# Wedderburnov izrek

Mojca Pesko

Fakulteta za matematiko in fiziko
Oddelek za matematiko

18. marec 2009

# Uvod

## Definicija

1. *Kolobar je množica $K$ z dvema binarnima operacijama. Prvo binarno operacijo imenujemo seštevanje,drugo pa množenje. Pri tem morajo biti izpolnjeni naslednji pogoji:*
   - *Za seštevanje je $K$ komutativna grupa*
   - *Za množenje je $K$ polgrupa*
   - *Obe operaciji povezujeta distributivnostna zakona*
2. *Obseg je tak kolobar z elementom $1 \neq 0$, v katerem je vsak od nič različen element enota.*
3. *Polje je komutativen obseg.*

# Uvod

## Definicija

1. *Kolobar je množica $K$ z dvema binarnima operacijama. Prvo binarno operacijo imenujemo seštevanje,drugo pa množenje. Pri tem morajo biti izpolnjeni naslednji pogoji:*
   - *Za seštevanje je $K$ komutativna grupa*
   - *Za množenje je $K$ polgrupa*
   - *Obe operaciji povezujeta distributivnostna zakona*
2. *Obseg je tak kolobar z elementom $1 \neq 0$, v katerem je vsak od nič različen element enota.*
3. *Polje je komutativen obseg.*

## Zgled

*Primer nekomutativnega obsega je obseg kvaternionov:*

$$\mathbb{H} = \left\{ \begin{pmatrix} \alpha & \beta \\ -\bar{\beta} & \bar{\alpha} \end{pmatrix} ; \alpha, \beta \in \mathbb{C} \right\}$$

# Wedderburnov izrek

# Wedderburnov izrek

**Izrek**

Vsak končen obseg je komutativen.

# Wedderburnov izrek

**Izrek**

Vsak končen obseg je komutativen.

**Definicija**

1. *Naj bo $s$ poljuben element obsega $R$. Označimo s $C_s$ množico vseh elementov, ki komutirajo s $s$, torej je:*

$$C_s = \{x \in R : xs = sx\}$$

*Množico $C_s$ imenujemo centralizator elementa $s$.*

2. *Center $Z$ je množica vseh elemetov,ki komutirajo z vsemi elementi v $R$.*

**Trditev**

*Če je $V$ vektorski prostor dimenzije $n$ nad obsegom $F$, je $V \cong F^n$.*

**Trditev**

*Če je $V$ vektorski prostor dimenzije $n$ nad obsegom $F$, je $V \cong F^n$.*

**Posledica**

*Če je $V$ vektorski porostor dimenzije $n$ nad končnim komutativnim obsegom $F$ s $q$ elementi, je $|V| = |F^n| = |F|^n = q^n$.*

**Trditev**

*Če je $V$ vektorski prostor dimenzije $n$ nad obsegom $F$, je $V \cong F^n$.*

**Posledica**

*Če je $V$ vektorski porostor dimenzije $n$ nad končnim komutativnim obsegom $F$ s $q$ elementi, je $|V| = |F^n| = |F|^n = q^n$.*

Na množici $R^* = R \setminus \{0\}$ definiramo relacijo
$r' \sim r \iff r' = x^{-1}rx$ za nekatere $x \in R^*$. Pravimo,da sta si elemeta $r'$ in $r$ konjugirana.

Z $A_s = \{x^{-1}sx : x \in R^*\}$ označimo ekvivalenčni razred elementa s.

Opazimo,da je $|A_s| = 1 \iff s \in Z$

## Lema

*Razredna formula:*

$$q^n - 1 = q - 1 + \sum_{i=1}^{t} \frac{q^n - 1}{q^{n_i} - 1},$$

*kjer je* $1 < \frac{q^n-1}{q^{n_i}-1} \in \mathbb{N}$ *za vsak* $i$.

## Lema

*Razredna formula:*

$$q^n - 1 = q - 1 + \sum_{i=1}^{t} \frac{q^n - 1}{q^{n_i} - 1},$$

*kjer je* $1 < \frac{q^n-1}{q^{n_i}-1} \in \mathbb{N}$ *za vsak* $i$.

## Trditev

$$(q^{n_i} - 1) \mid (q^n - 1) \Rightarrow n_i \mid n$$

## Definicija

*Ciklotomični polinom*

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

## Definicija

*Ciklotomični polinom*

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

## Trditev

*Koeficinti polinomov $\phi_n(x)$ so cela števila(to pomeni da je $\phi_d(x) \in \mathbb{Z}[x]$ za vsak i), kjer je konstantem koeficient enak 1 ali -1.*

## Definicija

*Ciklotomični polinom*

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

## Trditev

*Koeficinti polinomov $\phi_n(x)$ so cela števila(to pomeni da je $\phi_d(x) \in \mathbb{Z}[x]$ za vsak i), kjer je konstantem koeficient enak 1 ali -1.*