

2018.10.26.

5. konzultáció

Algebra és szám.

Polinomok faktorgyűrűi, kongruencia a témakör.

$$hf \equiv gh \pmod{m}$$

$$m \mid h(f-g) \quad \text{lko}(m, h) = d$$

$$\frac{m}{d} \mid \frac{h}{d}(f-g). \quad \text{de } \text{lko}\left(\frac{m}{d}, \frac{h}{d}\right) \nmid 1.$$

$$\mathbb{Z} \text{-ben: } a \mid b \text{ és } \text{lko}(a, b) = 1$$

$$\Downarrow \\ a \mid c \text{ volt.}$$

Adeptétel nélkül:  $\text{lko}(a, b) = 1$ . Ezt tudjuk.

$$1 = ax + by \quad / \cdot c$$

$$c = axc + byc$$

$$c \mid axc + byc \text{ lesz igaz.}$$

$$a \mid axc.$$

$$fu \equiv g \pmod{m}$$

$$fu + mv = g \text{ megoldható.}$$

$$F[x] \setminus (m) \text{ faktorgyűrű.}$$

$$\bar{f} \cdot \bar{u} = \bar{1} \quad \bar{u} = \bar{f}^{-1}$$

$$\Downarrow$$

$$fu \equiv 1 \pmod{m}$$

Fölbonthatatlan szám és prímszám fogalma volt.

$F[x]$ ,  $F$  test.

$f$  polinom felbonthatatlan, ha

- nem bomlik fel null a alacsonyabb fokú polinomok szorzatára  
(legalább első fokú)

Ha  $f = gh \Rightarrow g|1$  vagy  $h|1$  másféppen.

$f$  prímtelejtonságú, ha  $f|gh \Rightarrow f|g \vee f|h$ .

A prímek mindig felbonthatatlanok.

~~$p = ab \Rightarrow p|ab \Rightarrow p|a$~~

~~$p = \frac{a'b}{a}$~~   $\nearrow$  mert integritás-  
tételben vagyunk

$1 = a'b \Rightarrow \underline{\underline{b|1}}$

$\deg f \geq 1$ .

A felbonthatatlan számok prímek?

Indec  $\stackrel{?}{\Rightarrow}$  prím Ez igaz?

$\mathbb{Z}$ -ben:

$q$  indec és  $q|ab$ . Tfh  $q \nmid a$ , kell:  $q|b$ .

$\text{luko}(q, a) \sim 1$ .

$1 = qu + av \quad u, v \in \mathbb{Z}$ .

$b = qb'u + abv \Rightarrow \underline{\underline{q|b}}$ .

$F[x]$ -ben is működik.

Tehát: felbonthatatlan  $\equiv$  irreducibilis

Minden nem konstans polinomnak  $\exists$  irreducibilis felbontása.

Ha  $f \in F[x]$  és  $\deg f \geq 1$ :  $f$  felbontat irreducibilis polinomokra, és ez bizonyos dolgoktól eltérőre egyértelmű.  
ez ennyi.  $\square$

Még egy dolog:

R int. tart.  $q \in R$  irreducibilis, ha  $p, q \neq 1$ .  
 $q = ab \quad (a, b \in R)$   
 $\Downarrow$   
 $a \mid$  vagy  $b \mid$ .

$p \in R$  prímszem, ha  $p \mid ab \Rightarrow (p \mid a \vee p \mid b)$ .  
 $(a, b \in R)$

prímből következik, hogy irreducibilis.

$$a = q_1 q_2 \Rightarrow q_1 \mid a \wedge q_2 \mid a.$$

||

$$q_{11} q_{12} q_{21} q_{22}$$

$$q_{1i} \mid q_1 \wedge q_{2i} \mid q_2.$$

$$q_1 \mid a \wedge q_2 \mid a$$

$\Downarrow$

$$q_{1i} \mid a$$

$\Downarrow$

$$q_{2i} \mid a$$

lefelé szálló osztók.

Def.  $0 \neq a$  lecsúszó osztók.

② irreducibilis elem legkisebb prímszem.

