Every finite division ring is a field

Martin Maxa

March 23, 2012

Theorem

Every finite division ring R is commutative

centralizer

Definition

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

- elements which commute with s
- contains 0 and 1
- sub-division ring of R

center

Definition

The *center* Z is the set $Z = \bigcap_{s \in R} C_s$

- each element of Z commute with all elements of R
- all elements of Z commute
- 0 and 1 are in Z
- Z is finite field

on $R^* := R\backslash\{0\}$ an equivalence relation:

$$r' \sim r :\longleftrightarrow r' = x^{-1}rx \ \ \textit{for some } x \ \in R^* \tag{1}$$

equivalence class containing s

$$A_s := \{x^{-1}sx : s \in R^*\} \tag{2}$$

- $\mid A_s \mid = 1$ when s is in the center Z
- $\mid A_s \mid \geq 2$ implies contradiction

map f_s

define for $s \in R^*$ the map $f_s : x \longmapsto x^{-1}sx$ from R^* onto A_s.

- $x^{-1}sx = y^{-1}sy \longleftrightarrow yx^{-1} \in C_s^* \longleftrightarrow y \in C_s^* x$
- $C_s^* x = \{zx : z \in C_s^*\}$
- any element $x^{-1}sx$ is the image of precisely $\mid C_s^* \mid = q^{n_s} - 1$ elements in R^* under the map f_s

Class formula

Lemma (Class formula)

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

- note that $1 < \frac{q^n - 1}{q^{n_i} - 1} \in N$ for all i

Class formula

Lemma (Class formula)

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

- note that $1 < \dfrac{q^n - 1}{q^{n_i} - 1} \in N$ for all i

Lemma

$q^{n_i} - 1 \mid q^n - 1 \longrightarrow n_i \mid n$

n=an_i+r, $0 \leq r < n_i$ then $q^{n_i} - 1 \mid q^{an_i + r}$ implies:

$$q^{n_i} - 1 \mid (q^{an_i + r}) - (q^{n_i} - 1) = q^{n_i}(q^{(a-1)n_i + r} - 1)$$

- q^{n_i} and $q^{n_i} - 1$ are relatively prime
- $q^{n_i} - 1 \mid q^r - 1$ with $0 \leq r < n_i$
- this implies r=0

n-th roots of unity

Definition

Consider the polynomial $x^n - 1$. Its roots in C are called the *n-th roots of unity* .

- all roots λ of $x^n - 1$ have $\mid \lambda \mid = 1$
- they are the numbers $\lambda_k = exp(\frac{2k\pi i}{n}) = cos(\frac{2k\pi}{n}) + isin(\frac{2k\pi}{n})$ $0 \leq k \leq n - 1$
- some of the roots λ satisfy $\lambda^d = 1$ for $d < n$
- roots if unity form group where smallest positive exponent d such that λ^d =1 is order of λ

n-th roots of unity

Definition

Consider the polynomial $x^n - 1$. Its roots in C are called the *n-th roots of unity* .

- all roots λ of $x^n - 1$ have $\mid \lambda \mid = 1$
- they are the numbers $\lambda_k = exp(\frac{2k\pi i}{n}) = cos(\frac{2k\pi}{n}) + isin(\frac{2k\pi}{n})$ $0 \leq k \leq n-1$
- some of the roots λ satisfy $\lambda^d = 1$ for $d < n$
- roots if unity form group where smallest positive exponent d such that λ^d =1 is order of λ

Theorem (Lagrangue)

$d \mid n$ - the order of every element of a group divides the order of the group

Definition ($\phi_d(x)$)

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

- $x^n - 1 = \prod_{d|n} \phi_d(x)$ since every root has some order d

coefficinets of $\phi_d(x)$ are integers

Lemma

$\phi_n \in Z[x]$ for all n, where constant coefficient is either 1 or -1.

proof of lemma

proof by induction.

Let:

$\phi_n(x) = \sum_{j=0}^{n-l} a_j x^j$

$p(x) = \sum_{i=0}^{l} p_i x^i$

- for n=1 we have 1 as only root
- $x^n - 1 = p(x)\phi_n(x)$, with $p_0 = 1$ or $p_0 = -1$
- since $-1 = p_0 a_0$, $a_0 \in \{-1, 1\}$
- $\sum_{i=0}^{k} p_i a_{k-1} = \sum_{i=1}^{k} p_i a_{k-1} + p_0 a_k \in Z$
- by induction assumption, since $a_0, \ldots., a_{k-1}$ are in Z, so must be $p_0 a_k$. It implies p_0 is 1 or -1

$\square$

Let $n^i \mid n$ be one of the numbers appearing in class formula. Then

$$x^n - 1 = \prod_{d|n} \phi_d(x) = (x^{n_i} - 1)\phi_n(x) \prod_{d|n, d\nmid n_i, d\neq n} \phi_d(x) \qquad (3)$$

from this we can conclude:

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

this with class formula gives:

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

$\phi_n(x) \mid q-1$ **is contradiction with our assumption**

let $\lambda^* = a + ib$ be one of the roots, we have:

- $\lambda^* \neq 1$
- $\mid q - \lambda^* \mid^2 > q^2 - 2q + 1 = (q-1)^2$

this implies:

$$\mid \phi_n(q) \mid = \prod_{\lambda} \mid q - \lambda \mid > q - 1$$

$\phi_n(q)$ **cannot be a divisor of q-1**

Thanks for your attention.