Seminar 14 12.01.2021

Exc 1 Să se arate că avem următoarele izomorfisme de inele

$\mathbb{Q}[x]/(x^2-2) \simeq \mathbb{Q}[\sqrt{2}] \overset{(*)}{=} \{a+b\sqrt{2} \mid a,b\in\mathbb{Q}\}$, $\mathbb{Q}[x]/(x-3) \simeq \mathbb{Q}$,

$\varphi: \mathbb{Q}[x]\to\mathbb{Q}$, $\varphi(P(x))=P(3)$

$\mathbb{Q}[x]/(x^2-1) \simeq \mathbb{Q}\times\mathbb{Q}$.

T.F.I $\varphi: R\to S$ morf de inele $R/\mathrm{Ker}\,\varphi \simeq \mathrm{Im}\,\varphi$

Se aplică T.F.I

$\mathbb{Q}[x]/(x^2-2) \simeq \mathbb{Q}[\sqrt{2}]$.

Care e strategia? Definesc $\varphi: \mathbb{Q}[x] \longrightarrow \mathbb{Q}[\sqrt{2}]$, 1) $\boxed{\text{morfism de inele}}$

2) $\boxed{\text{surj}}$,

cu $\boxed{\mathrm{Ker}\,\varphi=(x^2-2)}$

$(\forall) P(x)\in\mathbb{Q}[x]$ $\varphi(P(x))=P(\sqrt{2})$ e morfism de inele (vezi teoremă C12)

(alegerea lui $P(\sqrt{2})$ a fost făcută pt. a satisface $\longrightarrow$ 3)

2) φ e surj. deoarece $\varphi(a+bx)=a+b\sqrt{2}$ $(\forall)$ $a,b\in\mathbb{Q}$ ($\overset{(*)}{\Rightarrow}$ $\Rightarrow \mathrm{Im}\,\varphi=\mathbb{Q}[\sqrt{2}]$)

3) Arătăm $\mathrm{Ker}\,\varphi=(x^2-2)$ cu dubla incluziune

"$\supseteq$" Fie $f(x) \in (x^2-2) \overset{def}{\Longrightarrow} f(x) = (x^2-2)\cdot g(x)$ cu $g(x) \in \mathbb{Q}[x]$.

$$\varphi(f(x)) = \varphi((x^2-2)\cdot g(x)) \xRightarrow[\text{morf de inele}]{\text{id. } \varphi} \varphi(x^2-2)\cdot\varphi(g(x)) \underset{\varphi}{\overset{def}{=}} \underbrace{((\sqrt{2})^2-2)}_{=0}\cdot g(\sqrt{2}) = 0$$

$\underset{\ker\varphi}{\overset{def}{\Longrightarrow}} f(x) \in \ker\varphi$.

"$\subseteq$" Fie $P(x) \in \ker\varphi \underset{\ker\varphi}{\overset{def}{\Longrightarrow}} \varphi(P(x)) = 0 \underset{\varphi}{\overset{def}{\Longrightarrow}} P(\sqrt{2}) = 0$. (1)

Aplicăm teorema împ. cu rest în $\mathbb{Q}[x]$: cu grad $r(x) < 2 \Rightarrow r(x) = aX+b$, $a,b \in \mathbb{Q}$

$$P(x) = (x^2-2)\cdot q(x) + r(x) \qquad q(x), r(x) \in \mathbb{Q}[x]$$

$$P(x) = (x^2-2)\cdot q(x) + aX+b \overset{(1)}{\Longrightarrow} \underset{0}{P(\sqrt{2})} = a\sqrt{2}+b \Rightarrow a\sqrt{2}+b=0$$

Dacă $a \neq 0 \Rightarrow \sqrt{2} = -\frac{b}{a} \in \mathbb{Q}$ ✂ $\Rightarrow a=0 \Rightarrow b=0 \Rightarrow r(x)=0$

$\Rightarrow P(x) = (x^2-2)\cdot q(x) \Rightarrow P(x) \in (x^2-2)\mathbb{Q}[x]\ (= (x^2-2))$ ▯

Aplicăm T.F.I și obținem $\mathbb{Q}[x]/(x^2-2) \simeq \mathbb{Q}[\sqrt{2}]$.

$$\mathbb{Q}[X]/(X^2-1) \underset{\substack{\uparrow \\ \text{LCR} \\ (\text{vezi } C_{13})}}{\simeq} \mathbb{Q}[X]/(X-1) \times \mathbb{Q}[X]/(X+1) \underset{\text{T.F.I}}{\simeq} \mathbb{Q} \times \mathbb{Q}$$

$$(\widehat{P(X)}, \overline{G(X)}) \longmapsto (P(1), G(-1))$$

$\square$

Exc 2 Arătați că $(X^m-1, X^n-1) = X^{(m,n)}-1$, unde $m,n \in \mathbb{N}^*$.

Obs $X^d-1 \mid X^m-1$, $X^d-1 \mid X^n-1$ deoarece

$m = dm_1, n = dn_1 \leadsto X^m-1 = (X^d)^{m_1}-1 = (X^d-1)\cdot((X^d)^{m_1-1}+\dots+1)$

$X^n-1 = \dots = (X^d-1)\cdot\dots$

$d=(m,n)$ se calc. cu alg. Euclid

$$X^m-1 = (X^n-1)\cdot(X^{m-n}+\dots+X^{m-qn}) + X^r-1 \quad (1)$$

$$X^n-1 = (X^r-1)\cdot(X^{n-r}+\dots+X^{n-q_1 r}) + X^{r_1}-1 \quad (2)$$

$$\dots$$

$$X^{r_{t-1}}-1 = (X^{r_t}-1)\cdot(\dots) + \boxed{X^{r_{t+1}}-1} \quad (t+2)$$

$$X^{r_t}-1 = (X^{r_{t+1}}-1)\cdot(\dots+1) + 0$$

$m = n\cdot q + r \quad (1) \Rightarrow r = m-qn$

$n = r\cdot q_1 + r_1 \quad (2)$

$\vdots$

$r_{t-1} = r_t \cdot q_{t+1} + \boxed{r_{t+1}} \quad (t+2)$

$r_t = r_{t+1}\cdot q_{t+2} + 0$

$$\boxed{d = r_{t+1}}$$

$(X^m-1, X^n-1) = X^{r_{t+1}}-1$, $r_{t+1} = d$ $\square$

Exemplu $(x^7-1, x^4-1) = x-1$ #

$$\begin{array}{r|l} x^7-1 & x^4-1 \\ \hline -x^7+x^3 & x^3 \\ \hline / \; x^3-1 & \end{array}$$

$$\begin{cases} x^7-1 = (x^4-1)\cdot x^3 + (x^3-1) \\ x^4-1 = (x^3-1)\cdot x + \boxed{(x-1)} \\ x^3-1 = (x-1)\cdot(x^2+x+1) + 0 \end{cases}$$

$7 = 4\cdot 1 + 3$

$4 = 3\cdot 1 + \boxed{1}$

$3 = 1\cdot 3 + 0$

$$\begin{array}{r|l} x^4-1 & x^3-1 \\ \hline -x^4+x & x \\ \hline / \; x-1 & \end{array}$$

Aplicație Calculați $\text{cmmdc}(x^{34}+\underbrace{x^{33}+\ldots+x+1}_{= f(x)}, \underbrace{x^{74}+x^{73}+\ldots}_{= g(x)}+x+1)$.

Obs. că

$x^{35}-1 = (x-1)f(x)$ și $f(1) \neq 0$

$x^{75}-1 = (x-1)g(x)$ și $g(1) \neq 0$ și avem $\text{cmmdc}(x^{35}-1, x^{75}-1) = x^{(35,75)}-1 = x^5-1$

Aplicăm rez. anterior și $\Rightarrow$

$$x^5-1 = \text{cmmdc}((x-1)f(x), (x-1)g(x)) \overset{f(1)\neq 0}{\underset{(g(1)\neq 0)}{=}} (x-1)\,\text{cmmdc}(f(x), g(x))$$

$\Rightarrow \text{cmmdc}(f(x), g(x)) = \dfrac{x^5-1}{x-1} = x^4+x^3+x^2+x+1$.

Exc 3 Fie $P(x)=x^3+3x^2-7x+5$ cu rădăcinile complexe $\alpha_1, \alpha_2, \alpha_3$.

Aflați polinomul monic F care are ca rădăcini pe:

$\underset{\beta_1}{2\alpha_1+1}, \underset{\beta_2}{2\alpha_2+1}, \underset{\beta_3}{2\alpha_3+1}$ (respectiv $\alpha_1-3, \alpha_2-3, \alpha_3-3$).

$$P(x)=x^3+3x^2-7x+5=(x-\alpha_1)(x-\alpha_2)(x-\alpha_3)$$

Var 1 (calculatorie) Viète $\Rightarrow$ (*) $\begin{cases}\alpha_1+\alpha_2+\alpha_3=-3\\ \alpha_1\alpha_2+\alpha_1\alpha_3+\alpha_2\alpha_3=-7\\ \alpha_1\alpha_2\alpha_3=-5\end{cases}$

$\cdot$ $\beta_1+\beta_2+\beta_3=2(\alpha_1+\alpha_2+\alpha_3)+3=-6+3=-3$

$\cdot\cdot$ $\beta_1\beta_2+\beta_1\beta_3+\beta_2\beta_3=(2\alpha_1+1)(2\alpha_2+1)+(2\alpha_1+1)(2\alpha_3+1)+(2\alpha_2+1)(2\alpha_3+1)=$
$=4(\alpha_1\alpha_2+\alpha_1\alpha_3+\alpha_2\alpha_3)+4(\alpha_1+\alpha_2+\alpha_3)+3=-28-12+3=-37$

$\therefore$ $\beta_1\beta_2\beta_3=(2\alpha_1+1)(2\alpha_2+1)(2\alpha_3+1)=8\alpha_1\alpha_2\alpha_3+4(\alpha_1\alpha_2+\alpha_1\alpha_3+\alpha_2\alpha_3)+2(\alpha_1+\alpha_2+\alpha_3)+1$
$=-40-28-6+1=-73$.

Din $\cdot, \cdot\cdot$ și $\therefore$ $\Rightarrow$ $F(x)=(x-\beta_1)(x-\beta_2)(x-\beta_3)=\boxed{x^3+3x^2-37x+73}$

Var 2 $\beta_j=2\alpha_j+1$, $j=\overline{1,3}$ $\Rightarrow$ $\alpha_j=\dfrac{\beta_j-1}{2}$ $j=\overline{1,3}$

$$P(x)=(x-\alpha_1)(x-\alpha_2)(x-\alpha_3)$$

$$P\left(\frac{x-1}{2}\right)=\left(\frac{x-1}{2}-\alpha_1\right)\left(\frac{x-1}{2}-\alpha_2\right)\left(\frac{x-1}{2}-\alpha_3\right)$$

$$P\left(\frac{x-1}{2}\right) = \frac{1}{8}\left(x-(2\alpha_1+1)\right)\left(x-(2\alpha_2+1)\right)\left(x-(2\alpha_3+1)\right) = \frac{1}{8}(x-\beta_1)(x-\beta_2)(x-\beta_3)$$

$$\Rightarrow F(x) = (x-\beta_1)(x-\beta_2)(x-\beta_3) = 8P\left(\frac{x-1}{2}\right) =$$

$$= 8\cdot\left(\frac{x-1}{2}\right)^3 + 8\cdot 3\cdot\left(\frac{x-1}{2}\right)^2 - 8\cdot 7\cdot\left(\frac{x-1}{2}\right) + 8\cdot 5 = x^3-3x^2+3x-1+6(x^2-2x+1)$$

$$-28(x-1)+40 = \boxed{x^3+3x^2-37x+73}$$

Criteriul lui Eisenstein Fie $P(x) = a_0 + a_1X + \dots + a_{n-1}X^{n-1} + a_nX^n \in \mathbb{Z}[x]$ a.î. există p-prim în $\mathbb{Z}$ cu propr:

1) $p \mid a_0, \dots, p \mid a_{n-1}$
2) $p \nmid a_n$
3) $p^2 \nmid a_0$.

Atunci $P(x)$ este ireductibil în $\mathbb{Q}[x]$.

Aplicații ① $P(x) = 2x^{72} - 3x^{60} + 15x^{40} - 6x^5 + 9x^3 - 6x - 3$. $P(x)$ este ireductibil în $\mathbb{Q}[x]$. Luăm $p=3$ și

1) $3 \mid -3$, $3 \mid -6$, $3 \mid 9$, $3 \mid -6$, $3 \mid 15$, $3 \mid -3$, $3 \mid 0$ (0 e coef. puterilor lui x care nu apar)
2) $3 \nmid 2$
3) $3^2 \nmid -3$

$\Rightarrow$

$P(X)$ e ireductibil în $\mathbb{Q}[X]$ conform criteriului lui Eisenstein.

(2) Avem polinoame ireductibile de orice grad ≥ 1 în $\mathbb{Q}[X]$. #

Fie $P(X) = X^n - 2$ și aplic criteriul lui Eisenstein pentru nr. prim $p = 2$, obținând astfel că P e ireductibil în $\mathbb{Q}[X]$ $(\forall) n \geq 1$.

(3) Arătați că polinomul $P(X) = X^6 + X^5 + X^4 + X^3 + X^2 + X + 1$ este ireductibil în $\mathbb{Q}[X]$.

Afirm $P(X)$ e ireductibil $\Longleftrightarrow$ $P(X+a)$ ireductibil pt un $a \in \mathbb{Q}$ (oarecare)

$$P(X) = \frac{X^7 - 1}{X - 1} \qquad P(X+1) = \frac{(X+1)^7 - 1}{(X+1) - 1} = \frac{X^7 + C_7^1 X^6 + \ldots + C_7^1 X + \cancel{1} - \cancel{1}}{X} \Rightarrow$$

$$F(X) = P(X+1) = X^6 + C_7^1 X^5 + C_7^2 X^4 + \ldots + C_7^1.$$

$F(X)$ ired. aplicând criteriul lui Eisenstein pentru $p = 7$ $\left(7 \mid C_7^k \; (\forall) \, k = \overline{1,6} \right)$

Exc 4 Arătați că polinomul $X^{100}-125$ este ireductibil în $\mathbb{Q}[X]$.

Din S13 (clasa X) rădăcinile lui $X^{100}-125$ sunt $\alpha=\sqrt[100]{125}, \varepsilon\alpha, \dots, \varepsilon^{99}\alpha$, unde $\varepsilon=\cos\frac{2\pi}{100}+i\sin\frac{2\pi}{100}$ (toate răd. sunt $\neq$).

Nu pot aplica Eisenstein direct.

Pp abs. că $P(X)=X^{100}-125$ este reductibil în $\mathbb{Q}[X] \overset{\text{def pol. red.}}{\Longrightarrow} P(X)=F(X)\cdot G(X)$ cu $F(X), G(X)\in\mathbb{Q}[X]$ și $\text{grad}(F(X))<100$ și $\text{grad}(G(X))<100$

$P(X)=(X-\alpha)(X-\varepsilon\alpha)\cdot\ldots\cdot(X-\varepsilon^{99}\alpha)$ pol. ired $\neq$ în $\mathbb{C}[X]$

Din unicitatea descompunerii unui polinom în produs de pol. ired în $\mathbb{C}[X]$ $\Longrightarrow F(X)=(X-\varepsilon^{j_1}\alpha)\cdot\ldots\cdot(X-\varepsilon^{j_r}\alpha)$, unde

$\overset{(*)}{0<r}=\text{grad}(F)<100$ și $0\le j_1<\ldots<j_r\le 99$; Însă $F(X)\in\mathbb{Q}[X]$

$\overset{\text{Viète}}{\Longrightarrow} (\varepsilon^{j_1}\alpha)\cdot\ldots\cdot(\varepsilon^{j_r}\alpha)\in\mathbb{Q} \Rightarrow |\varepsilon^{j_1+\ldots+j_r}\cdot\alpha^r|\in\mathbb{Q} \Rightarrow$

$|\varepsilon|^{j_1+\ldots+j_r}\cdot|\alpha|^r$

$|\varepsilon|=1$

$\Rightarrow |\alpha|^r\in\mathbb{Q} \Rightarrow \sqrt[100]{5^{3r}}\in\mathbb{Q} \Rightarrow 100 \mid 3r \xrightarrow[(3,100)]{|\alpha|^r} 100 \mid r$ ↯ $(*)$

$\Rightarrow$ P este ireductibil în $\mathbb{Q}[X]$.