CORPURI ŞI EXTINDERI DE CORPURI

1. Caracteristica unui corp. Corpuri prime.

Pe parcursul acestui capitol, dacă nu se menţionează altfel, prin corp se va înţelege corp comutativ.

Începem prin a reaminti noţiunea de caracteristică a unui corp. Fie K un corp şi $\varphi : \mathbb{Z} \to K$ aplicaţia definită prin $\varphi(n) = n \cdot 1_K$. Este evident că φ este morfism de inele. Deoarece $\ker \varphi$ este ideal al lui $\mathbb{Z}$ există $p \in \mathbb{N}$ astfel încât $\ker \varphi = p\mathbb{Z}$. (Să observăm că $p \neq 1$.) Avem două posibilităţi:

• $p = 0$, caz în care φ este injectiv, adică $n \cdot 1_K \neq 0$ pentru orice $n \neq 0$. În acest caz spunem că K este *corp de caracteristică zero* şi scriem $\operatorname{char} K = 0$. Mai mult, deoarece $n \cdot 1_K \neq 0$ pentru orice $n \neq 0$, îl putem extinde pe φ la un morfism injectiv $\overline{\varphi} : \mathbb{Q} \to K$ astfel: $\overline{\varphi}(m/n) = (m \cdot 1_K)(n \cdot 1_K)^{-1}$. Aşadar $\mathbb{Q}$ este izomorf cu un subcorp K_0 al lui K. Mai mult, orice subcorp al lui K îl conţine pe K_0, deci K_0 este intersecţia tuturor subcorpurilor lui K. Deoarece $\operatorname{char} \mathbb{Q} = 0$ deducem că $\mathbb{Q}$ nu are subcorpuri proprii.

• $p \neq 0$, caz în care φ se "extinde" la un morfism injectiv $\overline{\varphi} : \mathbb{Z}/p\mathbb{Z} \to K$ astfel: $\overline{\varphi}(\hat{n}) = n \cdot 1_K$. În acest caz spunem că K este *corp de caracteristică* p şi scriem $\operatorname{char} K = p$. Deoarece K este corp, în particular inel integru, $\operatorname{Im} \overline{\varphi}$ este inel integru (deoarece este subinel într-un inel integru). Deducem că $\mathbb{Z}/p\mathbb{Z}$ este inel integru, ceea ce implică p număr prim. În acest caz $\mathbb{Z}/p\mathbb{Z}$ este chiar corp, deci K conţine un subcorp K_0 izomorf cu $\mathbb{Z}/p\mathbb{Z}$. La fel ca în cazul precedent, orice subcorp al lui K îl conţine pe K_0, deci K_0 este intersecţia tuturor subcorpurilor lui K. Deoarece $\operatorname{char} \mathbb{Z}/p\mathbb{Z} = p$ deducem că $\mathbb{Z}/p\mathbb{Z}$ nu are subcorpuri proprii.

Să observăm că, pe scurt, caracteristica unui corp K este ordinul lui 1_K în grupul $(K, +)$.

Definiţia 1.1. *Un corp care nu are subcorpuri proprii se numeşte* corp prim.

Din cele de mai sus rezultă că orice corp prim este izomorf cu $\mathbb{Q}$ sau cu $\mathbb{Z}/p\mathbb{Z}$, unde p este un număr prim şi că orice corp conţine un unic subcorp izomorf cu unul dintre aceste corpuri (în funcţie de caracteristica sa).

2. Construcţii de corpuri. Adjuncţionare

Prezentăm în cele ce urmează câteva metode de a construi corpuri.

1. Fie R un inel comutativ şi unitar iar $\mathfrak{m}$ un ideal maximal al lui R. Atunci $R/\mathfrak{m}$ este corp.

Cazuri particulare:

(i) $R = \mathbb{Z}$ şi $\mathfrak{m} = p\mathbb{Z}$, unde $p > 0$ este număr prim. $\mathbb{Z}/p\mathbb{Z}$ este corp finit cu p elemente, numit *corpul claselor de resturi modulo* p.

(ii) $R = K[X]$ şi $\mathfrak{m} = (f)$, unde K este un corp oarecare iar $f \in K[X]$ un polinom ireductibil. Să observăm că dacă K este corp finit cu q elemente şi $\deg f = n$, atunci

$K[X]/(f)$ este corp finit cu q^n elemente. Vom arăta ulterior că orice corp finit se obţine în acest mod.

Exemplul 2.1. $\mathbb{Q}[X]/(X^2-2)$ este corp izomorf cu $\mathbb{Q}[\sqrt{2}] = \{a+b\sqrt{2} : a,b \in \mathbb{Q}\}$.
$\mathbb{R}[X]/(X^2+1)$ este corp izomorf cu $\mathbb{C}$.
$(\mathbb{Z}/2\mathbb{Z})[X]/(X^2+X+\hat{1})$ este corp finit cu patru elemente.

2. Corpul de fracţii al unui inel integru. Fie R un inel comutativ integru, $S = R\backslash\{0\}$. Atunci $S^{-1}R = \{a/s : a \in R, s \in S\}$ este corp, se notează cu $Q(R)$ şi se numeşte *corpul de fracţii al lui* R.

Cazuri particulare:
(i) $R = \mathbb{Z}$. Atunci $Q(R) = \{m/n : m,n \in \mathbb{Z}, n \neq 0\}$ se notează cu $\mathbb{Q}$ şi se numeşte *corpul numerelor raţionale.*
(ii) $R = K[X]$, K corp. Atunci $Q(R) = \{f/g : f,g \in K[X], g \neq 0\}$ se notează cu $K(X)$ şi se numeşte *corpul fracţiilor algebrice raţionale peste* K *în nedeterminata* X.
(iii) $R = K[X_1,\ldots,X_n]$, K corp. Atunci $Q(R) = \{f/g : f,g \in K[X_1,\ldots,X_n], g \neq 0\}$ se notează cu $K(X_1,\ldots,X_n)$ şi se numeşte *corpul fracţiilor algebrice raţionale peste* K *în nedeterminatele* $X_1,\ldots,X_n$.

Exerciţiul 2.2. (i) Fie R un inel integru. Determinaţi corpul de fracţii al inelului de polinoame $R[X_1,\ldots,X_n]$.
(ii) Arătaţi că $Q(\mathbb{Z}[i]) = \mathbb{Q}[i]$.
(iii) Arătaţi că $Q(\mathbb{Z}[[X]])$ este conţinut strict în $\mathbb{Q}((X)) = \{f/g : f,g \in \mathbb{Q}[[X]], g \neq 0\}$.

3. Corpuri obţinute prin adjuncţionare.

Se ştie că dacă $f : K \to L$ este un morfism de corpuri, atunci f este injectiv. Astfel $K \simeq f(K)$, deci K este izomorf cu un subcorp al lui L.

Definiţia 2.3. *Fie* L *un corp (inel) şi* $K \subset L$ *un subcorp (subinel). Spunem că* L *este o* extindere *a lui* K *sau că incluziunea* $K \subset L$ *este o* extindere de corpuri (inele).

Lema 2.4. *Fie* L *un corp (inel) şi* $(K_i)_{i\in I}$ *o familie de subcorpuri (subinele) a lui* L. *Atunci* $K = \bigcap_{i\in I} K_i$ *este subcorp (subinel) al lui* L.

Fie $K \subset L$ o extindere de corpuri (inele) şi $M \subset L$ o submulţime. Fie $K[M]$ intersecţia tuturor subinelelor lui L care conţin pe K şi M (cel mai mic subinel al lui L care conţine pe K şi M), respectiv $K(M)$ intersecţia tuturor subcorpurilor lui L care conţin pe K şi M (cel mai mic subcorp al lui L care conţine pe K şi M).

Definiţia 2.5. $K[M]$ *se numeşte* inelul obţinut prin adjuncţionarea lui M la K *iar* $K(M)$ *se numeşte* corpul obţinut prin adjuncţionarea lui M la K.

Propoziţia 2.6. *(i)* $K[M] = \{y \in L : \exists n \in \mathbb{N}\ \exists f \in K[X_1,\ldots,X_n]\ \exists \alpha_1,\ldots,\alpha_n \in M$ astfel încât $y = f(\alpha_1,\ldots,\alpha_n)\}$.
(ii) $K(M) = \{y \in L : \exists n \in \mathbb{N}\ \exists f,g \in K[X_1,\ldots,X_n]\ \exists \alpha_1,\ldots,\alpha_n \in M$ astfel încât $g(\alpha_1,\ldots,\alpha_n) \neq 0$ şi $y = f(\alpha_1,\ldots,\alpha_n)/g(\alpha_1,\ldots,\alpha_n)\}$.

Proof. (i) Notăm cu A mulţimea $\{y \in L : \exists n \in \mathbb{N}\ \exists f \in K[X_1, \ldots, X_n]\ \exists \alpha_1, \ldots, \alpha_n \in M$ astfel încât $y = f(\alpha_1, \ldots, \alpha_n)\}$.

Arătăm că A este subinel al lui L care conţine pe K şi M. De aici va rezulta $K[M] \subseteq A$. Fie $y, y' \in A$. Scriem $y = f(\alpha_1, \ldots, \alpha_n)$ şi $y' = g(\alpha'_1, \ldots, \alpha'_m)$ cu $f \in K[X_1, \ldots, X_n]$ şi $g \in K[X_1, \ldots, X_m]$. Fie $h, k \in K[X_1, \ldots, X_{n+m}]$ definite astfel:

$$h(X_1, \ldots, X_{n+m}) = f(X_1, \ldots, X_n) - g(X_{n+1}, \ldots, X_{n+m}),$$

$$k(X_1, \ldots, X_{n+m}) = f(X_1, \ldots, X_n)g(X_{n+1}, \ldots, X_{n+m}).$$

Avem $y - y' = h(\alpha_1, \ldots, \alpha_n, \alpha'_1, \ldots, \alpha'_m) \in A$ şi $yy' = k(\alpha_1, \ldots, \alpha_n, \alpha'_1, \ldots, \alpha'_m) \in A$. Deci A este subinel al lui L. Evident $K \subseteq A$ şi $M \subseteq A$.

Reciproc, fie B un subinel al lui L care conţine pe K şi M. Din forma elementelor lui A deducem că $A \subseteq B$, deci $A \subseteq K[M]$.
(ii) Analog. □

Remarca 2.7. $K(M)$ este corpul de fracţii al inelului $K[M]$.

Cazuri particulare de adjuncţie:
(i) M este o mulţime finită, $M = \{\alpha_1, \ldots, \alpha_n\}$. Atunci

$$K[\alpha_1, \ldots, \alpha_n] = \{f(\alpha_1, \ldots, \alpha_n) : f \in K[X_1, \ldots, X_n]\},$$

$$K(\alpha_1, \ldots, \alpha_n) = \{\frac{f(\alpha_1, \ldots, \alpha_n)}{g(\alpha_1, \ldots, \alpha_n)} : f, g \in K[X_1, \ldots, X_n] \text{ şi } g(\alpha_1, \ldots, \alpha_n) \neq 0\}.$$

(ii) M are un singur element, $M = \{\alpha\}$. Atunci $K[\alpha] = \{f(\alpha) : f \in K[X]\}$ iar $K(\alpha) = \{\frac{f(\alpha)}{g(\alpha)} : f, g \in K[X]$ şi $g(\alpha) \neq 0\}$.
(iii) Fie $\mathbb{Q} \subset \mathbb{R}$ extindere de corpuri şi $\alpha = \sqrt{2}$. Atunci $\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$ iar $\mathbb{Q}(\sqrt{2}) = \{\frac{a+b\sqrt{2}}{a'+b'\sqrt{2}} : a, b, a', b' \in \mathbb{Q}, (a', b') \neq (0, 0)\}$.
De fapt, $\mathbb{Q}[\sqrt{2}] = \mathbb{Q}(\sqrt{2})$, aceasta fiind, după cum urmează să vedem, o proprietate comună numerelor reale care sunt rădăcini de polinoame cu coeficienţi în $\mathbb{Q}$.

Definiţia 2.8. *Fie L un corp şi $K, K' \subset L$ subcorpuri. Corpul $K(K') = K'(K)$ obţinut prin adjuncţionarea lui K' la K (sau, echivalent, a lui K la K') se numeşte* compozitul corpurilor K şi K' în L.

Exemplul 2.9. Fie $K = \mathbb{Q}(\sqrt{2})$ şi $K' = \mathbb{Q}(\sqrt{3})$ subcorpuri ale lui $\mathbb{R}$. Atunci $KK' = \mathbb{Q}(\sqrt{2}, \sqrt{3})$.

Propoziţia 2.10. *Fie $K \subset L$ o extindere de corpuri.*
(i) $KL = L$ şi $K(\emptyset) = K$.
(ii) Dacă $M, N \subset L$ sunt submulţimi şi $N \subseteq M$, atunci $K(N) \subseteq K(M)$.
(iii) Dacă $M, N \subset L$ sunt submulţimi, atunci $K(M \cup N) = K(M)(N) = K(N)(M) = K(M)K(N)$.
(iv) Dacă $M \subset L$ este o submulţime, atunci $K(M) = \bigcup_{H \subseteq M, H \text{ finită}} K(H)$.

Proof. (i), (ii) şi (iii) sunt evidente.
(iv) Fie $E = \bigcup_{H \subseteq M, H \text{ finită}} K(H)$. Se arată uşor că E este un subcorp al lui L care conţine pe K şi M. □

3. Tipuri de extinderi de corpuri

Definiţia 3.1. *Fie $K \subset L$ o extindere de corpuri (inele). Extinderea se numeşte* de tip finit *sau* finit generată *dacă există $n \in \mathbb{N}$ şi $\alpha_1, \ldots, \alpha_n \in L$ astfel încât $L = K(\alpha_1, \ldots, \alpha_n)$ (respectiv $L = K[\alpha_1, \ldots, \alpha_n]$). Extinderea se numeşte* simplă *dacă există $\alpha \in L$ astfel încât $L = K(\alpha)$ (respectiv $L = K[\alpha]$).*

De exemplu, extinderea $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}, \sqrt{3})$ este extindere de tip finit iar extinderea $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2})$ este simplă. (Vom vedea ulterior că, de fapt, şi prima extindere este simplă.) În schimb, extinderea $\mathbb{Q} \subset \mathbb{R}$ nu este de tip finit.

Plecând de la observaţia că dacă $K \subset L$ este o extindere de corpuri (inele), atunci L este K-spaţiu vectorial (respectiv K-modul), putem da următoarea definiţie.

Definiţia 3.2. *Fie $K \subset L$ o extindere de corpuri (inele). Extinderea se numeşte* finită *dacă $\dim_K L < \infty$ (respectiv dacă L este K-modul finit generat) şi* infinită *în caz contrar. Se defineşte* gradul *extinderii, notat $[L : K]$, ca fiind $\dim_K L$ atunci când extinderea este finită şi ∞ când extinderea este infinită.*

De exemplu, extinderea $\mathbb{R} \subset \mathbb{C}$ este o extindere finită de grad 2, pe când extinderea $\mathbb{Q} \subset \mathbb{R}$ este infinită.

Să mai observăm că $[L : K] = 1$ dacă şi numai dacă $K = L$.

Propoziţia 3.3. *Orice extindere finită de corpuri (inele) este extindere de tip finit.*

Proof. Dacă $\alpha_1, \ldots, \alpha_n$ este sistem de generatori în K-spaţiul vectorial (respectiv K-modulul) L, atunci $L = K(\alpha_1, \ldots, \alpha_n)$ (respectiv $L = K[\alpha_1, \ldots, \alpha_n]$). □

Reciproc este fals: extinderea $\mathbb{Q} \subset \mathbb{Q}(X)$ este de tip finit, dar nu este finită.

Propoziţia 3.4. (Tranzitivitatea extinderilor finite) *Fie $k \subset K$ şi $K \subset L$ extinderi de corpuri. Atunci $[L : k] = [L : K][K : k]$.*

În particular, $k \subset L$ este extindere finită dacă şi numai dacă $k \subset K$ şi $K \subset L$ sunt extinderi finite.

Proof. Fie $(e_i)_{i \in I}$ o bază în K/k şi $(f_j)_{j \in J}$ o bază în L/K. Se arată că $(e_i f_j)_{(i,j) \in I \times J}$ este bază în L/k. □

Corolarul 3.5. *(i) Fie $k \subset K$ şi $K \subset L$ extinderi finite. Atunci $[K : k]$ şi $[L : K]$ divid pe $[L : k]$.*
(ii) Dacă $K \subset L$ este o extindere finită şi $[L : K] = p$, unde $p > 0$ este număr prim, atunci extinderea dată nu are extinderi intermediare proprii.

Ne punem acum întrebarea dacă şi extinderile de tip finit au proprietatea de tranzitivitate.

Propoziţia 3.6. (Tranzitivitatea extinderilor de tip finit) *Fie $k \subset K$ şi $K \subset L$ extinderi de corpuri. Atunci $k \subset L$ este extindere de tip finit dacă şi numai dacă $k \subset K$ şi $K \subset L$ sunt extinderi de tip finit.*

Proof. "$\Leftarrow$" Dacă $K = k(M)$ şi $L = K(N)$ cu M, N finite, atunci $L = k(M \cup N)$ şi $M \cup N$ este finită.
"$\Rightarrow$" Dacă $k \subset L$ este extindere de tip finit, atunci $K \subset L$ este extindere de tip

finit pentru că orice sistem de generatori ai lui L peste k este de asemenea sistem de generatori ai lui L peste K.

Rămâne de demonstrat că orice subextindere a unei extinderi de tip finit este de tip finit. Fie $x_1, \ldots, x_n$ o bază de transcendenţă în K peste k. Cum extinderea $k \subset k(x_1, \ldots, x_n)$ este de tip finit este suficient ca să arătăm că extinderea algebrică $k(x_1, \ldots, x_n) \subset K$ este de tip finit. Mai mult, extinderea $k(x_1, \ldots, x_n) \subset L$ este de tip finit, deci putem presupune că extinderea $k \subset K$ este algebrică (înlocuindu-l pe k cu $k(x_1, \ldots, x_n)$). Dacă aceasta nu este de tip finit, atunci nu este nici finită şi atunci pentru orice $d \geq 1$ există $k \subset K_d \subset K$ cu proprietatea că $[K_d : k] \geq d$. Fie acum $t_1, \ldots, t_m$ o bază de transcendenţă în L peste k. Atunci $[K_d(t_1, \ldots, t_m) : k(t_1, \ldots, t_m) = [K_d : k] \geq d$ pentru orice $d \geq 1$. Aşadar $k(t_1, \ldots, t_m) \subset L$ este extindere algebrică de grad infinit, deci nu este de tip finit, contradicţie. □

Remarca 3.7. Spre deosebire de situaţia de la extinderi de corpuri, există k-subalgebre ale lui $k[X, Y]$ care nu sunt finit generate, cum ar fi, spre exemplu, $k[XY, XY^2, \ldots, XY^n, \ldots]$. (Acest lucru nu se întâmplă totuşi pentru $K[X]$.)

Avem însă şi un rezultat pozitiv în acest context.

Lema 3.8. (Lema Artin-Tate) *Dacă $A \subset B \subset C$ sunt astfel încât A este inel noetherian, C este de tip finit peste A şi $B \subset C$ este extindere finită, atunci B este de tip finit peste A.*

Proof. Fie $c_1, \ldots, c_m \in C$ cu proprietatea că $C = A[c_1, \ldots, c_m]$ şi fie $\omega_1, \ldots, \omega_n \in C$ astfel încât $C = B\omega_1 + \cdots + B\omega_n$. Pentru orice $1 \leq i \leq m$ putem scrie

$$c_i = \sum_{j=1}^{n} b_{ij}\omega_j, \ b_{ij} \in B.$$

Analog, pentru orice $1 \leq i, j \leq n$, putem scrie

$$\omega_i\omega_j = \sum_{k=1}^{n} b_{ijk}\omega_k, \ b_{ijk} \in B.$$

Fie B_0 A-subalgebra lui B generată de (b_{ij}) şi (b_{ijk}), adică $B_0 = A[(b_{ij}), (b_{ijk})]$. Pentru că B_0 este o algebră de tip finit peste un inel noetherian, este ea însăşi inel noetherian (din teorema Hilbert a bazei).
Orice element al lui C se poate exprima ca un polinom în $c_1, \ldots, c_m$ cu coeficienţi în A. Făcând substituţii folosind cele două relaţii de mai sus obţinem că C este B_0-modul finit generat. Cum B_0 este noetherian, submodulul B este de asemenea finit generat ca B_0-module. Aceasta implică imediat că B este B_0-algebră de tip finit şi apoi că B este A-algebră de tip finit. □

Definiţia 3.9. *Fie $K \subset L$ o extindere de corpuri. Un element $\alpha \in L$ se numeşte* algebric peste K *dacă există $f \in K[X]$, $f \neq 0$, astfel încât $f(\alpha) = 0$. Un element care nu este algebric (peste K) se numeşte* transcendent *(peste K).*

Extinderea $K \subset L$ se numeşte extindere algebrică *dacă orice element al lui L este algebric peste K. În caz contrar se numeşte* extindere transcendentă.

O observaţie imediată este aceea că orice element $a \in K$ este algebric peste K fiind rădăcină a polinomului $f = X - a \in K[X]$.

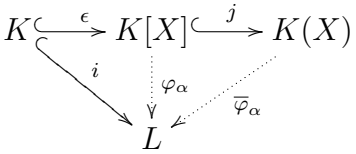
Exemplul 3.10. (i) Considerăm extinderea $\mathbb{Q} \subset \mathbb{R}$. Numărul $\sqrt{2}$ este algebric peste $\mathbb{Q}$, fiind rădăcină a polinomului $f = X^2 - 2 \in \mathbb{Q}[X]$. Pe de altă parte, π este transcendent peste $\mathbb{Q}$.
(ii) Extinderea $\mathbb{Q} \subset \mathbb{R}$ este transcendentă.
(iii) Extinderea $\mathbb{R} \subset \mathbb{C}$ este algebrică: orice număr complex $z = a + bi$, $a, b \in \mathbb{R}$, este rădăcină a polinomului $f = X^2 - 2aX + a^2 + b^2 \in \mathbb{R}[X]$.

Exerciţiul 3.11. Arătaţi că mulţimea numerelor reale care sunt algebrice peste $\mathbb{Q}$ este numărabilă.

Definiţia 3.12. *Fie $K \subset L_1$ şi $K \subset L_2$ extinderi de corpuri şi $\varphi : L_1 \to L_2$ un morfism de corpuri cu proprietatea că $\varphi_{|K} = \mathrm{id}_K$. Atunci φ se numeşte* K-morfism *de la L_1 la L_2. Dacă, mai mult, φ este izomorfism se va numi* K-izomorfism.

Propoziţia 3.13. *Fie $K \subset L$ extindere de corpuri şi $\alpha \in L$ transcendent peste K. Atunci $K(\alpha)$ şi $K(X)$ sunt K-izomorfe.*

Proof. Din proprietatea de universalitate a inelelor de polinoame există şi este unic un morfism de inele $\varphi_\alpha : K[X] \to L$ astfel încât $\varphi_\alpha \epsilon = i$ şi $\varphi_\alpha(X) = \alpha$. Deoarece α este transcendent peste K avem $\ker \varphi_\alpha = (0)$. Să mai observăm că $\mathrm{Im}(\varphi_\alpha) = K[\alpha]$.



Din proprietatea de universalitate a inelelor de fracţii există un unic morfism de inele $\overline{\varphi}_\alpha : K(X) \to L$ astfel încât $\overline{\varphi}_\alpha j = \varphi_\alpha$. Avem $\ker \overline{\varphi}_\alpha = (0)$ şi $\mathrm{Im}\, \overline{\varphi}_\alpha = K(\alpha)$. □

Rezultatul de mai sus ne spune că adjuncţionarea unui element transcendent peste un corp K are ca efect obţinerea unui corp de fracţii algebrice raţionale peste K.

Propoziţia 3.14. *Fie $K \subset L$ extindere de corpuri şi $\alpha \in L$. Următoarele afirmaţii sunt echivalente:*
(i) α este algebric peste K.
(ii) Există $f \in K[X]$ monic, ireductibil, cu $\deg f \geq 1$ astfel încât $K[\alpha]$ este K-izomorf cu $K[X]/(f)$.
(iii) $K[\alpha] = K(\alpha)$.
(iv) $[K(\alpha) : K] < \infty$.

Proof. (i) $\Rightarrow$ (ii) $\ker \varphi_\alpha \neq (0)$ deoarece α este algebric peste K. Aşadar există $f \in K[X]$ monic, cu $\deg f \geq 1$ astfel încât $\ker \varphi_\alpha = (f)$. Rezultă imediat că f este ireductibil. Din teorema fundamentală de izomorfism pentru inele deducem că $K[X]/(f)$ este K-izomorf cu $\mathrm{Im}\, \varphi_\alpha = K[\alpha]$.
(ii) $\Rightarrow$ (iii) Deoarece f este ireductibil, inelul factor $K[X]/(f)$ este corp, deci $K[\alpha]$ este corp şi în consecinţă $K[\alpha] = K(\alpha)$.
(iii) $\Rightarrow$ (i) Din proprietatea de universalitate a inelelor de polinoame există şi este unic un morfism de inele $\varphi_\alpha : K[X] \to L$ astfel încât $\varphi_\alpha \epsilon = i$ şi $\varphi_\alpha(X) = \alpha$. Deoarece $\mathrm{Im}(\varphi_\alpha) = K[\alpha]$, în cazul în care, prin absurd, α nu ar fi algebric peste K, ar rezulta că $K[X]$ este K-izomorf cu $K[\alpha]$. Însă egalitatea $K[\alpha] = K(\alpha)$ ne spune

că $K[\alpha]$ este corp, deci şi $K[X]$ ar trebui să fie corp, fals.
(ii) $\Rightarrow$ (iv) Cum $K[X]/(f)$ este K-spaţiu vectorial de dimensiune $\deg f$ şi $K[\alpha] = K(\alpha)$, obţinem că $[K(\alpha) : K] < \infty$.
(iv) $\Rightarrow$ (i) Dacă α ar fi transcendent peste K, din propoziţia 3.13 ar rezulta $[K(X) : K] < \infty$, fals. □

Se observă că polinomul f din propoziţia 3.14 este polinomul monic de grad minim cu proprietatea că $f(\alpha) = 0$. Acesta se va numi *polinomul minimal* al lui α peste K şi se va nota cu $\mathrm{Irr}(\alpha, K)$. Acesta este unic determinat de proprietăţile:
(i) $\mathrm{Irr}(\alpha, K) \in K[X]$ este monic.
(ii) $\mathrm{Irr}(\alpha, K)(\alpha) = 0$.
(iii) Dacă $g \in K[X]$ satisface $g(\alpha) = 0$, atunci $\mathrm{Irr}(\alpha, K) \mid g$.

Remarca 3.15. Rezultă imediat că $\{1, \alpha, \ldots, \alpha^{\deg f - 1}\}$ este K-bază în $K(\alpha)$.

Exemplul 3.16. Considerăm extinderea $\mathbb{Q} \subset \mathbb{R}$. Avem $\mathrm{Irr}(\sqrt{2}, \mathbb{Q}) = X^2 - 2$.

Propoziţia 3.17. *Orice extindere finită de corpuri este algebrică.*

Proof. Fie $K \subset L$ o extindere finită de corpuri şi $\alpha \in L$. Atunci $1, \alpha, \ldots, \alpha^n, \ldots$ sunt liniar dependente peste K, deci α este algebric peste K. □

4. Proprietăţi ale extinderilor algebrice

Vom prezenta în cele ce urmează câteva proprietăţi importante ale extinderilor algebrice.

Propoziţia 4.1. *O extindere de corpuri este extindere algebrică şi de tip finit dacă şi numai dacă este extindere finită.*

Proof. Fie $K \subset L$ o extindere de corpuri.
"$\Leftarrow$" Dacă $K \subset L$ este extindere finită, atunci, din propoziţia 3.17, acesta este algebrică. Este imediat că $K \subset L$ este şi extindere de tip finit, deoarece o bază în L peste K este, în particular, un sistem de generatori pentru L peste K.
"$\Rightarrow$" Deoarece extinderea $K \subset L$ este de tip finit există $a_1, \ldots, a_n \in L$ astfel încât $L = K(a_1, \ldots, a_n)$. Cum a_i este algebric peste K, acesta va fi algebric şi peste $K(a_1, \ldots, a_{i-1})$ şi din propoziţia 3.14(iv) avem că extinderea $K(a_1, \ldots, a_{i-1}) \subset K(a_1, \ldots, a_i)$ este finită. Fie $r_i = [K(a_1, \ldots, a_i) : K(a_1, \ldots, a_{i-1})]$. Vom arăta, prin inducţie după n, că $[L : K] = r_1 \cdots r_n$ şi că elementele $a_1^{i_1} \cdots a_n^{i_n}$ cu $0 \leq i_k < r_k$ pentru $k = 1, \ldots, n$ formează o K-bază în L.

Cazul $n = 1$ rezultă din remarca 3.15. Pentru $n > 1$, din ipoteza de inducţie ştim că $[K(a_1, \ldots, a_{n-1}) : K] = r_1 \cdots r_{n-1}$ şi că elementele $a_1^{i_1} \cdots a_{n-1}^{i_{n-1}}$ cu $0 \leq i_k < r_k$ pentru $k = 1, \ldots, n-1$ formează o K-bază în $K(a_1, \ldots, a_{n-1})$. Din $r_n = [K(a_1, \ldots, a_n) : K(a_1, \ldots, a_{n-1})]$ şi din tranzitivitatea extinderilor finite (vezi propoziţia 3.4) deducem că $[L : K] = r_1 \cdots r_n$ şi că elementele $a_1^{i_1} \cdots a_n^{i_n}$ cu $0 \leq i_k < r_k$ pentru $k = 1, \ldots, n$ formează o K-bază în L. □

Propoziţia 4.2. (Tranzitivitatea extinderilor algebrice) *Fie $k \subset K$ şi $K \subset L$ extinderi de corpuri. Atunci $k \subset L$ este extindere algebrică dacă şi numai dacă $k \subset K$ şi $K \subset L$ sunt extinderi algebrice.*

Proof. "⇒" Evident.
"⇐" Fie $\alpha \in L$. Atunci α este algebric peste K, deci există $f \in K[X]$, $f \neq 0$ cu $f(\alpha) = 0$. Scriem $f = a_0 + a_1X + \cdots + a_{n-1}X^{n-1} + X^n$, $a_i \in K$ şi observăm că α este algebric peste $k(a_0, a_1, \ldots, a_{n-1})$. Dar extinderea $k \subset k(a_0, a_1, \ldots, a_{n-1})$ este algebrică (ca fiind subextindere a extinderii algebrice $k \subset K$) şi de tip finit, deci este finită. Rezultă că şi extinderea $k \subset k(a_0, a_1, \ldots, a_{n-1})(\alpha)$ este finită, în particular algebrică, deci α este algebric peste k. □

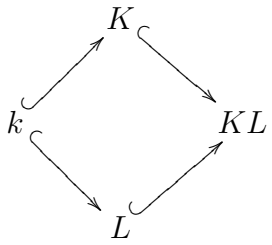
Corolarul 4.3. *Fie $K \subset L$ o extindere de corpuri şi $M \subset L$ o submulţime cu proprietatea că orice element al lui M este algebric peste K. Atunci extinderea $K \subset K(M)$ este algebrică şi $K[M] = K(M)$.*

Proof. Deoarece $K(M) = \bigcup_{H \subseteq M, H \text{ finită}} K(H)$ putem considera că M este mulţime finită. Scriem $M = \{\alpha_1, \ldots, \alpha_n\}$ şi formăm un lanţ de extinderi algebrice: $K \subset K(\alpha_1) \subset K(\alpha_1, \alpha_2) \subset \cdots \subset K(\alpha_1, \ldots, \alpha_n) = K(M)$. Din tranzitivitatea extinderilor algebrice (vezi propoziţia 4.2) rezultă că extinderea $K \subset K(M)$ este algebrică. □

Remarca 4.4. O extindere algebrică nu este neapărat finită după cum arată următorul exemplu: $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}, \sqrt[3]{2}, \ldots, \sqrt[n]{2}, \ldots)$.

Propoziţia 4.5. *Fie E un corp şi $k, K, L \subset E$ subcorpuri.*
(i) Dacă $k \subset K$ este extindere algebrică, atunci $L \subset KL$ este extindere algebrică.
(ii) Dacă $k \subset K$ şi $k \subset L$ sunt extinderi algebrice, atunci $k \subset KL$ este extindere algebrică.

Proof. Putem ilustra situaţia dată prin următoarea diagramă:



(i) $KL = L(K)$ şi cum elementele lui K sunt algebrice peste L rezultă că $L \subset KL$ este extindere algebrică (vezi corolarul 4.3).
(ii) Rezultă din (i) şi din tranzitivitatea extinderilor algebrice. □

Remarca 4.6. Propoziţia de mai sus rămâne adevărată dacă în loc de extinderi algebrice considerăm extinderi finite sau de tip finit.

Propoziţia 4.7. *Fie $K \subset L$ o extindere de corpuri. Atunci $K'_L = \{\alpha \in L : \alpha$ este algebric peste $K\}$ este subcorp al lui L şi extindere algebrică a lui K.*

Proof. Fie $\alpha, \beta \in K'_L$. Extinderea $K \subset K(\alpha, \beta)$ este algebrică, deci $\alpha - \beta$ şi $\alpha\beta$ sunt algebrice peste K. □

Definiţia 4.8. *Fie $K \subset L$ o extindere de corpuri. Corpul K'_L se numeşte* închiderea algebrică a lui K în L.

Să observăm că $K \subset L$ este extindere algebrică dacă şi numai dacă $K'_L = L$.

Exemplul 4.9. (a) $\sqrt{2}+\sqrt[15]{7}+\sqrt[3]{2+\sqrt[5]{4}}$ este algebric peste $\mathbb{Q}$.
(b) $e+\sqrt{3}$ este transcendent peste $\mathbb{Q}$.

Teorema 4.10. (Lema lui Zariski) *Fie $K \subset L$ o extindere de corpuri. Dacă $L = K[a_1, \ldots, a_n]$, adică L este K-algebră de tip finit, atunci extinderea este algebrică.*

Proof. Cazul $n = 1$ rezultă din propoziţia 3.14(iii). Presupunem $n > 1$ şi că nu toate elementele $a_1, \ldots, a_n$ sunt algebrice peste K. Putem acum renumerota elementele $a_1, \ldots, a_n$ astfel încât $a_1, \ldots, a_m$ $(m \geq 1)$ sunt algebric independente peste K (adică nu există $f \in K[X_1, \ldots, X_m]$, $f \neq 0$ cu $f(a_1, \ldots, a_m) = 0$) iar fiecare dintre elementele $a_{m+1}, \ldots, a_n$ este algebric peste corpul $F = K(a_1, \ldots, a_m)$. Aşadar $F \subset L$ este extindere finită. Din lema Artin-Tate aplicată lui $K \subset F \subset L$ deducem că F este K-algebră de tip finit. Scriem $F = K[b_1, \ldots, b_s]$, unde $b_i = f_i(a_1, \ldots, a_m)/g_i(a_1, \ldots, a_m)$ cu $f_i, g_i \in K[X_1, \ldots, X_m]$. Deoarece $a_1, \ldots, a_m$ sunt algebric independente peste K avem că $K[a_1, \ldots, a_m] \simeq K[X_1, \ldots, X_m]$. Fie $h \in K[a_1, \ldots, a_m]$ ireductibil cu proprietatea că $h \mid g_1 \cdots g_s + 1$, deci $(h, g_i) = 1$ pentru orice $i = 1, \ldots, m$. Cum însă F este corp, $h^{-1} \in F$, deci h^{-1} este polinom în $b_1, \ldots, b_s$, contradicţie. □

Remarca 4.11. (i) Partea finală a demonstraţiei lemei lui Zariski este echivalentă cu a arăta că un corp de fracţii algebrice raţionale peste K nu poate fi K-algebră de tip finit. Aceasta rezultă dintr-un fapt mai general: dacă R este un inel factorial care are o infinitate de elemente prime (neasociate), atunci $Q(R)$ corpul de fracţii al lui R nu este R-algebră de tip finit.
(ii) O reformulare a lemei lui Zariski este următoarea: Dacă $M \subset K[X_1, \ldots, X_n]$ este ideal maximal, atunci $K[X_1, \ldots, X_n]/M$ este extindere algebrică (finită) a lui K. (Reciproca este de asemenea adevărată.)

Exerciţiul 4.12. Fie K corp şi $\mathbb{Z}$-algebră de tip finit. Arătaţi că K este corp finit.

5. Corpuri algebric închise.

Definiţia 5.1. *Fie $K \subset L$ o extindere de corpuri. Dacă $K'_L = K$, atunci spunem că K este* algebric închis în L. *Un corp K se numeşte* algebric închis *dacă este algebric închis în orice extindere a sa.*

Exemplul 5.2. (a) K'_L este algebric închis în L.
(b) K este algebric închis în $K(X)$.

Nu este însă simplu să dăm exemple de corpuri algebric închise. Un astfel de exemplu este, după cum vom vedea, $\mathbb{C}$, corpul numerelor complexe.

Teorema 5.3. (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 $f(\alpha) = 0$. □

Corolarul 5.4. *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.*

Propoziţia 5.5. *Fie K un corp. Următoarele afirmaţii sunt echivalente:*
(i) Orice polinom $f \in K[X]$ cu $\deg f \geq 1$ se descompune în produs de polinoame de grad 1 din $K[X]$.
(ii) Orice polinom $f \in K[X]$ cu $\deg f \geq 1$ are cel puţin o rădăcină în K.
(iii) Orice polinom $f \in K[X]$ cu $\deg f \geq 1$ şi ireductibil este de grad 1.
(iv) K este corp algebric închis.

Proof. Sunt evidente (i) $\Rightarrow$ (iii), (iii) $\Rightarrow$ (ii), (ii) $\Rightarrow$ (i) şi (iii) $\Rightarrow$ (iv).
(iv) $\Rightarrow$ (iii) Fie $f \in K[X]$ ireductibil. Există $L \supset K$ şi $\alpha \in L$ astfel încât $f(\alpha) = 0$ (vezi teorema 5.3). Aşadar α este algebric peste K, deci $\alpha \in K$ şi $\mathrm{Irr}(\alpha, K) = X - \alpha$ ceea ce implică $f = c(X - \alpha)$, $c \in K^\times$. □

Corolarul 5.6. *Fie $K \subset L$ o extindere de corpuri. Dacă L este corp algebric închis, atunci K'_L este de asemenea corp algebric închis.*

Proof. Fie $f \in K'_L[X]$ cu $\deg f \geq 1$. Atunci $f \in L[X]$ şi cum L este algebric închis rezultă că există $\alpha \in L$ astfel încât $f(\alpha) = 0$. În particular, α este algebric peste K'_L. Dar K'_L este algebric închis în L, deci $\alpha \in K'_L$. □

Exemplul 5.7. Considerăm extinderea $\mathbb{Q} \subset \mathbb{C}$. Deoarece $\mathbb{C}$ este corp algebric închis, atunci şi $\mathbb{Q}'_{\mathbb{C}}$ este corp algebric închis. Acesta se numeşte *corpul numerelor algebrice*.

Vom demonstra acum că $\mathbb{C}$, corpul numerelor complexe, este algebric închis.

Teorema 5.8. (Teorema fundamentală a algebrei) $\mathbb{C}$ *este corp algebric închis.*

Proof. Începem prin a observa că este suficient să demonstrăm că orice polinom cu coeficienţi *reali* are o rădăcină complexă: dacă $f \in \mathbb{C}[X]$, considerăm $g = f\overline{f} \in \mathbb{R}[X]$. Fie $\alpha \in \mathbb{C}$ astfel încât $g(\alpha) = 0 \Rightarrow f(\alpha)\overline{f}(\alpha) = 0 \Rightarrow f(\alpha) = 0$ sau $\overline{f}(\alpha) = 0$. Dar $\overline{f}(\alpha) = 0$ implică $f(\overline{\alpha}) = 0$.

Fie acum $f \in \mathbb{R}[X]$, $\deg f = n \geq 1$ şi scriem $n = 2^k m$ cu $k \in \mathbb{N}$ şi m impar. Vom face inducţie după $k \geq 0$.
Pentru $k = 0$ avem $\deg f = m$ impar şi fie $\tilde{f} : \mathbb{R} \to \mathbb{R}$ funcţia polinomială asociată lui f. Deoarece $\tilde{f}$ este funcţie continuă şi limitele sale la $\pm\infty$ sunt $\pm\infty$ (sau invers), rezultă că $\tilde{f}$ are cel puţin un zero real.
Fie $k \geq 1$. Din corolarul 5.4 ştim că există o extindere $L \supset \mathbb{C}$ în care f are toate rădăcinile. Fie $\alpha_1, \ldots, \alpha_n \in L$ rădăcinile lui f şi $a \in \mathbb{R}$ arbitrar. Definim $z_{ij}^a = \alpha_i\alpha_j + a(\alpha_i + \alpha_j)$, $1 \leq i, j \leq n$ şi $g_a(X) = \prod_{1 \leq i < j \leq n}(X - z_{ij}^a)$. Avem $\deg g_a = 2^{k-1}\underbrace{m(2^k m - 1)}_{\text{impar}}$. Mai mult, $g_a \in \mathbb{R}[X]$ (deoarece coeficienţii lui g_a sunt polinoame simetrice în $\alpha_1, \ldots, \alpha_n$) şi din ipoteza de inducţie există o pereche (i, j), $1 \leq i < j \leq n$, cu $z_{ij}^a \in \mathbb{C}$. Cum $a \in \mathbb{R}$ a fost ales arbitrar va exista o pereche (i, j) şi $a, a' \in \mathbb{R}$, $a \neq a'$ astfel încât $z_{ij}^a, z_{ij}^{a'} \in \mathbb{C}$. De aici rezultă că $z_{ij}^a - z_{ij}^{a'} \in \mathbb{C} \Rightarrow \alpha_i + \alpha_j \in \mathbb{C} \Rightarrow \alpha_i\alpha_j \in \mathbb{C}$. În consecinţă $\alpha_i, \alpha_j \in \mathbb{C}$. □

Hilbert a generalizat teorema fundamentală a algebrei la inele de polinoame de mai multe nedeterminate.

Teorema 5.9. (Teorema lui Hilbert a zerourilor, forma slabă)
Fie K un corp algebric închis şi $f_1, \dots, f_m \in K[X_1, \dots, X_n]$. Dacă $(f_1, \dots, f_m) \neq K[X_1, \dots, X_n]$, atunci există $(\alpha_1, \dots, \alpha_n) \in K^n$ astfel încât $f_i(\alpha_1, \dots, \alpha_n) = 0$ pentru orice $i = 1, \dots, m$.

Proof. Fie M un ideal maximal în $K[X_1, \dots, X_n]$. Atunci $K[X_1, \dots, X_n]/M$ este o K-algebră de tip finit şi din lema lui Zariski rezultă că este extindere algebrică a lui K. Cum K este însă corp algebric închis deducem că $K = K[X_1, \dots, X_n]/M$. Dacă α_i este imaginea lui X_i mod M în K, atunci $X_i - \alpha_i \in M$, deci $(X_1 - \alpha_1, \dots, X_n - \alpha_n) \subseteq M$. Dar $(X_1 - \alpha_1, \dots, X_n - \alpha_n)$ este ideal maximal în $K[X_1, \dots, X_n]$, aşadar $(X_1 - \alpha_1, \dots, X_n - \alpha_n) = M$.
Deoarece $(f_1, \dots, f_m)$ este ideal propriu acesta este conţinut într-un ideal maximal, deci există $(\alpha_1, \dots, \alpha_n) \in K^n$ cu proprietatea că $(f_1, \dots, f_m) \subseteq (X_1 - \alpha_1, \dots, X_n - \alpha_n)$. De aici rezultă că $f_i(\alpha_1, \dots, \alpha_n) = 0$ pentru orice $i = 1, \dots, m$. □

6. Închiderea algebrică a unui corp

Definiţia 6.1. *Fie K un corp. Se numeşte* închidere algebrică *a lui K un corp $\overline{K}$ cu următoarele proprietăţi:*
(i) $K \subset \overline{K}$ este extindere algebrică;
(ii) $\overline{K}$ este corp algebric închis.

Vom arăta în cele ce urmează că orice corp admite o închidere algebrică şi că aceasta este unică (până la un K-izomorfism).

Teorema 6.2. *Orice corp admite o închidere algebrică.*

Înainte de a începe demonstraţia să construim *inele de polinoame într-o mulţime arbitrară de nedeterminate*. Fie $I \neq \emptyset$ o mulţime de indici. Notăm cu $\mathbb{N}^{(I)}$ mulţimea funcţiilor de suport finit definite pe I cu valori în $\mathbb{N}$. Definim suma a două funcţii de suport finit $\mu, \nu : I \to \mathbb{N}$ prin $(\mu+\nu)(i) = \mu(i)+\nu(i)$ pentru orice $i \in I$. Considerăm I ca o submulţime a lui $\mathbb{N}^{(I)}$ identificând $i \in I$ cu funcţia δ_i care duce pe i în 1 şi celelalte elemente din I în 0. Fie R un inel comutativ unitar şi $R[X_i : i \in I]$ mulţimea funcţiilor de suport finit definite pe $\mathbb{N}^{(I)}$ cu valori în R. Definim pe $R[X_i : i \in I]$ adunarea şi înmulţirea astfel:

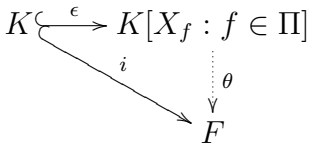
$$(f + g)(\mu) = f(\mu) + g(\mu) \text{ şi } (f * g)(\mu) = \sum_{\mu=\mu_1+\mu_2} f(\mu_1)g(\mu_2)$$

pentru orice $\mu \in \mathbb{N}^{(I)}$. Cu aceste două operaţii $R[X_i : i \in I]$ devine un inel comutativ unitar, elementul unitate fiind: $1(\mu) = 1$ dacă $\mu = 0$ şi $1(\mu) = 0$ dacă $\mu \neq 0$. $R[X_i : i \in I]$ se numeşte *inelul de polinoame în nedeterminatele $(X_i)_{i\in I}$ cu coeficienţi în R*. Pentru orice $i \in I$ avem o funcţie $X_i : \mathbb{N}^{(I)} \to R$ definită prin: $X_i(i) = 1$ şi $X_i(\mu) = 0$ pentru $\mu \neq i$. Pentru orice $n \in \mathbb{N}$ avem $X_i^n(ni) = 1$ şi $X_i^n(\mu) = 0$ pentru $\mu \neq ni$, unde $X_i^n = \underbrace{X_i * \cdots * X_i}_{\text{de } n \text{ ori}}$. Pentru orice $\mu \in \mathbb{N}^{(I)}$ definim $X^\mu = \prod_{i\in I} X_i^{\mu(i)}$

şi observăm că $X^\mu(\nu)$ este 1 când $\nu = \sum_{i\in I}\mu(i)i$ şi 0 altfel. În consecinţă, orice $f \in R[X_i : i \in I]$ se scrie în mod unic în forma $f = \sum_{\mu\in\mathbb{N}^{(I)}} f(\mu)X^\mu$.

Ca şi în cazul polinoamelor într-un număr finit de nedeterminate se arată că $R[X_i : i \in I]$ satisface proprietatea de universalitate a inelelor de polinoame. Să mai remarcăm că $R[X_i : i \in I] = \bigcup_{J\subseteq I,\, J \text{ finită}} R[X_i : i \in J]$.

Proof. Arătăm mai întâi că orice corp K are o extindere care este corp algebric închis. Fie $\Pi \subset K[X]$ mulţimea polinoamelor de grad ≥ 1. Construim inelul de polinoame $R = K[X_f : f \in \Pi]$ în nedeterminatele $(X_f)_{f\in\Pi}$ cu coeficienţi în K. Fie I idealul lui R generat de polinoamele $f(X_f)$, $f \in \Pi$. Să arătăm că I este ideal propriu. Dacă $I = R$, atunci $1 \in I$ şi deci $1 = \sum_{i=1}^n g_i f_i(X_{f_i})$ cu $g_i \in R$. Din teorema 5.3 rezultă că există o extindere $K \subset F$ şi $\alpha_1, \ldots, \alpha_n \in F$ astfel încât $f_i(\alpha_i) = 0$ pentru orice $i = 1, \ldots, n$. Din proprietatea de universalitate a inelelor de polinoame există un (unic) morfism $\theta : K[X_f : f \in \Pi] \to F$ astfel încât $\theta(X_{f_i}) = \alpha_i$ pentru $i = 1, \ldots, n$ şi $\theta(X_f) = 0$ pentru $f \neq f_1, \ldots, f_n$.



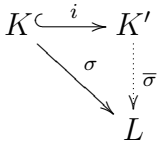
Atunci $1 = \theta(1) = \sum_{i=1}^n \theta(g_i)\theta(f_i(X_{f_i})) = \sum_{i=1}^n \theta(g_i)f_i(\alpha_i) = 0$, contradicţie.

Din lema lui Krull există $I \subseteq M \subsetneq R$ ideal maximal. Fie $K_1 = R/M$. Acesta este corp, extindere a lui K, cu proprietatea că *orice polinom din* $K[X]$ *are o rădăcină în* K_1, deoarece $f(\widehat{X_f}) = \widehat{f(X_f)} = 0$.

Procedând ca mai sus obţinem un şir de extinderi de corpuri $K \subset K_1 \subset \cdots \subset K_n \subset K_{n+1} \subset \cdots$ cu proprietatea că orice polinom din $K_n[X]$ are o rădăcină în K_{n+1}. Fie $L = \bigcup_{n=1}^\infty K_n$. Avem că L este corp şi orice polinom din $L[X]$ are o rădăcină în L, deci L este corp algebric închis. Acum nu avem decât să considerăm K'_L şi din corolarul 5.6 rezultă că K'_L este închidere algebrică a lui K. □

Definiţia 6.3. *Fie $K \subset K'$ o extindere de corpuri şi $\sigma : K \to L$ un morfism de corpuri. Un morfism $\overline{\sigma} : K' \to L$ cu proprietatea că $\overline{\sigma}_{|K} = \sigma$ se numeşte* extensie a lui σ *la* K'.

Să observăm că $\overline{\sigma}_{|K} = \sigma$ este echivalent cu $\overline{\sigma}i = \sigma$, adică diagrama următoare este comutativă.

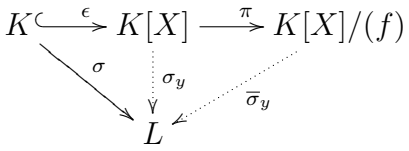


Fie K un corp, $f \in K[X]$, $f = a_0 + a_1X + \cdots + a_nX^n$ şi $\sigma : K \to L$ un morfism de corpuri. Vom nota $f^\sigma = \sigma(a_0) + \sigma(a_1)X + \cdots + \sigma(a_n)X^n \in L[X]$. (Să observăm că σ se extinde la un morfism $\sigma' : K[X] \to L[X]$ şi că, de fapt, $f^\sigma = \sigma'(f)$.)

Lema 6.4. *Fie $K \subset K(\alpha)$ o extindere algebrică simplă, L corp algebric închis şi $\sigma : K \to L$ morfism de corpuri. Atunci există $\overline{\sigma} : K(\alpha) \to L$ extensie a lui σ.*

Mai mult, numărul acestor extensii coincide cu numărul rădăcinilor distincte ale lui f^σ în L, unde $f = \mathrm{Irr}(\alpha, K)$.

Proof. Din propoziţia 3.14 ştim că $K(\alpha) = K[\alpha] \simeq K[X]/(f)$. Fie $y \in L$ o rădăcină a lui f^σ. Din proprietatea de universalitate a inelelor de polinoame există $\sigma_y : K[X] \to L$ cu $\sigma_y(X) = y$. Deoarece $f^\sigma(y) = 0$ avem că $(f) \subseteq \ker \sigma_y$ şi din proprietatea de universalitate a inelelor factor există $\overline{\sigma}_y : K[X]/(f) \to L$ care face următoarea diagramă comutativă:



Reciproc, fie $\overline{\sigma} : K(\alpha) \to L$ o extensie a lui σ. Atunci $f^\sigma(\overline{\sigma}(\alpha)) = 0$, deci $\overline{\sigma}(\alpha) \in L$ este rădăcină a lui f. □

Teorema 6.5. (Teorema de prelungire a lui Steinitz) *Fie $K \subset K'$ o extindere algebrică, L corp algebric închis şi $\sigma : K \to L$ morfism de corpuri. Atunci există $\overline{\sigma} : K' \to L$ extensie a lui σ.*

Proof. Fie

$$\mathcal{F} = \{(K_i, \sigma_i) : K \subseteq K_i \subseteq K' \text{ extindere intermediară}, \sigma_i : K_i \to L$$

$$\text{morfism de corpuri şi } \sigma_{i|K} = \sigma\}.$$

Se observă că $\mathcal{F} \neq \emptyset$ deoarece $(K, \sigma) \in \mathcal{F}$. Definim pe $\mathcal{F}$ o relaţie de ordine astfel:

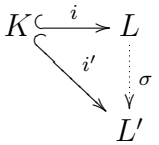
$$(K_i, \sigma_i) \preceq (K_j, \sigma_j) \text{ dacă şi numai dacă } K_i \subseteq K_j \text{ şi } \sigma_{j|K_i} = \sigma_i.$$

Vom arăta că $(\mathcal{F}, \preceq)$ este inductiv ordonată. Fie $(K_i, \sigma_i)_{i \in I}$ o parte total ordonată a lui $\mathcal{F}$. Aceasta este majorată de $(\bigcup_{i \in I} K_i, \tau)$, unde $\tau : \bigcup_{i \in I} K_i \to L$ se defineşte astfel: $\tau(x) = \sigma_i(x)$ dacă $x \in K_i$. (Se observă că total ordonarea ne garantează că $\bigcup_{i \in I} K_i$ este corp şi că τ este corect definită.)

Din lema lui Zorn rezultă că $\mathcal{F}$ admite (cel puţin) un element maximal, notat (K_0, σ_0). Dacă $K_0 \subsetneq K'$, atunci fie $\alpha \in K' - K_0$. Din lema 6.4 există $\overline{\sigma}_0 : K_0(\alpha) \to L$ extensie a lui σ_0, deci $(K_0, \sigma_0) \prec (K_0(\alpha), \overline{\sigma}_0)$, contradicţie. □

Corolarul 6.6. *Orice două închideri algebrice ale unui corp K sunt K-izomorfe.*

Proof. Fie L, L' închideri algebrice ale lui K. Considerăm diagrama



Din teorema de prelungire a lui Steinitz există $\sigma : L \to L'$ morfism de corpuri cu $\sigma_{|K} = i'$. Rezultă că $K \subset \sigma(L) \subset L'$ şi cum $K \subset L'$ este extindere algebrică avem că şi extinderea $\sigma(L) \subset L'$ este algebrică. Dar $\sigma(L) \simeq L$ este corp algebric închis, deci $\sigma(L) = L'$. În concluzie, σ este un K-izomorfism între L şi L'. □

O consecinţă acestui corolar este faptul că $\overline{\mathbb{Q}}$, închiderea algebrică a lui $\mathbb{Q}$, este (izomorfă cu) $\mathbb{Q}'_{\mathbb{C}}$.

7. Corpul de descompunere al unui polinom

Definiţia 7.1. *Fie K corp şi $f \in K[X]$ cu* $\deg f \geq 1$. *O extindere L a lui K se numeşte* corp de descompunere al lui f peste K *dacă există $a \in K^\times$ şi $\alpha_1, \ldots, \alpha_n \in L$ astfel încât $f(X) = a\prod_{i=1}^n (X - \alpha_i)$ şi $L = K(\alpha_1, \ldots, \alpha_n)$.*

Să observă că dacă L este corp de descompunere al unui polinom din $K[X]$, atunci $K \subset L$ este extindere algebrică.

Exemplul 7.2. (i) Fie $f = X^2 - 2 \in \mathbb{Q}[X]$. Avem că $\mathbb{Q}(\sqrt{2})$ este corp de descompunere al lui f peste $\mathbb{Q}$.
(ii) Fie $f = X^2 + 1 \in \mathbb{R}[X]$. Avem că $\mathbb{C}$ este corp de descompunere al lui f peste $\mathbb{R}$.
(iii) Fie $f = X^3 - 2 \in \mathbb{Q}[X]$. Avem că $\mathbb{Q}(\sqrt[3]{2}, \epsilon)$ este corp de descompunere al lui f peste $\mathbb{Q}$, unde ϵ este o rădăcină primitivă de ordin trei a unităţii.

Teorema 7.3. *Fie K un corp şi $f \in K[X]$ cu* $\deg f \geq 1$. *Atunci f admite un corp de descompunere şi acesta este unic până la un K-izomorfism.*

Proof. Fie $\overline{K}$ o închidere algebrică a lui K şi $\alpha_1, \ldots, \alpha_n$ rădăcinile lui f în $\overline{K}$. Atunci $L = K(\alpha_1, \ldots, \alpha_n)$ este corp de descompunere al lui f peste K. Scriem

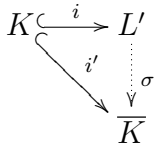
$$f(X) = a\prod_{i=1}^n (X - \alpha_i),$$

unde $a \in K^\times$.

Fie L' un alt corp de descompunere al lui f peste K. Avem

$$f(X) = a\prod_{i=1}^n (X - \alpha_i')$$

cu $\alpha_i' \in L'$ şi $L' = K(\alpha_1', \ldots, \alpha_n')$. Considerăm diagrama



Din teorema de prelungire a lui Steinitz există $\sigma : L' \to \overline{K}$ un K-morfism. Aşadar $f(X) = f^\sigma(X) = a\prod_{i=1}^n (X - \sigma(\alpha_i'))$ în $\overline{K}[X]$. Cum însă $f(X) = a\prod_{i=1}^n (X - \alpha_i)$ în $\overline{K}[X]$ rezultă că $\sigma(\alpha_1'), \ldots, \sigma(\alpha_n')$ diferă de $\alpha_1, \ldots, \alpha_n$ printr-o permutare, deci $\sigma(L') = L$. □

Să menţionăm că noţiunea de corp de descompunere se extinde uşor la o familie arbitrară de polinoame şi are aceleaşi proprietăţi.

8. Rădăcini multiple

Definiţia 8.1. *Fie K un corp, $f \in K[X]$ cu $\deg f \geq 1$ şi $\alpha \in \overline{K}$ o rădăcină a lui f. Aceasta se numeşte* rădăcină multiplă *dacă există $s \geq 2$ astfel încât $(X-\alpha)^s \mid f$. În caz contrar, α se numeşte* rădăcină simplă.

Deoarece $K[X]$ este K-spaţiu vectorial de bază $1, X, X^2, \ldots$ putem defini o unică aplicaţie liniară $d : K[X] \to K[X]$ astfel încât $d(X^i) = iX^{i-1}$ pentru $i \geq 1$ şi $d(1) = 0$.

Definiţia 8.2. *Dacă $f \in K[X]$, atunci $d(f)$ se numeşte* derivata polinomului *f.*

Vom nota $d(f)$ cu f'. Avem $a' = 0$ pentru orice $a \in K$. Dacă $f = a_0 + a_1X + \cdots + a_nX^n$, atunci $f' = a_1 + 2a_2X + \cdots + na_nX^{n-1}$. Mai mult, $(fg)' = f'g + fg'$ pentru orice $f, g \in K[X]$.

Propoziţia 8.3. *Fie K un corp, $f \in K[X]$ cu $\deg f \geq 1$ şi $\alpha \in \overline{K}$ o rădăcină a lui f. Atunci α este rădăcină multiplă a lui f dacă şi numai dacă $f(\alpha) = f'(\alpha) = 0$.*

Proof. "$\Rightarrow$" Există $s \geq 2$ astfel încât $(X-\alpha)^s \mid f$ (în $\overline{K}[X]$), deci $f = (X-\alpha)^s g$ cu $g \in \overline{K}[X]$. Cum $f' = s(X-\alpha)^{s-1}g + (X-\alpha)^s g'$ obţinem $f'(\alpha) = 0$.
"$\Leftarrow$" Scriem $f = (X-\alpha)g$ (în $\overline{K}[X]$) şi avem $f' = g + (X-\alpha)g'$. Din $f'(\alpha) = 0$ obţinem $g(\alpha) = 0$, deci $X - \alpha \mid g \Rightarrow (X-\alpha)^2 \mid f$. □

Corolarul 8.4. *Fie K un corp şi $f \in K[X]$ cu $\deg f \geq 1$. Atunci f nu are rădăcini multiple dacă şi numai dacă $(f, f') = 1$.*

Proof. "$\Rightarrow$" Dacă $(f, f') \neq 1$, atunci există $g \in K[X]$ cu $\deg g \geq 1$ astfel încât $g \mid f$ şi $g \mid f'$. Fie $\alpha \in \overline{K}$ o rădăcină a lui g. Rezultă $f(\alpha) = f'(\alpha) = 0$, deci α este rădăcină multiplă a lui f, contradicţie.
"$\Leftarrow$" Dacă, prin absurd, $\alpha \in \overline{K}$ ar fi o rădăcină multiplă a lui f, atunci $f(\alpha) = f'(\alpha) = 0$ şi vom avea că $\mathrm{Irr}(\alpha, K) \mid f$ şi $\mathrm{Irr}(\alpha, K) \mid f'$, contradicţie. □

Exerciţiul 8.5. Fie $K \subset L$ o extindere de corpuri.
(i) Fie $f, g \in K[X]$. Arătaţi că $(f, g) = 1$ în $K[X]$ dacă şi numai dacă $(f, g) = 1$ în $L[X]$.
(ii)* Fie $f, g \in K[X_1, \ldots, X_n]$, $n \geq 2$. Arătaţi că $(f, g) = 1$ în $K[X_1, \ldots, X_n]$ dacă şi numai dacă $(f, g) = 1$ în $L[X_1, \ldots, X_n]$.

9. Rădăcini ale unităţii. Polinoame ciclotomice

Fie K un corp şi $n \in \mathbb{N}$, $n \geq 1$. Presupunem $\mathrm{char}\, K = 0$ sau $\mathrm{char}\, K = p > 0$ şi $(p, n) = 1$. În aceste cazuri polinomul $X^n - 1 \in K[X]$ are n rădăcini distincte (în $\overline{K}$), deoarece $(X^n - 1)' = nX^{n-1} \neq 0$ şi $(X^n - 1, nX^{n-1}) = 1$.

Fie $U_n = \{\xi \in \overline{K} : \xi^n = 1\}$ mulţimea rădăcinilor polinomului $X^n - 1$.

Lema 9.1. *Fie K corp şi G un subgrup finit al lui $K^\times$. Atunci G este grup ciclic.*

Proof. G este grup abelian finit, deci $G \simeq \mathbb{Z}_{d_1} \oplus \cdots \oplus \mathbb{Z}_{d_r}$, unde $d_i \geq 2$ au proprietatea că $d_1 \mid \cdots \mid d_r$. Cum $g^{d_r} = 1$ pentru orice $g \in G$ rezultă că polinomul $X^{d_r} - 1 \in K[X]$ are $|G|$ rădăcini (distincte) în K, deci $|G| \leq d_r$. De aici rezultă imediat că G este ciclic. □

Corolarul 9.2. *U_n este grup ciclic de ordin n, deci are $\varphi(n)$ generatori.*

Proof. Dacă $\xi_1, \xi_2 \in U_n$, atunci $\xi_1\xi_2^{-1} \in U_n$ deoarece $(\xi_1\xi_2^{-1})^n = \xi_1^n(\xi_2^n)^{-1} = 1$. Aşadar U_n este subgrup finit al lui $\overline{K}^\times$, deci ciclic. Cum $|U_n| = n$ rezultă că $U_n \simeq \mathbb{Z}/n\mathbb{Z}$, deci U_n are $\varphi(n)$ generatori. □

Definiţia 9.3. *U_n se numeşte* grupul rădăcinilor de ordin n ale unităţii *iar un generator $\xi \in U_n$ se numeşte* rădăcină primitivă de ordin n a unităţii.

Să observăm că dacă $\xi \in U_n$ este rădăcină primitivă, atunci $U_n = \{1, \xi, \ldots, \xi^{n-1}\}$.

Propoziţia 9.4. *Fie $\xi \in U_n$ o rădăcină primitivă şi $m \in \mathbb{N}$, $m \geq 1$. Atunci ξ^m este rădăcină primitivă de ordin n a unităţii dacă şi numai dacă $(m, n) = 1$.*

Proof. "⇒" Fie $d = (m, n)$. Scriem $m = dm_1$, $n = dn_1$ cu $(m_1, n_1) = 1$. Dacă $d > 1$, atunci $(\xi^m)^{n_1} = 1$ implică $\text{ord}(\xi^m) < n$, contradicţie.
"⇐" Avem $(\xi^m)^n = (\xi^n)^m = 1$ şi dacă $(\xi^m)^r = 1$, atunci $n \mid mr$, deci $n \mid r$. Aşadar $\text{ord}(\xi^m) = n$. □

Definiţia 9.5. *Fie $n \in \mathbb{N}$, $n \geq 1$, $r = \varphi(n)$ şi $\xi_1, \ldots, \xi_r \in \overline{K}$ rădăcinile primitive de ordin n ale unităţii. Polinomul*

$$\Phi_n(X) = \prod_{i=1}^{r}(X - \xi_i)$$

se numeşte al n-lea polinom ciclotomic peste K.

Exerciţiul 9.6. *Arătaţi că $\Phi_n \in k[X]$, unde k este corpul prim al lui K.*

În cele ce urmează considerăm $K = \mathbb{Q}$.
Să notăm că $\Phi_1(X) = X-1$, $\Phi_2(X) = X+1$, $\Phi_3(X) = X^2+X+1$ şi $\Phi_4(X) = X^2+1$.
Vom da acum o metodă (recurentă) de calcul a polinoamelor ciclotomice.

Propoziţia 9.7.

$$X^n - 1 = \prod_{d|n} \Phi_d(X)$$

Proof. $X^n - 1 = \prod_{\xi \in U_n}(X - \xi) = \prod_{d|n} \prod_{\xi \in U_n,\, \text{ord}(\xi)=d}(X - \xi) = \prod_{d|n} \Phi_d(X)$. □

Corolarul 9.8. (Gauss)

$$n = \sum_{d|n} \varphi(d)$$

Proof. $n = \deg(X^n - 1) = \deg \prod_{d|n} \Phi_d(X) = \sum_{d|n} \deg \Phi_d(X) = \sum_{d|n} \varphi(d)$. □

Exemplul 9.9. (i) $\Phi_p(X) = \dfrac{X^p - 1}{\Phi_1(X)} = \dfrac{X^p - 1}{X - 1} = X^{p-1} + \cdots + X + 1.$

(ii) $\Phi_6(X) = \dfrac{X^6 - 1}{\Phi_1(X)\Phi_2(X)\Phi_3(X)} = X^2 - X + 1.$

Considerând şi alte exemple am putea concluziona că singurii coeficienţi posibili ai polinoamelor ciclotomice sunt $-1, 0, 1$. (De fapt aceasta este adevărat pentru $n \leq 104$ sau pentru orice n care are cel mult doi factori primi distincţi.) Însă pentru $n = 105$ acest lucru nu mai este adevărat.

Exerciţiul 9.10. (i) Determinaţi $\Phi_{105}(X)$.
(ii) Arătaţi că $\Phi_n(X)$ are doar coeficienţii 0 şi 1 dacă şi numai dacă n este putere a unui număr prim.

Exerciţiul 9.11. (i) Dacă $n \geq 3$ este impar, atunci $\Phi_{2n}(X) = \Phi_n(-X)$.
(ii) Dacă p este număr prim şi $m \in \mathbb{N}$, $m \geq 2$, atunci $\Phi_{p^m}(X) = \Phi_p(X^{p^{m-1}})$.
(iii) Dacă p este număr prim şi $n \in \mathbb{N}$ cu $p \nmid n$, atunci $\Phi_{pn}(X) = \Phi_n(X^p)/\Phi_n(X)$.
(iv) Pentru orice $n \geq 2$ avem $\Phi_n(X) = X^{\varphi(n)}\Phi_n(1/X)$.

Teorema 9.12. *Polinomul ciclotomic $\Phi_n(X)$ este polinom monic ireductibil în $\mathbb{Z}[X]$.*

Proof. (Dedekind, 1857) Să arătăm mai întâi că $\Phi_n(X) \in \mathbb{Z}[X]$. Vom proceda prin inducţie după $n \geq 1$. Pentru $n = 1$ ştim că $\Phi_1(X) = X - 1 \in \mathbb{Z}[X]$. În cazul general scriem $X^n - 1 = \Phi_n(X)u(X)$, unde $u(X) = \prod_{d|n,\, d<n} \Phi_d(X)$. Din ipoteza de inducţie $u \in \mathbb{Z}[X]$. Cum u este polinom monic putem împărţi cu rest orice polinom din $\mathbb{Z}[X]$ la u. În particular, există $q, r \in \mathbb{Z}[X]$ astfel încât $X^n - 1 = u(X)q(X) + r(X)$ şi $\deg r < \deg u$. Din unicitatea algoritmului de împărţire cu rest (în $\mathbb{C}[X]$) rezultă $r = 0$ şi $q(X) = \Phi_n(X)$, deci $\Phi_n(X) \in \mathbb{Z}[X]$.

Arătăm acum că $\Phi_n(X)$ este ireductibil în $\mathbb{Z}[X]$. Fie $h \in \mathbb{Z}[X]$ polinom monic ireductibil de grad ≥ 1 cu proprietatea că $h \mid \Phi_n$ (în $\mathbb{Z}[X]$). Scriem $\Phi_n = hf$ cu $f \in \mathbb{Z}[X]$ monic. Fie $\zeta \in \mathbb{C}$ o rădăcină a lui h şi $p > 0$ un număr prim cu $(p, n) = 1$. Vom demonstra că ζ^p este de asemenea rădăcină a lui h: $h(\zeta) = 0 \Rightarrow \Phi_n(\zeta) = 0$, deci ζ este rădăcină primitivă de ordin n a unităţii. Cum $(p, n) = 1$, din propoziţia 9.4 rezultă că şi ζ^p este rădăcină primitivă de ordin n a unităţii. Aşadar $\Phi_n(\zeta^p) = 0$, deci $h(\zeta^p) = 0$ sau $f(\zeta^p) = 0$. Să presupunem $h(\zeta^p) \neq 0$. Atunci $f(\zeta^p) = 0$, deci ζ este rădăcină a polinomului $f(X^p)$. Dar $\mathrm{Irr}(\zeta, \mathbb{Q}) = h$, deci $h(X) \mid f(X^p)$. Scriem $f(X^p) = h(X)g(X)$ cu $g \in \mathbb{Q}[X]$. La fel ca în prima parte a acestei demonstraţii se arată că $g \in \mathbb{Z}[X]$. Rezultă că $\overline{f}(X^p) = \overline{h}(X)\overline{g}(X)$ în $(\mathbb{Z}/p\mathbb{Z})[X]$. De aici se obţine $\overline{f}(X)^p = \overline{h}(X)\overline{g}(X)$ în $(\mathbb{Z}/p\mathbb{Z})[X]$, deci $\overline{f}$ şi $\overline{h}$ au un factor ireductibil de grad ≥ 1 în comun, adică $(\overline{f}, \overline{h}) \neq 1$ în $(\mathbb{Z}/p\mathbb{Z})[X]$. Dar $X^n - \overline{1} = \overline{\Phi}_n(X)\overline{u}(X) = \overline{h}(X)\overline{f}(X)\overline{u}(X)$. Rezultă că polinomul $X^n - \overline{1} \in (\mathbb{Z}/p\mathbb{Z})[X]$ are rădăcini multiple, fals.
În concluzie, ζ^p este rădăcină a lui h şi de aici deducem că ζ^m este rădăcină a lui h pentru orice $1 \leq m < n$ cu $(m, n) = 1$, deci h are ca rădăcini toate rădăcinile primitive de ordin n ale unităţii. Obţinem $\Phi_n \mid h \Rightarrow \Phi_n = h$, adică Φ_n este polinom ireductibil. □

Corolarul 9.13. *Φ_n este polinomul minimal (peste $\mathbb{Q}$) al oricărei rădăcini primitive de ordin n a unităţii.*

Exerciţiul 9.14. Fie $n \in \mathbb{N}$, $n \geq 2$. Arătaţi că:
(i) $[\mathbb{Q}(\cos 2\pi/n) : \mathbb{Q}] = \varphi(n)/2$.
(ii) $[\mathbb{Q}(\sin 2\pi/n) : \mathbb{Q}] = \phi(n)$ if $n \not\equiv 0 \bmod 4$
$[\mathbb{Q}(\sin 2\pi/n) : \mathbb{Q}] = \phi(n)/2$ if $n \equiv 0 \bmod 8$
$[\mathbb{Q}(\sin 2\pi/n) : \mathbb{Q}] = \phi(n)/4$ if $n \equiv 4 \bmod 8$.

Să remarcăm că în caracteristică pozitivă polinoamele ciclotomice nu mai sunt neapărat ireductibile: de exemplu, $\Phi_4(X) = X^2 + 1$ este reductibil peste $\mathbb{Z}/5\mathbb{Z}$.

Polinoamele ciclotomice sunt foarte utile în teoria numerelor. Un exemplu celebru îl reprezintă demostraţia dată de către Preda Mihăilescu conjecturii lui Catalan:

ecuaţia $x^p - y^q = 1$ cu p, q numere prime nu are alte soluţii în numere naturale nenule în afară de $3^2 - 2^3 = 1$.

Vom da şi noi un exemplu, mult mai simplu, desigur, dar care este totuşi caz particular al unei teoreme celebre în teoria numerelor, teorema lui Dirichlet asupra progresiilor aritmetice, care spune că dacă avem două numere naturale pozitive a şi d cu $(a, d) = 1$, atunci progresia aritmetică $(a + nd)_{n\geq 0}$ conţine o infinitate de numere prime. (În exemplul nostru $a = 1$.)

Propoziţia 9.15. *Fie $d \in \mathbb{N}$ cu $d \geq 2$. Există o infinitate de numere prime $p \equiv 1 \bmod d$.*

Proof. Să presupunem că există doar un număr finit de numere prime de forma $1 + nd$ şi fie acestea $p_1, \ldots, p_t$. Există $l \in \mathbb{N}$ suficient de mare astfel încât $N = \Phi_d(ldp_1 \cdots p_t) > 1$, $N \in \mathbb{N}$. Deoarece $\Phi_d \in \mathbb{Z}[X]$ şi $\Phi_d(0) = \pm 1$, avem $N \equiv \pm 1 \bmod p_i$ pentru orice $i = 1, \ldots, t$ şi $N \equiv \pm 1 \bmod d$. În particular, $p_i \nmid N$ pentru orice $i = 1, \ldots, t$. Cum însă $N > 1$ există un număr prim p cu $p \mid N$. De aici rezultă că $(p, d) = 1$ şi $\Phi_d(ldp_1 \cdots p_t) \equiv 0 \bmod p$. Dar $\Phi_d(X) \mid X^d - 1$, deci $(ldp_1 \cdots p_t)^d - 1 \equiv 0 \bmod p$, adică $(ldp_1 \cdots p_t)^d \equiv 1 \bmod p$. Vom arăta mai jos că ordinul lui $ldp_1 \cdots p_t$ în $(\mathbb{Z}/p\mathbb{Z})^\times$ este d. De aici deducem că $d \mid p - 1$, sau echivalent $p \equiv 1 \bmod d$. Am găsit astfel încă un număr prim de forma $1 + nd$, contradicţie.
Fie $a = ldp_1 \cdots p_t$. Deoarece $a^d \equiv 1 \bmod p$ avem $(p, a) = 1$. Fie $m = \operatorname{ord}(a)$ în $(\mathbb{Z}/p\mathbb{Z})^\times$ şi să presupunem că $m < d$. Ştim că $m \mid d$ şi $X^d - 1 = \Phi_d(X)u(X)$, unde $u(X) = \prod_{d' \mid d,\, d' < d} \Phi_{d'}(X)$. Din $\Phi_d(a) \equiv 0 \bmod p$ şi $a^m - 1 \equiv 0 \bmod p$ (deci $\Phi_{d'}(a) \equiv 0 \bmod p$ pentru un $d' \mid m$) rezultă că a este rădăcină multiplă a lui $X^d - 1$ modulo p, ceea ce este imposibil deoarece $(p, d) = 1$. □

O altă aplicaţie a polinoamelor ciclotomice se găseşte în demonstraţia dată de către Witt teoremei lui Wedderburn.

Mai întâi însă vom stabili un rezultat din teoria grupurilor finite şi anume *ecuaţia claselor de conjugare*.

Definiţia 9.16. *Fie G un grup. Două elemente $x, y \in G$ se numesc* conjugate *dacă există $g \in G$ astfel încât $y = gxg^{-1}$. Mulţimea ${}^G x = \{gxg^{-1} : g \in G\}$ se numeşte* clasa de conjugare a lui x în G *iar mulţimea $C_G(x) = \{g \in G : gx = xg\}$ se numeşte* centralizatorul lui x în G. *Definim* centrul grupului G *ca fiind $C(G) = \bigcap_{x \in G} C_G(x)$.*

Să observăm acum că putem defini pe G o relaţie de echivalenţă cu ajutorul conjugării astfel: $x \sim y$ dacă şi numai dacă x şi y sunt conjugate. Clasa de echivalenţă a unui element $x \in G$ în raport cu relaţia de echivalenţă introdusă este clasa de conjugare a lui x. Cum clasele de echivalenţă formează o partiţie deducem că pentru un grup finit G există $x_1, \ldots, x_m \in G$ cu proprietatea că

$$|G| = |{}^G x_1| + \cdots + |{}^G x_m|. \tag{9.1}$$

O clasă de conjugare este *trivială* dacă aceasta conţine doar un singur element. Mai precis, ${}^G x = \{x\}$, şi asta se întâmplă dacă şi numai dacă $x \in C(G)$. Vom separa în relaţia (9.1) clasele de conjugare triviale şi o rescriem astfel:

$$|G| = |C(G)| + |{}^G x_1| + \cdots + |{}^G x_r|,$$

unde $|{}^G x_i| > 1$ pentru orice $i = 1, \ldots, r$.

Să mai notăm că centralizatorul unui element şi centrul unui grup sunt subgrupuri.

Lema 9.17. *Fie G un grup (finit) şi $x \in G$. Atunci $|^G x| = [G : C_G(x)]$.*

Proof. Considerăm funcţia $f : (G/C_G(x))_s \longrightarrow {}^G x$ definită prin $f(gC_G(x)) = gxg^{-1}$. Aceasta este bine definită şi bijectivă. □

Propoziţia 9.18. (Ecuaţia claselor de conjugare) *Fie G un grup finit. Atunci există $x_1, \ldots, x_r \in G - C(G)$ cu proprietatea că*

$$|G| = |C(G)| + \sum_{i=1}^{r} [G : C_G(x_i)]. \tag{9.2}$$

Revenim acum la teorema lui Wedderburn.

Lema 9.19. *Fie $q, n \in \mathbb{N}$, $q \geq 1$ şi $n \geq 2$. Atunci $|\Phi_n(q)| > q - 1$.*

Proof. Fie $\xi = \cos\theta + i \sin\theta$ o rădăcină de ordin n a unităţii, $\xi \neq 1$. Este suficient să arătăm că $|q - \xi| > |q - 1|$. Dar $|q - \xi|^2 = (q - \cos\theta)^2 + \sin^2\theta = q^2 - (2\cos\theta)q + 1 > q^2 - 2q + 1 = (q-1)^2$. □

Teorema 9.20. ("Wedderburn's little theorem", 1905) *Orice corp finit este comutativ.*

Proof. Fie K un corp finit. Definim $C = \{x \in K : ax = xa \text{ pentru orice } a \in K\}$, *centrul lui K*. Este imediat că C este subcorp comutativ al lui K, deci $\operatorname{char} C = p > 0$. Atunci $|C| = p^m$, unde $m = [C : \mathbb{Z}/p\mathbb{Z}]$ şi $|K| = q^n$, unde $q = p^m$ şi $n = [K : C]$.

Presupunem $n > 1$. Fie $\alpha \in K^\times$ şi $C(\alpha) = \{x \in K : x\alpha = \alpha x\}$. Avem că $C(\alpha)$ este subcorp (nu neapărat comutativ) al lui K şi $C \subseteq C(\alpha)$. Să mai observăm că $C^\times$ este centrul grupului $K^\times$ iar $C(\alpha)^\times = \{x \in K^\times : x\alpha = \alpha x\}$ este centralizatorul lui α în $K^\times$. Mai mult, $|C(\alpha)| = q^{d(\alpha)}$ cu $d(\alpha) \mid n$. (Să notăm că $d(\alpha) = n \Leftrightarrow \alpha \in C^\times$.) Din ecuaţia claselor de conjugare (9.2) în $K^\times$ se obţine:

$$q^n - 1 = q - 1 + \sum_{\alpha \notin C^\times} \frac{q^n - 1}{q^{d(\alpha)} - 1}.$$

Dar $\Phi_n(X) \mid X^n - 1 \Rightarrow \Phi_n(q) \mid q^n - 1$ iar $\Phi_n(X) \mid \dfrac{X^n - 1}{X^{d(\alpha)} - 1} \Rightarrow \Phi_n(q) \mid \dfrac{q^n - 1}{q^{d(\alpha)} - 1}$ şi folosind ecuaţia claselor deducem că $\Phi_n(q) \mid q - 1$. Dar din lema 9.19 ştim că pentru $n \geq 2$ avem $|\Phi_n(q)| > q - 1$, contradicţie. □

10. Corpuri finite.

Deoarece orice corp finit este comutativ putem aplica rezultatele obţinute anterior în studiul acestora. Să începem prin a observa că un corp finit nu poate fi corp algebric închis.

Propoziţia 10.1. *Fie K un corp finit. Atunci K nu este algebric închis.*

Proof. Scriem $K = \{a_1, \ldots, a_n\}$ şi considerăm polinomul $f(X) = (X - a_1) \cdots (X - a_n) + 1$. Este evident că $f \in K[X]$ şi f nu are rădăcini în K. □

Să mai observăm că dacă K este un corp finit, atunci $\operatorname{char} K = p > 0$.

Propoziţia 10.2. *Dacă K este un corp finit, atunci există $p > 0$ un număr prim şi $n \in \mathbb{N}$, $n \geq 1$ astfel încât $|K| = p^n$.*

Proof. Fie $\operatorname{char} K = p > 0$. De aici rezultă că K este extindere finită a lui $\mathbb{Z}/p\mathbb{Z}$. Fie $n = [K : \mathbb{Z}/p\mathbb{Z}]$. În particular, K este $\mathbb{Z}/p\mathbb{Z}$-spaţiu vectorial de dimensiune n, deci $|K| = p^n$. □

Aşadar corpurile finite au ca număr de elemente o putere a unui număr prim. (Nu există un corp finit cu 6 elemente, de exemplu.)

Următoarea întrebare ar fi dacă există un corp finit cu p^n elemente pentru orice număr prim $p > 0$ şi orice număr natural $n \geq 1$. Un astfel de corp trebuie să fie o extindere de grad n a lui $\mathbb{Z}/p\mathbb{Z}$. Am văzut că dacă $f \in (\mathbb{Z}/p\mathbb{Z})[X]$ este un polinom ireductibil de grad n, atunci $(\mathbb{Z}/p\mathbb{Z})[X]/(f)$ este un corp cu p^n elemente, dar nu este clar că pentru orice $n \geq 1$ putem găsi un polinom ireductibil de grad n în $(\mathbb{Z}/p\mathbb{Z})[X]$.

Propoziţia 10.3. *Fie K un corp, $p > 0$ un număr prim şi $n \in \mathbb{N}$, $n \geq 1$. Atunci K este corp finit cu p^n elemente dacă şi numai dacă K este corp de descompunere al polinomului $X^{p^n} - X$ peste $\mathbb{Z}/p\mathbb{Z}$.*

Proof. "$\Rightarrow$" Deoarece $|K| = p^n$ avem $|K^\times| = p^n - 1$ şi $a^{p^n-1} = 1$ pentru orice $a \in K^\times$, deci $a^{p^n} = a$ pentru orice $a \in K$. De aici deducem că polinomul $X^{p^n} - X \in (\mathbb{Z}/p\mathbb{Z})[X]$ are p^n rădăcini distincte în K, deci mulţimea rădăcinilor sale coincide cu K. Aşadar $(\mathbb{Z}/p\mathbb{Z})(K) = K$ este corp de descompunere al lui $X^{p^n} - X$ peste $\mathbb{Z}/p\mathbb{Z}$.
"$\Leftarrow$" Putem considera $K \subset \overline{\mathbb{Z}/p\mathbb{Z}}$. Observăm că derivata polinomului $f(X) = X^{p^n} - X$ este -1, deci $(f, f') = 1$ şi din corolarul 8.4 concluzionăm că f nu are rădăcini multiple. Fie $L = \{\alpha \in \overline{\mathbb{Z}/p\mathbb{Z}} : f(\alpha) = 0\}$. Se arată uşor că L este un subcorp al lui $\overline{\mathbb{Z}/p\mathbb{Z}}$ cu p^n elemente. Dar $K = (\mathbb{Z}/p\mathbb{Z})(L) = L$, deci $|K| = p^n$. □

Corolarul 10.4. *Fie $p > 0$ un număr prim şi $n \in \mathbb{N}$, $n \geq 1$.*
(i) Există un corp finit cu p^n elemente (notat $\mathbb{F}_{p^n}$).
(ii) Orice două corpuri finite cu acelaşi număr de elemente sunt izomorfe.

Putem, de asemenea, descrie complet subcorpurile unui corp finit.

Propoziţia 10.5. *Fie $\mathbb{F}_{p^n}$ corpul finit cu p^n elemente, unde $p > 0$ este un număr prim şi $n \in \mathbb{N}$, $n \geq 1$. Orice subcorp al lui $\mathbb{F}_{p^n}$ are p^m elemente, unde $m \mid n$. Reciproc, dacă $m \mid n$ există un unic subcorp al lui $\mathbb{F}_{p^n}$ cu p^m elemente.*

Proof. Fie K un subcorp al lui $\mathbb{F}_{p^n}$. Avem următorul şir de extinderi de corpuri: $\mathbb{F}_p \subset K \subset \mathbb{F}_{p^n}$. Fie $m = [K : \mathbb{F}_p]$. Deducem că $|K| = p^m$ şi $m \mid [\mathbb{F}_{p^n} : \mathbb{F}_p] = n$.

Reciproc, dacă $m \mid n$ atunci $p^m - 1 \mid p^n - 1$, deci $X^{p^m-1} - 1 \mid X^{p^n-1} - 1$ în $\mathbb{F}_p[X]$ şi de aici obţinem că $X^{p^m} - X \mid X^{p^n} - X$ în $\mathbb{F}_p[X]$. Aceasta ne arată că orice rădăcină a lui $X^{p^m} - X$ este rădăcină a lui $X^{p^n} - X$, deci aparţine lui $\mathbb{F}_{p^n}$. Aşadar $\mathbb{F}_{p^n}$ conţine un corp de descompunere al lui $X^{p^m} - X$ peste $\mathbb{F}_p$. Din propoziţia 10.3 ştim că un astfel de corp de descompunere este corp finit cu p^m elemente.
Dacă ar exista două subcorpuri ale lui $\mathbb{F}_{p^n}$ cu p^m elemente, atunci polinomul $X^{p^m} - X$ ar avea mai mult de p^m rădăcini în $\mathbb{F}_{p^n}$, contradicţie. □

Exerciţiul 10.6. Arătaţi că:
(i) $\mathbb{F}_{p^m} \cap \mathbb{F}_{p^n} = \mathbb{F}_{p^d}$, unde $d = (m, n)$.
(ii) $\mathbb{F}_{p^m}\mathbb{F}_{p^n} = \mathbb{F}_{p^l}$, unde $l = [m, n]$.

Propoziţia 10.7. *Fie K un corp finit şi $n \in \mathbb{N}$, $n \geq 1$. Există o extindere finită de grad n a lui K şi orice două astfel de extinderi sunt K-izomorfe.*

Proof. Fie $K = \mathbb{F}_q$ cu $q = p^r$ şi L corp de descompunere al lui $X^{q^n} - X$ peste K. L este corp de descompunere al lui $X^{p^{nr}} - X$ peste K, deci este corp de descompunere al lui $X^{p^{nr}} - X$ peste $\mathbb{F}_p$. Rezultă că $|L| = p^{nr} = q^n$ şi $[F : K] = n$.
Dacă L' este o altă extindere de grad n a lui K rezultă că $|L'| = q^n = p^{nr}$, deci L' este corp de descompunere al lui $X^{p^{nr}} - X$ peste K şi în consecinţă este K-izomorf cu L. □

Corolarul 10.8. *Fie $p > 0$ un număr prim şi $\mathbb{F}_{p^\infty} = \bigcup_{n \geq 1} \mathbb{F}_{p^{n!}}$. Corpul $\mathbb{F}_{p^\infty}$ este închidere algebrică a lui $\mathbb{F}_{p^m}$ pentru orice $m \geq 1$.*

Proof. Deoarece $\mathbb{F}_{p^{1!}} \subset \mathbb{F}_{p^{2!}} \subset \cdots \subset \mathbb{F}_{p^{n!}} \subset \cdots$ rezultă imediat că $\mathbb{F}_{p^\infty}$ este corp. Cum $m \mid m!$ deducem şi că $\mathbb{F}_{p^m} \subset \mathbb{F}_{p^{m!}}$.

Fie $f \in \mathbb{F}_{p^\infty}[X]$ cu $\deg f \geq 1$. Există $n \geq 1$ cu proprietatea că $f \in \mathbb{F}_{p^{n!}}[X]$. Corpul de descompunere al lui f peste $\mathbb{F}_{p^{n!}}$ este o extindere finită a lui $\mathbb{F}_{p^{n!}}$, deci este un corp finit conţinut în $\mathbb{F}_{p^\infty}$. A rezultat că $\mathbb{F}_{p^\infty}$ este corp algebric închis. Este imediat că extinderea $\mathbb{F}_{p^m} \subset \mathbb{F}_{p^\infty}$ este algebrică, aşadar $\mathbb{F}_{p^\infty}$ este închidere algebrică al lui $\mathbb{F}_{p^m}$. □

Reamintim acum că dacă K este un corp finit atunci $K^\times$ este grup ciclic (vezi lema 9.1).

Propoziţia 10.9. *Orice extindere finită de corpuri finite este simplă.*

Proof. Fie $K \subset L$ o extindere finită de corpuri finite şi $\alpha \in L$ un generator al grupului $L^\times$. Avem $K(\alpha) \subseteq L$. Pe de altă parte, $K(\alpha)$ îl conţine pe 0 şi toate puterile lui α, deci conţine toate elementele lui L. Rezultă $L = K(\alpha)$. □

Corolarul 10.10. *Fie K un corp finit şi $n \in \mathbb{N}$, $n \geq 1$. Atunci există $f \in K[X]$ polinom ireductibil de grad n.*

Proof. Fie $K \subset L$ o extindere de grad n (vezi propoziţia 10.7). Aceasta este simplă (vezi propoziţia 10.9) şi fie $\alpha \in L$ astfel încât $L = K(\alpha)$. Polinomul $f = \mathrm{Irr}(\alpha, K)$ este un polinom ireductibil de grad n. □

Demonstraţia de mai sus ne arată că orice generator al lui $L^\times$ dă naştere unui polinom ireductibil şi este rădăcină a acestuia. Reciproc nu mai este adevărat: un polinom ireductibil dă naştere unei extinderi finite L, dar nu rezultă că rădăcinile sale sunt generatori ai grupului $L^\times$. De exemplu, $f = X^2 + 1 \in \mathbb{F}_3[X]$ este polinom ireductibil şi fie α este o rădăcină a lui f. Atunci $L = \mathbb{F}_3(\alpha)$ este un corp finit cu 9 elemente (extindere de grad 2 a lui $\mathbb{F}_3$), dar $\alpha^4 = 1$.

11. Polinoame ireductibile peste corpuri finite.

În cele ce urmează vom nota prin $\mathbb{F}_q$ corpul finit cu q elemente, unde q este o putere a unui număr prim.

Vom începe prin a determina rădăcinile polinoamelor ireductibile peste corpuri finite.

Lema 11.1. *Fie $f \in \mathbb{F}_q[X]$ un polinom ireductibil de grad m. Atunci $f \mid X^{q^n} - X$ dacă şi numai dacă $m \mid n$.*

Proof. "$\Rightarrow$" Fie α o rădăcină a lui f (în $\overline{\mathbb{F}}_q$). Deoarece $f \mid X^{q^n} - X$ vom avea $\alpha^{q^n} = \alpha$, deci $\alpha \in \mathbb{F}_{q^n}$ şi $\mathbb{F}_q(\alpha) \subset \mathbb{F}_{q^n}$. Cum $m = [\mathbb{F}_q(\alpha) : \mathbb{F}_q]$ şi $n = [\mathbb{F}_{q^n} : \mathbb{F}_q]$ rezultă $m \mid n$.
"$\Leftarrow$" Din propoziţia 10.5 ştim că $\mathbb{F}_{q^n}$ îl conţine pe $\mathbb{F}_{q^m}$ ca subcorp. Fie α o rădăcină a lui f (în $\overline{\mathbb{F}}_q$). Cum $[\mathbb{F}_q(\alpha) : \mathbb{F}_q] = m$ avem că $\mathbb{F}_q(\alpha) = \mathbb{F}_{q^m}$. Rezultă că $\alpha \in \mathbb{F}_{q^n}$, deci $\alpha^{p^n} = \alpha$, adică α este rădăcină a polinomului $X^{q^n} - X \in \mathbb{F}_q[X]$ şi deoarece f este ireductibil avem că $f \mid X^{q^n} - X$. □

Propoziţia 11.2. *Dacă $f \in \mathbb{F}_q[X]$ este un polinom ireductibil de grad m, atunci f are o rădăcină $\alpha \in \mathbb{F}_{q^m}$. Mai mult, toate rădăcinile lui f sunt simple şi coincid cu unul dintre elementele $\alpha, \alpha^q, \ldots, \alpha^{q^{m-1}}$ din $\mathbb{F}_{q^m}$.*

Proof. Fie α o rădăcină a lui f (în $\overline{\mathbb{F}}_q$). Cum $[\mathbb{F}_q(\alpha) : \mathbb{F}_q] = m$ avem că $\mathbb{F}_q(\alpha) = \mathbb{F}_{q^m}$. Să observăm acum că dacă $\beta \in \mathbb{F}_{q^m}$ este rădăcină a lui f, atunci şi β^q este de asemenea rădăcină a lui f. Scriem $f = a_0 + a_1X + \cdots + a_mX^m$ cu $a_i \in \mathbb{F}_q$ şi obţinem $f(\beta^q) = a_0 + a_1\beta^q + \cdots + a_m\beta^{qm} = a_0^q + a_1^q\beta^q + \cdots + a_m^q\beta^{mq} = (a_0 + a_1\beta + \cdots + a_m\beta^m)^q = f(\beta)^q = 0$. Aşadar elementele $\alpha, \alpha^q, \ldots, \alpha^{q^{m-1}}$ sunt rădăcini ale lui f.

Acum mai trebuie ca să verificăm că acestea sunt distincte. Presupunem că nu ar fi, deci $\alpha^{q^i} = \alpha^{q^j}$ cu $0 \leq i < j \leq m-1$. Ridicând egalitatea $\alpha^{q^i} = \alpha^{q^j}$ la puterea q^{m-j} obţinem $\alpha^{q^{m+i-j}} = \alpha^{q^m} = \alpha$ şi de aici $f \mid X^{q^{m+i-j}} - X$. Dar lema 11.1 ne spune că aceasta se întâmplă dacă şi numai dacă $m \mid m + i - j$, ceea ce este fals pentru că $0 < m + i - j < m$. □

Corolarul 11.3. *Fie $f \in \mathbb{F}_q[X]$ un polinom ireductibil de grad m. Atunci corpul de descompunere al lui f peste $\mathbb{F}_q$ este $\mathbb{F}_{q^m}$.*

Proof. Din propoziţia 11.2 ştim că rădăcinile lui f sunt $\alpha, \alpha^q, \ldots, \alpha^{q^{m-1}}$ şi $\mathbb{F}_q(\alpha) = \mathbb{F}_{q^m}$, deci corpul de descompunere al lui f peste $\mathbb{F}_q$ este $\mathbb{F}_{q^m}$. □

Corolarul 11.4. *Orice două polinoame ireductibile peste $\mathbb{F}_q$ de acelaşi grad au acelaşi corp de descompunere.*

Propoziţia 11.5. *Fie $n \in \mathbb{N}$, $n \geq 1$. Produsul tuturor polinoamelor monice şi ireductibile peste $\mathbb{F}_q$ al căror grad îl divide pe n este $X^{q^n} - X$.*

Proof. Din lema 11.1 ştim că dacă un polinom monic şi ireductibil peste $\mathbb{F}_q$ apare în descompunerea lui $X^{q^n} - X$, atunci gradul său îl divide pe n. Cum însă polinomul $X^{q^n} - X$ nu are rădăcini multiple, orice polinom monic şi ireductibil peste $\mathbb{F}_q$ al cărui grad îl divide pe n apare în descompunerea lui $X^{q^n} - X$ o singură dată. □

Exemplul 11.6. Fie $q = n = 2$. Polinoamele monice şi ireductibile din $\mathbb{F}_2[X]$ al căror grad îl divide pe 2 sunt $X, X + 1, X^2 + X + 1$. Este uşor de verificat că $X(X + 1)(X^2 + X + 1) = X^{2^2} - X$.

Exerciţiul 11.7. Descompuneţi în factori ireductibili polinomul $X^{15} + 1 \in \mathbb{F}_2[X]$.

Exerciţiul 11.8. (i) Fie $f \in \mathbb{F}_q[X]$ polinom ireductibil. Arătaţi că f rămâne ireductibil în $\mathbb{F}_{q^n}[X]$ dacă şi numai dacă $(\deg f, n) = 1$.
(ii) Descompuneţi polinomul $X^7 + 1 \in \mathbb{F}_4[X]$ în factori ireductibili.

În cele ce urmează notăm cu $N_q(d)$ numărul polinoamelor monice şi ireductibile peste $\mathbb{F}_q$ care au gradul d.

Corolarul 11.9.

$$q^n = \sum_{d|n} dN_q(d)$$

Proof. Rezultă din propoziţia 11.5 comparând gradul lui $X^{q^n} - X$ cu gradul obţinut din descompunerea acestuia în produs de polinoame monice şi ireductibile. □

Acest corolar ne va permite să obţinem o formulă explicită pentru numărul polinoamelor monice şi ireductibile peste $\mathbb{F}_q$ de un grad dat. Pentru aceasta avem nevoie de o funcţie aritmetică numită *funcţia lui Möbius*.

Definiţia 11.10. *Fie* $\mu : \mathbb{N}^* \to \mathbb{N}^*$ *definită astfel:*

$$\mu(n) = \begin{cases} 1 & \text{dacă } n = 1, \\ (-1)^k & \text{dacă } n \text{ este produs de } k \text{ numere prime distincte}, \\ 0 & \text{dacă } n \text{ se divide cu pătratul unui număr prim.} \end{cases}$$

μ *se numeşte* funcţia lui Möbius.

Exemplul 11.11. $\mu(5) = -1$, $\mu(35) = 1$, $\mu(50) = 0$.

Exerciţiul 11.12. Arătaţi că $\mu(n)$ coincide cu suma rădăcinilor primitive de ordin n ale unităţii.

Lema 11.13. *Funcţia lui Möbius satisface relaţia*

$$\sum_{d|n} \mu(d) = \begin{cases} 1 & \text{dacă } n = 1, \\ 0 & \text{dacă } n > 1. \end{cases}$$

Proof. Pentru $n > 1$ este suficient să considerăm divizorii d ai lui n pentru care $\mu(d) \neq 0$, adică $d = 1$ sau d liber de pătrate. Dacă $p_1, \ldots, p_r$ sunt divizorii primi distincţi ai lui n, atunci

$$\begin{aligned} \sum_{d|n} \mu(d) &= \mu(1) + \sum_{i=1}^{r} \mu(p_i) + \sum_{1 \leq i_1 < i_2 \leq r} \mu(p_{i_1} p_{i_2}) + \cdots + \mu(p_1 \cdots p_r) \\ &= 1 + (-1)\binom{r}{1} + (-1)^2\binom{r}{2} + \cdots + (-1)^r\binom{r}{r} \\ &= (1 + (-1))^r \\ &= 0. \end{aligned}$$

Cazul $n = 1$ este imediat. □

Teorema 11.14. (Formula de Inversiune a lui Möbius)
(i) (Varianta aditivă) *Fie* $(G, +)$ *un grup abelian şi* $h, H : \mathbb{N}^* \to G$ *două funcţii. Atunci*

$$H(n) = \sum_{d|n} h(d) \text{ pentru orice } n \in \mathbb{N}^*$$

dacă şi numai dacă

$$h(n) = \sum_{d|n} \mu(\frac{n}{d})H(d) = \sum_{d|n} \mu(d)H(\frac{n}{d}) \text{ pentru orice } n \in \mathbb{N}^*.$$

(ii) (Varianta multiplicativă) *Fie* $(G, \cdot)$ *un grup abelian şi* $h, H : \mathbb{N}^* \to G$ *două funcţii. Atunci*

$$H(n) = \prod_{d|n} h(d) \text{ pentru orice } n \in \mathbb{N}^*$$

dacă şi numai dacă

$$h(n) = \prod_{d|n} \mu(\frac{n}{d})H(d) = \prod_{d|n} \mu(d)H(\frac{n}{d}) \text{ pentru orice } n \in \mathbb{N}^*.$$

Proof. (i) "⇒" Egalitatea

$$\sum_{d|n} \mu(\frac{n}{d})H(d) = \sum_{d|n} \mu(d)H(\frac{n}{d})$$

este imediată, deoarece $\{d : d \mid n\} = \{\frac{n}{d} : d \mid n\}$.

Din ipoteză

$$\sum_{d|n} \mu(d)H(\frac{n}{d}) = \sum_{d|n} \mu(d) \sum_{c|\frac{n}{d}} h(c).$$

Din $c \mid \frac{n}{d}$ rezultă $c \mid n$ şi $d \mid \frac{n}{c}$. Reciproc, dacă $c \mid n$ iar $d \mid \frac{n}{c}$, atunci $d \mid n$ şi $c \mid \frac{n}{d}$. Aşadar

$$\sum_{d|n} \mu(d) \sum_{c|\frac{n}{d}} h(c) = \sum_{c|n} \sum_{d|\frac{n}{c}} \mu(d)h(c) = \sum_{c|n} h(c) \sum_{d|\frac{n}{c}} \mu(d).$$

Folosind lemma 11.13 obţinem

$$\sum_{d|\frac{n}{c}} \mu(d) = \begin{cases} 1 & \text{dacă } c = n, \\ 0 & \text{dacă } c < n \end{cases}$$

ceea ce conduce la

$$\sum_{c|n} h(c) \sum_{d|\frac{n}{c}} \mu(d) = h(n).$$

Celelalte implicaţii se demonstrează în mod asemănător. □

Aplicând formula de inversiune a lui Möbius obţinem

Teorema 11.15. *Numărul* $N_q(n)$ *al polinoamelor monice şi ireductibile din* $\mathbb{F}_q[X]$ *care au gradul* n *este*

$$N_q(n) = \frac{1}{n} \sum_{d|n} \mu(\frac{n}{d})q^d = \frac{1}{n} \sum_{d|n} \mu(d)q^{\frac{n}{d}}. \tag{11.1}$$

Proof. Fie $G = (\mathbb{Z}, +)$, $h(n) = nN_q(n)$ şi $H(n) = q^n$. Din corolarul 11.9 şi din varianta aditivă a formulei de inversiune a lui Möbius se obţine relaţia din enunţ. □

Exemplul 11.16. Numărul polinoamelor monice şi ireductibile din $\mathbb{F}_q[X]$ care au gradul 6 este

$$N_q(6) = \frac{1}{6}\left(\mu(1)q^6 + \mu(2)q^3 + \mu(3)q^2 + \mu(6)q\right) = \frac{1}{6}(q^6 - q^3 - q^2 + q).$$

Remarca 11.17. Relaţia (11.1) ne dă o demonstraţie alternativă a corolarului 10.10. Deoarece $\mu(1) = 1$ şi $\mu(d) \geq -1$ pentru orice $d \in \mathbb{N}^*$, rezultă

$$N_q(n) \geq \frac{1}{n}(q^n - q^{n-1} - \cdots - q) = \frac{1}{n}(q^n - \frac{q^n - q}{q-1}) > 0.$$

Corolarul 11.18. *Dacă $p_1, \ldots, p_r$ sunt divizorii primi distincţi ai lui n, atunci relaţia* (11.1) *se mai poate scrie astfel:*

$$N_q(n) = \frac{q^n - \sum_{i=1}^{r} q^{\frac{n}{p_i}} + \sum_{1 \leq i_1 < i_2 \leq r} q^{\frac{n}{p_{i_1} p_{i_2}}} - \cdots + (-1)^r q}{n}. \tag{11.2}$$

Exemplul 11.19. (i) Dacă n este număr prim, atunci $N_q(n) = \dfrac{q^n - q}{n}$.
În particular, pentru $n = q = 2$ găsim că $N_2(2) = 1$, deci avem un singur polinom (monic) ireductibil de grad 2 peste $\mathbb{F}_2$ iar acesta este $X^2 + X + 1$.
Pentru $q = 2$ şi $n = 3$ avem $N_2(3) = 2$. Cele două polinoame (monice) ireductibile de grad 3 peste $\mathbb{F}_2$ sunt $X^3 + X + 1$ şi $X^3 + X^2 + 1$.
(ii) Dacă $n = p^2$ cu p număr prim, atunci $N_q(n) = \dfrac{q^{p^2} - q^p}{p^2}$.
În particular, dacă $q = 2$ şi $n = 4$ găsim că $N_2(4) = 3$. Cele trei polinoame (monice) ireductibile de grad 4 peste $\mathbb{F}_2$ sunt X^4+X+1, X^4+X^3+1 şi $X^4+X^3+X^2+X+1$.
(ii) Dacă $n = p_1p_2$ cu p_1, p_2 prime distincte, atunci $N_q(n) = \dfrac{q^{p_1p_2} - q^{p_1} - q^{p_2} + q}{p_1p_2}$.

În relaţia (11.1) am determinat *numărul* polinoamelor monice şi ireductibile din $\mathbb{F}_q[X]$ de un grad dat. Acum vom prezenta o formulă pentru *produsul* polinoamelor monice şi ireductibile din $\mathbb{F}_q[X]$ de un grad dat.

Teorema 11.20. *Fie $I(q, n; X)$ produsul tuturor polinoamelor monice şi ireductibile din $\mathbb{F}_q[X]$ de grad n. Avem*

$$I(q, n; X) = \prod_{d|n} (X^{q^d} - X)^{\mu(\frac{n}{d})} = \prod_{d|n} (X^{q^{\frac{n}{d}}} - X)^{\mu(d)}. \tag{11.3}$$

Proof. Din propoziţia 11.5 deducem că

$$X^{q^n} - X = \prod_{d|n} I(q, d; X).$$

Acum nu avem decât să aplicăm formula de inversiune a lui Möbius, varianta multiplicativă, pentru $G = \mathbb{F}_q(X)^\times$, $h(n) = I(q, n; X)$ şi $H(n) = X^{q^n} - X$. □

Exemplul 11.21. Fie $q = 2$ şi $n = 4$. Produsul polinoamelor (monice) ireductibile de grad 4 din $\mathbb{F}_2[X]$ este

$$I(2, 4; X) = (X^{16} - X)^{\mu(1)}(X^4 - X)^{\mu(2)}(X^2 - X)^{\mu(4)} = \frac{X^{16} - X}{X^4 - X} = \frac{X^{15} - 1}{X^3 - 1}$$

$$= X^{12} + X^9 + X^6 + X^3 + 1.$$

O altă aplicaţie utilă a formulei de inversiune a lui Möbius este o formulă explicită de calcul pentru polinoamele ciclotomice.

Teorema 11.22. *Fie K un corp şi $n \in \mathbb{N}$, $n \geq 1$. Presupunem* $\operatorname{char} K = 0$ *sau* $\operatorname{char} K = p > 0$ *şi* $(p, n) = 1$. *Atunci*

$$\Phi_n(X) = \prod_{d|n} (X^d - 1)^{\mu(\frac{n}{d})} = \prod_{d|n} (X^{\frac{n}{d}} - 1)^{\mu(d)}. \tag{11.4}$$

Proof. Aplicăm formula de inversiune a lui Möbius, varianta multiplicativă, pentru $G = \mathbb{K}(X)^\times$, $h(n) = \Phi_n(X)$ şi $H(n) = X^n - 1$. □

Exemplul 11.23. Fie $K = \mathbb{Q}$. Avem

$$\Phi_6(X) = (X^6 - 1)^{\mu(1)} (X^3 - 1)^{\mu(2)} (X^2 - 1)^{\mu(3)} (X - 1)^{\mu(6)} = \frac{(X^6 - 1)(X - 1)}{(X^3 - 1)(X^2 - 1)}$$
$$= X^2 - X + 1.$$