

f21

Examen SAI, serie 15

30.01.2024

$$\textcircled{1} \quad f: \mathbb{R} \rightarrow \mathbb{R} \quad f(x) = \begin{cases} -x^2 + 6, & x \leq -2 \\ -\frac{2}{3}x - \frac{1}{3}, & -2 < x < 1 \\ x - 3, & x \geq 1 \end{cases}$$

$$f_1(x) = -x^2 + 6$$

$$f_2(x) = -\frac{2}{3}x - \frac{1}{3}, \quad f_{1,2,3}: \mathbb{R} \rightarrow \mathbb{R}$$

$$f_3(x) = x - 3$$

$$f_1(x) = 0 \Leftrightarrow 6 - x^2 = 0 \Leftrightarrow (\sqrt{6} - x)(\sqrt{6} + x) = 0 \Leftrightarrow x = \pm \sqrt{6}$$

$$\underset{x \in \mathbb{R}}{\max} f_1(x) = f_1\left(-\frac{b}{2a}\right) = f_1(0) = 6$$

$$-\sqrt{6} < -\sqrt{5} = -2$$

$$f_0(-2) = -4 + 6 = 2$$

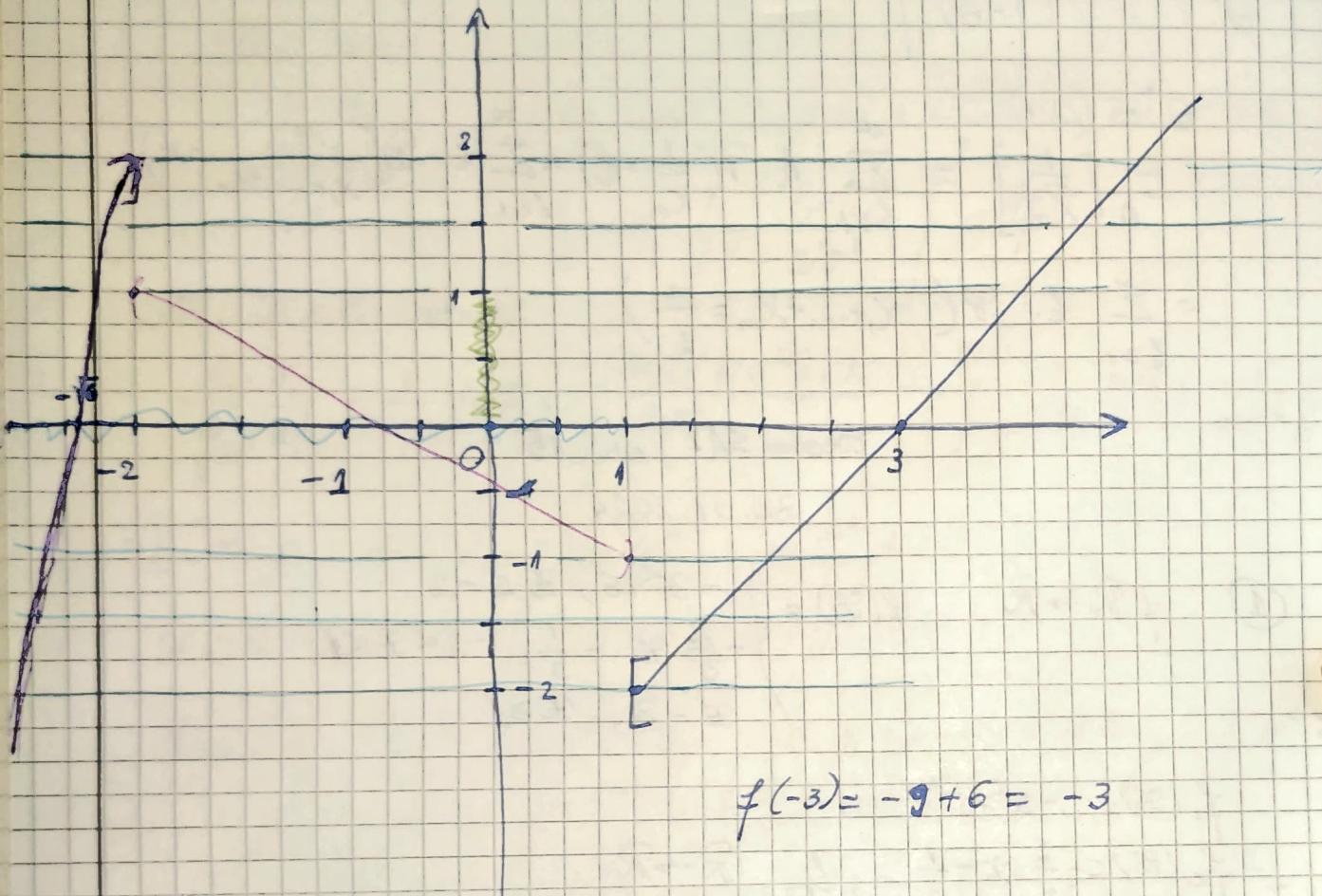
$$f_2(-2) = -\frac{2}{3} \cdot (-2) - \frac{1}{3} = \frac{4}{3} - \frac{1}{3} = \frac{3}{3} = 1$$

$$f_2(1) = -\frac{2}{3} - \frac{1}{3} = -\frac{3}{3} = -1$$

$$\therefore f_3(1) = 1 - 3 = -2 \quad f_3(3) = 0$$

Făcem graficul funcției f , folosindu-ne de restricțiile lui f_1, f_2, f_3

conform ramurilor functiei f .



Conform graficului, avem ca

$$f([-3, 1]) = f([-3, -2] \cup [-2, 0] \cup \{0\}) =$$

$$= f_1([-3, -2]) \cup f_2([-2, 0]) \cup f_3(\{0\}) =$$

$$= [-3, 2] \cup (-1, 1) \cup \{-2\} = [-3, 2]$$

$$f^{-1}((0, 1)) = (-\sqrt{6}, -\sqrt{5}) \cup \left(-2, -\frac{1}{2}\right) \cup (3, 5) =$$

$$-\bar{x}^2 + 6 = 1 \Leftrightarrow \bar{x}^2 = 5 \Leftrightarrow \bar{x} = \pm\sqrt{5} \quad \left| \begin{array}{l} \Rightarrow \bar{x} = -\sqrt{5} \\ \bar{x} \leq -2 \end{array} \right.$$

$$-\frac{2}{3}\bar{x} - \frac{1}{3} = 0 \Leftrightarrow \frac{2}{3}\bar{x} + \frac{1}{3} = 0 \Leftrightarrow \frac{2}{3}\bar{x} = -\frac{1}{3} \Leftrightarrow 2\bar{x} = -1 \quad \left| \begin{array}{l} \Rightarrow \bar{x} = -\frac{1}{2} \\ \Rightarrow \bar{x} < -2 \end{array} \right.$$

$$2\bar{x} - 3 = 1 \Leftrightarrow 2\bar{x} = 4$$

(e) $y \in \mathbb{R}$ ast. $|f^{-1}(\{y\})| = 2$.

Trbuie să găsim acelle numere $a \in \mathbb{R}$ pt. care dreapta $y = a$
intersectă G_f în două puncte.

Conform graficului $y \in [-2, -1] \cup [1, 2]$.

2)

$$\textcircled{2} \quad @ \quad G = \mathbb{Z}_2 \times \mathbb{Z}_5 \times \mathbb{Z}_8$$

elementele lui G au forma (a, b, c) , $a \in \mathbb{Z}_2$, $b \in \mathbb{Z}_5$, $c \in \mathbb{Z}_8$.

$$\text{ord}_G(a, b, c) = \text{cmmc}(\text{ord}_{\mathbb{Z}_2}(a), \text{ord}_{\mathbb{Z}_5}(b), \text{ord}_{\mathbb{Z}_8}(c))$$

$$\text{ord}(a) = 1 \text{ d.c. } a = \hat{0} \text{ și } = 2 \text{ d.c. } a = \hat{1}$$

conform Th. Lagrange, $\text{ord}(b) \mid |\mathbb{Z}_5| = 5$ deci

$$\begin{cases} \text{ord}(b) \in \{1, 5\} \\ \end{cases} \Rightarrow \begin{cases} \text{ord}(b) = 1 \text{ d.c. } b = \hat{0} \\ \text{ord}(b) = 5 \text{ d.c. } b \neq \hat{0}. \end{cases} \quad \begin{matrix} (\text{ord}(c) = 1 \Leftrightarrow \\ G \text{ este z.m. în} \\ c) \end{matrix}$$

$$\text{In } \mathbb{Z}_n: \text{ord}(\hat{k}) = \frac{n}{\text{cmmc}(n, k)}$$

$\Rightarrow_{\text{in } \mathbb{Z}_8}$; $\hat{1}, \hat{3}, \hat{5}, \hat{7}$ au ordinul 8

$\hat{0}$ are ordinul 1

$\hat{2}, \hat{6}$ au ordinul 4

$\hat{4}$ are ordinul 2.

$$\text{Dacă } \underline{(a, b, c)}, \text{cmmc}(\text{ord}_{\mathbb{Z}_2}(a), \text{ord}_{\mathbb{Z}_5}(b), \text{ord}_{\mathbb{Z}_8}(c)) =$$

$$= \text{cmmc}(\text{ord}(b), \text{ord}(c))$$

$$\left(\text{ord}(a) \mid \text{ord}(b) \wedge \text{ord}(a) \mid \text{ord}(c) \right)$$

Dacă $c \in \{\hat{0}, \hat{3}, \hat{5}, \hat{7}\}$, $b \neq \hat{0} \Rightarrow \text{ord}(a, b, c) = 40$ (T.a)

Dacă $\underline{b = \hat{0}}$, $a = \hat{0} \Rightarrow \text{ord}(a, b, c) = 8$ (T.a)

Dacă $c \in \{\hat{2}, \hat{6}\}$, $b \neq \hat{0} \Rightarrow \text{ord}(a, b, c) = 20$ (T.a)

Dacă $c \in \{\hat{4}\}$, $b = \hat{0} \Rightarrow \text{ord}(a, b, c) = 4$ (T.a)

Dacă $c=5$, $b \neq 0 \Rightarrow \text{ord}(a, b, c) = 10$ (Hg)

— „ — $b=5 \Rightarrow \text{ord}(a, b, c) = 2$ (Hg) \rightarrow 2 elem.

Dacă $c=5$, $b \neq 0$, $a=5 \Rightarrow \text{ord}(a, b, c) = 5$ (Hg)

Dacă $c=5$, $b \neq 0$, $a \neq 5 \Rightarrow \text{ord}(a, b, c) = 10$

Dacă $c=5$, $b=0$, $a=5 \Rightarrow \text{ord}(a, b, c) = 1$

Dacă $c=5$, $b=0$, $a \neq 5 \Rightarrow \text{ord}(a, b, c) = 2 \rightarrow$ în acm.

(B) Vînt izomorfie G și $\mathbb{Z}_5 \times \mathbb{Z}_{20}$?

Observăm că G are 4 elemente de ordin 5.

$$H := \mathbb{Z}_5 \times \mathbb{Z}_{20}.$$

Nu numărăm elementele de ordin 5 din H .

$(k, l) \in H$ și $\text{ord}(k, l) = 5 \Leftrightarrow \text{commc}(\text{ord}(k), \text{ord}(l)) = 5$

$\Rightarrow \left\{ \begin{array}{l} \text{ord}_{\mathbb{Z}_5}(k) = 1 \\ \text{ord}_{\mathbb{Z}_{20}}(l) = 5 \end{array} \right. \quad (\text{il divide pe } 5, \text{ deci trebuie să fie } 1)$

$\left\{ \begin{array}{l} \text{ord}_{\mathbb{Z}_{20}}(l) = 5 \Rightarrow \text{Presupunem } \alpha \leq l \leq 20 \text{ (alegoritm SCR de astăzi)} \end{array} \right.$

X

Nu
mai

$\Rightarrow \left\{ \begin{array}{l} \text{commc}(k, 20) = 1 \\ \text{ord}(k) = \frac{20}{\text{gmc}(k, 20)} = 5 \end{array} \right. \quad \left| \begin{array}{l} \text{lorim } k = 4l' \\ \Rightarrow \text{commc}(l', 5) = 1 \\ l \leq 20 \Rightarrow l' \leq 5 \end{array} \right. \quad \Rightarrow \text{commc}(l', 5) = 1$

$\Rightarrow l' \in \{1, 2, 3, 4\} \Rightarrow$ tot patru elemente de ordin 5.

Numeștem elementele de ordin 2: în G avem 3 elemente de ordin 2.

Ce rămâne: $\text{ord}(k)$, $\text{ord}_{\mathbb{Z}_5} \text{commc}(\text{ord}(k), \text{ord}(l)) = 2$ în H

$\Rightarrow \left\{ \begin{array}{l} \text{ord}(k) = 1, \text{ord}(l) = 2 \\ \text{ord}(k) = 2, \text{ord}(l) = 2 \\ \text{ord}(k) = 2, \text{ord}(l) = 1 \end{array} \right.$

În \mathbb{Z}_5 avem un element de ordin 2.

În \mathbb{Z}_{20} $\text{ord}_{\mathbb{Z}_{20}}(l) = \frac{20}{(\text{l}, 20)} < 2 \Rightarrow (\text{l}, 20) = 10 \Rightarrow \left(\frac{\text{l}}{10}, 2 \right) = 1$

$\Rightarrow \left(\frac{\text{l}}{10}, 20 \right) = 1 \Rightarrow \text{l} \equiv 0 \pmod{10} \quad \text{c.e. } \text{l} \in \{0, 10, 20\} \quad (\text{l} \in \mathbb{N})$

$\Rightarrow \frac{4}{10} = 1 \Leftrightarrow l=10 \Rightarrow$ în \mathbb{Z}_{20} există un elem. de ordin 2.

$$\Rightarrow \begin{cases} -k, l = (8, 10) \\ -k, l = (2, 10) \text{ tot } 3 \text{ " elem.} \\ -k, l = (2, 5) \end{cases}$$

în G există 5 elemente de ordin 4.

$$\text{în } H: \text{ord}(k, l) = 4 \Leftrightarrow \text{cmmc}(\underset{\mathbb{Z}_5}{\text{ord}}(k), \underset{\mathbb{Z}_{20}}{\text{ord}}(l)) = 4$$

$$\begin{aligned} &\rightarrow \text{ord}(k) = 1, \text{ord}(l) = 4 \\ &\rightarrow \text{ord}(k) = 2, \text{ord}(l) = 4 \\ &\rightarrow \text{ord}(k) = 4, \text{ord}(l) = 4 \\ &\rightarrow \text{ord}(k) = 5, \text{ord}(l) = 1 \\ &\rightarrow \text{ord}(k) = 5, \text{ord}(l) = 2 \\ &\rightarrow \text{ord}(k) = 5, \text{ord}(l) = 4 \end{aligned}$$

Decoare în \mathbb{Z}_n există ^{cel puțin} un element de ordin d , pentru orice divizor d

al lui n , $d \in \mathbb{N}$ (cum, de exemplu, $\left(\frac{m}{d}\right)$ care are ordinul d), ~~există~~

~~căci un element (k, l) care să satisfacă alturi pentru orice cau dintr-o~~
~~ale de mai sus, există cel puțin un elem. care să satisfacă aceea condiție.~~

Deci există cel puțin 5 elem. de ordin 4 (fără pătr. este un eș).

Deci G și H nu sunt izomorfe, având un nr. diferit de elem. de ordin 4.

(e) $f: \mathbb{Z}_5 \rightarrow \mathbb{Z}_8$ morfism

$$\text{Observăm că } f(m) = f(\underbrace{i + i + \dots + i}_m) = \underbrace{f(i) + f(i) + \dots + f(i)}_m = m \cdot f(i) \quad \forall m \in \mathbb{Z}_5.$$

Deci fiecare morfism este determinat de $f(i)$ (unde este singurul morfism).

$$\text{Mai observăm că } f(5) = f(0) \Leftrightarrow 5f(0) = 0 \text{ în } \mathbb{Z}_8.$$

$$\Rightarrow \text{ord}_{\mathbb{Z}_8}(f(0)) \text{ divide } 5 \quad (\text{totul } 5 \text{ este divizibil})$$

(deoarece $5^m = 1$ în G atunci $\text{ord}(5)$ divide m)

Dacă $\text{ord}_{\mathbb{Z}_8}(f(i))$ divide pe 8. (Th. Lagrange)

\hookrightarrow adică grupul

$$\Rightarrow \text{ord}(\bar{f}(\bar{i})) \mid 5, 8 \Rightarrow \text{ord}(\bar{f}(\bar{i})) = 1 \Leftrightarrow \bar{f}(\bar{i}) = \bar{0} \text{ în } \mathbb{Z}_8$$

$$\Rightarrow f(n) = m f(8) = m \cdot \bar{0} = \bar{0} \Rightarrow \text{Imaginul morfismului de la } \mathbb{Z}_8 \text{ în } \mathbb{Z}, \\ \forall n \in \mathbb{Z}_8, \text{ este el trivial } \bar{f}: \mathbb{Z}_8 \rightarrow \mathbb{Z} \quad \forall n \in \mathbb{Z}_8.$$

$$(3) \quad \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 5 & 7 & 1 & 8 & 3 & 4 & 2 & 6 \end{pmatrix}$$

$$(a) \sigma^{2024}$$

$$\sigma = (1 \ 5 \ 3)(2 \ 7)(4 \ 8 \ 6) \quad (\text{produs de cicli disjuncti})$$

$$\sigma^{2024} = (1 \ 5 \ 3)^{2024} (2 \ 7)^{2024} (4 \ 8 \ 6)^{2024} = \\ \text{cicli disjuncti} \\ \text{comute între ei}$$

$$\text{ord}(1 \ 5 \ 3) = \text{ord}(4 \ 8 \ 6) = 3 \quad (\text{fiecare ciclu de lungime } 3) \\ \text{ord}(2 \ 7) = 2$$

$$2024 = 3 \cdot 674 + 2$$

$$= (1 \ 5 \ 3)^{3 \cdot 674 + 2} ((2 \ 7)^2)^{1012} (4 \ 8 \ 6)^{3 \cdot 674 + 2} =$$

$$= (1 \ 5 \ 3)^{3 \cdot 674} \cdot (1 \ 5 \ 3)^2 \cdot \text{id}^{1012} \cdot ((4 \ 8 \ 6)^3)^{674} \cdot (4 \ 8 \ 6)^2 \\ = \text{id}^{674} \cdot (1 \ 3 \ 5) \cdot \text{id}^{674} \cdot (4 \ 6 \ 8)$$

$$= (1 \ 3 \ 5)(4 \ 6 \ 8)$$

$$\text{Alternativ, } \text{ord}(\sigma) = \text{cmmc}(\text{ord}(1 \ 5 \ 3), \text{ord}(2 \ 7), \text{ord}(4 \ 8 \ 6)) = \\ = [3, 2, 3] = 6$$

$$2024 = 6 \cdot 337 + 2$$

$$\sigma^{2024} = \sigma^{6 \cdot 337 + 2} = \sigma^{6 \cdot 337} \cdot \sigma^2 = (\sigma^6)^{337} \cdot \sigma^2 = \text{id}^{337} \cdot \sigma^2 = \\ = \sigma^2 = (1 \ 3 \ 5)(4 \ 6 \ 8)$$

$$(b) \sigma = (15)(53)(27)(48)(86) \quad (\text{prod. de trans.})$$

$$(c) (27) = (217)(25)$$

$\exists (a, b, c)$ un ciclu de lungime 3 ($a \neq b, a \neq c, b \neq c$). Atunci $(a, b, c) = (a\ b)(b\ c)$. Deci $E(a\ b\ c) = (-1)^2 = 1$.

Un produs de cicli de lungime 3 \rightsquigarrow signature

$$(a_1\ b_1\ c_1) \dots (a_n\ b_n\ c_n)$$

\uparrow \uparrow
nu neg. disjuncti

E este produs

$$E : (S_n, \sigma) \rightarrow \{-1, 0, 1\}$$

$$\text{are signature } \Leftrightarrow E(a_1\ b_1\ c_1) \dots (a_n\ b_n\ c_n) = E(a_1\ b_1\ c_1) \cdot E(a_2\ b_2\ c_2) \cdot \dots \cdot E(a_n\ b_n\ c_n) = \underbrace{1 \cdot \dots \cdot 1}_{\text{de } n \text{ ori}} = 1.$$

Deci un produs de cicli de lungime 3 este permutare pară.

$$\Rightarrow \text{Dar } E(\sigma) = (-1)^5 = -1 \text{ deci } \sigma \text{ e impară} \Rightarrow$$

$\Rightarrow \sigma$ nu se poate scrie ca produs de cicli de lungime 3.

$$(d) (1\ 2\ 3\ 4)(1\ 3\ 2\ 5) = (1\ 4\ 2)$$

$$(1\ 2\ 3\ 4)(1\ 2\ 3\ 5) = (1\ 3)(2\ 4)$$

$$(1\ 2\ 3\ 4)(1\ 3\ 4\ \underline{2})(1\ 2)(3\ 4) = (1\ 2)$$

$$\text{Deci } \sigma = (1\ 3\ 8\ 5)(1\ 8\ 3\ 5) \cdot (2\ 7\ 3\ 5)(2\ 3\ 5\ 4)(2\ 7\ 3\ 5) \cdot$$

$$\Leftrightarrow (4\ 6\ 7\ 8)(4\ 7\ 6\ 8) \circ$$

$$\textcircled{1} \quad (a) \quad \begin{array}{c} \overbrace{1+x+x^2}^{-1} \text{ in } Q[x] / (x^3-x-1) \\ \text{1+x+x}^2 \text{ inversabil in } Q[x] / (x^3-x-1) \end{array}$$

$\Leftrightarrow \text{ord}(x^3-x-1) = 3$ (Zn le da de roți)

$\Leftrightarrow \text{ord}(x^3-x-1) = 3 \Leftrightarrow x^3-x-1 \text{ red. in } Q[x]$

~~pentru că de grad 3 nu~~

decă x^3-x-1 are ord. în $Q[x]$

Răd. lui $\alpha_m x^m + \dots + a_1 x + a_0$ din Q sunt de forme

$\frac{a_0}{a_m}$ unde a_0 și b divid a_m .

Deci posibile răd. rationale ale lui x^3-x-1 sunt

$\{ \text{în multimi} \} \neq \emptyset \}. \text{ Observăm că numărul dintre aceste m.}$

nu e răd. a lui $x^3 - x - 1$. Deci $x^3 - x - 1$ e ireductibil în $\mathbb{Q}[x]$.

~~Deci $x^3 - x - 1$ nu e red. în $\mathbb{Q}[x]$~~

~~Deci $(x^3 + x + 1) \mid (x^3 - x - 1)$ $\Rightarrow x^3 - x - 1$ nu divide $x^2 + x + 1$, ceea ce e absurd.~~

că le vom te $\text{gcd}(m, p) = 1 \Leftrightarrow p \nmid m$

căci $\text{grad}(x^2 + x + 1) = 2 < 3$

$\text{grad}(x^3 - x - 1) = 3$

dacă $x^3 - x - 1$ ar divide

$x^2 + x + 1$, atunci

$x^2 + x + 1 = g(x) \cdot (x^3 - x - 1), g(x) \in \mathbb{Q}[x]$

$\Rightarrow \text{grad}(x^2 + x + 1) \geq \text{grad}(x^3 - x - 1)$ nu are sens.

$\Rightarrow x^2 + x + 1$ e inversabil în $\mathbb{Q}[x]/(x^3 - x - 1)$.

Alternativ, se poate face ca algoritmul lui Euclid pentru polinoame (împărțirea cu rest) să împărțească $x^3 - x - 1$ la $x^2 + x + 1$ împărțitorul (rest până când nu mai se împarte) și să verificăm că polinoamile sunt irreductibile (echivalență cu nr. prime pătratice).

Obs.: fără $x^2 + x + 1$ e irred. în $\mathbb{Q}[x]$ (polinoame cu coef. întregi - nu coprime)

De fapt, e meior să folosim Alg. Euclid pătraticele inversabile, deci ~~este~~ este o idee mai bună să folosim algoritmul de la început.

$$\begin{array}{r|l} x^3 - x - 1 & \\ -x^3 - x^2 - x & \hline \\ -x^2 - 2x - 1 & x - 1 \text{ rest } -x \\ +x^2 + x + 1 & \\ \hline -x & \\ \end{array}$$

grad = 1 < 2 = grad $x^2 + x + 1$

$$\begin{array}{r|l} x^2 + x + 1 & -x \\ -x^2 & \hline \\ x + 1 & -x - 1 \text{ rest } 1 \\ -x & \\ \hline 1 & \text{rest } 1 \end{array}$$

$$\Rightarrow \begin{cases} x^3 - x - 1 = (x^2 + x + 1)(x - 1) - x \\ x^2 + x + 1 = (-x)(-x - 1) + 1 \end{cases}$$

$$\Rightarrow 0 = (x^2 + x + 1) - (-x)(-x - 1)$$

$$= (x^2 + x + 1) + x(-x - 1) =$$

$$= (x^2 + x + 1) + (x + 1)(-x) =$$

$$= (x^2 + x + 1) + (x + 1)((x^2 - x - 1) - (x - 1)(x^2 + x + 1))$$

$$= (x + 1)(x^3 - x - 1) + (x^2 + x + 1)(1 - (x + 1)(x - 1))$$

$$= (x + 1)(x^3 - x - 1) + (x^2 + x + 1)(-x^2 + 2) = 1$$

$\xrightarrow{\text{modulo}}$

$$\underbrace{(x^3 - x - 1)}_{(x^3 - x - 1 = 8)} \cdot \underbrace{(-x^2 + 2)}_{\Rightarrow (x^2 + x + 1) = (-x^2 + 2)} = 0$$

am scris 0 ca o combinație liniară de $(x^3 - x - 1)$ și $(x^2 + x + 1)$ folosindu-ne de relațiile din Th. imp. anrest

$$(B) g \in Q[x] \text{ a.i. } \widehat{g}^2 = 0 \text{ în } A.$$

$$\widehat{g}^2 = 0 \text{ în } A \Leftrightarrow g^2 \in (x^3 - x - 1) \Leftrightarrow g^2 = (x^3 - x - 1) \cdot$$

$$\cdot g(x),$$

Cum $(x^3 - x - 1)$ e ireductibil și divide $g \cdot g^2$,
rezultă că $(x^3 - x - 1)$ divide g .

(ca la numere, dacă $p/k^2 \Rightarrow p/k$)

Invers, dacă $(x^3 - x - 1)$ divide g , atunci $(x^3 - x - 1)$ divide și g^2 .

Dacă $g^2 : x^3 - x - 1$ în $Q[x] \Leftrightarrow g : x^3 - x - 1$ în $Q[x]$

Dacă g sunt ~~totuși~~^{exact} multiplii de $x^3 - x - 1$ în $Q[x]$, atunci
atfel nu este idealul generat de $x^3 - x - 1$, I.e. $(x^3 - x - 1)$.

$$(5) f(x) = x^4 + 5x^3 + 2x + 1 \text{ irat. în } Q[x].$$

f are grad 4, deci f e redcuită dacă și numerele reale
racionali de către polinoamele anul de grad 3 și mai de grad 3 sau multipli
de grad 2 ireductibile.

Dacă f nu are nici o răd. comună cu un polinom de grad 3 și arcul de grad 2, atunci f are o răd. comună în \mathbb{Q} .

Potibile răd. ale lui f din \mathbb{Q} sunt $\{\pm i\}$, iar micăna nu este
a lui f.

Mai rămâne să verificăm dacă și că f nu este o produsă de două polinoame de grad 2 ireductibile.

Presupunem că $f = g \cdot h$, $\deg g = \deg h = 2$
 $g, h \in \mathbb{Q}[x]$

$$x^4 + 5x^3 + 2x + 1 = (x^2 + ax + b)(x^2 + cx + d)$$

Putem presupune că $g, h \in \mathbb{Z}[x]$. Dacă primul termen nu are coeficienți întregi, atunci putem înmulții cu cel mai mare divisor comun și obținez un polinom cu coeficienți întregi, fie că K, și obținem $Kf = g' \cdot h'$, $K \in \mathbb{Z}[x]$, $g', h' \in \mathbb{Z}[x]$.

Putem să presupunem că $h \in \mathbb{Z}[x]$ deoarece comunul cel. lui f este 1.

(Legea lui Gauss - numărul 52)

$$\Rightarrow x^4 + 5x^3 + 2x + 1 = (x^2 + ax + c)(x^2 + dx + e)$$

coeficienții lor sunt și pătratice
produsul lor e coef. lui x^4 adică 1.

$$\Rightarrow d + a = 5$$

egalăciunea

$$\begin{cases} c + e + ad = 0 \\ ae + cd = 2 \end{cases} \Rightarrow$$

$$c^2 = 1 \Rightarrow c = e = 1 \text{ sau } c = e = -1$$

$$\begin{cases} a + d = 2 \\ ad = 1 \end{cases} \Rightarrow \begin{cases} a = 1 \\ d = 1 \\ a = -1 \\ d = -1 \end{cases}$$

$$\Rightarrow -a - d = 2 \text{ și } c = e = -1$$

$$\begin{cases} a + d = 5 \\ -a - d = 2 \end{cases} \Rightarrow$$

$$\begin{cases} a + d = 2 \\ ad = 1 \\ a = 1 \\ d = 1 \end{cases}$$

$$x^4 + 5x^3 + 2x + 1 = (ax^2 + bx + c)(dx^2 + ex + f)$$

$$\left\{ \begin{array}{l} ad = 1 \\ ae + bd = 5 \end{array} \right.$$

$$ae + bd = 5 \quad | \cdot d \Rightarrow e + bd^2 = 5d$$

$$af + cd + be = 0$$

$$bf + ce = 2 \quad | \cdot c \Rightarrow bc + ec^2 = 2c$$

$$cf = 1$$

$$\rightarrow 1 + cd^2 + becd = 0 \Rightarrow d^2 + bedf$$

\exists

Alternativ, în $\mathbb{Z}_2[x]$: $\tilde{f}(x) = x^4 + x^3 + 1$ (cu rădăcini modula 2)

$$\tilde{f}(0) = 1 \quad \tilde{f}(1) = 1$$

Dacă f irred. în $\mathbb{Z}_2[x]$, atunci \tilde{f} irred în $\mathbb{Z}[x]$ și deci și în $\mathbb{Q}[x]$.

Obs. că \tilde{f} nu are răd. în $\mathbb{Z}_2[x]$. Deci \tilde{f} este redusibil de către

scrierea prod. a două polinoame irred. de grad 2 din $\mathbb{Z}_2[x]$

Polinoamele de grad 2 din $\mathbb{Z}_2[x]$: $\{x^2 + 1, x^2, x^2 + x, x^2 + x + 1\}$

Observăm că singurul ireducibil este $x^2 + x + 1$ și că și de grad 2 nu are rădăcini (celalte au rădăcine pe 0 și pe 1)

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

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

Cum $\tilde{f} \neq x^4 + x^3 + 1$, \tilde{f} nu se scrie ca prod. de polinoame irred. de grad 2 în $\mathbb{Z}_2[x] \Rightarrow f$ irred. $\Rightarrow \tilde{f}$ irred.

De a? Dacă $\deg(f) = \deg(\tilde{f})$ (coef. dominant nu se amorsează modulu 2) impune $f = g \cdot h$, $\deg g, \deg h \geq 1$ astfel

$\tilde{f} = \tilde{g} \cdot \tilde{h}$ și unde $\tilde{f}, \tilde{g}, \tilde{h}$ sunt obținute prin reducerea coef. modulo?

 (reducerea coef. modulo n este un morfism de mătăsărie de la $\mathbb{Z}[X]$ la $\mathbb{Z}_n[X]$ - & a făcut pe care, cred) cu $\deg \tilde{g}, \deg \tilde{h} \geq 1$

Dacă f e redusibil în $\mathbb{Z}[X]$ (ceea ce e dominantă la început)

 atunci \tilde{f} e redusibil în $\mathbb{Z}_n[X]$. deci

 dacă f e redusibil în $\mathbb{Z}_n[X]$, atunci f redusibil în $\mathbb{Z}[X]$.

 și dacă f nu are factori dominanți

 dominant al lui \tilde{f} este

 și $\deg f = \deg \tilde{f}$