finite sums of elements of H. That is

$$F = \{\sum_{i=1}^{n} b_i \mid b_i \in H\}$$

Obviously F is closed under addition. It is also closed under multiplication and abelian since

$$\sum_{i=1}^{n_1} b_i \sum_{i=1}^{n_2} c_i = \sum_{\substack{i\leq n_1\\ j\leq n_2}} b_i c_j = \sum_{\substack{i\leq n_1\\ j\leq n_2}} c_i b_j = \sum_{i=1}^{n_2} c_i \sum_{i=1}^{n_1} b_i =$$

Remember that D is of characteristic of a prime p. This means that $(p-1)1 = -1$ and $p \cdot 1 = 0$. Therefore F contains 0 and the additive inverses of elements in F. It is therefore a finite commutative integral domain. Meaning that F is a galois field by theorem 3.

$F^* \subseteq C_{D^*}(G) \subseteq N_{D^*}(G)$, which means that $xF^*x^{-1} = F^*$. Combine this with $x0x^{-1} = 0$ we have that $\sigma(a) = xax^{-1}$ is a mapping from $F \rightarrow F$.

$$\sigma(a_1a_2) = xa_1a_2x^{-1} = (xa_1x^{-1})(xa_2x^{-1}) = \sigma(a_1)\sigma(a_2)$$
$$\sigma(a_1 + a_2) = x(a_1 + a_2)x^{-1} = xa_1x^{-1} + xa_2x^{-1} = \sigma(a_1) + \sigma(a_2)$$

σ is therefore a homomorphism. $\sigma(a) = 0 \implies a = 0$. σ is therefore an automorphism.

$\sigma^m(a) = x^m a x^{-m} = ax^m x^{-1} = a$. Therefore σ^m is the identity on F. If $v < m$, then there exists an $a_v \in F$ such that $\sigma^v(a_v) = x^v a_v x^{-v} \neq a_v$. Therefore σ is an automorphism of order m. Since $\sigma(x^m) = xx^m x^{-1} = x^m$, x^m is in the subfield of F that are left invariant by σ. We call this field S. By theorem 17 we know that there exists an element $y \in F$ such that

$$N_{F/S}(y) = \sigma(y)\sigma^2(y)\cdots\sigma^m(y) = x^m$$

Let us look at the following expression, we want to show that it is equal to 0 (we denote $\sigma^0 = \sigma^m$):

$$f(x, y) = (x - y)(1 + \sum_{i=1}^{m-1}(\prod_{j=1}^{i}\sigma^{j-1}(y^{-1}))x^i) =$$

$$x + \sum_{i=1}^{m-1} x(\prod_{j=1}^{i}\sigma^{j-1}(y^{-1}))x^i - y - x - \sum_{i=2}^{m-1}(\prod_{j=2}^{i}\sigma^{j-1}(y^{-1}))x^i$$

Let $2 \leq r \leq m-1$. If we compare the terms here, we see that

$$(\prod_{j=2}^{r} \sigma^{j-1}(y^{-1}))x^r = (\prod_{j=2}^{r} x\sigma^{j-2}(y^{-1})x^{-1})x^r = x(\prod_{j=1}^{r-1} \sigma^{j-1}(y^{-1}))x^{r-1}$$

This means that all but two of the terms of $f(x,y)$ cancel out. If we then look at one of the remaining terms:

$$x(\prod_{j=1}^{m-1} \sigma^{j-1}(y^{-1}))x^{m-1} = (\prod_{j=1}^{m-1} x\sigma^{j-1}(y^{-1})x^{-1})x^m = (\prod_{j=1}^{m-1} \sigma^{j}(y^{-1})x^m =$$

$$(\sigma^m(y^{-1}))^{-1}(\prod_{j=1}^{m} \sigma^{j}(y^{-1}))x^m = yN_{F/S}(y^{-1})N_{F/S}(y) = y$$

The last thing we could do since the norm preserves multiplication. We can now say that

$$f(x,y) = (x-y)(1 + \sum_{i=1}^{m-1}(\prod_{j=1}^{i} \sigma^{j-1}(y^{-1}))x^i) = x(\prod_{j=1}^{m-1} \sigma^{j-1}(y^{-1}))x^{m-1} - y = 0$$

With this being the case we can say that either $x - y = 0$ or

$$1 + \sum_{i=1}^{m-1}(\prod_{j=1}^{i} \sigma^{j-1}(y^{-1}))x^i = 0 \tag{2}$$

We are going to show that the latter cannot be the case. If we assume it is the case, we arrive at a contradiction. (2) is a relation of the form:

$$1 + \sum_{v=1}^{t} c_{j_v} x^{j_v} = 0$$

where $c_{j_1} < c_{j_2} < \cdots < c_{j_t} < m$, $0 \neq c_{j_v} \in F$ and $c_t \neq 0$. Obviously $1 \neq 0$, and if $1 + c_{j_1}x^{j_1} = 0$, then we would get $x^{j_1} = -c_{j_1}^{-1} \in F$, which would be a contradiction. We can therefore also add that $1 < t < m$.

We want to show that if we have one of these relations, we can produce another one of that type of relation with fewer terms. We know that there exists some $a_{j_1} \in G \subseteq F^*$ such that $x^{j_1}a_{j_1}x^{-j_1} \neq a_{j_1}$. We multiply our relation by a_{j_1} from the right, and $a_{j_1}^{-1}$ from the left. We get

$$\begin{aligned}
0 = 1 + \sum_{v=1}^{t} a_{j_1}^{-1} c_{j_v} x^{j_v} a_{j_1} = \\
= 1 + \sum_{v=1}^{t} a_{j_1}^{-1} c_{j_v} x^{j_v} a_{j_1} x^{-j_v} x^{j_v} \\
= 1 + \sum_{v=1}^{t} a_{j_1}^{-1} c_{j_v} \sigma^{j_v}(a_{j_1}) x^{j_v} \\
= 1 + \sum_{v=1}^{t} d_{j_v} x^{j_v}
\end{aligned}$$

Since σ is an automorphism on F, σ^{j_v} is also an automorphism on F. Therefore $d_{j_v} \in F$. If we subtract this relation from our first relation we get

$$\begin{aligned}
0 = 1 + \sum_{v=1}^{t} c_{j_v} x^{j_v} - (1 + \sum_{v=1}^{t} d_{j_v} x^{j_v}) \\
= \sum_{v=1}^{t} (c_{j_v} - d_{j_v}) x^{j_v} \\
= c_{j_v} - d_{j_v} + \sum_{v=2}^{t} (c_{j_v} - d_{j_v}) x^{j_v}
\end{aligned}$$

Because of how we selected a_{j_1}, and since c_{j_1} and $a_{j_1}^{-1}$ both are elements of the same field F, we can conclude that

$$d_{j_1} = a_{j_1}^{-1} c_{j_1} \sigma^{j_1}(a_{j_1}) \neq a_{j_1}^{-1} c_{j_1} a_{j_1} = c_{j_1} a_{j_1}^{-1} a_{j_1} = c_{j_1}$$

With this being the case $c_{j_1} - d_{j_1} \neq 0$, and therefore it has an inverse. We denote $(c_{j_1} - d_{j_1})^{-1}(c_{j_v} - d_{j_v}) = e_{j_v}$. If we multiply the inverse we get a third relation

$$0 = (c_{j_1} - d_{j_1})^{-1}(c_{j_v} - d_{j_v} + \sum_{v=2}^{t} (c_{j_v} - d_{j_v}) x^{j_v}) = 1 + \sum_{v=2}^{t} e_{j_v} x^{j_v}$$

We can repeat this same process until we get a relation with fewer then two terms, which is impossible. Therefore

$$1 + \sum_{i=1}^{m-1} (\prod_{j=1}^{i} \sigma^{j-1}(y^{-1})) x^i = 0$$

presents us with a contradiction. We can thus conclude that $x - y = 0$, meaning $x = y \in F^* \subseteq C_{D^*}(G)$. We thus conclude by saying $N_{D^*}(G) = C_{D^*}(G)$. □

The only thing that remains before we have proven Wedderburn's little is the theorem that any finite group is abelian if the normalizer of all abelian subgroups of the gruop is the same as the centralizer of the subgroup. We recall that the centre of a group is the centralizer of a group, the subgroup that commute with all elements of the group. The centre of a group G is $C_G(G)$. We are going to use this concept when proving our last theorem.

Theorem 20. *Let G be a finite group. If for every abelian subgroup of G the normalizer of that group coincides with the centralizer, then G is abelian.*

Outline of the proof: $|G| = N$. We prove this by using induction. We assume that the theorem is correct for all groups of order less than G. From this we can assume that all subgroups of G are abelian. From here we have two cases, wither the centre is the identity, or it is not.

In the case in which the centre Z is not the identity we show that G is ableian. The first part to demonstrate this is to show that the quotient group G/Z is abelian. This is accomplished by showing that for any abelian subgroup $\overline{U}$ of G/Z, $N_{G/Z}(\overline{U}) = C_{G/Z}(\overline{U})$. We note that since $1 < |Z|$, $|G/Z| < |G|$. And by the induction hypothesis G/Z is abelian. We use this knowledge to show that for any two elements in $a, b \in G$, the element b is in the normalizer of the abelian subgroup generated by Z and a. Thus it is in the centralizer of that group. Meaning that $ab = ba$, G is abelian.

For the second part we show that $Z = e$ leads to a contradiction. One of the first consequences of this assumption is that G is not abelian. We look at maximal subgroups of G. Since G is not abelian it has a proper maximal subgroup U. We find that there are an equal number of conjugate subgroups of U and cosets of U. This leads us to show that the number of non-identity elements in all of the conjugate subgroups of U is somewhere in the range $[N/2, N-2]$. We can therefore wind another maximal subgroup V. The non-identity elements in the conjugate subgroups of V are all different from the ones in the conjugate subgroups of U. There are therefore more than N elements in G, a contradiction. Z is not the identity.

Proof. We are going to use strong induction on the size of the group to prove this theorem. Let $|G| = N$.

If $N = 1$ it is clear that G is abelian.

Now we are going to assume that the theorem is true for all groups that have order lower than N. One immediate consequence of this is that all the proper subgroups of G are abelian. Let Z be the centre of G.

Let us first consider the case in which $1 < |Z|$. If this is the case then $|G/Z| < |G|$. Let $\overline{U}$ be an abelian subgroup of G/Z. We want to show that $C_{G/Z}(\overline{U}) = N_{G/Z}(\overline{U})$. If $\overline{U} = G/Z$, we get that G/Z is abelian. We therefore assume that $\overline{U}$ is a proper subgroup of G/Z. Let U be the subgroup of G generated by the elements of the cosets of Z which are in $\overline{U}$. In other words $U = \{u \mid u \in \overline{u}, \overline{u} \in \overline{U}\}$. We can now rewrite $\overline{U} = \{uZ \mid u \in U\}$. Since $\overline{U}$ is a proper subgroup of G/Z, U is a proper subgroup of G, therefore U is abelian. Let $\overline{x} \in N_{G/Z}(\overline{U})$, and let $x \in \overline{x}$. We can rewrite this as $\overline{x} = xZ$ and $(xZ)\overline{U}(x^{-1}Z) = \overline{U}$. For any $u_1 \in U$ there is some $u_2 \in U$ such that

$$xZu_1Zx^{-1}Z = u_2Z$$
$$xu_1x^{-1}Z = u_2Z$$

We can find z_1 and z_2 in Z such that

$$xu_1x^{-1}z_1 = u_2z_2$$
$$xu_1x^{-1} = u_2z_2z_1^{-1} \in U$$

We can therefore write further that $xUx^{-1} = \{xux^{-1} \mid u \in \overline{u}, \overline{u} \in \overline{U}\} = \{u \mid u \in \overline{u}, \overline{u} \in \overline{U}\} = U$. Since $x \in N_G(U)$, we have $x \in C_G(U)$. This means that $xZ\overline{u} = xZuZ = uZxZ = \overline{u}xZ$, therefore we have that $\overline{x}\overline{U} = \overline{U}\overline{x}$. $\overline{x} \in C_{G/Z}(\overline{U})$. Since the order of G/Z is less than N it is abelian by the induction hypothesis.

We are going to show that G is abelian. Let a, b be any elements of G. Since Z is commutes with all of G, the subgroup of G generated by a and Z is abelian. We denote it as $(a, Z) = \{a^mz \mid z \in Z\}$. In the next equation we will use z_i to denote an element of Z. We will apply G/Z and (a, Z) being abelian and Z being a normal subgroup of G.

$$ba^mz_1b^{-1} = bz_2a^mb^{-1} = bz_2a^mz_3z_3^{-1}b^{-1} = a^mz_4bz_5z_3^{-1}b^{-1} = a^mz_6$$

Thus $b(a, Z)b^{-1} = (a, Z)$, since $b \in N_G((a, Z))$ we have that b commutes with (a, Z). In particular

$$ab = ba$$

We are going to show that Z being the identity leads to a contradiction. Z being the identity means that G is not abelian. Remember that a maximal subgroup is on which is not properly contained in any proper subgroup of G. Let U be a maximal subgroup. U is abelian.

Let us look at the conjugate subgroups of U, that is the subgroups of the form $xUx^{-1}, x \in G$. Our interests lie in finding out when they are the same, and finding how many elements are in all of the conjugate subgroups. If we look at when two conjugates are the same we see that

$$xUx^{-1} = yUy^{-1}$$
$$(y^{-1}x)U(y^{-1}x)^{-1} = U$$

The conjugates coincide if and only if $y^{-1}x \in N_G(U)$, or equivilantely $y^{-1}x \in C_G(U)$. This means that the group $(y^{-1}x, U)$ is abelian, since it is generated by an abelian group and an element the commutes with U. If $y^{-1}x$ is not in U then by U being maximal $(y^{-1}x, U) = G$. Since G is not abelian $y^{-1}x \in U$, since we are presented with a contradiction when it is not the case. The assumption that $y^{-1}x$ is not in U is therefore false. This leads us to conclude that $y^{-1}x \in C_G(U)$ if and only if $y^{-1}xU = U$, which is the case if and only if

$$yU = xU$$

The amount of conjugate subgroups directly therefore corresponds with the number of left cosets. Also recall that $|xUx^{-1}| = |xU| = |U| = |yU| = |yUy^{-1}|$. The number of these cosets is $(G : U)$. Let

$$\begin{gathered} xu_1x^{-1} = yu_2y^{-1} \\ (y^{-1}x)u_1(y^{-1}x)^{-1} = u_2 \end{gathered}$$

$y^{-1}x \in N_G(U)$, which means that $y^{-1}x \in U$, or $u_1 = u_2 = e$. If two elements from conjugate different subgroups are the same then they are the identity. Meaning that for two different conjugate subgroups their intersection is $\{e\}$. The number of non-identity elements in all of the conjugate groups of U is therefore

$$(G : U)(|U| - 1) = \frac{|G|}{|U|}(|U| - 1) = N - \frac{N}{|U|}$$

We now want to show that this means that there are more than N elements in G, a contradiction. Since G is not abelian it has a proper non-trivial subgroup, it therefore has a proper non-trivial maximal subgroup. We call it U. Since $2 \leq |U| \leq N/2$, we get

$$\frac{N}{2} \leq N - \frac{N}{|U|} \leq N - 2$$

There thus exists some non-identity element in G not contained in a conjugate subgroup of U.

Let V be a maximal subgroup containing that element. Since U is maximal, the group generated by U and V is therefore $(U, V) = G$. If we have some element in a in the intersection of U and V, we know that it commutes with $(U, V) = G$ since both U and V are abelian. Therefore $a \in Z = \{e\}$. If we then look at the conjugate subgroups of V, and when they coincide with conjugate subgroups of U

$$\begin{gathered} xUx^{-1} = yVy^{-1} \\ y^{-1}xU(y^{-1}x)^{-1} = V \end{gathered}$$

However, we know that V contains elements not in any conjugate subgroup of U. Meaning that the non identity elements of conjugate subgroups of V are wholly distinct from those of the conjugate subgroups of U. We therefore have

$$2N - \frac{N}{|U|} - \frac{N}{|V|} \geq N$$

Distinct non-identity elements of G, which is a contradiction. The assumption that G is not abelian leads to a contradiction. G is abelian. □

Wedderburn's little theorem states that a finite integral domain is a finite field. By theorem 3 a finite integral domain is a finite division ring. Theorem 19 combined with theorem 20 means that any finite divison ring is a finite field. Therefore any finite integral domain is a finite field.

References

[1] Phani Bhushan Bhattacharya, Surender Kumar Jain, and SR Nagpaul. *Basic abstract algebra*. Cambridge University Press, second edition edition, 1994.

[2] Hans J Zassenhaus. A group-theoretic proof of a theorem of maclagan-wedderburn. *Glasgow Mathematical Journal*, 1(2):53–63, 1952.