EVERY FINITE DIVISION RING IS A FIELD

PETER PHELAN

1. Introduction

In this report, we refer to R as a ring with multiplicative identity e. The proof presented by Daniel Matthews blends together an interesting mix of ingredients, group theory, linear algebra and complex numbers to arrive at a rather surprising result. As Daniel pointed out, what makes this result so unexpected is that it establishes a connection between the number of elements in a division ring and its multiplication being commutative. Originally proven by Joseph Wedderburn in 1905, it is often referred to as Wedderburn's theorem or Wedderburn's little theorem.

2. Wedderburn's Theorem

Wedderburn's theorem states that every finite division ring is a field. This is equivalent to the statement that every finite division ring is commutative, a point made clear by the following presentation of the well known definitions.

Definition 2.1. A ring is a set R equipped with the binary operations $+$ and $\cdot$ such that $(R, +)$ is an abelian group and $(R, \cdot)$ is a monoid where multiplication is distributive with respect to addition.

Definition 2.2. A division ring is a non-trivial ring R where every element has a multiplicative inverse.

Definition 2.3. A field is a non-trivial division ring R where multiplication is required to be commutative.

Before proceeding with the proof, we should recall some preliminary group theory. Suppose R is a division ring and $r \in R$.

Definition 2.4. The centraliser of r is the set $C_r(R) = \{x \in R \mid xr = rx\}$.

Definition 2.5. The centre of R is the set $Z(R) = \{x \in R \mid xs = sx,\ \forall s \in R\}$.

Suppose R is a finite division ring, we immediately obtain from these definitions that $Z(R) = \bigcap_{r \in R} C_r(R)$ and it can be easily verified that $C_r(R)$ and $Z(R)$ are sub-division rings. Since R is finite and all elements of $Z(R)$ commute we can say that $Z(R)$ is a field with $|Z(R)| = q$ for some $q \in \mathbb{N}$.

Date: 17/10/2018.

Theorem 2.6 (Wedderburn's Theorem)**.** *Let R be a finite division ring, then R is commutative.*

Proof. Let us assume that R is not commutative, this means there exists some $r \in R$ such that $C_r(R) \neq R$. We can consider R and $C_r(R)$ as vector spaces over $Z(R)$. If n and n_r are the dimensions of these vector spaces respectively, then we find that $|R| = q^n$, $|C_r(R)| = q^{n_r}$ and from our assumption $n > n_r$.

Define the equivalence relation $\sim$ on $R^* = R \setminus \{0\}$. Let $r_1, r_2 \in R^*$, then

$$r_1 \sim r_2 \iff r_1 = x^{-1} r_2 x \quad \text{for some } x \in R^*$$

It can be verified that this is an equivalence relation, thus we have the equivalence class $A_r = \{x^{-1}rx \mid x \in R^*\}$ of elements in R^* equivalent to r. Define the surjective map $q_r : R^* \to A_r$ sending $x \mapsto x^{-1}rx$. Suppose that for $x, y \in R^*$, $q_r(x) = q_r(y)$.

$$\begin{aligned} x^{-1}rx = y^{-1}ry &\iff (yx^{-1})r = r(yx^{-1}) \\ &\iff yx^{-1} \in C_r^*(R) = C_r(R) \setminus \{0\} \\ &\iff y \in C_r^*(R) \cdot x = \{zx \mid z \in C_r^*(R)\} \\ \therefore\ q_r(x) = q_r(y) &\iff y \in C_r^*(R) \cdot x \end{aligned}$$

Since $C_r(R)$ is a sub-division ring, the multiplicative identity $e \in C_r^*(R)$, so we know that $y = ey \in C_r^*(R) \cdot y$ which means both cosets $C_r^*(R) \cdot x$, $C_r^*(R) \cdot y$ share an element. Therefore $C_r^*(R) \cdot x = C_r^*(R) \cdot y$ and so we obtain:

$$q_r(x) = q_r(y) \iff C_r^*(R) \cdot x = C_r^*(R) \cdot y$$

Then $|A_r|$ is the index of $C_r^*(R)$, so by Lagrange's theorem $|R^*| = |C_r^*(R)| \cdot |A_r|$ and we obtain

$$|A_r| = \frac{|R^*|}{|C_r^*(R)|} = \frac{q^n - 1}{q^{n_r} - 1} \in \mathbb{Z}$$

Implying that $(q^{n_r} - 1) \mid (q^n - 1)$

Claim that this implies $n_r | n$. Lets assume the contrary, then $n = an_r + b$ for $0 < b < n_r$.

$$\begin{aligned} (q^{n_r} - 1) \mid (q^{an_r + b} - 1) &\implies (q^{n_r} - 1) \mid (q^{an_r + b} - 1) \\ &\implies (q^{n_r} - 1) \mid ((q^{an_r + b} - 1) - (q^{n_r} - 1)) \\ &\implies (q^{n_r} - 1) \mid q^{n_r}(q^{(a-1)n_r + b} - 1) \quad \text{and note that } (q^{n_r} - 1) \nmid q^{n_r} \\ &\implies (q^{n_r} - 1) \mid q^{n_r}(q^{(a-2)n_r + b} - 1) \quad \text{by the same technique} \\ &\implies \dots \\ &\implies (q^{n_r} - 1) \mid (q^b - 1) \\ &\Rightarrow\Leftarrow \text{since } b < n_r \end{aligned}$$

Therefore $n_r | n$

Let $s \in Z^*(R)$, then $A_s = \{x^{-1}sx \mid x \in R^*\} = \{s\}$ and $|A_s| = 1$. Now suppose $|A_s| = 1$, its single element must be s as $s = ese = (e)^{-1}se$ is always satisfied. Then we can say that $|A_s| = 1 \iff s \in Z^*(R)$. Since we've assumed that R is not commutative, there are equivalence classes A_r such that $|A_r| > 1$.

Let $\{A_k\}_{k=1}^m$ be the collection of all such non-trivial equivalence classes. Recall that R can be partitioned by its equivalence classes. In this way we obtain the class formula.

$$|R^*| = |Z^*(R)| + \sum_{k=1}^{m} |[A_k]| \implies q^n - 1 = q - 1 + \sum_{k=1}^{m} \frac{q^n - 1}{q^{n_{r_k}} - 1}$$

Now we turn our attention to matters of polynomials and complex numbers. Recall that the roots of the equation $x^n - 1 = 0$ are the n-th roots of unity $\zeta_n^m = \exp(\frac{2\pi i m}{n})$. Let λ be some root of unity. Some of these roots satisy $\lambda^d = 1$ for some $d < n$, take for example $\lambda = -1 \implies \lambda^2 = 1$.

Suppose for such a root λ we choose the smallest such d satisfying this equation, by definition this is the order of λ in the group of the roots of unity of $x^n - 1$. Recall that the order of every element of a group divides the order of the group by Lagranges theorem, which implies $d|n$.
Now suppose for $d < n$ that $d|n$. This means that $n = kd$ for some integer $k < n$. Let us consider $\zeta_n^k = \exp(\frac{2\pi i k}{n})$.

$$\begin{aligned}(\zeta_n^k)^d &= \exp(\frac{2\pi i k d}{n}) \\ &= \exp(\frac{2\pi i k d}{kd}) \\ &= \exp(2\pi i) \\ &= 1 \text{ by Euler's identity.}\end{aligned}$$

This means there exists λ such that $\lambda^d = 1$ and thus

$$\exists\lambda,\ \lambda^d = 1 \iff d|n \tag{1}$$

We define the n-th cyclotomic polynomial

$$\Phi_d(x) = \prod_{\lambda^d=1} (x - \lambda)$$

Since every root of unity has some order d, (1) implies that

$$x^n - 1 = \prod_{d|n} \Phi_d(x) \tag{2}$$

Claim that $\Phi_d(x) \in \mathbb{Z}[x]$ with constant term ± 1. Let us prove this claim by induction, first we consider the base case.

Suppose $d = 1$, then $\Phi_1(x) = x - 1$ since $\lambda = 1$ is the only root. The conditions are trivially satisfied and thus the base case is true.

Suppose the claim is true for all $k < d$, so $\Phi_k(x) \in \mathbb{Z}[x]$ with constant term ± 1 for all $k < d$. Then from (2) we know that

$$x^d - 1 = \Phi_d(x) \prod_{\substack{b|d \\ b \neq d}} \Phi_b(x) = (\sum_{i=0}^{l} a_i x^i)(\sum_{i=0}^{d-l} b_i x^i)$$
$$= \sum_{i=0}^{d} \sum_{k=0}^{i} a_k b_{k-i} x^i$$

By assumption all $b_i \in \mathbb{Z}$ and $b_0 = \pm 1$. Now we will compare the coefficients on both sides of the above equation, and briefly employ an inductive argument.

For the $i = 0$ term, we have $a_0 b_0 = -1$, $b_0 = \pm 1 \implies a_0 = \mp 1$
For the $i = 1$ term, we have $a_0 b_1 + a_1 b_0 = 0$. Since $a_0, b_0, b_1 \in \mathbb{Z} \implies a_1 \in \mathbb{Z}$
For the i-th term where $i < d$, we have $a_0 b_i + a_1 b_{i-1} + \cdots + a_{i-1} b_1 + a_i b_0 = 0$. Since by assumption $a_0, \ldots, a_{i-1}, b_0, \ldots, b_i \in \mathbb{Z} \implies a_i \in \mathbb{Z}$
Finally for the $i = d$ term, we have $a_d b_0 + (a_0 b_d + a_1 b_{d-1} + \cdots + a_{d-1} b_1) = 1$. Since $a_0, \ldots, a_{d-1}, b_0, \ldots, b_d \in \mathbb{Z} \implies a_d \in \mathbb{Z}$
Therefore all $a_i, b_i \in \mathbb{Z}$ for all $0 \leq i \leq d$ and thus $\Phi_k(x) \in \mathbb{Z}[x]$ with constant term ± 1 for all $k \in \mathbb{N}$ by induction

Let $n_1, \ldots, n_m$ be all of the n_r such that $n_r | n$ described above and consider the factorisation for any $0 \leq k \leq m$

$$x^n - 1 = (x^{n_k} - 1)\Phi_n(x) \prod_{\substack{d|n \\ d \nmid n_k \\ d \neq n}} \Phi_d(x)$$

from which we obtain that for all k

$$\Phi_n(x) | x^n - 1 \quad \text{and} \quad \Phi_n(x) | \frac{x^n - 1}{x^{n_k} - 1}$$

Therefore, by the class equation

$$\Phi_n(q) | (q - 1) \tag{3}$$

We claim that this is a contradiction.

$$\Phi_n(z) = \prod_{\lambda^d = 1} (z - \lambda)$$
$$\implies |\Phi_n(z)| = \prod_{\lambda^d = 1} |(z - \lambda)| \tag{4}$$

Let $\lambda = a + ib$ be some root of order n. We know that $n > 1$ since $R \neq Z(R)$ by our assumption, so $\lambda \neq 1$.

$$\begin{aligned}
|q-\lambda|^2 &= |q-a-ib|^2 \\
&= (q-a)^2 + b^2 \\
&= q^2 - 2aq + a^2 + b^2 \\
&= q^2 - 2aq + 1 \ \text{ since } \lambda^2 = a^2 + b^2 = 1 \\
&> q^2 - 2q + 1 \ \text{ since } \lambda \neq 1 \implies \mathrm{Re}\{\lambda\} = a < 1 \\
&= (q-1)^2
\end{aligned}$$

Therefore for all roots λ of order n

$$\begin{aligned}
&|q-\lambda| > q-1 \\
\implies &\prod_{\lambda^d=1} |(q-\lambda)| > q-1 \\
&\implies |\Phi_n(q)| > q-1 \ \text{ by (4)} \\
&\Rightarrow\!\Leftarrow \ \text{ by (3)}
\end{aligned}$$

Finally, our assumption has lead to a contradiction, so we conclude that R is commutative and thus a field. This proves the theorem. □

3. Additional comments

While not relevant to the above proof, I came across some interesting lore surrounding this theorem. Shortly after Wedderburn's first proof, Leonard Eugene Dickson provided an alternative. It was later noted that Wedderburn's original proof contained a gap and so there is some disagreement as to who should be credited with the proof.

On a more unusual note, among many alternative proofs is the one given by Theodore Kaczynski, or more commonly referred to as the Unabomber. Known for being a mathematicial prodigy, anarchist author and a terrorist, his alternative proof to this theorem was his first published work.

References

[1] Martin Aigner and Gunter M. Ziegler. Proofs from The Book. Springer-Verlag, Berlin, fifth edition, 2014. Including illustrations by Karl H. Hofmann