CURS 12: ARITMETICĂ ÎN $\mathbb{Z}$ ŞI $K[X]$

SAI

1. CORPURI

Definiţia 1. Inelul unitar R se numeşte **corp** dacă sunt îndeplinite condiţiile:
i) $1 \neq 0$.
ii) orice element nenul al lui R este inversabil.

Observaţia 2. Orice corp este inel integru.

Exemplul 3. Conform proprietăţilor cunoscute de la şcoala generală sau de la liceu, $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$ sunt corpuri comutative. $(\mathbb{Z}, +, \cdot)$ nu este corp, deoarece $2 \in \mathbb{Z}$ este nenul şi neinversabil.

Exemplul 4. Întrucât $U(\mathbb{Z}_n) = \{a \in \mathbb{Z}_n : (a, n) = 1\}$, deducem că inelul $\mathbb{Z}_n$ este corp dacă şi numai dacă n este număr prim.

Definiţia 5. Fie R un inel. O submulţime nevidă K a lui R se numeşte **subcorp** al lui R dacă K este corp în raport cu operaţiile induse de cele de pe R.

Propoziţia 6. Fie K un corp. O submulţime L a lui K cu cel puţin două elemente este subcorp al lui K dacă şi numai dacă sunt îndeplinite condiţiile:
i) $\forall x, y \in L \quad x - y \in L$ şi
ii) $\forall x, y \in L \setminus \{0\} \quad xy^{-1} \in L$.

Propoziţia 7. Fie K un corp şi L_α, $\alpha \in A$ subcorpuri ale acestuia. Atunci, $P_K = \bigcap_{\alpha \in A} L_\alpha$ este subcorp al lui K.

Definiţia 8. Un corp care nu admite subcorpuri proprii se numeşte **corp prim**.

Observaţia 9. Dat fiind un corp K, subcorpul său P_K este corp prim. El se numeşte **subcorpul prim** al lui K.

Fie K un corp de caracterisită $n \in \mathbb{N}^*$ şi P_K subcorpul său prim. Atunci, $1 \in P_K$, deci $\mathcal{M} = \{1, 1+1, \dots, \underbrace{1+1+\cdots+1}_{n-1}\} \subseteq P_K$. Este uşor de văzut că

$$(\underbrace{1+1+\cdots+1}_{u})-(\underbrace{1+1+\cdots+1}_{v})=\underbrace{1+1+\cdots+1}_{u-v \pmod n} \quad \text{şi}$$

$$(\underbrace{1+1+\cdots+1}_{u})(\underbrace{1+1+\cdots+1}_{v})=\underbrace{1+1+\cdots+1}_{uv \pmod n}.$$

De aici deducem că $\varphi : \mathbb{Z}_n \to \mathcal{M}$, $\varphi(\widehat{a}) = \underbrace{1+1+\cdots+1}_{a}$ este morfism de inele. Surjectivitatea acestuia fiind evidentă, din $|\mathbb{Z}_n| = |\mathcal{M}|$ obţinem şi injectivitatea. Aşadar, inelele $\mathbb{Z}_n$ şi $\mathcal{M}$ sunt izomorfe. Rezultă că $\mathbb{Z}_n$ este inel integru, de unde deducem că n este număr prim, deci $\mathcal{M} \cong \mathbb{Z}_n$ este subcorp al lui P_K, deci egal cu P_K. Am obţinut prin urmare:

Propoziţia 10. Caracteristica unui corp este fie zero, fie număr prim.

Propoziţia 11. Dacă K este un corp de caracteristică $p > 0$, atunci subcorpul său prim este izomorf cu $\mathbb{Z}_p$.

Procedând în mod similar, obţinem:

Propoziţia 12. Dacă K este un corp de caracteristică zero, atunci subcorpul său prim este izomorf cu $\mathbb{Q}$.

Din cele de mai sus rezultă şi:

Propoziţia 13. Singurul tip de corp prim de caracteristică p este $\mathbb{Z}_p$. Singurul tip de corp prim de caracteristică zero este $\mathbb{Q}$.

Exemplul 14. Considerăm submulţimea $\mathcal{H} = \left\{ \begin{pmatrix} a & b \\ -\overline{b} & \overline{a} \end{pmatrix} : a, b \in \mathbb{C} \right\}$ a lui $\mathcal{M}_2(\mathbb{C})$. Se constată că $\mathcal{H}$ este o parte stabilă a lui $\mathcal{M}_2(\mathbb{C})$ în raport cu adunarea şi cu înmulţirea matricilor. În raport cu legile induse, $\mathcal{H}$ are o structură de corp.

Definiţia 15. Corpul (necomutativ!) din exemplul anterior se numeşte **corpul cuaternionilor**. El se notează de obicei cu $\mathbb{H}$.

Exemplul 16. Fie R un domeniu de integritate. Pe $R \times (R \setminus \{0\})$ introducem relaţia $\sim$ astfel: $(a, s) \sim (b, t)$ dacă şi numai dacă $at = bs$. Se constată că această relaţie este de echivalenţă.
Notăm cu $\dfrac{a}{s}$ clasa elementului $(a, s) \in R \times (R \setminus \{0\})$ în raport cu relaţia $\sim$ şi cu M mulţimea factor $R \times (R \setminus \{0\})/\sim$.
Pe M introducem operaţiile $\dfrac{a}{s} + \dfrac{b}{t} = \dfrac{at + bs}{st}$ şi $\dfrac{a}{s} \cdot \dfrac{b}{t} = \dfrac{ab}{st}$.
Este uşor de văzut că aceste operaţii sunt corect definite şi că $(M, +, \cdot)$ este un corp comutativ.

Definiţia 17. Corpul construit în exemplul anterior se numeşte **corpul de fracţii al domeniului** R. O notaţie frecvent folosită pentru acest corp este $Q(R)$.

Exemplul 18. Corpul de fracţii al lui $\mathbb{Z}$ este $\mathbb{Q}$.

Definiţia 19. Dacă K este corp comutativ, corpul de fracţii al lui $K[X]$ se numeşte **corpul de fracţii raţionale în nedeterminata** X **cu coeficienţi în** K şi se notează $\mathbf{K}(\mathbf{X})$.

Observaţia 20. $K(X) = \left\{ \dfrac{f}{g} : f, g \in K[X],\ g \neq 0 \right\}$.

Observaţia 21. Dat fiind un domeniu de integritate R, funcţia $j_R : R \to Q(R)$, $j_R(a) = \dfrac{a}{1}$ este un morfism injectiv şi unitar de inele.

2. Morfisme de corpuri

Definiţia 22. Fie K şi L două corpuri. Funcţia $f : K \to L$ se numeşte **morfism de corpuri** dacă este morfism unitar de inele.

Exemplul 23. $i_1 : \mathbb{Q} \to \mathbb{R}$, $i_1(x) = x$, $i_2 : \mathbb{Q} \to \mathbb{C}$, $i_2(x) = x$, $i_3 : \mathbb{R} \to \mathbb{C}$, $i_3(x) = x$ şi $i_4 : \mathbb{Q} \to \mathbb{Q}(\sqrt{2})$, $i_4(x) = x$ sunt câteva exemple imediate de morfisme de corpuri.

Exemplul 24. Pentru orice corp K, $\mathbf{1}_K$ este automorfism de corpuri.

Exemplul 25. $\alpha : \mathbb{R} \to \mathbb{H}$, $\alpha(a) = \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$ este un morfism de corpuri.

Observaţia 26. Fie K un corp comutativ de caracteristică $p > 0$. Pentru orice $x \in K$ are loc relaţia

$$px = \underbrace{x + x + \cdots + x}_{p} = x(\underbrace{1 + 1 + \cdots + 1}_{p}) = 0.$$

Mulţumită comutativităţii, pentru orice $x, y \in K$ are loc

$$(xy)^p = x^p y^p.$$

Numărul p fiind prim, avem $p \mid \dbinom{p}{k}$ pentru orice $k \in \{1, 2, \ldots, p-1\}$.
Prin urmare, pentru orice $x, y \in K$ are loc relaţia

$$(x + y)^p = \sum_{k=0}^{p} \binom{p}{k} x^{p-k} y^k = x^p + y^p.$$

Drept consecinţă a acestei observaţii, obţinem

Exemplul 27. Fie K un corp comutativ de caracteristică $p > 0$. Atunci, $\varphi : K \to K$, $\varphi(x) = x^p$ este un endomorfism de corpuri.

Definiţia 28. Endomorfismul din exemplul anterior se numeşte **endomorfismul lui Frobenius**.

Se constată cu uşurinţă că toate morfismele din exemplele prezentate sunt injective (temă!). Aceasta este consecinţa unui fapt mai general, şi anume:

Propoziţia 29. Orice morfism de corpuri este injectiv.

(Temă: demonstraţi această propoziţie!)

3. Divizibilitate în domenii de integritate

Peste tot R este un domeniu de integritate; de cele mai multe ori el este considerat $\mathbb{Z}$ sau un inel de polinoame cu coeficienţi într-un corp comutativ K.

Definiţia 30. *Fie $a, b \in R$. Spunem că b divide a şi scriem $b \mid a$ dacă există $c \in R$ astfel încât $a = bc$.*

Elementele a şi b se numesc asociate în divizibilitate dacă şi numai dacă $a \mid b$ şi $b \mid a$, caz în care scriem $a \sim b$.

Exemplul 31. *(i) $a \mid 0$ şi $1 \mid a$, pentru orice $a \in R$.*

(ii) $a \mid f$ în $K[X]$, pentru orice $0 \neq a \in K$ şi $f \in K[X]$ ($f = a(a^{-1}f)$).

(iii) $1 + i \mid 2$ în $\mathbb{Z}[i]$ ($2 = (1 + i)(1 - i)$).

Propoziţia 32. *Fie $a, b, c \in R$.*

(i) $a \mid b$ dacă şi numai dacă $Rb \subseteq Ra$;

(ii) Dacă $a \mid b$ şi $b \mid c$ atunci $a \mid c$;

(iii) Dacă $a \mid b$ şi $a \mid c$ atunci $a \mid \alpha b + \beta c$, pentru orice $\alpha, \beta \in R$;

(iv) $a \sim b$ dacă şi numai dacă $Ra = Rb$, dacă şi numai dacă există $u \in U(R)$ astfel încăt $b = ua$.

Demonstraţie: (i) $a \mid b \Leftrightarrow \exists\, c \in R$ astfel încât $b = ca \Leftrightarrow b \in Ra \Leftrightarrow Rb \subseteq Ra$.

(ii) $a \mid b$ şi $b \mid c \Leftrightarrow Rb \subseteq Ra$ şi $Rc \subseteq Rb$, de unde rezultă că $Rc \subseteq Ra \Leftrightarrow a \mid c$.

(iii) Ca la (ii), avem $Rb \subseteq Ra$ şi $Rc \subseteq Ra$. Atunci, $\forall\, \alpha,\ \beta \in R$ avem $\alpha b + \beta c \in Rb + Rc \subseteq Ra + Ra = Ra$ şi, deci, $a \mid \alpha b + \beta c$.

(iv) $a \sim b \Leftrightarrow a \mid b$ şi $b \mid a \Leftrightarrow Rb \subseteq Ra$ şi $Ra \subseteq Rb \Leftrightarrow Ra = Rb$. O să arătăm că $Ra = Rb$ dacă şi numai dacă $b = ua$ pentru un anumit $u \in U(R)$.

" $\Rightarrow$ ". $b \in Rb = Ra$, deci $\exists\ u \in R$ cu $b = ua$. Analog, din $a \in Ra = Rb$, $\exists\ v \in R$ cu $a = vb$. Atunci $a = vb = vua$, deci $a(1 - vu) = 0$; cum R este domeniu de integritate, rezultă $a = 0$ sau $uv = 1$.

Dacă $a = 0$ atunci $Rb = Ra = \{0\}$, deci $b \in Rb = \{0\}$ implică $b = 0$. Clar $b = 1 \cdot a$ cu $1 \in U(R)$.

Dacă $a \neq 0$ atunci $uv = vu = 1$ şi, deci, $b = ua$ cu $u \in U(R)$; $u^{-1} = v$.

" $\Leftarrow$ " Fie $b = ua$ cu $u \in U(R)$. Cum $a \mid b$ rezultă $Rb \subseteq Ra$. Din $a = u^{-1}b$ deducem că $b \mid a$, deci $Ra \subseteq Rb$. Rezultă $Ra = Rb$.

Definiţia 33. *Fie $a, b \in R$.*

(i) Se numeşte un cel mai mare divizor comun al lui aşi b în R un element $d \in R$ cu proprietăţile:

(i_1) $d \mid a$ şi $d \mid b$;

(i_2) $\forall\ d' \in R$ astfel încât $d' \mid a$ şi $d' \mid b$ rezultă $d' \mid d$.

Dacă există, el se notează cu (a, b) şi este unic până la o asociere în divizibilitate.

(ii) Se numeşte un cel mai mic multiplu comun al lui a şi b în R un element $m \in R$ cu proprietăţile:

(ii_1) $a \mid m$ şi $b \mid m$;

(ii_2) $\forall\ m' \in R$ astfel încât $a \mid m'$ şi $b \mid m'$ rezultă $m \mid m'$.

Dacă există, el se notează cu $[a, b]$ şi este unic până la o asociere în divizibilitate.

Dacă $R \in \{\mathbb{Z}, K[X]\}$, (a, b) şi $[a, b]$ există pentru orice două elemente $a, b \in R$. Într-adevăr, dacă $a = 0$ sau $b = 0$, $(a, b) = \max\{a, b\}$ iar $[a, b] = 0$. Dacă $a, b \neq 0$, (a, b) se obţine cu algoritmul lui Euclid iar $[a, b] = \frac{ab}{(a,b)}$.

Pentru $R \in \{\mathbb{Z}, K[X]\}$, există $\varphi : R\backslash\{0\} \to \mathbb{N}$ funcţie cu următoarea proprietate:

(E) $\forall\ a, b \in R$ cu $b \neq 0$, $\exists!\ q, r \in R$ astfel încât $a = bq + r$, cu $r = 0$ sau $r \neq 0$ şi $\varphi(r) < \varphi(b)$.

Pentru $R = \mathbb{Z}$, $\varphi =\mid\ \mid$ este funcţia modul iar pentru $R = K[X]$, $\varphi = \mathrm{grad}(\ )$ este funcţia grad; în ambele situaţii (E) se reduce la teorema împărţirii cu rest.

Theorem 34. *(*Algoritmul lui Euclid.) *Fie R un domeniu de integritate pentru care există o funcţie $\varphi : R\backslash\{0\} \to \mathbb{N}$ cu proprietatea (E). Pentru $a, b \in R$ cu $a, b \neq 0$ considerăm algoritmul (se aplică succesiv teorema împărţirii cu rest până se obţine restul 0; algoritmul are un număr finit de paşi pentru că $\varphi(r_n) < \varphi(r_{n-1}) < \cdots < \varphi(r_1) < \varphi(b)$ în $\mathbb{N}$ şi este posibil ca el să conţină un singur pas):*

$a = bq_1 + r_1$ cu $r_1 \neq 0$ şi $\varphi(r_1) < \varphi(b)$;
$b = r_1q_2 + r_2$ cu $r_2 \neq 0$ şi $\varphi(r_2) < \varphi(r_1)$;
$\vdots$
$r_{n-2} = r_{n-1}q_{n+1} + r_n$ cu $r_n \neq 0$ şi $\varphi(r_n) < \varphi(r_{n-1})$;
$r_{n-1} = r_nq_{n+2}$
Atunci $r_n = (a, b)$.

Demonstraţie: $r_n \mid r_{n-1} \Rightarrow r_n \mid r_{n-2} \Rightarrow \cdots \Rightarrow r_n \mid b \Rightarrow r_n \mid a$.
Dacă $d' \mid a, b$ în R rezultă $d' \mid r_1 \Rightarrow d' \mid r_2 \Rightarrow \cdots \Rightarrow d' \mid r_n$. □

Lemma 35. *Dacă $R \in \{\mathbb{Z}, K[X]\}$ atunci orice ideal al lui R este principal.*

Demonstraţie: Fie $I \leq R$ un ideal nenul (idealul nul este principal, generat de 0) şi $X := \{\varphi(r) \mid 0 \neq r \in I\} \subseteq \mathbb{N}$. Cum X este nevidă, există $x \in X$ un prim element. Altfel spus, $\exists\ 0 \neq r \in I$ astfel încât $x = \varphi(r) \leq \varphi(a)$, $\forall\ 0 \neq a \in I$.

Clar $r \in I \Rightarrow Rr \subseteq I$. Dacă $a \in I$, scriem $a = rq + r_0$, $q, r_0 \in R$ cu $r_0 = 0$ sau $r_0 \neq 0$ şi $\varphi(r_0) < \varphi(r) = x$. Cum $r_0 = a - rq \in I$, din faptul că $x \in X$ este prim element rezultă $r_0 = 0$, deci $a = rq \in Rr$. Obţinem $I = Rr$, un ideal principal. □

Theorem 36. *Fie $R \in \{\mathbb{Z}, K[X]\}$ şi $a, b \in R$. Atunci*
(i) $Ra + Rb = R(a, b)$;
(ii) $Ra \cap Rb = R[a, b]$, în particular $[a, b]$ există;
(iii) $(a, b)[a, b]$ şi ab sunt asociate în divizibilitate.

Demonstraţie: (i) Se verifică uşor că $Ra + Rb$ este ideal în R, deci este principal: $\exists\ d \in R$ cu $Ra + Rb = Rd$. Din $Ra, Rb \subseteq Ra + Rb = Rd$ rezultă $d \mid a, b$. Dacă $d' \in R$ cu $d' \mid a, b$ atunci $Ra, Rb \subseteq Rd'$ şi, astfel, $Rd = Ra + Rb \subseteq Rd'$. Obţinem că $d' \mid d$ şi, deci, $d = (a, b)$.

(ii) Asemănător ca la (i): $Ra \cap Rb$ este ideal, deci $\exists\ m \in R$ cu $Ra \cap Rb = Rm$. Se arată că $m = [a, b]$.

(iii) Fie $d = (a, b)$ şi scriem $a = da'$, $b = db'$ pentru anumiţi $a', b' \in R$. Fie $m = [a, b]$, există cf. (ii); putem presupune $a, b \neq 0$, de unde $d, m \neq 0$.

Clar $a \mid \frac{ab}{d} = ab'$ şi $b \mid \frac{ab}{d} = a'b$, de unde $m \mid \frac{ab}{d}$; altfel spus, $dm \mid ab$. Cum $a \mid ab$ şi $b \mid ab$ rezultă că $m \mid ab$, adică $ab = md'$ cu $d' \in R$. Dacă scriem $m = a\alpha = b\beta$ cu $\alpha, \beta \in R$, atunci $ab = a\alpha d' = b\beta d'$. Rezultă $b = \alpha d'$ şi $a = \beta d'$, adică $d' \mid a, b$. Obţinem $d' \mid d$ şi, deci, $\frac{ab}{m} \mid d$ sau, echivalent, $ab \mid dm$. În concluzie, $dm \sim ab$. □

Proprietăţi pentru c.m.m.d.c.

Theorem 37. *Fie $R \in \{\mathbb{Z}, K[X]\}$ şi $a, b, c \in R$ nenule. Atunci:*

(i) Dacă $d = (a, b)$, există $\alpha, \beta \in R$ a.î. $d = \alpha a + \beta b$;
(ii) $(a, b) = 1$ dacă şi numai dacă există $\alpha, \beta \in R$ a.î. $\alpha a + \beta b = 1$;
(iii) Dacă $d = (a, b)$ atunci $\left(\frac{a}{d}, \frac{b}{d}\right) = 1$;
(iv) $(ac, bc) = c(a, b)$;
(v) Dacă $(a, c) = 1$ şi $(b, c) = 1$ atunci $(ab, c) = 1$;
(vi) Dacă $a \mid bc$ şi $(a, b) = 1$ atunci $a \mid c$.

Demonstraţie: (i) $Ra + Rb = Rd$.
(ii)" $\Rightarrow$ " rezultă din (i) iar " $\Leftarrow$ " rezultă astfel: $1 \in Ra + Rb = Rd$ implică $Rd = R$, adică $d \sim 1$.
(iii) Rezultă din (i) si (ii): $\alpha\frac{a}{d} + \beta\frac{b}{d} = 1$.
(iv) $Ra + Rb = Rd$ implică $Rac + Rbc = Rdc$.
(v) Scriem $1 = au + cv$ şi $1 = bu' + cv'$. Rezultă

$$\begin{aligned} 1 &= (au + cv)(bu' + cv') \\ &= abuu' + (auv' + bu'v + cvv')c \end{aligned}$$

de unde obţinem $(ab, c) = 1$.
(vi) $(a, b) = 1$ implică $(ac, bc) = c(a, b) = c$. Dar $a \mid bc$ şi $a \mid ac$, deci $a \mid c = (ac, bc)$. $\square$

4. Rădăcini ale polinoamelor

Peste tot, R este un inel comutativ şi unitar; în anumite situaţii R este şi fără divizori ai lui zero, adică un domeniu de integritate.

Definiţia 38. Fie $f \in R[X]$ şi $s \in S \supseteq R$, S un suprainel al lui R. Spunem că s este rădăcină a lui f dacă $\widetilde{f}(s) = 0$, unde funcţia $\widetilde{f} : S \to S$ este funcţia polinomială ataşată lui f.

Exemplul 39. *(i) 1 este rădăcină din $\mathbb{Z}$ a lui $f = X^2 - 3X + 2 \in \mathbb{Z}[X]$.*
(ii) $\frac{1}{2}$ este rădăcină din $\mathbb{Q}$ a lui $f = 2X^2 + X - 1 \in \mathbb{Z}[X]$.
(iii) $\frac{-1+i\sqrt{3}}{2}$ este rădăcină din $\mathbb{C}$ a lui $f = X^3 - 1 \in \mathbb{R}[X]$.

Am văzut că R domeniu de integritate implică $R[X]$ domeniu de integritate, deci are sens să considerăm problema divizibilităţii pentru două polinoame din $R[X]$.

Propoziţia 40. *Fie $R \subseteq S$ un suprainel al lui R, S domeniu de integritate. Dacă $s \in S$ şi $f \in R[X]$ atunci s este rădăcină a lui f dacă şi numai dacă $X - s \mid f$ în $S[X]$.*

Demonstraţie: $\exists\,!\ q, r \in S[X]$ a.î. $f = (X - s)q + r$ cu $grad(r) < 1$. În plus, $r = \widetilde{f}(s)$, deci s este rădăcină a lui f $\Leftrightarrow$ $\widetilde{f}(s) = 0$ $\Leftrightarrow$ $f = (X - s)q$ în $S[X]$ $\Leftrightarrow$ $X - s \mid f$ în $S[X]$. $\square$

Theorem 41. *Dacă R este domeniu de integritate şi $f \in R[X]$ are gradul $n \in \mathbb{N}$ atunci f are cel mult n rădăcini în R.*

Demonstraţie: Inducţie după n.

Dacă $n = 0$ atunci f este polinom constant nenul (altfel are gradul $-\infty$), deci nu are rădăcini.

Presupunem $n \geq 1$. Dacă f nu are rădăcini în R e gata: $0 \leq n$. Altfel, dacă $a \in R$ este rădăcină a lui f, din propoziţia precedentă avem $f = (X - a)q$, pentru un $q \in R[X]$. Cum R este domeniu de integritate, $grad(q) = n - 1$, deci q are cel mult $n - 1$ rădăcini în R. Pe de altă parte, dacă $a \neq b \in R$ este o altă rădăcină a lui f în R atunci $0 = \widetilde{f}(b) = (b - a)\widetilde{q}(b)$ şi cum R este domeniu iar $b - a \neq 0$ rezultă că b este rădăcină a lui q în R. Deducem astfel că f are cel mult $1 + (n - 1) = n$ rădăcini în R. $\square$

Observaţia 42. *Rezultatul din teorema precedentă nu rămâne adevărat dacă R are divizori ai lui zero nenuli: dacă $R = \mathbb{Z} \times \mathbb{Z}$ şi $f = (1, 0)X \in R[X]$ atunci f are gradul 1 şi o infinitate de rădăcini în R fiindcă $\widetilde{f}(0, k) = (1, 0)(0, k) = (0, 0)$, $\forall\ k \in \mathbb{Z}$.*

De asemenea, dacă $R = \mathbb{Z}_8$ şi $f = X^2 - \hat{1} \in \mathbb{Z}_8[X]$, atunci f are gradul 2 şi 4 rădăcini în R, anume $\hat{1}, \hat{3}, \hat{5}$ şi $\hat{7}$.

Corolar 43. *Fie R un domeniu de integritate şi $f, g \in R[X]$ cu $\widetilde{f} = \widetilde{g} : R \to R$. Dacă R este infinit atunci $f = g$.*

Demonstraţie: $f - g \in R[X]$ are ca rădăcină orice element din R. Cum R este infinit, rezultă $f - g = 0 \Leftrightarrow f = g$. $\square$

Corolar 44. *Fie R un domeniu de integritate şi $f, g \in R[X]$ cu $grad(f) \leq grad(g) = n \in \mathbb{N}$. Dacă $\widetilde{f}(a) = \widetilde{g}(a)$ pentru $n + 1$ elemente a din R atunci $f = g$.*

Demonstraţie: Dacă $0 \neq f - g \in R[X]$ atunci $f - g \neq 0$ are gradul $grad(f - g) \leq grad(g) = n$ şi cel puţin $n+1$ rădăcini, o contradicţie. $\square$

Definiţia 45. *Fie R un domeniu de integritate, $f \in R[X]$ şi $s \in S \supseteq R$. Spunem că s este rădăcină a lui f cu ordin de multiplicitate $m \in \mathbb{N}^*$ dacă*

$$(X - s)^m \mid f \quad \text{şi } (X - s)^{m+1} \nmid f.$$

Echivalent, $f = (X - s)^m g$ cu $g \in S[X]$ a.î. $\widetilde{g}(s) \neq 0$.

Propoziţia 46. *Fie R un domeniu de integritate, $0 \neq f \in R[X]$ şi $a_1, \cdot, a_t \in S \supseteq R$ rădăcini ale lui f în S cu ordine de multiplicitate $m_1, \cdots, m_t$. Atunci f se scrie*

$$f = (X - a_1)^{m_1} \cdots (X - a_t)^{m_t} g$$

cu $g \in S[X]$ *pentru care* $a_1, \cdots, a_t$ *nu sunt rădăcini ale sale în* S.

Demonstraţie: Inducţie după t, similară cu cea a teoremei 41. □

Corolar 47. (Relaţiile lui Viétè) *Fie* R *un domeniu de integritate,* $f = \sum_{i=1}^{n} a_i X^i \in R[X]$ *un polinom de grad* $n \geq 1$ *ce admite rădăcinile* $x_1, \cdots, x_n \in S \supseteq R$. *Atunci* $f = a_n(X-x_1)\cdots(X-x_n)$ *iar următoarele relaţii au loc:*

$a_n(x_1 + \cdots + x_n) = -a_1;$
$a_n(x_1x_2 + \cdots + x_1x_n + x_2x_3 + \cdots x_2x_n + \cdots + x_{n-1}x_n) = a_2;$
$\vdots$
$a_n x_1 x_2 \cdots x_n = (-1)^n a_0.$

Demonstraţie: Prima parte rezultă din propoziţia precedentă, din R domeniu rezultă g de grad 1, mai exact egal cu a_n. Relaţiile lui Viétè se obţin identificând coeficienţii din cele două scrieri ale lui f. □

Corolar 48. *(Teorema lui Wilson) Dacă* p *este număr prim atunci* $(p-1)! \equiv -1 (\mathrm{mod}\ p)$.

Demonstraţie: $f = X^{p-1} - \hat{1} \in \mathbb{Z}_p[X]$ are ca rădăcini elementele din $\mathbb{Z}_p \backslash \{\hat{0}\} := \mathbb{Z}_p^{\times}$ (cf. teoremei lui Lagrange; $\mathbb{Z}_p^{\times}$ este grup finit cu $p-1$ elemente). Conform ultimei relaţii Viétè avem

$$\hat{1} \cdot \hat{2} \cdots \widehat{p-1} = (-1)^{p-1}(-1)\hat{1} \text{ în } \mathbb{Z}_p \iff (p-1)! \equiv (-1)^p (\mathrm{mod}\ p).$$

Dacă $p = 2$ atunci $1! \equiv -1(\mathrm{mod}\ 2)$ este evidentă. Dacă p este impar atunci se obţine $(p-1)! \equiv -1(\mathrm{mod}\ p)$. □

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.