

## CURSUL 7: DIVIZIBILITATE ÎN $\mathbb{Z}$ ȘI ÎN $k[X]$

G. MINCU

În acest curs,  $k$  va desemna un corp comutativ.

### 1. TEOREME DE ÎMPĂRȚIRE CU REST

**Teorema 1 (Teorema împărțirii cu rest în  $\mathbb{Z}$ ).** *Pentru orice  $a, b \in \mathbb{Z}$  cu  $b \neq 0$  există și sunt unice  $q, r \in \mathbb{Z}$  cu proprietățile  $a = bq + r$  și  $0 \leq r < |b|$*

*Demonstrație:*

**Existența:** Fie  $r = a - bq$  cel mai mic număr întreg  $\geq 0$  de forma  $a - bx$  cu  $x \in \mathbb{Z}$ . Dacă  $a - bq \geq |b|$ , atunci  $0 \leq a - b(q + \text{sgn}(b)) < a - bq$ , contradicție.

**Unicitatea:** Fie  $q, r, q', r' \in \mathbb{Z}$  astfel încât  $a = bq + r = bq' + r'$  și  $0 \leq r, r' < |b|$ . Scăzând cele două expresii ale lui  $a$  rezultă  $b(q - q') = r' - r$ , deci  $r' - r = 0$  deoarece  $|r' - r| < |b|$ . Așadar  $r' = r$ , iar din egalitatea  $b(q - q') = 0$  și din  $b \neq 0$  rezultă  $q' = q$ .

**Teorema 2 (Teorema împărțirii cu rest în  $k[X]$ ).** *Fie  $f, g \in k[X]$ ,  $g \neq 0$ . Atunci, există și sunt unice  $q, r \in k[X]$  cu proprietățile  $f = gq + r$  și  $\text{grad } r < \text{grad } g$ .*

*Demonstrație:*

**Existența:** Facem inducție după gradul lui  $f$ ; vom nota cu  $a_f$  și  $a_g$  coeficienții dominanți ai polinoamelor  $f$ , respectiv  $g$ . Dacă  $\text{grad } f < \text{grad } g$ , luăm  $q = 0$  și  $r = f$ . Dacă  $\text{grad } f \geq \text{grad } g$ , există, conform ipotezei de inducție,  $q_1, r_1 \in k[X]$  astfel încât  $f - a_f a_g^{-1} X^{\text{grad } f - \text{grad } g} g = gq_1 + r_1$  și  $\text{grad } r_1 < \text{grad } g$ . Luăm  $q = a_f a_g^{-1} X^{\text{grad } f - \text{grad } g} + q_1$  și  $r = r_1$ .

**Unicitatea:** Fie  $q, r, q', r' \in k[X]$  astfel încât  $f = gq + r = gq' + r'$  și  $\text{grad } r, \text{grad } r' < \text{grad } g$ . Din primele relații rezultă  $(q - q')g = r' - r$ ; gradul membrului drept al acestei relații fiind mai mic decât  $\text{grad } g$ , rezultă  $q = q'$ . Înlocuind în ultima relație, obținem și  $r = r'$ .

**Corolarul 3.** Orice ideal al lui  $\mathbb{Z}$  este principal.

Orice ideal al lui  $k[X]$  este principal.

## 2. DIVIZIBILITATE

**Definiția 4.** Fie  $R$  un domeniu de integritate și  $a, b \in R$ . Spunem că  $a$  **divide**  $b$  în  $R$  (și scriem  $a|_R b$  sau, dacă nu este pericol de confuzie,  $a|b$ ) dacă există  $c \in R$  astfel încât  $b = ac$ .

**Propoziția 5.** Fie  $R$  un domeniu de integritate și  $a, b, c \in R$ . Atunci:

- i)  $a|_R b$  dacă și numai dacă  $bR \subset aR$ .
- ii) Dacă  $a|b$  și  $b|c$ , atunci  $a|c$ .
- iii) Dacă  $a|b$ , atunci  $a|bc$ .
- iv) Dacă  $a|b$  și  $a|c$ , atunci  $a|b + c$ .

**Definiția 6.** Fie  $R$  un domeniu de integritate și  $a, b \in R$ . Spunem că  $a$  **divide**  $b$  (și scriem  $a|b$ ) **în**  $R$  dacă există  $c \in R$  astfel încât  $b = ac$ .

**Definiția 7.** Fie  $R$  un domeniu de integritate și  $a, b \in R$ . Spunem că  $a$  și  $b$  sunt asociate în divizibilitate (și notăm  $a \sim_R b$  sau, dacă nu este pericol de confuzie,  $a \sim b$ ) dacă  $a|_R b$  și  $b|_R a$ .

**Propoziția 8.** Fie  $R$  un domeniu de integritate și  $a, b \in R$ . Atunci,  $a \sim_R b$  dacă și numai dacă există  $u \in U(R)$  astfel încât  $b = au$ .

**Observația 9.** •  $a \sim_{\mathbb{Z}} b$  dacă și numai dacă  $b = \pm a$ .

•  $f \sim_{k[X]} g$  dacă și numai dacă există  $\alpha \in k^*$  astfel încât  $g = \alpha f$ .

**Definiția 10.** Fie  $R$  un domeniu de integritate și  $a, b \in R$ . Spunem că  $d \in R$  este un **cel mai mare divizor comun** pentru  $a$  și  $b$  dacă:

- (i)  $d|a$  și  $d|b$ .
- (ii) Dacă  $d' \in R$  divide  $a$  și  $b$ , atunci  $d'|d$ .

**Definiția 11.** Fie  $R$  un domeniu de integritate și  $a, b \in R$ . Spunem că  $m \in R$  este un **cel mai mic multiplu comun** pentru  $a$  și  $b$  dacă:

- (i)  $a|m$  și  $b|m$ .
- (ii) Dacă  $m' \in R$  se divide prin  $a$  și prin  $b$ , atunci  $m|m'$ .

**Notăție:** Dacă  $R = \mathbb{Z}$  sau  $R = k[X]$ , iar  $a, b \in R$ , vom folosi notația  $(a, b)$  pentru cel mai mare divizor comun al lui  $a$  și  $b$  și notația  $[a, b]$  pentru cel mai mic multiplu comun al lui  $a$  și  $b$ .

**Observația 12.** Dacă două elemente ale unui domeniu de integritate  $R$  admit un cel mai mare divizor comun, acesta este determinat până la o asociere în divizibilitate.

**Propoziția 13.** Orice două numere întregi admit un cel mai mare divizor comun.

*Demonstrație:* Fie  $a, b \in \mathbb{Z}$ . Dacă  $b = 0$ , este clar că  $a$  este un cel mai mare divizor comun pentru  $a$  și  $b$ . Dacă  $b|a$ , avem  $(a, b) = b$ . Dacă

$b \neq 0$  și  $b \nmid a$ , aplicăm în mod repetat teorema de împărțire cu rest și obținem  $a = bq + r$ ,  $b = rq_1 + r_1$ ,  $r = r_1q_2 + r_2$  și așa mai departe. Cum  $r_0 \stackrel{\text{not}}{=} r, r_1, r_2, \dots$  este un șir strict descrescător de numere naturale, există  $n \in \mathbb{N}$  pentru care  $r_n = 0$ . Este însă clar că, în caz că numerele pe care le scriem în continuare există,  $(a, b) = (b, r) = (r, r_1) = \dots = (r_{n-2}, r_{n-1}) = (r_{n-1}, r_n)$ . Dar,  $(r_{n-1}, r_n)$  există și este egal cu  $r_{n-1}$ .  $\square$

**Observația 14.** Algoritmul care apare în demonstrația propoziției anterioare se numește **algoritmul lui Euclid**. Când aplicăm algoritmul lui Euclid pentru a găsi cel mai mare divizor comun a două numere întregi, acesta este dat de ultimul rest nenul.

Am demonstrat propoziția anterioară în așa fel încât să punem în evidență algoritmul lui Euclid, care este important și în sine. Putem da o demonstrație mai scurtă folosindu-ne de corolarul 3 și obținem următoarea propoziție:

**Propoziția 15.** Pentru orice două numere întregi  $a, b$  există  $(a, b)$  și  $[a, b]$  și avem:

- i)  $a\mathbb{Z} + b\mathbb{Z} = (a, b)\mathbb{Z}$
- ii)  $a\mathbb{Z} \cap b\mathbb{Z} = [a, b]\mathbb{Z}$
- iii)  $(a, b)[a, b] \sim ab$ .

Considerații similare sunt valabile pentru inele de tip  $k[X]$ ; avem:

**Propoziția 16.** Pentru orice două polinoame  $f, g \in k[X]$  există  $(f, g)$  și  $[f, g]$  și avem:

- i)  $fk[X] + gk[X] = (f, g)k[X]$
- ii)  $fk[X] \cap gk[X] = [f, g]k[X]$
- iii)  $(f, g)[f, g] \sim fg$ .

**Definiția 17.** Fie  $R$  un domeniu de integritate și  $a, b \in R$ . Spunem că  $a$  și  $b$  sunt relativ prime în  $R$  dacă cel mai mare divizor comun al lui  $a$  și  $b$  în  $R$  este 1.

**Propoziția 18.** Dacă  $R = \mathbb{Z}$  sau  $R = k[X]$ ,  $a, b, c, a_1, b_1 \in R$ , iar  $d = (a, b)$  atunci:

- (i) există  $\alpha, \beta \in R$  astfel încât  $\alpha a + \beta b = d$
- (ii) dacă  $a = da_1$ , iar  $b = db_1$ , atunci  $(a_1, b_1) = 1$
- (iii)  $(ac, bc) \sim (a, b)c$
- (iv) dacă  $a$  și  $b$  sunt prime cu  $c$ , atunci  $ab$  este prim cu  $c$ .
- (v) dacă  $a|bc$  și  $(a, b) = 1$ , atunci  $a|c$ .

**Definiția 19.** Date fiind numerele întregi  $a, b$  și  $n$ , spunem că  $a$  este **congruent cu  $b$  modulo  $n$**  (și notăm  $a \equiv b \pmod{n}$ ) dacă  $n|b - a$ .

**Observația 20.** În condițiile definiției anterioare,  $a \equiv b \pmod{n}$  dacă și numai dacă  $\widehat{a} = \widehat{b}$  în  $\mathbb{Z}_n$ .

**Teorema 21 (Euler).** Dacă  $a \in \mathbb{Z}$ ,  $n \in \mathbb{N}^*$  și  $(a, n) = 1$ , atunci  $a^{\varphi(n)} \equiv 1 \pmod{n}$ .

### 3. NUMERE PRIME

**Definiția 22.** Numărul întreg  $n$  se numește **prim** dacă are exact doi divizori naturali.

**Observația 23.** Divizorii naturali ai numărului prim  $n$  sunt 1 și  $|n|$ .

**Observația 24.** -1, 0 și 1 nu sunt numere prime.

**Definiția 25.** Numărul întreg  $n$  se numește **compus** dacă nu este prim și dacă  $|n| > 1$ .

**Exemplul 26.** Numerele 2, 3, -7, 211 sunt prime. Numerele 4, 6, 33, -148 sunt compuse.

**Propoziția 27.** Fie  $n \in \mathbb{Z} \setminus \{-1, 0, 1\}$ .  $n$  este prim dacă și numai dacă el îndeplinește condiția:

$$\forall a, b \in \mathbb{Z} \quad n|ab \Rightarrow n|a \vee n|b.$$

**Teorema 28 (Euclid).** Orice număr  $n \in \mathbb{Z} \setminus \{-1, 0, 1\}$  se poate scrie ca produs de numere prime.

*Demonstrație:* Presupunem că există numere  $n$  ca în enunț care nu se scriu ca produs de numere prime. Fie  $m$  cel mai mic număr natural cu această proprietate.  $m$  nefiind prim, putem scrie  $m = ab$  cu  $a$  și  $b$  mai mari decât 1. De aici rezultă că  $a$  și  $b$  sunt mai mici decât  $m$ , deci ele se scriu ca produs de numere prime. Prin urmare, și  $m$  are aceeași proprietate, contradicție.

**Teorema 29 (Euclid).** Mulțimea numerelor prime este infinită.

*Demonstrație:* Presupunem că există doar un număr finit de numere naturale prime, fie ele  $p_1, p_2, \dots, p_n$ . Atunci,  $N = p_1 p_2 \dots p_n + 1$  nu se divide prin niciun număr prim, contradicție.

**Teorema 30.** Orice număr  $n \in \mathbb{Z} \setminus \{-1, 0, 1\}$  se scrie în mod unic sub forma  $\pm p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r}$ ,  $p_1, p_2, \dots, p_r \in \mathbb{N}$  fiind numere prime distincte, iar  $\alpha_1, \alpha_2, \dots, \alpha_r \in \mathbb{N}^*$ .

*Demonstrație:* Existența scrierii este garantată de prima teoremă a lui Euclid. Vom demonstra că numărul  $\pm p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r}$  nu are altă scriere de acest tip. Procedăm prin inducție după  $u = \alpha_1 + \alpha_2 + \dots + \alpha_r$ : Dacă

$u = 1$ , avem de a face cu un număr prim, iar afirmația este evidentă. Dacă  $u > 1$ , presupunem că

$$(1) \quad \pm p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r} = \pm q_1^{\beta_1} q_2^{\beta_2} \dots q_s^{\alpha_s}.$$

Cum  $p_1$  este prim, el va divide cel puțin unul din factorii din membrul drept. Modulo o renumerotare, putem presupune că acest factor este  $q_1$ . Cum  $p_1$  și  $q_1$  sunt prime, deducem că ele sunt chiar egale. Simplificând relația (1) prin  $p_1$ , obținem  $\pm p_1^{\alpha_1-1} p_2^{\alpha_2} \dots p_r^{\alpha_r} = \pm p_1^{\beta_1-1} q_2^{\beta_2} \dots q_s^{\alpha_s}$ . Aplicând ipoteza de inducție, deducem că semnele coincid,  $r = s$ , și, modulo o renumerotare  $p_i = q_i$  și  $\alpha_i = \beta_i$ .

**Teorema 31 (Fermat).** *Dacă  $a \in \mathbb{Z}$ ,  $p \in \mathbb{N}$  este prim și  $p \nmid a$ , atunci  $a^{p-1} \equiv 1 \pmod{p}$ .*

#### 4. POLINOAME IREDUCTIBILE

**Definiția 32.** Polinomul  $f \in k[X] \setminus k$  se numește **reductibil** dacă poate fi scris ca produs de două polinoame neinvertibile. În caz contrar, spunem că  $f$  este **ireductibil**.

**Observația 33.** Polinoamele invertibile (care sunt exact cele constante nenule) nu sunt considerate nici reductibile, nici ireductibile.

**Exemplul 34.** Orice polinom de gradul I din  $k[X]$  este ireductibil

**Exemplul 35.** Orice polinom de grad  $\geq 2$  care are rădăcini în  $k$  este reductibil (conform teoremei lui Bézout).

**Exemplul 36.** Pentru polinoamele de grad 2 sau 3 din  $k[X]$ , ireductibilitatea este echivalentă cu absența (din  $k$  a) rădăcinilor.

**Exemplul 37.** Afirmația din exemplul anterior nu rămâne valabilă pentru polinoame de grad  $\geq 4$ . De exemplu,  $X^4 + 1 \in \mathbb{R}[X]$  este reductibil, dar nu are rădăcini reale.

**Observația 38.** Se întâmplă frecvent ca polinoame ireductibile din  $k[X]$  să devină reductibile în  $L[X]$  pentru anumite corpuri  $L$  care au  $k$  drept subcorp. De exemplu,  $X^2 + 1 \in \mathbb{R}[X]$ , care este ireductibil, este reductibil ca element al lui  $\mathbb{C}[X]$ .

Prezentăm câteva rezultate analoage celor de la paragraful de numere prime; demonstrațiile acestor rezultate se obțin cu ușurință din cele ale analogelor lor.

**Propoziția 39.** Fie  $f \in k[X] \setminus k$ .  $f$  este ireductibil dacă și numai dacă el îndeplinește condiția:

$$\forall g, h \in k[X] \quad f|gh \Rightarrow f|g \vee f|h.$$

**Teorema 40.** Orice polinom  $f \in k[X] \setminus k$  se poate scrie ca produs de polinoame ireductibile.

**Teorema 41.** Mulțimea polinoamelor monice ireductibile din  $k[X]$  este infinită.

**Teorema 42.** Orice polinom  $f \in k[X] \setminus k$  se scrie în mod unic sub forma  $ap_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r}$ ,  $p_1, p_2, \dots, p_r \in k[X]$  fiind polinoame monice ireductibile distincte,  $a \in k^*$ , iar  $\alpha_1, \alpha_2, \dots, \alpha_r \in \mathbb{N}^*$ .

**Definiția 43.** Polinomul  $f \in \mathbb{Z}[X]$  se numește **primitiv** dacă cel mai mare divizor comun al coeficienților săi este 1.

**Teorema 44 (Criteriul lui Eisenstein).** Fie  $h \in \mathbb{Z}[X]$  un polinom neconstant și primitiv. Dacă există un număr prim  $p$  care divide toți coeficienții lui  $f$  cu excepția celui dominant, iar  $p^2$  nu divide termenul liber al lui  $f$ , atunci  $f$  este ireductibil în  $\mathbb{Q}[X]$ .

## 5. TEOREMA FUNDAMENTALĂ A ALGEBREI

Următorul rezultat, pe care îl prezentăm fără demonstrație, este cunoscut sub numele de teorema fundamentală a algebrei:

**Teorema 45 (d'Alembert, Gauss).** Orice polinom neconstant cu coeficienți complecși are cel puțin o rădăcină complexă.

**Corolarul 46.** Polinoamele ireductibile cu coeficienți complecși sunt cele de gradul I.

**Corolarul 47.** Polinoamele ireductibile cu coeficienți reali sunt cele de gradul I și cele de gradul II cu  $\Delta < 0$ .

**Corolarul 48.** Orice polinom neconstant  $f \in \mathbb{C}[X]$  se scrie în mod unic sub forma  $a(X - z_1)^{\alpha_1} (X - z_2)^{\alpha_2} \dots (X - z_n)^{\alpha_n}$  cu  $a \in \mathbb{C}^*$  și  $z_1, z_2, \dots, z_n \in \mathbb{C}$ .

## 6. RĂDĂCINI ALE POLINOAMELOR. RELAȚIILE LUI VIÈTE

**Definiția 49.** Elementul  $a \in R$  se numește **rădăcină a** lui  $f \in R[X]$  dacă  $f(a) = 0$ .

**Teorema 50 (Bézout).** Fie  $f \in k[X]$ . Atunci,  $a \in k$  este rădăcină a lui  $f$  dacă și numai dacă  $X - a \mid f$ .

**Definiția 51.** Fie  $f \in k[X] \setminus \{0\}$  și  $a \in k$  o rădăcină a lui  $f$ . Numărul  $j \in \mathbb{N}$  cu proprietățile  $(X - a)^j \mid f$  și  $(X - a)^{j+1} \nmid f$  se numește **ordinul de multiplicitate** al lui  $a$ .

$$f = (X - a_1)^{m_1} (X - a_2)^{m_2} \cdots (X - a_r)^{m_r} g.$$

**Propoziția 54.** Fie  $f \in k[X] \setminus \{0\}$ ,  $n \in \mathbb{N}^*$  și  $a \in k$ .

b) Presupunând caracteristica lui  $k$  egală cu zero, dacă  $f(a) = f'(a) = \dots = f^{(n-1)}(a) = 0$  și  $f^{(n)}(a) \neq 0$ , atunci ordinul de multiplicitate al rădăcinii  $a$  a lui  $f$  este  $n$ .

**Propoziția 56.** Fie  $f = a_0 + a_1X + \cdots + a_nX^n \in k[X]$ ,  $a_n \neq 0$ . Presupunem că  $f$  are  $n$  rădăcini  $x_1, x_2, \dots, x_n$  în  $k$ . Atunci,  $f = a_n(X - x_1)(X - x_2) \cdots (X - x_n)$  și au loc **relațiile între rădăcini și coeficienți (relațiile lui Viète)**:

$$\begin{aligned} a_n(x_1 + x_2 + \cdots + x_n) &= -a_{n-1}, \\ a_n(x_1x_2 + x_1x_2 + \cdots + x_1x_n + \cdots + x_{n-1}x_n) &= a_{n-2}, \\ \dots\dots\dots \\ a_n(x_1x_2 \dots x_k + \cdots + x_{n-k+1}x_{n-k+2} \dots x_n) &= (-1)^k a_{n-k}, \\ \dots\dots\dots \\ a_n(x_1x_2 \dots x_n) &= (-1)^n a_0. \end{aligned}$$

**Teorema 58 (Wilson).** *Dacă  $p \in \mathbb{N}$  este prim, atunci  $(p-1)! \equiv -1 \pmod{p}$ .*

- [1] T. Dumitrescu, *Algebra*, Ed. Universităţii din Bucureşti, 2006.
- [2] I. D. Ion, N. Radu, *Algebra*, Ed. Universităţii din Bucureşti, 1981.
- [3] C. Năstăsescu, C. Niţă, C. Vraciu, *Bazele algebrei*, Ed. Academiei, Bucureşti, 1986.