Examen[1] la algebră, anul II, sem. II, matematică-informatică
10.06.2021

Problema 1. Fie N $\mathbb{Z}$-submodulul lui $F = \mathbb{Z}^5$ generat de $(6, 0, -3, 0, 3)$ şi $(0, 0, 8, 4, 2)$.

(1) Este N $\mathbb{Z}$-modul liber? Justificaţi. **(5 p.)**

(2) Găsiţi o bază $\{f_1, \dots, f_5\}$ în F şi $d_1, d_2 \in \mathbb{N}^*$, $d_1 \mid d_2$, cu proprietatea că $N = \langle d_1 f_1, d_2 f_2 \rangle$. **(10 p.)**

(3) Scrieţi modulul factor F/N ca o sumă directă de module ciclice. **(5 p.)**

(4) Aflaţi factorii invarianţi ai lui F/N. **(5 p.)**

(5) Aflaţi divizorii elementari ai lui F/N. **(5 p.)**

Problema 2.

(1) Arătaţi că nu există $\mathbb{Z}_2[X]$-module cu 10 elemente. **(5 p.)**

(2) Daţi două exemple de $\mathbb{Z}_2[X]$-module neizomorfe cu 32 de elemente. Sunt acestea izomorfe ca $\mathbb{Z}_2$-module? Justificaţi. **(10 p.)**

(3) Determinaţi, până la un izomorfism, toate grupurile abeliene cu 256 de elemente care conţin elemente de ordin 64. **(10 p.)**

Problema 3.

(1) Arătaţi că numărul real $\sqrt{2} + \sqrt[15]{7} + \sqrt[3]{2 + \sqrt[5]{4}}$ este algebric peste $\mathbb{Q}$. **(5 p.)**

(2) Fie $\alpha = \sqrt{1 + \sqrt{3}}$. Aflaţi polinomul minimal al lui α peste $\mathbb{Q}$. Justificaţi. **(5 p.)**

(3) Aflaţi gradul extinderii $\mathbb{Q} \subset \mathbb{Q}(\sqrt[3]{2}, \alpha)$. Justificaţi. **(5 p.)**

(4) Găsiţi un corp de descompunere al polinomului $X^7 + 1 \in \mathbb{F}_2[X]$. Justificaţi. **(10 p.)**

(5) Determinaţi rădăcinile lui $X^7 + 1$ în corpul de descompunere găsit. **(5 p.)**

(6) Descompuneţi polinomul $X^7 + 1 \in \mathbb{F}_4[X]$ în factori ireductibili. Justificaţi. **(10 p.)**

[1]**Toate subiectele sunt obligatorii. Se acordă 5 puncte din oficiu. Timp de lucru 2 ore.**

Examination paper[2]
10.06.2021

Problem 1. Let N be the $\mathbb{Z}$-submodule of $F = \mathbb{Z}^5$ generated by $(6, 0, -3, 0, 3)$ and $(0, 0, 8, 4, 2)$.

(1) Is N a free $\mathbb{Z}$-module? Justify your answer. **(5 p.)**
(2) Find a basis $\{f_1, \dots, f_5\}$ în F and $d_1, d_2 \in \mathbb{N}^*$, $d_1 \mid d_2$ with the property that $N = \langle d_1 f_1, d_2 f_2 \rangle$. **(10 p.)**
(3) Write the factor (quotient) module F/N as a direct sum of cyclic modules. **(5 p.)**
(4) Find the invariant factors of F/N. **(5 p.)**
(5) Find the elementary divisors of F/N. **(5 p.)**

Problem 2.

(1) Show that there are no $\mathbb{Z}_2[X]$-modules with 10 elements. **(5 p.)**
(2) Give two examples of $\mathbb{Z}_2[X]$-modules with 32 elements which are not isomorphic. Are these isomorphic as $\mathbb{Z}_2$-modules? Justify your answer. **(10 p.)**
(3) Find, up to isomorphism, all the abelian groups with 256 de elements which contain elements of order 64. **(10 p.)**

Problem 3.

(1) Show that the real number $\sqrt{2} + \sqrt[15]{7} + \sqrt[3]{2 + \sqrt[5]{4}}$ is algebraic over $\mathbb{Q}$. **(5 p.)**
(2) Let $\alpha = \sqrt{1 + \sqrt{3}}$. Find the minimal polynomial of α over $\mathbb{Q}$. Justify your answer. **(5 p.)**
(3) Find the degree of the field extension $\mathbb{Q} \subset \mathbb{Q}(\sqrt[3]{2}, \alpha)$. Justify your answer. **(5 p.)**
(4) Find a splitting field of the polynomial $X^7 + 1 \in \mathbb{F}_2[X]$. Justify your answer. **(10 p.)**
(5) Find the roots of the polynomial $X^7 + 1$ in the splitting field. **(5 p.)**
(6) Decompose the polynomial $X^7 + 1 \in \mathbb{F}_4[X]$ into irreducible factors. Justify your answer. **(10 p.)**

[2]**All the problems are mandatory. There are 5 points offered by default. The solutions should be sent after 2 hours. A single pdf file is allowed.**

① Examen 2021

I $N = \langle \underset{n_1}{\underset{\parallel}{(6,0,-3,0,3)}}, \underset{n_2}{\underset{\parallel}{(0,0,8,4,2)}} \rangle$

1) n_1, n_2 S.G. pentru N (așa este definit N)

Fie $a, b \in \mathbb{Z}$ a.î. $a n_1 + b n_2 = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}$

$\Rightarrow a \cdot 6 + b \cdot 0 = 0 \Rightarrow a = 0$

$a \cdot (-3) + b \cdot 8 = 0 \Rightarrow 8b = 0 \Rightarrow b = 0$

$\Rightarrow n_1, n_2$ L.i. peste $\mathbb{Z}$

$\Rightarrow$ ~~N liber~~.
N $\mathbb{Z}$-submodul liber (cu baza $\{n_1, n_2\}$)

2) $\begin{pmatrix} n_1 \\ n_2 \end{pmatrix} = \underset{A}{\underset{\parallel}{\begin{pmatrix} 6 & 0 & -3 & 0 & 3 \\ 0 & 0 & 8 & 4 & 2 \end{pmatrix}}} \begin{pmatrix} e_1 \\ e_2 \\ e_3 \\ e_4 \\ e_5 \end{pmatrix}$ unde $\{e_1 \ldots e_5\}$ baza canonică

$\mathbb{Z}$ inel principal $\Rightarrow \exists U \in GL_2(\mathbb{Z}), V \in GL_5(\mathbb{Z})$ a.î.

$D = \begin{pmatrix} d_1 & 0 & 0 & 0 & 0 \\ 0 & d_2 & 0 & 0 & 0 \end{pmatrix}$ ~~cu d_1, d_2~~ matrice diagonal canonică, d_1 / d_2 dacă $d_2 \neq 0$

și

$D = UAV$

(3)(2) Aducem A la forma diag. canonică:

$$\begin{pmatrix} 6 & 0 & -3 & 0 & 3 \\ 0 & 0 & 8 & 4 & 2 \end{pmatrix} \xleftrightarrow{L_1 = L_1 - L_2} \begin{pmatrix} 6 & 0 & -11 & -4 & 1 \\ 0 & 0 & 8 & 4 & 2 \end{pmatrix} \longleftrightarrow$$

$$\xleftrightarrow{C_1 \leftrightarrow C_5} \begin{pmatrix} 1 & 0 & -11 & -4 & 6 \\ 2 & 0 & 8 & 4 & 0 \end{pmatrix} \xleftrightarrow{L_2 = L_2 - 2L_1} \begin{pmatrix} 1 & 0 & -11 & -4 & 6 \\ 0 & 0 & 30 & 12 & -12 \end{pmatrix}$$

$$\xleftrightarrow[\substack{C_4 = C_4 + 4C_1 \\ C_5 = C_5 - 6C_1}]{C_3 = C_3 + 11C_1} \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 30 & 12 & -12 \end{pmatrix} \xleftrightarrow{C_2 \leftrightarrow C_3}$$

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 30 & 0 & 12 & -12 \end{pmatrix} \xleftrightarrow{C_2 = C_2 - 2C_4} \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 6 & 0 & 12 & -12 \end{pmatrix}$$

$$\xleftrightarrow[C_5 = C_5 + 2C_2]{C_4 = C_4 - 2C_2} \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 6 & 0 & 0 & 0 \end{pmatrix} = D = \begin{pmatrix} d_1 & 0 & \cdots \\ 0 & d_2 & \cdots \end{pmatrix}$$

$\Rightarrow d_1 = 1,\ d_2 = 6$

$$\begin{pmatrix} m_1 \\ m_2 \end{pmatrix} = \begin{pmatrix} m_1 \\ m_2 \end{pmatrix} \begin{pmatrix} e_1 \\ \vdots \\ e_5 \end{pmatrix}$$

U./

$$U\begin{pmatrix} m_1 \\ m_2 \end{pmatrix} = U\begin{pmatrix} m_1 \\ m_2 \end{pmatrix} V \cdot V^{-1} \begin{pmatrix} e_1 \\ \vdots \\ e_5 \end{pmatrix}$$

$$\underbrace{U A}_{G} = \underbrace{UAV}_{D} \underbrace{V^{-1}\begin{pmatrix} e_1 \\ \vdots \\ e_5 \end{pmatrix}}_{H}$$

Notez $G = U \cdot A$. A bază în N, $U \in GL_2(\mathbb{Z})$

③ $\Rightarrow U\cdot A = G$ bază în N

Notez $V^{-1}\begin{pmatrix} e_1 \\ \vdots \\ e_5 \end{pmatrix} = H$

$V \in GL_5(\mathbb{Z}) \Rightarrow V^{-1} \in GL_5(\mathbb{Z})$

$\begin{pmatrix} e_1 \\ \vdots \\ e_5 \end{pmatrix}$ bază în $\mathbb{Z}^5$

$\Rightarrow$

$\Rightarrow H$ bază în $\mathbb{Z}^5$

$G = D \cdot H$

$$\begin{pmatrix} g_1 \\ g_2 \end{pmatrix} = \begin{pmatrix} d_1 & 0 & 0 & 0 & 0 \\ 0 & d_2 & 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} h_1 \\ \vdots \\ h_5 \end{pmatrix}$$

$\Rightarrow g_1 = d_1 h_1$ și d_1 / d_2 $\left(\begin{matrix} d_1 = 1, d_2 = 6 \\ \text{și } 1/6 \end{matrix} \right)$

$g_2 = d_2 h_2$

Rămâne să calculez $h \Rightarrow$ Trebuie să calculez V^{-1} din $D = UAV$.

Operațiile pe coloane pe care le-am efectuat pentru a-l obține pe D au fost:

$$\begin{cases} C_1 \leftrightarrow C_5 \\ C_3 = C_3 + 11 C_1 \\ C_4 = C_4 + 4 C_1 \\ C_5 = C_5 - 6 C_1 \\ C_2 \leftrightarrow C_3 \\ C_2 = C_2 - 2C_4 \\ C_4 = C_4 - 2C_2 \\ C_5 = C_5 + 2C_2 \end{cases}$$

(4)

$$\Leftrightarrow \left\{ \begin{array}{l} P_{1,5} \\ T_{1,3}(11) \\ T_{1,4}(\cdot 4) \\ T_{1,5}(-6) \\ P_{2,3} \\ \cdot T_{4,2}(-2) \\ T_{2,4}(-2) \\ \cdot T_{2,5}(2) \end{array} \right. \Leftrightarrow \begin{array}{l} V = P_{1,5} \cdot T_{1,3}(11) \cdot T_{1,4}(4) \cdot \\ \cdot T_{1,5}(-6) \cdot P_{2,3} \cdot T_{4,2}(-2) \cdot \\ \cdot \ T_{2,4}(-2) \cdot T_{2,5}(2) \end{array}$$

$$\Downarrow$$

$$V^{-1} = T_{2,5}(-2) \cdot T_{2,4}(2) \cdot T_{4,2}(2) \cdot$$
$$\cdot P_{2,3} \cdot T_{1,5}(6) \cdot T_{1,4}(-4) \cdot T_{1,3}(-11) \cdot$$
$$\cdot P_{1,5}$$

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix} \longrightarrow \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 2 & -2 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

$$\longrightarrow \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 5 & 0 & 2 & -2 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix} \longrightarrow \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 5 & 2 & -2 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

$$\longrightarrow \begin{pmatrix} 1 & 0 & -11 & -4 & 6 \\ 0 & 0 & 5 & 2 & -2 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix} \longrightarrow \begin{pmatrix} 6 & 0 & -11 & -4 & 1 \\ -2 & 0 & 5 & 2 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 \end{pmatrix} =$$

$$= \begin{pmatrix} f_1 \\ f_2 \\ f_3 \\ f_4 \\ f_5 \end{pmatrix}$$

(5)

3) .

Fie $\{f_1 \dots f_5\}$ bază în F

$\Rightarrow$ ~~$F = f_1 \oplus f_2 \oplus f_3 \oplus f_4 \oplus f_5$~~ $\oplus f_5 \mathbb{Z}$

$F = f_1\mathbb{Z} \oplus f_2\mathbb{Z} \oplus f_3\mathbb{Z} \oplus f_4\mathbb{Z} \oplus f_5\mathbb{Z}$

Fie $\{g_1, g_2\}$ bază în N și $g_1 = f_1$
$g_2 = 6 f_2$

$\Rightarrow N = f_1\mathbb{Z} \oplus 6f_2\mathbb{Z}$

$$F/N = \frac{f_1\mathbb{Z} \oplus f_2\mathbb{Z} \oplus \dots\dots}{f_1\mathbb{Z} \oplus 6f_2\mathbb{Z}} \simeq 0 \oplus \frac{\mathbb{Z}}{6\mathbb{Z}} \oplus \mathbb{Z}^3 \simeq \mathbb{Z}_6 \oplus \mathbb{Z}^3$$

4) Factorii invarianți sunt : 6 (din partea de torsiune) și 3 (din partea liberă)

5) $\mathbb{Z}_6 \simeq \mathbb{Z}_2 \oplus \mathbb{Z}_3$ (lema chineză a resturilor)

$\Rightarrow$ Divizorii elementari sunt 2 și 3 .

⑥

II. 1) $\mathbb{Z}_2$ corp $\Rightarrow$ $\mathbb{Z}_2[X]$ inel principal.

$\Rightarrow$ Aplic teorema factorilor invarianți pt ~~un~~ M $\mathbb{Z}_2[X]$-modul ~~f.g.~~ ce ar finit de elemente:

$$M = \frac{\mathbb{Z}_2[X]}{(f_1)} \oplus \frac{\mathbb{Z}_2[X]}{(f_2)} \oplus \dots \oplus \frac{\mathbb{Z}_2[X]}{(f_n)}$$ (in particular, este și finit generat) ($f_1 \dots f_n$ polinoame $\in \mathbb{Z}_2[X]$)

Dar ~~$\mathbb{Z}_2[X]$~~

$$\# M = \# \frac{\mathbb{Z}_2[X]}{(f_1)} \cdot \dots\dots \cdot \# \frac{\mathbb{Z}_2[X]}{(f_n)}.$$ și

$$\# \frac{\mathbb{Z}_2[X]}{(f_i)} = 2^{\text{grad}(f_i)}.$$

$\Rightarrow$ $\# M$ este o putere a lui 2.

$\Rightarrow$ $\# M$ nu poate fi $2 \cdot 5$

2) Fie $A = \dfrac{\mathbb{Z}_2[X]}{(X^5)}$ și $B = \dfrac{\mathbb{Z}_2[X]}{(X)} \oplus \dfrac{\mathbb{Z}_2[X]}{(X^4)}$

$A \not\cong B$ ca și $\mathbb{Z}_2[X]$ module deoarece factorii invarianți ai lui A (i.e. X^5) nu coincid cu factorii invarianți ai lui B (i.e. X și X^4, $X \mid X^4$).

$$A = \{ \overbrace{\hat{a}_4 X^4 + \hat{a}_3 X^3 + \hat{a}_2 X^2 + \hat{a}_1 X + \hat{a}_0} \mid a_0 \dots a_4 \in \mathbb{Z}_2 \}$$

(7) $\Rightarrow$ A are $2^5 = 32$ elem.

$B = \mathbb{Z}_2 \oplus \{ a_3X^3 + a_2X^2 + a_1X + a_0 \mid a_0 \dots a_3 \in \mathbb{Z}_2 \}$

B are $2 \cdot 2^4 = 32$ elem.

$\mathbb{Z}_2$ este corp $\Rightarrow$ A și B admit câte o bază ca și $\mathbb{Z}_2$ spații vectoriale

$[A : \mathbb{Z}_2] = 5$ (deoarece $\# \mathbb{Z}_2$ are 2 elem., iar $\# A = 2^{[A:\mathbb{Z}_2]}$)

$[B : \mathbb{Z}_2] = 5$

$\Rightarrow A \simeq \mathbb{Z}_2^5 \simeq B$ ca și $\mathbb{Z}_2$ sp. vectoriale

3) $\cdot\ 256 = 2^8$

$64 = 2^6$

Orice grup abelian $\Rightarrow \mathbb{Z}$-modul.

Caut $\mathbb{Z}$-module care îl conțin și pe $\mathbb{Z}_{64}$ în descompunere.

Altfel, nu aș avea niciun element de ord 64.

Pt $G = G_1 \oplus G_2 \oplus \dots \oplus G_n$, $\text{ord}((g_1, g_2 \dots g_n)) =$

$= \text{LCM}(\text{ord}(g_1), \dots, \text{ord}(g_n))$

(8) (De exemplu, ~~...~~ $\mathbb{Z}_{2^5} \oplus \mathbb{Z}_{2^3}$ nu are elemente de ord 64 deoarece ~~...~~, ~~...~~ dacă $x \in \mathbb{Z}_{2^5} \oplus \mathbb{Z}_{2^3}$, $ord(x) \le LCM(2^5, 2^3) = 2^5 = 32$)

$256 = 2^8$. Scriu partițiile lui 8 care îl conțin și pe 6 ca și termen:

- 8
- 7 + 1
- 6 + 2
- 6 + 1 + 1

$\Rightarrow$ 4 Grupurile sunt (folosind th. fact. unic.):

$\mathbb{Z}_{256}$, $\mathbb{Z}_{128} \oplus \mathbb{Z}_2$, $\mathbb{Z}_{64} \oplus \mathbb{Z}_4$, $\mathbb{Z}_{64} \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$

3) (3) $\underbrace{\mathbb{Q} \subseteq \mathbb{Q}(\alpha)}_{4} \subseteq \mathbb{Q}(\sqrt[3]{2}, \alpha) = K$ (*)

$3 \left[\begin{array}{l} \cap \\ \mathbb{Q}(\sqrt[3]{2}) \end{array} \right.$

(**)

$\mu_{\sqrt[3]{2}, \mathbb{Q}} = X^3 - 2$ ired, monic $\Rightarrow [\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$

Eisenstein $p = 2$

Din tranzitivitatea extinderii algebrice,:

$[K : \mathbb{Q}] \vdots 4$ (*)

$[K : \mathbb{Q}] \vdots 3$ (**)

$\Rightarrow [K : \mathbb{Q}] \vdots 12$, deci ≥ 12

Dar observ că $\sqrt[3]{2}$ este răd. pentru $X^3 - 2 \in \mathbb{Q}(\alpha)[X]$

deci $[K : \mathbb{Q}(\alpha)] \leq 3$ $\Big\}$ $\Rightarrow [K : \mathbb{Q}(\alpha)] \leq 3 \cdot 4 = 12$

(*)

$\Rightarrow [K : \mathbb{Q}] = 12$

②

④ $x^7+\hat{1} \in F_2[X]$

③ $f=$

Obs. că $f(\hat{1}) = \hat{1}+\hat{1}=\hat{0}$

$\Rightarrow x+\hat{1} \mid f$

$\Rightarrow f = (x+\hat{1})\underbrace{(x^6+x^5+x^4+x^3+x^2+x+\hat{1})}_{g \text{ ired?}}$

$g(\hat{1}) = g(\hat{0}) = \hat{1} \Rightarrow$ nu are răd.

$\Rightarrow$ Singura posibilitate ca g să fie red. este să se desc. în grad 2 · grad 4 sau grad 3 · grad 3 ired fiecare.

I grad 2 · grad 4 $\Rightarrow x^2+x+\hat{1}$ singurul ired de gr 2

$$\begin{array}{l|l} x^6+x^5+x^4+x^3+x^2+x+\hat{1} & x^2+x+\hat{1} \\ \hline x^6+x^5+x^4 \quad {}^{\prime\prime}-{}^{\prime\prime} & (x^4+x) \\ \hline x^3+x^2+x+\hat{1} & \\ x^3+x^2+x & \\ \hline \hat{1} & \end{array}$$

$\hat{1} \rightarrow$ rest $\hat{1} \Rightarrow x^2+x+1 \nmid g$

③

II grad 3 · grad 3

Cont ired în $F_2[x]$ de grad 3:

$h = x^3 + ax^2 + bx + c$ cu $a, b, c \in F_2$

$h(\hat{0}) = c$ care vreau $\neq \hat{0}$

$\Downarrow$

$c = \hat{1}$

$h(\hat{1}) = \hat{1} + a + b + \hat{1} = a + b \underset{}{\overset{\text{Vreau}}{\neq}} \hat{0}$

$\Rightarrow$ • $a = 0, b = 1 \Rightarrow \boxed{x^3 + x + \hat{1}} \rightarrow$ ired (grad 3 fără răd.)

• $a = 1, b = 0 \Rightarrow \boxed{x^3 + x^2 + \hat{1}} \rightarrow$

$$\begin{array}{l|l} x^6 + x^5 + x^4 + x^3 + x^2 + x + \hat{1} & x^3 + x + \hat{1} \\ \hline x^6 + x^4 + x^3 & x^3 + x^2 + \hat{1} \\ \hline x^5 + x^2 + x + \hat{1} & \\ x^5 + x^3 + x^2 & \\ \hline x^3 + x + \hat{1} & \\ x^3 + x + \hat{1} & \\ \hline \hat{0} & \end{array}$$

OK.

$\Rightarrow$ Da, $f(x) = (x^3 + x + \hat{1}) \cdot (x^3 + x^2 + \hat{1})$

Deci $f(x) = (x + \hat{1})(x^3 + x + \hat{1})(x^3 + x^2 + \hat{1})$. , desc în fact. ired.

④

Vreau un corp în care cele 2 polin de gr 3 să aibă toate răd.

$\Rightarrow$ Mă mut în $\dfrac{F_2[X]}{X^3+X+\hat{1}} \overset{\varphi}{\simeq} F_{2^3} \overset{\text{notez}}{=:} K$

și teorema ne spun că $X^3+X+\hat{1}$ are toate răd. în K și

Două teoreme ne spun că $X^3+X+\hat{1}$ și $X^3+X^2+\hat{1}$ au același corp de desc.

$K = \{ a + br + cr^2 \,/\, a, b, c \in F_2 \}$

$\varphi(\hat{X}) = r$ rădăcina lui $X^3+X+\hat{1}$

⑤ $r^3 + r + \hat{1} = 0$. Notez x_1, x_2, x_3 rădăcinile

$x_1 = r$

Caut celelalte rădăcini:

$X^3+X+\hat{1} \,/\,'$ (derivez formal)

$3X^2+\hat{1} = X^2+\hat{1} \Rightarrow$

r nu e răd. pt $(X^3+X+\hat{1})'$,

decir r nu e răd. multiplă.

K are 8 elem.: $\underbrace{\hat{1}, \hat{0}, r}_{}$, $r+\hat{1}$, r^2, r^2+r, r^2+1, r^2+r+1

astea știu că nu sunt răd. noi.

Notez $P = x^3 + x + \hat{1}$

• $P(r+\hat{1}) = r^3 + 3r^2 + 3r + \hat{1} + r + \hat{1} + \hat{1} =$
$= r^3 + r^2 + r + 1 = r^2 \neq \hat{0}$

• $P(r^2) = r^6 + r^2 + 1$

Stim $r^3 + r + 1 = 0 \,/\cdot r$

$r^4 + r^2 + r = 0 \Rightarrow r^4 = r^2 + r$ (char $k = 2$)

$r^3 = r + 1$

$r^6 + r^4 + r^3 = 0$

$\Rightarrow r^6 = -r^3 - r^4 = r^4 + r^3$

$\Rightarrow r^6 = r^2 + r + r + 1 = r^2 + 1$

$\Rightarrow P(r^2) = r^2 + 1 + r^2 + 1 = 0$

$\Rightarrow r^2 = x_2$, a doua răd.

Aflu din Viète a 3-a răd, x_3:

~~$x_1 \cdot x_2 \cdot x_3 = 1 \Rightarrow r \cdot r^2 \cdot x_3 = 1$~~
~~$\Rightarrow x_3 = (r^3)^{-1}$~~

$x_1 + x_2 + x_3 = 0 \Rightarrow x_3 = -x_1 - x_2 = x_1 + x_2 = r^2 + r$

Deci $P(X) = (X + r)(X + r^2)(X + r^2 + r)$ (char $k = 2$, Deci „$-$" $=$ „$+$")

Fac la fel şi pt $G := x^3+x^2+\hat{1}$

$\cdot\ G(r) = r^3+r^2+\hat{1} = r^2+r \neq \hat{0}$

~~$G(r^2)=$~~

$\cdot\ G(r+\hat{1}) = r^3+3r^2+3r+\hat{1}+r^2+\hat{1}+\hat{1} =$

$= r^3+r+\hat{1} = \hat{0}$

$\Rightarrow r+\hat{1}$ răd. Notăm y_1, y_2, y_3 răd. lui G.

$y_1 = r+\hat{1}$

$G'(x) = \cancel{3r^2 = r}$

$3x^2 = x^2$

$G'(r+\hat{1}) = r^2+\hat{1} \neq \hat{0}$, $\underset{y_1}{\Rightarrow}$ răd. simplă

$\cdot\ G(r^2) = r^6+r^4+\hat{1} = r^2+\hat{1}+r^2+r+\hat{1} =$

$= r \neq \hat{0}$

$\cdot\ G(r^2+r) = r^6+3\cdot r^4\cdot r+3\cdot r^2\cdot r^2+r^3+r^4+r^2+\hat{1} =$

$r^2+r+r+\hat{1}+r^2+r+r^2+\hat{1} =$

$= r^2+1+r^5+$

$= \hat{1}+r+\cancel{r}+r^5 =$

[redacted]

Calculez r^5: $r^3+r+\hat{1}=0 \,/\cdot r^2$

$r^5+r^3+r^2=0 \Rightarrow r^5=r^3+r^2=$
$= r^2+r+1$

$\Rightarrow f(r^2+r) = r^2+2+1+1+r = r^2 \neq 0$

- $f(r^2+\hat{1}) = r^6+3r^4+3r^2+1+r^4+1+1 =$
$= r^6+r^2+1 = r^2+1+r^2+1=0$

$\Rightarrow y_2 = r^2+1$.

Scot din Viète y_3:

$y_1+y_2+y_3=1$

$\Rightarrow r+1+r^2+1+y_3=1$

$\underline{r^2+r+1=y_3}$

$\Rightarrow f=(X+\hat{1})(X+r)(X+r^2)(X+r^2+r)(X+r+1)\cdot(X+r^2+1)\cdot(X+r^2+r+1) \in \mathbb{F}_8$

(6.) În $F_4[X]$, $f=(X+\hat{1})(X^3+X+\hat{1})(X^3+X^2+\hat{1})$ desc în factori ired, pentru că $X^3+X+\hat{1}$ și $X^3+X^2+\hat{1}$ sunt de gr 3 și au răd doar în $F_8 \setminus F_2$.

$F_4 \not\subseteq F_8$