

Teorema Fundamentală a Algebrei.

Că o aplicație a polinoamelor simetrice și a aritmeticii din $K[x]$ vom demonstra în această secțiune următoare.

Teoremă. Fie $f \in \mathbb{C}[x]$ cu $\deg(f) \geq 1$. Atunci f are o rădăcină în \mathbb{C} .

Aveam nevoie de mai multe prezentări.

Propozitie. Fie K un corp comutativ și $g \in K[x]$ un polinom irreductibil. Atunci (g) este ideal maxim din $K[x]$.

Dem. Cum g e irreductibil $\Rightarrow g$ nu este inversabil, deci $(g) \neq K[x]$.

Fie I un ideal al lui $K[x]$ cu $(g) \subset I$. Arătăm că $I = (g)$ sau $I = K[x]$.

Cum orice ideal al lui $K[x]$ este principal, rezultă că există $h \in K[x]$ cu $I = (h)$. Atunci $(g) \subset (h)$, de unde ~~$g \in (h)$~~ , adică există $u \in K[x]$ cu $g = uh$.

Cum g este irreductibil rezultă că sau h este inversabil, și atunci $I = (h) = K[x]$, sau u este inversabil, și atunci $g \sim h$, de unde $I = (h) = (g)$.

Corolar. Fie g un polinom irreductibil în $K[x]$, K corp comutativ. Atunci încelul factor $\frac{K[x]}{(g)}$ este corp.

Dem. Rezulta imediat din faptul că încelul factor al unui încel comutativ printr-un ideal maxim este corp.

Vom avea nevoie de următoare leme simplă, care spune că dacă un corp este în bijectie cu o altă mulțime,

stunici structurile de corp se pot transfera pe respective multimi prin bjectiile date.

Lemă. Fie L un corp și E o multime astfel incât există $\gamma: E \rightarrow L$ funcție bijectivă. Atunci operațiile definite prin $u \oplus v \stackrel{\text{def.}}{=} \gamma^{-1}(\gamma(u) + \gamma(v))$, $u \odot v \stackrel{\text{def.}}{=} \gamma^{-1}(\gamma(u)\gamma(v))$ pt. orice $u, v \in E$, definesc o structură de corp pe E . În plus, γ devine astfel un izomorfism de coruri.

Dem. Verificăm axiomele corpului.

$$\begin{aligned} u \oplus v &= \gamma^{-1}(\gamma(u) + \gamma(v)) = \gamma^{-1}(\gamma(v) + \gamma(u)) = v \oplus u \\ (u \oplus v) \oplus w &= \gamma^{-1}(\gamma(u \oplus v) + \gamma(w)) = \gamma^{-1}(\gamma\gamma^{-1}(\gamma(u) + \gamma(v)) + \gamma(w)) \\ &= \gamma^{-1}(\gamma(u) + \gamma(v) + \gamma(w)) = \gamma^{-1}(\gamma(u) + \gamma(\gamma^{-1}(\gamma(u) + \gamma(v)) + \gamma(w)))) \\ &= \gamma^{-1}(\gamma(u) + \gamma(v \oplus w)) = u \oplus (v \oplus w) \end{aligned}$$

Dacă $0 = 0_L$, atunci $u \oplus \gamma^{-1}(0) = \gamma^{-1}(\gamma(u) + \gamma\gamma^{-1}(0)) = \gamma^{-1}(\gamma(u) + 0)$

$$= \gamma^{-1}(\gamma(u)) = u, \text{ deci } \gamma^{-1}(0) \text{ este element neutru pt. } \oplus.$$

$$u \oplus \gamma^{-1}(-\gamma(u)) = \gamma^{-1}(\gamma(u) + \gamma\gamma^{-1}(-\gamma(u))) = \gamma^{-1}(\gamma(u) - \gamma(u)) = \gamma^{-1}(0),$$

deci $\gamma^{-1}(-\gamma(u))$ este simetricul lui u în raport cu \oplus .

Asadar (E, \oplus) este grup abelian.

$$\begin{aligned} (u \odot v) \odot w &= \gamma^{-1}(\gamma(u \odot v)\gamma(w)) = \gamma^{-1}(\gamma(\gamma^{-1}(\gamma(u)\gamma(v)))\gamma(w)) \\ &= \gamma^{-1}(\gamma(u)\gamma(v)\gamma(w)) = \gamma^{-1}(\gamma(u)\gamma(\gamma^{-1}(\gamma(v)\gamma(w)))) \\ &= \gamma^{-1}(\gamma(u)\gamma(v \odot w)) = u \odot (v \odot w) \end{aligned}$$

Dacă $1 = 1_L$, atunci $u \odot \gamma^{-1}(1) = \gamma^{-1}(\gamma(u)\gamma(\gamma^{-1}(1))) = \gamma^{-1}(\gamma(u)1) = \gamma^{-1}(\gamma(u)) = u$,

și la fel $\gamma^{-1}(1) \odot u = u$, deci $\gamma^{-1}(1)$ este element neutru pt. \odot .

$$u \odot (v \oplus w) = \gamma^{-1}(\gamma(u) \gamma(v \oplus w)) = \gamma^{-1}(\gamma(u) \gamma(\gamma^{-1}(\gamma(v) + \gamma(w))))$$

$$= \gamma^{-1}(\gamma(u) \cdot (\gamma(v) + \gamma(w))) = \gamma^{-1}(\gamma(u) \gamma(v) + \gamma(u) \gamma(w))$$

$$(u \odot v) \oplus (u \odot w) = \gamma^{-1}(\gamma(u \odot v) + \gamma(u \odot w))$$

$$= \gamma^{-1}(\gamma(\gamma^{-1}(\gamma(u) \gamma(v))) + \gamma(\gamma^{-1}(\gamma(u) \gamma(w))))$$

$$= \gamma^{-1}(\gamma(u) \gamma(v) + \gamma(u) \gamma(w)),$$

de unde $u \odot (v \oplus w) = (u \odot v) \oplus (u \odot w)$. Similar se obțin distributivitățile la dreapta a lui \odot față de \oplus .

Dacă $u \in E$, $u \neq \gamma^{-1}(0)$, atunci $\gamma(u) \neq 0$, deci există $\gamma(u)^{-1}$ în L , și astfel $u \odot \gamma^{-1}(\gamma(u)^{-1}) = \gamma^{-1}(\gamma(u) \gamma(\gamma^{-1}(\gamma(u)^{-1})))$

$$= \gamma^{-1}(\gamma(u) \gamma(u)^{-1}) = \gamma^{-1}(1) \quad \text{și}$$

similar $\gamma^{-1}(\gamma(u)^{-1}) \odot u = \gamma^{-1}(1)$, de unde u este inversabil în E , cu inversul $\gamma^{-1}(\gamma(u)^{-1})$.

Pentru următoare (E, \oplus, \odot) este corp.

În plus, $\gamma(u \oplus v) = \gamma(\gamma^{-1}(\gamma(u) + \gamma(v))) = \gamma(u) + \gamma(v)$,

$$\gamma(u \odot v) = \gamma(\gamma^{-1}(\gamma(u) \gamma(v))) = \gamma(u) \gamma(v) \quad \text{și} \quad \gamma(\gamma^{-1}(1)) = 1,$$

decă γ este morfism de coruri. Cum el este și bijectiv, este chiar izomorfism de coruri.

Definiție. Fie K un corp comutativ. Se numește extindere (sau extindere de coruri) a lui K un corp ~~comutativ~~ comutativ E astfel încât K este subcorp al lui E .

Exemplu. \mathbb{R} este extindere a lui \mathbb{Q} , \mathbb{C} este extindere a lui \mathbb{R} .

Urmatăres propozitie este un pas cheie în demonstrarea teoremei fundamentale a algebrei.

Propozitie. Fie K un corp comutativ și $f \in K[x]$ cu $\deg(f) \geq 1$. Atunci există o extindere E a lui K astfel încât f are o rădăcină în E .

Demonstratie: Stim că f se scrie ca produs de polinoame ireductibile în $K[x]$. Fie g unul din între aceste polinoame ireductibile. Avem că $g \nmid f$ și vom arăta că există o extindere E a lui K în care g are o rădăcină; va rezulta că aceea este clar și o rădăcină a lui f în E .

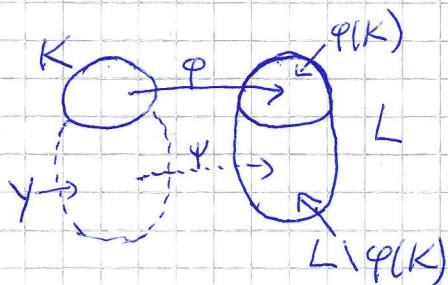
Cum g este ireductibil, avem că $L = \frac{K[x]}{(g)}$ este corp.

Împreună, aplică $\varphi: K \rightarrow \frac{K[x]}{(g)} = L$, $\varphi(a) = \hat{a}$ (clasa modulo idealul (g)), este morfism de corperi (verificare imediată, sau altfel, φ este compunerea $K \xrightarrow{\text{incl.}} K[x] \xrightarrow{\pi} \frac{K[x]}{(g)}$ între proiecția canonică și morfismul inclusiune, ambele fiind morfisme de bule). În particular, φ e injectiv.

Fie $g = a_m x^m + \dots + a_0$. Atunci $\hat{g} = 0$, de unde

$$\hat{a}_m \hat{x}^m + \dots + \hat{a}_0 = 0, \text{ sau } \varphi(a_m) x^m + \dots + \varphi(a_1)x + \varphi(a_0) = 0 \quad (*)$$

unde am notat $x = \hat{x} \in L$.



Considerăm o multime Y care este în bijecție cu $L \setminus \varphi(K)$ și astfel încât $Y \cap K = \emptyset$. Fie $\psi: Y \rightarrow L \setminus \varphi(K)$ o funcție bijectivă.

Eie $E = K \cup Y$. Atunci aplicatia $\gamma: E \rightarrow L$ definita prin

$$\gamma(t) = \begin{cases} \varphi(t), & \text{daca } t \in K \\ \psi(t), & \text{daca } t \in Y \end{cases}, \text{ este bijectie (fieind}$$

"recunoscere" bijectiilor $\varphi \circ \psi$). Aplicand Lemne precedente si obtinem ca pe E se poate defini o structura de corp induc de aceea lui L , via γ . Operatiile care definesc aceasta structura pe E sunt date de

$$u \oplus v = \gamma^{-1}(\gamma(u) + \gamma(v))$$

$$u \circ v = \gamma^{-1}(\gamma(u) \gamma(v)) \quad \forall \text{ orice } u, v \in E,$$

In acest fel E devine corp, iar $\gamma: E \rightarrow L$ izomorfism de corpuri, in particular E este comutativ (pt. cd si Leste).

Observam ca daca $u, v \in K$, atunci

$$u \oplus v = \gamma^{-1}(\gamma(u) + \gamma(v)) = \gamma^{-1}(\varphi(u) + \varphi(v)) = \gamma^{-1}(\underbrace{\varphi(u+v)}_{\in \text{Im } \varphi}) = u+v$$

si in fel $u \circ v = u v$, adica in K noile operatii

\oplus si \circ sunt identice cu $+$ si \cdot ale lui K . Altfel spus, ~~K este subcorpus~~ K (cu structura lui multiset de corp), este subcorp al lui E , sau E este o extindere a lui K .

Aplicand acum γ^{-1} (care este morfism de corpuri) relatiei $(*)$, obtinem $\gamma^{-1}(\varphi(a_m)) (\gamma^{-1}(x))^m + \dots + \gamma^{-1}(\varphi(a_1)) \gamma^{-1}(x) + \gamma^{-1}(\varphi(a_0)) = 0$.

Dor $\gamma^{-1}(\varphi(a)) = a$ pt. orice $a \in K$ (deoarece $\varphi(a) \in \varphi(K)$ si in $\varphi(K)$, γ^{-1} lucraza ca inversa lui $K \xrightarrow{\varphi} \varphi(K)$), de unde $a_m (\gamma^{-1}(x))^m + \dots + a_1 \gamma^{-1}(x) + a_0 = 0$. Aceste dobtin ca x are roodaina $\gamma^{-1}(x)$ in extinderea E a lui K , ceea ce inchide demonstratia.

Corolar. Fie K un corp comutativ și $f \in K[x]$ de grad $n \geq 1$.

Atunci există o extindere E a lui K în care f are n rădăcini (numerote cu multiplicițăți); astfel spus, f este produs de polinoame de grad 1 din $E[x]$.

Demonstratie. Inductie după n (ca pt. orice corp comutativ K orice $f \in K[x]$ de grad n , există o extindere E a lui K în care f are n rădăcini).

Pentru $n=1$: f are grad 1, deci are o rădăcină în K și atunci luna chiar $E = K$.

Bresupunem că este valabil pt. $n-1$ și demonstrăm pt. n , unde $n \geq 2$. Fie f de grad n . Din Propozitie prevedem că există o extindere F a lui K în care f are o rădăcină y . Atunci în $F[x]$ avem $f = (X-y) \cdot h$, unde $h \in F[x]$ are grad $n-1$.

Aplicăm ipoteza de inducție lui h și obținem că există o extindere E a lui F în care h are $n-1$ rădăcini.

Atunci $K \subset F \subset E$, deci E este o extindere a lui K și f are n rădăcini în E .

Propozitie. Fie K un corp comutativ, $f \in K[x]$ de grad $n \geq 1$ și fie E o extindere a lui K în care f are n rădăcini x_1, \dots, x_n (listate cu multiplicițăți). Atunci pentru orice polinom simetric $P \in K[X_1, \dots, X_n]$ avem $P(x_1, \dots, x_n) \in K$.

Demonstratie. Din Teorema fundamentală a polinoamelor simetrice stim că există $F \in K[X_1, \dots, X_n]$ astfel încât $P = F(s_1, \dots, s_n)$, unde s_1, \dots, s_n sunt polinoamele simetrice fundamentale din $K[X_1, \dots, X_n]$. Prin urmare $P = F(s_1, \dots, s_n)$ în $E[X_1, \dots, X_n]$ și evaluând în x_1, \dots, x_n (adică înlocuind

AR

31

$x_1 \in \mathbb{K}, \dots, x_n \in \mathbb{K}$) și obținem

$$P(x_1, \dots, x_n) = F(s_1(x_1, \dots, x_n), \dots, s_n(x_1, \dots, x_n)).$$

Cum x_1, \dots, x_n sunt rădăcinile lui $f \in \mathbb{K}[x]$, rezultă că
lui f îi este asociată $s_1(x_1, \dots, x_n), \dots, s_n(x_1, \dots, x_n) \in \mathbb{K}$,
și atunci cum $F \in \mathbb{K}[x_1, \dots, x_n]$ obținem că

$$F(s_1(x_1, \dots, x_n), \dots, s_n(x_1, \dots, x_n)) \in \mathbb{K}, \text{ de unde că}$$

$$\underline{P(x_1, \dots, x_n) \in \mathbb{K}}.$$

Putem demonstra acum rezultatul enunțat.

Teorema fundamentală a algebrei.

Eie $f \in \mathbb{C}[x]$ de grad ≥ 1 . Atunci f are o rădăcină în \mathbb{C} .

Demonstrare. Demonstremuți că pentru $f \in \mathbb{R}[x]$,

Eie $\deg(f) = 2^m \cdot h$ cu $m \in \mathbb{N}$ și h impar (adică m este exponentul lui 2 din descompunerea lui $\deg(f) = m$ ca produs de numere prime). Procedăm prin inducție după m ,

Pentru $m=0$, avem că n este impar. Dacă coeficientul dominant al lui f este pozitiv, atunci $\lim_{x \rightarrow -\infty} f(x) = -\infty$ și

$\lim_{x \rightarrow \infty} f(x) = \infty$, iar dacă coeficientul dominant este negativ,

avem $\lim_{x \rightarrow -\infty} f(x) = \infty$ și $\lim_{x \rightarrow \infty} f(x) = -\infty$. În ambele cazuri,

continuitatea lui f (prin urmare funcția $f: \mathbb{R} \rightarrow \mathbb{R}$, în
fapt este vorba de funcție polinomială asociată lui f)
garantează existența unui $x \in \mathbb{R}$ cu $f(x) = 0$.

(AR)

(32)

Presupunem că este tot pentru $m-1$ și demonstrăm pentru m , unde $m \in \mathbb{N}^*$. Este deci $f \in R[x]$ cu $\deg(f) = m = 2^m h$, cu h impar. Il privim pe f în $C[x]$ și aplicăm Coroloul de la pag. ; obținem că există o extindere E a lui C încercare fore n adăderi x_1, \dots, x_m . Într-un piccare $a \in R$ și piccare $1 \leq i < j \leq m$ considerăm elementul $z_{ij}^a = x_i + x_j + ax_i x_j \in E$.

Fixăm un $a \in R$ și considerăm polinomul

$$h^a(x) = \prod_{1 \leq i < j \leq m} (x - z_{ij}^a) = \prod_{1 \leq i < j \leq m} (x - x_i - x_j - ax_i x_j) \in E[x],$$

care are produl C_n^2 (deoarece există C_n^2 astfel de perechi (i, j) cu $1 \leq i < j \leq m$). Arătăm că $h^a(x) \in R[x]$.

Pt. aceasta considerăm polinomul de $n+1$ nedeterminate X, X_1, \dots, X_m

$$H^a(X, X_1, \dots, X_m) = \prod_{1 \leq i < j \leq m} (X - X_i - X_j - a X_i X_j) \in \cancel{R[X_1, \dots, X_m]}$$

Este clar că $h^a(x) = H^a(X, x_1, \dots, x_m)$.

Il privim pe H^a în $R[X_1, \dots, X_m][x]$, deci scriem

$$H^a(X, X_1, \dots, X_m) = \sum_{0 \leq r \leq C_n^2} P_r(X_1, \dots, X_m) X^r, \text{ unde}$$

$P_r \in R[X_1, \dots, X_m]$, pt. fiecare $0 \leq r \leq C_n^2$ (este clar că produl lui H^a în X este C_n^2 , deoarece H^a este produsul de C_n^2 factori; fiecare având grad 1 în X).

Observăm că pentru $\sigma \in S_m$ avem

$$H^a(X, X_{\sigma(1)}, \dots, X_{\sigma(m)}) = \prod_{1 \leq i < j \leq m} (X - X_{\sigma(i)} - X_{\sigma(j)} - a X_{\sigma(i)} X_{\sigma(j)})$$

$$\underline{\underline{(*)}} \quad \prod_{1 \leq i < j \leq m} (X - X_i - X_j - a X_i X_j) = H^a(X, X_1, \dots, X_n),$$

Egalitatea (*) având loc deoarece

$$\{(i, j) \mid 1 \leq i < j \leq m\} = \{(\min\{\sigma(i), \sigma(j)\}, \max\{\sigma(i), \sigma(j)\}) \mid 1 \leq i < j \leq m\}$$

(sau altfel spus, pt. orice $1 \leq i < j \leq m$ există $1 \leq i' < j' \leq n$ pt. care $i = \sigma(i')$, $j = \sigma(j')$) sau $i = \sigma(j')$, $j = \sigma(i')$, în
de altă parte, pt. orice $1 \leq i < j \leq m$ avem $1 \leq \sigma(i) < \sigma(j) \leq n$

sau $1 \leq \sigma(j) < \sigma(i) \leq n$. În urmare, factorii

din membrul stâng și membrul drept al egalității (*) se corespund doi adăpost.

De aici obținem că

$$\sum_{0 \leq r \leq C_m^2} P_r(X_{\sigma(1)}, \dots, X_{\sigma(m)}) X^r = \sum_{0 \leq r \leq C_m^2} P_r(X_1, \dots, X_n) X^r \text{ în}$$

$$\mathbb{R}[X_1, \dots, X_n][X], \text{ de unde } P_r(X_{\sigma(1)}, \dots, X_{\sigma(m)}) = P_r(X_1, \dots, X_n)$$

pt. orice $0 \leq r \leq C_m^2$. Cum aceasta este valabilă pt.
orice $\sigma \in S_n$, obținem că P_r este polinom simetric

din $\mathbb{R}[X_1, \dots, X_n]$ pt. orice r . Din proprietatea de lege
avem că $P_r(x_1, \dots, x_n) \in \mathbb{R}$ pt. orice $0 \leq r \leq C_m^2$ și căncă

$$h^a(X) = H^a(X, x_1, \dots, x_n) = \sum_{0 \leq r \leq C_m^2} P_r(x_1, \dots, x_n) X^r \in \mathbb{R}[X].$$

$$\text{Acum } \deg(h^a) = C_n^2 = \frac{n(n-1)}{2} = \frac{2^m h (2^m h - 1)}{2} = 2^{m-1} h (2^m h - 1).$$

Dacă $h(2^m h - 1)$ este irredusibil, deci exponentul lui 2 în $\deg(h^a)$ este $m-1$, și atunci îl putem elibera ipoteza de inducție lui h^a (despre care am arătat că este în $\mathbb{R}[x]$), obținând că h^a are o rădăcină în \mathbb{C} . Stăm să arătăm că $\mathbb{C} \subset E$ și rădăcinile lui h^a din E sunt z_{ij}^a , cu scris, și că urmă rezultă că există $1 \leq i < j \leq n$ cu $z_{ij}^a \in \mathbb{C}$.

Am arătat că există $a \in \mathbb{R}$ astfel încât $1 \leq i < j \leq n$ cu $z_{ij}^a \in \mathbb{C}$. Cum există o infinitate de numere reale (în felul de a) să fie un număr finit de permutări (i, j) cu $1 \leq i < j \leq n$, rezultă că există $a, b \in \mathbb{R}$, $a \neq b$ astfel că $z_{ij}^a, z_{ij}^b \in \mathbb{C}$ și aceeași permutație (i, j) , cu $1 \leq i < j \leq n$.

$$\text{Atunci } \begin{cases} x_i + x_j + a x_i x_j \in \mathbb{C} \\ x_i + x_j + b x_i x_j \in \mathbb{C} \end{cases} \quad \leftarrow \text{rădăcină} \Rightarrow (a-b)x_i x_j \in \mathbb{C},$$

deci și $x_i x_j \in \mathbb{C}$, și atunci și $x_i + x_j \in \mathbb{C}$.

Notăm cu $p = x_i x_j$ și $s = x_i + x_j$, avem că x_i și x_j sunt rădăcinile ecuației $z^2 - sz + p = 0$.

Cum o ecuație de grad 2 cu coeficienți reali are rădăcinile în \mathbb{C} , obținem că $x_i, x_j \in \mathbb{C}$, deci f este o rădăcină în \mathbb{C} și inducția este săracită.

Considerăm acum cazul general, în care $f \in \mathbb{C}[x]$.

$$\text{Fie } f(x) = a_m x^m + \dots + a_0, \text{ cu } a_0, \dots, a_m \in \mathbb{C}.$$

(AR) 35

Considerăm polinomul $f(x) = \bar{a}_n x^n + \dots + \bar{a}_0 \in \mathbb{C}[x]$, unde pt. $a \in \mathbb{C}$ am notat cu \bar{a} conjugatul complex al lui a .

~~Astăzi~~ f · $\bar{f} = \sum_{0 \leq j \leq 2n} c_j x^j$, unde coeficienții c_j sunt

dăsi de $c_j = \sum_{p+q=j} a_p \bar{a}_q$. Atunci

$$\bar{c}_j = \sum_{p+q=j} \bar{a}_p a_q = \sum_{q+p=j} a_q \bar{a}_p = c_j, \text{ deci } c_j \in \mathbb{R}.$$

Prin urmare $f \cdot \bar{f}$ este un polinom din $\mathbb{R}[x]$ și am demonstrat că un astfel de polinom (de grad ≥ 1) are o rădăcină în \mathbb{C} . Astăzi există $z \in \mathbb{C}$ cu

$(f \bar{f})(z) = 0$, adică $f(z) \bar{f}(z) = 0$. Deoarece $f(z) = 0$, atunci

f are rădăcina $z \in \mathbb{C}$ și suntem gata. Deoarece $\bar{f}(z) = 0$,

atunci $\bar{a}_n z^n + \dots + \bar{a}_0 = 0$ și conjugând, obținem că

$a_n(\bar{z})^n + \dots + a_0 = 0$, adică $f(\bar{z}) = 0$, de unde f are

rădăcina $\bar{z} \in \mathbb{C}$, și suntem gata!

Corolar. Fie $f \in \mathbb{C}[x]$ de grad $n \geq 1$. Atunci f are

n rădăcini în \mathbb{C} (numerate cu multiplicitate).

Formularea echivalentă: f se scrie ca produs de factori liniari (polinoame de grad 1) în $\mathbb{C}[x]$.

Demonstrare. Inductie după n .

Cazul $n=1$ este clar (polinom de grad 1),

Presupunem că avem pentru $n-1$ și demonstrația pentru n , unde $n \geq 2$. Fie $f \in \mathbb{C}[x]$ de grad n .

Să stim că Teorema că f are o rădăcină $x_1 \in \mathbb{C}$.

Așadar $f = (x - x_1) \cdot g$, cu $g \in \mathbb{C}[x]$. În plus,

$\deg(g) = n-1$. Așicurăm acum ipoteza de inducție

lui g și obținem $g = a(x - x_2) \cdots (x - x_n)$ pt. niște $x_2, \dots, x_n \in \mathbb{C}$ și $a \in \mathbb{C}^*$. Așadar $f = a(x - x_1)(x - x_2) \cdots (x - x_n)$, ceea ce încheie demonstrație.

O consecință imediată este :

Corolar. Polinoamele ireductibile din $\mathbb{C}[x]$ sunt polinoame de grad 1.

Discutăm acum polinoamele ireductibile din $\mathbb{R}[x]$.

Proprietate. Polinoamele ireductibile din $\mathbb{R}[x]$ sunt :

- polinoamele de grad 1
- polinoamele de grad 2 cu discriminant < 0
(adică $ax^2 + bx + c$ cu $a \neq 0$ și $b^2 - 4ac < 0$).

Dem. Polinoamele listate sunt ireductibile ; cele de grad 1 îm mod clar (restă orice corp comunitativ, folosind produsul), iar cele listate de grad 2 deoarece nu au rădăcini în \mathbb{R} (folosind corolariul polinoamelor ireductibile de grad 2 și 3 din $K[x]$).

Fie acum $f \in \mathbb{R}[x]$ ireductibil. Dacă f are o rădăcină reală a , atunci $f = (x-a) \cdot g$ pentru un $g \in \mathbb{R}[x]$. Cum f e ireductibil și $x-a$ nu este inversabil (având grad 1), rezultă că g e inversabil, deci $g = c \in \mathbb{R} \setminus \{0\}$. Atunci $f = c(x-a)$, un polinom de grad 1.

Presupunem acum că f nu are rădăcini reale. Din teorema fundamentală a algebrei știm că f are o rădăcină $z \in \mathbb{C}$; prin urmare $\bar{z} \in \mathbb{C} \setminus \mathbb{R}$. Atunci $(x-z)(x-\bar{z}) = x^2 - (z+\bar{z})x + z\bar{z} \in \mathbb{R}[x]$ și implicația f le $(x-z)(x-\bar{z})$ în $\mathbb{R}[x]$. Obținem

$$f = (x-z)(x-\bar{z}) \cdot g + ax+b \text{ pt. un } g \in \mathbb{R}[x] \text{ și } a, b \in \mathbb{R}$$

Biruiim egalitatea în $\mathbb{C}[x]$ și evoluăm după z . Obținem

$$0 = f(z) = 0 + az + b, \text{ de unde } az + b = 0.$$

Dacă $a \neq 0$, că rezulta $z = -\frac{b}{a} \in \mathbb{R}$, contradicție.

Așadar $a=0$ și atunci și $b=0$. Rezultă

$f = (x^2 - (z+\bar{z})x + z\bar{z}) \cdot g$ și cum f e ireductibil, trebuie ca g să fie inversabil, deci constant, $g=c \in \mathbb{R} \setminus \{0\}$.

Prin urmare $f = c(x^2 - (z+\bar{z})x + z\bar{z}) = c(x-z)(x-\bar{z})$, un polinom de grad 2 fără rădăcini reale, deci cu discriminant < 0.

Determinarea polinoanelor ireductibile din $\mathbb{Q}[x]$ este mult mai complicată. Urmatul rezultat ajută la determinarea unor polinoame ireductibile.

Teorema (Criteriul lui Eisenstein)

Eile $f = X^n + a_{n-1}X^{n-1} + \dots + a_0 \in \mathbb{Z}[x]$ un polinom monic de grad $n \geq 1$ astfel încât există prim ca $p | a_0, \dots, p | a_{n-1}$ și $p \nmid a_n$.

Atunci f este ireductibil în $\mathbb{Q}[x]$.

Demonstrare. Presupunem prin absurd că $f = gh$ cu $g, h \in \mathbb{Q}[x]$, monice de grade ≥ 1 . Eile $a, b \in \mathbb{N}^*$ minime astfel că $ag, bh \in \mathbb{Z}[x]$.

Astăzi că $a=b=1$. Într-adevăr, dacă $ab > 1$, fie q un divizor prim al lui ab . Eile $\varphi: \mathbb{Z}[x] \rightarrow \mathbb{Z}_2[x]$ morfismul de inele definit prin $\varphi(c_nx^n + \dots + c_0) = \hat{c}_n\hat{x}^n + \dots + \hat{c}_0$ (φ este redusă modulo 2). Cum $q | ab \Rightarrow q$ divide toti coeficienții lui abf , deci $\varphi(abf) = 0$. Dar $abf = (ag)(bh)$, deci $0 = \varphi(ag)\varphi(bh)$ în $\mathbb{Z}_2[x]$. Cum $\mathbb{Z}_2[x]$ este domeniu de integritate (\mathbb{Z}_2 e corp), obținem $\varphi(ag) = 0$ sau $\varphi(bh) = 0$.

Dacă $\varphi(ag) = 0 \Rightarrow q$ divide toti coeficienții lui ag , în particular și coeficientul dominant a ; în plus $\frac{a}{2}(ag) \in \mathbb{Z}[x]$, deci $\frac{a}{2}g \in \mathbb{Z}[x]$. Cum $\frac{a}{2} \in \mathbb{N}$ și $\frac{a}{2} < a$, aceasta contrazice minimulitatea lui a . La fel, $\varphi(bh) = 0$ contrazice minimulitatea lui b . În concluzie $ab = 1$, deci $a = b = 1$, de unde $g, h \in \mathbb{Z}[x]$.

Eile acum $\psi: \mathbb{Z}[x] \rightarrow \mathbb{Z}_p[x]$ redusă modulo p . Atunci $f = gh \Rightarrow \psi(f) = \psi(g)\psi(h)$ în $\mathbb{Z}_p[x]$. Dar $\psi(f) = X^n$, deci $\psi(g) = X^r$ și $\psi(h) = X^s$ pt. numerele $r, s \in \mathbb{N}$ cu $r+s=n$. Cum g, h au grade ≥ 1 și sunt monice $\Rightarrow r, s > 0$. Atunci termenii liberi din g și h se divid cu p , deci a_0 se divide cu p^2 , contradicție, ceea ce arată că demonstrația.

Concluzie, pt. orice $n \in \mathbb{N}^*$ polinomul $X^n + 2$ este ireductibil în $\mathbb{Q}[x]$ (explicând teorema pt. $p=2$), deci în $\mathbb{Q}[x]$ există polinoame ireductibile de orice grad ≥ 1 .