

N

Obnulfiri elementi v $M_2(\mathbb{Z}_2)$?

izolo $A \in M_2(\mathbb{Z}_2)$ $\exists: \det A = 1$.

$$A = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \quad \det A = ad - bc = 1$$

ali $a = 0 \Rightarrow b = c = 1$

...

N

let $\mathbb{Z}[i] = \{a + bi ; a, b \in \mathbb{Z}\}$ toloboi gaussoi
celin Gtevil.

a.) poišči vse obnulfirne elemente

b.) poišči vse razcepe rterila $\mathbb{Z}$ kot produkt
nevezcepih elementov v $\mathbb{Z}[i]$.

↪ nevezcepi so neobnulfirni elementi,
vzeličini od nič, ki jih se
lahko zapisati kot produkt
dveh obnulfirnih elementov

✓✓✓

Opomba: elementa, ki se razključata le

za množice z obnavljanjem elementov, sta asociativna.

razred in večkratne elemente je do
vstrega reda in asociativnosti razredno
množico določen.

opomba: gaussovemu celemu številu $a+bi$
lahko priredimo normo

$$N(a+bi) = a^2 + b^2$$

norma je vedno cela.

releq tega je $N(ab) = N(a)N(b)$

če je $a+bi$ obratljivo $\Rightarrow \exists c+di \exists$:

$$(a+bi)(c+di) = 1$$

$$N(a+bi)N(c+di) = N(1) = 1$$

torej z je obratljivo $\Leftrightarrow N(z) = 1$

^N
Pokaži, da je liho primestilo $p \in \mathbb{N}$ razcepno v
 $\mathbb{Z}[i] \Leftrightarrow p = 4t+1 \quad (t \in \mathbb{Z})!$

...

IDEALI

$I \subseteq K$ je IDEAL, če velja $I \subseteq K$ in

$$\forall i \in I, t \in K : it \in I \wedge ti \in I$$

na kratko $I \subseteq K$ in $tI \subseteq I$

primer $2\mathbb{Z}$ je ideal v $\mathbb{Z}$, $2\mathbb{Z}+1$ pa ni.

tipični primeri idealov

(a) ideal, generiran z elementom a .
(najmanjši ideal, ki vsebuje a)

$$(a) = \{ta \mid t \in K\}$$

glavni ideal

ideal je maksimalen, če $I \neq K$ in

$$I \subseteq J \subseteq K, \quad J \neq K \Rightarrow J = I \quad \text{ALI} \quad J = K$$

tg. ideal^{sk} je maksimalen $\Leftrightarrow$ ved K in I

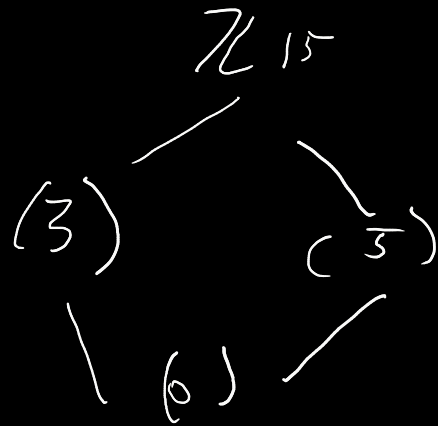
ni vsebovati drugih idealov.

$$0 := \{0\}.$$

N
poigči ideale v $\mathbb{Z}_8$, $\mathbb{Z}_{15}$ in $\mathbb{C}[x]$.

$$\mathbb{Z}_8: \quad \mathbb{Z}_8, 0, (2), (3), (4), (6)$$

$$\mathbb{Z}_{15}: \quad 0, \mathbb{Z}_{15}, (3), (5), (6) = (3)$$



for max ideals, $(3) \nmid (5)$.

