CURS 10

Divizibilitatea în inele de polinoame

Câteva aspecte legate de divizibilitatea polinoamelor au apărut în exemplele şi exerciţiile rezolvate din cursurile anterioare. În acest curs pornim de la premisa că toate acestea sunt cunoscute şi vom încerca să le adăgăm câteva chestiuni de detaliu aferente acestei teme. Un obiectiv, deja promis, al acestui curs este de a arăta că $\mathbb{Z}[X]$ e un domeniu factorial care nu e domeniu cu ideale principale.

Fie R un domeniu de integritate. Să începem prin a reaminti (din cursul 4) că $R[X]$ este, de asemenea, domeniu de integritate, iar elementele inversabile din $R[X]$ coincid cu elementele din R inversabile în R. Ca urmare, două polinoame $f, g \in R[X]$ sunt asociate în divizibilitate dacă şi numai dacă există un element $a \in R^*$ inversabil în R astfel încât $f = ag$.

Observaţiile 1. a) Folosind distributivitatea înmulţirii faţă de adunare în $R[X]$, rezultă că dacă $b \in R$ şi $f = a_0 + a_1X + \cdots + a_nX^n \in R[X]$, atunci

$$b \mid f \Leftrightarrow b \mid a_i,\ \forall i \in \{0, \ldots, n\}.$$

b) Cum $U(R[X]) = U(R)$, se deduce imediat că dacă $a \in R^*$ este element ireductibil în R, atunci elementul a este ireductibil şi în $R[X]$.
c) Dacă $p \in R^*$ este element prim în R, atunci p este prim şi în $R[X]$.

Într-adevăr, dacă $f = a_0 + a_1X + \cdots + a_nX^n$, $g = b_0 + b_1X + \cdots + b_mx^m$ sunt polinoame din $R[X]$ şi $p \nmid f$ şi $p \nmid g$, atunci există coeficienţi ai lui f şi coeficienţi ai lui g care nu se divid cu p. Fie a_k şi b_l coeficienţii cu cei mai mici indici care nu se divid cu p. Cum p este prim în R, avem, de asemenea, $p \nmid a_kb_l$. Prin urmare, coeficientul lui fg

$$c_{k+l} = a_0b_{k+l} + a_1b_{k+l-1} + \cdots + a_kb_l + \cdots + a_{k+l}b_0$$

nu se divide cu p deoarece $p \nmid a_kb_l$ şi toţi ceilalţi termeni se divid cu p. Deci fg nu se divide cu p.

Definiţia 2. Fie R un domeniu factorial. Un polinom $\varphi \in R[X]$ se numeşte **polinom primitiv** dacă cel mai mare divizor comun al coeficienţilor săi este 1. Dacă $f \in R[X]$ este nenul şi a este cel mai mare divizor comun al coeficienţilor lui f, atunci

$$f = a\varphi \tag{1}$$

unde φ este un polinom primitiv. O reprezentare de forma (1) a lui f se numeşte **canonică**.

Observaţiile 3. a) Un polinom asociat cu un polinom primitiv este primitiv.
b) Un polinom de gradul zero este primitiv dacă şi numai dacă este inversabil. Ca urmare, dacă K este un corp comutativ, atunci orice polinom nenul din $K[X]$ este primitiv.
c) Polinomul primitiv φ şi elementul $a \in R$ din (1) sunt unic determinate până la o asociere.

Într-adevăr, dacă avem şi $f = a'\varphi'$ cu $a' \in R$ şi φ' primitiv, atunci din $a\varphi = a'\varphi'$ rezultă că a' este un divizor comun al coeficienţilor lui f. Deci $a' \mid a$, adică $a = ua'$ cu $u \in R$. Întrucât $R[X]$ este domeniu de integritate urmează că $\varphi' = u\varphi$ de unde, în baza faptului că φ' este primitiv, deducem că u este inversabil şi de aici că $\varphi \sim \varphi'$ şi $a \sim a'$.

Lema 4. (**Lema lui Gauss**) Dacă R este un domeniu factorial, atunci produsul a două polinoame primitive din $R[X]$ este un polinom primitiv.

Demonstraţie. Fie $\varphi_1, \varphi_2 \in R[X]$ polinoame primitive şi $\varphi = \varphi_1\varphi_2$. Dacă φ nu ar fi primitiv, atunci ar exista $d \in R$ neinversabil care să fie un divizor comun al tuturor coeficienţilor lui φ. Domeniul R fiind factorial, elementul d are o descompunere în factori ireductibili. Fie p este unul dintre aceşti factori. Atunci p este şi prim şi din $p \mid \varphi_1\varphi_2$ rezultă că $p \mid \varphi_1$ sau $p \mid \varphi_2$. Ţinând cont de observaţia 1 a), aceasta contrazice faptul că φ_1 şi φ_2 sunt polinoame primitive. □

Corolarul 5. a) Dacă $f_1, f_2 \in R[X]$ şi $f_1 = a_1\varphi_1$, $f_2 = a_2\varphi_2$ sunt reprezentări canonice ale lui f_1 şi f_2, iar $a = a_1a_2$, $\varphi = \varphi_1\varphi_2$, atunci $f_1f_2 = a\varphi$ este o reprezentare canonică a lui f_1f_2.
b) Dacă $f \in R[X]$ şi notăm cu $c(f)$ cel mai mare divizor comun al coeficienţilor lui f, corolarul anterior ne arată că $c(f_1f_2) = c(f_1)c(f_2)$.
c) Dacă $a_1, a_2 \in R^*$ şi $\varphi_1, \varphi_2 \in R[X]$ sunt polinoame primitive, atunci

$$a_1\varphi_1 \mid a_2\varphi_2 \Leftrightarrow a_1 \mid a_2 \text{ şi } \varphi_1 \mid \varphi_2.$$

La finalul cursului anterior am văzut că dacă K este un corp comutativ, domeniul de integritate $K[X]$, împreună cu funcţia grad, este un domeniu euclidian (deci şi domeniu cu ideale principale şi domeniu factorial). Acest fapt rezultă din **teorema împărţirii cu rest pentru polinoame cu coeficieţi într-un corp comutativ** K: *pentru orice polinoame* $f, g \in K[X]$, $g \neq 0$, *există două polinoame* $q, r \in K[X]$ *unic determinate astfel încât* $f = gq + r$ *şi* $\operatorname{grad} r < \operatorname{grad} g$.

Dar dacă domeniul de integritate R peste care se constuieşte domeniul de integritate $R[X]$ nu este corp? Cu siguranţa domeniul $R[X]$ nu mai este euclidian, pentru că aşa cum rezultă din teorema următoare, nu este un domeniu cu ideale principale.

Teorema 6. Dacă R este domeniu de integritate şi R nu este corp, atunci $R[X]$ are ideale care nu sunt principale.

Demonstraţie. Întrucât domeniul de integritate R nu este corp rezultă că există $a \in R^*$ neinversabil. Să presupunem prin reducere la absurd că idealul (a, X) este principal, adică există $f \in R[X]$ astfel încât $(a, X) = (f) = fR[X]$. Rezultă că $f \mid a$ şi $f \mid X$. Din $f \mid a$ deducem că $f \in R$, ceea ce împreună cu $f \mid X$, implică f inversabil (deoarece X este ireductibil). Conform cu propoziţia 5 ii), avem $(f) = R[X]$ şi, implicit, $(a, X) = R[X]$. Cum $1 \in R[X]$ se deduce că

$$\exists g, h \in R[X] : \ ag + Xh = 1.$$

Dacă b_0 este termenul liber al lui g atunci termenul liber al polinomului $ag + Xh$ este ab_0, prin urmare, $ab_0 = 1$, ceea ce contrazice alegerea lui a ca fiind neinversabil.

Contradicţia infirmă presupunerea că idealul (a, X) este principal. Prin urmare, idealul (a, X) nu este principal, ceea ce completează demonstraţia teoremei. □

Corolarul 7. Inelul $\mathbb{Z}[X]$ al polinoamelor cu coeficienţi întregi este un domeniu de integritate care are ideale care nu sunt principale.

Dar *dacă domeniul R este factorial atunci inelul $R[X]$ este, de asemenea, un domeniu factorial.* Demonstrarea acestei proprietăţi generale trece prin inelul polinoamelor cu coeficienţi în corpul fracţiilor domeniului de integritate R. Din raţiuni de spaţiu, dar şi pentru că utilitatea principală pe care o dăm acestui rezultat se va referi la $\mathbb{Z}[X]$, vom continua prezentarea analizând, în principal, inelul $\mathbb{Z}[X]$ (care între inele de polinoame cu coeficienţi numerici este singurul pentru care inelul coeficienţilor nu este corp). Prin exerciţii rezolvate, vom începe prin a arăta că acesta este factorial şi vom continua cu câteva proprietăţi referitoare la elementele sale ireductibile (= prime).

Exerciţiul 1. Fie $f \in \mathbb{Z}[X]$ cu grad $f \geq 1$. Să se arate că f este ireductibil în $\mathbb{Z}[X]$ dacă şi numai dacă f este ireductibil în $\mathbb{Q}[X]$ şi primitiv în $\mathbb{Z}[X]$.

Soluţie: Folosind definiţia ireductibilităţii şi definiţia polinoamelor primitive, din f ireductibil în $\mathbb{Q}[X]$ şi primitiv în $\mathbb{Z}[X]$ rezultă imediat f ireductibil în $\mathbb{Z}[X]$.

Reciproc, din f ireductibil în $\mathbb{Z}[X]$ rezultă că c.m.m.d.c. al coeficienţilor lui f (în $\mathbb{Z}$) este 1, adică f este primitiv în $\mathbb{Z}[X]$. Dacă $q_1, q_2 \in \mathbb{Q}[X]$ şi

$$f = q_1 q_2, \tag{2}$$

iar $b_i \in \mathbb{Z}$ $(i = 1, 2)$ e un multiplu comun al numitorilor coeficienţilor lui q_i, atunci putem scrie

$$q_1 = \frac{a_1}{b_1} h_1 \text{ şi } q_2 = \frac{a_2}{b_2} h_2 \tag{3}$$

unde $a_1, a_2 \in \mathbb{Z}$ şi $h_1, h_2 \in \mathbb{Z}[X]$ sunt primitive în $\mathbb{Z}[X]$. Din (2) şi (3) rezultă că în $\mathbb{Z}[X]$ avem:

$$b_1 b_2 f = a_1 a_2 h_1 h_2.$$

Din lema lui Gauss rezultă că $h_1 h_2$ este primitiv în $\mathbb{Z}[X]$. Şi f este primitiv în $\mathbb{Z}[X]$. Ca urmare, c.m.m.d.c. al coeficienţilor polinomului din membrul stâng este $b_1 b_2$ şi c.m.m.d.c. al coeficienţilor polinomului din membrul drept este $a_1 a_2$. Deducem că $a_1 a_2 = b_1 b_2$ sau $a_1 a_2 = -b_1 b_2$, ceea ce implică $f = \pm h_1 h_2$. Acum, din ipoteza f ireductibil în $\mathbb{Z}[X]$ rezultă că sau h_1 sau h_2 este inversabil în $\mathbb{Z}[X]$, adică $h_1 \in \{-1, 1\}$ sau $h_2 \in \{-1, 1\}$. Deci $q_1 \in \mathbb{Q}^*$ sau $q_2 \in \mathbb{Q}^*$ şi astfel am arătat că f este ireductibil în $\mathbb{Q}[X]$.

Exerciţiul 2. Să se arate că $\mathbb{Z}[X]$ este un domeniu factorial.

Soluţie: Folosim teorema 9 şi observaţia 11 b) din cursul 8. Dacă în şirul de polinoame nenule

$$f_1, f_2, \ldots, f_n, \ldots \tag{4}$$

$f_{n+1} \mid f_n$ $(n = 1, 2, \ldots)$ şi $f_n = a_n \varphi_n$ $(n = 1, 2, \ldots)$ sunt reprezentările canonice ale acestor polinoame, atunci în şirurile

$$a_1, a_2, \ldots, a_n, \ldots \tag{5}$$

$$\varphi_1, \varphi_2, \ldots, \varphi_n, \ldots \tag{6}$$

fiecare element se divide prin următorul. Întrucât $\mathbb{Z}$ este factorial rezultă că există un $n_1 \in \mathbb{N}^*$ astfel încât pentru $n \geq n_1$ termenii şirului (5) să fie asociaţi. Din $\varphi_{n+1} \mid \varphi_n$ urmează că

$$\operatorname{grad} \varphi_1 \geq \operatorname{grad} \varphi_2 \geq \cdots \geq \operatorname{grad} \varphi_n \geq \ldots.$$

Deci există un $n_2 \in \mathbb{N}$ astfel încât pentru $n \geq n_2$ termenii şirului (6) să aibă acelaşi grad, adică diferă unul de altul prin factori din $\mathbb{Z}^*$. Dar aceşti factori sunt elemente inversabile din $\mathbb{Z}^*$ deoarece termenii şirului (6) sunt polinoame primitive. Rezultă că pentru $n \geq \max\{n_1, n_2\}$ termenii şirului (4) sunt polinoame asociate. Deci conform observaţiei 11 b) din cursul 8, condiţia 1) din teorema 9 din cursul 9 este verificată.

Pentru a finaliza problema este suficient să mai arătăm că orice polinom ireductibil $f \in \mathbb{Z}[X]$ este prim. Dacă $f \in \mathbb{Z}$ atunci, întrucât $\mathbb{Z}$ este factorial, rezultă că f este prim în $\mathbb{Z}$, de unde (conform observaţiei 3 c) urmează că f este prim în $\mathbb{Z}[X]$. Dacă $f \in \mathbb{Z}[X] \setminus \mathbb{Z}$, atunci grad $f \geq 1$ şi f este primitiv. Din exerciţiul anterior rezultă că f este ireductibil în $\mathbb{Q}[X]$, iar cum $\mathbb{Q}[X]$ este

factorial deducem că f este prim în $\mathbb{Q}[X]$. Prin urmare dacă $f \mid g_1 g_2$ cu $g_1, g_2 \in \mathbb{Z}[X]$ atunci $f \mid g_1$ sau $f \mid g_2$ în $\mathbb{Q}[X]$.

Să considerăm că $f \mid g_1$ în $\mathbb{Q}[X]$. Rezultă că există $q_1 \in \mathbb{Q}[X]$ astfel încât $g_1 = fq_1$. Fie $g_1 = bg_1'$ cu $b \in \mathbb{Z}$ un c.m.m.d.c. al coeficienţilor întregi ai lui g_1. Evident $g_1' \in \mathbb{Z}[X]$ este primitiv. Luăm, de asemenea, $a \in \mathbb{Z}$ un multiplu comun al numitorilor coeficienţilor lui q_1 şi $c \in \mathbb{Z}$ c.m.m.d.c. al coeficienţilor lui $aq_1 \in \mathbb{Z}$. Atunci $aq_1 = cq_1'$ cu $q_1' \in \mathbb{Z}[X]$ primitiv şi

$$abg_1' = cfq_1'. \tag{7}$$

Polinoamele g_1' şi fq_1' sunt primitive şi în (7) avem două reprezentări canonice în $\mathbb{Z}[X]$ ale aceluiaşi polinom cu coeficienţi întregi. Prin urmare, $g_1' \sim fq_1'$ în $\mathbb{Z}[X]$. Rezultă că f divide pe g_1' şi, implicit, pe g_1 în $\mathbb{Z}[X]$. Deci f e prim în $\mathbb{Z}[X]$.

Observaţiile 8. a) Inelul $\mathbb{Z}[X]$ este un exemplu de domeniu factorial care nu este un domeniu cu ideale principale.
b) Corpul $\mathbb{Q}$ este cel mai mic corp în care poate fi scufundat domeniul de integritate $\mathbb{Z}$, adică e corpul fracţiilor lui $\mathbb{Z}$. Demonstraţia faptului că $R[X]$ este factorial când R e un domeniu factorial urmează, fără modificări majore, raţionamentul din soluţiile exerciţiilor 2 şi 3, rolul lui $\mathbb{Q}$ fiind preluat de corpul fracţiilor lui R.

Exerciţiul 3. (**Criteriul lui Eisenstein**) Fie $n \in \mathbb{N}^*$ şi

$$f = a_0 + \cdots + a_{n-1}X^{n-1} + a_nX^n \in \mathbb{Z}[X]$$

un polinom primitiv. Să se arate că dacă există un număr prim p cu proprietatea că

$$p \,|\, a_0, \ldots, p \,|\, a_{n-1} \text{ şi } p^2 \nmid a_0$$

atunci polinomul f este ireductibil peste $\mathbb{Z}$ (şi peste $\mathbb{Q}$).

Soluţie: Cum f este primitiv şi $p \mid a_0, \ldots, p \mid a_{n-1}$ avem $a_n \neq 0$ şi $p \nmid a_n$, deci $\operatorname{grad} f \geq 1$ de unde rezultă că f este neinversabil. Să presupunem că $f = gh$, cu polinoamele

$$g = b_0 + b_1X + \cdots + b_mX^m \text{ şi } h = c_0 + c_1X + \cdots + c_pX^p,$$

neinversabile în $\mathbb{Z}[X]$ ($b_0, \ldots, b_m, c_0, \ldots, c_p \in \mathbb{Z},\ m, p \in \mathbb{N},\ b_m \neq 0 \neq c_p,\ m + p = n$). Dacă am avea $m = 0$, cum $g = b_0$ este neinversabil în $\mathbb{Z}$, $b_0 \mid f$ implică $b_0 \mid (a_0, \ldots, a_n) = 1$, contradicţie.

Aşadar, $m \geq 1$ şi, din aceleaşi motive, $p \geq 1$ şi avem

$$b_0c_0 = a_0,\ b_1c_0 + b_0c_1 = a_1,\ b_2c_0 + b_1c_1 + b_0c_2 = a_2, \ldots,\ b_mc_p = a_n. \tag{8}$$

Cum p este prim şi $p \mid a_0 = b_0c_0$ avem $p \mid b_0$ sau $p \mid c_0$. Dar $p^2 \nmid a_0$. Rezultă că dacă $p \mid b_0$ atunci $p \nmid c_0$, iar dacă $p \mid c_0$ atunci $p \nmid b_0$. Să considerăm că $p \mid b_0$ şi $p \nmid c_0$. Din $p \mid a_1 = b_1c_0 + b_0c_1$ şi $p \mid b_0$ deducem că $p \mid b_1c_0$, iar cum $p \nmid c_0$, avem $p \mid b_1$. Similar, din a treia egalitate din (8), cum $p \mid b_0$, $p \mid b_1$ şi $p \nmid c_0$ rezultă $p \mid b_2$. Procedând analog şi cu celelalte egalităţi din (8), şi din a $(m+1)$-a egalitate deducem că $p \mid b_m$, deci $p \mid a_n = b_mc_p$, ceea ce contrazice faptul că $(a_0, \ldots, a_{n-1}, a_n) = 1$.

Ireductibilitatea peste $\mathbb{Q}$ rezultă folosind exerciţiul 1.

Observaţia 9. a) Folosind criteriul lui Eisenstein cu $p = 2$ rezultă că pentru orice $n \in \mathbb{N}^*$, polinomul $f = X^n + 2$ este ireductibil în $\mathbb{Z}[X]$ deci şi în $\mathbb{Q}[X]$. Dacă $p \in \mathbb{Z}$ este prim atunci p este ireductibil în $\mathbb{Z}[X]$, dar nu este ireductibil în $\mathbb{Q}[X]$.

b) Dacă polinoamele ireductibile din $\mathbb{C}[X]$ sunt polinoamele de gradul 1 şi în $\mathbb{R}[X]$ nu există polinoame ireductibile de grad mai mare decât 2 (vezi exerciţiul 2 din cursul 7), observaţia anterioară ne arată că în $\mathbb{Q}[X]$ există polinoame ireductibile de orice grad $n \in \mathbb{N}^*$ (şi nu există polinoame ireductibile de grad 0), iar în $\mathbb{Z}[X]$ există polinoame ireductibile de orice grad $n \in \mathbb{N}$.

Exerciţiul 4. a) Fie R, R' domenii de integritate şi $\psi : R \to R'$ un izomorfism de inele. Să se arate că $p \in R$ este element ireductibil (prim) în R dacă şi numai dacă $\psi(p)$ este element ireductibil (prim) în R'.
b) Fie R un domeniu de integritate, $a, b \in R$, a inversabil şi $f \in R[X]$. Să se arate că f este ireductibil dacă şi numai dacă $f(aX + b)$ este ireductibil.

Soluţie: a) Fie $a, x, y \in R$. Cum avem

$$a = xy \Leftrightarrow \psi(a) = \psi(x)\psi(y)$$

şi orice izomorfism de inele cu unitate este unital, luând $a = 1$, rezultă că x este inversabil în R dacă şi numai dacă $\psi(x)$ este inversabil în R'. Aşadar, p este nenul şi neinversabil dacă şi numai dacă $\psi(p)$ este nenul şi neinversabil în R'.

Dacă $p \in R$ este ireductibil şi $\psi(p) = x'y'$ cum ψ este izomorfism, există $x, y \in R$, unic determinate, astfel încât $\psi(x) = x'$ şi $\psi(y) = y'$. Evident, $x = \psi^{-1}(x')$ şi $y = \psi^{-1}(y')$ şi

$$\psi(p) = x'y' = \psi(x)\psi(y) \Rightarrow p = xy \overset{p \text{ ireductibil}}{\Longrightarrow} x \in U(R) \text{ sau } y \in U(R).$$

Cum ψ conservă elementele inversabile, rezultă că $x' = \psi(x)$ e inversabil în R' sau $y' = \psi(y)$ e inversabil în R'. Deci $\psi(p)$ este element ireductibil.

Dacă $p \in R$ este un element prim şi $\psi(p) \mid x'y'$ (cu $x', y' \in R'$), atunci există $z' \in R'$ astfel încât $\psi(p)z' = x'y'$. Aplicăm izomorfismul ψ^{-1} şi rezultă $p \mid \psi^{-1}(x')\psi^{-1}(y') = xy$ în R. De aici se deduce că $p \mid x$ sau $p \mid y$. Dacă $p \mid x$, aplicând ψ, rezultă că $\psi(p) \mid \psi(x) = x'$, iar dacă $p \mid y$, atunci $\psi(p) \mid \psi(y) = y'$. Deci $\psi(p)$ este element prim.

Reciprocele se obţin înlocuind izomorfismul ψ cu ψ^{-1}.
b) Se verifică uşor (fie direct, fie folosind proprietatea de universalitate a inelului de polinoame $R[X]$) că $f \mapsto f(aX + b)$ este o corespondenţă care furnizează un endomorfism al domeniului $R[X]$ şi că acest endomorfism este o bijecţie (deci e un automorfism) pentru care inversa e dată de corespondenţa $f \mapsto f(a^{-1}X - a^{-1}b)$. În continuare se aplică punctul a).

Exerciţiul 5. Fie p un număr prim. Să se arate că polinomul

$$f = X^{p-1} + X^{p-2} + \cdots + X + 1 \in \mathbb{Z}[X]$$

este ireductibil peste $\mathbb{Q}$.

Soluţie: Arătăm că $f = \dfrac{X^p - 1}{X - 1}$ este ireductibil peste $\mathbb{Z}$, deci şi peste $\mathbb{Q}$. Din problema anterioară avem f ireductibil în $\mathbb{Z}[X]$ dacă şi numai dacă

$$f(X + 1) = \frac{(X + 1)^p - 1}{(X + 1) - 1} = X^{p-1} + \sum_{k=1}^{p-1} \mathsf{C}_p^k X^{p-k} + p$$

este ireductibil în $\mathbb{Z}[X]$. Ştim că $\mathsf{C}_p^k = \dfrac{p(p-1)\cdots(p-k+1)}{k!} \in \mathbb{N}$ şi, pentru că p este prim, dacă $1 \leq k \leq p-1$, atunci $(p, k!) = 1$. Din aceste motive, rezultă $k! \mid (p-1)\cdots(p-k+1)$, deci $p \mid \mathsf{C}_p^k$.

Aşadar $p \mid \mathsf{C}_p^1, \ldots, p \mid \mathsf{C}_p^p - 1$, $p \mid p$. Dar $p^2 \nmid p$, deci, conform criteriului lui Eisenstein, $f(X+1)$ este ireductibil în $\mathbb{Z}[X]$.