SEMINAR 12: ARITMETICĂ ÎN INELELE $\mathbb{Z}$ ŞI $k[X]$ (II)

Fie k un corp comutativ fixat ($\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ sau $\mathbb{F}_p$). Precum în $\mathbb{Z}$, notăm cu $(\ ,\ )$ cel mai mare divizor comun şi cu $[\ ,\ ]$ cel mai mic multiplu comun. Algoritmul lui Euclid se transferă cuvânt cu cuvânt în $k[X]$ (relaţia de ordine fiind recuperată via noţiunea de grad). Spre exemplu:

1. Să se determine (f, g), $[f, g]$ şi să se scrie (f, g) ca şi combinaţie liniară între f şi g în următoarele cazuri:
(a) $f = X^4 + X^3 - 7X^2 - X + 6$, $g = X^3 - X^2 - 4X + 4$ în $\mathbb{Q}[X]$;
(b) $f = \frac{1}{3}X^3 - X^2 - \frac{1}{12}X + \frac{1}{4}$, $g = \frac{1}{9}X^3 - \frac{1}{18}X^2 - X + \frac{1}{2}$ în $\mathbb{Q}[X]$;
(c) $f = X^3 + 2X^2 + X + 2$, $g = X^3 - iX^2 - 4X + 4i$ în $\mathbb{C}[X]$;
(d) $f = X^3 + \hat{3}X^2 + \hat{4}X + \hat{2}$, $g = X^3 + \hat{4}X^2 + X + \hat{1}$ în $\mathbb{F}_5[X]$.

Soluţie. Aici aş putea să trec peste - aţi făcut la liceu asemenea chestiuni... Vedem două metode pentru a determina (f, g).
(a) Mai întâi, folosim algoritmul lui Euclid (adică împărţim). Avem

$$X^4 + X^3 - 7X^2 - X + 6 = (X + 2)(X^3 - X^2 - 4X + 4) + (-X^2 + 3X - 2)$$

Apoi, împărţim $X^3 - X^2 - 4X + 4$ la restul $X^2 - 3X + 2$ (nu contează că am schimbat semnul: c.m.m.d.c este unic până la o constantă nenulă). Avem

$$X^3 - X^2 - 4X + 4 = (X^2 - 3X + 2)(X + 2)$$

Astfel, ultimul rest nenul este $X^2 - 3X + 2$, şi deci acesta este (f, g).

Pentru a determina $[f, g]$, folosim faptul că $[f, g](f, g) = fg$. Dar, mai întâi, împărţim pe f şi g la $X^2 - 3X + 2$: obţinem

$$f = (X^2 - 3X + 2)(X^2 + 4X + 3)$$
$$g = (X^2 - 3X + 2)(X + 2)$$

de unde,

$$[f, g] = \frac{fg}{(f, g)} = (X^2 + 4X + 3)(X + 2)(X^2 - 3X + 3)$$
$$= X^5 + 3X^4 - 5X^3 - 15X^2 + 4X + 12$$

În fine, pentru a depista combinaţia liniară, parcurgem drumul invers din algoritm: $X^2 - 3X + 2 = (X + 2)g - f$.

Însă observaţi şi o a doua metodă: descompunem în factori ireductibili. Avem că

$$\begin{aligned} f &= X^3(X+1) - 7X^2 - X + 7 - 1 \\ &= X^3(X+1) - 7(X^2-1) - (X+1) \\ &= X^3(X+1) - 7(X+1)(X-1) - (X+1) \\ &= (X+1)(X^3 - 7X + 7 - 1) \\ &= (X+1)((X-1)(X^2+X+1) - 7(X-1)) \\ &= (X+1)(X-1)(X^2+X-6) \\ &= (X+1)(X-1)(X^2-4+X-2) \\ &= (X+1)(X-1)((X+2)(X-2)+X-2) \\ &= (X+1)(X-1)(X-2)(X+3) \end{aligned}$$

iar

$$\begin{aligned} g &= X^2(X-1) - 4(X-1) \\ &= (X-1)(X^2-4) \\ &= (X-1)(X-2)(X+2) \end{aligned}$$

şi deci, luând factorii comuni la puterile cele mai mici,

$$(f, g) = (X-1)(X-2) = X^2 - 3X + 2$$

(De fapt, am lucrat numai în $\mathbb{Z}[X]$.)

(b) Din nou, ca să fie calculul mai lejer, ţineţi cont de faptul că (f, g) e unic până la o constantă (astea-s elementele inversabile dintr-un $k[X]$). Astfel, în locul lui f luăm $12f = 4X^3 - 12X^2 - X + 3$, iar în locul lui g, $18g = 2X^3 - X^2 - 18X + 9$ şi începem algoritmul.

(c) La al doilea pas va trebui să împărţiţi pe g la $(2+i)X^2+5X+2-4i$; nu faceţi asta din prima: înlocuiţi-l pe g cu $(2+i)g$ şi apoi continuaţi.

2. Pentru orice $n \in \mathbb{N}$, polinomul $X^2 - X + 1$ divide polinomul $X^{12n+2} - X^{6n+1} + 1$ în $\mathbb{C}[X]$.

Soluţie. Notăm $f = X^{12n+2} - X^{6n+1} + 1$ şi $g = X^2 - X + 1$. Observăm că rădăcinile lui g sunt simple ($\Delta \neq 0$), aşa că e suficient să arătăm că rădăcinile lui g se află printre cele ale lui f. Fie $\alpha \in \mathbb{C}$ cu $g(\alpha) = 0$.

Înmulţim egalitatea $\alpha^2-\alpha+1=0$ cu $\alpha+1$ şi obţinem $\alpha^3+1=0$ sau $\alpha^3=-1$; deci $\alpha^6=1$. Astfel,

$$\begin{aligned} f(\alpha) &= \alpha^{12n+2}-\alpha^{6n+1}+1=(\alpha^6)^{2n}\alpha^2-(\alpha^6)^n\alpha+1\\ &= \alpha^2-\alpha+1=0 \end{aligned}$$

3. Pentru orice $m,n\in\mathbb{N}^*$ avem următorarele proprietăţi în $k[X]$:
(a) $X^m-1\mid X^n-1$ dacă şi numai dacă $m\mid n$.
(b) $(X^m-1,X^n-1)=X^{(m,n)}-1$.

Soluţie. *(a)* Dacă $m\mid n$, $n=lm$, atunci

$$X^n-1=(X^m)^l-1=(X^m-1)(X^{m(l-1)}+\ldots+X^m+1)$$

şi deci $X^m-1\mid X^n-1$.
Reciproca reiese din *(b)*: dacă $X^m-1\mid X^n-1$, atunci $X^m-1\mid X^{(m,n)}-1$, de unde $m=(m,n)$ (din motive de grade), aşa că $m\mid n$.
(b) Să zicem că $m\leq n$. Atunci scriem $n=qm+r$, $0\leq r<m$, şi avem că

$$\begin{aligned} X^n-1 &= X^{qm+r}-X^r+X^r-1=X^r(X^{qm}-1)+X^r-1\\ &= X^r(X^m-1)((X^m)^{q-1}+\ldots+X^m+1)+X^r-1 \end{aligned}$$

iar $deg(X^r-1)<deg(X^m-1)$. Cu alte cuvinte, restul împărţirii lui X^n-1 la X^m-1 este X^r-1.
Astfel, continuând algoritmul lui Euclid pentru n şi m în $\mathbb{Z}$, obţinând resturile $r_1,r_2,\ldots$, în algoritmul lui Euclid pentru X^n-1 şi X^m-1 din $k[X]$ se contorizează resturile $X^{r_1}-1$, $X^{r_2}-1,\ldots$. În particular, ultimul rest nenul va fi $X^{r_j}-1$, r_j fiind ultimul rest nenul din algoritmul pentru n şi m, adică $r_j=(n,m)$.

Ca o aplicaţie, vedem:

4. Fie $f=X^{23}+X^{22}+\ldots+X+1$ şi $g=X^{15}+X^{14}+\ldots+X+1$ în $\mathbb{Q}[X]$. Să se determine (f,g).

Soluţie. Observăm că $(X-1)f=X^{24}-1$ şi $(X-1)g=X^{16}-1$, iar $((X-1)f,(X-1)g)\sim(X-1)(f,g)$ (sunt asociate în divizibilitate). Dar

$$\begin{aligned} ((X-1)f,(X-1)g) &= X^{(24,16)}-1=X^8-1\\ &= (X-1)(X^7+\ldots+X+1) \end{aligned}$$

(cf. ex. 2. *(b)*), şi deci $(f,g)=X^7+\ldots+X+1$.

Problema centrală, atât în $\mathbb{Z}$, cât şi în $k[X]$, e de a găsi criterii de primalitate, respectiv de ireductibilitate. În $k[X]$ aţi văzut criteriul cel mai important: cel al lui Eisenstein. Sunt multe alte criterii, însă nu trebuie mereu să săriţi imediat la acestea. De exemplu:

5. Să se cerceteze ireductibilitatea lui $f \in k[X]$ în următoarele cazuri:
(a) $f = X^4 + 1$, $k = \mathbb{Q}$, $k = \mathbb{R}$, $k = \mathbb{C}$, $k = \mathbb{F}_3$.
(b) $f = X^4 + 3X^2 + 2$, $k \in \{\mathbb{Q}, \mathbb{R}, \mathbb{C}\}$.
(c) $f = X^3 + X + \hat{3}$, $k = \mathbb{F}_5$.

Soluţie. *(a)* Observăm că

$$\begin{aligned} f &= X^4 + 2X^2 + 1 - 2X^2 = (X^2+1)^2 - (\sqrt{2}X)^2 \\ &= (X^2 + \sqrt{2}X + 1)(X^2 - \sqrt{2}X + 1) \\ &= (X - x_1)(X - x_2)(X - x_3)(X - x_4) \end{aligned}$$

unde $x_1 = \frac{-1-i}{\sqrt{2}}$, $x_3 = \frac{1-i}{\sqrt{2}}$, $x_2 = \overline{x}_1$, $x_4 = \overline{x}_3$. Deoarece f nu are rădăcini în $\mathbb{Q}$, acesta nu poate fi scris ca un produs $f = gh$ cu $deg(g) = 1$ şi $deg(h) = 3$, $g, h \in \mathbb{Q}[X]$, aşa că mai rămâne posibilitatea de a scrie f ca produs de polinoame de grad 2; însă această scriere a lui f e $(X^2+\sqrt{2}X+1)(X^2-\sqrt{2}X+1)$, iar aceste polinoame nu au coeficienţi în $\mathbb{Q}$. Aşadar, f este ireductibil peste $\mathbb{Q}$.
Scrierea $f = (X^2 + \sqrt{2}X + 1)(X^2 - \sqrt{2}X + 1)$ arată că, în schimb, f e reductibil în $\mathbb{R}[X]$. Mai mult, aceşti factori sunt ireductibili în $\mathbb{R}[X]$, căci discriminantul lor e $-2 < 0$. Apoi, f e reductibil în $\mathbb{C}[X]$ având descompunerea $f = (X-x_1)(X-\overline{x}_1)(X-x_3)(X-\overline{x}_3)$ (aşa cum asigură teorema funadamentală a algebrei).
În fine, peste $\mathbb{F}_3 = \frac{\mathbb{Z}}{3\mathbb{Z}}$ avem

$$\begin{aligned} X^4 + \hat{1} &= X^4 + \hat{2}^2 = X^4 + \hat{4}X^2 + \hat{2}^2 - \hat{4}X^2 = (X^2+\hat{2})^2 - (\hat{2}X)^2 \\ &= (X^2 - \hat{2}X + \hat{2})(X^2 + \hat{2}X + \hat{2}) = (X^2 + X + \hat{2})(X^2 + \hat{2}X + \hat{2}) \end{aligned}$$

iar $X^2 + X + \hat{2}$ şi $X^2 + \hat{2}X + \hat{2}$ sunt ireductibile peste $\mathbb{F}_3$ căci nu au rădăcini în $\mathbb{F}_3$.

(c) Observăm că $f(\hat{1}) = \hat{0}$, şi deci $f = (X-\hat{1})g = (X+\hat{4})g$, pentru un $g \in \mathbb{F}_5[X]$. Atunci $3 = deg(f) = deg(g)+1$, şi scriem $g = \hat{a}X^2+\hat{b}X+\hat{c}$. Avem

$$\begin{aligned} X^3 + X + \hat{3} &= (X + \hat{4})(\hat{a}X^2 + \hat{b}X + \hat{c}) \\ &= \hat{a}X^3 + \widehat{b + 4a}X^2 + \widehat{4b + c}X + \hat{4}c \end{aligned}$$

de unde $\hat{a} = \hat{1}$, $\hat{b}+4\hat{a} = 0$ (şi deci $\hat{b} = \hat{1}$) şi $4\hat{b}+\hat{c} = \hat{1}$ (deci $\hat{c} = -\hat{3} = \hat{2}$). Astfel, $f = (X + \hat{4})(X^2 + X + \hat{2})$. Însă g e de grad 2 şi nu are rădăcini în $\mathbb{F}_5$: $g(\hat{0}) = \hat{2}$, $g(\hat{1}) = \hat{4}$, $g(\hat{2}) = \hat{3}$, $g(\hat{3}) = \hat{4}$ şi $g(\hat{4}) = \hat{2}$. Aşadar, f e reductibil, iar $f = (X + \hat{4})(X^2 + X + \hat{2})$ e descompunerea sa în factori ireductibili peste $\mathbb{F}_5$.

6. Polinomul $f = X^4 + X^3 - X^2 + X + \hat{1}$ e ireductibil în $\mathbb{F}_2[X]$.

Soluţie. Să presupunem că avem $f = gh$, cu $g, h \in \mathbb{F}_2[X]$, $deg(g) \geq 1$ şi $deg(h) \geq 1$. Observăm că f nu are rădăcini în $\mathbb{F}_2$, aşa că trebuie să avem $deg(g) \neq 1$ şi $deg(h) \neq 1$. Atunci scriem $g = X^2 + aX + b$ şi $h = X^2 + cX + d$ (fiind peste $\mathbb{F}_2$, g şi h sunt monice automat, neavând gradul 1) şi avem

$$X^4 + X^3 + X^2 + X + \hat{1} = X^4 + (a + c)X^3 + (ac + d + b)X^2 + (bc + ad)X + bd$$

Astfel,
$$\begin{cases} bd = \hat{1} \\ bc + ad = \hat{1} \\ ac + b + d = \hat{1} \\ a + c = \hat{1} \end{cases}$$
Din prima obţinem $b = d = \hat{1}$ şi deci a treia oferă $ac = \hat{1}$, de unde $a = c = \hat{1}$, aşa că a patra oferă contradicţia $\hat{0} = \hat{1}$.

De precizat că, în general, dacă un polinom nu are rădăcini, nu rezultă neapărat că e ireductibil. De exemplu, $X^4 + X^2 + \hat{1}$ nu are rădăcini în $\mathbb{F}_2$, însă e clar reductibil: $X^4 + X^2 + \hat{1} = (X^2 + X + \hat{1})^2$ ($char = 2$). Totuşi, implicaţia e adevărată când gradul polinomului e 2 sau 3 (evident, cele de grad 1 având mereu o rădăcină).

Până acum am folosit doar definiţia. Ne uităm la:

7. Următoarele polinoame sunt ireductibile în $\mathbb{Q}[X]$:
(a) $f = X^n - 2$, $n \in \mathbb{N}$
(b) $f = X^{p-1} + X^{p-2} + \ldots + X + 1$, $p \in \mathbb{N}$ fiind prim.

Soluţie. *(a)* Observăm că $2 \mid -2$, $2^2 \nmid -2$ şi $2 \nmid 1$. Cum 2 e prim în $\mathbb{Z}$, criteriul Eisenstein spune că $X^n - 2$ e ireductibil în $\mathbb{Q}[X]$.
(b) Încă o dată, dacă suntem în cadrul unei teorii, nu facem distincţie între două obiecte izomorfe: orice fenomen petrecut într-un obiect, are loc şi în celălalt, şi invers.

Aici observăm automorfismul de $\mathbb{Q}$ - algebră $\varphi : \mathbb{Q}[X] \to \mathbb{Q}[X]$, dat prin $\varphi(X) = X + 1$, $\varphi|_{\mathbb{Q}} = id_{\mathbb{Q}}$. Într-adevăr, φ^{-1} există : e dat prin $\varphi^{-1}(X) = X - 1$ (φ e doar o translaţie...). Astfel, f e ireductibil dacă şi numai dacă $\varphi(f)$ e ireductibil. Dar

$$\begin{aligned}\varphi(f) = \varphi(\frac{X^p - 1}{X - 1}) &= \frac{(X+1)^{p-1} - 1}{X} \\ &= X^{p-1} + C_p^1 X^{p-2} + \ldots + C_p^i X^{p-i-1} + \ldots + C_p^{p-1}\end{aligned}$$

(φ se extinde evident la $\mathbb{Q}(X)$), iar pentru orice $1 \leq i \leq p-1$, avem $p \mid C_p^i$ (din formula $i(i-1)\ldots 1 \cdot C_p^i = p(p-1)\ldots(p-i+1)$ şi din faptul că p e prim - cf. Seminar 11, ex. 4), $p^2 \nmid C_p^{p-1} = p$ şi $p \nmid 1$. Aşadar, criteriul Eisenstein spune că $\varphi(f)$ e ireductibil în $\mathbb{Q}[X]$.

Iată un alt criteriu:

Teoremă (Criteriul reducţiei). Fie A un inel comutativ (unitar) şi $\varphi : \mathbb{Z} \to A$ un morfism de inele. Acesta se extinde la morfismul $\overline{\varphi} : \mathbb{Z}[X] \to A[X]$, prin $\overline{\varphi}(a_0 + a_1 X + \ldots + a_n X^n) = \varphi(a_0) + \varphi(a_1)X + \ldots + \varphi(a_n)X^n$. Dat un $f \in \mathbb{Z}[X]$, dacă $\overline{\varphi}(f)$ e ireductibil în $A[X]$ şi $deg(\overline{\varphi}(f)) = deg(f)$, atunci f e ireductibil în $\mathbb{Q}[X]$.

De obicei, testarea se face pentru un morfism canonic $\mathbb{Z} \to \frac{\mathbb{Z}}{p\mathbb{Z}}$.

Dacă până acum s-a pus în evidenţă legătura aritmetică dintre $\mathbb{Z}$ şi inelele $k[X]$, trebuie să fim conştienţi că, atunci când $k = \mathbb{C}$, intervine şi ciclotomia în aceste aspecte aritmetice.

Ne amintim că pentru orice $n \in \mathbb{N}^*$, μ_n notează grupul rădăcinilor de ordin n ale unităţii din $\mathbb{C}$. Probabil aţi văzut în semestrul 1 următorul rezultat:

Teoremă. Pentru $m, n \in \mathbb{N}^*$ oarecare, avem:
(a) $\mu_m \subseteq \mu_n \Leftrightarrow m \mid n$
(b) $\mu_m \cap \mu_n = \mu_{(m,n)}$.

Acum, luând în discuţie polinomul $X^n - 1 \in \mathbb{Z}[X]$, *(a)* şi *(b)* din teorema anterioară se traduc exact în *(a)* şi *(b)* din ex. 3 (într-adevăr, rădăcinile din $\mathbb{C}$ ale lui $X^n - 1$ sunt exact elementele lui μ_n).

Pentru $n \in \mathbb{N}^*$, vom nota cu P_n mulţimea rădăcinilor primitive de ordin n ale unităţii (generatorii lui μ_n). Polinomul

$$\Phi_n = \prod_{\zeta \in P_n} (X - \zeta)$$

se numeşte al n-lea polinom ciclotomic (se numeşte astfel pentru că "ciclotomie" înseamnă diviziune circulară, şi avem în vedere interpretarea geometrică a elementelor lui μ_n: sunt vârfurile unui poligon regulat înscris în cercul unitate).

Continuăm data viitoare pe acest drum sublim deschis de către Gauss, anume cel dat de metodele ciclotomice.