Seminarul 4 de Algebră II

Grupele 103 şi 104 - 2020-2021

1 Corpuri (cont.)

Exercițiul 1.1: Fie p prim și K un corp cu char $K = p$. Considerăm aplicația

$$\varphi : K \to K,\ \varphi(x) = x^p.$$

Atunci:

i) φ este morfism de corpuri.

ii) Dacă K este finit, φ este izomorfism de corpuri.

Exercițiul 1.2: Arătați că $K = \mathbb{Z}[i]/(3)$ este un corp cu 9 elemente și char $K = 3$.

Exercițiul 1.3: Fie $\mathbb{H}$ corpul cuaternionilor şi aplicaţiile

$$T : \mathbb{H} \to \mathbb{H},\ T(x) = x + \overline{x}$$
$$N : \mathbb{H} \to \mathbb{H},\ N(x) = x\overline{x}.$$

a) Calculaţi produsul $(1 + 2i - j + k)(2 - i + 3j + 2k)$.

b) Arătaţi că $T(x), N(x) \in \mathbb{R}$ şi $x^2 - T(x)x + N(x) = 0$ pentru orice $x \in \mathbb{H}$.

c) Calculaţi inversul lui $1 + 2i - j + k$ în $\mathbb{H}$.

d) Determinaţi centrul lui $\mathbb{H}$.

e) Rezolvaţi ecuaţia $x^2 = -1$ în $\mathbb{H}$.

2 Inele de polinoame

Exercițiul 2.1: Fie x un element nilpotent în inelul comutativ R.

a) Demonstraţi că rx este nilpotent, pentru orice $r \in R$.

b) Demonstraţi că $1 + x$ este inversabil.

c) Demonstraţi că $u + x$ este inversabil, pentru orice u inversabil în R.

Exercițiul 2.2: Fie R un inel comutativ şi $f = a_0 + a_1X + ... + a_nX^n \in R[X]$.

a) Demonstraţi că f este inversabil $\in R[X]$ dacă şi numai dacă a_0 este inversabil şi $a_1, ..., a_n$ sunt nilpotente în R.

b) Demonstraţi că f este nilpotent în $R[X]$ dacă şi numai dacă $a_0, a_1, ..., a_n$ sunt nilpotente în R.

c) Demonstraţi că f este divizor al lui zero în $R[X]$ dacă şi numai dacă există $a \in R$ nenul astfel încât $af = 0$.

d) Demonstraţi că f este idempotent în $R[X]$ dacă şi numai dacă a_0 este idempotent în R şi $a_1 = a_2 = \ldots = a_n = 0$.

Exercițiul 2.3: Determinaţi numărul polinoamelor de grad 2 din $\mathbb{Z}_{36}[X]$ care sunt:

a) inversabile;

b) nilpotente.

3 Temă

Exercițiul 3.1: Fie R un inel comutativ şi $f = \sum_{i\geq 0} a_i X^i \in R[[X]]$ (inelul de serii formale).

a) Demonstraţi că f este inversabil $\in R[[X]]$ dacă şi numai dacă a_0 este inversabil în R.

b) Demonstraţi că dacă f este nilpotent în $R[[X]]$, atunci a_i este nilpotent în R, $\forall i \geq 0$. Este adevărată şi reciproca?

c) Demonstraţi că f este idempotent în $R[[X]]$ dacă şi numai dacă a_0 este idempotent în R şi $a_i = 0, \ \forall i \geq 1$.

Temă

3 Inele de polinoame & Inelul factor (cont.)

Exercițiul 3.1: Folosind Teorema fundamentală de izomorfism, demonstrați că

a) $R[X]/_{(X-a)} \simeq R$ pentru R un inel comutativ şi $a \in R$;

b) $\mathbb{Z}[X]/_{(n)} \simeq \mathbb{Z}_n[X]$;

c) $\mathbb{Z}[X]/_{(X^2-2)} \simeq \mathbb{Z}[\sqrt{2}]$;

d) $\mathbb{Z}[X]/_{(X^2+1)} \simeq \mathbb{Z}[i]$;

e) $\mathbb{R}[X]/_{(X^2+1)} \simeq \mathbb{C}$;

f) $\mathbb{R}[X]/_{(X^2-1)} \simeq \mathbb{R} \times \mathbb{R}$;

g) $\mathbb{C}[X]/_{(X^2+1)} \simeq \mathbb{C} \times \mathbb{C}$.

Exercițiul 3.2: Calculați $\mathbb{Z}[X]/_{(2X-1)}$.

Exercițiul 3.3: Fie R un inel comutativ. Demonstrați că $R[X]$ nu este local.

Exercițiul 3.4:

a) Arătați că $\mathbb{Q}[X]/_{(X^2-1)} \simeq \mathbb{Q} \times \mathbb{Q}$.

b) Determinați idempotenții lui $\mathbb{Z}[X]/_{(X^2-1)}$.

c) Arătați că $\mathbb{Z}[X]/_{(X^2-1)}$ este canonic inclus strict în $\mathbb{Z} \times \mathbb{Z}$.

d) Arătați că $\mathbb{Z}[X]/_{(X^2-1)} \not\simeq \mathbb{Z} \times \mathbb{Z}$.

Exercițiul 3.5: (Teorema I de izomorfism) Folosiți Teorema Fundamentală de Izomorfism pentru a demonstra:

Fie R un inel și $I \subset J$ ideale ale lui R. Atunci

$$\frac{R/_I}{J/_I} \simeq R/_J.$$

Observația 3.6: Dacă $\varphi : R \to S$ este un izomorfism de inele, $I \trianglelefteq R, J \trianglelefteq S$ astfel încât $\varphi(I) = J$, atunci $R/_I \simeq S/_J$.

Exercițiul 3.7: Calculați:

a) $\mathbb{Z}[X]/_{(2,X)}$

b) $\mathbb{Z}[X]/_{(7,X-2)}$

c) $\mathbb{Z}[X]/_{(X+5, X-2)}$

d) $\mathbb{Z}[X]/_{(X^2+X+1)}$

e) $\mathbb{Z}[X]/_{(7, X^2+X+1)}$

f) $\mathbb{Z}[i]/_{(7+i)}$

g) $\mathbb{Z}[i]/_{(1+2i)}$

Exercițiul 3.8:

a) Pentru p, q prime, demonstraţi că $\mathbb{Z}[X]/_{(X^2-p)} \simeq \mathbb{Z}[X]/_{(X^2-q)}$ dacă şi numai dacă $p = q$.

b) Demonstraţi că $\mathbb{Z}[\sqrt{7}]/_{(6+\sqrt{7})}$ este un corp cu 29 elemente.

Exercițiul 3.9: Fie idealul $I = (3, X^3 - X^2 + 2X + 1) \trianglelefteq \mathbb{Z}[X]$. Arătaţi că I nu este ideal principal şi că $\mathbb{Z}[X]/_I$ nu este corp.

Polinoame

Seminar 5

Problema 1. Dacă α, β sunt rădăcinile polinomului $X^2 - 6X + 1 \in \mathbb{R}[X]$, atunci pentru orice $n \in \mathbb{N}$ avem că $\alpha^n + \beta^n \in \mathbb{Z}$ şi nu este divizibil cu 5.

Problema 2. Când este polinomul $X^{3m} + X^{3n+1} + X^{3p+2} \in \mathbb{Q}[X]$ divizibil cu $X^4 + X^2 + 1$?

Problema 3. Rezolvaţi în numere reale sistemul de ecuaţii

$$\begin{cases} x^5 + y^5 = 33 \\ x + y = 3 \end{cases}$$

$\Rightarrow \begin{cases} u + v = 5 \\ u^4 + v^4 = 97 \end{cases}$

Problema 4. Rezolvaţi în numere reale ecuaţia $\underbrace{\sqrt[4]{97 - x}}_{u} + \underbrace{\sqrt[4]{x}}_{v} = 5$.

Problema 5. Fie a, b două rădăcini ale polinomului $X^4 + X^3 - 1$. Demonstraţi că ab este o rădăcină a polinomului $X^6 + X^4 + X^3 - X^2 - 1$.

Problema 6. Fie a, b, c numere reale nenule astfel încât $a + b + c \neq 0$ şi

$$\frac{1}{a} + \frac{1}{b} + \frac{1}{c} = \frac{1}{a+b+c}.$$

$\Rightarrow S_1 S_2 = S_3$ se află răd. $\begin{cases} \text{una } \mathbb{R} \\ \pm i \end{cases}$

Demonstraţi că pentru orice număr întreg impar n

$$\frac{1}{a^n} + \frac{1}{b^n} + \frac{1}{c^n} = \frac{1}{a^n + b^n + c^n}.$$

Tip examen

Problema 7. Fie polinomul $P(X) = X^3 - 4X^2 + X + 1 \in \mathbb{R}[X]$ care are rădăcinile complexe $\alpha_1, \alpha_2, \alpha_3$. Scrieţi polinomul monic care are rădăcinile:

(1) $2\alpha_1 - 3, 2\alpha_2 - 3, 2\alpha_3 - 3$;
(2) $\frac{1}{\alpha_1}, \frac{1}{\alpha_2}, \frac{1}{\alpha_3}$;
(3) $\alpha_1^2 + 2, \alpha_2^2 + 2, \alpha_3^2 + 2$.

Engel

Problema 8. Fie $P(X)$ un polinom cu coeficienţi ~~întregi~~ naționali de grad n astfel încât $P(k) = \frac{k}{k+1}$ pentru $k = 0, ..., n$. Calculaţi $P(n+1)$.

Problema 9. Date $2n$ numere distincte două câte două $a_1, \ldots, a_n, b_1, \ldots, b_n$, umplem o matrice $n \times n$ astfel: pe poziţia (i, j) în matrice punem numărul $a_i + b_j$. Demonstraţi că dacă produsul elementelor de pe fiecare coloană este constant, atunci şi produsul elementelor de pe fiecare linie este constant.

Problema 10. Scrieţi ca polinom de polinoamele simetrice fundamentale următoarele polinoame:

(1) $P(X_1, X_2, X_3) = (X_1 - X_2)^2 (X_2 - X_3)^2 (X_3 - X_1)^2 \in \mathbb{Q}[X_1, X_2, X_3]$;

(2) $F(X_1, X_2, X_3) = X_1^4X_2 + X_1^4X_3 + X_2^4X_1 + X_2^4X_3 + X_3^4X_1 + X_3^4X_2 \in \mathbb{Q}[X_1, X_2, X_3]$;

(3) $G(X_1, X_2, X_3, X_4) = (X_1 + X_2 - X_3 - X_4)(X_1 + X_3 - X_2 - X_4)(X_1 + X_4 - X_2 - X_3)$.

Problema 11. a) Dacă $x, y, z \in \mathbb{C}$ sunt astfel încât $x + y + z = 1$, $x^2 + y^2 + z^2 = 2$ (3) şi $x^3 + y^3 + z^3 = 3$ (5), determinaţi valoarea lui $x^4 + y^4 + z^4$. $=7$, dar $x^5+y^5+z^5 \neq 9$.

b) Demonstraţi că numerele x, y, z care satisfac condiţiile anterioare nu sunt raţionale dar că $x^n + y^n + z^n \in \mathbb{Q}$ pentru orice număr natural n.

Problema 12*. Fie p un număr prim. Demonstraţi că $\mathbb{Z}[i]/(p)$ este un inel cu p^2 elemente şi este corp dacă şi numai dacă $p \equiv 3 \pmod 4$, eventual urmând paşii:

(1) Demonstraţi că are loc izomorfismul de inele $\mathbb{Z}[i]/(p) \cong \mathbb{Z}_p[X]/(X^2 + \hat{1})$.

(2) Demonstraţi că $\mathbb{Z}[i]/(p)$ este corp dacă şi numai dacă ecuaţia $x^2 \equiv -1 \pmod p$ nu are soluţii.

(3) Demonstraţi că, dacă $p = 2$, ecuaţia $x^2 \equiv -1 \pmod p$ are soluţii.

(4) Demonstraţi, eventual folosind Teorema lui Wilson, că, dacă $p \equiv 1 \pmod 4$, ecuaţia $x^2 \equiv -1 \pmod p$ are soluţii.

(5) Demonstraţi, eventual folosind Teorema lui Fermat, că, dacă există x cu $x^2 \equiv -1 \pmod p$ atunci $p \equiv 1 \pmod 4$.

(6) Concluzionaţi.

Putnam

Problema 13*. Fie $n \geq 3$ un număr întreg. Fie $f(X)$ şi $g(X)$ polinoame cu coeficienţi reali astfel încât punctele $(f(1), g(1))$, $(f(2), g(2)), \ldots, (f(n), g(n))$ în $\mathbb{R}^2$ sunt vârfurile unui poligon regulat cu n laturi, aşezate în ordine inversă acelor de ceasornic. Demonstraţi că cel puţin unul dintre polinoamele $f(X)$ şi $g(X)$ are gradul mai mare sau egal cu $n - 1$.

Problema 14*. Fie a, b, c numere întregi care sunt laturile unui triunghi. Demonstraţi că dacă ecuaţia

$$x^2 + (a + 1)x + b - c = 0$$

are rădăcini întregi atunci triunghiul este isoscel.

Problema 15*. Fie $f(X) \in \mathbb{Z}[X]$ un polinom şi $n \geq 3$. Demonstraţi că nu există numerele întregi distincte două câte două $a_1, \ldots, a_n$ astfel încât $f(a_1) = a_2$, $f(a_2) = a_3, \ldots, f(a_{n-1}) = a_n$, $f(a_n) = a_1$. (Indicaţie: este generalizarea unei probleme făcute în seminarul 4)

Problema 16*. Fie $f_1, f_2, \ldots, f_k$ polinoame neconstante cu coeficienţi întregi. Demonstraţi că pentru o infinitate de numere naturale n toate numerele $f_1(n), \ldots, f_k(n)$ sunt compuse. (Indicaţie: $a - b | f(a) - f(b)$ pentru $a \neq b \in \mathbb{Z}$ şi $f(X) \in \mathbb{Z}[X]$)

Problema 17*. Fie $f(X) \in \mathbb{Z}[X]$ un polinom de grad $n \geq 2$. Demonstraţi că polinomul $f(f(X)) - X$ are cel mult n rădăcini întregi. (Indicaţie: folosiţi problema anterioară.)

Problema 18*. Fie $P(X)$ un polinom de grad $n > 1$ cu coeficienţi întregi şi k un număr natural nenul. Considerăm polinomul $Q(X) = \underbrace{P(P(...(P}_{k \text{ ori}}(X)...)))$. Demonstraţi că există cel mult n întregi astfel încât $Q(t) = t$. (Indicaţie: folosiţi problema anterioară.)

IMO

Polinoame

Seminar 8

Problema 1. Fie a, b, c numere reale astfel încât $a + b + c = 0$. Demonstraţi că:

$$\frac{a^5 + b^5 + c^5}{5} = \left(\frac{a^3 + b^3 + c^3}{3}\right)\left(\frac{a^2 + b^2 + c^2}{2}\right).$$

Problema 2. Demonstraţi că pentru numerele naturale nenule $m, n \in \mathbb{N}^*$ avem $(X^m - 1, X^n - 1) = X^{(m,n)} - 1$. În particular, $(2^n - 1, 2^m - 1) = 2^{(n,m)} - 1$.

Problema 3. Fie p un număr prim şi considerăm polinomul $F(X) = X^{p-1} + \cdots + X + 1$. Calculaţi restul împărţirii polinomului $F(X^p)$ la $F(X)$.

Putnam 2015 **Problema 4.** Determinaţi toate numerele naturale nenule $n < 10^{100}$ pentru care simultan n divide 2^n, $n - 1$ divide $2^n - 1$ şi $n - 2$ divide $2^n - 2$.

Problema 5. Calculaţi $(X^{23} + \cdots + X + 1, X^{53} + \cdots + X + 1)$.

Problema 6. Fie m, n numere naturale nenule relativ prime şi $a > 1$ un număr real astfel încât $a^m + \frac{1}{a^m}$ şi $a^n + \frac{1}{a^n}$ sunt întregi. Demonstraţi că $a + \frac{1}{a}$ este de asemenea un întreg.

Problema 7. Determinaţi toate polinoamele $P(X) \in \mathbb{R}[X]$ astfel încât $P(0) = 0$ şi $P(x^2 + 1) = P(x)^2 + 1$ pentru orice $x \in \mathbb{R}$.

Problema 8. Există un polinom nenul $f(X) \in \mathbb{C}[X]$ astfel încât $Xf(X-1) = (X+1)f(X)$?

Problema 9. Determinaţi toate polinoamele $P(X) \in \mathbb{C}[X]$ astfel încât $XP(X - 1) = (X - 5)P(X)$.

Problema 10. Arătaţi că polinomul $P(X) = (1 + X + \cdots + X^n)^2 - X^n \in \mathbb{Q}[X]$ este reductibil, unde $n \geq 2$ este un număr natural.

Problema 11. Fie f un polinom neconstant având coeficienţii numerele naturale nenule. Demonstraţi că dacă n este un număr natural, atunci $f(n)$ divide $f(f(n) + 1)$ dacă şi numai dacă $n = 1$.

Problema 12*. Fie a, b două numere raţionale pozitive astfel încât pentru un $n \geq 2$ numărul $\sqrt[n]{a} + \sqrt[n]{b}$ este raţional. Demonstraţi că $\sqrt[n]{a}$, $\sqrt[n]{b}$ sunt de asemenea raţionale.

Problema 13*. Există un şir infinit de numere reale nenule $a_0, a_1, a_2, \ldots$ astfel încât pentru orice $n = 1, 2, 3, \ldots$ polinomul

$$p_n(X) = a_0 + a_1 X + a_2 X^2 + \ldots + a_n X^n$$

are exact n rădăcini reale distincte?

Problema 14*. Fie $f(X) \in \mathbb{Q}[X]$ un polinom de grad n. Atunci $f(n) \in \mathbb{Z}$ pentru orice $n \in \mathbb{Z}$ dacă şi numai dacă există numerele întregi $a_0, a_1, \ldots, a_n$ astfel încât

$$f(X) = a_0 + a_1 X + a_2 \frac{X(X-1)}{2!} + \cdots + a_n \frac{X(X-1)\cdots(X-n+1)}{n!}.$$

Polinoame

Seminariile 9 şi 10

Problema 1. Testaţi dacă următoarele polinoame sunt ireductibile în $\mathbb{Q}[X]$:

(i) $3X^2 - 7X - 1$; i

(ii) $6X^3 - 3X - 18$; $= 3(2x^3 - x - 6)$; i $-3x + 2x$

(iii) $X^3 - 7X + 1$; i

(iv) $X^3 - 9X - 9$. i

Problema 2. Determinaţi toate polinoamele ireductibile de grad ≤ 5 din $\mathbb{Z}_2[X]$.

Problema 3. Demonstraţi folosind criteriul lui Eisenstein că următoarele polinoame sunt ireductibile (pentru fiecare din ele este precizat inelul unde este ireductibil):

(1) $P(X) = X^{12} + 2X^5 + 4X^3 + 14X + 6$ în $\mathbb{Q}[X]$; ✓

(2) $P(X) = X^n - 2$ în $\mathbb{Q}[X]$; ✓

(3) $f(X) = X^{p-1} + X^{p-2} + \ldots + X + 1$, unde p este un număr natural prim, este ireductibil în $\mathbb{Q}[X]$;

(4)* $P(X, Y, Z) = X^2 - YZ$ în $\mathbb{R}[X, Y, Z]$;

(5)* $P(X, Y) = X^2 + Y^2 - 1$ în $\mathbb{R}[X, Y]$;

(6) $P(X) = X^{2^n} + 1$ în $\mathbb{Q}[X]$. $X^{p^n} + p - 1$

Problema 4. Să se arate că $\mathbb{Z}_2[X]/(X^3 + X + \hat{1})$ şi $\mathbb{Z}_2[X]/(X^3 + X^2 + \hat{1})$ sunt corpuri izomorfe.

Problema 5. Fie F un corp. Arătaţi că dacă $a_0 + a_1X + \ldots + a_nX^n \in F[X]$ este ireductibil, atunci la fel este şi $a_n + a_{n-1}X + \ldots + a_0X^n$.

Problema 6. Fie $f(X) = X^2 - 3$, $g(X) = X^2 - 2X - 2$, $f, g \in \mathbb{Q}[X]$. Să se arate că f şi g sunt ireductibile peste $\mathbb{Q}$ şi are loc următorul izomorfism de inele $\mathbb{Q}[X]/(f(X)) \cong \mathbb{Q}[X]/(g(X))$.

Problema 7. Descompuneţi $X^n - 1$, $1 \leq n \leq 8$, în produs de polinoame ireductibile în $\mathbb{Q}[X], \mathbb{R}[X], \mathbb{C}[X], \mathbb{Z}_2[X]$.

Problema 8. Fie $L := \mathbb{Z}_2[X]/(X^3 + X + \hat{1})$ şi $f(X) = X^4 + X^2 + \hat{1} \in \mathbb{Z}_2[X]$. Să se arate că L este corp şi să se studieze ireductibilitatea lui f în $L[X]$.

Problema 9. Fie K un corp, $f \in K[X]$ un polinom neconstant şi $a, b \in K$, $a \neq 0$. Arătaţi că f este ireductibil în $K[X]$ dacă şi numai dacă $f(aX + b)$ este ireductibil în $K[X]$.

Problema 10. Arătaţi că polinomul $P(X) = X^{105} - 9$ este ireductibil în $\mathbb{Q}[X]$.

Problema 11. Demonstraţi că polinomul $P(X) = X^{101} + 101X^{100} + 102$ este ireductibil în $\mathbb{Q}[X]$.

Problema 12. Dacă $a_1, \ldots, a_n \in \mathbb{Z}$ sunt distincte două câte două atunci polinomul $f(X) = (X - a_1)(X - a_2)\cdots(X - a_n) - 1$ este ireductibil în $\mathbb{Q}[X]$.

Problema 13. Dacă $a_1, \ldots, a_n \in \mathbb{Z}$ sunt distincte două câte două atunci polinomul $f(X) = (X - a_1)^2(X - a_2)^2\cdots(X - a_n)^2 + 1$ este ireductibil în $\mathbb{Q}[X]$.

Problema 14. Fie p un număr prim natural. Demonstraţi că polinomul

$$P(X) = X^{p-1} + 2X^{p-2} + 3X^{p-3} + \ldots + (p-1)X + p$$

este ireductibil în $\mathbb{Q}[X]$.

Problema 15*. Demonstraţi că polinomul $f(X) = X^4 - 10X^2 + 1$ este ireductibil în $\mathbb{Q}[X]$, dar este reductibil în $\mathbb{Z}_p[X]$ pentru orice număr prim p.

Problema 16*. Să se arate că polinoamele $f(X,Y) = X^2 - Y^3$, respectiv $g(X,Y) = Y^2 - X^2 - X^3$ sunt ireductibile în $\mathbb{R}[X,Y]$.

Problema 17*. Să se arate că polinomul $f(T) = T^3 - X^3 \in \mathbb{Z}_5(X^5)[T]$ este ireductibil peste corpul $\mathbb{Z}_5(X^5)$.

Problema 18*. Polinomul $X^p - X + a \in \mathbb{Z}[X]$, unde p este număr prim astfel încât $(p, a) = 1$ este ireductibil în $\mathbb{Q}[X]$.

MO: 1993 → **Problema 19*.** Fie $n > 1$ un număr natural şi $f(X) = X^n + 5X^{n-1} + 3$. Demonstraţi că $f(X)$ este ireductibil în $\mathbb{Q}[X]$.

Problema 20*. (Criteriul de ireductibilitate al lui Cohn) Fie $b \geq 2$ şi p un număr prim. Scriem p în baza b, i.e. $p = a_nb^n + \ldots + a_1b + a_0$ cu $0 \leq a_i \leq b - 1$. Atunci polinomul $f(X) = a_nX^n + a_{n-1}X^{n-1} + \ldots + a_1X + a_0$ este ireductibil în $\mathbb{Q}[X]$.

2 Criterii de ireductibilitate pentru polinoame

Propoziția 2.1: *Fie R un domeniu şi $f \in R[X]$, $\deg f \geq 2$. Dacă f are o rădăcină în R, atunci este reductibil în $R[X]$.*

Propoziția 2.2: *Fie R un domeniu şi $f \in R[X]$ monic. Dacă $\deg f = 2$ sau 3, atunci f este ireductibil în $R[X]$ dacă şi numai dacă nu are rădăcini în R.*

Propoziția 2.3: *Fie $f = a_n X^n + ... + a_1 X + a_0 \in \mathbb{Z}[X]$. Dacă $\frac{r}{s} \in \mathbb{Q}$ este o rădăcină a lui f cu $(r,s) = 1$, atunci $r \mid a_0$ şi $s \mid a_n$.*

Propoziția 2.4: ("Schimbare de variabile") *Fie K un corp comutativ şi $a, b \in K, a \neq 0$. Atunci $f(X) \in K[X]$ este ireductibil dacă şi numai dacă $f(aX+b) \in K[X]$ este ireductibil.*

Propoziția 2.5: *Fie K un corp comutativ. Atunci $a_0 + a_1 X + ... + a_n X^n \in K[X]$ este ireductibil dacă şi numai dacă $a_n + a_{n-1} + ... + a_1 X + a_0 \in K[X]$ este ireductibil.*

Teorema 2.6: (Lema lui Gauss pentru $\mathbb{Z}$) *Fie $f \in \mathbb{Z}[X]$. Presupunem că cel mai mare divizor comun al coeficienţilor lui f este 1.*

Atunci f este ireductibil în $\mathbb{Z}[X] \iff f$ este ireductibil în $\mathbb{Q}[X]$.

Teorema 2.7: (Lema lui Gauss) *Fie R inel factorial şi $f \in R[X]$. Presupunem că cel mai mare divizor comun al coeficienţilor lui f este 1.*

Atunci f este ireductibil în $R[X] \iff f$ este ireductibil în $Q(R)[X]$.

Propoziția 2.8: (Criteriul lui Eisenstein) *Fie p prim şi $f = X^n + a_{n-1}X^{n-1} + ... + a_1 X + a_0 \in \mathbb{Z}[X]$, $n \geq 1$. Presupunem că $p \mid a_k$ pentru orice $0 \leq k \leq n-1$ şi $p^2 \nmid a_0$. Atunci f este ireductibil în $\mathbb{Q}[X] \iff$ ireductibil în $\mathbb{Z}[X]$.*

Propoziția 2.9: (Criteriul lui Eisenstein (variantă)) *Fie p prim şi $f = a_n X^n + a_{n-1}X^{n-1} + ... + a_1 X + a_0 \in \mathbb{Z}[X]$, $n \geq 1$. Presupunem că $p \nmid a_n$, $p \mid a_k$ pentru orice $0 \leq k \leq n-1$ şi $p^2 \nmid a_0$. Atunci f este ireductibil în $\mathbb{Q}[X]$.*

Propoziția 2.10: (Criteriul lui Eisenstein, limbaj de ideale prime)

a) Fie R un domeniu şi $f = X^n + a_{n-1}X^{n-1} + ... + a_1 X + a_0 \in R[X]$ un polinom **monic**.

Presupunem că există $P \trianglelefteq R$ un ideal prim astfel încât $a_k \in P$ pentru orice $0 \leq k \leq n-1$ dar $a_0 \notin P^2$. Atunci f este ireductibil în $R[X]$.

b) Fie R un inel factorial şi $f = a_n X^n + a_{n-1}X^{n-1} + ... + a_1 X + a_0 \in R[X]$.

Presupunem că există $P \trianglelefteq R$ un ideal prim astfel încât $a_n \notin P$, $a_k \in P$ pentru orice $0 \leq k \leq n-1$ dar $a_0 \notin P^2$. Atunci f este ireductibil în $Q(R)[X]$.

Propoziția 2.11: (Criteriul reducerii) *Fie R un domeniu şi $I \trianglelefteq R, I \neq R$. Dacă $f \in R[X]$* **monic** *este ireductibil în $\left({R}/{I}\right)[X]$, atunci este ireductibil în $R[X]$.*

Teorema 2.12: (Criteriul lui Cohn) *Fie $b \in \mathbb{N}, b \geq 2$ şi $p \in \mathbb{N}$ prim a cărui scriere în baza b este*

$$p = a_0 + a_1 b + a_2 b^2 + ... + a_n b^n,\ 0 \leq a_i < b.$$

Atunci polinomul $a_0 + a_1 X + a_2 X^2 + ... + a_n X^n \in \mathbb{Z}[X]$ este ireductibil (în $\mathbb{Z}[X]$ şi $\mathbb{Q}[X]$).

(S9-10)

Seminar 9-10.

① Fie K un corp comutativ și $n\in\mathbb{N}^*$. Dacă $f\in K[X_1,\dots,X_n]$, definim funcția polinomială $\tilde{f}$ asociată lui f astfel $\tilde{f}:K^n\to K$, $\tilde{f}(a_1,\dots,a_n)=f(a_1,\dots,a_n)$ pt. orice $a_1,\dots,a_n\in K$ [unde $f(a_1,\dots,a_n)$ este evaluarea lui f în $a_1,\dots,a_n$; altfel spus, dacă $\varphi:K[X_1,\dots,X_n]\to K$ este unicul morfism de inele pt. care $\varphi(\alpha)=\alpha$ pt. orice $\alpha\in K$, iar $\varphi(X_1)=a_1,\dots,\varphi(X_n)=a_n$ (existența lui φ rezultă din proprietatea de universalitate a inelelor de polinoame) atunci $f(a_1,\dots,a_n)$ este chiar $\varphi(f)$].

Să se arate că dacă K este infinit și $f,g\in K[X_1,\dots,X_n]$ pentru care $\tilde{f}=\tilde{g}$, atunci $f=g$.
Rămâne afirmația adevărată pt. K finit?

② Să se determine c.m.m.d.c al numerelor întregi 625873 și 540053 și să se scrie acesta ca o combinație liniară a celor două numere.

③ Fie $m,n\in\mathbb{N}^*$. Să se arate că $(2^m-1,2^n-1)=2^{(m,n)}-1$.

④ Fie $n\in\mathbb{N}^*$. Să se arate că $(n!+1,(n+1)!+1)=1$.

⑤ Fie $a,b\in\mathbb{Z}\setminus\{0\}$ și $d=(a,b)$. Fie $c\in\mathbb{Z}$. Să se arate că ecuația $ax+by=c$ are soluții $x,y\in\mathbb{Z}$ dacă și numai dacă $d\mid c$. În acest caz, cum se determină toate soluțiile ecuației?

S 9-10

(a)

(6) Să se rezolve ecuația $4x + 14y = 6$, unde $x, y \in \mathbb{Z}$.

(7) Fie $m, n \in \mathbb{N}^*$ cu m impar. Să se arate că $(2^m - 1, 2^n + 1) = 1$.

(8) Fie $F_n = 2^{2^n} + 1$ pentru $n \geq 0$. Să se arate că $F_0 \cdot F_1 \cdot \ldots \cdot F_{n-1} = F_n - 2$ pentru orice $n \in \mathbb{N}^*$. Deduceți că $(F_n, F_m) = 1$ pentru orice $n \neq m$.

(9) Fie $f = X^4 + 3X^3 + 2X^2 + X - 1$, $g = X^4 + 3X^2 + 2X + 3 \in \mathbb{Q}[X]$. Să se determine c.m.m.d.c și c.m.m.m.c al lui f și g în $\mathbb{Q}[X]$ și să se scrie (f, g) ca o combinație liniară de f și g cu coeficienți în $\mathbb{Q}[X]$.

(10) Să se determine c.m.m.d.c al polinoamelor $f = X^4 - 4X^3 + 1$ și $g = X^3 - 3X^2 + 1$ în $\mathbb{R}[X]$.

(11) Să se determine suma și intersecția idealelor $(X^3 + 1)$ și $(X^5 + 1)$ în $\mathbb{R}[X]$.

(12) Fie K un corp comutativ și $m, n \in \mathbb{N}^*$. Să se arate că $(X^m - 1, X^n - 1) = X^{(m,n)} - 1$ în $K[X]$.

(S 9-10) (5)

(13) Fie $f = X^{23} + X^{22} + \dots + X + 1$, $g = X^{15} + X^{14} + \dots + X + 1 \in \mathbb{Q}[X]$.

Să se calculeze (f, g).

(14) Care dintre polinoamele

$X^2 + X + \hat{1}$, $X^3 + X + \hat{1}$, $X^4 + X^2 + X + \hat{1}$, $X^4 + X^2 + \hat{1}$, $X^4 + X^3 + X^2 + X + \hat{1}$

din $\mathbb{Z}_2[X]$ sunt ireductibile?

(15) Să se determine toate polinoamele ireductibile de grad ≤ 4 din $\mathbb{Z}_2[X]$.

(16) Să se scrie ca produs de polinoame ireductibile în $\mathbb{Z}_2[X]$ fiecare dintre polinoamele:

(a) $X^5 + X^3 + \hat{1}$

(b) $X^6 + X^4 + X + \hat{1}$

(c) $X^{15} + \hat{1}$.

(17) Este $X^4 + \hat{1}$ ireductibil în $\mathbb{Z}_3[X]$?

Seminarul 10+ de Algebră II

Grupa 101 - 2023-2024

Exercițiul 1: Demonstraţi că $X^3 + nX + 2$ este ireductibil peste $\mathbb{Q}$ pentru toţi $n \in \mathbb{Z}, n \neq 1, -3, -5$.

Exercițiul 2: Fie $f(X) \in \mathbb{Z}[X]$ şi $m \in \mathbb{Z}, n \in \mathbb{N}$. Demonstraţi că dacă niciunul dintre $f(m), f(m+1), ..., f(m+n)$ nu se divide cu $n+1$, atunci $f(X)$ nu are rădăcini întregi.

lucrăm în $\mathbb{Z}_{n+1}$

Exercițiul 3:

duce $\mathbb{Z}$ în $\mathbb{Z}$.

a) Pentru p, q prime, demonstraţi că $\mathbb{Z}[X]/_{(X^2-p)} \simeq \mathbb{Z}[X]/_{(X^2-q)}$ dacă şi numai dacă $p = q$.

are răd. p $\qquad$ n

b) Demonstraţi că $\mathbb{Z}[\sqrt{7}]/_{(6+\sqrt{7})}$ este un corp cu 29 elemente.

c) Este inelul $\mathbb{Z}[i\sqrt{19}]/_{(4+i\sqrt{19})}$ un corp?

Exercițiul 4:

a) Fie K un corp cu char $K \neq 2$ și $A \subset K[X,Y]$ subinelul polinoamelor simetrice din $K[X,Y]$. Demonstrați că
$$A/_{(X^2+Y^2)} \simeq K[X].$$

b) Demonstrați că
$$\mathbb{C}[X,Y]/_{(X^2+Y^2)} \not\simeq \mathbb{C}[X].$$

c) Demonstrați că
$$\mathbb{R}[X,Y]/_{(X^2+Y^2)} \not\simeq \mathbb{R}[X].$$

Exercițiul 5: Demonstrați că $K[X,Y]/_{(Y^2-X)}$ și $K[X,Y]/_{(Y^2-X^2)}$ nu sunt izomorfe, pentru orice corp K.

Exercițiul 6: Fie K un corp, $f \in K[X]$ un polinom neconstant şi $a, b \in K, a \neq 0$. Arătaţi că f este ireductibil în $K[X]$ dacă şi numai dacă $f(aX+b)$ este ireductibil în $K[X]$.

Exercițiul 7: Folosiţi criteriul lui Eisensten pentru a demonstra că următoarele polinoame sunt ireductibile:

a) $X^{12} + 2X^5 + 4X^3 + 14X + 6 \in \mathbb{Q}[X]$;

b) $X^n - 2 \in \mathbb{Q}[X]$;

c) $X^4 + 4X^3 + 6X^2 + 2X + 1 \in \mathbb{Q}[X]$.

Exercițiul 8: Demonstrați că $X^{n-1} + X^{n-2} + ... + X + 1$ este ireductibil peste $\mathbb{Q}$ dacă și numai dacă n este prim.

Exercițiul 9: Spunem că un polinom cu coeficienți întregi $f(X)$ este *Eisenstein modulo p*, unde p este un număr prim, dacă există $a \in \mathbb{Z}$ astfel încât $f(X+a)$ este ireductibil conform criteriului lui Eisenstein aplicat numărului prim p.

Determinați toate numerele prime p pentru care $f(X) = X^3 + 63$ este *Eisenstein modulo p*. În plus, pentru fiecare astfel de p precizați și un $a \in \mathbb{Z}$ ca mai sus.

Exercițiul 10: Demonstrați că polinomul $f(X) = X^{101} + 101X^{100} + 102$ este ireductibil în $\mathbb{Q}[X]$.

Exercițiul 11: Demonstrați că $P(X) = X^{105} - 9$ este ireductibil în $\mathbb{Q}[X]$.

Exercițiul 12: Fie p prim și $n \in \mathbb{N}$. Arătați că $f(X) = X^{p^n} + p - 1$ este ireductibil în $\mathbb{Q}[X]$.

Exercițiul 13: Fie p un număr prim și $F(X) = X^{p-1} + ... + X + 1 \in \mathbb{Q}[X]$. Calculați restul împărțirii lui $F(X^p)$ la $F(X)$.

Exercițiul 14: Arătați că $P(X) = (1 + X + ... + X^n)^2 - X^n \in \mathbb{Q}[X]$ este reductibil pentru orice $n \geq 2$.

Exercițiul 15: Fie $a_1, ..., a_n \in \mathbb{Z}$ distincte. Demonstrați că

$$f(X) = (X - a_1)(X - a_2)...(X - a_n) - 1$$

este ireductibil în $\mathbb{Q}[X]$.

Exercițiul 16: Determinați $n \geq 1$ pentru care

$$f(X) = (X - 1)(X - 2)...(X - n) + 1$$

este ireductibil în $\mathbb{Q}[X]$.

Exercițiul 17: Fie $a_1, ..., a_n \in \mathbb{Z}$ distincte. Demonstrați că

$$f(X) = (X - a_1)^2(X - a_2)^2...(X - a_n)^2 + 1$$

este ireductibil în $\mathbb{Q}[X]$.

Exercițiul 18: Fie $f(X) \in \mathbb{Z}[X]$, $\deg f > 1$, monic. Demonstrați că există un polinom $g(X) \in \mathbb{Z}[X]$ astfel încât $f(g(X))$ este polinom reductibil.

$f(x) \mid f(g(x))$
$g(x) = f(x) + x$

Exercițiul 19: Demonstrați că:

a) $(X^2 - 2) \in \mathrm{Max}(\mathbb{Q}[X])$;

b) $(X^n - 2) \in \mathrm{Max}(\mathbb{Q}[X])$;

c) $(4, X) \notin \mathrm{Max}(\mathbb{Z}[X])$;

d) $(2 + i) \in \mathrm{Max}(\mathbb{Z}[i])$;

e) $(2, X^4 + X^3 + 1) \in \mathrm{Max}(\mathbb{Z}[X])$;

Exercițiul 20: Decideți dacă următoarele ideale sunt maximale în $\mathbb{Z}[X]$:

a) $(5, X^3 + 2X^2 + 4X + 3)$;

b) $(7, X^4 + X^2 + 2)$.

Exercițiul 21: Fie K corp şi $f \in K[X]$. Descrieţi idealele inelului $K[X]/_{(f)}$.

Exercițiul 22: Determinați toate idealele inelului $\mathbb{Z}[X]/_{(2, X^3+1)}$. Precizaţi care dintre ele sunt maximale.

Exercițiul 23:

a) Calculaţi numărul de ideale maximale ale lui $\mathbb{Z}[X]$ care conţin idealul $(13, X^{507} + 54X^{338} + 62)$.

b) Calculaţi numărul de polinoame monice ireductibile din $\mathbb{R}[X]$ care îl divid pe $X^{44} + 3X^{22} + 3$.

Exercițiul 24: Fie R un domeniu şi $I \trianglelefteq R, I \neq R$. Dacă $f \in R[X]$ **monic** este ireductibil în $\left(R/_I\right)[X]$, atunci este ireductibil în $R[X]$.

Exercițiul 25: Demonstraţi că următoarele polinoame sunt ireductibile:

a) $X^5 + 9X^2 + 4X + 7 \in \mathbb{Z}[X]$;

b) $X^4 - 3X^3 + 6X^2 - 2X + 1 \in \mathbb{Z}[X]$;

c) $X^2 + XY + 1 \in \mathbb{Z}[X, Y]$.

Exercițiul 26: Fie p prim. Arătaţi că:

a) Mulțimea $\mathbb{Z}_p \setminus \{\hat{0}\}$ este grup cu înmulțirea din $\mathbb{Z}_p$. Deduceți că $a^{p-1} = \hat{1}$ pentru orice $a \in \mathbb{Z}_p \setminus \{\hat{0}\}$.

b) Polinomul $f = X^{p-1} - \hat{1} \in \mathbb{Z}_p[X]$ are rădăcinile simple $\hat{1}, ...\widehat{p-1}$.

c) Folosind relațiile lui Viète, deduceți Teorema lui Wilson:

$$(p-1)! \equiv -1 (\text{mod } p).$$

d) Deduceţi că -1 este rest pătratic modulo $p \iff p = 2$ sau $p \equiv 1 \pmod 4$.

Exercițiul 27*: Demonstraţi că polinomul $X^4 + 1$ este ireductibil în $\mathbb{Q}[X]$, dar reductibil în $\mathbb{Z}_p[X]$ pentru orice p prim.

Exercițiul 28: Fie $R = \{f \in \mathbb{R}[X] \mid f(0) \in \mathbb{Q}\}$ şi $I = \{f \in R \mid f(0) = 0\}$. Demonstraţi că R este inel şi că I este ideal al lui R care nu este finit generat.

Exercițiul 29: Arătaţi că $\mathbb{Z}_2[X]/_{(X^3 + X + \hat{1})}$ şi $\mathbb{Z}_2[X]/_{(X^3 + X^2 + \hat{1})}$ sunt corpuri izomorfe.

Exercițiul 30: Construiți un corp cu:

a) 8 elemente;

b) 9 elemente;

c) 125 de elemente.

Exercițiul 31: Fie p un număr prim și $f = X^p - X + \hat{1} \in \mathbb{Z}_p[X]$.

a) Arătați că f nu are rădăcini în $\mathbb{Z}_p$.

b) Arătați că, dacă f are o rădăcină într-un corp L, $\mathbb{Z}_p \subset L$, atunci f are toate rădăcinile în L.

c) Arătați că f este ireductibil în $\mathbb{Z}_p[X]$.

Exercițiul 32: Fie $n > 1$ natural. Demonstraţi că polinomul $X^n + 5X^{n-1} + 3$ este ireductibil în $\mathbb{Q}[X]$.

Exercițiul 33*: Fie $A = \{f \in \mathbb{Q}[X] \mid f \text{ nu are termen de grad } 1\}$. Demonstrați că A este subinel unitar al lui $\mathbb{Q}[X]$ și

$$\mathbb{Q}[X,Y]\big/(X^3 - Y^2) \simeq A.$$

Exercițiul 34: Fie $R = \{f : [0,1] \to \mathbb{R} \mid f \text{ continuă}\}$. Pentru orice $c \in [0,1]$, fie

$$\mathfrak{m}_c = \{f \in R \mid f(c) = 0\}.$$

Demonstrați că $\mathfrak{m}_c$ este ideal maximal al lui R.

Exercițiul 35*: Fie $R = \{f : [0,1] \to \mathbb{R} \mid f \text{ continuă}\}$.

a) Demonstrați că, folosind notațiile din exercițiul precedent, *orice* ideal maximal al lui R este de tipul $\mathfrak{m}_c$, pentru un $c \in [0,1]$.

b) Demonstrați că, dacă $b \neq c$, $\mathfrak{m}_b \neq \mathfrak{m}_c$.

c) Demonstrați că $\mathfrak{m}_c \neq (X - c)$, idealul generat de funcția polinomială $X - c$.

d) Demonstrați că $\mathfrak{m}_c$ nu este ideal finit generat.

Exercițiul 36*: Fie $n \geq 3$ întreg. Fie $f, g \in \mathbb{R}[X]$ astfel încât punctele $(f(1), g(1))$, $(f(2), g(2)), \ldots, (f(n), g(n)) \in \mathbb{R}^2$ sunt vârfurile unui poligon regulat cu n laturi, aşezate în sens trigonometric. Demonstraţi că cel puţin unul dintre polinoamele f şi g are grad mai mare sau egal cu $n - 1$.

Exercițiul 37*: Fie $f_1, \ldots, f_k \in \mathbb{Z}[X]$ polinoame neconstante. Demonstraţi că există o infinitate de valori $n \geq 1$ pentru care $f_1(n), \ldots, f_k(n)$ sunt toate numere compuse.

Problema 1.

a) Dacă $x, y, z \in \mathbb{C}$ sunt astfel încât $x+y+z=1, x^2+y^2+z^2=2$ şi $x^3+y^3+z^3=3$, determinaţi valoarea lui $x^4+y^4+z^4$. $= \frac{25}{6}$

b) Demonstraţi că numerele x, y, z care satisfac condiţiile anterioare nu sunt raţionale dar că $x^n+y^n+z^n \in \mathbb{Q}$ pentru orice număr natural n.

Problema 2.

a) Daţi un exemplu de polinom simetric omogen de grad 10 în 4 variabile şi cu 12 termeni sau explicaţi de ce un astfel de polinom nu există.

b) Fie polinomul simetric $f(X_1, X_2, X_3) = (X_1^8+2X_2^4X_3^4)(X_2^8+2X_1^4X_3^4)(X_3^8+2X_1^4X_2^4) \in \mathbb{Z}[X_1, X_2, X_3]$ şi $g \in \mathbb{Z}[X_1, X_2, X_3]$ astfel încât $f(X_1, X_2, X_3) = g(s_1, s_2, s_3)$, conform Teoremei fundamentale a polinoamelor simetrice. Calculaţi $g(0,0,1)$ şi arătaţi că g nu este polinom simetric.

c) Fie $h \in \mathbb{Z}[X_1, X_2, X_3]$ cu proprietatea că $\sigma^*(h) = \epsilon(\sigma) \cdot h$ pentru orice $\sigma \in S_3$. Demonstraţi că $h(X_1, X_2, X_3) = (X_1-X_2)(X_1-X_3)(X_2-X_3)h_1(X_1, X_2, X_3)$ pentru un $h_1 \in \mathbb{Z}[X_1, X_2, X_3]$ polinom simetric.

Problema 3. Determinaţi toate idealele I din $\mathbb{R}[X]$ pentru care inelele $\mathbb{R}[X]/I$ şi $\mathbb{R}$ sunt izomorfe.

Seminar 2 - Algebră 2

Lema chineză a resturilor (LCR): $\mathbb{Z}_{n_1 \dots n_r} \simeq \mathbb{Z}_{n_1} \times \dots \times \mathbb{Z}_{n_r}$ izo de inele

$(n_i, n_j) = 1 \ \forall i \neq j$. $\Leftrightarrow$ sist. (*) de congruențe:

$$\begin{cases} x \equiv a_1 \pmod{n_1} \\ \vdots \\ x \equiv a_r \pmod{n_r} \end{cases}$$ are sol unică mod $\underline{n_1 \dots n_r} = N$

$a_i \in \mathbb{Z}$

Fie x_i sol congr. $\frac{N}{n_i} x_i \equiv 1 \pmod{n_i} \Rightarrow$

$$\Rightarrow \boxed{x = \sum_{i=1}^{m} a_i x_i \cdot \frac{N}{n_i} \pmod N}$$

Pb0 Rez. sist. de congr. $\begin{cases} 23x \equiv 2 \pmod 7 \\ 35x \equiv 3 \pmod 8 \\ 22x \equiv 4 \pmod 9 \end{cases}$

Sist $\Leftrightarrow \begin{cases} 2x \equiv 2 \pmod 7 \\ 3x \equiv 3 \pmod 8 \\ 4x \equiv 4 \pmod 9 \end{cases} \Leftrightarrow \begin{cases} x \equiv 1 \pmod 7 \\ x \equiv 1 \pmod 8 \\ x \equiv 1 \pmod 9 \end{cases} \Rightarrow$

$\Rightarrow \boxed{x = 7 \cdot 72k + 1}$

$\boxed{Pb1}$ Să se arate că pt $\forall n \in \mathbb{N}^*$, $\exists$ n nr. nat consec. a.î niciunul dintre ele nu e putere de nr. prim

(IMO - 89)

$$\begin{cases} x \equiv 0 \pmod{2\cdot 3} \\ x \equiv -1 \pmod{5\cdot 7} \\ \vdots \\ x \equiv -(n-1) \pmod{p_{2n-1}\, p_{2n}} \end{cases}$$

: are sol unică mod $p_1 \cdots p_{2n}$.

Euclid $\Rightarrow \mathcal{P} = \{p_1, p_2, \dots\}$

mult. nr. prime e ∞.

$\boxed{Pb\,2}$ Să se arate că $\forall n \in \mathbb{N}^*$ și nr. distincte $a_1, \dots a_n \in \mathbb{N}$ $\exists$ un nr. $b \neq 0$ a.î $ba_1, \dots, ba_n$ sunt puteri perfecte de nr. nat.

$\boxed{n=2}$, $a_1 = 5$, $a_2 = 2\cdot 3$.

$b = 2^2 \cdot 3^2 \cdot 5^3 \Rightarrow a_1 b = (2\cdot 3\cdot 5^2)^2$

$a_2 b = (2\cdot 3\cdot 5)^3$

La general, $p_1 \dots p_m$ = toate nr. prime din desc. în mod. de prime ale lui $a_1, \dots, a_n$.

$a_k = p_1^{\alpha_{1,k}} \dots p_m^{\alpha_{m,k}}$ $\forall k = \overline{1,n}$ nu toate $\alpha_{i,k}$ nule.

$b = p_1^{\beta_1} \dots p_m^{\beta_m}$

Iau β_k să fie sol $\begin{cases} \beta_k \equiv -\alpha_{k,1} \pmod{q_1} \\ \vdots \\ \beta_k \equiv -\alpha_{k,m} \pmod{q_m} \end{cases}$

unde $q_1 \dots q_m$ sunt nr. prime distincte.

Obs: $(m_1, m_2) = 1 \Rightarrow m_1\mathbb{Z} + m_2\mathbb{Z} = \mathbb{Z}$

($m_1\mathbb{Z}$ și $m_2\mathbb{Z}$ sunt comaximale)

LCR pt inele: Fie R inel com. Fie $I_1, \dots, I_n \trianglelefteq R$ comaximale 2 câte 2. ($I_i + I_j = R$ $\forall i \neq j$) $\Rightarrow$

$$\boxed{R/_{I_1 \cap \dots \cap I_n} \simeq R/_{I_1} \times \dots \times R/_{I_n}}, \quad \boxed{I_1 \cap \dots \cap I_n = I_1 \cdots I_n}$$

izo de inele $\qquad IJ = \{ \sum a_i b_i \mid a_i \in I, b_i \in J \}$

Dem: temă ("extindeți" dem. algoritmică de la $\mathbb{Z}$)

$\boxed{Pb_3}$ a) $\mathbb{Q}[X]/_{(X^2-1)} \simeq \mathbb{Q} \times \mathbb{Q}$

b) $\mathbb{Z}[X]/_{(X^2-1)} \not\simeq \mathbb{Z} \times \mathbb{Z}$

$\mathbb{Q}[X]/_{(X^2+X+5)} = \{ a\hat{x} + b \mid a, b \in \mathbb{Q} \} \overset{?}{\simeq} \mathbb{Q} \times \mathbb{Q}$

($\Leftrightarrow$ Pot da pe $\mathbb{Q} \times \mathbb{Q}$ o str. de inel a.î să am izo?)

$I_1 = (X-1) \quad \Rightarrow \quad I_1 + I_2 = \mathbb{Q}[X]$.

$I_2 = (X+1) \qquad \frac{1}{2}(X+1) - \frac{1}{2}(X-1) = 1 \in I_1 + I_2$

$\mathbb{Q}[X]/_{(X-a)} \simeq \mathbb{Q}$.

$\mathbb{Q}[X] \xrightarrow{\varphi} \mathbb{Q}, \quad \varphi(P(X)) = P(a) \overset{\text{Bézout}}{\Longrightarrow} \ker \varphi = (X-a)$

b) $(x-1)\mathbb{Z}[X]+(x+1)\mathbb{Z}[X] \neq \mathbb{Z}[X]$

$$\mathbb{Z}[X]/_{(x-1,x+1)} \simeq \mathbb{Z}[X]/_{(2,x+1)} \simeq \frac{\mathbb{Z}[X]/(x+1)}{(2,x+1)/_{(x+1)}}$$

$$\simeq \frac{\mathbb{Z}}{2\mathbb{Z}} \simeq \mathbb{Z}_2 \not\simeq \mathbb{Z}\times\mathbb{Z}$$

<u>Sau</u>: $\mathrm{Idem}(\mathbb{Z}\times\mathbb{Z}) = \{(0,0),(0,1),(1,0),(1,1)\}$.

$\mathrm{Idem}\left(\mathbb{Z}[X]/_{(x^2-1)}\right) = \{\hat{0},\hat{1}\}$.

$\mathbb{Z}[X]/_{(x^2-1)} = \{\widehat{ax+b} \mid a,b\in\mathbb{Z}\}$.

$(\widehat{ax+b})^2 = \widehat{ax+b} \Leftrightarrow \underbrace{\widehat{a^2x^2}}_{+a^2} + \widehat{2abx} + \widehat{b^2} = \widehat{ax+b}$

$\widehat{x^2} = \hat{1}$

$\widehat{a(2b-1)x + (b^2-b+a^2)} = 0$

$\Rightarrow \begin{cases} a(2b-1)=0 \\ b^2-b+a^2=0 \end{cases} \Rightarrow a=0 \Rightarrow b^2=b \Rightarrow b=0$ sau 1.

$\boxed{\text{Pb 5}}$ Arătați că idealele lui $R_1\times\ldots\times R_n$ (prod. direct de inele) sunt de forma $I_1\times\ldots\times I_n$ cu $I_j \trianglelefteq R_j$ (totul com).

<u>Dem</u>: $R_1\times\ldots\times I_n/_{I_1\times\ldots\times I_n} \simeq R_1/_{I_1}\times\ldots\times R_n/_{I_n}$

! $\mathbb{Q}[\sqrt{2}] \not\simeq \mathbb{Q}[\sqrt{3}]$

(izo ca $\mathbb{Q}$ sp. vect., dar nu sunt izo ca inele)

$\to$ Fie $\pi_i : R \to R_i$, $\pi_i(a) = a_i$ morf. surj. de inele

$\pi_i(R) = R_i$

$\boxed{\text{„}\supseteq\text{"}}$ Fie $J_i \trianglelefteq R_i$. Dem că ~~Rp~~ $J_1 \times .. \times J_m \trianglelefteq R$

$x = (x_1, \dots, x_m) \in J_1 \times .. \times J_m$.
$y \in (y_1, \dots, y_m)$

$x - y = (\underbrace{x_1 - y_1}_{\in J_1}, \dots, \underbrace{x_m - y_m}_{\in J_m}) \in J_1 \times .. \times J_m$

$\alpha x = (\underbrace{\alpha_i x_1}_{\in J_1}, \dots \underbrace{\alpha_i x_m}_{\in J_m}) \in J_1 \times \dots \times J_m \quad \forall \alpha \in R$

$\boxed{\text{„}\subseteq\text{"}}$ Fie $J \trianglelefteq R \Rightarrow \underbrace{\pi_i(J)}_{\text{not } J_i} \trianglelefteq R_i \Rightarrow J = J_1 \times \dots \times J_m$

evident $J \trianglelefteq J_1 \times .. \times J_m$.

$x = (x_1, \dots, x_m) \in J_1 \times .. \times J_m$.

$x_i \in \pi_i(J) \Rightarrow \exists\, a \in J$ cu $\pi_i(a) = x_i$

$a = (a_1, \dots, a_{i-1}, x_i, a_{i+1}, \dots, a_m)$
$e_i = (0, \dots, 0, 1, 0, \dots, 0)$ $\Big| \Rightarrow \underbrace{e_i\, a}_{(0, \dots, 0, x_i, 0 \dots 0)} \in R$.

$\Rightarrow x = \sum (0, \dots, 0, x_i, 0, \dots 0) \in J$.

$R_1 \times .. \times R_m / J_1 \times .. \times J_m \xrightarrow{\varphi} R_1/J_1 \times .. \times R_m/J_m$

$\varphi(a_1 \dots a_n) = (a_1 + J_1, \dots, a_n + J_n)$ morf surj. de inele

cu $\ker \varphi = J_1 \times .. \times J_m$.

$\operatorname{Im} \varphi = R_1/J_1 \times \dots \times J_m/J_n \Rightarrow$ TFI.

Seminar 3 - Algebră 2

Recapitulare: Ideale, inele factor

$\boxed{R \text{ inel com.}}$; unitar (am $1 \in R$)

$P(X) \in k[X] \setminus k$,
$\uparrow$
corp

- com. $\Rightarrow P$ are ~~deg~~ nr. de rădăcini $\leq \deg P$
- necom $\Rightarrow P$ poate avea $> \deg P$ răd

ex: $X^2+1 \in \mathbb{H}[X]$

$I \trianglelefteq R$ dc $\begin{cases} (I,+) \leq (R,+) \\ \forall \alpha \in R \\ \forall a \in I \end{cases} \Big\} \Rightarrow \alpha a \in I.$

Op. cu ideale:

$I_1 + I_2 = \{ a+b \mid a \in I_1, b \in I_2 \}$

$I_1 \cdot I_2 = \{ \sum_{\text{finite}} a_i b_i \mid a_i \in I_1, b_i \in I_2 \}$

$I_1 : I_2 = \{ a \in R \mid a I_2 \subseteq I_1 \} \supseteq I_1$

Coresp. alg. - geometrie: varietate $\leftrightarrow$ ideal radical.

$$\boxed{I_1 \cdot I_2 \subseteq I_1 \cap I_2 \subseteq I_1 + I_2}$$

Dc. $I_1 + I_2 = R \Rightarrow I_1 \cdot I_2 = I_1 \cap I_2$.

$a\mathbb{Z} + b\mathbb{Z} = (a,b)\mathbb{Z}$

$a\mathbb{Z} \cap b\mathbb{Z} = [a,b]\mathbb{Z}$

$a\mathbb{Z} : b\mathbb{Z} = \{ t \in \mathbb{Z} \mid t \cdot b\mathbb{Z} \subset a\mathbb{Z} \} = \frac{a}{(a,b)}\mathbb{Z}$

$a\mathbb{Z} \cdot b\mathbb{Z} = ab\mathbb{Z}$

Pb1 $18\mathbb{Z} + (2\mathbb{Z} \cap 3\mathbb{Z}) = 18\mathbb{Z} + 6\mathbb{Z} = 6\mathbb{Z}$.

Pb2 Th. coresp. a idealelor: R, S inele, $f: R \to S$ morf. surj.
Atunci $\exists$ o coresp. bij între idealele lui S și id. lui R care conțin pe $\ker f$ $\iff$ [$\exists\, \varphi: \{I \trianglelefteq R \mid I \supseteq \ker \varphi\} \to \{J \trianglelefteq S\}$
$\exists\, \psi: \{J \trianglelefteq S\} \to \{I \trianglelefteq R \mid I \supseteq \ker \varphi\}$
a.î. $\varphi \circ \psi = \psi \circ \varphi = 1$].

În plus, această coresp. bij. se extinde și la mț. id. prime, resp. max.

Dem: $\varphi(I) = f(I) \trianglelefteq S$ corect def. $\Rightarrow \ker \varphi = \{I \mid \varphi(I) = 0\}$

$\psi(J) = f^{-1}(J)$ corect def.

$\varphi \circ \psi = f(f^{-1}(J)) = J$

$\psi \circ \varphi = f^{-1}(f(I)) = I$

$a \in f^{-1}(f(I)) \Rightarrow f(a) \in f(I) \Rightarrow f(a) = f(c)$ cu $c \in I$

$\Rightarrow f(c-a) = 0 \Rightarrow a-c \in \ker f \in I$ ~~$\Rightarrow c$~~ $\Rightarrow a \in I$.
$c \in I$

Pb3 Descrieți id. lui R/I, $I \trianglelefteq R$ și aplicați pt. $\mathbb{Z}_n$

$p: R \to R/I = S$, $p(a) = \hat{a}$ pr. canonică (morf. surj. de inele)

$$\{I' \leq R \mid I' \supseteq I\} \underset{\psi}{\overset{\varphi}{\rightleftarrows}} \{J \trianglelefteq R/I\}$$

Aplic th. coresp. pt $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$.

$\{ m\mathbb{Z} \mid m\mathbb{Z} \supseteq n\mathbb{Z} \} \underset{\psi}{\overset{\varphi}{\rightleftarrows}} \{ J \trianglelefteq \mathbb{Z}_n \}$
$(m \mid n)$

$\{ m\mathbb{Z} \mid m \mid n \} \underset{\psi}{\overset{\varphi}{\rightleftarrows}} m\mathbb{Z}/_{n\mathbb{Z}} = \hat{m}\,\mathbb{Z}_n \trianglelefteq \mathbb{Z}_n$

$\boxed{\text{Pb 4}}$ $N(\mathbb{Z}_n) = ?$

$n = p_1^{a_1} \dots p_k^{a_k} \Rightarrow |N(\mathbb{Z}_n)| = \dfrac{n}{p_1 \dots p_k}$

$\hat{x} \in N(\mathbb{Z}_n) \Rightarrow x \,\vdots\, (p_1 \dots p_k)$

! $|U(\mathbb{Z}_n)| = \varphi(n)$

$U(R_1 \times \dots \times R_n) \simeq U(R_1) \times \dots \times U(R_n)$

$\forall p$ prim, $\forall n \in \mathbb{N}^* \Rightarrow \exists!$ corp cu p^n elem. până la un izo.

Th 1 izo: Fie R un inel (com), $I, J \trianglelefteq R$, $I \subseteq J$

Atunci $\boxed{\dfrac{R/I}{J/I} \underset{f}{\simeq} R/J}$

izo de inele

Dem: Caut f surj cu $\ker f = J/I$
$\operatorname{Im} f = R/J$

$f : R/I \to R/J$, $f(\hat{x}) = \overline{x}$

$\hat{x} = \hat{y} \Rightarrow x - y \in I \subseteq J$

$\overline{x} = \overline{y} \Rightarrow f(\hat{x}) = f(\hat{y}) \Rightarrow f$ bine def.

f surj: $\overline{x} \in R/J \Rightarrow f(\hat{x}) = \overline{x}$.

f morf.: $\hat{x}, \hat{y} \in R \Rightarrow f(\hat{x} + \hat{y}) = f(\widehat{x+y}) = \overline{x+y}$
$= \bar{x} + \bar{y}$
$= f(\hat{x}) + f(\hat{y})$

la fel și pt $f(\hat{x} \cdot \hat{y}) = f(\hat{x}) \cdot f(\hat{y})$.

$f(\hat{1}) = \bar{1}$

$\ker f = \{ \hat{x} \mid f(\hat{x}) = \bar{x} \} \Rightarrow x \in J \Rightarrow \ker f = J/J$

$\operatorname{Im} f = R/J$ (f surj) $\Rightarrow$ TFI.

Temă: 1) R inel, $a \in R$ inv. la stg + dr $\Rightarrow a \in U(R)$.

2) Dați ex. de inel R + elem b care e inv. la stg, dar nu la dr.

3) R inel, $a \in R$ inv. la stg, dar nu la dr. $\overset{?}{\Rightarrow}$ a are o ∞ de inverși la dr.

89 4) R inel și $A \in M_{m \times n}(R)$, $B \in M_{n \times m}(R)$. Dem că

$I_m - AB$ inv $\Leftrightarrow I_n - BA$ inv.

5) Det. toate morf. de inele
$\mathbb{Z} \to \mathbb{Z}$
$\mathbb{Z} \to \mathbb{Q}$
$\mathbb{Q} \to \mathbb{Z}$
$\mathbb{Q} \to \mathbb{Q}$
$\mathbb{Z}_m \to \mathbb{Z}_n$
$\mathbb{R} \to \mathbb{R}$
$\mathbb{C} \to \mathbb{C}$
$\mathbb{Q}[\sqrt{3}] \to \mathbb{Q}[\sqrt{3}]$.

Seminar 4 - Alg. - 21.03.2024

Ideale prime / maximale

$\mathbb{Q}[\sqrt[3]{3}] = \mathbb{Q}(\sqrt[3]{3})$ $\simeq$ $\mathbb{Q}[X]/_{(X^3-2)}$ ← corp.

În general: $\mathbb{Q}[X]/_{X^n-2}$ → corp.

$Spec(R) = \{P \mid P \text{ ideal prim}\}$ ← spectrul lui R.

$Max(R) = \{M \mid M \text{ ideal maximal}\}$

$P \in Spec(R) \overset{def}{\iff} P \trianglelefteq R,\ P \neq R$ a.î. $\forall a, b \in R$ cu $ab \in P$ $\Rightarrow a \in P$ sau $b \in P$.

↑ corespunde nr. prime.

$P \in Max(R) \overset{def}{\iff} M \trianglelefteq R,\ M \neq R$ şi $\forall\ J \trianglelefteq R$ cu $M \subseteq J \subseteq R$ $\Rightarrow M = J$ sau $J = R$.

Caract. gr. abeliene:

1) $\left.\begin{array}{l} G \text{ abelian} \\ |G| = n \end{array}\right\} \Rightarrow G \simeq \mathbb{Z}_{d_1} \times \mathbb{Z}_{d_2} \times \ldots \times \mathbb{Z}_{d_2}$

$1 < d_1 \mid d_2 \mid \ldots \mid d_2$ cu $d_1 \ldots d_2 = n$

$|G| = 12 \Rightarrow G \simeq \mathbb{Z}_{12}$ sau $G \simeq \mathbb{Z}_2 \times \mathbb{Z}_6$.

2) $\left.\begin{array}{l} G \text{ abelian} \\ \text{finit generat} \end{array}\right\} \Rightarrow G \simeq \mathbb{Z}^t \times \mathbb{Z}_{d_1} \times \mathbb{Z}_{d_2} \times \ldots \times \mathbb{Z}_{d_2}$

$\boxed{\mathbb{Z}, \mathbb{Z}_n, \mathbb{Z}[i], k[X], \mathbb{Z}[X]}$ ← de bază pt. licență.

$\boxed{1}$ $Spec(\mathbb{Z}) = ?$ și $Max(\mathbb{Z}) = ?$

$n\mathbb{Z} \in Spec(\mathbb{Z})$, $n \neq \pm 1$ $(n\mathbb{Z} \neq \mathbb{Z})$

$ab \in n\mathbb{Z} \Rightarrow a \in n\mathbb{Z}$ sau $b \in n\mathbb{Z}$ $\Rightarrow n = p$ prim sau $n = 0$.

Dc. $n = kl \neq$ prim $\Rightarrow kl \in n\mathbb{Z}$
$k \notin n\mathbb{Z}$ și $l \notin n\mathbb{Z}$.

$Spec(\mathbb{Z}) = \{(0)\} \cup \{p\mathbb{Z} \mid p \text{ prim}\}$

$n\mathbb{Z} \in Max\,\mathbb{Z} \Rightarrow n\mathbb{Z} \subseteq m\mathbb{Z} \subseteq \mathbb{Z} \Leftrightarrow 1 \mid m \mid n$.

$n \neq 0$

$n\mathbb{Z} \subsetneq m\mathbb{Z} \subsetneq \mathbb{Z} \Leftrightarrow n$ are diviz proprii (nu e prim)

$\Rightarrow n = p$ prim.

$Max(\mathbb{Z}) = \{p\mathbb{Z} \mid p \text{ prim}\}$.

$\boxed{P}$ $P \in Spec(R) \Leftrightarrow R/_P$ dom. de integritate

$\boxed{M}$ $M \in Max(R) \Leftrightarrow R/_M$ e corp

(Max ⊆ Spec)

Lema lui Krull: Fie R un inel com. $I \trianglelefteq R$, $I \neq R$

$\Rightarrow \exists$ un id. maximal M care $M \supseteq I$.

⇓

$\forall R$ inel com $\Rightarrow Max(R) \neq \emptyset \Rightarrow (Spec(R) \neq \emptyset)$

$\boxed{n \neq 0}$ $\mathbb{Z}/_{n\mathbb{Z}} = \mathbb{Z}_n$ e dom $\Leftrightarrow$ $\mathbb{Z}_n$ corp $\Leftrightarrow$ $n = p$ prim.

$R \xrightarrow{\varphi} S$ morf. surj $\Rightarrow \exists$ o coresp. bij. între

$\mathrm{Spec}(S) \longleftrightarrow \{ p \in \mathrm{Spec}(R) \mid p \supset \ker \varphi \}$

$\mathrm{Max}(S) \longleftrightarrow \{ M \in \mathrm{Max}(R) \mid M \supset \ker \varphi \}$

$\boxed{n \geq 2}$ $\mathrm{Spec}(\mathbb{Z}_n) = \{ p\mathbb{Z}_n \mid p \text{ prim}, p \mid n \}$
$\overset{\shortparallel}{\mathrm{Max}(\mathbb{Z}_n)}$.

$\mathrm{Spec}(\mathbb{Z}/_{n\mathbb{Z}}) \longleftrightarrow \{ p \in \mathrm{Spec}(\mathbb{Z}) \mid \underset{p\mathbb{Z} \Leftrightarrow p \mid n}{\overset{}{p \supseteq n\mathbb{Z}}} \}$

$\mathbb{Z} \xrightarrow{\pi} \mathbb{Z}_n$ $\quad \ker \pi = n\mathbb{Z}$.
$a \longmapsto \hat{a}$

Lem: $R \xrightarrow{\pi} R/_J$, $a \mapsto \hat{a}$, $J \trianglelefteq R$.

$S/_{\varphi(J)} \simeq R/_J$.

Fie $\mathcal{J}/_J \trianglelefteq R/_J \Rightarrow \mathcal{J}/_J \in \mathrm{Spec}(R/_J) \Leftrightarrow \dfrac{R/_J}{\mathcal{J}/_J} \simeq \cancel{R/_J}\ R/_{\mathcal{J}}$ dom

$\mathcal{J} \supseteq J$

$\Leftrightarrow \underline{\mathcal{J} \in \mathrm{Spec}(R)}$

$\mathrm{Max}(k[X]) \longleftrightarrow$ pol. ired. din $k[X]$

$\mathrm{Max}(\mathbb{C}[X]) \longleftrightarrow$ pol. monice de gr. 1.

$Max(\mathbb{C}[X_1,\dots,X_n]) = \{(X_1-a_1,\dots,X_n-a_n) \mid a_i \in \mathbb{C}\}$

Th. Hilbert a zerourilor, forma slabă

$\boxed{Pb}$ $m,n \in \mathbb{N}$, $\begin{cases} A \in M_{m\times n}(R) \\ B \in M_{n\times m}(R) \end{cases}$, R inel com

$I_m - AB$ inv $\Leftrightarrow$ $I_n - BA$ inv

Ciornă: $1 + X + X^2 + \dots = \frac{1}{1-X} = (1-X)^{-1}$ în $R[[X]]$.

$C \overset{not}{=} (I_m - AB)^{-1} = I_m + AB + (AB)^2 + \dots$ ✓

$(I_n - BA)^{-1} = I_n + BA + BABA + \dots,$?

$BCA = BA + (BA)^2 + \dots$

$I_n + BCA = I_n + BA + (BA)^2 + \dots$

Rezolvare: Pp. $I_m - AB$ inv și not. C inv. sa. Se arată că $\boxed{I_n + BCA}$ inversa lui $I_n - BA$.

$\mathbb{F}_8 = \mathbb{F}_{2^3} \simeq \mathbb{Z}_2[X]/(X^3+X+\hat{1})$

$\simeq \mathbb{Z}_2[X]/(X^3+X^2+\hat{1})$

temă: găsiți un izo.

(Funcția lui Möbius)

$\boxed{Pb2}$ $\mathbb{Z}[i]$; $\langle 5\rangle, \langle 3\rangle \overset{?}{\in} Spec(\mathbb{Z}[i])$

$\in Max(\mathbb{Z}[i])$

Ex de corpuri "exotice":

$$M = \left\{ \begin{pmatrix} \hat{a} & \hat{b} \\ -\hat{b} & \hat{a} \end{pmatrix} \middle| \hat{a}, \hat{b} \in \mathbb{Z}_p, p \text{ prim}, p \equiv 3 \bmod 4 \right\}$$

$(M, +, \cdot)$ corp. com. ← temă

$\mathbb{Z}[i]/_{\langle 3\rangle} = \{ \widehat{a+bi} \mid a, b \in \mathbb{Z} \}$

$\widehat{a+bi} = \widehat{c+di} \overset{def}{\Longleftrightarrow} (a+bi) - (c+di) \in \langle 3\rangle \Leftrightarrow$

$\Leftrightarrow (a-c) + i(b-d) = 3x + 3yi \Leftrightarrow \begin{cases} a-c = 3x \\ b-d = 3y \end{cases} \Leftrightarrow \begin{cases} a \overset{3}{\equiv} c \\ b \overset{3}{\equiv} d \end{cases}$

$\Rightarrow \mathbb{Z}[i]/_{\langle 3\rangle} = \{ \widehat{a+bi} \mid a, b \in \{0,1,2\} \}$

Analog $\mathbb{Z}[i]/_{\langle 5\rangle} = \{ \widehat{a+bi} \mid a, b \in \{0, 1, \dots, 4\} \}$

→ evident corp.

! $a, b \in R$ $\quad a \sim b$ asociere în divizibilitate $\Leftrightarrow a = bu$, $u \in U(R)$

$U(\mathbb{Z}[i]) = \{\pm 1, \pm i\}$

"$\supseteq$" evident

$\boxed{\subseteq}$ $z \in U(\mathbb{Z}[i]) \Rightarrow z\cdot z' = 1 \Rightarrow N(z)\cdot N(z') = 1$

$N(z) = |z|$, $N(z') = |z'|$ $= 1 \mid (\ )^2$

$|z|^2 \cdot |z'|^2 = 1$

$(a^2+b^2)\ (c^2+d^2)$

$6 = 2\cdot 3 = (-2)\cdot(-3)$

$5 = (2+i)(2-i) = (1+2i)(1-2i)$.

asoc. în divizibilitate.

$-i(2+i) = -2i+1$.

$(2+i)(2+4i) = \hat{0}$ în $\mathbb{Z}[i]/_{\langle 5\rangle} \Rightarrow$ nu e corp.

! $\mathcal{J}(R_1\times\dots\times R_n) = \{J_1\times\dots\times J_n \mid J_i \trianglelefteq R_i\}$

mulț. de ideale — produs direct de inele.

$\mathrm{Spec}(R_1\times\dots\times R_n) = ?$ $\quad \mathrm{Max}(R_1\times\dots\times R_n) = ?$

$$(R_1\times\dots\times R_n)/(J_1\times\dots\times J_n) \simeq \underbrace{(R_1/_{J_1})\times\dots\times(R_n/_{J_n})}$$

dom $\Leftrightarrow \exists\, i = \overline{1,n}$ a.î. $R_i/_{J_i}$ dom.

$R_j/_{J_j} = \{0\}$ $\forall j \neq i$.

$$\Rightarrow \mathrm{Spec}(R_1\times\dots\times R_n) = \bigcup_{j=1}^{n} R_1\times\dots\times \mathrm{Spec}(R_j)\times\dots\times R_n.$$

$$\mathrm{Max}(R_1\times\dots\times R_n) = \bigcup_{j=1}^{n} R_1\times\dots\times \mathrm{Max}(R_j)\times\dots\times R_n.$$

6/7 /7

$\boxed{7b}$ Dați ex de. ∃ de inel care este produs direct netrivial

de 3 inele și care are $\begin{cases} 21 \text{ de ideale} \\ 3 \text{ maximale.} \end{cases}$

$\boxed{R}$ nu există: $R_1 \times R_2 \times R_3 = R$

$$|\mathcal{I}(R)| = |\mathcal{I}(R_1)| \cdot |\mathcal{I}(R_2)| \cdot |\mathcal{I}(R_3)| = 21 = 3 \cdot 7$$

$$\Rightarrow |\mathcal{I}(R_1)| = 1 \Rightarrow R_1 = \{0\}.$$

b) în loc de 21 pun 42.

ex: $\mathbb{Z}_2 \times \mathbb{Z}_{2^2} \times \mathbb{Z}_{2^6}$

! $|\mathcal{I}(\mathbb{Z}_{p^\alpha})| = \alpha + 1$

Dacă vreau inele neizomorfe $\Rightarrow$ un ex: $\mathbb{Q} \times \mathbb{Z}_{3^2} \times \mathbb{Z}_{7^6}$.

c) Dați ex ~~de ∃~~ de 2 inele neizomorfe care sunt produs direct de 3 inele și au 57 de ideale și au * maximale.

$\mathrm{Max}(\mathbb{Q} \times \mathbb{Z} \times \mathbb{Z}_{10^9+7})$

Seminar 6 - Algebră - 16.04.2024

- urm. 3 săpt. marți + joi (seminar
  sala 8

- test 25.04.2024 (1h de la 15^{00}-16^{00})

! Temă de gândire:
1) $d \in \mathbb{Z}^* \setminus \{1\}$ liber de pătrate. Arătați că $\forall$ ideal din $\mathbb{Z}[\sqrt{d}]$ poate fi gen. minimal cu cel mult 2 elem.
2) Dați ex. (dc. ∃) de ideal al lui $\mathbb{Z}[X]$ care poate fi gen. minimal cu n elem $\forall n \geq 1$.

Def: Un inel R com. unitar cu $0 \neq 1$ s.n. noetherian dc. $\forall$ ideal al său e finit generat.

Construcții: R noetherian $\Rightarrow R[X]$ noeth. (Th. Hilbert a bazei)
$\Rightarrow R[[X]]$ noeth.
$\Rightarrow R[X_1, \dots, X_n]$ noeth.
$\Rightarrow R/_I$ noeth cu $I \trianglelefteq R$

Ex: $R = k$ corp com $\Rightarrow$ e inel noeth. (are 2 ideale $\{0\} = (0)$, $R = (1)$)
$R = \mathbb{Z}$ noeth ($\forall$ id. al lui $\mathbb{Z}$ e gen. de un elem)
$R = k[X]$
$R = \mathbb{Z}[i]$
$R = \mathbb{Z}[X]$ noeth.

Fapte generale : $\begin{cases} \text{- elem. inv } U(R) \ni 1 \\ \text{- diviz. ai lui 0 } D(R) \ni 0 \\ \text{- nilpotenți } N(R) \ni 0 \\ \text{- idempotenți} \end{cases}$

În particular, pt $\boxed{R = \mathbb{Z}_m}$ $\begin{cases} \Rightarrow U(\mathbb{Z}_m) = \{\hat{k} \mid (k, m) = 1\} \\ \quad |U(\mathbb{Z}_m)| = \varphi(m) \\ \Rightarrow N(\mathbb{Z}_m) = (p_1 \cdots p_r)\mathbb{Z}_m \\ \quad m = p_1^{\alpha_1} \cdots p_r^{\alpha_r} \\ \quad \alpha_i \geq 1. \\ \Rightarrow D(\mathbb{Z}_m) = \mathbb{Z}_m \setminus U(\mathbb{Z}_m) \end{cases}$

$\boxed{Pb_1}$ Fie R = inel com., $x, y \in N(R)$. Atunci $r, s \in U(R)$

a) $x+y,\ xy,\ xa \in N(R)\ \forall a \in R$.

b) $rs \in U(R)$, $x + r \in U(R)$

Dem: a) $x^n = y^m = 0 \Rightarrow \begin{cases} (x+y)^{n+m} = 0 \\ (xy)^{\min(n,m)} = 0 \\ (xa)^n = 0 \end{cases}$

b) inv. lui rs este $s^{-1}r^{-1}$

$x^n = x^{n+1} = 0 \Rightarrow$ pot pp. n imp.

$\underbrace{x^n}_{0} + r^n = (x+r)(x^{n-1} - x^{n-2}r + \dots + r^{n-1})$

$r^n \in U(R)$

$\boxed{Pb2}$ $R[X] = \{ \sum_{0}^{n} a_i X^i \mid n \in \mathbb{N}, a_i \in R \}$

a) $U(R[X]) = \{ \underline{a_0 + \dots + a_n X^n} \mid a_0 \in U(R)$ și $a_i \in \mathcal{N}(R), i=\overline{1,n} \}$
$\qquad\qquad\qquad\qquad \overset{\shortparallel}{A}$

b) $\mathcal{N}(R[X]) = \{ \underbrace{a_0 + a_1 X + \dots + a_n X^n}_{\overset{\shortparallel}{B}} \mid a_i \in \mathcal{N}(R) \}$

c) $D(R[X]) = \{ \underbrace{a_0 + \dots + a_n X^n}_{f} \mid \exists\, a \in R \setminus \{0\}$ a.î. $af = 0 \} = C$

Cazuri particulare: 1) k corp $\Rightarrow k[X]$ dom.

$U(k[X]) = U(k) = k \setminus \{0\}$

$\mathcal{N}(k[X]) = \{0\}$

2) Det # pol. de deg ≤ 2 care sunt $\begin{cases} \text{inv.} \\ \text{nilpotente} \\ \text{diviz. } 0. \end{cases}$

$\boxed{R = \mathbb{Z}_{155}}$

$|U(\mathbb{Z}_{155})| = \varphi(155) = \frac{155}{3} = 58.$

$|\mathcal{N}(\mathbb{Z}_{155})| = \frac{155}{6} = 25.$, $|D(\mathbb{Z}_{155})| = 155 - 58 = 96$

$|U(\mathbb{Z}_{155}[X]_{\le 2})| = 58 \cdot 25 \cdot 25.$

$|\mathcal{N}(\mathbb{Z}_{155}[X]_{\le 2})| = 25 \cdot 25 \cdot 25.$

$|D(\mathbb{Z}_{155}[X]_{\le 2})| = ?$ ← temă !

Înapoi la pb: b) evident $B \subseteq \mathcal{N}(R[X])$

"$\supseteq$" inducție după n.

$\boxed{n = 0}$ ✓

$\boxed{n-1 \Rightarrow n}$ $f = a_0 + \dots + a_n X^n$, $f^k = 0 \Rightarrow a_n^k = 0 \Rightarrow a_n \in \mathcal{N}(R)$

$\Rightarrow a_n X^n \in \mathcal{N}(R[X]) \Rightarrow f - a_n X^n \in \mathcal{N}(R[X])$

$\uparrow$ discomd

a) evident $U(R[X]) \supseteq A$.

"$\subseteq$" $f(x) = a_0 + \dots + a_n X^n \in U(R[X]) \Rightarrow f \cdot g = 1$.

$g(x) = b_0 + \dots + b_m X^m$

$$\Rightarrow \begin{cases} a_0 b_0 = 1 \Rightarrow a_0, b_0 \in U(R) \\ a_0 b_1 + a_1 b_0 = 0 \quad | \cdot a_m^{m+1} \Rightarrow a_m^{m+1} b_0 = 0 \Rightarrow a_n^{m+1} = 0. \\ \vdots \\ a_m b_{m-1} + a_{m-1} b_m = 0 \quad | \cdot a_m \Rightarrow a_n^2 b_{m-1} = 0 \\ a_m b_m = 0 \end{cases}$$

ex (utilitate tehnică): Arătă că $Y^m - X^n$ e ired în $\mathbb{C}[X,Y]$

$(m,n) = 1$

rez. în urm. seminarii

c) evident $\Delta(R[X]) \supseteq C$

$f = a_0 + \dots + a_n X^n$ (deg g minim)

$g = b_0 + \dots + b_m X^m$ $\Big\}$ $f \cdot g = 0 \Rightarrow$

$$\Rightarrow \begin{cases} a_0 b_0 = 0 \\ a_0 b_1 + a_1 b_0 \\ \vdots \\ a_m b_{m-1} + a_{m-1} b_m = 0 \Rightarrow a_{n-1} b_m = 0 \\ a_m b_m = 0 \end{cases}$$

$\Rightarrow f(x) \cdot (a_m g(x)) = 0 \Rightarrow a_m g(x) = 0$

$\Rightarrow a_m b_i = 0 \ \forall i$.

$\Rightarrow f(x)(a_{n-1} g(x)) = 0 \Rightarrow$

$\Rightarrow a_{n-1} g(x) = 0$

$\Downarrow$

$a_{n-1} b_i = 0$

$\vdots$

$a_i b_j = 0 \ \forall i, j$

$\Rightarrow \boxed{b_m f = 0}$

$\boxed{Pb_2}$ $R[[X]] = \{ \sum_{i\geq 0} a_i X^i \mid a_i \in R \}$

a) $U(R[[X]]) = \{ \sum_{i\geq 0} a_i X^i \mid a_0 \in U(R) \} = A$

b) $\mathcal{N}(R[[X]]) \subseteq \{ \sum_{i\geq 0} a_i X^i \mid a_i \in \mathcal{N}(R)\ \forall i \} = B$

c) $D(R[[X]]) \supseteq \{ \sum_{i\geq 0} a_i X^i \mid \exists a \in R\setminus\{0\}$ a.î. $a a_i = 0\ \forall i \} = C$

! Temă de gândire: ex $f \in B$ care nu e nilpotent.

Obs: 1) R = noeth ⇒ am = peste tot

2) R = oarecare ⇒ nu am neap. = în b) și c)

b) Dem: la fel ca la $\mathcal{N}(R[X])$, doar că merg de la $a_0 \downarrow a_n$

a) "⊇" $f(x) = \sum a_i X^i$, $a_0 \in U(R)$. Construiesc
$g(x) = \sum b_i X^i$ a.î. $f \cdot g = 1 \Leftrightarrow \begin{cases} a_0 b_0 = 1 \Rightarrow b_0 = a_0^{-1} \\ a_1 b_0 + a_0 b_1 \Rightarrow b_1 = a_0^{-1}(a_1 b_0) \\ \vdots \end{cases}$

Inele factor

R = inel com $\qquad$ $R[X] \xrightarrow{\varphi} S$ $\quad$ φ ← morf. de inele

$R/_J$ = inel factor $\qquad$ TFI $R[X]/_{\ker\varphi} \simeq \operatorname{Im}\varphi$

$R[X]/_I$, $I \trianglelefteq R[X]$
$\shortparallel$
?

R, S inele, $\varphi : R \to S$ morf. de inele. Vreau $\bar{\varphi} : R[X] \xrightarrow{\bar{\varphi}} S$ morf.

$\forall b \in S \Rightarrow (\exists!)\, \bar{\varphi}$ a.î. $\begin{cases} \bar{\varphi}/_R = \varphi \\ \bar{\varphi}(x) = b \end{cases}$ morf. $\Bigg\}$ Prop. de univ.

$\bar{\varphi}(f(x)) = f(b)$.

* Dați ex. de morf. $\begin{cases} \mathbb{Z}[X] \to \mathbb{Z}_5 \\ \mathbb{Q}[X] \to \mathbb{Q}[\sqrt{3}] \end{cases}$

a) $\mathbb{Z} \xrightarrow{p} \mathbb{Z}_5$, $p(a) = \hat{a}$

$\mathbb{Z}[X] \xrightarrow{\tilde{p}} \mathbb{Z}_5$, $\tilde{p}\left(\sum_0^n a_i X^i\right) = \sum_0^n \hat{a}_i \hat{1}^i$ = morf.

de inele conform Prop. de univ.

$\mathbb{Z} \overset{i}{\hookrightarrow} \mathbb{R}$

$\mathbb{Z}[X] \overset{\eta}{\hookrightarrow} \mathbb{R}$

$\eta(f(x)) = f(\sqrt{3})$ morf. de inele.

Utilitate $V = \{(t^2, t^3) \mid t \in \mathbb{R}\}$ varietate

$I(V) = \{(x^3 - y^2) \trianglelefteq \mathbb{R}[X, Y]\}$

---

* $R[X]/_{(X-a)} \simeq R$

Dem: TFI + Bezout.

* $\mathbb{Z}[X]/_{n\mathbb{Z}[X]} \simeq \mathbb{Z}_n[X]$ $\forall n \geq 2$.

Vreau $\varphi : \mathbb{Z}[X] \to \mathbb{Z}_n[X]$ morf. de inele a.î. $\ker\varphi = n\mathbb{Z}[X]$

$\varphi(\sum a_i X^i) = \sum \bar{a}_i X^i$ e morf.

$\ker\varphi = \{f = 0\} = \{\sum_{0}^{m} \bar{a}_i X^i \mid \bar{a}_i = 0\} = n\mathbb{Z}[X]$

$\ast$ $\mathbb{Z}[X]/_{(X^2+1)} \simeq \mathbb{Z}[i]$

$\mathbb{Z}[X] \xrightarrow{\varphi} \mathbb{Z}[i]$, $\varphi(f(X)) = f(i)$

$\varphi(a+bX) = a+bi \Rightarrow \varphi$ surj.

! **Temă**: 1) $\mathbb{Q}[X]/_{(X^n-2)}$ corp (X^n-2 ired)

2) $\mathrm{Spec}(\mathbb{Z}[X])$, $\mathrm{Max}(\mathbb{Z}[X])$ (după Paște)

3) Arată că $(3, X^2+1) \in \mathrm{Max}(\mathbb{Z}[X])$ + nu e principal

4) Pt. joi ce știm din fișă.

Seminar 6 - Algebră 2

$\boxed{R \text{ inel com. } 1 \in R}$

$a \in R \Rightarrow R[X]/_{(X-a)} \simeq R.$

$\widehat{P(X)} \longmapsto P(a)$

$m \in \mathbb{N}_{\geq 2} \Rightarrow \mathbb{Z}[X]/_{m\mathbb{Z}[X]} \simeq \mathbb{Z}_m[X]$

$\widehat{\sum a_i X^i} \longmapsto \sum \overline{a_i} X^i.$

$\boxed{Pb1}$ c) $\mathbb{Z}[X]/_{(X^2-2)} \simeq \mathbb{Z}[\sqrt{2}]$

$\varphi : \mathbb{Z}[X] \longmapsto \mathbb{Z}[\sqrt{2}]$

$\varphi(P) = P(\sqrt{2})$ din th. coresp. $\begin{cases} a \mapsto a \in \mathbb{Z} \\ X \mapsto \sqrt{2} \end{cases}$ morf. ~~surj~~.

surj. din $\forall\, a + b\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$.

$P(a+bX) \longmapsto a + b\sqrt{2}.$

$\ker \varphi = (X^2 - 2)$ . . . .

$R \subseteq S \ni b \Rightarrow R[b] = \bigcap S' = \{P(b) \mid P(X) \in R[X]\}$

S' subinel S, $R \subseteq S'$, $b \in S'$

$\tilde{\varphi}(P(X))$ unde

$\varphi : R \mapsto S$

$a \mapsto a \in R$

$X \mapsto b$

<u>Temă de gândire</u>: $\mathbb{Q}[X]/_{(X^n-2)} \simeq \mathbb{Q}[\sqrt[n]{2}] \leftarrow$ corp.

❗ Th împ. cu rest peste un inel R funcționează dc.

<u>$LC(g) \in U(R)$</u>, $g \in R[X] \setminus \{0\}$.

e) $\mathbb{R}[X]/_{(X^2+1)} \simeq \mathbb{C}$

$\varphi(f) = f(i)$ morf. surj. de inele $\Rightarrow \mathbb{R}[X]/_{(X^2+1)} \simeq \mathbb{R}[i] \simeq \mathbb{C}$.

$\varphi: \mathbb{R}[X] \to \mathbb{C}$.

<u>Prop</u>: Fie $f \in R[X]$, R inel com. și $LC(f) \in U(R)$ $\deg f = n \geq 1$. Atunci pt. inelul factor $R[X]/_{(f)} = \{\widehat{a_0 + \dots + a_{n-1}X^{n-1}} \mid a_i \in R\} = \Delta$, mt. Δ reprez. un SCR (sistem complet de repr z.)

<u>Dem</u>: $g \in R[X]$

$g(X) = f(X) \cdot q(X) + r(X)$, $\deg r < \deg f$

$\Rightarrow g(X) - r(X) = f(X) \cdot q(X) \in (f) \Rightarrow \widehat{g(X)} = \widehat{r(X)}$, $r \in \Delta$.

$\hat{g} = \hat{r}_1, \hat{g} = \hat{r}_2$

Fie $r_1, r_2 \in \Delta$ cu $r_1(X) \neq r_2(X) \Rightarrow r_1(X) - r_2(X) \in (f)$

$\Rightarrow \underbrace{r_1(X) - r_2(X)}_{\deg \leq n-1} = \underbrace{f(X)}_{\deg n} \cdot h(X)$. $\Rightarrow r_1(X) = r_2(X)$.

$= \mathbb{Z}[X]/(2X+1) \simeq \mathbb{Z}[\frac{-1}{2}]$.

$\boxed{\text{Pb}}$ $\mathbb{Q}[X]/(X^2-2X+6)$. Vreau o sh. de inel pe $\mathbb{Q}\times\mathbb{Q}$

a.î. $\mathbb{Q}\times\mathbb{Q} \simeq \mathbb{Q}[X]/(X^2-2X+6)$

$$\mathbb{Q}[X]/(X^2-2X+6) = \{\widehat{aX+b} \mid a,b\in\mathbb{Q}\}$$

$$\widehat{aX+b} + \widehat{cX+d} = \widehat{(a+c)X+(b+d)} \Rightarrow (a,b)\oplus(c,d) = (a+b, c+d$$

$$(\widehat{aX+b})(\widehat{cX+d}) = \widehat{acX^2 + (ad+bc)X + bd}$$

$$\widehat{X^2} = \widehat{2X-6} \qquad = \widehat{(2ac+ad+bc)X + (bd-6ac)}$$

$$\Rightarrow (a,b)\odot(c,d) = (2ac+ad+bc,\ bd-6ac).$$

$\boxed{\text{Pb}}$ $\mathbb{R}[X]/(X^2-1) \simeq \mathbb{R}\times\mathbb{R}$. ← prod. direct de inele.

$\boxed{\text{Var 1}}$ TFI: $P(X) \longmapsto (P(-1), P(1))$

$$\mathbb{R}[X] \xrightarrow{\varphi} \mathbb{R}\times\mathbb{R}.$$

$X \longmapsto b = (-1,1) \Rightarrow \sum a_i X^i \longmapsto \sum (a_i, a_i) b^i$

$a \longmapsto (a,a)$

$= (\sum a_i(-1)^i, \sum a_i \cdot \cancel{1^i})$

$= (P(-1), P(+1))$

$P\in \ker(\varphi) \Rightarrow P(1)=P(-1)=0 \Rightarrow (X-1)\mid P$, $(X+1)\mid P$ $\Rightarrow P \,\vdots\, (X^2-1)$.

$\boxed{\text{Var 2}}$ $(X^2-1) = (X-1, X+1)$

$(X-1)+(X+1) = \mathbb{R}[X] \Rightarrow \mathbb{R}[X]/(X^2-1) \simeq \mathbb{R}[X]/(X-1) \times \mathbb{R}[X]/(X+1) \simeq \mathbb{R}\times\mathbb{R}$.

$\boxed{Pb}$ Este $(3, X^2+1)$ ideal maximal $\mathbb{Z}[X]$?

$$\frac{\mathbb{Z}[X]}{(3,X^2+1)} \simeq \frac{\mathbb{Z}[X]/(3)}{(3,X^2+1)/(3)} \simeq \frac{\mathbb{Z}_3[X]}{(X^2+\hat{1})} \quad (\text{în } \mathbb{Z}_3[X]\ X^2+\hat{1} \text{ ired} \Rightarrow \text{corp}).$$

$$\frac{\mathbb{Z}[X]}{(3,X^2+1)} \simeq \frac{\mathbb{Z}[X]/(X^2+1)}{(3,X^2+1)/(X^2+1)} \cancel{\simeq} = \frac{\mathbb{Z}[i]}{3\mathbb{Z}[i]} = \{\bar{a}+\bar{b}i \mid a,b\in\{0,1,2\}\}$$

$\uparrow$ corp.

! În $k[X]$, $\operatorname{Max}(k[X]) = \{(f) \mid f \text{ ired în } k[X]\}$

Temă: $\left(\mathbb{Z}_3[X]/(X^2+\hat{1}), \oplus, \odot\right)$ inel

$\boxed{Pb_2}$ $\mathbb{Z}[X]/(2X-1) \simeq \mathbb{Z}[\frac{1}{2}]$

$S = \{1, 2, 2^2, 2^3, \dots\} \Rightarrow S^{-1}\mathbb{Z} = \{\frac{a}{2^n} \mid a\in\mathbb{Z}, n\in\mathbb{Z}\}$

$\varphi : \mathbb{Z}[X] \to \mathbb{Z}[\frac{1}{2}]$

$\varphi(P) = P(\frac{1}{2})$ $\Big\} \Rightarrow \ker\varphi = (2X-1)$

Temă: R inel oarecare com + unitar.

$R[X]/(aX-b) = S^{-1}R$, $a\in R\setminus N(R)$, $b\in U(R)$.

$S = \{1, a, a^2, \dots\}$.

$\boxed{Pb}$ $\mathbb{Z}[i]/(1+2i) = ?$

$$\mathbb{Z}[i]/(1+2i) \simeq \frac{\mathbb{Z}[X]/(X^2+1)}{(2X+1)} \simeq \frac{\mathbb{Z}[X]/(X^2+1)}{(2X+1, X^2+1)/(X^2+1)} \simeq \frac{\mathbb{Z}[X]}{(2X+1, X^2+1)} \simeq$$

$$\simeq \frac{\mathbb{Z}[x]/(2x+1)}{(2x+1, x^2+1)/(2x+1)} \simeq \frac{\mathbb{Z}[\frac{-1}{2}]}{(0, \frac{5}{3})} = \dots$$

↑ temă

Fapt: $(a) = (ua)$, R inel com. $a \in R$, $u \in U(R)$.

$(1+2i) = (i-2)$

$$\mathbb{Z}[i]/(1+2i) \simeq \frac{\mathbb{Z}[i]}{(i-2)} \simeq \frac{\mathbb{Z}[x]/(x^2+1)}{(x-2)} = \frac{\mathbb{Z}[x]/(x^2+1)}{(x-2, x^2+1)/(x^2+1)} \simeq$$

$$\simeq \frac{\mathbb{Z}[x]}{(x-2, x^2+1)} \simeq \frac{\mathbb{Z}[x]/(x-2)}{(x-2, x^2+1)/(x-2)} \simeq \frac{\mathbb{Z}}{(5)} \simeq \mathbb{Z}_5.$$

Temă: $\mathbb{Z}[i]/(a+bi)$ are a^2+b^2 elem. (Caz part. $a = \pm 1$, $b = \pm 1$) Scan

$\boxed{\text{Pb8}}$ b) $\mathbb{Z}[\sqrt{7}]/(6+\sqrt{7}) \simeq ?$

$$\mathbb{Z}[\sqrt{7}]/(6+\sqrt{7}) \simeq \frac{\mathbb{Z}[x]/(x^2-7)}{(6+x)} \simeq \frac{\mathbb{Z}[x]/(x^2-7)}{(6+x, x^2-7)/(x^2-7)} \simeq$$

$$\simeq \frac{\mathbb{Z}[x]}{(6+x, x^2-7)} \simeq \frac{\mathbb{Z}[x]/(6+x)}{(6+x, x^2-7)/(6+x)} \simeq \frac{\mathbb{Z}}{(29)} \simeq \mathbb{Z}_{29}.$$

Seminar 7 - Algebră 2

Th. împ. cu rest, Bézout, Viète

$\boxed{Pb1}$ α, β răd. ec. $X^2-6X+1 \in \mathbb{R}[X]$

$\forall n \in \mathbb{Z} \Rightarrow \begin{cases} \alpha^n+\beta^n \in \mathbb{Z} \\ 5 \nmid (\alpha^n+\beta^n) \end{cases}$

$\Rightarrow \alpha = 3+2\sqrt{2}$

$\beta = 3-2\sqrt{2}$.

$(3+2\sqrt{2})^n + (3-2\sqrt{2})^n \in \mathbb{Z}$.

$P_n - S_1 P_{n-1} + S_2 P_{n-2} = 0 \quad \forall n \geq 2$.

$P_n - 6P_{n-1} + P_{n-2} = 0$ inducție după n

$\overline{P_n} - \overline{P_{n-1}} + \overline{P_{n-2}} = 0$. $(\text{mod } 5)$.

$\begin{cases} \overline{P_1} = \overline{1} \\ \overline{P_2} = \overline{2} \end{cases} \Rightarrow P_3 \; . \; - \; - \; .$

$\boxed{Pb2}$ Det. restul împ. pol

a) $P(X) = X^{100} - 2X^{50} + 4$ la X^2-1 și la $(X-1)^2$

b) $P(X) = X^{444} + X^{333} + X^{222} + X^{111} + 1$ la $X^4+X^3+X^2+X+1$

a) $P(X) = (X^2-1)q(X) + r(X)$. $\Rightarrow r(X) = aX+b$.

$P(1) = 3 = a+b$.

$P(-1) = 3 = -a+b$ $\Rightarrow a=0, b=3 \Rightarrow r(X) = 3$.

$P(X) = (X-1)^2 h(X) + r(X)$, $r(X) = aX+b$.

$P(1) = a+b = 3$.

$P'(X) = (X-1)(\ldots) + a$, $P'(1) = 0 = a$. $\Rightarrow a=0$

$b=3$.

b) $F(x) = x^{444} + x^{333} + x^{222} + x^{111} + 1$

$= (x^4 + x^3 + x^2 + x + 1)\, g(x) + ax^3 + bx^2 + cx + d.$

$\uparrow$

pol ired. in $\mathbb{Q}[x]$.

Iau $\varepsilon \neq 1$ cu $\varepsilon^5 = 1$

$F(\varepsilon) = F(\varepsilon^2) = F(\varepsilon^3) = F(\varepsilon^4) \Rightarrow$ 4 ec. are sol unică

$(a, b, c, d) = (0, 0, 0, 0)$

$\boxed{\text{Pb8}}$ $P \in \mathbb{Q}[x]$, $\deg P = n$.

$P(k) = \frac{k}{k+1}$, $k = \overline{0, n}$ $\Rightarrow P(0) = 0 \Leftrightarrow P = X \cdot f(x)$.

$P(n+1) = ?$

$g(x) = (x+1)P(x) - X$ are $n+1$ răd.

$(x+1)P(x) - X = a\cancel{X}(X-1)(X-2)\ldots(X-n)$.

$X \cdot f(x)$

$(x+1)f(x) - 1 = a(x-1)(x-2)\ldots(x-n)$

$\Rightarrow P(x) = X \cdot \frac{a(X-1)\ldots(X-n)+1}{X+1}$.

$P(n+1) = (n+1) \cdot \frac{a \cdot n \cdot (n-1)\ldots 1 + 1}{n+2}$.

$\boxed{\text{Pb9}}$ $2n$ nr. distincte 2 câte 2 $a_1, \ldots, a_n, b_1, \ldots b_n$ sunt puse într-o mat. $C \in M_{n \times n}$. $c_{ij} = a_i + b_j$. Dem. că dc. prod. elem. de pe fiecare col. = const. $\Rightarrow$ prod. elem. de pe fiecare linie = const.

pe col j: $(a_1 + b_j) \ldots (a_n + b_j) = k$

$P(x) = (a_1 + X) \ldots (a_n + X) - k$ are n răd distincte $b_1 \ldots b_n$

$F(x) = \prod_1^m (x + b_i) - \prod_1^m (x - a_i) - \prod (a_i b_k)$

$F(x) - k$ are răd $a_1 \dots a_n$.

$\boxed{\text{Pb5 - IMO}}$ $\cos\frac{\pi}{7} - \cos\frac{2\pi}{7} + \cos\frac{3\pi}{7} = \frac{1}{2}$

$\phi_m(x) \in \mathbb{Z}[x]$ - sal m-lea pol. ciclotomic.

$x^n - 1 = \prod_{d|n} \phi_d(x)$.

Teoremă: $\phi_m(x)$ ired. în $\mathbb{Q}[x] \Rightarrow \mathbb{Z}[x]$.

$\phi_3(x) = x^2 + x + 1 \in \mathbb{Z}[x]$

$\phi_m(x) = \prod_{\varepsilon \in S} (x - \varepsilon)$

S = mulț. răd. prim. de ord n ale unității.

$m \geq 2$, $\varepsilon_m = \cos\frac{2\pi}{m} + i\sin\frac{2\pi}{m} \in \mathbb{C} \setminus \mathbb{R} \Rightarrow \phi_m(x)$ - pol. minimal al lui ε_m peste $\mathbb{Q}$.

$\deg \phi_m = \varphi(m)$

$[\mathbb{Q}(\varepsilon_m) : \mathbb{Q}] = \deg \phi_m(x) = \varphi(m)$ gradul extinderii.

$\cos\frac{2\pi}{m} = \frac{\varepsilon_m + \overline{\varepsilon_m}}{2}$

$$\underbrace{\underbrace{\mathbb{Q} \subseteq \mathbb{Q}(\cos\tfrac{2\pi}{m})}_{\frac{\varphi(m)}{2}} \subseteq \mathbb{Q}(\varepsilon_m)}_{\varphi(m)}$$

(the inclusion $\mathbb{Q}(\cos\frac{2\pi}{m}) \subseteq \mathbb{Q}(\varepsilon_m)$ has degree 2)

$\cos\frac{\pi}{7} = -\cos\frac{2\pi}{13}$, $\varphi(13) = 6$.

$$\phi_{14} = \frac{x^{14}-1}{(x^7-1)(x+1)} = \frac{x^7+1}{x+1} = x^6 - x^5 + x^4 - x^3 + x^2 - x + 1$$

$(x^7-1) = \phi_7$, $(x+1) = \phi_2$

$\phi_{14}(\varepsilon_{14}) = 0 \Rightarrow \varepsilon_{14}^6 - \varepsilon_{14}^5 + \varepsilon_{14}^4 - \varepsilon_{14}^3 + \varepsilon_{14}^2 - \varepsilon_{14} + 1 = 0$

$$\varepsilon_{14}^3\left(\varepsilon_{14}^3 - \varepsilon_{14}^2 + \underbrace{\varepsilon_{14}^1 - 1 + \frac{1}{\varepsilon_{14}}}_{t} - \frac{1}{\varepsilon_{14}^2} + \frac{1}{\varepsilon_{14}^3}\right) = 0$$

$\Rightarrow$ $t = 2\cos\frac{\pi}{7} = \varepsilon_{14} + \frac{1}{\varepsilon_{14}} = \varepsilon_{14} + \overline{\varepsilon_{14}}$

$t = 2\alpha$.

$t^3 - 3t - (t^2-2) + t - 1 = 0$

$t^3 - t^2 - 2t + 1 = 0$

$8\alpha^3 - 4\alpha^2 - 4\alpha + 1 = 0 \quad |:8.$

$\alpha^3 - \frac{1}{2}\alpha^2 - \frac{1}{2}\alpha + \frac{1}{8} = 0 \Rightarrow \alpha$ e răd. pol. minimal

$x^3 - \frac{1}{2}x^2 - \frac{1}{2}x + \frac{1}{8} = 0$

$\Rightarrow 4\alpha^3 - 2\alpha^2 - 2\alpha \cancel{+1} = \frac{-1}{2}$

$$\cos\frac{\pi}{7} - \cos\frac{2\pi}{7} + \cos\frac{3\pi}{7} = \alpha - (2\alpha^2 - 1) + (4\alpha^3 - 3\alpha)$$
$$= 4\alpha^3 - 2\alpha^2 - 2\alpha + 1 = \frac{1}{2}.$$

Th. fundam. a pol. sim: Fie R inel com, $f \in R[X_1, \dots X_n]$

$\boxed{\text{sim}} \Rightarrow \exists!\ g \in R[Y_1, \dots Y_n]$ a. î. $f = g(s_1, \dots, s_n)$ unde

$s_1 \dots s_n$ = pol. sim. fundam în $x_1 \dots x_n$.

(Algebra membership.)

$$s_i(x_1, \dots x_n) = \sum_{j_1 < \dots < j_i} x_{j_1} \cdots x_{j_i}$$

$\boxed{\text{Pb}}$ $J = (X-1)$. Dați ex. de sist. minimal de gen pt J cu 2024 elem.
(n)

$J = (f_1, \dots, f_n)$; $f_j = \prod_{i \neq j}^{n+1} (X - i)$, $j = \overline{2, n+1}$.

$X_1^3 X_2^1 X_3^{2024} <_{lex} X_1^3 X_2^2 X_3^0$

Deg RevLex

CoCoA
↓
Genova
↓
Singular
(~~Kaisod~~
(Kaiserslautern)

Macaulay 2

Seminar 8 - Algebră 2

$\boxed{Pb_1}$ $P(X_1, X_2, X_3) = (X_1 - X_2)^2 (X_1 - X_3)^2 (X_2 - X_3)^2 \in \mathbb{R}[X_1, X_2, X_3]$

pol. sim.

$P = g(s_1, s_2, s_3) = ?$

$LT_<(P) = X_1^4 X_2^2$, $LC_<(P) = 1$ P omogen de deg 6.

$X_1^4 X_2^2 \longrightarrow s_1^{4-2} s_2^{2-0} s_3^0 = s_1^2 s_2^2$

$X_1^4 X_2 X_3 \longrightarrow s_1^{4-1} s_2^{1-1} s_3^1 = s_1^3 s_3$

$X_1^3 X_2^3 \longrightarrow s_1^{3-3} s_2^{3-0} s_3^0 = s_2^3$

$X_1^3 X_2^2 X_1 \longrightarrow s_1^{3-2} s_2^{2-1} s_1^1 = s_1 s_2 s_3$

$X_1^2 X_2^2 X_3^2 \longrightarrow s_1^{2-2} s_2^{2-2} s_3^2 = s_3^2$

$P(X_1, X_2, X_3) = a s_1^2 s_2^2 + b s_1^3 s_3 + c s_2^3 + d s_1 s_2 s_3 + e s_3^2$

$\shortparallel$

$LC_<(P) = 1$

X_1	X_2	X_3	s_1	s_2	s_3	P	
1	1	0	2	1	0	0	$\Rightarrow 4 + c + 2d = 0$
2	-1	-1	0	-3	2	0	$\Rightarrow 0 = -27c + 4e$
$-1/2$	1	1	$3/2$	0	$-1/2$	0	$\Rightarrow 0 = -\frac{27}{4}b - \frac{1}{8}c + \frac{e}{4} = 0$
1	1	1	3	3	1	0	$\Rightarrow 0 = 81a + 27b + 27c + 9d + e$

$\Rightarrow P(X_1, X_2, X_3) = s_1^2 s_2^2 - 4 s_1^3 s_2 - 4 s_2^3 + 18 s_1 s_2 s_3 - 27 s_3^2$

Formulele lui Newton:

$P_k = x_1^k + \dots + x_n^k \in \mathbb{R}[x_1, \dots, x_n]$

$\uparrow$
sim

$\boxed{k \geq n}$ $P_k - S_1 P_{k-1} + S_2 P_{k-2} - \dots + (-1)^n S_n \cdot P_{k-n} = 0$

$\boxed{k \leq n}$ $P_k - S_1 P_{k-1} + S_2 P_{k-2} - \dots + (-1)^{k-1} S_{k-1} P_{n-k} + (-1)^k k S_k = 0$

$\boxed{Pb2}$ Calculați: $(\sin 20°)^7 + (\sin 40°)^7 \pm (\sin 80°)^7$

$\sin 60° = \frac{\sqrt{3}}{2} = 3 \sin 20° - 4 \sin^3 20°$

$P(x) = 4x^3 - 3x + \frac{\sqrt{3}}{2}$ are răd $\sin 20°, \sin 40°, -\sin 80°$

$\Downarrow$ Viete

$S_1 = 0$

$S_2 = \dots$ $\Rightarrow$ Newton. $P_7 \dots$

$S_3 = \dots$

$\boxed{Pb3}$ $A \in M_n(\mathbb{C})$, $\operatorname{tr} A = \dots = \operatorname{tr}(A^n) = 0$. $\overset{?}{\Rightarrow} A^n = O_n$.

$\lambda_1 + \dots + \lambda_n = 0 \Rightarrow S_1 = 0$

$\lambda_1^2 + \dots + \lambda_n^2 = 0 \Rightarrow S_2 = 0$

$\vdots$

$\lambda_1^n + \dots + \lambda_n^n = 0 \Rightarrow S_n = 0$

Viete $\Rightarrow P_A(x) = (x - \lambda_1) \dots (x - \lambda_n) = x^n$

$\Rightarrow A^n = O_n$.

$\boxed{Pb4}$ $x^4 + x^3 - 1 = 0$ are răd a, b, c, d.

Vreau ab răd. pt. $x^6 + x^4 + x^3 - x^2 - 1 = 0$.

$\Rightarrow \sum a = -1$ $\quad \sum abc = 0$

$\sum ab = 0$ $\quad abcd = -1 \Rightarrow a, b, c, d \neq 0$.

Se pot rescrie în funcție de $\underbrace{a+b}_{\alpha_1}, \underbrace{c+d}_{\alpha_2}, \underbrace{ab}_{\alpha_3}, \underbrace{cd}_{\alpha_4}$

$$\begin{cases} \alpha_1+\alpha_2 = -1 \\ \alpha_3+\alpha_4+\alpha_1\alpha_2 = 0 \\ \alpha_2\alpha_3+\alpha_1\alpha_4 = 0 \\ \alpha_3\alpha_4 = -1 \end{cases} \Rightarrow \boxed{\alpha_4 = \frac{-1}{\alpha_3}}$$

$$\alpha_1\alpha_2 = -\alpha_3-\alpha_4 = -\alpha_3+\frac{1}{\alpha_3} = \frac{1-\alpha_3^2}{\alpha_3}$$

$$\alpha_1+\alpha_2=-1$$

$$\alpha_2\alpha_3 - \frac{\alpha_1}{\alpha_3} = 0 \Rightarrow \alpha_2 = \frac{\alpha_1}{\alpha_3^2} \Rightarrow -1 = \alpha_1\left(1+\frac{1}{\alpha_3^2}\right)$$

$$\Rightarrow \boxed{\alpha_1 = \frac{-\alpha_3^2}{1+\alpha_3^2}} \quad \Rightarrow \boxed{\alpha_2 = \frac{-1}{1+\alpha_3^2}}$$

$$\alpha_1\alpha_2 = -\alpha_3+\frac{1}{\alpha_3} \Rightarrow \frac{\alpha_3^2}{(1+\alpha_3^2)^2} = \frac{(1-\alpha_3^2)}{\alpha_3^{\cancel{4}}} \Rightarrow$$

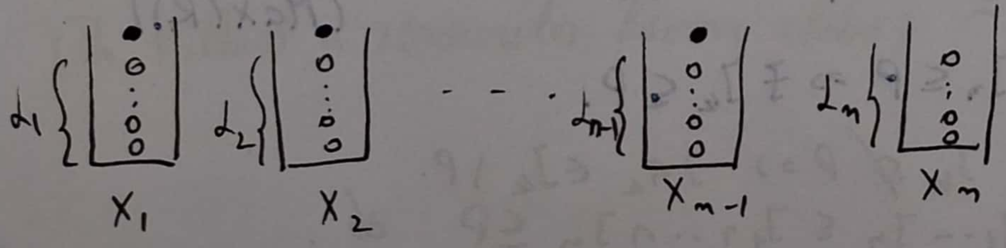
$$\Rightarrow \alpha_3^3 = (1-\alpha_3^2)(1+\alpha_3^2)^2 \Rightarrow X^6+X^4+X^3-X^2-1=0$$

are rad α_3.

$\boxed{\text{Pb5}}$ a) câte monoame de deg d în n variab. există?

b) # monoamelor de deg 8 în $\mathbb{Q}[X_1 \ldots X_5] <_{lex} X_1^3X_3X_5$

a) $X_1^{\alpha_1} \ldots X_n^{\alpha_n}$ cu $d = \alpha_1+\ldots+\alpha_n$.



$\longrightarrow$ $\boxed{\underbrace{0\ldots00}_{d_1}\bullet \ldots \bullet \underbrace{0\ldots00}_{d_{m-1}}\bullet \underbrace{0\ldots00}_{d_m}}$ $\leftarrow d + m - 1$

d ↑ goale, $m-1$ ↑ pline

Nr. de pol = # moduri în care pot să aleg bilele negre $\binom{m+d-1}{m-1} = \binom{m+d-1}{d}$

b) $X_1^3 X_3 X_5^4 \to 1$ pol.

$X_1^3 X_4^{d} X_5^{5-d} \Rightarrow 6$ pol.

$X_1^2 \underline{\qquad}$ 4 variab + deg 6 $\Rightarrow \binom{9}{6} = \binom{9}{3}$

$X_1 \underline{\qquad}$ 4 variab + deg 7 $\Rightarrow \binom{10}{3}$.

$\underline{\qquad}$ 4 variab + deg 8 $\Rightarrow \binom{11}{3}$.

<u>Pb test</u>: Inel cu 4 id. max + nr. minim de ideale.

$\mathbb{Z}_{2\cdot3\cdot5\cdot7} \to 16$ ideale.

M_1, M_2, M_3, M_4 id. max $\Rightarrow$ sunt comax.

$(M_1 \times M_2 \times M_3 \times M_4 \overset{\text{LCR}}{=\!=} M_1 \cap M_2 \cap M_3 \cap M_4$

$\forall$ intersecții dif $\Rightarrow$ id. dif.

Lemă: R inel com, $I_1, \ldots I_n \trianglelefteq R$, $P \in \operatorname{Spec}(R)$ $(\operatorname{Max}(R))$

a.î. $I_1 \cap \ldots \cap I_n \subseteq P \Rightarrow \exists I_k \subseteq P$.

<u>Dem</u>: $\forall k \Rightarrow I_k \not\subseteq P \Rightarrow \exists a_k \in I_k \setminus P$.

$a_1 \ldots a_n \in I_1 \ldots I_n \subseteq I_1 \cap \ldots \cap I_n \subseteq P$ ↯.

$\forall$ inel finit $\simeq \mathbb{Z}_{p_1^{\alpha_1}} \times \dots \times \mathbb{Z}_{p_k^{\alpha_k}}$

Vreau 4 id max $\Rightarrow \mathbb{Z}_{p_1^{\alpha_1}} \times \dots \times \mathbb{Z}_{p_4^{\alpha_4}}$

$\geq (\alpha_1+1) \dots (\alpha_4+1) \geq 2^4 = 16$ ideale.

$\boxed{\text{Pb6}}$ $\underset{\substack{\uparrow \\ \text{inel com}}}{R}[X,Y]/(X-Y) \simeq R[X]$

Știu $R[X]/(X-a) \simeq R$.

$R[X,Y]/(X-Y) \simeq \dfrac{(\overset{A'}{\overset{\shortparallel}{R[X]}})[Y]}{(X-Y)} \simeq R[X]$.
$ \in A'$

$\boxed{\text{Pb7}}$ $k[X,Y]/(Y^2-X) \not\simeq k[X,Y]/(Y^2-X^2)$ $\forall k$ corp com.

$k[X,Y]/(Y^2-X) \simeq \dfrac{k[Y][X]}{(X-Y^2)} \simeq k[Y]$ dom. integritate.

în $k[X,Y]/(Y^2-X^2)$ $\underset{\neq \bar{0}}{(\widehat{X-Y})}\underset{\neq \bar{0}}{(\widehat{X+Y})} = \bar{0}$

Temă de gândire: $\sqrt[2]{2} \pm \sqrt[3]{3} \pm \dots \pm \sqrt[25]{25} \in \mathbb{R} \setminus \mathbb{Q}$.

$\sqrt[m_1]{a_1} + \dots + \sqrt[m_k]{a_k} \in \mathbb{Q} \Leftrightarrow \sqrt[m_i]{a_i} \in \mathbb{Q}$ $\forall i$

$\forall$ corp alg. închis

Weak Nullstellensatz : $\mathrm{Max}(\mathbb{C}[X_1, \dots, X_n])$
(Th. Hilbert a zerourilor forma slabă) $= \{(X_1-a_1), \dots, (X_n-a_n)) \mid a_i \in \mathbb{C}\}$

$$\frac{\mathbb{C}[X_1,\dots,X_n]}{(X_1-a_1,\dots,X_n-a_n)} \simeq \frac{\mathbb{C}[X_1,\dots,X_{n-1}][X_n]/(X_n-a_n)}{(X_1-a_1,\dots,X_n-a_n)/(X_n-a_n)} \simeq \dots \simeq \mathbb{C}.$$

<u>Temă de gândire</u>: $\mathrm{Max}(\mathbb{R}[X,Y]),\ \mathrm{Max}(\mathbb{Z}[X]) = ?$

$\boxed{\text{Pb 8}}$ $\frac{\mathbb{R}[X,Y]}{(X^2+1,Y)} \in \mathrm{Max}(\mathbb{R}[X,Y])$

$$\frac{\mathbb{R}[X,Y]}{(X^2+1,Y)} \simeq \frac{\mathbb{R}[X][Y]/(Y)}{(X^2+1,Y)/(Y)} \simeq \frac{\mathbb{R}[X]}{(X^2+1)} \simeq \mathbb{C}.$$

$\boxed{\text{Pb 9}}$ $\mathrm{char}\, k \neq 2$, $A \subseteq k[X,Y]$ ← subinelul pol. sim.

$A = k[S_1,S_2]$, $S_1 = X+Y$, $S_2 = XY$.

$$A/(X^2+Y^2) \simeq k[X]$$

$$A/(X^2+Y^2) \simeq \frac{k[S_1,S_2]}{(S_1^2-2S_2)} \simeq \frac{k[S_1,S_2]}{(S_2-\frac{1}{2}S_1^2)} \simeq k[S_1] \simeq k[X].$$

Seminar 9 - Algebră 2

Pb1 $\mathbb{Q}[X]/_{(X^n-2)} \simeq \mathbb{Q}[\sqrt[n]{2}]$

$\varphi : \mathbb{Q}[X] \longrightarrow \mathbb{Q}[\sqrt[n]{2}]$

$\varphi(P) = P(\sqrt[n]{2})$ morf. surj. de inele

$\ker \varphi \supseteq (X^n - 2)$

„$\subseteq$"?

Pp. R.A $\exists$ $a_0 + a_1\sqrt[n]{2} + \dots + a_{n-1}\sqrt[n]{2^{n-1}} = 0$. Vreau

$\{1, \sqrt[n]{2}, \dots, \sqrt[n]{2^{n-1}}\}$ bază în $\mathbb{Q}^n$.

$2a_{n-1} + a_0\sqrt[n]{2} + \dots + a_{n-2}\sqrt[n]{2^{n-1}} = 0$

$\vdots$

$$\Rightarrow \begin{pmatrix} a_0 & a_1 & \dots & a_{n-1} \\ 2a_{n-1} & a_0 & \dots & a_{n-2} \\ \vdots & & \ddots & \\ 2a_1 & 2a_2 & \dots & a_0 \end{pmatrix} \begin{pmatrix} 1 \\ \sqrt[n]{2} \\ \vdots \\ \sqrt[n]{2^{n-1}} \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$

. Mă uit mod 2 $\Rightarrow$ $a_0 \vdots 2$.

Analog $\underline{a_i \vdots 2}$

<u>Temă de gândire</u>: $\sqrt{m_1} + \dots + \sqrt{m_k} \in \mathbb{Q} \Leftrightarrow \sqrt{m_i} \in \mathbb{Q}$ $\underline{\forall i}$

! Dc. P, F pol în $\mathbb{Z}[X]$ și $(P(X), F(X)) = G(X)$ $\not\Rightarrow$ $(P(k), F(k)) = G(k)$.

ex: $P(X) = X$, $F(X) = X-2$ $\Rightarrow (P, F) = 1$.

$(P(6), F(6)) = 2 \neq 1$.

$a, b \in R \Rightarrow (a,b) = d \Rightarrow d = a \cdot \lambda + b \cdot \mu$

$\uparrow$

euclidian / principal.

$\boxed{\text{Pb 2}}$ $(X^n - 1, X^m - 1) = X^{(n,m)} - 1$ (dem. identitatea pt. $(k^n - 1, k^m - 1) = k^{(n,m)} - 1$, $k \geq 2$).

$m \geq n$, $m = n q_1 + r_1$

$$
\begin{array}{l|l}
X^m - 1 & X^n - 1 \\
\hline
-X^m + X^{m-n} & X^{m-n} + X^{m-2n} + \dots + X^{\overset{r_1}{m - q_1 n}} \\
\hline
X^{m-n} - 1 & \\
\vdots & \\
\hline
X^{r_1} - 1 &
\end{array}
$$

$X^m - 1 = (X^n - 1) \cdot (X^{m-n} + \dots + X^{r_1}) + X^{r_1} - 1$

$n_1 = r_1 q_1 + r_2 \Rightarrow X^n - 1 = (X^{r_1} - 1)(\dots) + X^{r_2} - 1)$

$\vdots$ Alg. Euclid.

$(X^n - 1, X^m - 1) = (X^{(n,m)} - 1)$.

$\boxed{\text{Pb 3}}$ $f = X^{23} + X^{22} + \dots + X + 1$

$g = X^{15} + X^{14} + \dots + X + 1$

$(f, g) = ?$

$(X-1) f = X^{24} - 1$

$(X-1) g = X^{16} - 1)$

$\Rightarrow (f, g) = \dfrac{(X^{24} - 1, X^{16} - 1)}{X - 1} = \dfrac{X^8 - 1}{X - 1}$

<u>Temă</u>: $X^4 + 1$, $X^4 - 10X^2 + 1$ sunt ired. în $\mathbb{Q}[X]$ / red. în $\mathbb{Z}_p[X]$ $\forall p$ prim.

$\uparrow$

$(X+1)^4 + 1$ Eis.

! 2, 3 sau 6 sunt resturi pătratice mod $\forall p$.

$\left(\frac{2}{p}\right)\cdot\left(\frac{3}{p}\right)=\left(\frac{6}{p}\right)$, $X^4-10X^2+1 = (X^2-5)^2-2^2\cdot 6$
$=(X^2+1)^2-2^2\cdot 3X^2$
$=(X^2-1)^2-2^2\cdot 2X^2$

$\boxed{\text{Pb4}}$: $(2^m-1, 2^n+1)=1$

~~$m<n \Rightarrow (2^{n-m}+1) \vdots d$~~
~~$(2^m-1)\vdots d$~~

$d=(2^m-1, 2^n+1)$

$\left.\begin{array}{l} d \mid 2^m-1 \\ d \mid 2^n+1 \Rightarrow d \mid 2^{2n}-1 \end{array}\right\} \Rightarrow$

$\Rightarrow d \mid 2^{(m,2n)}-1 \Rightarrow d \mid 2^{(m,n)}-1 \Rightarrow d \mid 2^d-1 \Rightarrow \left.\begin{array}{l} d \mid 2^n-1 \\ d \mid 2^n+1 \end{array}\right| \Rightarrow$

$\Rightarrow d \mid 2 \Rightarrow \boxed{d=1}$.

$\boxed{\text{Pb5}}$ $F_n = 2^{2^n}+1$, $n\geq 0$

$F_0F_1\dots F_{n-1} = F_n - 2 \overset{?}{\Rightarrow} (F_n, F_m)=1$. $n\neq m$.

$F_0F_1\dots F_{n-1} = F_n-2$ (inductive)!

$m<n \Rightarrow F_n = 2+F_0\dots F_m F_{m+1}\dots F_n \Rightarrow$

$d=(F_n, F_m) \Rightarrow \left.\begin{array}{l} d \mid F_n \\ d \mid F_m \end{array}\right\} \Rightarrow d \mid 2 \Rightarrow \underline{d=1}$.

$\boxed{\text{Pb6}}$ k com., $f\in k[X_1,\dots X_n]$ $\forall n\geq 1$.

$\tilde{f}: k^n \to k$, $\tilde{f}(a_1,\dots a_n)=f(a_1,\dots, a_n)$

k infinit $+$ $\tilde{f}=\tilde{g} \Rightarrow f=g$

k finit $\cancel{\Rightarrow}$.

Contra ex. pt. finit, $|k| = n = p^t \Rightarrow f = X^n - X$
$g = 0$.

k infinit, Inducție după n

$\underline{n=1}$ $\tilde{f} - \tilde{g} = 0 \Rightarrow f - g = 0$.

$\underline{n-1 \Rightarrow n}$ $f \in k[X_1, .., X_{n-1}][X_n] \Rightarrow f = f_0 + f_1 X_n + .. + f_k X_n^k$

$f_i \in k[X_1, .., X_{n-1}]$. Iau $a_1, ..., a_{n-1} \in k$.

$f(a_1, ..., a_{n-1}, x) \in k[X]$

$\tilde{f} - \tilde{g} = 0 \Rightarrow f(a_1, ..., a_{n-1}, x) - g(a_1, ..., a_{n-1}, x) = 0 \; \forall x \in k$.

$$\Rightarrow \begin{cases} f_0(a_1, ..., a_{n-1}) - g_0(a_1, ..., a_{n-1}) = 0 \\ \vdots \\ f_k(a_1, ..., a_{n-1}) - g_k(a_1, ..., a_{n-1}) = 0 \end{cases} \Rightarrow \text{ind. } \underline{f_i = g_i}.$$

$\Rightarrow f = g$.

$\boxed{Pb 7}$ $f(x) \in \mathbb{C}[X]$ cu $x f(x-1) = (x+1) f(x)$

Inducție $(x-n) | f(x) \; \forall n \in \mathbb{N} \Rightarrow$ nu există f.

$\boxed{Pb 8}$ $x P(x-1) = (x-5) P(x)$. $\Rightarrow P(x) = x f_1(x)$.

$\cancel{x}(x-1) f_1(x-1) = \cancel{x}(x-5) f_1(x) \Rightarrow f_1(x) = (x-1) f_2(x)$.

$(x-2) f_2(x-1) = (x-5) f_2(x) \Rightarrow f_2(x) = (x-2) f_3(x)$

$(x-3) f_3(x-1) = (x-5) f_3(x) \Rightarrow f_3(x) = (x-3) f_4(x)$

$(x-4) f_4(x-1) = (x-5) f_4(x) \Rightarrow f_4(x) = (x-4) f_5(x)$.

$\cancel{(x-5)} f_5(x-1) = \cancel{(x-5)} f_5(x) \Rightarrow f_5(x) = k$.

Seminar 10 Algebră 2

Polinoame ireductibile

$k[X] \longrightarrow \forall$ ideal $I \trianglelefteq k[X]$

$\uparrow$ corp com.

$I = (f(x))$, $f(x) \in k[X]$

$R^* = R \setminus \{0\}$

$\mathbb{Z}$	$k[X]$
$\forall a \in \mathbb{Z} \setminus \{0, \pm 1\} = \mathbb{Z}^* \setminus U(\mathbb{Z})$	$\forall f \in k^*[X] \setminus U(k[X])$ ($U(k[X]) = k^*$)
$a \doteq \pm p_1^{a_1} \ldots p_n^{a_n}$	$f \doteq c f_1^{\alpha_1} \ldots f_n^{\alpha_n}$
Euclid: $P = \{2, 3, 5, \ldots\}$	$f_1, \ldots, f_n$ ired + monice dif 2 câte 2
$\lvert P \rvert = \infty$	Euclid: $P' =$ mt. pol. ired.
	$\lvert P' \rvert = \infty$ ($\forall k$ corp)

f ired în $k[X] \iff f$ nu se poate scrie ca $g \cdot h$ cu $g, h \in k[X]$, $\deg g, \deg h < \deg f$.

$\boxed{P}$ $f \in k[X]$, $\deg f = 2$ sau $3 \Rightarrow f$ ired. $\iff f$ nu are răd.

$\boxed{P1}$ $f \in k[X]$ neconst + ired $\iff (f) \in \mathrm{Max}(k[X])$

$$\mathrm{Max}(k[X]) \overset{\text{bij}}{\longleftrightarrow} \{ f \mid f \text{ ired} + \text{monic} \}$$

$\boxed{Q1}$ $f \in k[X]$. Cum testăm dc. f ired?

$\boxed{Q2}$ $f \in k[X]$ ired $\overset{?}{\Longleftrightarrow}$ $\deg f = ?$ ($\deg f = 1$ $\forall f \in k[X]$ ired. $\Rightarrow$ k = corp alg. închis)

$\boxed{Q3}$ Fixat k, care sunt gradele posibile ale pol ired?

Criteriul Eisenstein: $f(X) = a_n X^n + \dots + a_0 \in R[X]$
(R) inel factorial

Pp $\exists$ p prim cu $\begin{cases} p \mid a_0, \dots p \mid a_{n-1} \\ p \nmid a_n \\ p^2 \nmid a_0 \end{cases}$ $\Rightarrow$ f ired în $Q(R)[X]$.

Dacă, în plus, $\underset{\overset{\parallel}{GCD(a_0, \dots a_m)}}{c(f)} \sim 1 \overset{def}{\Longleftrightarrow} f$ primitiv $\Rightarrow$ f ired.

în $R[X] \Leftrightarrow f$ ired în $Q(R)[X]$.

$R \to k[Y]$, $R \to k[Y_1, \dots Y_n]$, $R \to \mathbb{Z}[Y]$

! $f(X) = 2X^7 - 18X^6 + 12X^5 + 24X^2 + 6 \in \mathbb{Z}[X]$

f ired. în $\mathbb{Q}[X]$ cf. Eisenstein $p = 3$.

$f(X) = \underline{2}(\quad)$ red în $\mathbb{Z}[X]$

$U(\mathbb{Z}[X]) = U(\mathbb{Z}) = \{\pm 1\}$

f ired. în $k[X] \Leftrightarrow f = g \cdot h \Rightarrow g \sim f$ sau $h \sim f$

$ \underset{U(R[X])}{} \quad g \sim 1$ sau $h \sim 1$

R dom., $f \in R^*[X] \setminus U(R)$ f ired. în $R[X] \Leftrightarrow \forall f = g \cdot h$ $\Rightarrow g \sim 1$ sau $h \sim 1$

Pb1 $f(x)=x^3-mx+2\in\mathbb{Z}[x]$ ired în $\mathbb{Q}[x] \iff m=?$

$\Updownarrow$ $\deg f=3$

f nu are răd în $\mathbb{Q}$.

f are răd. $\frac{p}{q}$ cu $(p,q)=1,\ q\neq 0 \Rightarrow \frac{p}{q}\in\{\pm 1, \pm 2\}$

$f(1)=3-m=0 \iff m=3$ $\qquad$ $f(2)=10-2m=0\iff m=5$

$f(-1)=1+m=0 \iff m=-1$ $\qquad$ $f(-2)=2m-6 \iff m=3$.

$\Rightarrow m\in\mathbb{Z}\setminus\{3,-1,5\}$

Obs: 1) k corp finit $\Rightarrow |k|=p^t$, p prim, $t\geq 1$

2) $\mathbb{Q}[x]$: x^n-2 ired cf Eisenstein, $p=2$

Am2 Prop $\mathbb{Z}_p$ (corp finit) $\boxed{x^{p^n}-x=\prod_{d\mid n} F_d}$

p - prim

unde F_d = prod. pol. monic de deg d.

Am3 Prop Putem număra # pol monice ired de deg $d\geq 1$ din $\mathbb{Z}_p[x]$. În plus, pot înlocui $\mathbb{Z}_p$ cu un corp k finit $|k|=q=p^t$ și tot ce e mai sus rămâne valabil.

$\overset{\shortparallel}{\mathbb{F}_q}$

Pb2 # ~~ired~~ pol deg ≤ 5 în $\mathbb{Z}_2[x]$ $\leftarrow$ Alg. Berlekamp $\Downarrow$ (factorizarea $\downarrow$ pol. peste k corp finit)

deg 1: $x,\ x+\bar{1}$

deg 2: $x^2+x+\bar{1}$

deg 3: $x^3+x^2+\bar{1},\ x^3+x+\bar{1}$

$\underline{\deg 4}$: ... ... $\Rightarrow X^4+X^3+\bar{1}$?

Pp. $P(X)=X^4+X^3+\bar{1}=g\cdot h$.

$P(0)=P(1)=\bar{1} \Rightarrow \deg g=\deg h=2 \Rightarrow$

$p(X)=(X^2+aX+b)(X^2+cX+d)$

$\Rightarrow \begin{cases} \bar{1}=c+a \\ \bar{0}=d+b+ac \\ \bar{0}=ad+bc \\ \bar{1}=bd \end{cases}$

$\Rightarrow b=d=1 \Rightarrow a+c=\bar{0}=\bar{1}$ ∄ $\Rightarrow$ ired.

$\underline{Pb3}$: X^4-10X^2+1 ireductibil în $\mathbb{Q}[X]$

red. în $\forall\, \mathbb{Z}_p$ p prim

$\left.\begin{array}{l} F(X)=X^4-10X^2+1 \in \mathbb{Z}[X] \text{ ired în } \mathbb{Q}[X] \\ C(F)=1 \end{array}\right\} \Leftrightarrow F$ ired în $\mathbb{Z}[X]$

Pp. F red în $\mathbb{Z}[X]$ $F=(X^2+aX+b)(X^2+cX+d)$

$\begin{cases} \bar{0}=a+c \\ -10=d+b+ac=2b-a^2 \\ \bar{0}=ad+bc=a+c \\ 1=bd \Rightarrow b=d=\pm 1 \end{cases}$ . . . . .

$F(X)$ = red în $\mathbb{Z}_p[X]$ p-prim.

$\underline{p=2} \Rightarrow F(X)=X^4+1=(X^2+1)^2$

$\underline{p=3} \Rightarrow F(X)=X^4+2X^2+1=(X^2+1)^2$

$\underline{p=5} \Rightarrow F(X)=X^4-4=(X^2-2)(X^2+2)$

$\underline{p\geq 7}$ $F(X)=\begin{cases} (X^2-5)^2-2^2\cdot 6X^2 \\ (X^2-1)^2-2^2\cdot 2X^2 \\ (X^2+1)^2-2^2\cdot 3\cdot X^2 \end{cases}$

Unul dintre 2, 3, 6 e rest pătratic mod p $\left(\frac{6}{p}\right)=\left(\frac{2}{p}\right)\left(\frac{3}{p}\right)$

Pb4 k corp, $f \in k[X]$ pol neconst, $a, b \in k$, $a \neq 0$, f ired în $k[X]$ $\Leftrightarrow$ $f(aX+b)$ ired în $k[X]$.

$$\varphi : k[X] \to k[X] \quad \text{bij}$$
$$\varphi(X) \longmapsto aX+b$$
$$\varphi(\alpha) \longmapsto \alpha \in k.$$

φ surj $\Rightarrow$ $\varphi(P(a^{-1}(X-b))) = P$

φ inj $\varphi(P) = 0 \Rightarrow \varphi(aX+b) = 0$ $\forall X \in k$.

$$\begin{array}{ccc} R & \xrightarrow{\sim} & S \\ \cup\!\!\! \mid & & \cup\!\!\! \mid \\ J & & \varphi(J) \end{array} \Rightarrow R/_J \simeq S/\varphi(J)$$

Pb5: $P(X) = X^{p-1} + \dots + X + 1$ p = prim.

$P(X) = \dfrac{X^p - 1}{X-1}$ ired în $\mathbb{Q}[X] \Leftrightarrow P(X+1)$ ired în $\mathbb{Q}[X]$

$P(X) = \dfrac{(X+1)^p - 1}{X} = X^{p-1} + C_p^1 X^{p-2} + \dots + C_p^p$, $C_p^k = \binom{p}{k}$

$\boxed{C_p^k \,\vdots\, p}$ $\Rightarrow$ ired din cr. Eisenstein

Pb6: $P(X,Y) = X^2 + Y^2 - 1$ în $\mathbb{R}[X,Y]$

! $k[X_1, \dots X_m]$ inel factorial, $Q(k[X_1, \dots X_n]) = k(X_1, \dots X_n)$

$P(X,Y) = Y^2 + (X^2 - 1) = F_X(Y)$

term liber în $(\mathbb{R}[X])[Y]$

ired cf Eisenstein în $\mathbb{R}(X)[Y]$ $p = X-1$

$c(P) = GCD(1, X^2 - 1) = 1$.

Pb10: $p(X) = X^{105} - 9$ ired. în $\mathbb{Q}[X]$

$X^n - a^m$, a liber de pătrate, $m \geq 2$

în $\mathbb{R}[X]$ evident

în $\mathbb{Q}[X]$ ec. $X^{105} = 9$ are răd $\underbrace{\sqrt[105]{9}}_{\alpha}, \varepsilon\alpha, \ldots, \varepsilon^{104}\alpha$

$\varepsilon = \cos\frac{2\pi}{105} + i\sin\frac{2\pi}{105}$

PpRA. $f = g \cdot h$, $g, h \in \mathbb{Q}[X]$

$f(0) = \underset{\in\mathbb{Q}}{g(0)}\,\underset{\in\mathbb{Q}}{h(0)}$, $g = (X - \alpha\varepsilon^{i_1}) \ldots (X - \alpha\varepsilon^{i_k})$

$|g(0)| = \alpha^k = 9^{\frac{k}{105}} \Rightarrow 105 \mid k$ (F).

Pb11: $X^n - Y^m = P(X,Y)$ ired în $k[X,Y]$, $(m,n) = 1$.

$k[X,Y] \to k[T]$

P. Univ: $X \longmapsto T^m$

$Y \longmapsto T^n$ morf de inele

$a \in k \longmapsto a$ $\quad \varphi(X^n - Y^m) = (T^m)^n - (T^n)^m = 0$

$\Downarrow$

$\ker\varphi \supset (X^n - Y^m)$

$\boxed{I_n \subset ''}$ $f \in \ker\varphi \Rightarrow f \in k[X,Y] = k[Y][X]$

$\Rightarrow \exists\, g, r \in k[Y][X]$ cu $\deg_X r < n$. a.î. $f = g(X^n - Y^m) + r$

$\varphi(f) = 0 \Rightarrow 0 = a_{n-1}(T^n)T^{m(n-1)} + \ldots + a_1(T^n)T^m + a_0(T^n)$

$T^{n c + m b}$ $\quad b = \overline{0, n-1}$

$nc_1 + mb_1 = nc_2 + mb_2 \Rightarrow n \mid m(b_2 - b_1) \Rightarrow n \mid b_2 - b_1$

$\Rightarrow b_2 = b_1$.

$a_i(Y) \neq 0 \Rightarrow LT_<(a_i(T^n)T^{mi}) = c_i T^{nd_i} T^{mi} = c_i T^{nd_i + mi}$

Fie $i_0 = \max\{i \mid a_i(Y) \neq 0\}$ dc. $i_0 = -1$ ✓.

altfel $LT_<(a_{i_0}(T^n)T^{mi_0})$ nu apare în scrierea niciunui pol $a_j(T^n)T^{mj}$ cu $j < i_0$.

Seminar 11 - Algebră 2

Rezolvare test 2

Pb 2 a) $\sum_{sym} x^a y^b z^c T^d$ cu $a+b+c+d=10$

a,b,c,d:
- 24, dif.
- 1, egale
- 4, $a=b=c\neq d$
- 6, $a=b, c=d$.
- 12, $a=b\neq c\neq d$.

b) $f(X_1,X_2,X_3)=(X_1^8+2X_2^4X_3^4)(X_2^8+2X_1^4X_3^4)(X_3^8+2X_1^4X_2^4)$

$\cancel{g(s_1,s_2,s_3)=f(X_1,X_2,X_3)}$

$\cancel{f \text{ nu e sim}}$

$g(0,0,1)=f(1,\varepsilon,\varepsilon^2)=27$
$g(1,0,0)=f(1,0,0)=0$ $\Big\}\Rightarrow g$ nu e sim.

c) $\cancel{\sigma^* h=\varepsilon(\sigma)h}$, $h\in\mathbb{Z}[X_1,X_2,X_3]$

$\cancel{h=(X_1-X_2)(X_2-X_3)(X_1-X_3)\cdot p(X_1,X_2,X_3)}$
sim.

$h(X_1,X_2,X_3)=-h(X_2,X_1,X_3)$ în $\mathbb{Z}[X_1,X_2,X_3]$

$\Rightarrow h(X_1,X_1,X_3)=0$

X_1 = răd pt h în $\mathbb{Z}[X_1,X_3][X_2]\Rightarrow X_2-X_1\mid h$

La fel pt $X_1-X_3\mid h$, $X_2-X_3\mid h\Rightarrow(X_1-X_2)(X_2-X_3)(X_1-X_3)\mid h$

$\boxed{\text{Pb3}}$ $\mathbb{R}[X]/_J \simeq \mathbb{R} \Rightarrow J = ?$

J e maximal ($\mathbb{R}[X]/_J$ = corp), $J = (f) \Rightarrow f$ ired.

$\Rightarrow f$ are $\deg 1 / 2$

$\deg 1$: $\mathbb{R}[X]/_{(f)} \simeq \mathbb{R}$

$\deg 2$: $f(x) = (x - z)(x - \bar{z})$ $\Rightarrow$ $\mathbb{R}[X]/_{(f)} \simeq \mathbb{C}$.

$\boxed{\text{Pb1}}$ ~~$f \in \mathbb{Z}[X]$, $f(x) = x^3 + 63$.~~ $\underbrace{X^{p^n} + p - 1}_{f(x)}$ e ired. în $\mathbb{Z}[X]$

$f(x+1) = (x+1)^{p^n} + p - 1 = X^{p^n} + \dots$

$p \mid C_{p^n}^k = \dfrac{p^n!}{k!\,(p^n-k)!} = \dfrac{p^n(p^n-1)\dots(p^n-k+1)}{k!}$

$v_p(m!) = \left\lfloor \frac{m}{p} \right\rfloor + \left\lfloor \frac{m}{p^2} \right\rfloor + \dots$

$v_p(C_{p^n}^k) = \sum\limits_{i=1}^{k+1} \left\lfloor \frac{p^n}{p^i} \right\rfloor - \underbrace{\left\lfloor \frac{p^n - k}{p^i} \right\rfloor - \left\lfloor \frac{k}{p^i} \right\rfloor}$

" = " p.t. $\{a\} + \{b\} < 1$.

$k = p^s \cdot \ell \Rightarrow$ iau $\underline{i = s+1}$.

$\boxed{\text{Sau}}$

$(x+1)^{p^n} = X^{p^n} + 1 \pmod p$ ← Frobenius de n ori.

$= X^{p^n} + \sum C_{p^n}^k X^k \cdot \cancel{\;} + 1$ $\Bigg\} \Rightarrow p \mid C_{p^n}^k$

Pb2 $f(x) = (x-a_1)\dots(x-a_n)-1$ ired în $\mathbb{Q}[X]$.

monic <=> ired în $\mathbb{Z}[X]$.

$f = g \cdot h$.

$f(a_i) = g(a_i) \cdot h(a_i) = -1 \Rightarrow h(a_i) + g(a_i) = 0$

$\tilde{f} = g + h \in \mathbb{Z}[X]$ deg $< n$ are n răd a_i $\Rightarrow g = -h$

$f = -h^2(x)$ coef dom -1 $\cancel{\text{ct}}$.

Pb3 $f(x) = (x-1)\dots(x-n)+1$ ired în $\mathbb{Q}[X]$

$f = g \cdot h \Rightarrow g(a_i)\, h(a_i) = 1 \Rightarrow (g-h)(a_i) = 0 \Rightarrow g = h$.

$\Rightarrow f = g^2$

$f\left(\frac{3}{2}\right) = \frac{1}{2} \cdot \frac{-1}{2} \cdot \frac{-3}{2} \cdot \dots \cdot \frac{-2n-3}{2} < -1$, $n \geq 5$

$n \leq 4$ calcule ...

Pb4 $f \in \mathbb{Z}[X]$ monic, $\deg f > 1$. $\overset{?}{\Rightarrow} \exists g(x) \in \mathbb{Z}[X]$ a.î. $f \circ g$ red.

$g(x) - x \mid f(g(x)) - f(x)$ $\Big/ \Rightarrow f(x) \mid \cancel{g \circ f}\ f(g(x))$.

Iau $g(x) = x + f(x)$

Pb5 $\mathbb{Z}[X]/(2, x^4+x^3+1) \simeq \mathbb{Z}_2[X]/(x^4+x^3+1) \simeq \mathbb{F}_{16}$.

ired

$\boxed{Pb6}$ Nr. de ideale max. conținute în $(13, X^{507}+54X^{338}+62)$

$=$ nr. de factori ired. ai lui $X^{507}+\hat{54}X^{338}+\hat{62}$ în $\mathbb{Z}_{13}[X]$

$507 = 3\cdot 13^2$

$338 = 2\cdot 13^2$

$\Rightarrow X^{507}+\overline{54}X^{338}+\overline{62} = (X^3+\overline{54}X^2+\overline{62})^{13^2} = (X^3+2X^2+3)^{13}$

$= (X+1)^{13^2}(X-2)^{13^2}(X+5)^{13^2}$

$\Rightarrow \left|\mathrm{Max}\left(\frac{\mathbb{Z}[X]}{(13, X^{507}+54X^{338}+62)}\right)\right| = 3.$

$\boxed{Pb7}$ # pol. monici care divid $X^{44}+3X^{22}+3 \in \mathbb{R}[X]$

t^2+3t+3 nu are răd în $\mathbb{R}$. $\Rightarrow X^{44}+3X^{22}+3$ nu

are răd în $\mathbb{R}$

$\to$ răd $z, \bar{z} \in \mathbb{C}\setminus\mathbb{R}$. $\Rightarrow$ răd lui f sunt $w_1, \dots w_{22}$

$\varphi_1, \dots \varphi_{22}$

cu $w_i^{22} = z$, $\varphi_i^{22} = \bar{z}$ $\Rightarrow$ 22 de perechi de răd. complexe

$\Rightarrow$ 22 de pol.

! $X^2+XY+1 \in \mathbb{R}[X,Y]$ ired ($\Leftarrow$ ired mod Y).

$\boxed{Pb8}$ $R = \{f \in \mathbb{R}[X] \mid f(0) \in \mathbb{Q}\}$

$I = \{f \in R \mid f(0) = 0\}$

I nu e fin. generat.

$I \supset (X) = \{Xf \mid f \in R\} \leftarrow$ coef lui $X \in \mathbb{Q}$.

Pp. $f = (f_1, \dots, f_k) \subset R$

$f_i = \dots + a_i X$, $a_i \in \mathbb{R}$

$\forall f \in I \Rightarrow \dots + aX$, $a \in \langle a_1, \dots a_k \rangle_{\mathbb{Q}} \Rightarrow$

$\Rightarrow \mathbb{R} = \langle a_1, \dots a_k \rangle_{\mathbb{Q}}$ ⨳.

$\boxed{\text{Pbs}}$ $n \geq 3$. $f, g \in \mathbb{R}[X]$ a.î. $(f(1), g(1)), \dots, (f(n), g(n)) \in \mathbb{R}^2$ vf. polig. reg cu n lat. în sens trigo. Cel puțin unul dintre f, g are $\deg \geq n-1$.

Putem pp. că e polig. reg. centrat în $(0,0)$.

$h(x) = f(x) + i g(x) \in \mathbb{C}[X]$.

$h(j)$, $j = \overline{1,n}$ vf. polig. reg $\overset{?}{\Rightarrow}$ $\deg h \geq n-1$.

$w^n = 1$, w răd. primitivă $\Rightarrow h(k+1) = w\, h(k)$

$g(x) = h(x+1) - w h(x)$ are $n-1$ răd $\Rightarrow h(x+1) = w\, h(x)$ imposibil.

sau $\deg h \geq n-1$