Every finite division ring is a field

Martin Maxa

A ring with unit R is called a *division ring*, if each non-zero element of R has a multiplicative inverse. To prove that every finite division ring is also a field we need to show only that R is commutative. For this reason we can reformulate the theorem we want to prove as follows:

Theorem 1. *Every finite division ring R is commutative.*

Definition 2. For an element s in R let C_s be the set $\{x \in R : xs = sx\}$. We call C_s the *centralizer* of s.

Definition 3. The *center Z of a ring R* is the set $Z = \bigcap_{s \in R} C_s$.

In particular 0 and 1 are in Z and all elements in Z commute, so that Z is a finite field.

We have $q = |Z|$, $|R| = q^n$ and $|C_s| = q^{n_s}$ for some integers n, n_s.

Now consider on the set $R^\star := R \setminus \{0\}$ the equivalence relation

$$r^{'} \sim r \Leftrightarrow r^{'} = x^{-1}rx \text{ for some } x \in R^\star$$

and let

$$A_s := \{x^{-1}sx : x \in R^\star\}$$

be the equivalence class containing s.

We now prove the main theorem by contradiction. Let us assume that there is some $s \in R$ such that the centralizer C_s is not all of R or equivalently, that $n_s < n$. By our assumption, there are classes A_s with $|A_s| \geq 2$.

Now define for $s \in R^\star$ the map $f_s \colon x \mapsto x^{-1}sx$ from $R^\star$ onto A_s.

We have:

$$x^{-1}sx = y^{-1}sy \Leftrightarrow yx^{-1} \in C_s^\star \longleftrightarrow y \in C_s^\star x$$

where $C_s^\star x = \{zx : z \in C_s^\star\}$ has size $|C_s^\star|$. Hence any element $x^{-1}sx$ is the image of precisely $q^{n_s} - 1$ elements in $R^\star$ under the map f_s.
Note that $|R^\star| = |A_s||C_s^\star|$. In particular

$$\frac{|R^\star|}{|C_s^\star|} = \frac{q^n - 1}{q^{n_s} - 1} = |A_s|$$

is an integer for all s.

Now denote by $A_1, \ldots, A_t$ the equivalence classes containing more than one element. Hence, by our assumption, we know $t \geq 1$. Since $|R^\star| = |Z^\star| + \sum_{i=1}^{t} |A_i|$

This gives the proof of so-called class formula

Lemma 4 (Class formula)**.**

$$q^n - 1 = q - 1 + \sum_{i=1}^{t} \frac{q^n - 1}{q^{n_i} - 1} \text{ where } 1 < \frac{q^n - 1}{q^{n_i} - 1} \in N \text{ for all } i.$$

Lemma 5. *We have* $q^{n_i} - 1 \mid q^n - 1 \Rightarrow n_i \mid n$*, in particular* $n_i \mid n$ *for all* i*.*

Now we denote by G the group of the *n-th roots of the unity* in the complex numbers.

By the Lagrange theorem, we have $d \mid n$ whenever d is the order of some $\Lambda \in G$.

We proceed now to define another tool we need:

Definition 6. $\phi_d(x) := \prod_{order(\lambda)=d}(x - \lambda)$

Since every root has some order d, we can write

$$x^n - 1 = \prod_{d|n} \phi_d(x).$$

Here is important lemma for our proof:

Lemma 7. *The polynomial* ϕ_n *lies in* $\mathbb{Z}[x]$ *and the absolute coeficient of* ϕ_n *is either 1 or* -1*.*

We now finish the proof of the Theorem: Let $n_i \mid n$ be one of the numbers appearing in Lemma 5. Then

$$x^n - 1 = \prod_{d|n} \phi_d(x) = (x^{n_i} - 1)\phi_n(x) \prod_{d|n, d\nmid n_i, d\neq n} \phi_d(x)$$

We conclude that in $\mathbb{Z}$:

$$\phi_n(q) \mid q^n - 1 \quad \text{and} \quad \phi_n(q) \mid \frac{q^n - 1}{q^{n_i} - 1} \qquad \text{for all } i$$

From this and the Class Formula (Lemma 4) we obtain:

$$\phi_n(q) \mid q - 1.$$

But here we have a contradiction, because:

$$|\phi_n(q)| = \prod_{order(\lambda)=n} |q - \lambda| > q - 1.$$

This implies that $\phi_n(q)$ cannot be a divisor of $q - 1$.

Conclusion

As we can see the proof by contradiction contains only elementary algebraic tools. Because of its simplicity and elegance it deserves its place in The Book.