TEORIA LUI GALOIS

I ELEMENTE ALGEBRICE ŞI TRANSCENDENTE. EXTINDERI ALGEBRICE

Definiţie. Dacă K şi k sunt două corpuri astfel încât k este un subcorp al lui K, spunem că K este o **extindere** a lui k şi se notează: $k \subset K$.

Fie k un corp, K o extindere a sa şi M o submulţime a lui K. Intersecţia tuturor subcorpurilor lui K care conţin pe k şi submulţimea M, este un subcorp al lui K şi o extindere a lui k care conţine mulţimea M. Acest subcorp al lui K se notează cu k(M) şi este corpul obţinut prin adjuncţionare la k a elementelor mulţimii M. Corpul k(M) este corpul de fracţii al inelului k[M] generat peste k de mulţimea M.

Fie I o mulţime; notăm cu k(X; I) corpul său de fracţii; acesta poate fi privit ca obţinut prin adjuncţionare la k a nedeterminatelor $X_i, i \in I$.

Definiţie O **extindere** K a unui corp k se numeşte de **tip finit** dacă există o submulţime finită M a lui K, astfel încât k(M) = K.

Dacă există un element $x \in K$ astfel încât K =k(x), atunci K se numeşte extind ere **simplă** a lui k.

Fie K un corp şi $\alpha_1, \alpha_2, \ldots, \alpha_n$ numere complexe arbitrare. Considerăm toate corpurile care sunt extinderi ale lui K şi care conţin numerele $\alpha_1, \alpha_2, \ldots, \alpha_n$. Asfel de corpuri există, deoarece, de exemplu, printre acestea se află corpul C al numerelor complexe. Intersecţia tuturor acestor corpuri este, de asemenea, un corp şi este cea mai mică extindere a lui K, ce conţine numerele $\alpha_1, \alpha_2, \ldots, \alpha_n$; se notează cu $K(\alpha_1, \alpha_2, \ldots, \alpha_n)$ şi se numeşte **extinderea generată de numerele** $\alpha_1, \alpha_2, \ldots, \alpha_n$.

O **extindere** K a lui k se numeşte **finit generată**, dacă există elementele $\alpha_1, \alpha_2, \ldots, \alpha_n$, astfel încât $K = k(\alpha_1, \alpha_2, \ldots, \alpha_n)$.Se verifică uşor că:

1) $k(\alpha_1, \alpha_2, \ldots, \alpha_n) = k$, dacă şi numai dacă $\alpha_1, \alpha_2, \ldots \alpha_n \in k$;

2) $k(\alpha_1, \alpha_2, \ldots, \alpha_n) = k(\alpha_1, \ldots, \alpha_i)\ (\alpha_{i+1}, \ldots, \alpha_n)$ pentru orice $1 \leq i \leq n$;

3) Dacă K este o extindere finită a lui k cu baza $\alpha_1, \alpha_2, \ldots, \alpha_n$, atunci $K = k(\alpha_1, \alpha_2, \ldots, \alpha_n)$, adică este finit generată.

Notăm cu $k[\alpha_1, \alpha_2, \ldots, \alpha_n] = \{x \in C /$ există $f \in k[X_1, \ldots, X_n],\ x = f(\alpha_1, \ldots, \alpha_n)\}$. Se observă că $k[\alpha_1, \alpha_2, \ldots, \alpha_n]$ este un subinel al lui C şi este cel mai mic subinel al lui C care conţine corpul k şi elementele $\alpha_1, \alpha_2, \ldots, \alpha_n$ şi că

$$k[\alpha_1, \alpha_2, \ldots, \alpha_n] \subseteq k(\alpha_1, \alpha_2, \ldots, \alpha_n).$$

Propoziţie. Fie k $\subseteq$ K o extindere de corpuri. Sunt adevărate următoarele afirmaţii:

i) k(K) = K, iar k(M) = k dacă şi numai dacă submulţimea M este din k.

ii) Dacă M şi N sunt două submulţimi ale lui K, atunci k (M$\cup$N)=k(M)(N)= = k(N)(M).

iii) Dacă $\{M_i\}_{i \in I}$ este un system de submulţimi ale lui K filtrant la dreapta(adică pentru orice i,j$\in$I, există l $\in$I astfel încât $M_i \subseteq M_l$ şi $M_j \subseteq M_l$) şi M=$\bigcup_{i \in I} M_i$, atunci k(M) = $\bigcup_{i \in I} k(M_i)$.

Demonstraţie.

Afirmaţiile i) şi ii) rezultă direct din definiţia de mai sus. Pentru demonstrarea afirmaţiei din iii) este suficient să observăm că deoarece sistemul { M_i},i$\in$I este filtrant la dreapta, $\bigcup_{i \in I} k(M_i)$ este un subcorp al lui K.

Comentarii. În condiţiile teoremei , se notează de obicei cu k(M, N) corpul k(M $\cup$ N).

Definiţie .O **extindere** K a corpului k se numeşte **finită**, dacă există în corpul K un număr finit de elemente α_1 , α_2 ,….,α_n astfel încât orice element $\beta \in$K se scrie în mod unic sub forma unei combinaţii liniare de elemente, cu coeficienţi în corpul k: β = $a_1 \alpha_1 + \ldots\ldots + a_n \alpha_n$; $a_1,a_2,\ldots,a_n \in$k. Sistemul de elemente α_i , i $\in \{1,\ldots,n\}$, care are această proprietate se numeşte **bază** a extinderii K peste corpul k.Sistemul de elemente $\alpha_1,\ldots..,\alpha_n$ este o bază a lui K peste k, dacă:

1) generează liniar extinderea K peste k.
2) sunt liniar independente peste corpul k.

Propoziţie. Fie K o extindere a corpului k şi $\alpha_1,\ldots..,\alpha_n$, o bază a lui K peste k. Dacă $\beta_1,\ldots..,\beta_m$, sunt elemente din K, astfel încât m>n, atunci există b_1, $b_2,\ldots,b_m \in$ K, nu toate nule, astfel încât: $b_1 \beta_1 + \ldots\ldots + b_m \beta_m = 0$.

În particular, rezultă că două baze ale lui K peste k au acelaşi număr de elemente.

Definiţie. Se numeşte **gradul extinderii** K peste k, numărul elementelor dintr-o bază arbitrară a lui K peste k, şi se notează $[K : k.]$

Observaţii. 1) [K: k] = 1, dacă şi numai dacă K =k.

Intr-adevăr, dacă K =k, atunci [K: k]=1,deoarece 1 este o bază a extinderii K peste k. Reciproc, presupunem [K:k]=1; fie { α } o bază a lui K peste k. Atunci există un a $\in$k, astfel încât 1=aα . Deci $\alpha = a^{-1}$, de unde rezultă că $\alpha \in$k şi deci K =k.

2) Dacă K este o extindere finită a lui k, [K : k] este egal cu dimensiunea lui K peste k, considerat ca spaţiu vectorial.

Propoziţie. Fie k $\subseteq$K $\subseteq$L, extinderi de corpuri. Dacă K este extindere finită a lui k şi L extindere finită a lui K, atunci L este extindere finită a lui k şi în plus [K : k] [L : K] = [L :k] (tranzitivitatea extinderilor finite).

Definiţii. 1) Fie K un corp. Un număr complex α se numeşte **algebric** peste K, dacă există un polinom nenul f $\in$K[X], astfel încât f(α) =0.

2) Un număr comlex α care nu este algebric peste K, se numeşte **transcendent** peste corpul K.

3) Un număr complex α , care este algebric (respectiv transcendent) peste corpul numerelor raţionale Q, se numeşte simplu număr algebric (respec--tiv număr transcendent).

4) Dacă α este algebric peste K, polinomul unitar nenul f $\in$K[X] de grad

cel mai mic, astfel încât f (α) = 0, se numeşte **polinomul minimal** al lui α .

Observaţii. 1) Polinomul minimal al lui α este unic determinat.

2) Polinomul minimal este ireductibil.

Definiţie. O **extindere** K a lui k se numeşte **algebrică** dacă orice element al lui K este algebric peste k.

Exemple : 1) Numărul $\sqrt{2}$ este algebric peste corpul Q, deoarece este rădăcina polinomului $X^2 - 2 \in Q[X]$, care este şi polinomul său minimal.

2) Numărul $\sqrt{2}+\sqrt{3}$ este algebric peste corpul Q, deoarece este rădăcina polinomului $X^4 - 10X^2 + 1 \in Q[X]$, care este şi polinomul său minimal.

3) Corpul numerelor complexe C este o extindere algebrică a corpului numerelor reale R. Într-adevăr, dacă z =a+ib, este un număr complex, atunci z este rădăcina polinomului: $X^2 - 2aX + (a^2+b^2) \in R[X]$. Deducem că [C : R] = 2.

4) Numerele complexe i = $\sqrt{-1}$, $\sqrt{-2}$, $\sqrt[4]{-3}$, $\sqrt{-5}$, (1+i $\sqrt{3}$)/2, sunt numere algebrice, deoarece ele sunt respective rădăcini ale polinoamelor din Q [X]: $X^2 + 1$, X^2+2, X^4+3, X^2+5, X^2+X+1.

5) Numerele e, π sunt transcendente peste corpul numerelor raţionale Q.

Propoziţie. Dacă K este o extindere finită a lui k, atunci K este algebrică peste k.

Demontraţie:Presupunem că n = [K : k] şi fie $\alpha \in K$. Considerăm elementele: 1, α , $\alpha^2, \ldots, \alpha^n$, care sunt în număr de n+1. Atunci există $a_0, a_1, \ldots, a_n \in k$, nu toate nule, astfel încât $a_0+a_1\alpha+a_2\alpha^2+\ldots+a_n\alpha^n = 0$.Polinomul $f = a_0+a_1X+\ldots+a_nX^n$ aparţine lui k [X], şi este nenul. Cum f(α)=0, înseamnă că α este algebric peste k.

Propoziţie. Fie K un corp şi α un număr complex algebric peste K. Atunci K(α) este o extindere finită a lui K şi [K(α) : K] este egal cu gradul polinomului minimal al lui α . În plus, K(α) = K[α], unde K[α] ={g(α) / g$\in$K[X] }.

Corolar. Fie K = k($\alpha_1, \ldots, \alpha_n$) şi $\alpha_1, \ldots, \alpha_n$ algebrice peste k. Atunci K este o extindere finită a lui k.În plus, k(α_1 , …, α_n)=k [$\alpha_1, \ldots, \alpha_n$].

Corolar. Dacă K este o extindere algebrică şi finit generată a lui k, atunci K este o extindere finită a lui k.

Corolar. Dacă E este o extindere algebrică a lui K şi F este o extindere algebrică a lui E, atunci F este o extindere algebrică a lui K.

Definiţie. Fie k un corp şi K o extindere a sa. Corpul k este algebric închis în K, dacă orice element din K, algebric peste, aparţine lui k. Dacă corpul k se consideră ca extindere a lui însuşi, atunci k este, evident, algebric închis în k.

Propoziţie. Dacă k$\subseteq$K este o extindere de corpuri şi k' corpul elementelor din K algebrice peste k, atunci k'este algebric închis în K.

Propoziţie. Fie k un corp. Următoarele afirmaţii sunt echivalente:

a) k este algebric închis;
b) orice polinom de grad ≥ 1 din k[X], are o rădăcină în k;
c) orice polinom de grad ≥ 1 din k[X], are toate rădăcinile în k;
d) orice polinom de grad ≥ 1 din k[X], se descompune în produs finit de factori liniari ;
e) singurele polinoame ireductibile din k[X], sunt cele de grad 1.

Observaţii. 1) Corpul numerelor raţionale Q nu este algebric închis, deoarece polinomul $X^2+1 \in Q[X]$ este ireductibil şi nu este de gradul .

2) Analog, corpul numerelor reale R, nu este algebric închis, deoarece

acelaşi polinom, considerat ca polinom în R[X], este ireductibil.

Propoziţie. Un corp finit nu este algebric închis

Demonstraţie. Fie k un corp finit. Va fi suficient să arătăm că există un polinom de grad >1 în k[X], care nu are nici o rădăcină în k. Considerăm polinomul $f = X(X-1)\prod_{i=0}^{n}(X - a_i) + 1$, unde 0, 1, $a_1,\ldots,a_n$, sunt elementele corpului k .Se observă că f nu are nici o rădăcină în k, căci pentru orice a $\in$ k, avem: f(a) = 1.

Teorema (fundamentală a algebrei sau teorema lui d'Alembert) .

Corpul numerelor complexe este algebric închis.

Propoziţie. Fie k un corp şi K, un corp algebric închis, extindere a corpului k. Atunci Atunci corpul k' al elementelor din K, algebrice peste k, este şi el algebric închis.

Teoremă. Orice corp k are o extindere K care este corp algebric închis.

Corolar. Pentru orice corp k există o extindere algebrică $\bar{k}$ a lui k care este un corp algebric închis.

Definiţie. O extindere algebrică $\bar{k}$ a corpului k, care este algebric închisă, se numeşte închidere algebrică a lui k.

Comentarii. 1) Corolarul precedent, arată că orice corp are o închidere algebrică.

2) Două închideri ale unui corp k sunt k- izomorfe.

Corolar. Fie K un corp. Dacă $\bar{K} = \{ \alpha \in C / \alpha$ algebric peste K$\}$, atunci $\bar{K}$ este un subcorp al lui C.

Demonstraţie.Fie $\alpha, \beta \in \bar{K}$. Avem $\alpha + \beta, \alpha\beta \in K(\alpha, \beta)$.Deoarece $K(\alpha, \beta)$ este o extindere finită a lui K, aceasta este algebrică şi deci $\alpha + \beta, \alpha\beta \in \bar{K}$. Analog, dacă $\alpha \in \bar{K}$ şi $\alpha \neq 0$, atunci $\alpha^{-1} \in K(\alpha)$. Deoarece $K(\alpha)$ este o extindere finită a lui K, ea este şi algebrică. Deci $\alpha^{-1} \in \bar{K}$.

Definiţie. Corpul $\bar{K}$ se numeşte închiderea algebrică a lui K în C. Deci C - $\bar{K}$ este mulţimea numerelor transcendente peste K. În cazul particular K = Q, corpul $\bar{Q}$ se numeşte mulţimea numerelor algebrice.

II GRUPUL LUI GALOIS

Fie K un corp. Notăm cu Aut(K) mulţimea tuturor automorfismelor (unitare) de inel, ale lui K. Aut(K) este un subgrup al lui S(K), al tuturor permutărilor mulţimii K, căci dacă $\sigma, \tau \in$ Aut(K), atunci $\sigma\tau^{-1} \in$ Aut (K).

Definiţie. Fie k un subcorp al lui K. Notăm cu G(K/k) mulţimea acelor elemente $\sigma \in$ Aut(K), care au proprietatea că $\sigma(a) = a$, pentru orice $a \in k$, adică cele care sunt k- automorfisme.

G(K/k) este un subgrup al lui Aut(K), şi-l numim **grupul lui Galois** al extinderii K a lui k.

Definiţii. Fie E şiF două extinderi ale corpului k Un omomorfism(respectiv izomorfism) de corpuri $\sigma : E \to F$ cu proprietatea $\sigma(x)=x$, oricre ar fi $x \in k$, se numeşte k-omomorfism (respective k-izomorfism). Dacă E este o extindere a lui k şi $\sigma : E \to E$ un k-izomorfism, σ se numeşte k- automorfism.

Propoziţie. Dacă E este o extindere algebrică a lui k şi $\sigma : E \to E$ un k-omomorfism, atunci σ este un k-automorfism.

Observaţii. Fie M şi N două mulţimi odonate, relaţiile respective le notăm pe ambele cu $\leq$. Atunci o funcţie $\varphi : M \to N$ se numeşte morfism de mulţimi ordonate (sau omomorfism de mulţimi ordonate sau încă funcţie monotonă), dacă oricare ar fi $x_1, x_2 \in M$, cu $x_1 \leq x_2$, rezută $\varphi(x_1) \leq \varphi(x_2)$ şi antimorfism de mulţimi ordonate (sau antiomomorfism de mulţimi ordonate sau încă funcţie antimonotonă), dacă oricare ar fi $x_1, x_2 \in M$, cu $x_1 \leq x_2$, rezultă $\varphi(x_2) \leq \varphi(x_1)$.Funcţia identică 1_M: $M \to M$ este un morfism de mulţimi ordonate.Morfismul (antimorfismul) φ de mulţimi ordonate se numeşte izomorfism(antiizomorfism) de mulţimi ordonate, dacă există un morfism (respectiv un antimorfism) de mulţimi ordonate $\psi : N \to M$, astfel ca $\varphi\psi = 1_N$ şi $\psi\varphi = 1_M$.

Observaţie. Orice izomorfism (antiizomorfism) de mulţimi ordonate este o funcţie bijectivă. Reciproc, nu.

Propoziţie. Un morfism (antimorfism) $\varphi : M \to N$ de mulţimi ordonate este izomorfism (antiizomorfism), dacă şi numai dacă este o bijecţie, iar pentru $x, x' \in M$, următoarele afirmaţii sunt echivalente:

a) $x \leq x'$

b) $\varphi(x) \leq \varphi(x')$, (respectiv $\varphi(x) \geq \varphi(x')$).

Exemple. 1) Fie Pun corp prim. Atunci Aut(P)este format dint-un singur element, identitatea lui P.

Într-adevăr, dacă P este finit,afirmaţia rezultă din faptul că Peste generat ca grup aditiv de elementul unitate. Dacă P este infinit , el este izomorf cu Q. Orice Automorfism al lui Q induce pe Z automorfismul identic, Z fiind generat ca grup aditiv de 1, care are o singură extindere la Q: automorfismul identic. Mai mult, dacă K este un corp şi P este corpul prim conţinut în K, atunci orice automorfism al lui K induce pe P automorfismul identic. Aşadar, Aut(K) = G(K/P).

2)Fie $Q(i\sqrt{2})$, extinderea lui Q.Să determinăm grupul $G(Q(i\sqrt{2})/Q)$. Fie $u \in G(Q(i\sqrt{2})/Q)$.Atunci $u(r+si\sqrt{2}) = u(r)+u(s)u(i\sqrt{2}) = r+su(i\sqrt{2})$.Deoarece $(i\sqrt{2})^2+2=0$, obţinem $0 =u((i\sqrt{2})^2) +2=(u(i\sqrt{2}))^2 +2$.De aici,deducem că $u(i\sqrt{2})= i\sqrt{2}$ sau $u(i\sqrt{2})= - i\sqrt{2}$.În primul caz u este automorfismul identic, iar în al doilea, este automorfismul definit prin $u(r+si\sqrt{2})=r-si\sqrt{2}$. Deci grupul $G(Q(i\sqrt{2})/Q)$ este format din două elemente, şi prin urmare, este izomorf cu Z_2.

Comentarii. Fie Kun corp, extindere a corpului k, şi H un subgrupal lui G(K/k). Notăm cu K^H elementele $x \in K$ cu proprietatea $u(x)=x$, pentru orice $u \in H$, adică elementele din K care sunt invariate de elementele din H. Se constată că K^H este un subcorpal lui K, care conţine pe k.

Într-adevăr, dacă $x,y \in K^H$, rezultă $u(x-y)=u(x)-u(y)=x-y$, pentru orice $u \in H$, deci $x-y \in K^H$, şi dacă $y \neq 0$, $u(xy^{-1})=u(x).u(y^{-1})=x.y^{-1}$, pentru orice $u \in H$, deci $xy^{-1} \in K^H$.
Dacă $H' \subseteq H$, rezultă $K^{H'} \supseteq K^H$. Se stabileşte astfel o funcţie de la mulţimea subgrupurilor lui G(K/k) la mulţimea extinderilor lui k conţinute în K, funcţie care este antimonotonă, dacă considerăm pe cele două mulţimi ordonarea dată de relaţia de incluziune.
Fie L un subcorp al lui K, care conţine pe k. Acestui corp îi putem asocia grupul G(K/L), care este evident un subgrup al lui G(K/k), iar dacă L' este un alt subcorp al lui K, cu $L' \supseteq L$,atunci $G(K/L') \subseteq G(K/L)$.
Se obţine astfel o funcţie antimonotonă(pentru relaţia de incluziune), de la subcorpurile lui K, care conţin pe k, la subgrupurile grupului lui Galois G(K/k).
În principal, teorema fundamentală a teoriei lui Galois, dă condiţii în care cele două funcţii, definite mai sus, sunt inverse una celeilalte

III CORPURI FINITE

Pentru început vom presupune corpuri care nu sunt comutative, dacă nu se specifică altfel.

Fie $K \subseteq L$ o extindere de corpuri cu un număr finit de elemente; presupunem că corpul K are q elemente. Corpul L este spaţiu vectorial (la stânga) peste K şi fie $r = \dim_K L$.Atunci din faptul că orice element $x \in L$ se scrie, în mod unic, sub forma $x = \sum_{i=1}^{r} a_i x_i$, $x_1, x_2, \ldots, x_r$, fiind o bază a lui L peste K şi $a_i \in K$, deducem că corpul L are q^r elemente. Dacă L' este un subcorp al lui L care conţine pe K şi $s = \dim_K L'$, atunci s divide pe r. Orice corp finit K este de caracteristică $p>0$ şi deci conţine corpul prim Z_p, deci K va avea p^n elemente, unde $n = \dim_{Z_p} K$.

Teoremă. Orice subgrup finit al grupului multiplicativ al elementelor nenule dintr-un corp comutativ este ciclic.

Lemă. Fie G un grup comutativ şi a_i, $i=1,2,\ldots,k$, elemente din G, de ordin respectiv n_i, $i=1,2,\ldots,k$, astfel încât numerele naturale n_i să fie relativ prime două câte două.

Atunci ordinul elementului $a = \prod_{i=1}^{k} a_i$ este egal cu $\prod_{i=1}^{n} n_i$.

Comentarii. Fie K un corp comutativ algebric închis, de exponent caracteristic p şi $n>1$ un număr întreg cu proprietatea $(p,n)=1$. **Notăm cu U_n mulţimea rădăcinilor polinomului $X^n - 1$ în K. Elementele lui U_n se numesc rădăcini de grad n ale unităţii în K**. Se verifică, că U_n cu înmulţirea din K, este grup, numit **grupul rădăcinilor de grad n ale unităţii** din K. U_n are n elemente. Din teorema precedentă, rezultă că U_n este grup ciclic şi deci este izomorf cu Z_n..

Orice generator al grupului U_n se numeşte **rădăcină primitivă de grad n a unităţii.** Numărul acestor rădăcini este $\varphi(n)$, unde φ este funcţia lui Euler.

Comentarii.

Definiţie. Fie n>1 un număr natural; notăm cu $\varphi(n)$ numărul numerelor naturale nenule mai mici decât n şi prime cu n. Acest număr se numeşte **indicatorul lui Euler.**

Teorema(lui Euler). Fie n număr natural >1, şi a un număr întreg prim cu n. Atunci $a^{\varphi(n)} \equiv 1 \pmod n$.

Corolar. **(Teorema lui Fermat)**

Dacă p>1 este număr natural prim şi a un număr întreg care nu se divide cu p, atunci $a^{p-1} \equiv 1 \pmod p$

Propoziţie. Fie n>1, un număr întreg şi $n = p_1^{k_1} p_2^{k_2} \dots p_r^{k_r}$, descompunerea sa în produs de numere prime, unde $p_1,\dots,p_r$ sunt distincte. Atunci $\varphi(n) = n(1-\frac{1}{p_1})(1-\frac{1}{p_2})\dots(1-\frac{1}{p_r})$.

Dacă ξ este o rădăcină primitivă de grad n a unităţii şi m un număr întreg relativ prim cu n, atunci, ξ^m este încă o rădăcină primitivă de grad n a unităţii, căci ordinul lui ξ coincide cu ordinul lui ξ^m.Mai mult, toate rădăcinile primitive de ordinul n ale unităţii sunt de această formă, căci ele sunt în număr de $\varphi(n)$.

În continuare, vom considera cazul în care K = C. Dacă ξ este o rădăcină primitivă de grad n a unităţii din C,atunci corpul $Q(\xi)$, care este corpul de descompunere al polinomului X^n-1 în C peste Q,se numeşte al **n – lea corp ciclotomic.**

Lemă. Fie Aun inel factorial, K corpul său de fracţii, x un element dintr-o extindere a lui K, care este rădăcină a unui polinom unitar $h \in A[X]$.
Atunci polinomul minimal al lui x peste K, are coeficienţii în A.

Teoremă. Fie ξ o rădăcină de grad n a unităţii din C, şi fie f polinomul minimal al lui ξ (peste Q). Atunci $f \in Z[X]$ şi este polinomul minimal al oricărei rădăcini primitive de grad n a unităţii. În plus, gradul lui f este egal cu $\varphi(n)$, şi deci $[Q(\xi) : Q] = \varphi(n)$.

Comentarii.

1) Polinomul minimal al unei rădăcini primitive a unităţii(şi deci al tuturor rădăcinilor primitive), de grad n, se numeşte al **n-lea polinom ciclotomic**, şi se notează cu $\mathbf{F_n}$(sau cu Φ_n).

Deoarece orice rădăcină primitivă de grad $d \geq 1$, a unităţii, cu d divide pe n, este şi o rădăcină de grad n a unităţii, şi orice rădăcină de grad n a unităţii, este o rădăcină primitivă de grad d a unităţii, pentru un d convenabil, d divide pe n, iar $(F_d, F_{d'}) = 1$ dacă d şi d' sunt divizori distincţi ai lui n, rezultă că avem relaţia: $X^n - 1 = \prod_{d/n} F_d$, $d \geq 1$. Ţinând seama de egalitatea gradelor, rezultă: $n = \sum_{d/n} \varphi(d)$, $d \geq 1$.

2) Fie Gun grup şi C(G), centrul grupului G, adică mulţimea elementelor din G care comută cu orice element din G. Se constată că C(G) este subgrup abelian şi orice subgrup al lui C(G) este subgrup normal al lui G.

Definiţie. Pentru un element $a \in G$, notăm cu $C(a) = \{x \in G / ax = xa\}$. C(a) este un subgrup în G şi se numeşte **centralizatorul** elementului a.

Pentru un grup G se introduce următoarea relație de echivalență: dacă $a,b \in G$, spune că a este conjugat cu b, dacă $x \in G$ astfel încât $x^{-1}ax=b$. Clasele de echivalență sociate acestei relații de echivalență, se numesc clase de elemente conjugate.

Pentru fiecare element $a \in G$, aplicația care asociază unui element $x \in G$, elementul $x^{-1}ax$, din clasa de echivalență a lui a este evident surjectivă şi se verifică imediat că relația de echivalență asociată cestei aplicații coincide cu relația de echivalență la dreapta, asociată centralizatorului elementului a.

Într-adevăr, relația $x^{-1}ax=y^{-1}ay$ este echivalentă cu relația : $yx^{-1}a=ayx^{-1}$, adică cu $yx^{-1} \in C(a)$. De aici, rezultă că numărul elementelor din clasa de elemente conjugate cu a coincide cu indicele centralizatorului elementului a. Dacă notăm cu [G:N] indicele subgrupului N al grupului G, rezultă: $[G:(1)] = [C(G):(1)]+\sum_a [G:C(a)]$, unde suma se extinde după elementele unui sistem de reprezentanți ai claselor de elemente conjugate, care nu aparțin lui C(G). Această relație este cunoscută sub numele de formula claselor de elemente conjugate.

Teoremă. (Wedderburn). Orice corp finit este comutativ.

Teoremă. Două corpuri finite cu acelaşi număr de elemente sunt izomorfe.

Comentarii. Fie Kun corp de caracteristică p>0. Aplicația $u: K \to K$, definită prin:$u(x)=x^p$, este un endomorfism de inel al lui K, numit **endomorfismul lui Frobenius**, căci, pentru $x,y \in K$, avem evident u(xy)=u(x)+u(y). De asemenea, $u(x+y)=u(x)+u(y)$, căci $(x+y)^p = x^p +y^p$, deoarece C_p^s (combinări de p elemente luate s) se divid cu p dacă p>1, este un număr prim. În general u este un endomorfism injectiv, iar dacă K este finit sau este algebric închis,rezultă imediat că este şi surjectiv, deci în aceste două cazuri este automorfism al lui K.

Definiție. Un corp K de caracteristică zero sau de caracteristică p>0, pentru care morfismul u de mai sus este izomorfism, se numeşte **corp perfect.**

Exemple. Corpurile finite şi cele algebric închise sunt corpuri perfecte.

Notăm cu u^s puterea de ordin s a endomorfismului u (definit mai sus) al corpului K de caracteristică p>0.Evident u este automorfism dacă şi numai dacă u^s este automorfism.

Propoziție. Fie K un corp algebric închis, de caracteristică p>0. Atunci K conține un singur corp finit cu p^r elemente, pentru orice r>0. Acest corp este format din elementele lui K invariate de u^r.

Corolar. Fie un corp finit cu p^r elemente. Corpul K conține un subcorp L cu p^s elemente, dacă şi numai dacă s divide pe r.

Demonstrație.

Într-adevăr, dacă K conține subcorpul L, atunci: $[K:L][L:Z_p]=[K:Z_p]$, şi deci s divide pe r, căci $r=[K:Z_p]$, iar $s=[K:Z_p]$.

Reciproc: fie r = st şi $\bar{K}$ o închidere algebrică a lui K. Atunci conform propoziției precedente, K este subcorpul lui $\bar{K}$ format din elementele invariate de u^r , iar elementele invariate de u^s, fomează un subcorp L a lui K de ordin p^s, unde u este endomorfismul lui Frobenius.

Corpul finit care are p^r elemente, p>0 fiind un număr întreg prim, se notează cu $\mathbf{F_P^r}$ sau $\mathbf{GF(p^r)}$. În particular, corpul prim de caracteristică p se notează F_p.

IV EXTINDERI ALGEBRICE NORMALE

Lemă. Fie Ko extindere algebrică a corpului k şi u un endomorfism al lui K, care lasă Iavariate elementele lui k.Atunci u este un automorfism.

Propoziţie. Fie k un corp, Ko extindere algebrică a sa, şi $\bar{k}$ o închidere algebrică a lui k care conţine pe K. Atunci următoarele afirmaţii sunt echivalente:

a) Orice k-automorfism al lui $\bar{k}$ induce un k-automorfism al lui K.
b) Orice polinom ireductibil din k[X], care are o rădăcină în K, are toate rădăcinile în K.
c) Pentru orice automorfism u al lui $\bar{k}$ peste k, rezută $u(K) \subseteq K$.

Definiţie. Fie Kun corp, extindere algebrică a corpului k.Se spune că corpul K este **extindere normală** a lui k, dacă satisface proprietăţile echivalente din propoziţia precedentă.

Comentarii. 1) Dăm o definiţie echivalentă a unei extinderi normale. Fie Kun corp; două **numere** α, β , **algebrice** peste K, se numesc **conjugate**, dacă au acelaşi polinom minimal.

Exemple: a) Numerele 1+i şi 1-i sunt conjugate, deoarece sunt rădăcinile aceluiaşi polinom minimal $X^2-2X+2 \in Q[X]$.

b)Numerele $\sqrt{2}+\sqrt{3}$ şi $\sqrt{2}-\sqrt{3}$ sunt conjugate, deoarece sunt rădăcinile polinomului minimal $X^4-10X^2+1 \in Q[X]$.

Definiţie. O extindere K a lui k se numeşte **normală** peste k, dacă K este o extindere finită a lui k şi orice număr conjugat cu un număr din K,aparţine de asemenea lui K.

Extinderile normale ale corpului Q se numesc **corpuri normale.**

2) Pentru a da o formă echivalentă a noţiunii de extindere normală, introducem noţiunea de corp de descompunere al unui polinom.

Definiţie. Fie K un corp şi $f \in K[X]$, un polinom cu $n=grad(f) \geq 1$. Din teorema lui D'Alembert(teorema fundală a algebrei), f are n rădăcini complexe; fie acestea $\alpha_1, \alpha_2, \ldots, \alpha_n$. Corpul $K(\alpha_1, \alpha_2, \ldots, \alpha_n)$ se numeşte **corpul de descompunere** peste K a lui f. Dacă $f \in Q[X]$, atunci corpul de descompunere al lui f peste Q se numeşte, simplu, corp de descompunere al lui f.

Teoremă. Fie K o extindere a lui k. Atunci K este normală peste k dacă şi numai dacă K este corpul de descompunere al unui polinom cu coeficienţi din K.

Exemple. 1) Închiderea algebrică $\bar{k}$ a corpului k este extindere normală a lui k.

2) Fie k un corp şi K un corp de descompunere al unui polinom $f \in k[X]$. Atunci K este extindere normală a lui k. Într-adevăr, fie u un k-automorfism al unei închideri algebrice $\bar{k}$ a lui k, care conţine pe K. Dacă $\{x_i\}, i \in \{1,2,\ldots,n\}$, sunt toate rădăcinile polinomului f în k, atunci K este generat de aceste rădăcini. Elementele

$u(x_i), i \in \{1,2,\ldots,n\}$, sunt de asemenea rădăcini ale lui f în K şi deci sunt aceleaşi rădăcini, deoarece u este bijectivă. Cum u(K) este generat peste k de $u(x_i)$, $i \in \{1,..,n\}$, rezută că u(K) = K.

3) Orice extindere de grad 2 a unui corp este normală. Într-adevăr, fie k un corp şi Kun corp de extindere de grad 2 a lui k. Dacă $x \in K$, $x \notin k$, atunci 1,x este o bază a lui K peste k, deci K =k(x). Dacă f este polinomul minimal al lui x, atunci gradul lui f este 2. Deoarece f are o rădăcină în K, rezută că şi cealaltă rădăcină este tot în K.Aşadar K este corpul de descompunere al lui f şi deci K este o extindere normală a lui k.

4) Orice corp finit K este o extindere normală a oricărui subcorp al său. Într-adevăr, dacă K are p^r elemente, unde p este caracteristica corpului K, atunci el este corpul de descompunere al polinomului X^{p^r} -X, peste orice subcorp al său.

5) Corpul $K = Q(\sqrt[4]{3})$, considerat ca extindere a lui Q, nu este normală. În adevăr, polinomul minimal al lui $\sqrt[4]{3}$ este X^4 -3 şi acesta nu are toate rădăcinile în K. Acest polinom nu are toate rădăcinile reale.

Propoziţie. Fie $K \supseteq K \supseteq k$, extinderi algebrice de corpuri. Dacă L este extindere normală a lui k, atunci L este extindere normală şi a lui K.

Demonstraţie. Fie $\bar{k}$ o închidere algebrică a lui k care conţine pe L. Din ipoteză, rezultă că, orice element, $u \in G(\bar{k}/k)$, induce k- automorfism al lui L şi afirmaţia propoziţiei rezultă din că $G(\bar{k}/K)$ este un subgrup al lui $G(\bar{k}/k)$.

Propoziţie. Fie $k \subseteq L$ o extindere de corpuri şi K_1, K_2 două extinderi algebrice ale lui k conţinute în L.Se notează cu K_1K_2 subcorpul lui L generat de K_1 şi K_2.($K_1K_2 = k(K_1,K_2)$ şi este numit **compozitul** corpurilor K_1 şi K_2).

i) Dacă K_1 extindere normală a lui k, atunci K_1K_2 este o extindere normală a lui K_2.

ii) Dacă K_1 şi K_2 sunt extinderi normale ale lui k, atunci K_1K_2 şi $K_1 \cap K_2$ sunt extinderi normale ale lui k.

Propoziţie. Fie k un corp şi Ko extindere finită a sa. Atunci există o extindere normală finită a lui k, care conţine pe K.

Demontraţie. Fie $K = k(x_1,x_2,\ldots,x_n)$ şi fie $f_i \in k[X]$, polinomul minimal al lui x_i, $i = 1,2,\ldots,n$. Atunci corpul de descompunere L al polinomului $f = \prod_{i=1}^{n} f_i$, conţinut într-o închidere algebrică $\bar{k}$ a lui k, care conţine pe K, este evident o extindere finită şi normală a lui k care conţine pe K.

Comentarii. 1) Observăm că corpul L, construit în propoziţia precedentă, este cea mai "mică" extindere normală a lui k care conţine pe K.

2) Fie k un corp şi $\bar{k}$ o închidere algebrică a sa. Atunci două elemente $x,y \in \bar{k}$ se numesc conjugate peste k, dacă au acelaşi polinom minimal. Numărul elementelor conjugate cu un element x din $\bar{k}$, este egal cu numărul rădăcinilor distincte ale polinomului minimal al luix.

Propoziţie. Fie k un corp şi K = k(x), o extindere algebrică normală simplă a sa.Atunci ordinul grupului G(K/k) este egal cu numărul conjugaţilor lui x. În particular, ordinul grupului G(K/k) este cel mult egal cu [K:k].

Corolar. Fie Kun corp finit cu p^r elemente şi k un subcorp al său cu p^s elemente,unde p>0, este caracteristica lui K. Atunci G(K/k) este un grup ciclic de ordin d=r/s şi un generator al său este u^s, unde u: $K \to K$ este morfismul $u(x)=x^p$, pentru orice $x \in K$. În particular, $G(K/Z_p)$ este ciclic, un generator al său fiind u.

Observaţii. 1) Extinderile algebrice normale de corpuri nu au proprietatea de tranzitivitate. În adevăr, am văzut că $Q(\sqrt[4]{3})$, nu este extindere normală a lui Q, deşi $Q(\sqrt{3})$ este extindere normală a lui Q, iar $Q(\sqrt[4]{3})$ este extindere normală a lui $Q(\sqrt{3})$.

2) Noţiunea de extindere normală a fost extinsă extinsă de către matematicianul român Dan Barbilian (1895 – 1961), la cazul extinderilor nealgebrice.

V. EXTINDERI ALGEBRICE SEPARABILE

Definiţii. 1) Fie $k \subseteq K$ o extindere algebrică de corpuri şi $x \in K$. Vom spune că x este **separabil** peste k, dacă polinomul minimal al lui x nu are rădăcini multiple. În cazul contrar, vom spune că x este **neseparabil** peste k.

2) Extinderea K a lui k se numeşte separabilă, dacă orice element din K este separabil peste k, în cazul contrar, extinderea se numeşte neseparabilă.

Propoziţie. Fie k un corp. Dacă caracteristica lui k este 0, orice element algebric peste k este separabil peste k.Dacă caracteristica lui k este $p \neq 0$, atunci un element x algebric peste k este separabil peste k, dacă şi numai dacă polinomul minimal al lui x peste k, nu aparţine lui $k[X^p]$.

Propoziţie. i) Un corp k este perfect dacă şi numai dacă orice element algebric peste k este separabil .

ii) Un corp k este perfect dacă şi numai dacă orice extindere algebrică a sa, este separabilă.

Lemă. Fie k un corp de caracteristică p>0, şi $a \in k$ asfel încât polinomul X^p –a să nu aibă rădăcini în k. Atunci polinomul X^{pm}-a este ireductibil în k[X], pentru orice $m \geq 1$ număr întreg. În particular, polinomul X^p-a este ireductibil.

Propoziţie. Fie $k \subseteq K \subseteq L$ extinderi de corpuri.Dacă $x \in L$ este un element separabil peste k, atunci x este separabil pete K.În particular, dacă L este extindere separabilă a lui k, atunci L este extindere separabilă a lui K.

Demonstraţie. Fie $f \in k[X]$, polinomul minimal al lui x peste K. Atunci rezultă că f=gh în K[X]. Cum x este separabil peste k, f nu are rădăcini multiple. Deci nici g nu are rădăcini multiple şi x rezultă element separabil peste K.

Corolar. Orice extindere algebrică a unui corp perfect este corp perfect.În particular, o extindere algebrică a unui corp finit este un corp perfect.

Propoziţie. Fie $k \subseteq K$ o extindere algebrică de corpuri, de caracteristică p>0.

i) Dacă K este o extindere algebrică separabilă a lui k , atunci $K = k(K^p)$.

ii) Dacă $[K:k] < \infty$ şi $K = k(K^p)$, atunci K este extindere separabilă a lui k.

Corolar. Fie k un corp de caracteristică p>0 şi x un element dintr-o extindere a lui k, algebric peste k.Atunci x este separabil peste k dacă şi numai dacă $k(x)=k(x^p)$. Dacă x este este separabil peste k, atunci k(x) este extindere separabilă a lui k.

Propoziţie. Dacă $k \subseteq K$ şi $K \subseteq L$ sunt extinderi algebrice separabile de corpuri, atunci $k \subseteq L$ este extindere separabilă.(tranzitivitatea extinderilor separabile).

Corolar. Dacă k este un corp şi M o submulţime de elemente algebrice separabile dntr-o extindere a lui k, atunci corpul k(M) este o extindere algebrică sparabilă a lui k.

Corolar. Fie $k \subseteq K$ o extindere algebrică de corpuri.Atunci mulţimea elementelor din K separabile peste k, formează un subcorp al lui K, care conţine pe k (numit închiderea separabilă a lui k în K).

Comentarii. 1) Dacă k este un corp şi $\bar{k}$ o închidere algebrică a sa, atunci subcorpul k' al elementelor din k care sunt separabile peste k se numeşte închiderea separabilă a lui k

3) Fie $k \subseteq K$ o extindere simplă de corpuri. Un generator al lui K peste k se mai numeşte element primitiv al extinderii K.

Definiţie. O extindere E a K se numeşte **simplă**, dacă există un $\alpha \in E$,astfel încât: $E = K(\alpha)$.

Teorema (elementului primitiv)

Fie k un corp şi K o extindere finită şi separabilă a lui k. Atunci K este exindere simplă a lui k.

Demonstraţie. Dacă k este corp finit, rezultă că şi K este un corp finit şi dacă x este un generator al grupului multiplicativ al elementelor nenule din K, atunci evident K=k(x). Examinăm cazul în care k este un corp infinit. Deoarece K este extindere finită a lui k, rezultă K este de forma: $K = k(x_1,x_2,\ldots,x_n)$, unde $x_1,x_2,\ldots,x_n$ sunt elemente din K algebrice peste k. Efectuând o inducţie după n, se vede că este suficient să demonstrăm afirmaţia pentru n=2, adică putem presupune că K= k(x,y).

Fie f polinomul minimal al lui x, g polinomul minimal al lui y, şi $\bar{K}$ o închidere algebrică a corpului K. În $\bar{K}$, conform ipotezei, polinomul f are n = gradf rădăcini distincte $x=x_1,x_2,\ldots,x_n$ iar polinomul g are m =gradg rădăcini distincte $y=y_1,y_2,\ldots,y_m$. Deoarece corpul k are o infinitate de elemente, există în k un element c astfel încât egalitatea $x_1+cy_1=x_i+cx_j$, să fie verificată dacă şi numai dacă i=j =1.

Arătăm că elementul $z=x_1+cy_1=x+cy$ are proprietatea k(z)=K. Este suficient să arătăm că $x,y \in k(z)$ şi pentru aceasta este suficient să observăm că unul dintre aceste elemente aparţine lui k(z)=k'. Se observă că polinoamele f(z-cX) şi g, cu coeficienţi în k', au ca rădăcină comună pe y şi numai pe acaesta, datorită faptului că relaţia $x_1+cy_1=x_i+cy_j$ este verificată numai pentru i=j=1. De aici, rezultă că cel mai mare divizor comun al acestor polinoame în k'[X] este X-y, deci $y \in k'$.

Corolar. Fie K un corp, extindere finită de gradul n a corpului k. Dacă K este extindere normală şi separabilă a lui k, atunci ordinul grupului G(K/k) este egal cu n.

Comentarii. 1) Acestă teoremă, arată că mulţimea extinderilor finite, mulţimea extinderilor algebrice finit generate şi mulţimea extinderilor algebrice simple coincid.

2) Noţiunea de extindere separabilă de corpuri, se utilizează în matematică şi în cazul în care extinderile nu sunt neapărat algebrice. În cazul general, definiţia extinderii separabile va generaliza definiţia din cazul extinderilor algebrice. Teorema care urmează dă posibilitatea unei astfel de generalizări.

Definiţie. 1) Fie A un inel. Un element $x \in A$, se numeşte nilpotent, dacă există un întreg n>1, astfel încât $x^n = 0$. Evident 0 este element nilpotent.

2) Dacă 0 este singurul element nilpotent din A, vom spune că A este inel redus.

Teoremă. Fie K o extindere algebrică a corpului k. Atunci următoarele afirmații sunt echivalente:

a) K este extindere separabilă a lui k.
b) Pentru orice extindere finită k' a lui k, cu $k'^{p} \subseteq k$, unde p este exponentul caracteristic al lui k, inelul $K \otimes_k k'$ este redus.
c) Pentru orice extindere finită k' a lui k, inelul $K \otimes_k k'$ este redus.

VI. TEOREMA FUNDAMENTALĂ A TEORIEI LUI GALOIS

Definiție. O extindere algebrică K a unui corp k se numeşte **galoisiană,** dacă este normală şi separabilă.

Teoremă. (Teorema fundamentală a teoriei lui Galois).
Fie K o extindere galoisiană şi finită a corpului k, cu grupul lui Galois G.
Atunci aplicația care asociază fiecărui subgrup H a lui G, subcorpul K^H al lui K, este bijectivă şi antimonotonă.
Corpul K^H este extindere normală a lui k, dacă şi numai dacă subgrupul H este normal în G.
Dacă H este subgrup normal în G, restricția elementelor lui G la K^H induce un izomorfism al grupului G/H cu grupul lui Galois al extinderii $K^H \supseteq k$.

Demonstație.

Ştim(din paragraful:"Grupul lui Galois"), că aplicația este antimonotonă. Mai trebuie să arătăm că este bijectivă. Este suficient să arătăm că avem relațiile : $G(K/K^H) = H$, (1), pentru orice subgrup H a luiG, şi $K^{G(K/L)} = L$,(2), pentru orice extindere L a lui k, conținută în K. Într-adevăr, aceste relații ne spun că inversa aplicației de mai sus, este cea care asociază unei extinderi L a lui k, conținută în K, subgrupul lui G format din elementele care invariază elementele lui L.

Incluziunea $G(K/K^H) \supseteq H$, este evidentă.

Fie n ordinul subgrupului H. Pentru a demonstra (1), arătăm că ordinul lui $G(K/K^H)$ este cel mult n. Din ultimul corolar, paragraful precedent (K fiind extindere finită normală şi separabilă a lui K^H), deducem că, ordinul lui $G(K/K^H)$ este egal cu $[K : K^H]$. Fie x un element primitiv al extinderii $K^H \subseteq K$. Considerăm polinomul

$$f = \prod_{\sigma \in H} (X - \sigma(x)).$$

Evident, coeficienții lui f, sunt invarianți la elementele din H, deci $f \in K^H[X]$. Aşadar, gradul lui x este $\leq n$ şi deci $[K:K^H] \leq n$.

Să demonstrăm relația (2).Avem evident $K^{G(K/L)} \supseteq L$. De aici rezultă, că grupul lui Galois al lui K peste L, coincide cu grupul lui Galois al lui K peste $K^{G(K/L)}$. Deoarece K

este extindere galoisană finită a lui $K^{G(K/L)}$ şi L, putem aplica corolarul precedent. Se obţine: $[K:K^{G(K/L)}] = [K:L] = \text{ord}G(K/L)$; de aici se obţine egalitatea (2).

Fie H subgrup normal în G şi $x \in K^H$. Este suficient să arătăm cătoţi conjugaţii lui x aparţin lui K^H. Dacă x' este un astfel de conjugat, atunci există un element $u \in G(K/k)$, astfel încât x'= u(x).Avem $uvu^{-1}(x') = uv(x) = u(x) = x'$, pentru orice $v \in H$, şi deoarece $uHu^{-1} = H$, rezultă că $x' \in K^H$.

Reciproc, fie K^H extindere normală a lui k şi $f: G(K/k) \to G(K^H/k)$, aplicaţia de restricţie. Aplicaţia f există deoarece K^H este extindere normală a lui k. Evident, f este un morfism de grupuri(restricţia de aplicaţii păstrează compunerea lor), şi în plus, ea este surjectivă, căci orice element u din $G(K^H/k)$ se extinde la un automorfism u al închiderii algebrice a lui k, care la rândul său induce un automorfism u' al lui K peste k, a cărui restricţie la K^H coincide cu u. Nucleul lui f este subgrupul lui G(K/k), care invariază toate elementele lui K^H, adică Kerf = H, conform relaţiei (1). De aici, rezultă că H este subgrup normal în G. De asemenea rezultă şi ultima afirmaţie a teoremei.

Propoziţie. Fie k un corp şi K,L două extinderi ale lui k conţinute într-o închidere Algebrică $\bar{k}$ a lui k. Dacă K este extindere galoisiană finită a lui k, atunci KL = k(L,K) este o extindere galoisiană finită a lui L şi aplicaţia $f: G(KL/L) \to G(K/k)$, definită prin f(u) = restricţia lui u la K,este injectivă.

Demonstraţie. Fie $x_1, x_2, \ldots, x_n$ un sistem de elemente în K astfel încât $K = k(x_1, x_2, \ldots, x_n)$. Atunci $KL = k(K,L) = k(L)(K) = k(L)(x_1, x_2, \ldots, x_n) = L(x_1, x_2, \ldots, x_n)$. Deoarece $x_1, x_2, .., x_n$ sunt algebrice peste k, rezultă că ele sunt algebrice şi peste L, deci $[KL: L] < \infty$. Faptul că extinderea $KL \supseteq L$ este normală, rezultă din a treia propoziţie, de la "Extinderi algebrice normale". Deoarece $x_1, x_2, \ldots, x_n$ sunt separabile peste k, ele sunt separabile şi peste L şi (din al treilea corolar de la paragraful precedent), deducem că KL este separabilă peste L. Fie $u \in G(KL/L)$, astfel încât $f(u) = 1_K$, adică u(a)=a, pentru orice $a \in K$ şi cum u(a)=a şi pentru orice $a \in L$, rezultă că u este identitatea lui KL.

Propoziţie. Fie K o extindere galoisiană finită de grad n a corpului k. Atunci grupul lui Galois G(K/k) este un grup de permutări de grad n.

Demonstraţie. Fie x un element primitiv al acestei extinderi. Deci K = k(x) şi fie f polinomul minimal al lui x.

Dacă $x = x_1, x_2, \ldots, x_n \in K$ sunt toate rădăcinile lui f, atunci oricărui element $u \in G(K/k)$ îi corespunde permutarea $u(x_1), \ldots, u(x_n)$ a elementelor $x_1, x_2, \ldots, x_n$ şi aplicaţia astfel definită este injectivă.

VII. CARACTERIZAREA ECUAŢIILOR REZOLUBILE PRIN RADICALI

Fie k un corp de caracteristică zero. În acest paragraf, vom considera o închidere algebrică $\bar{k}$ a lui k, şi toate extinderile algebrice ale lui k, vor fi conţinute în $\bar{k}$.

Definiţie. Un element $x \in \bar{k}$, este **radical** peste k, dacă x este o rădăcină a unui polinom

de forma (1):$X^n - a$, $a \in k$.

Comentarii. 1) Observăm că un polinom de acest tip, nu are rădăcini multiple şi ele se obţin din una dintre ele, prin înmulţire cu rădăcinile polinomului (2) $X^n - 1$, adică cu rădăcinile de grad n ale unităţii.

2) Aşadar, dacă θ este o rădăcină a polinomului (1) şi ξ o rădăcină primitivă de grad n a unităţii, atunci toate rădăcinile lui (1) sunt de forma $\xi^i\theta$, cu $\theta \le i \le n-1$ şi sunt distincte.

Definiţie. Se numeşte **extindere radicală simplă** a lui k, corpul de descompunere al unui polinom de forma (1).

Observaţie. Deci, dacă K este acest corp, el este extindere normală a lui k şi cu notaţiile de mai sus, avem: $K = k(\xi, \theta)$.

Definiţie. O **extindere algebrică** L a lui k se numeşte **radicală** peste k, dacă există şirul de subcorpuri: $k = K_0 \subseteq K_1 \subseteq K_2 \subseteq \ldots \subseteq K_n = L$, astfel încât K_{i+1} să fie extindere radicală simplă a lui K_i, pentru i = 0,1,2,….,s-1.

Comentarii. 1) Din definiţie rezultă, imediat,că dacă K este o extindere radicală a lui k, iar L o extindere radicală a lui K, atunci L este o extindere radicală a lui k(tranzitivitatea extinderilor radicale), şi orice extindere radicală este este extindere finită.

2) Deoarece extinderile normale nu au proprietatea de tranzitivitate , o extindere radicală nu este neapărat normală. Astfel $Q(\sqrt[4]{3})$ este extindere radicală a lui Q, care nu este normală.

Teoremă. Orice extindere radicală L a corpului k este conţinută într-o extindere radicală normală.

Definiţie. 1) Fie $f \in k[X]$, un polinom de grad >0; spunem că **ecuaţia f = 0 este rezolubilă prin radicali**, dacă există o extindere radicală K a lui k (deci şi o extindere radicală normală), care conţine rădăcinile polinomului f.

2) Dacă $f \in k[X]$ este un polinom de grad >0, **vom numi grupul lui Galois al lui f**, grupul lui Galois al corpului de descompunere al lui f peste k.

Comentarii. Fie G un grup. Şirul de subgrupuri: $G=G_0 \supseteq G_1 \supseteq \ldots \supseteq G_n = (e)$, (1), este este normal, dacă G_{i+1} este subgrup în G_i, pentru orice i=0,1,…,n-1.Numărul n se numeşte lungimea şirului, iar grupurile G_i/G_{i+1} se numesc factorii şirului.

Spunem că şirul normal (1) este rezolubil, dacă toţi factorii săi sunt grupuri abeliene.

Un **grup** se numeşte **rezolubil**, dacă posedă un şir rezolubil. Rezultă că orice grup abelian este rezolubil. Există grupuri neabeliene care sunt rezolubile.

Un subgrup al unui grup rezolubil este rezolubil. Orice grup factor al unui grup rezolubil este rezolubil.

Teoremă. Fie H un subgrup normal al unui grup G. Atunci G este rezolubil dacă şi numai dacă H şi G/H sunt rezolubile.

Teoremă. Fie k un corp de caracteristică zero şi K o extindere finită şi normală a sa. Atunci K este conţinută într-o extindere radicală dacă şi numai dacă grupul lui Galois G(K/k) este rezolubil.

Teoremă. Fie k un corp de caracteristică zero şi $f \in k[X]$ un polinom de grad >0. Atunci ecuaţia f = 0 este rezolubilă prin radicali dacă şi numai dacă grupul lui Galois al lui f este rezolubil.

Comentarii.

Fie K un corp comutativ; atunci ordinul elementului $1 \in K$, în grupul aditiv (K,+) poate fi finit sau infinit. Spunem că **corpul K are caracteristica zero** (sau este de caracteristică zero), dacă ord(1) este infinit, adică $m.1 \neq 0$, pentru orice număr întreg pozitiv m. Spunem că **corpul K este de caracteristică n**, dacă, ord(1) = n, adică n este cel mai mic număr întreg pozitiv astfel încât n.1 = 0.

Caracteristica unui corp K este 0 sau un număr prim.

Exemple: 1) Dacă p este prim, atunci Z_p este un corp de caracteristică p.

2) Corpurile Q,R C au caracteristica zero.

3) Într-un corp K de caracteristică p sunt adevărate egalitățile :

$px = 0$;

$(x \overset{+}{\underset{-}{}} y)^p = x^p \overset{+}{\underset{-}{}} y^p$;

$(xy)^p = x^p y^p$.

Lemă. Dacă $k \subset L$ este o extindere normală de corpuri de grad n cu grupul lui Galois ciclic şi corpul k conține rădăcinile de gradul n ale unității, atunci $K = k(\theta)$, unde θ este rădăcină a unui polinom de forma $X^n - a \in k[X]$.

Propoziție. Fie k un corp şi K o extindere finită şi normală a sa cu G(K/k) grup ciclic. Atunci corpul K este conținut într – o extindere radicală a lui k.

Demonstrație. Fie m=[K:k]=ordG(K/k), ξ fiind o rădăcină primitivă de gradul m a unității şi $L=K(\xi)$. Se observă că L este o extindere normală a lui k. Este suficient să arătăm că L este extindere radicală a lui $k(\xi)$ şi deci şi a lui k. Observăm că $G(L/k(\xi)) \subset G(K/k)$. Deci $G(L/k(\xi))$ este un grup ciclic de ordin n, unde n este un divizor al lui m. Afirmația propoziției rezultă din lema anterioară.

Corolar. Orice ecuație algebrică de grad ≤ 4 este rezolubilă prin radicali.(Rezultă din ultima teoremă şi din faptul că, pentru $n \leq 4$ grupurile S_n sunt rezolubile).

VIII . EXTINDERI TRANSCENDENTE. GRADUL DE TRASCENDENȚĂ AL UNEI EXTINDERI.

Definiție. Fie k un corp şi K o extindere a sa. Spunem că K este o **extindere transcendentă** a lui k, dacă nu este algebrică peste k.

Exmple: 1) Orice corp de fracții raționale peste un corp k, este evident o extindere transcendentă a lui k.

2) Corpul numerelor reale R este extindere transcendentă a corpului numerelor rele R.

Comentarii. 1) Dacă M este o submulțime de elemente algebric independente dintr-o extindere K a corpului k, atunci orice submulțime a sa este algebric independentă.

2) Extinderea K a corpului k se numeşte extindere transcendentă pură dacă se obține prin adjuncționare la k a unei mulțimi de elemente algebric independente peste k.

3) Orice extindere transcendentă pură a unui corp k este izomorfă peste k cu un corp de fracţii raţionale peste k.

Propoziţie. Fie K un corp, extindere a corpului k şi M,N două sisteme de elemente din K. Presupunem că elementele din M sunt algebric independente peste k. Atunci următoarele afirmaţii sunt echivalente:

a) Elementele reuniunii disjuncte a lui M cu N, sunt algebric independente peste k.
b) Elementele mulţimii N sunt algebric independente peste k(M).

Definiţie. Fie K un corp, extindere a corpului k. O submulţime,M a lui K, se numeşte **bază de transcendenţă** a lui K peste k, dacă elementele sale sunt algebric independente pete k şi K este extindere algebrică a lui k(M). Evident nedeterminatele constituie o bază de transcendenţă peste k, pentru orice corp de fracţii raţionale k(X;I).

Teoremă. Fie K un corp, extindere a corpului k, M o mulţime din K cu elemente algebric independente peste k şi $N \supseteq M$ un sistem de elemente din K, astfel încât, corpul K să fie extindere algebrică a lui k(N). Atunci există o bază de transcendenţă B a lui K peste k, care conţine pe M şi este conţinută în N.

Teoremă. Fie K un corp, extindere a corpului k Atunci orice două baze de transcendenţă ale lui K peste k, sunt cardinal echivalente (adică există o bijecţie între cele două baze de transcencenţă).

Definiţie. Cardinalul unei baze de transcendenţă a extinderii K, a corpului k se numeşte **gradul de transcendenţă** al lui K peste k şi va fi notat cu $\mathbf{tr_kK}$. Dacă K nu posedă o bază de transcendenţă finită, se notează de obicei $\text{grad}_k K = \infty$.

Propoziţie. Fie $k \subseteq K \subseteq L$ extinderi de corpuri. Atunci:

$$\text{grad } tr_k L = \text{grad } tr_k K + \text{grad } tr_K L.$$

Demonstrţie. Fie M şi N o bază de transcendenţă a lui K peste k, respectiv o bază de transcendenţă a lui L peste K. Va fi suficient să arătăm că $M \cup N$ este o bază de transcendenţă a lui L peste k. Din prima propoziţie , rezultă că elementele acestei mulţimi sunt algebric independente peste k. Rămâne să mai arătăm că, L este extindere algebrică a lui k(M), deci K(N) = k(M ∪ N)(K) este extindere algebrică a lui k(M ⋃ N). Însă L este extindere algebrică a lui k(M ∪ N). Însă L este extindere algebrică a lui K(N), deci L este şi extindere algebrică a lui k(M ∪ N).

Observaţie. Noţiunile de independenţă algebrică şi de bază de transcendenţă sunt analoage cu noţiunile de independenţă liniară şi de bază pentru module.

IX. GRUPUL LUI GALOIS AL UNUI POLINOM.

Definiţie. Fie K un corp şi f un polinom din K[X], de $\text{grad}(f) \geq 1$. Notăm cu E corpul de descompunere al lui f, care este o extindere normală al lui K. **Grupul G = G(E/K) se numeşte grupul lui Galois asociat polinomului**

f.

Propiziție. Fie $f \in K[X]$ un polinom ireductibil cu $n = grad(f) \geq 1$. Dacă G este grupul Galois al acestui polinom, atunci G este izomorf cu un subgrup al lui σ_n.

Demonstrație. Dacă $X = \{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ sunt rădăcinile lui f, atunci $E = K(\alpha_1, .., \alpha_n)$. Fie $u \in G$. Cum u este un K-omomorfism, atunci $u(\alpha_i)$ este o rădăcină a lui f. Deci $u(X) \subseteq X$ şi cum u este injectivă, rezultă u (X) = X. Dar, f este ireductibil, deci $\alpha_1, \ldots, \alpha_n$ sunt distincte între ele. Notăm cu S_X mulțimea aplicațiilor bijective ale lui X în X. Deci S_X este un grup care este izomorf cu σ_n.

Definim $\varphi : G \to S_X$, $\varphi(u) = u/X$. Este evident că φ este un omomorfism de grupuri. Dovedim că φ este injectivă, adică, să verificăm că $Ker\,\varphi = \{1_e\}$. Dacă $u \in Ker\,\varphi$, atunci $u/X = 1_X$, adică $u(\alpha_i) = \alpha_i$ $(1 \leq i \leq n)$. Deoarece $E = K(\alpha_1, .., \alpha_n) = K[\alpha_1, ,,,,,. \alpha_n]$, fie $x \in K[\alpha_1, \ldots, \alpha_n]$. Există $f \in K[X_1, \ldots, X_n]$, astfel încât $x = f(\alpha_1, \ldots., \alpha_{n)}$. Dar, atunci $u(x) = u(f(\alpha_1, \ldots., \alpha_n)) = f(u(\alpha_1), \ldots, u(\alpha_n)) = f(\alpha_1, \ldots, \alpha_n) = x$. Deci $u = 1_E$. Cum φ este injectivă , rezultă că $G \cong Im\,\varphi$. Dar $Im\,\varphi$ este un subgrup în S_X şi deci este izomorf cu un subgrup al lui σ_n.

Definiție. Fie G un subgrup al lui σ_n. Subgrupul G se numeşte **tranzitiv** dacă, oricare ar fi $1 \leq i, j \leq n$, există o permutare $\sigma \in G$, , astfel încât $\sigma(i) = j$

Propoziție. Fie G un subgrup al lui σ_n. Presupunem că:

1) n este număr prim;
2) G este tranzitiv;
3) G conține o transpoziție; atunci $G = \sigma_n$.

Teoremă. Fie K un corp astfel încât $K \subseteq R$. Fie $f \in K[X]$, un polinom ireductibil cu gradf = p, p fiind număr prim. Dacă f are numai rădăcini complexe, atunci grupul lui Galois G al lui f este izomorf cu σ_p.

Teoremă. Pentru orice număr prim $p \geq 5$ există un polinom cu coeficienți raționali de grad egal cu p al cărui grup Galois este izomorf $\sigma_{p.}$.

X. APLICAȚII

1) Fie A un inel comutativ unitar. Notăm cu U(A) mulțimea elementelor inversabile din A. Atunci U(A) este grup abelian față de operația de înmulțire din inelul A.

Notăm $M(A) = U(A) \times A$. Pe M(A) definim operația "$*$" astfel: fie (a,b) şi(c,d) două elemente din M(A); atunci

$$(a,b) * (c,d) = (ac,bc+d).$$

Se verifică, imediat, că operația "$*$" este asociativă. Elementul (1,0) este element neutru în M(A), iar dacă $(a,b) \in M(A)$, atunci (a^{-1},ba^{-1}) este inversul său. Deci M(A) este un grup (în general neabelian).

Definim aplicația $\varphi : M(A) \to U(A)$, $\varphi(a,b) = a$. Aplicația φ este omomorfism surjectiv de grupuri şi $\text{Ker}\,\varphi = \{(a,b)/\varphi(a,b) = 1\} = \{(a,b) \in M(A)/a = 1\} = \{(1,b)/b \in A\}$. $\text{Ker}\,\varphi$ este izomorf cu grupul abelian subiacent structurii de inel a lui A.

Conform teoremei : Un grupG este rezolubil dacă şi numai dacă H şi G/H sunt rezolubile, unde H este un subgrup al lui G, rezultă că M(A) este un grup rezolubil.

Considerăm un caz particular.

Fie inelul $A = Z_n$. Atunci $U(Z_n) = Z_n^* = \{\hat{a}/(a,n) = 1\}$

Notă $M_n = M(Z_n) = Z_n^* \times Z_n$. Se observă că M_n este un grup finit rezolubil. Ordinul său este egal cu $n\varphi(n)$, unde $\varphi(n)$ este indicatorul lui Euler al numărului natural n.

2) Grupurile simetrice $\sigma_1, \sigma_2, \sigma_3, \sigma_4$ sunt rezolubile.

(Grupul de permutări al mulțimii {1,2,…,n} se numeşte **grupul simetric de grad n,** notat σ_n sau S_n).

Într-adevăr, considerăm grupul altern A_n (format din toate permutările pare ale lui σ_n). A_n este subgrup normal al lui σ_n şi $\sigma_n / A_n \cong \{-1,1\}$. A_n are $\frac{n!}{2}$ elemente. Studiem grupurile A_n, pentru n = 1,2,3,4.

Pentru n = 1, $A_1 = \{e\}$; pentru n = 2, $A_2 = \{e\}$.Dacă n = 3, A_3 este ciclic(are trei elemente) şi deci abelian. Rezultă că $\sigma_1, \sigma_2, \sigma_3$ sunt rezolubile.

Pentru n = 4, A_4 are 12 elemente. Considerăm în A_4 elementele:

$H = \{e, t_1 = (12)(34), t_2 = (13)(24), t_3 = (14)(23)\}$. Evident $H \subseteq A_4$.

Au loc relațiile:

$t_1^2 = t_2^2 = t_3^2 = e$; $t_1t_2 = t_2t_1 = t_3$, $t_1t_3 = t_3t_1 = t_2$ şi $t_2t_3 = t_3t_2 = t_1$.

Deci H este un subgrup al lui A_4. Mai mult, H este abelian şi este un subgrup normal în σ_4. Într-adevăr, demonstrăm că $at_ia^{-1} \in H$, pentru orice $a \in \sigma_4$ şi $i \in \{1,2,3,4\}$. Cum a este un produs de transpoziții, este suficient să considerăm cazul când a este o transpoziție:

a = (12); $(12)t_1(12) = t_1$; $(12)t_2(12) = t_3$; $(12)t_3(12) = t_2$;
a = (13); $(13)t_1(13) = t_3$; $(13)t_2(13) = t_2$; $(13)t_3(13) = t_1$;
a = (14); $(14)t_1(14) = t_2$; $(14)t_2(14) = t_1$; $(14)t_3(14) = t_3$;
a = (23); $(23)t_1(23) = t_2$; $(23)t_2(23) = t_1$; $(23)t_3(23) = t_3$;
a = (24); $(24)t_1(24) = t_3$; $(24)t_2(24) = t_2$; $(24)t_3(24) = t_1$;
a = (34); $(34)t_1(34) = t_1$; $(34)t_2(34) = t_3$; $(34)t_3(34) = t_2$.

Deoarece A_4/H are trei elemente, înseamnă că este grup ciclic, deci abelian. Atunci A_4 este grup rezolubil. Deoarece σ_4 / A_4 este izomorf cu grupul {-1,1}, în raport cu operația de înmulțire, rezultă că σ_4 este rezolubil.

Deci, pentru σ_4 se construieşte următorul şir normal de subgrupuri cu factorii grupuri abeliene: (e) $\subseteq$ K $\subseteq$ A_4 $\subseteq \sigma_4$, în care:

K = { e, (12)(34), (13)(24), (14)(23)}, numit **grupul lui Klein.**

3) Grupurile σ_n, pentru n$\geq$5, nu sunt grupuri rezolubile.

Demonstrație: prin metoda reducerii la absurd. Presupunem că σ_n ar fi rezolubil. Atunci ar exista un şir rezolubil: σ_n = $G_0 \supseteq G_1 \supseteq \ldots \supseteq G_m$ = (e); (1). Demonstrăm că acest fapt ne conduce la o contradicție. Spunem că o permutare u$\in \sigma_n$ este un ciclu, dacă există $1 \leq i_1, i_2, \ldots, i_s \leq n$ distincte, astfel încât $u(i_k) = i_{k+1}$, k = 1,2,…s-1 şi $u(i_s) = i_1$, iar u(j) = j, pentru $j \neq i_1, i_2, \ldots, i_s$. Cclul de mai sus se notează, de obicei, cu $(i_1\ i_2 \ldots i_s)$ şi se numeşte lungimea lui u. O transpoziție este un ciclu de lungime 2.

Fie G un subgrup al lui σ_n, care conține toate ciclurile de lungime trei şi H ,un subgrup normal în G, cu G/H grup abelian. Fie (ijk) un ciclu de lungime trei din G. Considerăm, de asemenea, ciclurile (jis),(kit), unde $1 \leq i,j,k,s,t \leq n$ sunt numere distincte.

Atunci $v = (jis)^{-1}(kit)^{-1}(jis)(kit) = (ijk)$. Deoarece G/H este grup abelian, rezultă că (ijk)$\in$H şi deci H conține şi el toate ciclurile de lungime trei. Aplicând rezultatul de mai sus, şirului (1), rezută că, fiecare G_i, i = 0,1,…,m, conține toate ciclurile de lungime trei, ceea ce este imposibil.

Mai mult, pentru n$\geq$5, A_n nu conține subgrupuri normale proprii(adică diferite de (1) şi de A_n). Un astfel de grup se numeşte **grup simplu.**

4) Exemplu de grup Galois.

Fie $Q(\sqrt{3}) = \{a+b\sqrt{3} / a, b \in Q\}$. Este limpede că $[Q(\sqrt{3}): Q] = 2$ şi $Q(\sqrt{3})$ este o extindere normală a lui Q, ca fiind corpul de descompunere al polinomului $X^2 - 3$. Rezultă că grupul lui Galois $G(Q(\sqrt{3})/Q)$ are două elemente şi anume aplicația identică a lui $Q(\sqrt{3})$ şi automorfismul $\sigma : Q(\sqrt{3}) \to Q(\sqrt{3})$, $\sigma(a+b\sqrt{3}) = a - b\sqrt{3}$.

Comentarii. 1) Fie K o extindere arbitrară a lui k. Notăm cu G(K/k) mulțimea k – automorfismelor lui K. G(K/k) împreună cu operația de compunere a funcțiilor este un grup. Elementul neutru al acestui grup este funcția identică $1_K: K \to K$, $1_K(x) = x$.

Grupul G(K/k) se numeşte grupul lui Galois asociat extinderii K.

2) Dacă K este o extindere normală a lui k, atunci G(K/k) este un grup finit având ordinul egal cu [K:k].

5) Exemplu de extindere normală.

a) $Q(\sqrt{2}) = \{a+b\sqrt{2} / a,b \in Q\}$ este o extindere normală a lui Q. Într – adevăr, $[Q(\sqrt{2}):Q] = 2$ şi cojugatul lui $a+b\sqrt{2}$ este $a - b\sqrt{2}$.

b) C este o extindere normală a lui R.

Într – adevăr, [C:R] = 2 şi conjugatul lui a+bi este a-bi.

6) Exemple de corpuri de descompunere.

a) Fie polinomul $f = X^4 - 2 \in Q[X]$. Rădăcinile lui f sunt: $\sqrt[4]{2}$, $-\sqrt[4]{2}$, $i\sqrt[4]{2}$,$-i\sqrt[4]{2}$.

Atunci corpul de descompunere al lui f este:

$E = Q(\sqrt[4]{2}, -\sqrt[4]{2}, i\sqrt[4]{2}, -i\sqrt[4]{2}) = Q(i, \sqrt[4]{2})$.

b) Dacă considerăm tot polinomul $f = X^4 - 2$, dar cu coeficienți în R[X], atunci corpul de descompunere al lui f peste R este:

$E = R(\sqrt[4]{2}, -\sqrt[4]{2}, i\sqrt[4]{2}, -i\sqrt[4]{2}) = R(i) = C$.

7) Pentru orice număr prim $p \geq 5$, există un polinom f de grad p, având grupul Galois asociat izomorf cu σ_p. Cum σ_p, pentru $p \geq 5$, nu este rezolubil, rezultă că ecuația $f = 0$, nu este rezolvabilă prin radicali(relativ la corpul Q).

8) Fie $f \in R[X]$, un polinom arbitrar. Ecuația $f = 0$ este rezolvabilă prin radicali, relativ la corpul R.

Într – adevăr, f se descompune intr – un produs finit de polinoame de grad ≤ 2, cu coeficienți în R. Atunci putem presupune $f \in R[X]$ cu $gradf \leq 2$. Dar ecuația $f = 0$ este rezolvabilă prin radicali, relativ la corpul R. Greutatea, însă constă în faptul de a scrie un polinom $f \in R[X]$, ca un produs finit de polinoame ireductibile de grad ≤ 2.

9) **Fie $n \geq 1$, un număr natural. Notăm cu $m_1, m_2, \ldots, m_r$ numerele naturale mai mici ca n şi prime cu n. Să se arate relațiile:**

a) $\sum_{j=1}^{r} \sin \frac{2m_j \cdot \pi}{n} \cdot = 0$; $\sum_{j=1}^{r} \cos \frac{2m_j \cdot \pi}{n} \in \mathbf{Z}$.

b) n divide $2(m_1+m_2+\ldots..+m_r)$.

Rezolvare.

Cele $r = \varphi(n)$ rădăcini ale unității de ordinul n de forma:

(1) $x_{m_j} = \cos \frac{2m_j \cdot \pi}{n} + i \sin \frac{2m_j \cdot \pi}{n}$, j = 1,2,….,r, se numesc **rădăcini primitive de ordinul n ale unității.** (Fiecare din aceste r rădăcini, este un generator al **grupului ciclic U_n al rădăcinilor de ordin n ale unității** şi aceştia sunt singurii generatori ai lui Un).

Polinomul $\Phi_n(X) = \prod_{j=1}^{r} (X - \cos \frac{2m_j \cdot \pi}{n} - i \sin \frac{2m_j \cdot \pi}{n})$ se numeşte **cel de–al n–lea polinom ciclotomic.** El are gradul $r = \varphi(n)$.

În cele ce urmează, pentru simplitate, vom nota (uneori) o rădăcină a unității(de un anumit ordin) cu ξ, iar prin P_n vom înțelege **mulțimea rădăcinilor primitive de ordin n ale unității.** Avem notațiile:

$$U_n = \{x \in C / x^n = 1\} = \{\cos \frac{2k\pi}{n} + i \sin \frac{2k\pi}{n} / k = 0,1,2,\ldots,n-1\}.$$

$$P_n = \{\cos \frac{2m_j \cdot \pi}{n} + i \sin \frac{2m_j \cdot \pi}{n} / 0 \leq m_j \leq n-1, (m_j, n) = 1, j = 1,2,\ldots,r\}.$$

Observăm că $P_n \subseteq U_n$ şi $\Phi_n(X) = \prod_{\xi \in P_n} (X - \xi)$. Vom demonstra două leme.

Lema 1. Pentru orice $n \in N$, $n \geq 1$, are loc egalitatea: $X^n - 1 = \prod_{d/n} \Phi_d(X)$.

Demonstrație.

Arătăm că familia de mulțimi $\{P_d$ / d divizor natural lui n$\}$, este o partiție a mulțimii U_n a tuturor rădăcinilor de ordin n ale unității. Arătăm că:

1) $U_n = \bigcup_{d/n} P_d$;

2) $P_{d_1} \cap P_{d_2} = \Phi$, pentru orice d_1, d_2 divizori naturali distincți ai lui n.

Pentru a demonstra 1), să observăm, mai întâi, că dacă d_0/n, atunci pentru orice $\xi \in P_{d_0}$ avem $\xi \in U_n$ (căci $\xi^{d_0} = 1$ implică $\xi^n = 1$), ceea ce înseamnă că $P_{d_0} \subseteq U_n$. Rezultă $\bigcup_{d/n} P_d \subseteq U_n$. Pentru cealaltă incluziune ,considerăm un element arbitrar, $\xi \in U_n$, $\xi = \cos\frac{2k\pi}{n} + i \sin \frac{2k\pi}{n}$, cu $0 \le k \le n-1$. Simplificând fracția k/n prin (k,n) obținem o fracție ireductibilă q/d_0, unde $(q,d_0) = 1$ şi d_0 divide n. Atunci elementul $\xi = \cos\frac{2q\pi}{d_0} + i \sin\frac{2q\pi}{d_0}$ aparține mulțimii $\bigcup_{d/n} P_d$.

Pentru a demonstra 2), vom arăta că, dacă există $\xi \in P_{d_1} \cap P_{d_2}$, atunci $d_1 = d_2$.

Într – adevăr, dacă $\xi \in P_{d_1} \cap P_{d_2}$ putem scrie:

$\xi = \cos\frac{2k_1 \cdot \pi}{d_1} + i \sin\frac{2k_1 \cdot \pi}{d_1} = \cos\frac{2k_2 \cdot \pi}{d_2} + i \sin\frac{2k_2 \cdot \pi}{d_2}$, unde $0 \le k_1 \le d_1 - 1$, $(k_1, d_1) = 1$, respectiv $0 \le k_2 \le d_2 - 1$, $(k_1,k_2) = 1$. Rezultă:

$\cos\frac{2k_1 \cdot \pi}{d_1} = \cos\frac{2k_2 \cdot \pi}{d_2}$ şi $\sin\frac{2k_1 \cdot \pi}{d_1} = \sin\frac{2k_2 \cdot \pi}{d_2}$ şi cum $\frac{2k_1 \cdot \pi}{d_1}, \frac{2k_2 \cdot \pi}{d_2} \in [0,2\pi)$

deducem că $\frac{2k_1 \cdot \pi}{d_1} = \frac{2k_2 \cdot \pi}{d_2}$, adică $\frac{k_1}{d_1} = \frac{k_2}{d_2}$. Deoarece un număr rațional pozitiv se reprezintă, în mod unic, ca fracție ireductibilă(cu termeni naturali),din ultima egalitate, rezultă : $k_1 = k_2$ şi $d_1 = d_2$. Ținând seama de rezultatul stabilit, de definiția polinomului ciclotomic şi de descompunerea în factori liniari a polinomului $X^n - 1$, putem scrie:

$X^n - 1 = \prod_{\xi \in U_n} (X - \xi) = \prod_{\xi \in \bigcup_{d/n} P_d} (X - \xi) = \prod_{d/n} \prod_{\xi \in P_d} (X - \xi) = \prod_{d/n} \Phi_d(X)$ şi lema 1 este demonstrată.

Lema 2. Pentru orice $n \in N$, $n \ge 1$, polinomul $\Phi_n(X)$ are coeficienți întregi.

Demonstrație: prin inducție după n.

Pentru n = 1, avem: $\Phi_1(X) = X - 1 \in Z[X]$.

Presupunem teorema adevărată pentru toate polinoamele $\Phi_k(X)$, k<n şi să o demonstrăm şi pentru n. Conform lemei 1, avem:

$\Phi_n(X) = \frac{X^n - 1}{\prod_{d/n, d<n} \Phi_d(X)}$; polinoamele $\Phi_d(X)$ cu d<n sunt în baza ipotezei de inducție, polinoame cu coeficienți întregi şi sunt polinoame unitare(orice polinom ciclotomic este unitar, adică are coeficientul dominant egal cu 1 – din definiție).

Rezultă că polinomul g = $\prod_{d/n,d<n} \Phi_d(X)$ este un polinom unitar cu coeficienți întregi.

Dar polinomul $\Phi_n(X)$ este câtul împărțirii polinomului $X^n - 1 \in Z[X]$, prin polinomul unitary $g \in Z[X]$. Ținând seama de modul efectiv cum se face o împărțire de polinoame, rezultă că acest polinom cât este cucoeficienți întregi. Aşadar, $\Phi_n(X) \in Z[X]$ şi, lema 2 este demonstrată.

a) Polinomul ciclotomic $\Phi_n(X)$ are rădăcinile $\chi_{m_1}, \ldots, \chi_{m_r}$, care apar în (1). Ținând seama că $\Phi_n(X)$ este un polinom unitar şi are coeficienții întregi (lema 2), folosind formulele lui Viete, rezultă că suma $\chi_{m_1} + \ldots + \chi_{m_r}$ este un număr întreg. Aşadar $\sum_{j=1}^{r}(\cos\frac{2m_j \cdot \pi}{n} + i \sin\frac{2m_j \cdot \pi}{n}) \in Z$, adică $(\sum_{j=1}^{r}(\cos\frac{2m_j \cdot \pi}{n}) + i$ $(\sum_{j=1}^{r}\sin\frac{2m_j \cdot \pi}{n}) \in Z$, de unde rezultă $\sum_{j=1}^{r}\sin\frac{2m_j \cdot \pi}{n} = 0$ şi $\sum_{j=1}^{r}(\cos\frac{2m_j \cdot \pi}{n}) \in Z$.

b) Pentru n = 1 şi n = 2 se verifică uşor. Pentru $n \geq 3$, demonstrăm că n divide $m_1 + m_2 + \ldots + m_r$. Avem:

$$\Phi_n(-1) = \prod_{j=1}^{r}(-1 - \cos\frac{2m_j \cdot \pi}{n} - i \sin\frac{2m_j \cdot \pi}{n}) =$$

$$= (-1)^r \prod_{j=1}^{r}[2\cos\frac{m_j \cdot \pi}{n}(\cos\frac{m_j \cdot \pi}{n} + i \sin\frac{m_j \cdot \pi}{n})] =$$

$$= (-1)^r 2^r(\prod_{j=1}^{r}\cos\frac{m_j \cdot \pi}{n})\,(\cos\frac{\sum_{j=1}^{r} m_j \cdot \pi}{n} + i \sin\frac{\sum_{j=1}^{r} m_j \cdot \pi}{n}).$$

Deoarece $\Phi_n \in Z[X]$, rezultă că $\Phi_n(-1)$ este un număr real (chiar întreg), deci $\sin\frac{\sum_{j=1}^{r} m_j \cdot \pi}{n} = 0$.

Există atunci q natural, astfel încât $\frac{\sum_{j=1}^{r} m_j \cdot \pi}{n} = q\pi$, deci $\sum_{j=1}^{r} m_j = qn$.

10) Să se calculeze polinoamele ciclotomice: $F_1, F_2, \ldots, F_6$ şi F_p, pentru p număr prim.

Reamintim că, polinomul minimal al unei rădăcini primitive a unității(şi deci a tuturor rădăcinilor primitive) de grad n, se numeşte **al n-lea polinom ciclotomic** şi se notează cu F_n (sau cu Φ_n). (Avem relația: $X^n - 1 = \prod_{d/n} F_d$, $d \geq 1$; $n = \sum_{d/n} \varphi_d$; $d \geq 1$.)

Evident, $F_1 = X - 1$

$F_2 = X + 1$ (-1 este rădăcina primitivă de grad 2 a unității, {-1,1} este grupul rădăcinilor 2 – are ale unității).

$F_3 = X^2 + X + 1$ ($X^3 - 1 = F_1 F_3 = (X - 1)F_3$).

Polinomul F_4 se obține făcând câtul: $\frac{X^4-1}{\prod_{d/4;d\neq 4} F_d} = \frac{(X^2-1)(X^2+1)}{(X-1)(X+1)} = X^2+1$

La fel $F_6 = \frac{X^6-1}{\prod_{d/6;d\neq 6} F_d} = \frac{(X^3-1)(X^3+1)}{(X-1)(X+1)(X^2+X+1)} = X^2-X+1.$

$F_p = \frac{X^p-1}{F_1} = X^{p-1} + X^{p-2} + \ldots.+X + 1$. În particular $F_5 = X^4 + X^3 + X^2 + X + 1$.

11) Fie μ :N $\to$ Z, funcția definită prin

$\mu(n) =$

$$\begin{cases} 0, & \text{dacă } n \text{ se divide prin pătratu unui numău prim.} \\ (-1)^k, & \text{dacă } n = p_1 \ldots p_k \text{ unde } \{p_i\} \text{ sunt numere prime distincte.} \\ 1, & \text{dacă } n = 1. \end{cases}$$

Să se arate că:

i) μ este funcție multiplicativă, adică μ (nm) = μ (n) μ (m), dacă (n,m) $\cong$ 1;

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

iii) $F_n(X) = \prod_{d/n} (X^{n/d} - 1)^{\mu(d)}$ **, unde F_n(X) este al n-lea polinom ciclotomic.**

Funcția μ se numeşte funcția lui Mobius.

Rezolvare.

ii) Fie n>1, $n = \prod_{i=1}^{s} p_i^{r_i}$, $p_i \neq p_j$, pentru $i \neq j$. Singurii divizori d ai lui n, pentru care μ (d) $\neq$ 0, sunt :

$\{1, p_1, p_2, \ldots, p_n, p_1p_2, \ldots, p_ip_j, \ldots., p_1p_2p_3, \ldots., p_ip_jp_n, \ldots\ldots., p_1p_2\ldots\ldots p_s\}$. Deci $\sum_{d/n} \mu(d) =$

$= \mu(1) + \sum_{i=1}^{s} \mu(p_i) + \sum_{i<j} \mu(p_ip_j) + \ldots.+ \mu(p_1p_2\ldots.p_n) = 1 - C_s^1 + \ldots.+(-1)^s C_S^S =$

$= (1-1)^s = 0.$

iii) Notăm $g(d) = X^d - 1$. Folosind : $X^n - 1 = \prod_{d/n} F_d$, avem: $g(n) = \prod_{d/n} F_d$ şi deci

$$\prod_{d/n} g(\frac{n}{d})^{\mu(d)} = \prod_{d/n} \prod_{d'/\frac{n}{d}} F_{d'}^{\mu(d)} = \prod_{dd'/n} F_{d'}^{\mu(d)} = \prod_{d'/n} F_{d'}^{\sum_{d/\frac{n}{d'}} \mu(d)} = F_n, \text{ în baza lui ii).}$$

12) Să se determine F_{p^n} $F_{p^nq^m}$ $F_{p^nq^mt^s}$ pentru p,q,t numere prime distincte, iar n,m,s $\in$ N. Observați că $F_{p^n} = F_p(X^{p^{N-1}})$, $F_{p^nq^m} = F_{pq}(X^{p^{n-1}q^{m-1}})$ şi

$F_{p^n q^m t^s} = F_{pqt}(X^{p^{n-1}q^{m-1}t^{s-1}})$.

Să se scrie efectiv forma polinoamelor: F_8 , F_9 , F_{10} , F_{12} , F_{72} , F_{180}.

Rezolvare.

Folosind exercițiul precedent, avem:

$F_{p^n} = (X^{p^n} - 1)^{\mu(1)} (X^{p^{n-1}} - 1)^{\mu(p)} \prod_{i\geq 2}^{n} (X^{p^{n-i}} - 1)^{\mu(p^i)}$. Dar $\mu(p^i) = 0$, pentru i≥2 şi rezultă: $F_{p^n} = \dfrac{X^{p^n} - 1}{X^{p^{n-1}} - 1} = X^{p^{n-1}(p-1)} + X^{p^{n-1}(p-2)} + \ldots\ldots + 1$. Deci $F_{p^n} = F_p(X^{p^{n-1}})$.

Folosind exercițiul precedent, obținem: $F_{p^n q^m} =$

$= (X^{p^n q^m} - 1)^{\mu(1)} (X^{p^{n-1}q^m} - 1)^{\mu(p)} (X^{p^n q^{m-1}} - 1)^{\mu(q)} (X^{p^{n-1}q^{m-1}} - 1)^{\mu(pq)}$, deoarece pentru ceilalți divizori d avem $\mu(d) = 0$. Rezultă:

$F_{p^n qm} = \dfrac{(X^{p^n q^m} - 1)(X^{p^{n-1}q^{m-1}} - 1)}{(X^{p^{n-1}qm} - 1)(X^{p^n q^{m-1}} - 1)} = \dfrac{(Y^{pq} - 1)(Y - 1)}{(Y^q - 1)(Y^p - 1)}$, unde $Y = X^{p^{n-1}q^{m-1}}$, adică

$F_{p^n q^m} = F_{pq}(X^{p^{n-1}q^{m-1}})$, iar $F_{pq} = \dfrac{X^{p(q-1)} + X^{p(q-2)} + \ldots + 1}{X^{q-1} + X^{q-2} + \ldots\ldots + 1}$.

Obținem:

$F_8 = F_{2^3} = F_2(X^{2^2}) = X^4 + 1$, $F_9 = F_{3^2} = F_3(X^3) = X^6 + X^3 + 1$,

$F_{10} = \dfrac{X^5 + 1}{X + 1} = X^4 - X^3 + X^2 - X + 1$, $F_{12} = F_{2^2 3} = F_6(X^2) = X^4 - X^2 + 1$,

$F_{72} = F_6(X^{2^2 3}) = X^{24} - X^{12} + 1$. Analog, deducem: $F_{180} = F_{30}(X^6)$, unde

$F_{30} = \dfrac{(X^{30} - 1)(X^3 - 1)(X^5 - 1)(X^2 - 1)}{(X^6 - 1)(X^{15} - 1)(X^{10} - 1)(X - 1)} = \dfrac{X^{15} + 1}{(X^5 + 1)(X^2 - X + 1)} = \dfrac{X^{10} - X^5 + 1}{X^2 - X - 1} =$

$= X^8 + X^7 - X^5 - X^4 - X^3 + X + 1$.

Deci $F_{180} = X^{48} + X^{42} - X^{30} - X^{24} - X^{18} + X^6 + 1$.

13) Să se descompună în factori ireductibili în Z[X], polinomul: $X^{12} - 1$.

Rezolvare.

$X^{12} - 1 = \prod_{d/12} F_d$. Deoarece F_d sunt toți ireductibili, rezultă că descompunerea dată, este exact descompunerea lui $X^{12} - 1$ în factori ireductibili.

Deci $X^{12} - 1 = F_1 F_2 F_3 F_4 F_6 F_{12} =$

$= (X - 1)(X + 1)(X^2 + X + 1)(X^2 + 1)(X^2 - X + 1)(X^4 - X^2 + 1)$, conform exercițiilor 10 şi 12.

14) Fie K un corp algebric închis, q un număr natural prim diferit de caracteristica lui K, iar U_n grupul rădăcinilor de grad n ale unității din K (n>2).

Să se arate că:

$V_q = \bigcup_{t \in N} U_{q^t}$ **este un subgrup al grupului multiplicativ al elementelor nenule din K, izomorf cu Z_q / Z, unde Z_q este inelul de fracţii al lui Z în raport cu sistemul multiplicativ {1, q, ….., q^s,….}.**

Rezolvare

Fie $\xi \neq 1$ o rădăcină q – ară a unităţii în K. Observăm că orice rădăcină x a ecuaţiei $X^{q^t} - \xi$ este rădăcină primitivă în $U_{q^{t+1}}$. Într-adevăr, dacă ordx < q^{t+1}, atunci ar rezulta ordx/q^t, deoarece ordx/q^{t+1}, căci $x^{q^{t+1}} = \xi^q = 1$. Obţinem 1 = $x^{q^t} = \xi$, ceea ce este fals. Construim prin recurenţă şirul următor:

$x_1 = \xi$, $x_2 = \xi^{1/q}$ (adică o rădăcină a ecuaţiei $x^q = \xi$),….,$x_{i+1}=x_i^{1/q}$,….

Evident x_i generează U_{q^i}.

Fie aplicaţia $f_q : Z_q/Z \to V_q$, definită prin $\frac{f}{q}(\text{cls}\frac{m}{q^t} \text{mod} Z) = x_t^m$, unde $t \in N$, iar $m \in Z$.

Dacă $\frac{m}{q^t} \equiv \frac{m'}{q^{t'}} \text{mod} Z$, atunci $\frac{m}{q^t} = \frac{m'}{q^{t'}} + r$, $r \in Z$. Presupunem de exemplu, t > t'. Avem :

$x_i^m = x_i^{m'q^{t-t'}+rq^t} = x_t^{m'q^{t-t'}} = x_{t'}^{m'}$ (deoarece $x_i^{q^{t-t'}} = x_{t'}$) şi rezltă că f_q este bine definită. Evident, f_q este morfism de grupuri şi $\ker f_q = (0)$. Dar, observăm că $x_i \in \text{Im} f_q$ pentru orice $i \geq 1$. Cum $\{x_i\}_{i \geq 1}$ generează V_q, deducem că f_q este izomorfism.

15) Fie k un corp finit de caracteristică p > 0. Să se arate că:

i) Pentru orice număr natural n, există un polinom ireductibil de grad n, în k[X];

ii) Pentru orice polinom P ireductibil în k[X], există $n \in N$, astfel încât:

P/ X^{p^n} - X.

Rezolvare.

i) k fiind finit, are un număr de p^s elemente, $s \geq 1$. Fie $n \in N$ şi G $GF_{p^{sn}}$ corpul de descompunere al polinomului $X^{p^{sn}} - X$ peste k. Fie $x \in GF^*_{p^{sn}}$ un gerator al grupului multiplicativ $GP^*_{p^{sn}}$. Avem : k(x) = $GF_{p^{sn}}$ şi [k(x):k] = n. Evident minimal al lui x este ireductibil în k[X] şi de grad n.

ii) Fie P un polinom ireductibil din k[X] şi x o rădăcină a sa într-o extindere a lui k. Evident k(x) este încă finit şi coincide cu mulţimea rădăcinilor unui polinom de forma:

$X^{p^n} - X$, $n \in N$, într-o extindere algebric închisă a lui k. În particular, avem

x^{p^n} - x = 0 şi deci P/ $X^{p^n} - X$.

16) Să se afle care dintre următoarele extinderi sunt normale:

i) $Q \subseteq Q(a)$, unde a este o rădăcină a polinomului $X^3 - 2$.

ii) $Q(i,\sqrt{3}) \subseteq Q(I,\sqrt{3}$,b), unde b este o rădăcină a polinomului $X^3 - 2$.

iii) $GF_2(X^2) \subseteq GF_2(X)$.

iv) $GF_2 \subseteq GF_2[X]/(X^3+X+1)$.

Rezolvare.

$X^3 - 2$ are în Q(a) doar rădăcina a. Deci, i) nu este noemală.

Extinderea ii) este normală, deoarece rădăcinile lui $X^3 - 2$ sunt de forma: a, ρ a, ρ^2 a, iar $\rho = \frac{-1+i\sqrt{3}}{2} \in$ Q(i, $\sqrt{3}$).

Extinderea iii) este corpul de descompunere al polinomului $Y^2 - X^2 \in$ $\in GF_2(X^2)[Y]$ (ambele soluții (X) coincide), deci este normală.

Extinderea iv) este normală,deoarece orice extindere finită a unui corp finit este normală.

17) Să se arate că orice extindere algebrică a unui corp perfect este perfect.

Fie k un corp perfect şi k ⊆ K, o extindere algebrică a lui k. Deci k ⊆ L este o extindere separabilă. Deducem că extinderea K ⊆ L este separabilă, şi deci K este perfect.

18) Fie k ⊆ K o extindere de tip finit de corpuri, de caracteristică p> 0. Să se arate că dacă K este un corp perfect, atunci extinderea k ⊆ K este algebrică şi k este un corp perfect.

Rezolvare.

Dacă x ∈ K, este un transcendent peste k, atunci $x^{1/p^s} \in$ K, pentru orice s ∈ N, K fiind perfect. Dar extinderea k → k(x, $x^{1/p}$, …., x^{1/p^s} ,….)nu poate fi de tip finit, ceea ce contrazice ipoteza. Deci k ⊆ K este algebrică.

Dacă k nu este perfect, alegem x ∈ k – k^p, ca şi mai sus, K conține k($x^{1/p}$, x^{1/p^2} ,…., x^{1/p^s} ,…) şi nu poate fi de tip finit peste k.

19) Să se găsească elementul primitiv al extinderilor Q ⊆ Q($\sqrt{3}$, $\sqrt{7}$), Q ⊆ Q($\sqrt{3}$, $\sqrt[3]{2}$), $GF_5(X^5) \subseteq GF_5(X)$.

Are extinderea $GF_5(X^5, Y^5) \subseteq GF_5(X, Y)$ **un element primitiv?**

Rezolvare.

Elementul $\sqrt{3}+\sqrt{7}$ generează prima extindere, deoarece $1 \neq \frac{\sqrt{3}-(-\sqrt{3})}{\sqrt{7}-(-\sqrt{7})}$, şi este şi suficient, conform demonstrației teoremei elementului primitiv.

Similar, observăm că $\sqrt[3]{2}$ +i$\sqrt{3}$, generează a doua extindere, deoarece $1 \neq \frac{i\sqrt{3}-(-i\sqrt{3})}{\sqrt[3]{2}(1-\frac{-1+i\sqrt{3}}{2})}$. Extinderea, admite ca element primitiv, pe orice element de forma: $\sqrt[3]{2} + ai\sqrt{3}$, cu a ∈ Q – {0}.

A treia extindere este generată de X(are element primitiv, deşi nu este separabilă)

Extinderea $GF_5(X^5, Y^5) \subseteq GF(X, Y)$, nu admite un element primitive.

Într -adevăr, dacă P$\in GF_5(X,Y)$, atunci:
$[GF_5(X^5,Y^5,P): GF_5(X^5,Y^5)] \leq 5$, deoarece P este soluție a polinomului $Z^5 - P^5 \in GF_5(X^5,Y^5)[Z]$.Pe de altă pare, avem:
$[GF_5(X^5,Y) : GF_5(X^5,Y^5)]=5$ şi $[GF_5(X,Y): GF_5(X^5,Y)]=5$, întrucât XşiY sunt soluții ale polinoamelor $Z^5 - X^5$ respectiv $Z^5 - Y^5$. Deci gradul extinderii $GF_5(X^5,Y^5) \subseteq GF_5(X,Y)$ este 25, şi nu putem avea $GF_5(X^5,Y^5,P) = GF_5(X,Y)$. Teorema citată nu se aplică, extinderea nefiind separabilă.

20) Fie k un corp de caracteristică p> 0, f = X^p – X + a $\in$k[X], un polinom ireductibil şi x o rădăcină a lui f într–o închidere algebrică a lui k. Să se arate că extinderea k$\subseteq$k(x) este normală şi separabilă. Determinați grupul Galois G(k(x)/k).

Rezolvare.

Polinomul f are, în k(x) soluțiile:{x, x+1,….,x+p-1}, care sunt evident diatincte. Într-adevăr, dacă $0 \leq i<p$, atunci avem
$(x+i)^p – (x+i)+a = x^p –x+a+i^p –I = 0$, deoarece i$\in GF_p \subseteq$k şi elementele lui GF_p sunt soluțiile ecuației $X^p = X$. Deci k(x) este corpul de descompunere al polinomului f peste k. În plus x fiind separabil, extinderea k$\subseteq$k(x) este separabilă şi deci galoisiană de grad p. Deci G(k(x)/k) are p elemente, de unde rezultă:
G(k(x)/k)$\cong$Z/pz.

k-automorfismul u:k(x)$\rightarrow$k(x), definit prin u(x) = x+1, generează, evident G(k(x)/k), adică avem G(k(x)/k) = {1,u,u^2,….,u^{p-1}}.

21) Fie K corpul de descompunere al polinomului $X^3 – 2$ peste Q. Determinați grupul Galois G(K/Q) şi toate subcorpurile lui K. Care dintre acestea sunt extinderi normale ale lui Q?

Rezolvare.

Avem: K = Q(i$\sqrt{3}$, $\sqrt[3]{2}$) şi [K:Q] = 6. Deci G(K/Q) are 6 elemente(extinderea Q$\subseteq$K este galoisiană, deoarece ea este normală(corp de descompunere al unui polinom) şi separabilă(caracteristică zere)), el este izomorf cu S_3 sau cu Z/6Z.

Arătăm că el este izomorf cu S_3 .

A da un Q-automorfism u al lui K revine la a da u(i$\sqrt{3}$) şi u($\sqrt[3]{2}$), care nu pot fi decât rădăcini conjugate cu i$\sqrt{3}$, respectiv $\sqrt[3]{2}$. Alcătuim următorul tabel:

	I	u	v	vu	v^2	$v_u{}^2$
$\sqrt[3]{2}$	$\sqrt[3]{2}$	$\sqrt[3]{2}$	$\rho\sqrt[3]{2}$	$\rho\sqrt[3]{2}$	$\rho^2\sqrt[3]{2}$	$\rho^2\sqrt[3]{2}$
i$\sqrt{3}$	i$\sqrt{3}$	- i$\sqrt{3}$	i$\sqrt{3}$	- i$\sqrt{3}$	i$\sqrt{3}$	- i$\sqrt{3}$

unde $\rho = \frac{-1+i\sqrt{3}}{2}$, ($\rho^2$ este conjugata lui ρ). Calculele au fost făcute ţinând cont de alegerea lui u şi v, adică: $(uv)(\sqrt[3]{2}) = v(\sqrt[3]{2}) = \rho\sqrt[3]{2}$ şi $(vu)(i\sqrt{3}) = v(-i\sqrt{3}) = -i\sqrt{3}$. Evident, $(uv)(\sqrt[3]{2}) = u(\rho\sqrt[3]{2}) = u(\rho)u(\sqrt[3]{2}) = \rho^2\sqrt[3]{2}$, $(uv)(i\sqrt{3}) = u(i\sqrt{3}) = -i\sqrt{3}$, deci $uv = v^2u \neq vu$, adică G(K/Q) este necomutativ şi izomorf cu S_3 ($u \to$ transpoziţie; $v \to$ permutare pară $\neq I$, adică ciclu de lungime trei).
Subgrupurile proprii ale lui G(K/Q) sunt:

$H_1 = \{I,u\}$, $H_2 = \{I, vu\}$, $H_3 = \{I,v^2u\}$ şi $H_4 = \{I,v,v^2\}$.

Determinăm subcorpurile lui K fixate de ele. Evident, u invariază $Q(\sqrt[3]{2})$; deci F_1(notăm prin F_i, i = 1,..,4, corpul fixat de H_i), conţine $Q(\sqrt[3]{2})$. Conform teoriei lui Galois, avem :$[K : F_1] = ord H_1 = 2$. Pe de altă parte, $[K:Q(\sqrt[3]{2})] = 2$, de unde rezută: $[F_1:Q(\sqrt[3]{2})] = 1$, adică $F_1 = Q(\sqrt[3]{2})$. La fel, observăm că:

$F_2 = Q(\rho^2\sqrt[3]{2})$, $F_3 = Q(\rho\sqrt[3]{2})$ şi $F_4 = Q(i\sqrt{3})$. Deoarece F_4 este extindere pătratică a lui Q, ea este o extindere normală.

Extinderile F_i/Q, i=1,2,3 nu sunt normale. Observăm că H_i nu sunt subgrupuri normale în G(K/Q), pentru i=1,2,3 pe când H_4 subgrup normal, deoarece are idicele 2.

22) Determinaţi grupul lui Galois $Q \subseteq Q(i,\sqrt[4]{2})$ şi toate subcorpurile lui $Q(i,\sqrt[4]{2})$. Care dintre acestea, sunt extinderi normale ale lui Q?

Rezolvare.

Observăm că extinderea $Q \subseteq Q(\sqrt[4]{2})$ are gradul 4, X^4-2 este polinomul minimal al lui $\sqrt[4]{2}$, iar extinderea $Q(\sqrt[4]{2}) \subseteq Q(\sqrt[4]{2},i)$ are gradul 2.
Deci $G(Q(i,\sqrt[4]{2})/Q)$ are 8 elemente(extindera $Q \subseteq Q(i,\sqrt[4]{2})$ este galoisiană, deoarece este normală(este corpul de descompunere al polinomului X^4-2) şi evident separabilă).
Descriem modul cum acţionează elementele lui $G(Q(i,\sqrt[4]{2})/Q)$, pe generatorii extinderii din următorul tabel:

	I	u	v	v^2	v^3	vu	uv	v^2u
$\sqrt[4]{2}$	$\sqrt[4]{2}$	$\sqrt[4]{2}$	$i\sqrt[4]{2}$	$-\sqrt[4]{2}$	$-i\sqrt[4]{2}$	$i\sqrt[4]{2}$	$-i\sqrt[4]{2}$	$-\sqrt[4]{2}$
i	i	-i	i	i	i	-i	-i	-i

Deci G este necomutativ ($vu \neq uv$) şi cum $v^4 = u^2 = I$, deducem că el este diedral.
Subgrupurile proprii ale G sunt:
$H_1 = \{I,u\}$, $H_2 = \{I,v,v^2, v^3\}$, $H_3 = \{I,v^2\}$, $H_4 = \{I,vu\}$, $H_5 = \{I,u,v\}$, $H_6 = \{I, v^2, u\}$, $H_7 = \{I,v^2,u , v^2u\}$, $H_8 = \{I, vu, uv, v^2\}$.
Determinăm corpurile F_i, i = 1,2,…,8 fixate de H_i. Evident, H_1 invariază pe $Q(\sqrt[4]{2})$ şi cum $[Q(\sqrt[4]{2},i):Q(\sqrt[4]{2}] = 2 = ord H_1$, rezultă $F_1 = Q(\sqrt[4]{2})$. La fel $F_2 = Q(i)$, $F_3 = Q(i,\sqrt[4]{2})$.

Un element $\notin Q$ invariat de vu, se găseşte mai greu, de aceea procedăm astfel :

i) Găsim un element x al extinderii $Q \subseteq Q(i, \sqrt[4]{2})$(de exemplu: $i+\sqrt[4]{2}$).

ii) Observăm că $y = x+(vu)(x)$ este invariant de vu (dacă ord vu ar fi fost n, atunci am fi luat $x+(vu)(x)+\ldots..+(vu)^{n-1}x$).

În cazul nostru $y = \sqrt[4]{2} + i + i\sqrt[4]{2} - i = \sqrt[4]{2}(1+i)$. Avem extinderea: $Q \subseteq Q(\sqrt[4]{2}(1+i))$ de grad 4, căci $Q \subseteq Q(i\sqrt{2})$ este de grad 2(polinomul minimal fiind X^2+2), iar $Q(i\sqrt{2}) \subseteq Q(\sqrt[4]{2}(1+i))$ este tot de grad2(polinomul minimal fiind: $X^2-2i\sqrt{2}$). Deci $[Q(\sqrt[4]{2}, i): Q(\sqrt[4]{2}(1+i))] = 2 = \text{ord } H_4$, de unde rezultă $F_4 = Q(\sqrt[4]{2}(1+i))$.

La fel $F_7 = Q(\sqrt{2})$,iar $F_8 = Q(i\sqrt{2})$(atenție F_3 conține strict F_8).

Se observă că F_2, F_7, F_8 sunt extinderi normale ale lui Q,fiind pătratice(sau H_2, H_7, H_8 sunt de indice 2).

De asemenea $Q \subseteq F_3$ este normală, fiind corpul de descompunere al lui $(X^2+1)(X^2-2)$.

F_4 şi F_5 nu sunt extinderi normale ale lui Q, deoarece H_4, H_5 nu sunt divizori normali(de exemplu: $v^{-1}(vu)v = uv \notin H_4$).

Evident, F_1 şi F_6 nu sunt extinderi normale ale lui Q.