ARITMETICA ÎN $\mathbb{Z}$ ŞI $K[X]$

1. Divizibilitate. Algoritmul lui Euclid.

Să începem prin a observa că inelele $\mathbb{Z}$ şi $K[X]$ (K corp comutativ) sunt domenii de integritate, $U(\mathbb{Z}) = \{-1, 1\}$ şi $U(K[X]) = K^{\times}$.

Teorema 1.1. (Teorema de împărţire cu rest în $\mathbb{Z}$) *Fie $a, b \in \mathbb{Z}$, $b \neq 0$. Atunci există $q, r \in \mathbb{Z}$ unice cu proprietatea că $a = bq + r$ şi $0 \leq r < |b|$.*

Proof. Existenţa. Fie $r = \min\{a - bx : x \in \mathbb{Z} \text{ şi } a - bx \geq 0\}$. Scriem $r = a - bq$, $q \in \mathbb{Z}$. Dacă $r \geq |b|$, atunci $0 \leq a - b(q + \operatorname{sgn}(b)) < r$, contradicţie. Aşadar $r < |b|$. *Unicitatea.* Fie $q', r' \in \mathbb{Z}$ cu proprietatea că $a = bq' + r'$ şi $0 \leq r' < |b|$. Atunci $b(q - q') = r' - r$ şi de aici obţinem $|b||q - q'| = |r' - r| < |b|$, deci $q = q'$ şi $r = r'$. $\square$

Definiţia 1.2. *Numărul întreg q din teorema de mai sus se numeşte* câtul împărţirii lui a la b, *iar r se numeşte* restul împărţirii lui a la b.

Exemplul 1.3. Fie $a = -17$ şi $b = 2$. Scriem $-17 = 2(-9) + 1$, deci $q = -9$ şi $r = 1$.

Remarca 1.4. Dacă în teorema de împărţire cu rest în $\mathbb{Z}$ cerem $|r| < |b|$ în loc de $0 \leq r < |b|$, atunci existenţa rămâne adevărată însă nu mai avem unicitate pentru cât şi rest: de exemplu, $5 = 2 \cdot 2 + 1 = 2 \cdot 3 + (-1)$.

În cele ce urmează R va desemna $\mathbb{Z}$ sau $K[X]$.

Definiţia 1.5. *Fie $a, b \in R$. Spunem că b* divide *a dacă există $c \in R$ astfel încât $a = bc$ şi scriem $b \mid a$. Se mai spune că b* este divizor al lui *a sau că a* este multiplu al lui *b.*

Remarca 1.6. (i) $1 \mid a$ şi $a \mid 0$ pentru orice $a \in R$.
(ii) Dacă $b \neq 0$, atunci $b \mid a$ dacă şi numai dacă restul împărţirii lui a la b este 0.
(iii) Dacă $b \mid a$, atunci $|b| \leq |a|$ pentru $R = \mathbb{Z}$, respectiv $\deg b \leq \deg a$ pentru $R = K[X]$.

Să enunţăm acum câteva proprietăţi simple ale relaţiei de divizibilitate.

Propoziţia 1.7. *(i) $a \mid b$ dacă şi numai dacă $bR \subseteq aR$.*
(ii) $a \mid a$ oricare ar fi $a \in R$.
(iii) $a \mid b$ şi $b \mid c \Rightarrow a \mid c$.
(iv) $a \mid b_i$, $\forall\, i = 1, \ldots, n \Rightarrow a \mid \sum_{i=1}^{n} \alpha_i b_i$, $\forall\, \alpha_i \in R$.

Definiţia 1.8. *Fie $a, b \in R$. Spunem că a şi b* sunt asociate în divizibilitate *dacă $a \mid b$ şi $b \mid a$.*

Notaţie: $a \sim b$.

Remarca 1.9. (i) "$\sim$" este o relaţie de echivalenţă pe R.
(ii) $a \sim 1$ dacă şi numai dacă $a \in U(R)$.

Din propoziţia 1.7(i) rezultă imediat că a este asociat în divizibilitate cu b dacă şi numai dacă $aR = bR$.

Propoziţia 1.10. *Fie $a, b \in R$. Atunci a şi b sunt asociate în divizibilitate dacă şi numai dacă $b = \pm a$ pentru $R = \mathbb{Z}$, respectiv $b = au$, $u \in K^\times$ pentru $R = K[X]$.*

Definiţia 1.11. *Fie $a, b \in R$. Spunem că un element $d \in R$ este un* cel mai mare divizor comun *al elementelor a, b dacă:*
(i) $d \mid a$ şi $d \mid b$,
(ii) $d' \mid a$ şi $d' \mid b$ implică $d' \mid d$.

Notaţie: c.m.m.d.c.(a, b) sau gcd(a, b) sau (a, b).

Definiţia 1.12. *Fie $a, b \in R$. Spunem că un element $m \in R$ este un* cel mai mic multiplu comun *al elementelor a, b dacă:*
(i) $a \mid m$ şi $b \mid m$,
(ii) $a \mid m'$ şi $b \mid m'$ implică $m \mid m'$.

Notaţie: c.m.m.m.c.(a, b) sau lcm(a, b) sau $[a, b]$.

Remarca 1.13. (i) Dacă $d_1, d_2 \in R$ sunt fiecare un cel mai mare divizor comun al elementelor a, b, atunci $d_1 \sim d_2$. Reciproc, dacă $d_1 \sim d_2$ şi d_1 este un cel mai mare divizor comun al elementelor a, b, atunci şi d_2 este un cel mai mare divizor comun al elementelor a, b. De aceea vom considera ca fiind c.m.m.d.c.(a, b) orice element al lui R care este un cel mai mare divizor comun al elementelor a, b şi vom spune că c.m.m.d.c.(a, b) *este unic până la o asociere în divizibilitate.*
(ii) Consideraţii similare sunt valabile şi pentru cel mai mic multiplu comun a două elemente $a, b \in R$.

Definiţia 1.14. *Două elemente $a, b \in R$ se numesc* prime între ele *sau* relativ prime *dacă* c.m.m.d.c.$(a, b) = 1$.

Vom demonstra că în inelul R orice două elemente au un c.m.m.d.c.

Algoritmul lui Euclid. Fie $a, b \in R$, $b \neq 0$. Scriem $a = bq_1 + r_1$ cu $0 \leq r_1 < |b|$, respectiv $\deg r_1 < \deg b$. Dacă $r_1 \neq 0$, atunci scriem $b = r_1 q_2 + r_2$ cu $0 \leq r_2 < r_1$, respectiv $\deg r_2 < \deg r_1$. Dacă $r_2 \neq 0$, atunci scriem $r_1 = r_2 q_3 + r_3$ cu $0 \leq r_3 < r_2$, respectiv $\deg r_3 < \deg r_2$ şi aşa mai departe. Obţinem astfel un şir strict descrescător de numere naturale $r_1 > r_2 > \cdots$, respectiv $\deg r_1 > \deg r_2 > \cdots$ care nu poate fi infinit, deci va exista un $n \in \mathbb{N}^*$ astfel încât $r_n \neq 0$ şi $r_{n+1} = 0$.

Să arătăm că r_n este un c.m.m.d.c. al elementelor $a, b \in R$. Deoarece $r_{n+1} = 0$ avem $r_{n-1} = r_n q_{n+1}$, deci $r_n \mid r_{n-1}$. Din relaţia $r_{n-2} = r_{n-1} q_n + r_n$ deducem că $r_n \mid r_{n-2}$. Astfel obţinem $r_n \mid r_i$ pentru orice $i = 1, \ldots, n$. Din relaţia $b = r_1 q_2 + r_2$ rezultă $r_n \mid b$ iar apoi din $a = bq_1 + r_1$ rezultă $r_n \mid a$. În concluzie, r_n este un divizor comun al lui a şi b.

Fie acum d un divizor comun al lui a şi b. Din relaţia $a = bq_1 + r_1$ deducem că $d \mid r_1$ şi pas cu pas obţinem $d \mid r_i$ pentru orice $i = 1, \ldots, n$. În particular, $d \mid r_n$.

În concluzie, c.m.m.d.c.(a, b) este ultimul rest nenul din algoritmul lui Euclid aplicat perechii (a, b).

Exemplul 1.15. Fie $a = 18$ şi $b = 24$. Avem $18 = 24 \cdot 0 + 18$, $24 = 18 \cdot 1 + 6$, $18 = 6 \cdot 3$. Aşadar $(18, 24) = 6$.

Exerciţiul 1.16. Calculaţi $(24, 54)$ în $\mathbb{Z}$ cu algoritmul lui Euclid.

Exerciţiul 1.17. Calculaţi $(X^4 - 4X^3 + 1, X^3 - 3X^2 + 1)$ în $\mathbb{R}[X]$ cu algoritmul lui Euclid.

Propoziţia 1.18. *Fie $a, b, c \in R \setminus \{0\}$.*
(i) Dacă $d = (a, b)$, atunci există a', b' cu $a = da'$, $b = db'$ şi $(a', b') = 1$.
(ii) $(ac, bc) = (a, b)c$.
(iii) $(a, b) = 1$ şi $(a, c) = 1$ implică $(a, bc) = 1$.
(iv) (Lema lui Euclid) *$a \mid bc$ şi $(a, b) = 1$ implică $a \mid c$.*
(v) $a \mid c$, $b \mid c$ şi $(a, b) = 1$ implică $ab \mid c$.
(vi) Există $[a, b]$ şi $(a, b)[a, b]$ este asociat în divizibilitate cu ab.

Proof. (i) Fie $d' = (a', b')$. Deoarece $d' \mid a'$ şi $d' \mid b'$ rezultă că $dd' \mid a$ şi $dd' \mid b$, deci $dd' \mid d$ şi cum $d \neq 0$ obţinem $d' \mid 1$, adică $d' \sim 1$.
(ii) Egalitatea rezultă din algoritmul lui Euclid.
(iii) Fie $d = (a, bc)$. Din $d \mid a$ şi $a \mid ac$ rezultă că $d \mid ac$, deci $d \mid (ac, bc)$. Din (ii) obţinem $d \mid c$ şi cum $d \mid a$ rezultă $d \mid 1$.
(iv) Din (ii) avem că $(ac, bc) = c$. Dar $a \mid ac$ şi $a \mid bc$, deci $a \mid c$.
(v) Din (ii) avem că $(ac, bc) = c$. Dar $ab \mid ac$ şi $ab \mid bc$, deci $ab \mid c$.
(vi) Fie $d = (a, b)$. Atunci există a', b' cu $a = da'$, $b = db'$ şi $(a', b') = 1$. Fie $m = da'b'$. Deoarece $m = ab' = ba'$ rezultă $a \mid m$ şi $b \mid m$. Fie $m' \in R$ astfel încât $a \mid m'$ şi $b \mid m'$. Avem că $a' \mid \frac{m'}{d}$ şi $b' \mid \frac{m'}{d}$. Din (v) rezultă $a'b' \mid \frac{m'}{d}$, deci $m \mid m'$. □

Propoziţia 1.19. *Orice ideal al lui R este principal.*

Proof. Fie I un ideal nenul al lui R. Fie $a \in I$, $a \neq 0$ cu $|a|$ minim dacă $R = \mathbb{Z}$, respectiv $\deg a$ minim dacă $R = K[X]$. Vom arăta că $I = aR$. Evident, $aR \subseteq I$. Reciproc, fie $b \in I$. Atunci $b = aq + r$ cu $0 \leq r < |a|$, respectiv $\deg r < \deg a$. Dar $r = b - aq \in I$ şi atunci neapărat $r = 0$, deci $b = aq \in aR$. □

Propoziţia 1.20. *Fie $a, b \in R$. Avem:*
(i) $aR + bR = (a, b)R$;
(ii) $aR \cap bR = [a, b]R$.

Proof. (i) Deoarece R este inel principal, $aR + bR$ este ideal principal, deci există $d \in R$ cu proprietatea că $aR + bR = dR$. Cum $aR \subseteq dR$ şi $bR \subseteq dR$ rezultă $d \mid a$ şi $d \mid b$. Fie acum $d' \in R$ cu proprietatea că $d' \mid a$ şi $d' \mid b$, equivalent $aR \subseteq d'R$ şi $bR \subseteq d'R$. Avem $dR = aR + bR \subseteq d'R$, deci $d' \mid d$.
(ii) Deoarece R este inel principal, $aR \cap bR$ este ideal principal, deci există $m \in R$ cu proprietatea că $aR \cap bR = mR$. Cum $mR \subseteq aR$ şi $mR \subseteq bR$ rezultă $a \mid m$ şi $b \mid m$. Fie acum $m' \in R$ cu proprietatea că $a \mid m'$ şi $b \mid m'$, equivalent $m'R \subseteq aR$ şi $m'R \subseteq bR$. Avem $m'R \subseteq aR \cap bR = mR$, deci $m \mid m'$. □

Corolarul 1.21. *Fie $a, b \in R$ şi $d = (a, b)$. Atunci există $r, s \in R$ astfel încât $d = ar + bs$.*

Remarca 1.22. Folosind corolarul precedent putem da o altă demonstraţie propoziţiei 1.18.

Exerciţiul 1.23. Determinaţi $(X^2 - 1)\mathbb{Q}[X] \cap (X^3 - 1)\mathbb{Q}[X]$ şi $(X^2 - 1)\mathbb{Q}[X] + (X^3 - 1)\mathbb{Q}[X]$.

2. Elemente prime. Elemente ireductibile

În continuare R va desemna $\mathbb{Z}$ sau $K[X]$.

Definiţia 2.1. *(i) Un element $p \in R$ se numeşte* prim *dacă $p \neq 0$, $p \notin U(R)$ şi $p \mid ab$ implică $p \mid a$ sau $p \mid b$.*
(ii) Un element $q \in R$ se numeşte ireductibil *dacă $q \neq 0$, $q \notin U(R)$ şi $q = ab$ implică $a \in U(R)$ sau $b \in U(R)$.*
Un element care nu este ireductibil se numeşte reductibil.

Remarca 2.2. Un element asociat cu un element prim (ireductibil) este de asemenea element prim (ireductibil).

Propoziţia 2.3. *Orice element prim este ireductibil.*

Proof. Dacă $p \in R$ este element prim şi $p = ab$, atunci $p \mid ab$ şi de aici rezultă $p \mid a$ sau $p \mid b$. Să presupunem că $p \mid a$. Atunci există $a' \in R$ astfel încât $a = pa'$ şi înlocuind în $p = ab$ obţinem $p = pa'b$, de unde $1 = a'b$, deci $b \in U(R)$. □

Este adevărat şi reciproc.

Propoziţia 2.4. *Orice element ireductibil este prim.*

Proof. Fie $q \in R$ un element ireductibil. Să presupunem că $q \mid ab$. Fie $d = (q, a)$. Scriem $q = dq'$ şi $a = da'$. Deoarece q este ireductibil rezultă $d \in U(R)$ sau $q' \in U(R)$. În primul caz $1 = (q, a)$ şi din Lema lui Euclid obţinem $q \mid b$. În cazul al doilea $q = (q, a)$ şi astfel $q \mid a$. □

Remarca 2.5. (i) Un număr $p \in \mathbb{Z}$ este *prim* dacă $p \notin \{-1, 0, 1\}$ şi are ca divizori doar pe ± 1 şi $\pm p$.
(ii) Un polinom $f \in K[X]$ este *ireductibil* dacă nu se poate scrie ca produs de două polinoame de grad ≥ 1.

Definiţia 2.6. *Un număr întreg care nu este prim se numeşte* compus*, iar un polinom care nu este ireductibil se numeşte* reductibil*.*

Exemplul 2.7. (i) Numerele $\pm 2, \pm 3, \pm 5, \ldots$ sunt numere prime.
(ii) X este polinom ireductibil, iar X^2 este reductibil.

Propoziţia 2.8. *(i) Orice polinom de gradul întâi din $K[X]$ este ireductibil.*
(ii) Un polinom de grad 2 sau 3 din $K[X]$ este ireductibil dacă şi numai dacă nu are rădăcini în K.

Proof. (i) Evident.
(ii) În general, un polinom ireductibil $f \in K[X]$ nu are rădăcini în K. Aceasta rezultă imediat din lema lui Bézout. Reciproc, dacă $f \in K[X]$ cu $\deg f = 2, 3$ şi nu are rădăcini în K, atunci f este ireductibil, altminteri s-ar descompune într-un produs de două polinoame dintre care cel puţin unul are gradul 1. Dar orice polinom de grad 1 din $K[X]$ are o rădăcină în K, contradicţie. □

Exemplul 2.9. (i) Polinomul $X^2 - 2$ este ireductibil în $\mathbb{Q}[X]$, dar este reductibil în $\mathbb{R}[X]$.
(ii) Polinoamele $X^2 + X + 1$ şi $X^3 + X + 1$ sunt ireductibile în $\mathbb{Z}_2[X]$. Pe de altă

parte, polinomul $X^4 + X^2 + 1$ nu are rădăcini în $\mathbb{Z}_2$, dar este reductibil în $\mathbb{Z}_2[X]$: $X^4 + X^2 + 1 = (X^2 + X + 1)^2$.

Exerciţiul 2.10. Determinaţi polinoamele ireductibile de grad ≤ 5 din $\mathbb{Z}_2[X]$.

Exerciţiul 2.11. Descompuneţi polinomul $X^{56} - X^{49} - X^7 + 1$ în produs de polinoame ireductibile în $\mathbb{Z}_7[X]$.

Propoziţia 2.12. *Fie $p \in R$ element prim. Atunci inelul factor R/pR este corp.*

Proof. Fie $\widehat{a} \in R/pR$, $\widehat{a} \neq \widehat{0}$. Aceasta înseamnă că $a \notin pR$, adică $p \nmid a$. Aşadar $(p, a) = 1$. Atunci există $u, v \in R$ cu proprietatea că $pu + av = 1$. Trecând la clase de resturi modulo idealul pR obţinem $\widehat{a}\,\widehat{v} = \widehat{1}$, deci $\widehat{a}$ este inversabil. $\square$

Remarca 2.13. Rezultatul de mai sus ne ajută să construim corpuri finite. De exemplu, $\mathbb{Z}_2[X]/(X^2 + X + 1)$ este corp finit cu 4 elemente.

Propoziţia 2.14. *Dacă $a \in R$ este un element nenul şi neinversabil, atunci acesta admite o descompunere în produs finit de elemente prime şi această scriere este unică (până la o asociere în divizibilitate şi abstracţie făcând de ordinea factorilor).*

Proof. Existenţa. Presupunem că există $a \in R$ nenul şi neinversabil care nu se scrie ca produs de numere prime, respectiv ca produs de polinoame ireductibile. Îl alegem pe a de modul, respectiv grad minim cu această proprietate. Cum a nu poate fi număr prim, respectiv polinom ireductibil, există $a_1, a_2 \in R$ nenule şi neinversabile astfel încât $a = a_1 a_2$. Atunci $|a_i| < |a|$, respectiv $\deg a_i < \deg a$ pentru $i = 1, 2$. Datorită alegerii lui a, elementele a_1, a_2 se pot scrie ca produs de numere prime, respectiv ca produs de polinoame ireductibile. Dar atunci şi a este produs de numere prime, respectiv produs de polinoame ireductibile, contradicţie.
Unicitatea. Fie $a = p_1 \cdots p_m = p'_1 \cdots p'_n$ cu $p_i, p'_j \in R$ elemente prime. Vom demonstra (prin inducţie după m) că $m = n$ şi există $\sigma \in S_n$ astfel încât $p_i \sim p'_{\sigma(i)}$ pentru orice $i = 1, \ldots, m$.
Dacă $m = 1$, atunci $p_1 = p'_1 \cdots p'_n$. Deoarece p_1 este prim acesta este ireductibil şi rezultă că $n = 1$.
Presupunem acum că $m > 1$. Din $p_m \mid p'_1 \cdots p'_n$ obţinem că există j astfel încât $p_m \mid p'_j$ şi cum p'_j este ireductibil rezultă $p_m \sim p'_j$. Să considerăm $j = n$, scriem $p_m = up'_n$ cu $u \in U(R)$ şi prin simplificare obţinem $p_1 \cdots (up_{m-1}) = p'_1 \cdots p'_{n-1}$. Acum aplicăm ipoteza de inducţie şi deducem că $m - 1 = n - 1$ şi există $\sigma' \in S_{n-1}$ astfel încât $p_i \sim p'_{\sigma'(i)}$ pentru orice $i = 1, \ldots, m - 1$. $\square$

Corolarul 2.15. *Fie $a, b \in R$ nenule şi neinversabile. Dacă $a = \prod_{i=1}^r p_i^{k_i}$, $b = \prod_{i=1}^r p_i^{l_i}$, unde p_i sunt elemente prime, atunci $(a, b) = \prod_{i=1}^r p_i^{\min(k_i, l_i)}$ şi $[a, b] = \prod_{i=1}^r p_i^{\max(k_i, l_i)}$.*

Teorema 2.16. *Mulţimea numerelor prime pozitive, respectiv mulţimea polinoamelor ireductibile şi monice din $K[X]$ este infinită.*

Proof. Presupunem că mulţimea numerelor prime pozitive, respectiv mulţimea polinoamelor ireductibile şi monice din $K[X]$ este finită. Să notăm cu $p_1, \ldots, p_r$ elementele sale. Atunci $N = p_1 \cdots p_r + 1$ admite o descompunere în factori primi, respectiv polinoame ireductibile şi de aici rezultă că există $i \in \{1, \dots, r\}$ cu proprietatea că $p_i \mid N$. Dar cum $p_i \mid p_1 \cdots p_r$ rezultă $p_i \mid 1$, contradicţie. $\square$

Exerciţiul 2.17. Determinaţi c.m.m.d.c. şi c.m.m.m.c. pentru polinoamele $f = (X-1)(X^2-1)(X^3-1)(X^4-1)$ şi $g = (X+1)(X^2+1)(X^3+1)(X^4+1)$ din $\mathbb{Q}[X]$.

3. Teorema fundamentală a algebrei

Teorema 3.1. (Teorema lui Kronecker) *Fie K un corp şi $f \in K[X]$ cu $\deg f \geq 1$. Atunci există o extindere L a lui K în care f are cel puţin o rădăcină.*

Proof. Deoarece f se descompune în produs de polinoame ireductibile este suficient să demonstrăm teorema pentru cazul în care f este ireductibil şi de grad ≥ 2. Fie $L = K[X]/(f)$. Ştim că L este corp iar morfismul canonic $K \to L$ este injectiv, deci putem considera că L este o extindere a lui K. Fie $\alpha = X \bmod (f)$ (clasa lui X modulo idealul (f)). Este imediat că $\alpha \in L$ şi $f(\alpha) = 0$. $\square$

Corolarul 3.2. *Fie K un corp şi $f \in K[X]$ cu $\deg f \geq 1$. Atunci există o extindere L a lui K în care f are toate rădăcinile.*

Teorema 3.3. (Teorema fundamentală a algebrei) *Orice polinom $f \in \mathbb{C}[X]$ cu $\deg f \geq 1$ are cel puţin o rădăcină în $\mathbb{C}$.*

Proof. Este suficient să demonstrăm teorema pentru polinoame $f \in \mathbb{R}[X]$. Dacă $f \in \mathbb{C}[X]$, $f = a_0 + a_1X + \cdots + a_nX^n$, considerăm $\overline{f} = \overline{a}_0 + \overline{a}_1X + \cdots + \overline{a}_nX^n$, unde $\overline{a}_i$ este conjugatul complex al lui a_i. Fie $g = f\overline{f}$. Avem că $g \in \mathbb{R}[X]$ şi dacă teorema este adevărată pentru polinoamele din $\mathbb{R}[X]$, atunci există $z_0 \in \mathbb{C}$ astfel încât $g(z_0) = 0$. Dar $g(z_0) = f(z_0)\overline{f}(z_0)$, de unde $f(z_0) = 0$ sau $\overline{f}(z_0) = 0$, adică $f(\overline{z}_0) = 0$, deci f are o rădăcină complexă.
Presupunem acum că $f \in \mathbb{R}[X]$. Fie $n = \deg f$ şi scriem $n = 2^km$ cu $k \geq 0$ şi m impar. Vom face demonstraţia prin inducţie după k.
Pentru $k = 0$ avem $\deg f = m$ impar şi atunci există $x_0 \in \mathbb{R}$ astfel încât $f(x_0) = 0$.
În cazul în care $k \geq 1$ considerăm L o extindere a lui $\mathbb{C}$ în care f are toate rădăcinile. Fie $x_1, \dots, x_n \in L$ rădăcinile lui f şi $a \in \mathbb{R}$ arbitrar. Fie $z_{ij}^a = x_ix_j + a(x_i + x_j)$ pentru orice $1 \leq i, j \leq n$. Considerăm polinomul

$$g_a = \prod_{1 \leq i < j \leq n} (X - z_{ij}^a).$$

Evident $g_a \in L[X]$ şi $\deg g_a = \binom{n}{2} = 2^{k-1}m(2^km - 1)$. Se observă că $m(2^km-1)$ este număr impar, deci putem aplica ipoteza de inducţie lui g_a cu condiţia ca $g_a \in \mathbb{R}[X]$. Să demonstrăm acest lucru. Se observă mai întâi că polinomul g_a este simetric în $x_1, \dots, x_n$, deoarece dacă schimbăm pe x_i cu x_j în g_a acesta nu se modifică. Aşadar coeficienţii lui g_a sunt polinoame simetrice în $x_1, \dots, x_n$ şi din teorema fundamentală a polinoamelor simetrice rezultă că aceştia sunt polinoame de coeficienţii lui f, deci aparţin lui $\mathbb{R}$.
Din ipoteza de inducţie există o pereche (i, j) cu $i < j$ astfel încât $z_{ij}^a \in \mathbb{C}$. Cum a a fost ales arbitrar va exista o pereche (i, j) cu $i < j$ şi $a, b \in \mathbb{R}$, $a \neq b$, cu proprietatea că $z_{ij}^a, z_{ij}^b \in \mathbb{C}$. Rezultă $z_{ij}^a - z_{ij}^b \in \mathbb{C}$, deci $x_i + x_j \in \mathbb{C}$ şi de aici $x_ix_j \in \mathbb{C}$. Aşadar x_i, x_j sunt rădăcinile unei ecuaţii de gradul al doilea cu coeficienţi complecşi, deci sunt numere complexe. $\square$

Corolarul 3.4. *(i) Fie $f \in \mathbb{C}[X]$ cu $\deg f \geq 1$. Atunci f este ireductibil dacă şi numai dacă $\deg f = 1$.*
(ii) Fie $f \in \mathbb{R}[X]$ cu $\deg f \geq 1$. Atunci f este ireductibil dacă şi numai dacă $\deg f = 1$ sau $\deg f = 2$ şi f nu are rădăcini reale.

Corolarul 3.5. *(i) Fie $f \in \mathbb{C}[X]$ cu $\deg f \geq 1$. Atunci f se scrie în mod unic sub forma*

$$f = a(X - a_1)^{k_1} \cdots (X - a_m)^{k_m}$$

cu $a \in \mathbb{C}^\times$, $a_1, \ldots, a_m \in \mathbb{C}$ distincte şi $k_1, \ldots, k_m \in \mathbb{N}^*$.
(ii) Fie $f \in \mathbb{R}[X]$ cu $\deg f \geq 1$. Atunci f se scrie în mod unic sub forma

$$f = a(X - a_1)^{k_1} \cdots (X - a_r)^{k_r}(X^2 + b_1X + c_1)^{l_1} \cdots (X^2 + b_sX + c_s)^{l_s}$$

cu $a \in \mathbb{R}^\times$, $a_1, \ldots, a_r \in \mathbb{R}$ distincte, $b_1, c_1, \ldots, b_s, c_s \in \mathbb{R}$ cu $b_i^2 < 4c_i$ pentru orice $i = 1, \ldots, s$ şi $k_1, \ldots, k_r, l_1, \ldots, l_s \in \mathbb{N}^*$.

Remarca 3.6. În $\mathbb{Q}[X]$ există polinoame ireductibile de orice grad. De exemplu, polinomul $X^n - 2$ este ireductibil în $\mathbb{Q}[X]$ pentru orice $n \geq 1$.

Exerciţiul 3.7. Arătaţi că polinomul $X^n - 2$ este ireductibil în $\mathbb{Q}[X]$ pentru orice $n \geq 1$.

Exerciţiul 3.8. Descompuneţi polinomul $X^n - 1$, $1 \leq n \leq 6$, în produs de polinoame ireductibile în $\mathbb{Q}[X]$, $\mathbb{R}[X]$, respectiv $\mathbb{C}[X]$.