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

G. MINCU

În acest curs, k va desemna un corp comutativ.

1. teoreme de împărţire cu rest

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

Demonstraţie:
Existenţa: Fie $r = a - bq$ cel mai mic număr întreg ≥ 0 de forma $a - bx$ cu $x \in \mathbb{Z}$. Dacă $a - bq \geq |b|$, atunci $0 \leq a - b(q + \text{sgn}(b)) < a - bq$, contradicţie.
Unicitatea: Fie $q, r, q', r' \in \mathbb{Z}$ astfel încât $a = bq + r = bq' + r'$ şi $0 \leq r, r' < |b|$. Scăzând cele două expresii ale lui a rezultă $b(q - q') = r' - r$, deci $r' - r = 0$ deoarece $|r' - r| < |b|$. Aşadar $r' = r$, iar din egalitatea $b(q - q') = 0$ şi din $b \neq 0$ rezultă $q' = q$.

Teorema 2 (**Teorema împărţirii cu rest în** $k[X]$)**.** *Fie $f, g \in k[X]$, $g \neq 0$. Atunci, există şi sunt unice $q, r \in k[X]$ cu proprietăţile $f = gq + r$ şi grad $r <$ grad g.*

Demonstraţie:
Existenţa: Facem inducţie după gradul lui f; vom nota cu a_f şi a_g coeficienţii dominanţi ai polinoamelor f, respectiv g. Dacă $\text{grad}\, f < \text{grad}\, g$, luăm $q = 0$ şi $r = f$. Dacă $\text{grad}\, f \geq \text{grad}\, g$, există, conform ipotezei de inducţie, $q_1, r_1 \in k[X]$ astfel încât $f - a_f a_g^{-1} X^{\text{grad}\, f - \text{grad}\, g} g = gq_1 + r_1$ şi $\text{grad}\, r_1 < \text{grad}\, g$. Luăm $q = a_f a_g^{-1} X^{\text{grad}\, f - \text{grad}\, g} + q_1$ şi $r = r_1$.
Unicitatea: Fie $q, r, q', r' \in k[X]$ astfel încât $f = gq + r = gq' + r'$ şi $\text{grad}\, r, \text{grad}\, r' < \text{grad}\, g$. Din primele relaţii rezultă $(q - q')g = r' - r$; gradul membrului drept al acestei relaţii fiind mai mic decât $\text{grad}\, g$, rezultă $q = q'$. Înlocuind în ultima relaţie, obţinem şi $r = r'$.

Corolarul 3. Orice ideal al lui $\mathbb{Z}$ este principal.
Orice ideal al lui $k[X]$ este principal.

2. DIVIZIBILITATE

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

Propoziţia 5. Fie R un domeniu de integritate şi $a, b, c \in R$. Atunci:
i) $a|_R b$ dacă şi numai dacă $bR \subset aR$.
ii) Dacă $a|b$ şi $b|c$, atunci $a|c$.
iii) Dacă $a|b$, atunci $a|bc$.
iv) Dacă $a|b$ şi $a|c$, atunci $a|b + c$.

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

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

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

Observaţia 9. • $a \sim_{\mathbb{Z}} b$ dacă şi numai dacă $b = \pm a$.
• $f \sim_{k[X]} g$ dacă şi numai dacă există $\alpha \in k^*$ astfel încât $g = \alpha f$.

Definiţia 10. Fie R un domeniu de integritate şi $a, b \in R$. Spunem că $d \in R$ este un **cel mai mare divizor comun** pentru a şi b dacă:
(i) $d|a$ şi $d|b$.
(ii) Dacă $d' \in R$ divide a şi b, atunci $d'|d$.

Definiţia 11. Fie R un domeniu de integritate şi $a, b \in R$. Spunem că $m \in R$ este un **cel mai mic multiplu comun** pentru a şi b dacă:
(i) $a|m$ şi $b|m$.
(ii) Dacă $m' \in R$ se divide prin a şi prin b, atunci $m|m'$.

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

Observaţia 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.

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

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

$b \neq 0$ şi $b \nmid a$, aplicăm în mod repetat teorema de împărţire cu rest şi obţinem $a = bq + r$, $b = rq_1 + r_1$, $r = r_1q_2 + r_2$ şi aşa mai departe. Cum $r_0 \overset{\text{not}}{=} r, r_1, r_2, \ldots$ este un şir 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, $(a, b) = (b, r) = (r, r_1) = \ldots = (r_{n-2}, r_{n-1}) = (r_{n-1}, r_n)$. Dar, (r_{n-1}, r_n) există şi este egal cu r_{n-1}. $\square$

Observaţia 14. Algoritmul care apare în demonstraţia propoziţiei anterioare se numeşte **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 propoziţia anterioară în aşa fel încât să punem în evidenţă algoritmul lui Euclid, care este important şi în sine. Putem da o demonstraţie mai scurtă folosindu-ne de corolarul 3 şi obţinem următoarea propoziţie:

Propoziţia 15. Pentru orice două numere întregi a, b există (a, b) şi $[a, b]$ şi 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) $(a, b)[a, b] \sim ab$.

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

Propoziţia 16. Pentru orice două polinoame $f, g \in k[X]$ există (f, g) şi $[f, g]$ şi avem:
i) $fk[X] + gk[X] = (f, g)k[X]$
ii) $fk[X] \cap gk[X] = [f, g]k[X]$
iii) $(f, g)[f, g] \sim fg$.

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

Propoziţia 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 şi b sunt prime cu c, atunci ab este prim cu c.
(v) dacă $a|bc$ şi $(a, b) = 1$, atunci $a|c$.

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

Observaţia 20. În condiţiile definiţiei anterioare, $a \equiv b \pmod{n}$ dacă şi numai dacă $\widehat{a} = \widehat{b}$ în $\mathbb{Z}_n$.

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

3. NUMERE PRIME

Definiţia 22. Numărul întreg n se numeşte **prim** dacă are exact doi divizori naturali.

Observaţia 23. Divizorii naturali ai numărului prim n sunt 1 şi $|n|$.

Observaţia 24. -1, 0 şi 1 nu sunt numere prime.

Definiţia 25. Numărul întreg n se numeşte **compus** dacă nu este prim şi dacă $|n| > 1$.

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

Propoziţia 27. Fie $n \in \mathbb{Z} \setminus \{-1, 0, 1\}$. n este prim dacă şi numai dacă el îndeplineşte condiţia:

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

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

Demonstraţie: Presupunem că există numere n ca în enunţ 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 şi b mai mari decât 1. De aici rezultă că a şi b sunt mai mici decât m, deci ele se scriu ca produs de numere prime. Prin urmare, şi m are aceeaşi proprietate, contradicţie.

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

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

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

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

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

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

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

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

4. polinoame ireductibile

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

Observaţia 33. Polinoamele inversabile (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 ≥ 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 absenţa (din k a) rădăcinilor.

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

Observaţia 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; demonstraţiile acestor rezultate se obţin cu uşurinţă din cele ale analoagelor lor.

Propoziţia 39. Fie $f \in k[X] \setminus k$. f este ireductibil dacă şi numai dacă el îndeplineşte condiţia:

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

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

Teorema 41. Mulţimea 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 $\alpha_1, \alpha_2, \dots, \alpha_r \in \mathbb{N}^*$.

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

Teorema 44 (**Criteriul lui Eisenstein**)**.** *Fie $h \in \mathbb{Z}[X]$ un polinom neconstant şi primitiv. Dacă există un număr prim p care divide toţi coeficienţii lui f cu excepţia 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 demonstraţie, este cunoscut sub numele de teorema fundamentală a algebrei:

Teorema 45 (**d'Alembert, Gauss**)**.** *Orice polinom neconstant cu coeficienţi complecşi are cel puţin o rădăcină complexă.*

Corolarul 46. Polinoamele ireductibile cu coeficienţi complecşi sunt cele de gradul I.

Corolarul 47. Polinoamele ireductibile cu coeficienţi reali sunt cele de gradul I şi 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 $a \in \mathbb{C}^*$ şi $z_1, z_2, \dots z_n \in \mathbb{C}$.

6. Rădăcini ale polinoamelor. Relaţiile lui Viète

Definiţia 49. Elementul $a \in R$ se numeşte **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 şi numai dacă $X - a | f$.*

Definiţia 51. Fie $f \in k[X] \setminus \{0\}$ şi $a \in k$ o rădăcină a lui f. Numărul $j \in \mathbb{N}$ cu proprietăţile $(X-a)^j | f$ şi $(X-a)^{j+1} \nmid f$ se numeşte **ordinul de multiplicitate** al lui a.

Propoziţia 52. Fie $f \in k[X]$ un polinom nenul, $a_1,a_2,\ldots,a_r \in R$ rădăcini distincte ale lui f, iar pentru fiecare $i \in \{1,2,\ldots,r\}$ fie m_i ordinul de multiplicitate al lui a_i. Atunci, există $g \in R[X]$ astfel încât

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

Definiţia 53. Prin **derivata** polinomului $f = \sum_{i=0}^{n} a_iX^i \in R[X]$ înţelegem polinomul $f' = \sum_{i=1}^{n} ia_iX^{i-1} \in R[X]$. Considerând definită derivata de ordin n (notată $f^{(n)}$) a lui f, prin **derivata de ordin** $n+1$ **a lui** f înţelegem polinomul $(f^{(n)})'$.

Propoziţia 54. Fie $f \in k[X]\setminus\{0\}$, $n \in \mathbb{N}^*$ şi $a \in k$.
a) Dacă a este rădăcină cu ordin de multiplicitate n pentru f, atunci $f(a) = f'(a) = \cdots = f^{(n-1)}(a) = 0$.
b) Presupunând caracteristica lui k egală cu zero, dacă $f(a) = f'(a) = \cdots = f^{(n-1)}(a) = 0$ şi $f^{(n)}(a) \neq 0$, atunci ordinul de multiplicitate al rădăcinii a a lui f este n.

Corolarul 55. Dacă $f \in k[X]$ este un polinom nenul de grad n, atunci f are cel mult n rădăcini în k.

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

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

Observaţia 57. Dacă S este domeniu de integritate, k este subcorp al lui S, iar $f \in k[X]\setminus\{0\}$ de gradul n are (toate) rădăcinile $x_1,x_2,\ldots,x_n$ în S, atunci pentru orice polinom simetric $g \in k[X_1,X_2,\ldots,X_n]$ avem $g(x_1,x_2,\ldots,x_n) \in k$.

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

Bibliografie

[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.