Rezolvarea ecuaţiilor algebrice prin radicali

Nicolae Claudius

2008

Cuprins

Rezumat

Lucrarea tratează abstract problema rezolvării ecuaţiilor polinomiale prin radicali.

Fiind dat un polinom $f(x) \in K[X]$ locul natural de căutare a rădăcinilor sale este corpul K şi extinderile acestuia.

În prima parte încercăm să înţelegem extinderile de corpuri. Avem în vedere noţiunile de extindere algebrică, normală, separabilă, corp de descompunere al unui polinom, închideri algebrice şi normale. Demonstrăm existenţa corpului de descompunere al unui polinom. Dăm o descriere completa a corpurilor finite. Vedem corespondenţa între o extindere şi corpul de descompunere al unui polinom, dăm un criteriu pentru existenţa rădăcinilor multiple şi unul pentru ireductibilitate. Spre sfîrşit demonstrăm existenţa şi unicitatea (abstracţie de un izomorfism) a închiderilor algebrice.

În a doua parte vorbim despre corespondenţa Galois, corespondenţă care reduce problema rezolvării ecuaţiilor la probleme mai simple din teoria grupurilor. Începem cu automorfismele unei extinderi şi proprietăţile acestora. Introducem noţiunea de grup Galois. Urmează corespondenţa Galois şi consecinţe ale acesteia. Tot aici prezentăm şi teorema fundamentală a algebrei.

În a treia parte abordăm rezolvarea ecuaţiilor prin radicali susţinută de informaţiile construite apriori. Începem prin a observa grupul Galois al polinoamelor $X^n - a$ iar apoi trecem la problema generală. Dăm condiţiile necesare şi suficiente ca o ecuaţie să fie rezolvabilă prin radicali şi metode de rezolvare.

În partea a patra se aplica teoria dezvoltată pentru situaţii practice.

Partea I
Extinderi de corpuri

1 Extinderi de corpuri

1.0.0.1 Definiţie. *Fie L corp şi K subcorp. Spunem că L/K este* ***extindere de corpuri****.*

1.0.0.2 Definiţie. *Dacă M este subcorp al lui L care contine K, spunem că M este* ***corp intermediar****.*

1.0.0.3 Definiţie. *Fie L/K extindere de corpuri. Fie S submulţime a lui L.* ***Subcorpul generat de S****, notat cu $K(S)$, este cel mai mic corp al lui L care contine K şi S.*

Spunem că S ***generează*** *L/K dacă $L = K(S)$. Spunem că L/K este* ***finit generat*** *dacă exista o mulţime finită S care generează L/K. Spunem că L/K este* ***simpla (primitivă)*** *dacă exista un singur element $a \in L$ care generează L/K, $L = K(a)$. În acest caz spunem că a este* ***generator primitiv (simplu)****.*

1.0.0.4 Definiţie. *Fie L corp.* ***Subcorpul prim al lui*** *L este ce mai mic corp care contine* 1*.*

1.0.0.5 Propoziţie. *Fie L corp şi K subcorpul său prim.*

Dacă caracteristica e zero, atunci $K \simeq \mathbb{Q}$. Dacă caracteristica e p, atunci K este izomorf cu $\mathbb{F}_p$.

Demonstraţie. Fie R cel mai mic inel care contine 1. Observam că K este corpul de fracţii al lui R.

Avem doua cazuri. Dacă caracteristica este p, ştim că $R \simeq \mathbb{Z}_p$. Cum acesta este izomorf cu $\mathbb{F}_p$, care este corp, atunci K este izomorf cu $\mathbb{F}_p$.

Altfel caracteristica este zero. În acest caz R este izomorf cu $\mathbb{Z}$. În acest caz corpul de fracţii K al lui R este izomorf cu $\mathbb{Q}$.

1.0.0.6 Definiţie. *Fie L/K extindere de corpuri.* ***Gradul*** *extinderii notat $[L : K]$, este dimensiunea lui L peste K considerat ca spaţiu vectorial peste K.*

Spunem că L/K este ***extindere finită*** *dacă L este un spaţiu vectorial finit dimensional peste K.*

1.0.0.7 Lema. *Fie F un corp finit.*

Atunci ordinul q al lui F este puterea unui număr prim.

Demonstraţie. Fie p caracteristica lui F. $p \neq 0$ deoarece F nu poate contine $\mathbb{Q}$, mulţime infinită. Deci p este prim şi F este extindere a lui $\mathbb{F}_p$. Cum F este finit, extinderea $F/\mathbb{F}_p$ este finită. Dar orice spaţiu vectorial finit dimensional peste $\mathbb{F}_p$ este izomorf pe structura de spaţiu vectorial, cu suma directă de corpuri $\mathbb{F}_p$. În particular cardinalul lui F este egal cu cardinalul produsului cartezian de $\mathbb{F}_p$ de un număr finit de ori, şi cardinalul unui produs este produsul cardinalelor. Deci $q = p^d$ unde d este gradul extinderii $F/\mathbb{F}_p$.

1.0.0.8 Propoziţie (legea turnurilor). *Fie L/K extindere şi M corp intermediar.*

Atunci

$$[L : K] = [L : M][M : K].$$

Demonstraţie. Considerăm întîi posibilitatea ca una din cele doua extinderi L/M sau M/K să fie infinită. În acest caz L ar contine un număr infinit de vectori liniar independenţi peste K şi e clar că şi L/K este infinită.

Altfel presupunem că atât L/M cat şi M/K sunt extinderi finite. Fie $e_1, e_2, ..., e_m$ baza pentru L/M şi $f_1, f_2, ..., f_n$ baza pentru M/K. În acest caz

$$[L : M] = m \quad si \quad [M : K] = n.$$

Este suficient să demonstrăm că $e_i f_j$ pentru $i = 1...m$ şi $j = 1...n$ este o baza pentru $[L : K]$, deoarece atunci

$$[L : K] = mn = [L : M][M : K].$$

Trebuie să demonstrăm că $\{e_i f_j\}$ formează un sistem de generatori şi sunt liniar independenţi.

Fie $l \in L$. Deoarece $e_1, ..., e_m$ este o baza pentru L/M, $\exists a_1, ..., a_m \in M$ astfel încât

$$l = \sum_j a_j e_j.$$

Cum $a_i \in M$ şi $f_1, ..., f_n$ este o baza pentru M/K, pentru fiecare i $\exists b_{ij} \in K$ astfel încât

$$a_i = \sum b_{ij} f_j.$$

De aici rezultă

$$\begin{aligned} l &= \sum_i a_i e_i \\ &= \sum_i \left(\sum_j b_{ij} f_j \right) e_i \\ &= \sum_{i,j} b_{ij} (e_i f_j). \end{aligned}$$

Deci $l$este combinaţie liniară de e_işi f_j peste K deci $e_i f_j$ generează L/K. În ceea ce priveşte independenţa liniară, fie

$$\sum_{i,j} b_{ij} e_i f_j = 0.$$

Trebuie să demonstrăm ca

$$b_{ij} = 0.$$

După o eventuală reordonare avem

$$\sum_i \left(\sum b_{ij} f_j \right) e_i = 0.$$

Fie

$$a_i = \sum_j b_{ij} f_j.$$

Atunci $a_i \in M$ şi

$$\sum_i a_i e_i = 0.$$

Cum $e_1, ..., e_n$ sunt liniar independenţi peste M, rezultă ca

$$\sum_j b_{ij} f_j = a_i = 0.$$

Din independenţa $f_1, ..., f_n$ peste K, obţinem $b_{ij} = 0$ pentru toţi i şi j. Deci $\{e_i f_j\}$ este o baza pentru L/K.

1.0.0.9 Definiţie. *Fie L/K extindere de corpuri şi $a \in K$. Spunem că a este* ***algebric*** *peste K dacă $\exists f(x) \in K[X]$ astfel încât $f(a) = 0$. Polinomul monic de grad minim cu aceasta proprietate se numeşte* ***polinom minimal*** *al lui a peste K şi îl vom nota cu $m_a(x)$.*

Dacă nu exista un astfel de polinom spunem că a este transcendent peste K.

O extindere L/K se numeşte algebrică dacă orice element din L este algebric peste K.

1.0.0.10 Teorema. *e şi π sunt transcendente (peste $\mathbb{Q}$).*

1.0.0.11 Lema. *Fie R un domeniu de integritate în care orice ideal este principal şi I un ideal prim netrivial al sau.*

Atunci R/I este corp.

Demonstraţie. Este suficient să demonstrăm că I este maximal. Fie $I \subset J \subset R$, unde J este un ideal al lui R. Din ipoteza rezultă $I =< a >$ şi $J =< b >$. Cum $a \in J$, b divide a. Cum I este prim rezulta că a este ireductibil, deci b este fie unitatea că z în care $J = R$, sau b asociat în divizibilitate cu a caz în care $J = I$. În ambele cazuri I este maximal.

1.0.0.12 Teorema. *Fie L/K extindere de corpuri şi $a \in L$. Fie $M = K(a)$.*

Dacă a este transcendent peste K, atunci M este izomorf cu corpul de funcţii raţionale din K, adică corpul de fracţii $K(x)$ al $K[X]$. În particular orice doua elemente transcendente generează extinderi izomorfe.

Dacă a este algebric peste K, atunci

$$K(a) = K[a] \simeq K[X]/ < m_a(x) > .$$

În particular orice doua elemente ale lui L cu acelaşi polinom minimal generează extinderi izomorfe.

Demonstraţie. Este clar că $K(a)$ este cel mai mic corp care contine $K[a]$, adică $K(a)$ poate fi identificat cu corpul de fracţii $K[a]$.

Data fiind o extindere L/K şi un element $a \in L$ exista un homomorfism de inele unic

$$\phi = ev_a : K[X] \to L$$

care îl duce pe X în a. Aceasta este o consecinţa a proprietăţii de universalitate a inelelor de polinoame. Nucleul lui ev_a este un ideal I în $K[X]$ care consta în polinoamele $f(x) \in K[X]$ care-l anulează pe a.

Imaginea lui ϕ este evident $K[a]$. Din teorema de izomorfism

$$K[a] \simeq K[X]/I.$$

Cum $K(a)$ este o submulţime a lui L rezultă că $K[a]$ este domeniu de integritate. Atunci I trebuie să fie ideal prim. Dacă a este transcendent atunci I este idealul nul şi avem un izomorfism $K[a] \simeq K[X]$, ceea ce conduce la rezultat.

Fie a algebric deci I netrivial. Cum K este corp, $K[X]$ este domeniu Euclidian, deci $K[X]$ este ideal principal. Deci exista polinomul $f(x) \in K[X]$ astfel încât $I =< f(x) >$. Deoarece K este corp, din moment ce $f(x) \neq 0$, putem întotdeauna sa-l normalizăm pe $f(x)$ astfel încât să fie monic. Este clar că în acest caz $f(x) = m_a(x)$. Cum I este prim, f este ireductibil. Din 1.0.0.11 $K[X]/ < f(x) >$ este corp. Deci $K(a)$ este corp şi prin definiţie $K[a] = K(a)$.

1.0.0.13 Lema. *Fie L/K extindere de corpuri şi a algebric peste K. Atunci polinomul minimal al a divide orice polinom care are a ca rădăcină. În particular un polinom monic care are a ca rădăcină este polinomul minimal al lui a dacă este ireductibil.*

Demonstraţie. În demonstraţia 1.0.0.11 am arătat că polinomul minimal generează idealul tuturor funcţiilor care au a ca *rădăcină* şi faptul că acesta este ideal prim.

1.0.0.14 Corolar. *Fie L/K extindere de corpuri şi $a \in L$ algebric. Fie d gradul polinomului minimal al a.*

Atunci $[K(a) : K] = d$.

Demonstraţie. Este suficient să demonstrăm că $1, a, a^2, ..., a^{d-1}$ formează o baza pentru $K(a)$.

Întîi demonstrăm că sunt sistem de generatori. Fie polinomul minimal

$$X^d + a_{d-1}X^{d-1} + ... + a_0$$

astfel încât

$$(a)^d + a_{d-1}(a)^{d-1} + ... + a_0 = 0.$$

Cum $K(a) = K[a]$ şi ultimul este generat de puterile lui a este suficient să demonstrăm că a^n este combinaţie liniară de $1, a, a^2, ..., a^{d-1}$. Dacă $n < d$ nu avem nimic de demonstrat. Altfel, prin inducţie, e suficient să demonstrăm că a^n este combinaţie liniară de $1, a, a^2, ..., a^{n-1}$. Dar

$$\begin{aligned} a^n &= a^{n-d}a^d \\ &= a^{n-d}(-a_{d-1}a^{d-1} - ...a_0) \\ &= -a_{d-1}a^{n-1} - ...a_0a^{n-d}. \end{aligned}$$

Deci $1, a, a^2, ..., a^{d-1}$ generează $K(a)/K$.

Acum în ceea ce priveşte independenţa liniară, fie

$$\sum b_i a_i = 0.$$

Fie $g(x) = \sum b_i X^i$. atunci a este rădăcină a lui $g(x)$. Cum gradul lui $g(x)$ este mai mic decât gradul lui $m_a(x)$, polinomul minimal al lui a rezultă că $g(x) \equiv 0$. Atunci toţi $b_i = 0$ deci avem liniar independenţă.

Deci $1, a, a^2, ..., a^{d-1}$ formează o baza.

1.0.0.15 Lema. *Fie L/K extindere de corpuri.*

Atunci L/K este finită dacă $L = K(a_1, a_2, ..., a_n)$ unde toţi a_i sunt algebrici peste K. În particular toate elementele lui L sunt algebrice peste K.

Demonstraţie. Consecinţa a celor de mai sus.

1.0.0.16 Lema. *Fie L/K extindere de corpuri. Fie M submulţime a lui L alcătuită din toate elementele lui L algebrice peste K.*

Atunci M este corp intermediar.

Demonstraţie. Fie $a \in K$. Atunci a este rădăcină a polinomului $X - a$. Deci a este algebric peste K şi $K \subset M$.

Observam că $c \in M$ dacă c este algebric peste K dacă $K(x)/K$ este extindere finită.

Fie $a, b \in M$. Este suficient să demonstrăm că $a+b, -a, ab, 1/a$ sunt în M. Toate acestea sunt elemente ale $K(a, b)$. Astfel este suficient să demonstrăm că $K(a, b) \in M$. Cum a şi b sunt în M, $K(a)/K$ şi $K(b)/K$ sunt finite. Deci $K(a, b)/K(b)$ este finită şi din legea turnurilor

$$[K(a, b) : K] = [K(a, b) : K(b)][K(b) : K]$$

rezultă că $K(a,b)/K$ este finită. Fie $c \in K(a,b)$. Atunci din legea turnurilor

$$[K(a,b) : K] = [K(a,b) : K(c)][K(c) : K]$$

deci $K(c)/K$ este finită. Atunci c este algebric peste K şi $c \in M$.
Deci $K(a,b) \in M$ q.e.d.

1.0.0.17 Teorema. *Fie L/K extindere finită de corpuri.*
Atunci L/K este primitivă (simpla) dacă exista numai un număr finit de corpuri intermediare.

Demonstraţie. Fie L/K extindere primitivă. Fie a un generator primitiv astfel încât $L = K(a)$. Fie M corp intermediar. Este clar că $L = M(a)$. Fie $f_M(x)$ polinomul minimal al lui a peste M.

Arătam că $f_M(x)$ determina M. Observam întâi că $f_M(x) \in M[X]$ şi că $f_M(x)$ este monic şi ireductibil. Fie M' subcorpul lui M generat de coeficienţii lui $f_M(x)$. Din definiţia lui M', $f_M(x) \in M'[X]$. Cum $f_{M'}(x)$ este polinomul minimal al lui a peste M', rezultă că $f_{M'}$ divide f_M. Cum f_M este ireductibil în $M[X]$, este cu siguranţa ireductibil şi în $M'[X]$ rezultă că $f_M = f_{M'}$. Deci

$$[L : M] = [L : M']$$

deoarece amândouă sunt egale cu gradul lui f_M. Pe de alta parte

$$[L : K] = [L : M][M : K] = [L : M'][M' : K]$$

din legea turnurilor aplicată atât pentru $L/M/K$ cat şi $L/M'/K$. Astfel

$$[M : K] = [M' : K].$$

Fie extinderile $M/M'/K$. Avem

$$[M/K] = [M : M'][M' : K].$$

Tragem concluzia că $[M : M'] = 1$ deci $M = M'$. Dar evident M' este determinat de f_M deci M este de asemenea determinat de f_M.

Observam că exista un număr finit de posibilităţi pentru alegerea lui f_M. f_M divide f_K în L, deoarece $L[X]$ este factorial, şi factorizarea poate fi făcută într-un număr finit de moduri. Deci numărul de corpuri intermediare este finit.

Vrem să demonstrăm mai departe că L/K este primitivă. Vom demonstra numai în cazul L infinit. Cazul corpurilor finite se va demonstra în 5.

Presupunem prin reducere la absurd că extinderea L/K nu este primitivă. Fie $a \in L$ astfel încât $[K(a) : K]$ este maximală. Din presupunere putem alege $b \in L$ care se afla în $K(a)$. Considerăm corpurile intermediare $K(a+lb)$ unde $l \in K$. Deoarece avem un număr infinit de valori pentru l şi numai un număr finit pentru corpurile intermediare exista $l \neq u \in K$ astfel încât

$$K(a + lb) = K(a + ub) = M.$$

Evident $a + lb$ şi $a + ub \in M$. Astfel

$$(a + lb) - (a + ub) = lb + ub = (l - u)b$$

se afla în K. Cum $l \neq u$ are sens împărţirea la $l - u$, tragem concluzia că $b \in M$. Deci

$$(a - lb) - lb = a \in M.$$

deci a şi $b \in M$. Cum $a \in M$, $K(a) \subset M$. Cum $b \in M$, incluziunea este strictă. Deci gradul lui M peste K este mai mare decât $K(a)$ peste K. Cum $M = K(c)$, pentru $c = a + lb$ obţinem contradicţie. Deci L/K extindere primitivă.

2 Corpul de descompunere al unui polinom

2.0.0.18 Definiţie. *Fie K corp şi $f \in K[X]$. Spunem că f* ***se descompune în*** *K dacă $\exists a_1, a_2, ..., a_n \in K$ astfel încât*

$$f(x) = l(x - a_1)(x - a_2)(x - a_3)...(x - a_n)$$

Spunem că extinderea L/K este ***corpul de descompunere a lui*** *f dacă f se descompune în L şi nu exista nici un corp intermediar M în care f să se descompună.*

2.0.0.19 Lema. *Fie $f \in K[X]$, L/K extindere de corpuri în care f se descompune*

$$f(x) = (x - a_1)(x - a_2)(x - a_3)...(x - a_n)$$

unde $a_1, a_2, a_3 ... a_n \in L$.
Atunci $M = K(a_1, a_2, a_3, ..., a_n)$ *este corpul de descompune al lui* f.
Demonstraţie. Evident.

2.0.0.20 Lema (existenţa). *Fie* $f(x) \in K[X]$ *un polinom.*
Atunci $f(x)$ *are corp de descompunere.*
Demonstraţie. Conform 2.0.0.19 este suficient să găsim o extindere în care f să se descompună. Demonstraţia se face prin inducţie după gradul d al lui f . Dacă $d = 1$ atunci f este un polinom liniar

$$f = ax + b = a(x - \alpha),$$

unde $\alpha = -b/a \in K$ deci K/K este corp de descompunere în acest caz.
Presupunem rezultatul adevărat pentru orice extindere de grad mai mic ca n.
Presupunem că $f(x)$ este ireductibil. Atunci f este de asemenea prim deoarece $K[X]$ este inel factorial. Atunci $< f(x) >$ este ideal prim şi inelul factorial

$$\frac{K[X]}{< f(x) >},$$

este de fapt un corp L extindere a lui K. Mai mult α denota mulţimea factor la stânga (coset) $x+ < f(x) >$, atunci $L = K(\alpha)$, şi α este rădăcină a lui $f(X)$. Astfel putem sa-l factorizăm pe f ca

$$f(x) = (x - \alpha)g(x),$$

unde $g(x) \in L[X]$.
Putem să presupunem ca

$$f(x) = g(x)h(x),$$

unde ambele polinoame $g(x)$şi $h(x)$au gradul cel puţin 1. Continuăm în doi paşi. Întâi găsim o extindere, M/K în care g(x) se descompune. Apoi găsim o extindere L/M în care $h(x)$ se descompune. Este evident că putem face asta deoarece gradurile lui g şi h sunt mai mici ca n. Rezulta că f se descompune în L/K.

Acum că ştim existenţa corpului de descompunere, vrem informaţii asupra unicităţii. Aplicăm acelaşi argument ca mai sus. La pasul de inducţie, în cazul $f(x)$ reductibil, vom avea doua extinderi intermediare M/K şi M'/K. Apoi vrem să argumentăm că L/M şi L'/M' sunt extinderi izomorfe.

2.0.0.21 Definiţie. *Spunem că două extinderi L/K şi L'/K' sunt izomorfe dacă exista izomorfism ele de inele $\psi : L \to L'$ şi $\phi : K \to K'$ astfel încât următoarea diagrama este comutativă*

$$\begin{array}{ccc} L & \xrightarrow[\psi]{} & L' \\ \uparrow & & \uparrow \\ K & \xrightarrow[\phi]{} & K' \end{array}$$

Acest rezultat se poate organiza ca o categorie, aceea a extinderii corpurilor. Obiectele sunt extinderi de corpuri L/K iar morfismele sunt perechi de aplicaţii liniare pe structurile de inel, astfel încât diagrama să fie comutativă.

2.0.0.22 Lema. *Fie L/K o extindere simpla (primitivă). unde $a \in L$, $\phi : K \to K'$ şi extinderea de corpuri L'/K' , $b \in L'$.*

Atunci $\exists \psi : L \to L'$ astfel încât $\psi(a) = b$, dacă b este rădăcina imaginii polinomului minimal al lui a.

Demonstraţie. Prima direcţie este audienţa. Presupunem că exista un astfel de ψ. Atunci

$$\begin{aligned} \phi(m_a)(b) &= \psi(m_a)(\psi(a)) \\ &= \psi(m_a(a)) \\ &= 0. \end{aligned}$$

Presupunem că şi invers este adevărat. Presupunem fără a restrânge generalitatea că $L' = K'(b)$. Atunci

$$L \simeq \frac{K[X]}{< m_a(x) >}$$

şi

$$L' \simeq \frac{K'[X]}{< m_b(x) >}.$$

Dar deoarece b este rădăcină a $\phi(m_a(x))$, rezultă că $m_b(x)$ divide $m_a(x)$.

Definim homomorfismul de inele

$$f : K[X] \to \frac{K'[x]}{< m_b(x) >}$$

ca fiind compunerea homomorfismelor de inele

$$K[X] \to K'[X]$$

a cărui existenţa este garantată de proprietatea de universalitate a inelelor de polinoame şi de proiecţia canonică

$$K'[X] \to \frac{K'[X]}{< m_b(x) >}.$$

Am văzut că $m_a(x) \in Ker(f)$. Avem $< m_a(x) > \subset Ker(f)$. Astfel din proprietatea de universalitate avem aplicaţia indusă

$$\frac{K[X]}{< m_a(x) >} \to \frac{K'[X]}{< m_b(x) >}.$$

Cele doua izomorfisme de mai sus induc homomorfismul de inele

$$\psi : L \to L'$$

care extinde ϕ şi îl duce pe a (corespunzînd lui $x+ < m_a(x) >$) în b.

2.0.0.23 Lema. *Fie $\phi : K \to K'$ homomorfism de inele. Fie $f(x) \in K[X]$ polinom şi fie $f'(x) \in K'[X]$ polinomul corespondent în $K'[X]$. Fie L/K corp de descompunere pentru $f(x)$ şi fie L'/K' un corp în care $f'(x)$ se descompune. Atunci exista morfismul indus (ϕ, ψ), în categoria extinderi lor de corpuri, astfel încât exista homomorfismul de inele $\psi : L \to L'$ astfel încât următoarea diagrama să fie comutativă*

$$\begin{array}{ccc} L & \xrightarrow[\psi]{} & L' \\ \uparrow & & \uparrow \\ K & \xrightarrow[\phi]{} & K' \end{array}$$

Mai mult, dacă ϕ este izomorfism şi L' peste K' este corp de descompunere pentru $f'(x)$, atunci şi ψ este izomorfism.

Demonstraţie. Demonstrăm prin inducţie după gradul n al extinderii de corpuri L/K. Dacă gradul este 1 nu avem nimic de demonstrat pentru că $L = K$ şi putem să luăm $\psi = \phi$.

Presupunem rezultatul adevărat pentru orice extindere de grad mai mic ca n. Alegem o rădăcină $a \in L$ a lui $f(x)$, care nu se afla în K. Fie $m(x)$ polinomul minimal al lui a.Atunci $m(x)$ divide $f(x)$ deoarece a este o rădăcină a lui $f(x)$. Fie $m'(x) \in K'[X]$ polinomul corespunzător lui $m(x)$. Deoarece $f'(x)$ se descompune în L' rezultă că $\exists b \in L'$ rădăcină a lui $m'(x)$. Conform 2.0.0.22 putem să găsim un homomorfism de inele π care sa-l extindă pe ϕ

$$\begin{array}{ccc} K(a) & \xrightarrow[\pi]{} & K'(b) \\ \uparrow & & \uparrow \\ K & \xrightarrow[\phi]{} & K' \end{array}$$

Cum $[K(a) : K] > 1$, conform legii turnurilor rezultă că $[L : K(a)] < [L : K]$. Atunci, prin inducţie, putem găsi ψ exstensie a lui π

$$\begin{array}{ccc} L & \xrightarrow[\psi]{} & L' \\ \uparrow & & \uparrow \\ K(a) & \xrightarrow[\pi]{} & K'(b) \end{array}$$

Cum ψ extinde π şi π extinde ϕ înseamnă că ψ extinde ϕ, aşa cum doream.

Avem L'/K' corp de descompunere pentru $f'(x)$ şi ϕ izomorfism. Cum ψ este homomorfism de inele între cele doua corpuri rezultă ca ψ este injectivă. Rezulta că

$$[L : K] \leq [L' : K'].$$

Înlocuind π cu inversa obţinem prin simetrie

$$[L' : K'] \leq [L : K].$$

Astfel

$$[L : K] = [L' : K'].$$

Cum orice aplicaţie liniară injectivă între doua spaţii vectoriale de aceeaşi dimensiune este bijectivă, rezultă ca ψ este izomorfism.

Folosim acest rezultat pentru a da o descriere completa corpurilor finite.

2.0.0.24 Definiţie. *Fie G grup. Se numeşte **exponentul** lui G c.m.m.m.c al ordinelor elementelor lui G.*

2.0.0.25 Lema *Fie G un grup abelian finit de ordin n.*

Atunci exponentul m al lui G este cea mai mica valoare r astfel încât $g^r = e$ pentru $\forall g \in G$. În particular $m = n$ dacă G este ciclic.

Demonstraţie. Din clasificarea grupurilor abeliene finit generate putem găsi $m_1, m_2, m_3 ... m_k \in \mathbb{Z}$ astfel încât

$$G \simeq \mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \mathbb{Z}_{m_3} \times ... \mathbb{Z}_{m_k},$$

unde m_i divide m_{i+1}. În acest caz este clar ca $m = m_k$.

2.0.0.26 Lema. *Fie G un subgrup finit al grupului multiplicativ al unui corp K.*

Atunci G este ciclic.

Demonstraţie. Fie m exponentul lui G şi n ordinul lui G. G este abelian deoarece K este corp. Astfel $m \leq n$ şi pentru $\forall a \in G$ $a^m = 1$, deci orice element din G este rădăcină a polinomului

$$X^m - 1 \in F[X].$$

Dar un polinom de grad m are cel mult m rădăcini deci $n \leq m$. Atunci $m = n$ şi G este ciclic.

2.0.0.27 Teorema. *Fie L un corp finit de ordinul $q = p^n$.*

Atunci elementele lui L sunt cele q rădăcini ale polinomului $X^q - X \in L[X]$. În particular L este corpul de descompunere al polinomului $X^q - X$. Mai mult $\exists a \in L$ astfel încât $L = \mathbb{F}_p(a)$.

Demonstraţie. Fie G mulţimea elementelor nenule din L. Atunci G este un subgrup finit al grupului multiplicativ. Deci elementele lui G sunt cele $q - 1$ rădăcini ale polinomului

$$X^{q-1} - 1.$$

Deci elementele lui L sunt într-adevăr rădăcinile polinomului

$$X^q - X.$$

Fie a un generator al grupului ciclic G. Atunci $G =< a >$, rezultă $L = \mathbb{F}(a)$.

Acum ne punem întrebarea, data fiind o extindere de corpuri, exista întotdeauna un polinom pentru care extinderea este corp de descompunere?

3 Extinderi normale

3.0.0.28 Definiţie. *Fie L/K extindere de corpuri. Spunem că L/K este* ***normală*** *dacă orice polinom ireductibil $f(x) \in K[X]$ care are o rădăcină în L are toate rădăcinile în L.*

3.0.0.29 Propoziţie. *Fie L/K extindere de corpuri.*

Atunci L/K este extindere normală finită dacă este corpul de descompunere al unui polinom $f(x) \in K[X]$.

Demonstraţie. Fie L/K extindere normală finită. Alegem $a_1, a_2, ..., a_n$ astfel încât

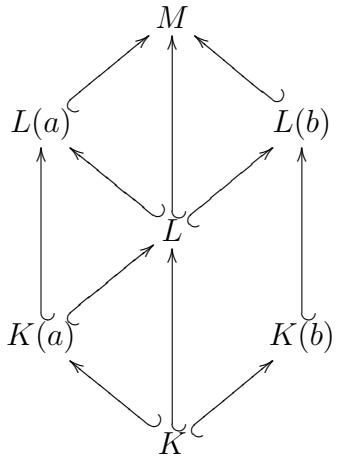
$$L = K(a_1, a_2, ..., a_n).$$

Fie $m_i(x)$ polinomul minimal al a_i. Atunci $m_i(x)$ se descompune peste L deoarece L/K extindere normală. Deci $f(x)$, produsul tuturor polinoamelor $m_i(x)$, se descompune în L/K. Rezulta că L/K corp de descompunere pentru $f(x)$.

Acum fie L/K corpul de descompunere al unui polinom $f(x)$. Alegem un polinom monic $m(x)$ cu o rădăcină $a \in L$ (aşa încât de fapt $m(x)$ este polinomul minimal al lui a peste K). Fie M/L corp de descompunere pentru $m(x) \in L[X]$. Este clar că M/K este corp de descompunere pentru $m(x)$. E de ajuns atunci să demonstrăm că $L = M$.

Alegem orice rădăcină $b \in M$ a lui $m(x)$. Trebuie să demonstrăm că $b \in L$.

Considerăm următoarea latice de incluziuni



Observam întâi că extinderile $K(a)/K$ şi $K(b)/K$ sunt izomorfe deoarece a şi b au acelaşi polinom minimal. Similar extinderile $L(a)/K(a)$ şi $L(b)/K(b)$ sunt izomorfe deoarece amândouă sunt corpuri de descompunere pentru $f(x)$. Rezulta din legea turnurilor ca

$$[L(a) : K] = [L(b) : K].$$

Dar din nou din legea turnurilor

$$[L(a) : K] = [L(a) : L][L : K]$$

şi

$$[L(b) : K] = [L(b) : L][L : K]$$

astfel

$$[L(a) : L] = [L(b) : L].$$

Cum $a \in L$ termenul stâng al regalităţii este 1. Atunci $b \in L$ q.e.d.

3.0.0.30 Lema. (consecinţa a 3.0.0.29) *Fie L/K extindere normală finită şi fie M un corp intermediar.*

Atunci L/M este normală.

Demonstraţie. Din 3.0.0.29 L/K este corpul de descompunere al unu polinom $f(x) \in K[X]$. Dar atunci L/M este corpul de descompunere pentru acelaşi polinom şi din 3.0.0.29 rezultă că L/M extindere normală.

Alternativ, am putea să demonstrăm direct. Fie $a \in L$ rădăcină a lui $f(x) \in M[X]$ un polinom ireductibil. Fie $m(x)$ polinomul minimal al lui a peste K. Atunci $f(x)$ divide $m(x)$ în $M[X]$. Cum $m(x)$ se descompune în L, rezultă că şi $f(x)$ se descompune în L.

3.0.0.31 Definiţie. *Fie L/K extindere de corpuri.*

Se numeşte ***închidere normală*** *pentru L/K un corp N/L astfel încât N/K normală, şi nu exista alte corpuri intermediare între N şi L cu aceasta proprietate.*

3.0.0.32 Lema. *Fie L/K extindere finită.*

Atunci exista o închidere normală pentru L/K şi oricare doua inchideri normale sunt izomorfe peste L.

Demonstraţie. Fie $a_1, a_2...a_n$ generatorii L/K. Fie N/L corpul de descompunere al produsului polinoamelor minimale. Atunci N/L este corpul

de descompunere pentru acelaşi polinom, deci N/K este normală. Este clar că orice alta inchideri normală trebuie să fie corp de descompunere pentru aceleaşi polinoame.

4 Extinderi separabile

4.0.0.33 ***Definiţie.*** *Fie K corp şi $m(x) \in K[X]$ polinom ireductibil.*

Spunem că $m(x)$ este ***separabil*** *dacă nu are rădăcini multiple într-un corp de descompunere. Spunem că un polinom arbitrar este separabil dacă orice factor ireductibil al sau este separabil.*

Spunem că extinderea de corpuri L/K este separabilă dacă polinomul minimal al oricărui element din L este separabil.

4.0.0.34 **Definiţie** *Fie R inel comutativ. Se numeşte* ***derivată formală*** *o funcţie*

$$D : R[X] \to R[X]$$

astfel încât dacă $f(x) \in R[X]$ este de forma

$$f(x) = a_n X^n + a_{n-1} X^{n-1} + ...a_0,$$

atunci $f'(x) = D(f(x))$, derivată formală a lui f este definită ca

$$f'(x) = n a_n X^{n-1} + (n-1) a_{n-1} X^{n-2} + ... + a_1.$$

4.0.0.35 **Lema.** *Derivată formală este o aplicaţie R-liniară (considerînd $R[X]$ ca un modul peste R, prin restricţia scalarilor) care satisface regula lui Leibniz*

$$D(fg) = D(f)g + fD(g).$$

Mai mult dacă se da un homomorfism de inele $\phi : R \to S$ atunci derivata formală $S[X] \to S[X]$ este aplicaţia liniară obţinută prin extinderea scalarilor.

Demonstraţie. Considerăm ecuaţia

$$D(fg) = D(f)g + fD(g).$$

Fixandu-l pe g observam că ambii termeni sunt funcţii liniare $R[X] \to R[X]$, de f. Termenul din stânga este o compunere de doua aplicaţii liniare, înmulţirea cu g şi D, şi compunerea aplicaţiilor liniare este aplicaţie liniară. Similar termenul din dreapta este o suma de doua aplicaţii liniare, unde o funcţie este compunerea în celălalt sens. Cum $R[X]$este liber generat de puterile lui X, putem să considerăm $f(x) = x^m$. Similar considerăm $g(x) = x^n$. În acest caz termenul din stânga este

$$D(x^{m+n}) = (m+n)x^{m+n-1},$$

şi termenul din dreapta este

$$\begin{aligned} D(x^m)x^n + x^m D(x^n) &= (mx^{m-1})x^n + x^m(nx^{n-1}) \\ &= (m+n)x^{m+n-1}. \end{aligned}$$

Ultima afirmaţie este clară deoarece amândouă funcţiile sunt liniare şi au acelaşi efect pe x^n.

4.0.0.36 Lema. *Fie $f(x)$ polinom peste K.*

Atunci f are o rădăcină multiplă dacă $f(x)$ şi $f'(x)$ au o rădăcină comună într-un corp de descompunere.

Demonstraţie. Din ultima afirmaţie a 4.0.0.35, trecînd la un corp de descompunere al lui $f(x)$, putem să considerăm că $f(x)$ se descompune în K.

Dacă $f(x)$ are o rădăcină multiplă atunci $f(x) = (x-a)^2 g(x)$, pentru un polinom $g(x)$. În acest caz

$$f'(x) = 2(x-a)g(x) + (x-a)^2 g'(x),$$

astfel încât a este o rădăcină comună a lui $f(x)$ şi a lui $f'(x)$. Atunci putem scrie

$$f(x) = (x-a)g(x),$$

deci

$$f'(x) = g(x) + (x-a)g'(x).$$

Deci a trebuie să fie o rădăcină a lui $g(x)$. Dar atunci $x-a$ divide $g(x)$ deci a este rădăcină multiplă a lui $f(x)$.

4.0.0.37 Lema. *Fie $m(x) \in K[X]$ un polinom ireductibil peste un corp K.*

Atunci $m(x)$ are o rădăcină multiplă dacă $m'(x) \equiv 0$.

În particular $m(x)$ este neseparabil dacă

$$m(x) = \sum a_i x^{p_i}.$$

Demonstraţie. Din 4.0.0.36 $m(x)$ are o rădăcină multiplă dacă $m(x)$ şi $m'(x)$ au o rădăcină comună a. Cum $m(x)$ este ireductibil rezultă că $m(x)$ este un multiplu al polinomului minimal al lui a şi ori $m(x)$ îl divide pe $m'(x)$ ori $m'(x) \equiv 0$. Cum $m'(x)$ are gradul cu unu mai mic decât $m(x)$, singura varianta posibila este a doua.

4.0.0.38 Propoziţie. *Fie L/K o extindere finită de corpuri.*

Atunci L/K este separabilă dacă $[L : K]$ este coprim cu caracteristica. În particular orice extindere de corpuri în caracteristica zero este separabilă.

Demonstraţie. Presupunem că L/K nu este separabilă şi alegem $a \in L$ astfel încât $m(x)$, polinomul minimal al lui a este neseparabil. Din 4.0.0.37 $m(x)$ are gradul multiplu de p. În particular p ar divide termenul din stânga al egalităţii

$$[L : K] = [L : K(a)][K(a) : K]$$

deci divide şi termenul din dreapta, contradicţie.

5 Caracterizarea corpurilor finite

5.0.0.39 Definiţie-Lema. *$\mathbb{F}_q$ denota corpul unic de ordinul q unde $q = p^n$, p număr prim.*

Demonstraţie. Din 2.0.0.27 L este corpul de descompunere al $X^q - X$. Rezulta că F este unic din unicitatea corpului de descompunere.

În ceea ce priveşte existentă, fie F corpul de descompunere al $X^q - X$. Cum

$$D(X^q - X) = qX^{q-1} - 1 = -1$$

nu are nici o rădăcină, nu are nici rădăcini comune cu $X^q - X$. Deci $X^q - X$ are q rădăcini distincte în F deci F are cel puţin q elemente.

Pe de alta parte dacă a şi b sunt rădăcini ale $X^q - X$ atunci sunt şi $a + b$ (din moment ce q este putere a lui p) şi ab. Rezulta că orice element al

corpului generat de orice mulţime de rădăcini a $X^q - X$ este o rădăcină a $X^q - X$. Deci orice element din L este o rădăcină a $X^q - X$. Deci L are cel mult q elemente. Rezulta că L are exact q elemente.

5.0.0.40 Teorema. (criteriul lui Eisenstein) *Fie*

$$f(x) = a_n X^n + a_{n-1} X^{n-1} + ...a_0 \in R[X] = \mathbb{F}_p[s][x]$$

şi un polinom ireductibil fixat $p = p(s) \in R$. astfel încât

1. *p nu divide a_n*
2. *p divide $a_{n-1}, a_{n-2}, ..., a_0$*
3. *p^2 nu divide a_0*

Atunci $f(x) \in K[X] = \mathbb{F}_p(s)[X]$ este ireductibil.

Demonstraţie. Întâi aplicăm lema lui Gauss. Dacă luăm $R = \mathbb{F}_p[s]$ atunci corpul de fracţii F al lui R este K. Cum $f(x) \in R[X]$, lema lui Gauss ne informează că e suficient să demonstrăm că $f(x)$ este ireductibil în $R[X]$.

Dacă nu ar fi am găsi $g(x), h(x) \in R[X]$ astfel încât

$$f(x) = g(x)h(x).$$

cu

$$g(x) = b_l X^l + b_{l-1} X^{l-1} + ... + b_0$$

şi

$$h(x) = c_m X^m + c_{m-1} X^{m-1} + ... + c_0.$$

Fie atunci

$$R \to \frac{R}{< p >} = F$$

reducerea modulo p. Cum R este inelul de polinoame peste un corp şi p este ireductibil, am văzut deja că f este corp. F este chiar un corp finit de caracteristica p, izomorf cu $\mathbb{F}_q$ unde q este putere de număr prim.

Aceasta aplicaţie determina, din proprietatea de universalitate a inelelor de polinoame, aplicaţia

$$R[X] \to F[X].$$

Avem

$$\begin{aligned} x^n &= \hat{m}(x) \\ &= \hat{f}(x)\hat{g}(x). \end{aligned}$$

Am notat cu $\hat{f}$ reducerea modulo p.

Cum $F[X]$ este inel factorial şi $x \in F[X]$ este prim avem $\hat{f}(x) = x^l$ şi $\hat{g}(x) = x^m$. Atunci $\hat{b_0} = \hat{c_0} = 0$. Deci p divide atât b_0 cat şi c_0. Atunci p^2 divide $a_0 = b_0 c_0$.

6 Închiderea algebrică a unui corp

6.0.0.41 Definiţie. *Fie K corp. Închiderea algebrică a lui K (notăm $L = \overline{K}$) este o extindere algebrică de corpuri L/K astfel încât orice polinom din $K[X]$ se descompune în L.*

Spunem că K este algebric închis dacă $K = \overline{K}$.

6.0.0.42 Lema. *Fie L/K extindere de corpuri. Sunt echivalente:*

1. *L/K este algebrică şi L este algebric închis.*
2. *$L = \overline{K}$ este închiderea algebrică a lui K.*
3. *L/K este algebrică şi pentru orice extindere finită N/L, $N = L$.*

Demonstraţie. "$1 \Rightarrow 2$" clar.

"$2 \Rightarrow 3$". Fie N/L extindere finită. Trecînd la o extindere normală putem să considerăm N/L corp de descompunere pentru $f(x) \in L[X]$. Fie $L/M/K$ corpul intermediar generat de coeficienţii lui $f(x)$. Atunci $f(x) \in M[X]$.

Cum $f(x)$ se descompune în N putem găsi un corp intermediar $N/N'/M$ care este corp de descompunere pentru $f(x)$ peste M. Cum $M \subset L$ şi L/K este algebrică, M/K este de asemenea algebrică. Cum este şi finit generată, M/K este finită. Analog pentru N'/M. Din legea turnurilor N'/K este finită. Alegem $a \in N'$. Atunci a este algebric peste K. Fie $m(x) \in K[X]$ polinom minimal al lui a. Din premiza $m(x)$ se descompune în L. Atunci $N' \subset L$. Atunci $N = L$, deoarece am arătat că $f(x)$ se descompune în L, rezultă 3.

"$3 \Rightarrow 1$". Fie $f(x) \in L[X]$. Trebuie să arătam că $f(x)$ se descompune în L. Fie N/L corp de descompunere pentru $f(x)$. Atunci N/L este finit, rezultă $N = L$ deci $f(x)$ se descompune în L.

6.0.0.43 Lema. *Închiderea algebrică a unui corp este unică.*

Demonstraţie. Fie K corp şi L_1, L_2 doua inchideri algebrice ale lui K. Vrem să găsim un izomorfism între L_1 şi L_2.

Fie P mulţimea tripleţilor $a = (M_1, M_2, \phi)$ unde ϕ este un izomorfism al $M_1 \subset L_1$ cu $M_2 \subset L_2$. Spunem că $a < b = (N_2, N_2, \psi)$ dacă $M_1 \subset N_1$, $M_2 \subset N_2$ şi ψ extinde ϕ.

Aplicăm lema lui Zorn. Fie Q o mulţime total ordonată al lui P.

Fie N_1 reuniunea după M_1 şi N_2 reuniunea după M_2. Definim $\psi : N_1 \to N_2$. Fiind dat $m \in N_1$, alegem $a \in Q$, astfel încât $m \in M_1$. Alegem apoi $\psi(m) = \phi(m)$. ψ este bine definit deoarece Q este total ordonată. Se verifica uşor că ψ este automorfism. Deci Q este dominat de tripletul (M, N, ψ).

Din lema lui Zorn, exista a tripletul maximal. Presupunem că $M_1 \neq L_1$. Alegem $a \in L_1 - M_1$. Fie $N_1 = M_1(a)$. Fie $m(x)$ polinomul minimal al lui a peste K. Atunci $m(x)$ se descompune în L_2. Alegem $b \in L_2$. Atunci putem să extindem ϕ la $\psi : N_1 \to N_2 = M_2(b)$, contradicţie.

6.0.0.44 Lema. *Închiderea algebrică a unui corp exista.*

Demonstraţie. Fie T o mulţime în corespondenţa bijectivă cu familia polinoamelor neconstante din $K[X]$. Fie $R = K[T]$ inel de polinoame şi I ideal în R generat de toate elementele de forma $f(t_f)$, unde $t_f \in T$, adică dacă

$$f(x) = X^n + a_{n-1}X^{n-1} + ... + a_0,$$

unde $a_i \in K$, atunci

$$f(t_f) = (t_f)^n + a_{n-1}(t_f)^{n-1} + ... + a_0.$$

Idealul I este propriu. Dacă nu este, $1 \in I$, şi $\exists t_1...t_n \in T$ distincte şi polinoamele $h_1(T), ..., h_n(T) \in K[T]$ cu

$$1 = h_1(T)f_1(t_1) + ... + h_n(T)f_n(t_n).$$

Atunci considerăm extinderea de corpuri $K(a_1, ..., a_n)$, unde a_i este rădăcină a lui $f_i(t_i)$ (f_i sunt neconstante). Dacă avem variabile în $h_i(T)$ altele decât $t_1, ..., t_n$ le notăm cu $t_{n+1}, ..., t_m$. Evaluînd cînd $t_i = a_i$ dacă $i \leq n$ şi $t_i = 0$ dacă $i \geq n+1$ (evaluarea este un homomorfism de inele $K[T] \to K(a_1, ..., a_n)$, termenul din dreapta este 0 şi avem contradicţia $1 = 0$.

Deci exista un ideal maximal M în R care-l contine pe I. Definim $L = R/M$. Demonstraţia continua în următorii paşi.

i) L/K este extindere de corpuri.

L este corp deoarece M este ideal maximal. Aplicaţia compusă

$$K \overset{incl}{\rightarrow} K[T] = R \overset{surj}{\rightarrow} R/M = L$$

nu este $\equiv 0$ deoarece $1 = 1$, şi deoarece este injectivă putem să identificăm K cu imaginea ei.

îi) Orice polinom neconstant $f(x) \in K[X]$ se descompune în $L[X]$.

Prin definiţie, $\exists t_f \in T$ cu $f(t_f) \in I \subset M$ şi mulţimea factor (coset) $t_f + M \in R/M = L$ este o rădăcină a lui $f(x)$. Rezulta prin inducţie după grad că $f(x)$ se descompune peste L.

iii) Extinderea L/K este algebrică.

Arătam că toate $t_f + M$ sunt algebrice peste K ceea ce este evident deoarece t_f este rădăcină a $f(x) \in K[X]$.

iv) L este algebric închis.

Fie $g(x) \in L[X]$ şi fie $E = L(a_1, ..., a_m)$ corp de descompunere al lui $g(x)$ peste K. Avem un turn de corpuri $E/L/K$ unde L/K şi E/L sunt extinderi algebrice, rezultă E/K extindere algebrică deci $p(x) = Irr(a_1, K) \in K[X]$. Din îi) $p(x)$ se descompune peste L deci $\{a_1, ..., a_m\} \subseteq L$ adică $E \subset L$ deci $g(x)$ se descompune în $L[X]$ deci L este algebric închis.

Partea II
Teorie Galois

7 Automorfismele unei extinderi

7.0.0.45 Definiţie. *Fie L/K extindere de corpuri.*

Un K-automorfism al lui L/K este un automorfism al lui L care-l fixează (înviorează) pe K.

Prin ϕ îl fixează pe K înţelegem că ϕ restricţionat la K este identitatea.

7.0.0.46 Definiţie-Lema. *Fie L/K extindere de corpuri.*

***Grupul Galois** al lui L/K notat cu $G(L/K)$ este subgrupul mulţimii tuturor K-automorfismelor de la L la L.*

Demonstraţie. Se observa uşor că K-automorfismele lui L împreuna cu compunerea formează o structura de grup.

7.0.0.47 Propoziţie. *Fie L/K extindere normală şi M corp intermediar. Sunt echivalente:*

1. *M/K este normală.*
2. *Pentru orice K-automorfism ϕ al L/K, $\phi(M) \subset M$.*
3. *Pentru orice K-automorfism ϕ al L/K, $\phi(M) = M$.*

Demonstraţie. "$1 \Rightarrow 2$". Fie ϕ K-automorfism al L/K. Alegem $a \in M$ cu $\phi(a) = b$. Atunci b este rădăcină a polinomului minimal m. Cum M/K este normală, şi a este rădăcină a lui $m(x)$, $m(x)$ se descompune în M. În particular $b \in M$.

"$2 \Rightarrow 3$". Fie ϕ K-automorfism al lui L/K. Cum L/K este finită atunci şi M/K este finită. Deoarece ϕ este automorfism atunci

$$[\phi(M) : K] = [M : K].$$

Pe de alta parte din ipoteza $\phi(M) \subset M$. Deci din legea turnurilor $[M : \phi(M)] = 1$.

"$3 \Rightarrow 1$". Fie $f(x)$ polinom ireductibil şi $a \in M$ o rădăcină a lui $f(x)$. Cum L/K este normală, $f(x)$ se descompune în L. Fie b orice alta rădăcină a lui $f(x)$. Atunci putem găsi un automorfism ϕ al lui L care-l duce pe a în b. Cum $\phi(M) \subset M$ rezultă că $b \in M$. Atunci $f(x)$ se descompune în M.

7.0.0.48 Lema. *Fie L/K extindere de corpuri, fie $a \in L$ algebric cu polinomul minimal $m(x)$ şi fie $M = K(a)$ corpul intermediar generat de a. Fie d gradul lui M/K. Fie $\phi : K \to K'$ homomorfism de inele.*

Atunci exista cel mult d homomorfisme de inele $\psi : M \to L'$ care-l extind pe ϕ, cu egalitatea dacă a este separabil şi imaginea lui m se descompune în L'.

Demonstraţie. Gradul lui $m(x)$ este d. Fie $m'(x)$ polinomul corespunzător în $K'[X]$. Atunci $m'(x)$ are cel mult d rădăcini, cu egalitatea dacă a este separabil. Pe de alta parte orice aplicaţie ψ care-l extinde pe ϕ este determinată de acţiunea pe a şi exista un automorfism care-l duce pe a în b dacă b este rădăcină a lui $m'(x)$.

7.0.0.49 Lema. *Fie L/K extindere separabilă şi M/K corp intermediar.*

Atunci M/K şi L/M sunt amândouă separabile.

Demonstraţie. Fie $a \in L$. Fie $f(x)$ polinomul minimal al lui a peste M $g(x)$ polinomul minimal peste K. Atunci $f(x)$ divide $g(x)$. Pe de alta parte $g(x)$ este separabil, pentru că nu are rădăcini multiple, deoarece L/K este separabilă. Deci nici $f(x)$ nu are rădăcini multiple, deci L/M este separabilă.

7.0.0.50 Propoziţie. *Fie L/K extindere finită de corpuri şi $\phi : K \to K'$ homomorfism de inele şi L'/K' extindere oarecare.*

Atunci exista cel mult d homomorfisme de inele $\psi : L \to L'$ care-l extind pe ϕ cu egalitatea dacă L/K este separabilă şi L'/K' corpul de descompunere al unui polinom ale cărui rădăcini generează L/K.

Demonstraţie. Demonstrăm prin inducţie după gradul lui L/K. Pentru $L = K$ rezultatul este evident. Altfel alegem $a \in L - K$. Fie d gradul lui $M = K(a)/K$. Din 7.0.0.49 exista cel mult $d = [M : K]$ homomorfisme de inele $\pi : M \to L'$ care-l extind pe ϕ. Pe de alta parte cum $[M : K] > 1$, din legea turnurilor $[L : M] < [L : K]$. Prin inducţie exista cel mult $[L : M]$ homomorfisme de inele $\psi : L \to L'$ cere-l extind pe π dat. Deoarece orice ψ extinde cel puţin un π, exista cel mult $[L : K] = [L : M][M : K]$ extinderi ale lui ϕ, cu egalitatea dacă a este separabil şi polinomul minimal al lui a se descompune în L.

7.0.0.51 Corolar. *Fie L/K extindere finită şi fie M extindere intermediară.*

Atunci L/K este separabilă dacă L/M şi M/K sunt separabile.

Demonstraţie. Din 7.0.0.48 este suficient să demonstrăm că dacă L/M şi M/K sunt separabile atunci L/K este separabilă. Fie N/L inchideri normală a lui L/K. Din 7.0.0.50 exista $[M/K]$ homomorfisme de inele $\pi : M \to N$ a căror restricţie la K este identitatea şi pentru fiecare π sunt $[L : M]$ homomorfisme de inel $\psi : L \to N$ care-l extind pe π. Astfel exista cel puţin $[L : K] = [L : M][M : K]$ homomorfisme de inel $\psi : L \to N$ care extind identitatea. Rezulta din 7.0.0.50 că L/K este separabilă.

7.0.0.52 Corolar. *Fie L/K extindere finită cu $L = K(a_1, a_2...a_n)$.*

Atunci L/K este separabilă dacă toţi a_i sunt separabili.

Demonstraţie. Fie M_i corpul intermediar generat de a-ul primului i. Aplicînd 7.0.0.51 şi facînd inducţie după i obţinem rezultatul.

8 Extinderi Galois

8.0.0.53 Definiţie. *Fie L/K extindere de corpuri.*

*Spunem că L/K este **extindere Galois (galoisiană)** dacă este normală şi separabilă.*

8.0.0.54 Lema. *Fie L/K extindere finită de corpuri.*

Atunci L/K este Galois dacă este corpul de descompunere al unui polinom separabil $f(x) \in K[X]$.

Demonstraţie. Din cele de mai sus.

8.0.0.55 Lema. *Fie L/K o extindere separabilă, şi N/K o închidere normală.*

Atunci N/K este Galois.

Demonstraţie. Închiderea normală a unei extinderi separabile L/K este corpul de descompunere al unu polinom separabil deoarece orice factor ireductibil al polinomului are o rădăcină în L. Rezultatul urmează din 8.0.0.54.

8.0.0.56 Teorema. *Fie L/K extindere finită.*

Atunci L/K este Galois dacă exista $[L : K]$ K-automorfisme ale lui L/K.

Demonstraţie. Fie L/K Galois. Atunci exista $[L : K]$ K-automorfisme ale lui L/K conform 7.0.0.47 şi 7.0.0.50.

Presupunem că exista $[L : K]$ K-automorfisme ale lui L/K. Fie N/K o închidere normală. Atunci sunt cel mult $[L : K]$ homomorfisme de inele

$\psi : L \to N$. Rezulta că L/K e separabilă din 7.0.0.50 şi că orice homomorfism de inele este de fapt un automorfism, deci L/K este normală din 7.0.0.47.

8.0.0.57 Definiţie. *Fie L corp şi X o mulţime de automorfisme ale lui L. Corpul **fixat de** X notat cu L^X este mulţimea tuturor elementelor lui K care sunt fixate de orice element al lui X.*

Observam că $L^X = L^G$ unde G este grupul de automorfisme generat de X.

8.0.0.58 Lema. *Fie $L/M/K$ extindere de corpuri. Fie G un grup de automorfisme ale lui L şi H un subgrup. Atunci:*

1. $G \subset Gal(L/L^G)$.
2. $K \subset L^{Gal(L/K)}$.
3. $L^G = L^H$.
4. $Gal(L/M) \subset Gal(L/K)$.

Demonstraţie. Fie G un grup de K-automorfisme ale lui L. Trebuie să demonstrăm că funcţiile

$$G \to L^G \qquad si \qquad M \to Gal(L/M),$$

sunt corespondenţe antimonotone (în ceea ce priveşte incluziunea) între subgrupurile lui G şi corpurile intermediare $L/M/K$. Punctul principal este să stabilim că L/K este Galois, şi dorim

$$[L : K] = G.$$

8.0.0.59 Definiţie. *Fie R un inel. Notăm R^* grupul multiplicativ al unităţilor lui R. Dacă R este corp atunci $R^* = R - \{0\}$.*

8.0.0.60 Definite. *Fie G grup şi K corp. Un **caracter** este o aplicaţie nenulă $\chi : G \to K$ astfel încât aplicaţia indusă*

$$G \to K^*$$

este homomorfism.

8.0.0.61 Lema. *Fie G grup şi K corp.*

Atunci orice mulţime de caractere este liniar independentă.

Demonstraţie. Presupunem prin reducere la absurd că nu este. Atunci putem găsi caracterele $\chi_1 ... \chi_n$ şi scalarii $a_1 ... a_n \in K$ astfel încât

$$\sum_{i=1}^{n} a_i \chi_i = 0$$

unde nu toţi a_i sunt 0. Alegem $n > 0$ cel mai mic număr cu aceasta proprietate. În particular $a_i \neq 0$ pentru toţi i. $n \neq 1$ căci altfel $0 = a_1 \chi_1(1) = a_1$. Cum $\chi_1 \neq \chi_n$ exista $h \in G$ astfel încât $\chi_1(h) \neq \chi_n(h)$.

Avem

$$\sum_{i=1}^{n} a_i \chi_i(g) = 0,$$

pentru orice $g \in G$. În particular aceasta ecuaţie este adevărată şi pentru hg în locul lui g. Rezulta

$$\begin{aligned} 0 &= \sum_{i=1}^{n} a_i \chi_i(hg) \\ &= \sum_{i=1}^{n} a_i \chi_i(h) \chi_i(g). \end{aligned}$$

Inmulţim prima ecuaţie cu $\chi_n(h) \neq 0$, pentru a obţine doua ecuaţii cu acelaşi ultim termen

$$\sum_{i=1}^{n} a_i \chi_n(h) \chi_i(g) = 0$$

$$\sum_{i=1}^{n} a_i \chi_i(h) \chi_i(g) = 0.$$

Dacă scădem a doua ecuaţie din prima obţinem o ecuaţie de forma

$$\sum_{i=1}^{n} b_i \chi_i(g) = 0.$$

unde $b_i = a_i(\chi_i(h) - \chi_i(n))$. Cum aceasta este adevărată pentru $\forall g \in G$, avem

$$\sum_{i=0}^{n} b_i \chi_i = 0.$$

Din presupunere $b_1 \neq 0$, aşa că avem o dependentă liniară mai mica, netrivială. Contradicţie.

8.0.0.62 Lema. *Orice mulţime de automorfisme ale unui corp L sunt liniar independente.*

Demonstraţie. Orice automorfism ϕ determina şi este determinat de caracterul

$$\chi : L^* \to L$$

şi rezultatul urmează ca o consecinţa a 8.0.0.61.

8.0.0.63 Lema. *Fie L corp şi X o mulţime de automorfisme ale lui L cu corpul fixat $K = L^X$.*

Atunci

$$[L : K] \geq |X|$$

unde precizăm că numai partea stânga să fie infinită dacă partea dreapta este infinită.

Demonstraţie. Presupunem prin reducere la absurd că nu este aşa. Atunci L/K este finit. Fie $l_1, l_2...l_m$ o baza. Din premiza putem găsi $\sigma_1, \sigma_2, ..., \sigma_n$ automorfisme ale L/K cu $n > m$. Considerăm sistemul de $m \times n$ ecuaţii

$$\sum_j \sigma_j(l_i)x_j = 0.$$

Cum sunt n necunoscute şi $m < n$ ecuaţii, exista soluţia netrivială $a_1, a_2, ..., a_n \in K$ (eliminare Gauss).

Afirm că

$$\sum_j a_j\sigma_j = 0.$$

Fie $l \in L$. Atunci exista $b_1, b_2, ..., b_m \in K$ astfel încât

$$l = \sum_i b_i l_i.$$

În acest caz

$$l = \sum_j a_j\sigma_j(l) = \sum_j a_j\sigma\left(\sum_i b_i l_i\right)$$

$$\begin{aligned} &= \sum_i \sum_j a_j b_i \sigma(l_i) \\ &= \sum_i b_i \left(\sum_j a_j \sigma(l_j) \right) \\ &= 0, \end{aligned}$$

Deci ceea ce afirm este adevărat. Dar aceasta contrazice că orice mulţime de automorfisme este liniar independentă.

8.0.0.64 Lema. *Fie L un corp şi G un grup finit de K-automorfisme ale lui L.*

Atunci

$$[L : K] = |G|.$$

În particular L/K este Galois.

Demonstraţie. Deja am văzut că

$$[L : K] \geq G.$$

Fie $\sigma_1, \sigma_2, ..., \sigma_m$ elementele lui G. Atunci putem găsi $l_1, l_2, ..., l_n \in L$ liniar independente, cu $n > m$. Avem m ecuaţii

$$\sum_i \sigma_i(l_j) x_j = 0$$

cu $n > m$ necunoscute, putem găsi o soluţie nebanală $a_1, a_2, ..., a_n$. După o eventuală rearanjare putem lua σ_1 identitatea. Prima ecuaţie este astfel

$$\sum a_i l_i = 0.$$

Deoarece $l_1 ... l_n$ sunt liniar independente peste K rezultă că nu toţi $a_i \in K$. Din toate aceste soluţii o alegem pe cea cu cel mai mic număr r de $a_i \neq 0$. Putem lua fără a restrânge generalitatea $a_i = 0$ dacă $i > r > 0$. Din nou, fără a restrânge generalitatea, după o eventuală rescalare, considerăm că $a_r = 1$. Cum nu toţi $a_i \in K$ putem să presupunem că $a_1 \notin K$. În particular $r = 1$.

Cum K este corpul fixat de G şi $a_1 \notin K$ exista un element al lui $\sigma \in G$ care nu-l fixează pe a_1. Cum aplicaţia

$$G \to G$$

data de multiplicarea la stânga cu σ este bijectivă (inversul ei este înmulţirea cu inversul lui σ) rezultă ca, deoarece σ_i parcurge elementele lui G, la fel şi $\sigma \circ \sigma_i$ (nu neapărat în aceeaşi ordine). Cum σ este homomorfism de inele aplicînd-o fiecăreia din ecuaţiile de mai sus, rezultă că obţinem o nouă soluţie a acestor ecuaţii

$$\sum_i \sigma_j(l_j)b_i = 0$$

unde $b_i = \sigma(a_i)$. Din ipoteza $b_1 \neq a_1$. Înmulţind primul set de ecuaţii cu b_1 şi pe al doilea cu a_1 şi facînd diferită între ele obţinem soluţia

$$\sum_i \sigma_i(l_j)c_i = 0$$

unde $c_r \neq 0$ dar $c_1 = 0$. Contradicţie cu alegerea iniţială a $a_1, ..., a_n$.

9 Teorema fundamentală a teoriei lui Galois

9.0.0.65 Teorema (fundamentală a teoriei lui Galois). *Fie L/K extindere Galois finită. Atunci exista o bijecţie antimonotonă între subgrupurile Galois ale $Gal(L/K)$ şi corpurile intermediare $L/M/K$. Fiind dat un subgrup H fie $M = L^H$ şi dat fiind un corp intermediar $L/M/K$ fie $H = Gal(L/M)$.*

Demonstraţie. Fie H subgrup al lui G. Fie $M = L^H$ şi luăm $H' = Gal(L/M)$. Vrem să arătam că $H = H'$. Am demonstrat deja că $H \subset H'$ şi $G = [L/K]$ finit. Este suficient să demonstrăm că H' are cardinalul cel mult cat H. Dar

$$|H| = [L : M]$$

şi exista cel mult $[L : M]$ automorfisme ale L/M, astfel

$$|K| \leq [L : M] = |H|.$$

Deci $H = H'$ şi compunerea într-un sens este identitatea.

Invers plecăm de la $L/M/K$. Fie $H = Gal(L/M)$ şi $N = L^H$. Ştim deja că

$$M \subset N$$

şi din legea turnurilor e suficient să demonstrăm că

$$[L : N] \geq [L : M].$$

Cum L/K este Galois, atunci şi L/M este Galois. Însă atunci

$$[L : M] = |H|.$$

Cum H este mulţime de automorfisme ale L/N, avem

$$[L : N] \geq |H|.$$

Deci $M = N$ şi compunerea celălalt sens este identitatea. Deci avem o corespondenţa bijectivă. Am văzut deja că aceasta corespondenţa este antimonotonă fata de incluziunea pe mulţmi.

9.0.0.66 Teorema. *Fie L/K extindere separabilă finită.*
Atunci L/K este simpla (primitivă).

Demonstraţie. E suficient să demonstrăm că numărul de corpuri intermediare este finit. Fie $M/L/K$ închiderea normală, deci M/K este Galois. În acest caz grupul Galois este finit şi avem un număr finit de subgrupuri ale lui G. Din corespondenţa Galois avem un număr intermediar de extinderi finit.

9.0.0.67 Teorema (asupra corespondenţei Galois). *Fie L/K extindere Galois finită. Atunci avem bijecţie antimonotonă între subgrupurile lui $Gal(L/K)$ şi corpurile intermediare $L/M/K$. Fie H un subgrup, $M = L^H$ şi dat fiind un corp intermediar $L/M/K$, fie $H = Gal(L/M)$.*

Mai mult M/K este normală dacă H este normal în G. În acest caz $Gal(M/K) \simeq G/H$.

Demonstraţie. Am demonstrat deja existenţa corespondenţei.

Ştim că M/K este normală dacă $\forall \phi \in G, \phi(M) = M$. Fie M/K normală. Definim aplicaţia

$$f : G \to Gal(M/K)$$

care-l duce pe ϕ în restricţia ψ a lui ϕ la M. Cum M/K este normală ψ este automorfism al M/K. Se verifica uşor că f este homomorfism de grupuri, al cărei nucleu este H, deci H este normal. Rezulta că G/H este izomorf cu un subgrup al $Gal(M/K)$. Dar

$$\begin{aligned} |Gal(M/K)| &= [M : K] \\ &= [L : K]/[L : M] \\ &= |G|/|H| \end{aligned}$$

unde am folosit legea turnurilor şi faptul că L/M şi L/K sunt extinderi Galois, deci $Gal(M/K) \simeq G/H$.

Acum luăm H normal. G are o acţiune canonică pe L. Fie $m \in M$ şi $\phi \in G$. Fie $n = \phi(m)$. Cum H îl fixează pe m atunci $H = \phi H \phi^{-1}$ îl fixează pe n. Din corespondenţa stabilită, singurele elemente ale lui L fixate de H sunt elementele lui M. Deci $n \in M$ şi $\phi(M) \subset M$. Rezulta M/K normală.

9.0.0.68 Definiţie. *Fie R un inel de caracteristica p. Aplicaţia*

$$\Phi : R \to R$$

definită ca

$$\Phi(a) = a^p$$

este un homomorfism de inele, numit ***funcţia Frobenius****.*

9.0.0.69 Teorema. *Fie L/K extindere de corpuri finite.*

Atunci L/K este Galois. Mai mult, grupul Galois este ciclic, generat de o putere Frobenius.

Demonstraţie. Ştim deja că $L \simeq \mathbb{F}_q$, $K = \mathbb{F}_r$ unde q şi r puteri ale lui p, $q = p^n$ şi $r = p^m$, unde $m|n$ şi $d = n/m$ este gradul extinderii. Mai mult L este corpul de descompunere al polinomului $X^q - X$ şi elementele nenule ale lui L sunt exact rădăcinile unităţii. Cum Φ este injectivă şi L este finit, Φ este evident automorfism al lui L.

Corpul fixat de Φ^k este mulţime tuturor elementelor lui L cu proprietatea

$$a^t = a$$

unde $t = p^k$, adică toate rădăcinile polinomului

$$X^t - X.$$

Dar atunci Φ^m îl fixează pe K şi cea mai mica putere a lui Φ^m care-l fixează pe K este d. Astfel

$$< \Phi^m >$$

este subgrup al grupului Galois de ordinul d. Cum grupul Galois are ordinul d, teorema este demonstrată.

9.0.0.70 Lema. *Fie $f(x) \in \mathbb{R}[X]$ de grad impar.*

Atunci $f(x)$ are o rădăcină reală.

Demonstraţie. Presupunem fără a restrânge generalitatea că $f(x)$ este monic. Putem scrie

$$f(x) = X^n + \sum a_i X_i$$

Fie $m = max|a|$ şi alegem $x > nm$. Atunci

$$\begin{aligned} f(x) &\geq x^n - \left|\sum a_i x_i\right| \\ &\geq x^n - \sum |a_i|\,|x_i| \\ &\geq x^n - nmx^{n-1} \\ &\geq x^{n-1}(x - nm) > 0. \end{aligned}$$

Analog $f(x) < 0$, pentru $x < -nm$. Deci $f(x)$ trebuie să aibe un 0 din teorema valorii intermediare.

10 Teorema Fundamentală a Algebrei

10.0.0.71 Teorema (Teorema Fundamentală a Algebrei - D'Alembert). *$\mathbb{C}$ este închiderea algebrică a lui $\mathbb{R}$.*

În particular $\mathbb{C}$ este algebric închis.

Demonstraţie. Fie $L/\mathbb{C}$ extindere finită. E suficient să demonstrăm că $L = \mathbb{C}$. Trecînd la o închiderea normală putem spune că $L/\mathbb{C}$ este Galois. Fie $G = Gal(L/\mathbb{C})$. Fie H un 2-subgrup Sylow. Fie $M = L^H$ corpul fixat corespunzător.

Atunci $M/\mathbb{R}$ are grad impar. Fie $a \in M$ şi fie $f(x)$ polinomul minimal al lui a. Atunci $f(x)$ are gradul impar, deci o rădăcină reală. Cum $f(x)$ este ireductibil, gradul sau trebuie să fie unu. Dar atunci $a \in \mathbb{R}$ şi astfel $M = \mathbb{R}$. Deci $L/\mathbb{R}$ are gradul putere de doi. Analog pentru $L/\mathbb{C}$.

Presupunem că G nu este grupul trivial. Din teorema lui Sylow exista un subgrup H al lui G de index doi. Atunci am avea o extindere $M/\mathbb{C}$ de grad doi. Cum caracteristica este zero, ar exista un element $a \in M$ astfel încât $a^2 \in \mathbb{C}$. Dar $\mathbb{C}$ este închis pentru rădăcina pătrată, contradicţie. Deci G este trivial şi $L = \mathbb{C}$.

Partea III
Ecuaţii rezolvabile prin radicali

11 Extinderi Radicale şi Ciclice

11.0.0.72 Definiţie *Fie K corp. Un element $\omega \in K$ se numeşte* ***rădăcină primitivă de ordinul n a unităţii*** *dacă*

$$\omega^n = 1$$

şi nici o putere mai mica a sa nu este egala cu unu.

Fie L/K un corp de descompunere pentru $X^n - 1$. ***Polinomul ciclotomic de ordinul n*** *este prin definiţie*

$$\Phi_n(x) = \prod_{\omega}(X - \omega)$$

unde produsul parcurge rădăcinile de ordinul n ale unităţii.

11.0.0.73 Definiţie. *Fie L/K extindere Galois cu grupul Galois G.*

Fie $a \in L$. Spunem că b este ***conjugatul*** *lui a dacă b este în aceeaşi orbită ca şi a sub acţiunea lui G.*

11.0.0.74 Lema. *Fie L/K extindere Galois cu grupul Galois G. Fie $f(x) \in L[X]$ polinom care se descompune în L.*

Atunci $f(x) \in K[X]$ dacă mulţimea rădăcinilor lui $f(x)$ este o reuniune de orbite ale lui G. Mai mult,$f(x)$ este ireductibil dacă rădăcinile sale sunt o orbită în G. În particular dacă $a \in L$ atunci polinomul minimal al lui a este

$$\prod_{b}(X - b)$$

unde produsul parcurge conjugaţii lui a.

Demonstraţie. E suficient să demonstrăm că $f(x) \in K[X]$ este ireductibil dacă mulţimea rădăcinilor lui $f(x)$ este o orbită a lui G. Fie

$$f(x) = \prod_{b}(X - b)$$

unde produsul parcurge conjugaţii lui $a \in L$. Atunci $f(x)$ este invariant sub acţiunea grupului Galois deoarece orice element al grupului schimba factorii între ei şi asta nu afectează produsul. Atunci fiecare coeficient al lui $f(x)$ e invariant fata de orice element al lui G, adică fiecare coeficient se afla în $L^G = K$, deci $f(x) \in K[X]$.

Pe de alta parte G acţionează tranzitiv pe rădăcinile oricărui polinom ireductibil.

11.0.0.75 Lema. *$\Phi_n(x)$ este din corpul de baza K.*

Demonstraţie. $X^n - 1$ este un polinom cu coeficienţii în K. Fie L/K corp de descompunere cu grupul Galois G. $\Phi_n(x)$ divide $X^n - 1$ în L. Fie ω o rădăcină de ordinul n a unităţii. Atunci celelalte rădăcini ale $X^n - 1$ sunt cele n puteri ale ω

$$\omega, \omega^2, \omega^3, ..., \omega^n.$$

Deci $L = K(\omega)$. Deci acţiunea unui element $\phi \in G$ este determinată de efectul asupra ω. Cum ϕ trimite ω într-un alt generator conjugaţii lui ω sunt toţi rădăcini primitive ale unităţii. Rezultatul urmează din 11.0.0.74.

11.0.0.76 Lema.

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

Demonstraţie. Evident, deoarece orice rădăcină de ordinul n a unităţii este o rădăcină primitivă a unităţii pentru un d unic cu $d|n$.

11.0.0.77 Lema. *În caracteristica zero, $\Phi_n(x) \in \mathbb{Z}[X]$.*

Demonstraţie. Ştim deja că $\Phi_n(x) \in \mathbb{Q}[X]$. Prin inducţie,

$$X^n - 1 = \Phi_n(x) f(x)$$

unde, prin inducţie rezultă $f(x) \in \mathbb{Z}[X]$.

11.0.0.78 Definiţie. *Notăm cu U_n grupul unităţilor în $\mathbb{Z}_n$.*

11.0.0.79 Propoziţie. *Fie K un corp a cărei caracteristica este coprimă cu n şi fie L/K corp de descompunere pentru $X^n - 1$.*

Atunci grupul Galois G al L/K este izomorf cu un subgrup al U_n, cu egalitatea dacă $\Phi_n(x)$ este ireductibil peste K.

Demonstraţie. X^n-1 este separabil deoarece derivata lui este $nX^{n-1} \neq 0$. Deci L/K este Galois. Fie ω rădăcină primitivă de ordinul n a unităţii. Definim aplicaţia

$$f : G \to U_n$$

care-l duce pe σ în i, unde $\sigma(\omega) = \omega^i$. Aplicaţia este bine definită deoarece σ trebuie să permute rădăcinile lui $X^n - 1$, şi rădăcinile nu sunt altceva decât puterile lui ω. Pe de alta parte, ω este generatorul lui L/K, deci ω^i este de asemenea generatorul lui L/K. Deci şi ω^i este de asemenea rădăcină primitivă a unităţii. Deci i şi n sunt prime între ele, deci i este o unitate modulo n. Mai mult σ este determinat de acţiunea să pe ω, deci f este injectivă.

Presupunem că $f(\sigma) = i$ şi $f(\tau) = j$. Atunci $\sigma(\omega) = \omega^i$ şi $\tau(\omega) = \omega^i$. În acest caz

$$\begin{aligned}(\tau \circ \sigma)(\omega) &= \tau(\sigma(\omega)) \\ &= \tau(\omega^i) \\ &= (\tau(\omega))^i \\ &= (\omega^j)^i \\ &= \omega^{ij}.\end{aligned}$$

Deci $f(\tau\sigma) = ij$ şi f este un grup de homomorfisme. Calculul de mai sus arată de asemenea că dacă alegem o alta rădăcină primitivă a unităţii ω^i, τ de asemenea acutizează asupra ω^i, ridicînd la puterea j. Deci G este izomorf cu un subgrup din U_n. Acum $G = U_n$ dacă putem transforma ω într-o alta rădăcină primitivă a unităţii. Dar din 11.0.0.79 aceasta este echivalent cu a spune că $\Phi_n(x)$ este ireductibil.

11.0.0.80 Teorema. *$\Phi_n(x)$ este ireductibil în $\mathbb{Q}$.*

Demonstraţie. Presupunem prin reducere la absurd că nu este. Din lema lui Gauss putem scrie

$$\Phi_n(x) = f(x)g(x)$$

unde $f(x)$ şi $g(x)$ sunt polinoame monice cu coeficienţi din $\mathbb{Z}[X]$ de grad cel puţin unu şi $f(x)$ este ireductibil.

Presupunem că ω este rădăcină a lui $f(x)$. Fie p prim care nu-l divide pe n. Arătam că ω^p este rădăcină a lui $f(x)$. Presupunem prin reducere la absurd că nu este. Atunci ω^p este o rădăcină a lui $g(x)$. Dar atunci ω este

o rădăcină a lui $h(x) = g(x^p)$. Deci $f(x)$ divide $h(x)$, deoarece $f(x)$ este polinomul minimal al lui ω. Avem deci

$$h(x) = f(x)k(x).$$

Reducînd modulo p

$$\mathbb{Z} \to \mathbb{F}_p.$$

Obţinem $\bar{h}(x) = \bar{g}(x^p) = (\bar{g}(x))^p$. Fie q un factor ireductibil al $\bar{f}(x) \in \mathbb{F}_p[X]$. Atunci q divide $\bar{g}(x)$ şi q^2 divide $\bar{f}\bar{g} = \bar{\Phi}_n(x)$. Dar $\Phi_n(x)$ nu ar fi separabil, contradicţie deoarece n şi p sunt prime între ele.

Deci ω^p este rădăcină a lui $f(x)$. Fiind data o rădăcină primitivă de ordinul n a unităţii, putem să o scriem ca ω^m, pentru un m coprim cu n. În acest caz

$$m = p_1 p_2 ... p_k$$

pentru numerele prime $p_1, p_2, ..., p_k$ coprime cu n. Repetînd argumentul de mai sus de k ori, obţinem că ω^m este rădăcină a lui $f(x)$. Atunci $f(x) = \Phi_m(x)$, contradicţie.

11.0.0.81 Lema. *Fie L/K corp de descompunere al lui $X^n - a \in K[X], a \neq 0$.*

Atunci exista un corp intermediar M care este corp de descompunere pentru $X^n - 1$.

Demonstraţie. Dacă $n = mp$ şi $a = b^p$, unde p este caracteristica lui K, atunci

$$X^n - a = (X^m - b)^p.$$

Astfel putem să presupunem că n este coprim cu caracteristica. În particular $X^n - a$ are n rădăcini distincte $a_1, ..., a_n$.

Fie a şi b doua rădăcini ale $X^n - a$. Atunci a/b este o rădăcină a $X^n - 1$. Deci

$$\frac{a_i}{a_1} \qquad unde \qquad 1 \leq i \leq n$$

sunt n rădăcini distincte ale lui $X^n - 1$.

11.0.0.82 Lema. *Fie K un corp de descompunere pentru $X^n - 1$ şi L/K o extindere Galois cu grupul Galois G de grad coprim cu caracteristica.*

Atunci L/K este corpul de descompunere al unui polinom ireductibil $X^n - a$ dacă grupul Galois G este ciclic de ordinul n.

Demonstraţie. Fie L/K corpul de descompunere al $X^n - a$ un polinom ireductibil. Fie α o rădăcină a polinomului $X^n - a$ şi $\omega \in K$ o rădăcină primitivă de gradul n a unităţii. Am văzut că dacă α este rădăcină a lui $X^n - a$ atunci celelalte rădăcini $\xi\alpha$, unde $\xi = \omega^i$ sunt rădăcini de gradul n ale unităţii. Definim aplicaţia

$$f : G \to \mathbb{Z}_n$$

care-l duce pe σ în i. Cum α generează L acţiunea lui σ este determinată de acţiunea pe α deci f este injectivă. Grupul Galois este tranzitiv pe rădăcini, deoarece $X^n - a$ este ireductibil deci f este surjectivă.

Fie σ şi $\tau \in G$, $f(\sigma) = i$ şi $f(\tau) = j$. Deci $\sigma(\alpha) = \omega^i\alpha$ şi $\tau(\alpha) = \omega^j\alpha$. În acest caz

$$\begin{aligned}(\tau \circ \sigma)(\alpha) &= \tau(\sigma(\alpha)) \\ &= \tau(\omega^i\alpha) \\ &= \omega^i\tau(\alpha) \\ &= \omega^i\omega^j\alpha \\ &= \omega^{i+j}\alpha.\end{aligned}$$

Rezulta că f este homomorfism de grupuri, deci f este izomorfism.

Presupunem acum că G este ciclic cu generatorul σ. Atunci automorfismele

$$1, \sigma, \sigma^2, ..., \sigma^{n-1}$$

sunt distincte, şi deci independente peste L. Deci

$$1 + \omega\sigma + \omega^2\sigma^2 + ... + \omega^{n-1}\sigma^{n-1} \neq 0.$$

Deci $\exists\beta \in L$ astfel încât

$$\alpha = \beta + \omega\sigma(\beta) + \omega^2\sigma^2(\beta) + ... + \omega^{n-1}\sigma^{n-1}(\beta) \neq 0.$$

Observam că $\sigma(\alpha) = \omega^{-1}(\alpha)$. Fie $a = \alpha^n$. Atunci a este invariat de σ, din G, $a \in K = L^G$. G acţionează tranzitiv pe rădăcinile lui $X^n - a$, care sunt $\omega^i\alpha$ deci $X^n - a$ este ireductibil. Deci α are gradul n peste K deci $L = K(\alpha)$.

11.0.0.83 Corolar. *Fie $X^p - a \in K[X]$, unde p este un număr prim coprim cu caracteristica şi $X^p - 1$ se descompune în K.*

Atunci ori $X^p - a$ se descompune în K ori $X^p - a$ este ireductibil.

Demonstraţie. Fie L/K corpul de descompunere al $X^p - a$. Atunci grupul Galois G este un subgrup al $\mathbb{Z}_p$, deoarece α este o rădăcină a lui $X^p - a$ rezultă că acţiunea oricărui element din G îl trimite pe α în $\omega^i \alpha$, unde $i \in \mathbb{Z}_p$ ca mai sus. Deci ori G este grupul trivial, cînd $X^p - a$ se descompune în K ori $G = \mathbb{Z}_p$, cînd grupul Galois acţionează tranzitiv pe rădăcinile lui $X^p - a$ şi $X^p - a$ este ireductibil.

12 Rezolvabilitatea prin radicali

12.0.0.84 Definiţie. *Şirul de grupuri*

$$e = G_0 \subset G_1 \subset G_2 \subset ... \subset G_n = G$$

se numeşte ***rezolubil*** *dacă toţi factorii sai sunt grupuri abeliene.*

Un grup G se numeşte ***rezolubil*** *dacă contine un şir rezolubil.*

12.0.0.85 Propoziţie. *Fie L/K corp de descompunere al polinomului $X^n - a \in K[X]$, unde n este coprim cu caracteristica.*

Atunci grupul Galois este rezolubil.

Demonstraţie. Fie $L/M/K$ corp de descompunere pentru $X^n - 1$ şi H subgrupul corespunzător al lui G. Atunci H este grupul Galois al lui L/M, H este normal în G şi G/H este grupul Galois al M/K. Am văzut deja că G/H este abelian. Deci este suficient să demonstrăm că H este rezolubil. În particular putem să considerăm că $X^n - 1$ se descompune în K. Fie $n = lm$. Fie $L/M/K$ corp de descompunere pentru $X^m - a$. Atunci M/K este normală deci subgrupul corespunzător H al lui G este normal de asemenea. Extinderea L/M este un corp de descompunere pentru $X^l - b$ unde $b^m = a$. Cum

$$0 \to H \to G \to G/H \to 0$$

este o secvenţa exactă (imaginea uneia este nucleul celeilalte), şi grupurile din capete sunt grupuri Galois pentru $X^n - b$ şi $X^n - a$, reducem problema la cazul cînd n este prim.

Deci putem considera $X^n - a$ ireductibil, caz în care G este abelian.

12.0.0.86 Definiţie. *Fie $f(x) \in K[X]$ polinom.*

Spunem că $f(x)$ este rezolvabil prin radicali dacă exista un şir de extinderi

$$K = R_0 \subset R_1 \subset R_2 \subset ... \subset R_n$$

astfel încât $R_i = R_{i-1}(\alpha_i)$, unde $a_i = \alpha_i^{m_i} \in R_i$ pentru un m_i coprim cu caracteristica şi $f(x)$ se descompune în R_n.

12.0.0.87 Lema. *Fie $f(x) \in K[X]$ rezolvabil prin radicali.*

Atunci putem găsi un şir de extinderi ca în 12.0.0.86 astfel încât R_n/K este Galois.

Demonstraţie. Avem

$$K = S_0 \subset S_1 \subset ... \subset S_n$$

astfel încât $S_i = S_{i-1}(\alpha_i)$, unde $a_i = \alpha_i^{m_i} \in S_i$ pentru un m_i coprim cu caracteristica şi $f(x)$ se descompune în S_n.

Fie R_1 corpul de descompunere al lui $X^{m_1} - a_1$. Evident S_1 este (izomorf cu) o submulţime a lui R_1. Atunci R_1 contine un corp de descompunere pentru $X^n - 1$, M_1 şi cele doua extinderi R_1/M_1 şi M_1/K sunt radicale.

Acum fie polinomul $X^{m_2} - a_2$. $a_2 \in K$ dar nu neapărat şi lui K. Pe de alta parte

$$\prod_{\phi \in G} (X^{m_2} - \phi(a_2))$$

este invariant sub acţiunea Grupului Galois G al extinderii R_1/K şi deci este din $K[X]$. Fie R_2/R_1 extindere a unui corp de descompunere. Atunci R_2/K este Galois şi evident R_2/K este o succesiune de extinderi radicale. Prin inducţie obţinem rezultatul.

12.0.0.88 Lema. *Fie L/K extindere finită de corpuri şi $L/M/K$ şi $L/N/K$ doua corpuri intermediare astfel încât L este corpul generat de M şi N. M/K este Galois cu grupul Galois G.*

Atunci L/N este Galois, cu grupul Galois I izomorf cu

$$H = Gal(M/M \cap N) \subset G.$$

Demonstraţie. Fie M/K corpul de descompunere al $f(x)$. Atunci şi L/N este corp de descompunere deoarece $f(x)$ este separabil. În particular L/N este Galois.

Fie $\sigma \in I$. Atunci σ este automorfism al L/K. Cum M/K este normală, $\sigma|_M$ este automorfism al M/K. Deci avem un homomorfism de grupuri

$$\rho : I \to G.$$

Fie $a_1, a_2, a_3, ..., a_n$ rădăcinile lui $f(x)$. $\rho(\sigma)$ este aplicaţia identică dacă acţionează identic pe rădăcini. Atunci σ este de asemenea identitatea. Rezulta că ρ este injectivă. Este evident că $\rho(\sigma)$ fixează $M \cap N$, deci imaginea lui ρ este subgrup în H. Pe de alta parte dacă $\alpha \notin N$, atunci exista σ care nu-l fixează pe α. Deci corpul fixat al imaginii este conţinut în $M \cap N$.

12.0.0.89 Teorema (criteriu de rezolvabilitate). *Fie $f(x) \in K[X]$ polinom separabil al cărui grup Galois are ordinul n coprim cu caracteristica.*

Atunci $f(x)$ este rezolvabil prin radicali dacă grupul sau Galois este rezolubil.

Demonstraţie. Presupunem că grupul Galois este rezolubil. Fie $\bar{K}$ închiderea algebrică a lui K. Fie L'/K extinderea obţinută prin adjuncţionarea a n rădăcini ale unităţii, şi fie N subcorpul lui $\bar{K}$ care contine atât L cat şi L'. Atunci L'/K este extindere radicală şi extinderea N/L' este izomorfă cu un subgrup al lui G.

Putem deci să spunem că $X^n - 1$ se descompune în K. Cum G este rezolubil putem găsi un şir de subgrupuri, fiecare normal în următorul, cu factorul un grup ciclic de ordin prim. Deci exista secvenţa de extinderi

$$K = R_0 \subset R_1 \subset R_2 \subset ... \subset R_n = L$$

unde R_i/R_{i-1} este extindere de grad $p = p_i$ prim, astfel încât $X^p - 1$ se descompune în K. Atunci R_i/R_{i-1} este corp de descompunere pentru $X^p - a$ pentru un $a \in R_{i-1}$.

Fie $f(x)$ rezolubil prin radicali. Fie L/K corp de descompunere pentru $f(x)$ şi N/L extindere Galois a lui K, o succesiune de extinderi radicale. Atunci grupul Galois al lui N/K este rezolubil şi G este factorul unui grup rezolubil, deci el însuşi rezolubil.

12.0.0.90 Lema. *Fie $f(x)$ polinom raţional ireductibil de grad prim p cu exact doua rădăcini nereale.*

Atunci grupul Galois G al $f(x)$ peste $K = \mathbb{Q}$ este grupul simetric S_p.

Demonstraţie. Acţiunea grupului Galois este determinată de acţiunea să pe rădăcini. Trebuie să verificam doar dacă obţinem întregul S_p. Este suficient să demonstrăm că G contine un p-ciclu şi o transpoziţie.

Fie L/K corp de descompunere pentru $f(x)$. Fie a o rădăcină a lui $f(x)$. Atunci $M = K(a)/K$ are gradul p. Rezulta din legea turnurilor că gradul extinderii L/K este divizibil cu p. Deci grupul Galois are ordinul divizibil cu p şi din teorema lui Sylow G contine un element de ordinul p. Cum $G \subset S_p$, şi singurele elemente de ordinul p ale lui S_p sunt p-cicluri rezultă că G contine un p ciclu.

Deoarece $f(x)$ este polinom real, conjugarea complexă acţionează pe rădăcinile lui. Deoarece sunt exact doua rădăcini complexe, conjugarea complexă corespunde unei transpoziţii.

12.0.0.91 Teorema (Abel-Ruffini). *Pentru $n \geq 5$ ecuaţia de gradul n peste un corp K*

$$f(x) = (X - y_1)(X - y_2)...(X - y_n)$$

nu poate fi rezolvată ***prin radicali****.*

Demonstraţie. Am văzut că $E = K(y_1, ..., y_n)$ este corpul funcţiilor raţionale în n variabile cu coeficienţi în K, şi dacă $F = K(a_0, ..., a_{n-1})$, unde a_i sunt coeficienţii lui $f(x)$, atunci E este corpul de descompunere al lui $f(x)$ peste F.

Demonstrăm întâi că $Gal(E/F) \simeq S_n$. Ştim că dacă A şi R sunt domenii de integritate şi $\varphi : A \to R$ este izomorfisme atunci $a/b \to \varphi(a)/\varphi(b)$ este un izomorfism al corpurilor de fracţii $Frac(a) \to Frac(R)$. În particular, dacă $\sigma \in S_n$ atunci exista un automorfism $\tilde{\sigma}$ al $K[y_1, ..., y_n]$ definit de $\tilde{\sigma} : f(y_1, ..., y_n) \to f(y_{\sigma_1}, ..., y_{\sigma_n})$ adică $\tilde{\sigma}$ doar permute variabilele şi $\tilde{\sigma}$ se extinde la un automorfism σ^* al $E = Frac(K[y_1, ..., y_n])$. Ecuaţiile lui Viete arată că σ^* fixează F şi deci $\sigma^* \in Gal(E/F)$. Deoarece σ este determinată de acţiunile pe rădăcini $\sigma \to \sigma^*$ este o injecţie $S_n \to Gal(E/F)$, deci $|S_n| \leq |Gal(E/F)|$. Pe de alta parte am văzut că grupul Galois este izomorf cu un subgrup al S_n şi de aici obţinem inegalităţi inversa $|S_n| \geq |Gal(E/F)|$ deci $Gal(E/F) \simeq S_n$. Cum S_n nu e grup rezolubil pentru $n \geq 5$ rezulta că $f(x)$ nu este rezolvabil prin radicali.

13 Ecuaţii de gradul trei şi patru

13.0.0.92 Lema. *Fie $f(x) \in K[X]$ polinom separabil de grad n. Atunci grupul sau Galois este un subgrup al S_n, grupul de permutări al rădăcinilor.*

Demonstraţie. Evident, deoarece orice automorfism al unui corp de descompunere este determinat de acţiunea să pe rădăcini.

$A_n \subset S_n$ deci $H = G \cap A_n \subset G$ este egal fie cu G ori de index doi. În cazul din urma, din teorema fundamentală rezultă că exista o extindere de grad doi M/K.

13.0.0.93 Definiţie. Fie $f(x) \in K[X]$ un polinom care se descompune

$$f(x) = l(X - a_1)(X - a_2)...(X - a_n).$$

Se numeşte **discriminantul** Δ pătratul produsului

$$\delta = \prod_{i<j}(a_i - a_j).$$

13.0.0.94 Lema. *Fie $f(x) \in K[X]$ polinom cu corpul de descompunere L/K şi discriminantul $\Delta \in L$.*

$\Delta = 0$ dacă $f(x)$ are rădăcini multiple. Mai mult dacă $\Delta \neq 0$ atunci $\Delta \in K$ şi $X^2 - \Delta$ se descompune în $K[X]$ dacă grupul Galois este un subgrup al A_n.

Demonstraţie. Dacă $\Delta \neq 0$ atunci $f(x)$ este separabil şi L/K este Galois.

Ştim că δ este invariant sub acţiunea A_n şi că orice element din S_n îl fixează pe δ pană la un semn. Deci $\Delta = \delta^2$ aparţine unui corp fixat de G, şi din teorema fundamentală a teoriei lui Galois acesta este K.

În sfîrşit, $X^2 - \Delta$ se descompune în K dacă $\delta \in K$, adică δ este invariat de G adică $G \in A_n$.

13.0.0.95 Definiţie. *Fie K corp şi $l_1, l_2, l_3, ..., l_n$ n scalari. Determinantul*

$$\begin{vmatrix} 1 & 1 & 1 & ... & 1 \\ l_1 & l_2 & l_3 & ... & l_n \\ l_1^2 & l_2^2 & l_3^2 & ... & l_n^2 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ l_1^{n-1} & l_2^{n-1} & l_3^{n-1} & ... & l_n^{n-1} \end{vmatrix}$$

*Se numeşte **determinant Vandermonde**.*

13.0.0.96 Lema. *Determinantul Vandermonde este egal cu*

$$\begin{vmatrix} 1 & 1 & 1 & ... & 1 \\ l_1 & l_2 & l_3 & ... & l_n \\ l_1^2 & l_2^2 & l_3^2 & ... & l_n^2 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ l_1^{n-1} & l_2^{n-1} & l_3^{n-1} & ... & l_n^{n-1} \end{vmatrix} = \prod_{i<j}(l_i - l_j).$$

Demonstraţie. Putem înlocui l_i cu variabila X_i. În acest caz ambii termeni ai egalitaţii sunt polinoame simetrice în $X_1, X_2, X_3, ..., X_n$, elemente ale inelului $R = K[X_1, X_2, ..., X_n]$. Deoarece factorizarea este unică şi consideraţii de grad este suficient să demonstrăm $X_i - X_j$ este factor al termenului din stânga, adică acesta dispare cînd $l_i = l_j$ (evident, avem doua coloane egale), şi că coeficienţii se potrivesc.

13.0.0.97 Observaţie. *Cu ajutorul determinantului Vandermonde putem verifica dacă A_n este subgrup normal verificînd dacă o transpoziţie ce acţionează pe δ schimba semnul ceea ce este evident din proprietăţile determinantului (schimba semnul cînd interschimbăm doua coloane).*

$$\begin{aligned} \Delta &= \delta^2 \\ &= \delta \cdot \delta \\ &= \begin{vmatrix} 1 & 1 & 1 & ... & 1 \\ a_1 & a_2 & a_3 & ... & a_n \\ a_1^2 & a_2^2 & a_3^2 & ... & a_n^2 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a_1^{n-1} & a_2^{n-1} & a_3^{n-1} & ... & a_n^{n-1} \end{vmatrix} \cdot \begin{vmatrix} 1 & 1 & 1 & ... & 1 \\ a_1 & a_2 & a_3 & ... & a_n \\ a_1^2 & a_2^2 & a_3^2 & ... & a_n^2 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a_1^{n-1} & a_2^{n-1} & a_3^{n-1} & ... & a_n^{n-1} \end{vmatrix} \\ &= \begin{vmatrix} 1 & 1 & 1 & ... & 1 \\ a_1 & a_2 & a_3 & ... & a_n \\ a_1^2 & a_2^2 & a_3^2 & ... & a_n^2 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a_1^{n-1} & a_2^{n-1} & a_3^{n-1} & ... & a_n^{n-1} \end{vmatrix} \cdot \begin{vmatrix} 1 & a_1 & a_1^2 & ... & a_1^{n-1} \\ 1 & a_2 & a_2^2 & ... & a_2^{n-1} \\ 1 & a_3 & a_3^2 & ... & a_3^{n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & a_n & a_{n1}^2 & & a_n^{n-1} \end{vmatrix}. \end{aligned}$$

Am folosit faptul că transpunerea nu afectează determinantul.

13.0.0.98 Propoziţie. *Fie $f(x) \in K[X]$ polinom ireductibil de grad trei.*

Atunci grupul sau Galois este izomorf cu A_3 dacă $X^2 - \Delta$ se descompune în K şi este egal cu S_3 altfel.

Demonstraţie. Grupul Galois este un subgrup tranzitiv al S_3, care sunt numai doua, A_3 şi S_3. Dar $G \subset A_3$ dacă $X^2 - \Delta$ se descompune în K.

Aceasta ne oferă o metoda de rezolvare a ecuaţiei de gradul trei. Mai întâi calculăm corpul intermediar M corespunzător lui A_3 adică adjuncţionăm $\sqrt{\Delta}$. Rezultatul este o extindere de corpuri care are grupul Galois izomorf cu $\mathbb{Z}_3$ deci trebuie să existe o expresie care implica δ şi coeficienţii ecuaţiei din care să extragem rădăcină de ordinul trei.

13.0.0.99 Propoziţie. *Fie $f(x) \in K[X]$ polinom ireductibil de gradul patru.*

Atunci grupul sau Galois este izomorf cu

1. *S_4 (grupul simetric),*
2. *D_4 (grupul diedral),*
3. *$\mathbb{Z}_4$,*
4. *A_4 sau*
5. *$V = \{e, (1,2)(3,4), (1,3)(2,4), (1,4), (2,3)\}$.*

Ultimele doua au loc cînd $X^2 - \Delta$ se descompune în K.

Demonstraţie. Grupurile de mai sus sunt singurele tranzitive ale S_4.

Aceasta la fel ne oferă o metoda de rezolvare a ecuaţiilor de grad patru. Întâi adjuncţionăm $\delta = \sqrt{\Delta}$ pentru a reduce grupul Galois la A_4. Folosim faptul că $V \subset A_4$ este subgrup normal cu factorul $\mathbb{Z}_3$ ca să găsim mai departe o extindere de corpuri obţinută prin adjuncţionarea rădăcinilor potrivite. Reducem astfel grupul Galois la $\mathbb{Z}_2 \times \mathbb{Z}_2$. Extinderea care mai rămîne este obţinută prin adaugarea succesivă de rădăcini pătrate.

Deci forma generală a soluţiei unei ecuaţii de grad patru implica numai radicali de ordinul doi şi patru.

Partea IV
Aplicaţii

13.0.0.100 Exerciţiu. *Polinomul $X^5 - 6x + 3$ nu este rezolvabil prin radicali.*

Rezolvare. Este suficient să demonstrăm că polinomul este ireductibil şi are trei rădăcini reale.

Ireductibilitatea rezultă din criteriul lui Eisenstein. $f(0) = 3$, $f(-3) < 0$ şi $f(2) > 0$ şi din teorema valorii intermediare $f(x)$ are cel puţin trei rădăcini reale. Zerourile reale ale funcţiei sunt intercalate cu zerourile derivatei $f(x) = 5X^4 - 6$, care are numai doua rădăcini reale.

13.0.0.101 Exerciţiu. *Sa se calculeze grupul Galois al polinomului $X^6 - 1$ peste $\mathbb{Q}$.*

Rezolvare. Din 11.0.0.79 G este izomorf cu U_6. Dintre numerele $1, 2, 3, 4, 5$ numai 1 şi 5 sunt coprime cu 6. Deci G are ordinul doi şi este izomorf cu $\mathbb{Z}_2$.

13.0.0.102 Exerciţiu. *Calculul de grupuri Galois.*

Rezolvare. Fie $L = \mathbb{C}/\mathbb{R}$. Atunci L/K este Galois (de grad doi) şi grupul Galois are ordinul doi. $L = \mathbb{R}(i)$. i este rădăcină a $X^2 - 1$, ireductibil, şi orice automorfism al L/K trebuie sa-l ducă pe i într-o alta rădăcină. Avem numai doua rădăcini posibile, $\pm i$. Una da identitatea şi cealaltă conjugarea complexă.

Similar pentru orice alta extindere de grad doi.

Sa calculăm grupul Galois al $X^4 - 2$ peste $K = \mathbb{Q}$. Pentru aceasta ne uităm la corpul de descompunere L/K al $X^4 - 2$ şi calculăm acest grup Galois.

Calculăm întâi corpul de descompunere. Întâi trebuie să adjuncţionăm o rădăcină de gradul 4 a lui 2. Fie aceasta a. Obţinem $M = K(a)$ şi cum $X^4 - 2$ este ireductibil avem o extindere de grad 4. Adăugăm acum o rădăcină primitivă de ordinul 4 a unităţii. O notăm i şi $i^2 = -1$. Putem alege a astfel încât să fie reală. Atunci $i \notin M$ şi L/M extindere de grad 2. Din legea turnurilor avem o extindere de grad 8. L/K este separabilă deoarece $X^4 - 2$ este separabil (caracteristica zero).

Deci $|G| = 8$. Căutăm generatori şi relaţii. Fie extinderea $L = M(i)/M$. Aceasta are ordinul doi şi exista un automorfism τ care-l fixează pe M (adică

pe a) care interschimbă i cu $-i$. Deci un automorfism al L/K este dat de τ unde acţiunea lui τ pe generatori este

$$\tau(a) = a \qquad si \qquad \tau(i) = -i.$$

În al doilea rînd exista un automorfism σ al L/K care duce a în orice alta rădăcină, în particular în ia. σ nu trebuie neapărat să fixeze i. Dacă nu-l fixează atunci $\tau\sigma$ fixează i şi duce a în $-ia$. Atunci σ duce a în ia. Deci

$$\sigma(a) = ia \qquad si \qquad \sigma(i) = i.$$

$\sigma^4 = 1$ şi $\tau^2 = 1$. În particular σ şi τ generează doua subgrupuri ale lui G de ordinul 4 şi 2. Rezulta că σ şi τ sunt generatorii lui G. Pentru a afla relaţiile este suficient să calculăm conjugatul lui σ prin τ, $\tau\sigma\tau$. Acesta îl duce pe i în i şi pe a în $-ia$. Deci $\tau\sigma\tau^{-1} = \sigma^3$. Deci descrierea lui G este:

Generatori: σ şi τ.

Relaţii: $\sigma^4 = \tau^2 = e$, $\tau\sigma\tau^{-1} = \sigma^3$.

Recunoaştem grupul diedral de ordinul opt D_4, simetriile pătratului. Acţiunea lui G este determinată de acţiunea pe cele patru rădăcini $\pm a, \pm ia$ care se aranjează într-un pătrat în planul complex.

Acum listăm subgrupurile şi corpurile intermediare. Am calculat deja subgrupurile lui D_4. Fie H un subgrup. Atunci ordinul lui H divide ordinul lui G deci $|H| \in \{1, 2, 4, 8\}$. Pentru 1 şi 8 avem grupul trivial şi întregul D_4.

Fie $|H| = 2$. Atunci H este generat de un element de ordinul doi. Sunt cinci astfel de elemente: cele doua răsturnări diagonale, cele doua răsturnări diagonale şi rotaţia la 180°. Deci H este unul din

$$< \tau >, \quad < \sigma^2\tau >, \quad < \sigma\tau >, \quad < \sigma^3\tau >, \quad < \sigma^2 > .$$

Acum fie $|G| = 4$. O posibilitate este $< \sigma >$ sau încercăm să combinăm elemente de ordin doi. Orice subgrup al lui G de ordin patru are indexul doi, şi orice subgrup de index doi este normal. Dacă H este de ordinul patru atunci este normal în G. Dar un subgrup H al lui G este normal dacă este o reuniune de clase de conjugare. Răsturnarile pe diagonală respectiv laterale sunt în aceeaşi clasă de conjugare, deci putem să le combinăm, doua diagonale sau doua laterale fără a combina diagonal cu lateral. Deci subgrupurile de grad patru sunt

$$< \sigma >, \quad < \tau, \sigma^2 >, \quad < \sigma\tau, \sigma^2 > .$$

Acum corpurile corespunzătoare. La extreme avem $\mathbb{Q}$ şi $\mathbb{Q}(a, i)$ corespunzătoare lui G respectiv $\{e\}$. Dacă $M/\mathbb{Q}$ este de grad patru atunci subgrupul

corespunzător H are ordinul patru şi index doi. Deci căutăm trei subcorpuri de grad doi

$$\mathbb{Q}(i), \quad \mathbb{Q}(\sqrt{2}), \quad \mathbb{Q}(i\sqrt{2}).$$

Acestea corespund în ordine subgrupurilor de ordin patru.

Căutăm corpuri intermediare de grad patru. Acestea corespund subgrupurilor de ordin doi deci căutăm cinci astfel de corpuri. Unul evident este $\mathbb{Q}(a)$ corespunzător lui τ. Similar $\mathbb{Q}(ia)$ corespunde lui $\sigma^2\tau$. Mai avem $\mathbb{Q}(i, \sqrt{2})$ corespunzînd lui σ^2. Acum vrem să calcula corpul intermediar asociat lui $\sigma\tau$. Scriem elementele generale din L şi raţionăm cînd aceste sunt fixate de de $\sigma\tau$. Ştim că M contine $\mathbb{Q}(i\sqrt{2})$ deci avem nevoie doar de o baza pentru $\mathbb{Q}(a, i)/\mathbb{Q}(i\sqrt{2})$, aceasta fiind

$$1, \quad a, \quad i, \quad ia.$$

Deci elementul general al lui $\mathbb{Q}(a, i)$ este

$$a + ba + ci + d(ia).$$

care este trimis în

$$a + bia - ci + d(a).$$

Deci $c = 0$ şi $b = d$. Deci corpul fixat corespunzător este $\mathbb{Q}((1 + i)a)$. Similar celălalt corp de grad patru este $\mathbb{Q}((1 - i)a)$.

13.0.0.103 Exerciţiu. *Calculul grupului Galois în corpuri finite.* $f(x) = X^4 + X + 1$ *peste corpul* $\mathbb{F}_2$.

Rezolvare. Problema esenţială este factorizarea lui $f(x)$. $f(x)$ cu siguranţa nu are factori liniari deoarece nu are rădăcini. Presupunem că $f(x)$ ar fi reductibil. Atunci

$$X^4 + X + 1 = (X^2 + aX + b)(X^2 + cX + d)$$

unde $a, b, c, d \in \mathbb{F}_2$. Uitandu-ne la coeficientul lui X^3 avem $c = -a = a$ şi uitandu-ne la coeficientul constant avem $bd = 1$ deci $b = d = 1$. Atunci

$$X^4 + X + 1 = (X^2 + ax + 1)(X^2 + aX + 1) = X^4 + aX^2 + 1$$

contradicţie.

Deci $X^4 + X + 1$ este ireductibil. Fie L corpul de descompunere şi a rădăcină a lui $f(x)$. Atunci $M = \mathbb{F}_2(a)$ este normală, deoarece toate extinderile corpurilor finite sunt normale. Deci $L = M$ şi $L/\mathbb{F}_2$ are gradul patru. Deci grupul Galois este ciclic de ordinul patru.

13.0.0.104 Exerciţiu. *Sa se calculeze* Φ_6.

Rezolvare. Din Euler

$$\begin{aligned}\Phi_1\Phi_2\Phi_3\Phi_6 &= X^6-1\\ &= (X^3)^2-1\\ &= (X^3-1)(X^3-1)\\ &= (X^3-1)(X+1)(X^2-X+1).\end{aligned}$$

Deci $\Phi_6 = X^2-X+1$.

Bibliografie

[1] Artin E., Arthur N. Milgram *Galois Theory* Dover Publications Inc, 1998

[2] Dummit David S., R. M. Foote *Abstract Algebra* John Wiley & Sons, 2005

[3] Ion D. Ion, N. Radu *Algebra* Editura didactică şi pedagogică, 1991

[4] Lean-Pierre Tignol *Galois' Theory of Algebraic Equations* World Scientific, 2001

[5] Năstăsescu C., Niţă C. *Teoria calitativă a ecuaţiilor algebrice* Editura Tehnica, 1979

[6] Rotman, J. *Advanced Modern Algebra* Prentice Hall, 2003