Every finite division ring is a field

Chapter 5

Rings are important structures in modern algebra. If a ring R has a multiplicative unit element 1 and every nonzero element has a multiplicative inverse, then R is called a *division ring*. So, all that is missing in R from being a field is the commutativity of multiplication. The best-known example of a non-commutative division ring is the ring of quaternions discovered by Hamilton. But, as the chapter title says, every such division ring must of necessity be infinite. If R is finite, then the axioms force the multiplication to be commutative.

This result which is now a classic has caught the imagination of many mathematicians, because, as Herstein writes: "It is so unexpectedly interrelating two seemingly unrelated things, the number of elements in a certain algebraic system and the multiplication of that system."

Ernst Witt

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

This beautiful theorem which is usually attributed to MacLagan Wedderburn has been proved by many people using a variety of different ideas. Wedderburn himself gave three proofs in 1905, and another proof was given by Leonard E. Dickson in the same year. More proofs were later given by Emil Artin, Hans Zassenhaus, Nicolas Bourbaki, and many others. One proof stands out for its simplicity and elegance. It was found by Ernst Witt in 1931 and combines two elementary ideas towards a glorious finish.

Proof. Our first ingredient comes from a blend of linear algebra and basic group theory. For an arbitrary element $s \in R$, let C_s be the set $\{x \in R : xs = sx\}$ of elements which commute with s; C_s is called the *centralizer* of s. Clearly, C_s contains 0 and 1 and is a sub-division ring of R. The *center* Z is the set of elements which commute with all elements of R, thus $Z = \bigcap_{s \in R} C_s$. In particular, all elements of Z commute, 0 and 1 are in Z, and so Z is a *finite field*. Let us set $|Z| = q$.

We can regard R and C_s as vector spaces over the field Z and deduce that $|R| = q^n$, where n is the dimension of the vector space R over Z, and similarly $|C_s| = q^{n_s}$ for suitable integers $n_s \geq 1$.

Now let us assume that R is not a field. This means that for *some* $s \in R$ the centralizer C_s is not all of R, or, what is the same, $n_s < n$.

On the set $R^* := R \backslash \{0\}$ we consider the relation

$$r' \sim r \quad :\Longleftrightarrow \quad r' = x^{-1} r x \quad \text{for some } x \in R^*$$