Frobenius' Theorem

Richard Koch

February 6, 2015

Theorem 1 (Frobenius) *If a finite dimensional vector space over R has a product making it a (possibly noncommutative) field, then the resulting field is isomorphic to R, C, or H.*

Proof: We give a proof by R. S. Palais, published in the American Mathematical Monthly for April, 1968.

Call the object D. Since $1 \in D$, $R \subset D$. If this is all of D, we are done. Otherwise let $d \notin R$ be in D. Since $\dim(R) < \infty$, the elements $1, d, d^2, \ldots$ are eventually linearly dependent. Hence there is a polynomial $P(x)$ over R such that $P(d) = 0$. By the fundamental theorem of algebra, P can be factored into linear and quadratic terms, so $P_1(d)P_2(d)\ldots P_k(d) = 0$. By field axioms, one of these terms is zero. If d satisfies a linear equation, then $d \in R$, so assume $ad^2 + bd + c = 0$. Then

$$d = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

It follows that $\sqrt{b^2 - 4ac} \in D$. If this is real, then d would be real. So $b^2 - 4ac < 0$ and $\sqrt{b^2 - 4ac} = \sqrt{4ac - b^2}i$ where $i \in D$ satisfies $i^2 = -1$.

We will use this argument again, so just for the record, notice that if d is some other element not in R, we can still write $d = r_1 + r_2 j$ for an element j satisfying $j^2 = -1$.

Return to the specific y used originally, and the i we produced satisfying $i^2 = -1$. It follows that $C \subset D$. If $C = D$, we are done. So suppose C is not all of D.

If we ignore the general multiplication in D and only notice that elements in D can be scalar multiplied by elements in C on the left, we see that D is a vector space over C.

Define $T : D \to D$ by $T(x) = xi$. This is a C-linear transformation. Let

$$D_+ = \{x | T(x) = ix\} = \{x | xi = ix\}$$

$$D_- = \{x | T(x) = -ix\} = \{x | xi = -ix\}$$

Each is a subspace of D. The intersection of these subspaces is $\{0\}$ because an element in both satisfies $ix = -ix$, so $2ix = 0$ and $x = 0$. The sum of the two subspaces is everything, because for any $x \in D$ we have $i\frac{x-ixi}{2} = \frac{x-ixi}{2}i$ and $i\frac{x+ixi}{2} = -\frac{x+ixi}{2}i$, so

$$x = \frac{x - ixi}{2} + \frac{x + ixi}{2}$$

Every element of C is in D_+. Conversely, if $e \in D_+$ then e commutes with all complex numbers. The elements $1, e, e^2, \ldots$ are eventually linearly dependent over C, so e satisfies a polynomial $P(x)$. Factor $P = P_1(X) \ldots P_k(X)$, noting that over C, every irreducible factor is linear. So for some i, $P_i(X) = 0$ and $e \in C$.

Notice the the product of any two elements of D_- is in D_+, for $ix = -xi$ and $iy = -iy$ implies $ixy = -xiy = xyi$.

Let y be a nonzero element of D_-. Then the previous paragraph shows that right multiplication by y gives a complex linear map $D_- \to D_+$ which is one-to-one. Consequently, D_- must be one-dimensional over C. We conclude that the dimension of D over R is 4.

Suppose again that y is a nonzero element of D_-. By the argument at the start of the proof, we can write $y = r_1 + r_2 j$ for j some element satisfying $j^2 = -1$.

Then $y^2 \in D_+$ and $y^2 = r_1^2 + 2r_1 r_2 j - r_2^2$. This element is in C, so either $r_1 r_2 = 0$ or else $j \in C$ and consequently $y \in C$, which is impossible. So $r_1 = 0$ or $r_2 = 0$. If $r_2 = 0$, $y \in R$, which is impossible. So $r_1 = 0$ and $j \in D_-$.

We conclude that $1, i, j, ij$ is a basic of D, since j generates D_- over C. Note that $ij = -ji$ by definition of D_-. It follows that $(ij)^2 = ijij = -ijji = -1$. Define $k = ij$. Then $i^2 = j^2 = k^2 = -1$. Also $ij = k = -ji$. Also $jk = jij = -ijj = i$ and $kj = ijj = -i$. Finally $ki = iji = -jii = j$ and $ik = iij = -j$. QED.