proof of Wedderburn's theorem

Canonical name	ProofOfWedderburnsTheorem
Date of creation	2013-03-22 13:10:50
Last modified on	2013-03-22 13:10:50
Owner	lieven (1075)
Last modified by	lieven (1075)
Numerical id	8
Author	lieven (1075)
Entry type	Proof
Classification	msc 12E15

We want to show that the multiplication operation in a finite division ring is abelian.

We denote the centralizer in D of an element x as $C_D(x)$.

Lemma. The centralizer is a subring.

0 and 1 are obviously elements of $C_D(x)$ and if y and z are, then $x(-y) = -(xy) = -(yx) = (-y)x$, $x(y+z) = xy + xz = yx + zx = (y+z)x$ and $x(yz) = (xy)z = (yx)z = y(xz) = y(zx) = (yz)x$, so $-y, y+z$, and yz are also elements of $C_D(x)$. Moreover, for $y \neq 0$, $xy = yx$ implies $y^{-1}x = xy^{-1}$, so y^{-1} is also an element of $C_D(x)$.

Now we consider the center of D which we'll call $Z(D)$. This is also a subring and is in fact the intersection of all centralizers.

$$Z(D) = \bigcap_{x \in D} C_D(x)$$

$Z(D)$ is an abelian subring of D and is thus a field. We can consider D and every $C_D(x)$ as vector spaces over $Z(D)$ of dimension n and n_x respectively. Since D can be viewed as a module over $C_D(x)$ we find that n_x divides n. If we put $q := |Z(D)|$, we see that $q \geq 2$ since $\{0,1\} \subset Z(D)$, and that $|C_D(x)| = q^{n_x}$ and $|D| = q^n$.

It suffices to show that $n = 1$ to prove that multiplication is abelian, since then $|Z(D)| = |D|$ and so $Z(D) = D$.

We now consider $D^* := D - \{0\}$ and apply the conjugacy class formula.

$$|D^*| = |Z(D^*)| + \sum_x [D^* : C_{D^*}(x)]$$

which gives

$$q^n - 1 = q - 1 + \sum_x \frac{q^n - 1}{q^{n_x} - 1}$$

.

By Zsigmondy's theorem, there exists a prime p that divides $q^n - 1$ but doesn't divide any of the $q^m - 1$ for $0 < m < n$, except in 2 exceptional cases which will be dealt with separately. Such a prime p will divide $q^n - 1$ and each of the $\frac{q^n-1}{q^{n_x}-1}$. So it will also divide $q - 1$ which can only happen if $n = 1$.

We now deal with the 2 exceptional cases. In the first case n equals 2, which would D is a vector space of dimension 2 over $Z(D)$, with elements of the form $a + b\alpha$ where $a, b \in Z(D)$. Such elements clearly commute so $D = Z(D)$ which contradicts our assumption that $n = 2$. In the second case,

$n = 6$ and $q = 2$. The class equation reduces to $64 - 1 = 2 - 1 + \sum_x \frac{2^6-1}{2^{n_x}-1}$ where n_x divides 6. This gives $62 = 63x + 21y + 9z$ with x, y and z integers, which is impossible since the right hand side is divisible by 3 and the left hand side isn't.