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.*

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 dat de

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 $f = X - a \in K[X]$.

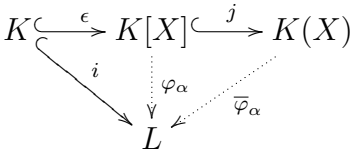
Exemplul 3.10. (i) Considerăm extinderea $\mathbb{Q} \subset \mathbb{R}$. Numărul $\sqrt{2}$ este algebric peste $\mathbb{Q}$, fiind rădăcină a polinomului $f = X^2 - 2 \in \mathbb{Q}[X]$. Pe de altă parte, π este transcendent peste $\mathbb{Q}$.
(ii) Extinderea $\mathbb{Q} \subset \mathbb{R}$ este transcendentă.
(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.*

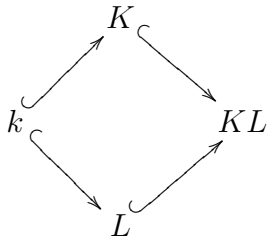
Proof. "⇒" Evident.
"⇐" Fie $\alpha \in L$. Atunci α este algebric peste K, deci există $f \in K[X]$, $f \neq 0$ cu $f(\alpha) = 0$. Scriem $f = a_0 + a_1X + \cdots + a_{n-1}X^{n-1} + X^n$, $a_i \in K$ şi observăm că α este algebric peste $k(a_0, a_1, \ldots, a_{n-1})$. Dar extinderea $k \subset k(a_0, a_1, \ldots, a_{n-1})$ 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. □

Propoziţia 4.4. *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. □

Propoziţia 4.5. *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 4.6. *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 4.7. (a) $\sqrt{2} + \sqrt[15]{7} + \sqrt[3]{2 + \sqrt[5]{4}}$ este algebric peste $\mathbb{Q}$.
(b) $e + \sqrt{3}$ este transcendent peste $\mathbb{Q}$.

Remarca 4.8. (a) O extindere algebrică nu este neapărat finită după cum arată următorul exemplu: $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}, \sqrt[3]{2}, \ldots, \sqrt[n]{2}, \ldots)$.
(b) O extindere de tip finit nu este neapărat finită după cum arată următorul exemplu: $\mathbb{Q} \subset \mathbb{Q}(X)$.

Teorema 4.9. (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 4.10. (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 4.11. 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 $\mathbb{C}$, 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 $f_1, \ldots, f_m \in K[X_1, \ldots, X_n]$. Dacă $(f_1, \ldots, f_m) \neq K[X_1, \ldots, X_n]$, atunci există $(\alpha_1, \ldots, \alpha_n) \in K^n$ astfel încât $f_i(\alpha_1, \ldots, \alpha_n) = 0$ pentru orice $i = 1, \ldots, m$.

Proof. Fie M un ideal maximal în $K[X_1, \ldots, X_n]$. Atunci $K[X_1, \ldots, X_n]/M$ 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 $K = K[X_1, \ldots, X_n]/M$. Dacă α_i este imaginea lui X_i mod M în K, atunci $X_i - \alpha_i \in M$, deci $(X_1 - \alpha_1, \ldots, X_n - \alpha_n) \subseteq M$. Dar $(X_1 - \alpha_1, \ldots, X_n - \alpha_n)$ este ideal maximal în $K[X_1, \ldots, X_n]$, aşadar $(X_1 - \alpha_1, \ldots, X_n - \alpha_n) = M$.
Deoarece $(f_1, \ldots, f_m)$ este ideal propriu acesta este conţinut într-un ideal maximal, deci există $(\alpha_1, \ldots, \alpha_n) \in K^n$ cu proprietatea că $(f_1, \ldots, f_m) \subseteq (X_1 - \alpha_1, \ldots, X_n - \alpha_n)$. De aici rezultă că $f_i(\alpha_1, \ldots, \alpha_n) = 0$ pentru orice $i = 1, \ldots, m$. □