

2018.10.12.

h. ResultációAlgebra és

Test felbontási polinoma számelméleti jón.

$$f \mid g \wedge g \mid f \Rightarrow \left. \begin{array}{l} fh_1 = g \\ gh_2 = f \end{array} \right\} fh_1h_2 = f$$

 $f = 0$ eset triviális.

$$h_1h_2 = 1$$

mi ez?

$$h_1 \text{ és } h_2 \text{ is } \in F^* = F \setminus \{0\}$$

 h_1 és h_2 nemtriviális konstansok.

Van multiplikatív inverzük.

 $f \sim g$ ekvivalenciareláció.

$$a \in F^*$$

$$g = fa$$

$$ga^{-1} = f$$

Transzitiv.

$$f \mid g \text{ és } g \mid f,$$

$$g \mid h \text{ és } h \mid g$$

$$\frac{1}{f} \mid h. \text{ h/f teljesül. } \square$$

Az oszthatóság gyűrűben értelmezhető.

[A test felbontási polinoma integritástestben állhatna.]

$$f = x^4 + x^3 + x^2 + 1$$

$$g = x^3 + 1$$

$$\mathbb{Z}_2[x].$$

$$(x^4 + x^3 + x^2 + 1) : (x^3 + 1) = x + 1$$

$$\begin{array}{r} - \quad x^4 + x \\ \hline x^3 + x^2 + x + 1 \\ x^3 + 1 \\ \hline x^2 + x \end{array}$$

$$f = g(x+1) + x^2 + x.$$

világos példa.

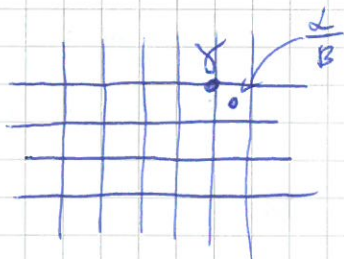
Legyenek $\mathbb{Z}[i]$ Gauss-egészek.

integrálstankönyv.

$\alpha, \beta \in \mathbb{Z}[i]$ legyenek. $\exists \gamma, \sigma \in \mathbb{Z}[i]$, hogy

$$\alpha = \beta\gamma + \sigma \quad \text{ahol} \quad |\sigma|^2 < |\beta|^2.$$

Gauss-egészek:



Ha $\beta \neq 0$.
t.h.

$\frac{\alpha}{\beta}$ kiszámolható.

De nem biztos, hogy

$$\frac{\alpha}{\beta} \in \mathbb{Z}[i].$$

Biztosan lesz olyan

pont, hogy 1-nél kisebb távolságra

van $\frac{\alpha}{\beta}$ -től - ilyen a γ pont.

$$\text{Ha: } \left| \frac{\alpha}{\beta} - \gamma \right|^2 < 1$$

$$\left| \frac{\alpha}{\beta} - \gamma \right| < 1 \text{ legyen.}$$

< 1 lesz igaz.

$$\cdot |\beta|$$

$$\left| \frac{\alpha}{\beta} - \gamma \right| = a < 1 \text{ legyen.}$$

$$|\alpha - \beta\gamma| = a|\beta| < |\beta|$$

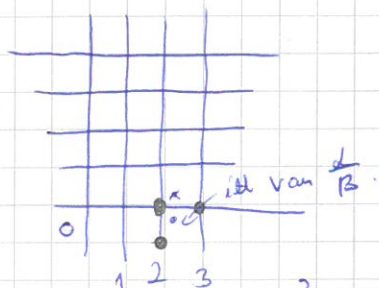
< 1

$$\alpha - \beta\gamma = \sigma \quad \alpha = \beta\gamma + \sigma, \quad |\sigma|^2 < |\beta|^2.$$

Pelda:

$$\left. \begin{aligned} \alpha &= 5 + 2i \\ \beta &= 2 + i \end{aligned} \right\}$$

$$\frac{\alpha}{\beta} = \frac{5 + 2i}{2 + i} \cdot \frac{2 - i}{2 - i} = \frac{10 + 2 - i}{4 + 1} = \frac{12 - i}{5} = \frac{12}{5} - \frac{i}{5}$$



3 pont is jó γ -nak

$$\gamma_1 = 2, \quad \gamma_2 = \beta, \quad \gamma_3 = 2 - i$$

$$(5 + 2i) = 2(2 + i) + 1 \quad \text{jó.}$$

$$\underbrace{(5 + 2i)}_{\alpha} = \underbrace{(2 + i)}_{\beta} \underbrace{(2 - i)}_{\gamma} + \underbrace{2i}_{\sigma} \quad \text{is jó.}$$

Van maradékos osztás itt is.

$$\text{Leko}(f, g) = f \text{ ut } g \text{v előáll.}$$

Nyomatjuk az euklideszi algoritmust.

Lesz egy utolsó nemzér maradék.

$$f = g u_1 + r_1$$

$$g = r_1 u_2 + r_2$$

$$r_1 = r_2 u_3 + r_3$$

$\vdots$

$$r_{n-2} = r_{n-1} u_n + \boxed{r_n}$$

$$r_{n-1} = r_n u_{n+1} + \underline{\underline{0}}$$

③

← az utolsó nemzér.

A linkomb hogy jön?

$$r_n = \text{luko}(f, g) \text{ megvan.}$$

Neu oszthatunk.

$$r_{n-3} g_n = r_{n-2} g_{n-1} g_n + r_{n-1} g_n$$

$$\textcircled{r_{n-2} - r_n} = r_{n-1} g_n \quad \nearrow \text{beírható.}$$

$$r_{n-3} g_n = r_{n-2} (g_{n-1} g_n + 1) - r_n \quad \text{beírható fel.}$$

r_{n-1} kielve est kell nyitni tovább.

Két eseményszak...

Kongruencia polinomgyűrűben.

$$f, g, m \in F[X], \quad m \neq 0:$$

$$f \equiv g \pmod{m} \Leftrightarrow m \mid f - g.$$

most is ekvivalenciareláció.

$F[X]/(m)$ osztályok. Van falterhelés.

$$\text{Ha } \bar{f}, \bar{g} \in F[X]/(m)$$

$$\bar{f} + \bar{g} = \overline{f + g}$$

$$f' \in \bar{f} \quad g' \in \bar{g}$$

$$f' \equiv f \pmod{m}$$

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

össze lehet
adni őket.

Q

$$f' + g' \equiv f + g \pmod{m}$$

$$\left. \begin{array}{l} m \mid f - f' \\ m \mid g - g' \end{array} \right\} \text{ jón.}$$

így az összegük is osztható.

$$f, g \in F[x] \quad \exists h \in F[x]$$

$$\exists fh \equiv g \pmod{m}$$

3,5-es elemű
test.

