MINISTERIL ÎNVĂȚĂMÎNTULUI
AL REPUBLICII MOLDOVA
UNIVERSITATEA DE STAT DIN TIRASPOL

Catedra de algebră superioară

B.Țarălungă, V.Bordan

ELEMENTE DIN TEORIA EXTINDERILOR ALGEBRICE A CÂMPURILOR

(Indicații metodice)

Chișinău 1996

PREFAȚĂ

Prezenta lucrare metodică se adresează studenților matematiceni dar si celor interesați de matematică.

Scopul lucrării este de a prezenta elementele de bază din teoria extinderilor finite a câmpurilor și unele proprietăți elementare a câmpurilor finite, cât și o metodă de construire a câmpurilor finite.

Lucrarea este structurată în trei paragrafe: în primul paragraf sunt expuse unele tipuri de extinderi a câmpurilor și relațiile între ele, în paragraful doi se expun proprietățile elementare a câmpurilor finite și metoda de construire a lor, iar în paragraful trei se propun spre rezolvare un set de probleme. Bibliografia cuprinde acele surse pe care autorii s-au bazat la întocmirea acestei lucrări.

§1.Elemente din teoria extinderilor finite a câmpurilor.

1.1.Noțiune de extindere, element algebric și polinom minimal.

Să reamintim, că prin câmp înțelegem un inel comutativ $(F,+,\cdot)$ cu unitatea 1, $0 \neq 1$ și orice element $a \in F, a \neq 0$ este simetrizabil în raport cu înmulțirea, $\forall\, a \in F, a \neq 0\ \exists\ a^{-1} \in F$, astfel încât $a \cdot a^{-1} = a^{-1} \cdot a = 1$.

***Exemple*.**

1) $(\mathbb{Q},+,\cdot)$ câmpul numerelor raționale.
2) $(\mathbb{R},+,\cdot)$ câmpul numerelor reale.
3) $(\mathbb{C},+,\cdot)$ câmpul numerelor complexe.
4) $(\mathbb{Z}_p,+,\cdot)$ câmpul claselor de restul modulo – p ,p – număr prim

Fie un câmp F, încât $F \subset E$.Atunci E se numește extindere a câmpului F.

Exemple.

1. Câmpul numerelor reale este extindere a câmpului numerelor raționale, $\mathbb{R} \supset \mathbb{Q}$.
2. Câmpul numerelor complexe este extindere a câmpului numerelor reale, $\mathbb{C} \supset \mathbb{R}$.
3. Câmpul din 4 elemente este extindere a câmpului claselor de resturi modulo 2 .

Fie $F \subset E$ și $\alpha \in E$. Pot fi două cazuri:

I. Există un polinom $f(x) \neq 0$ cu coeficienți din câmpul F, încât α este soluția a polinomului $f(x)$: $f(\alpha) \neq 0$. În caz de α se numește elemente algebrice a lui E este F.

II. Nu există nici un polinom nenul cu coeficienți din F pentru care α să fie soluție. În acest caz α se numește element transcendent al câmpului E pentru cîmpul F.

Să observăm, că orice element din F este element algebric peste F. Este evident și faptul, că orice element algebric peste F este element algebric și peste orice extindere a lui F.

Să menționăm că afirmația inversă nu are loc în general. De exemplu orice număr complex este număr algebric peste câmpul numerelor reale $\mathbb{R}$, însă există numere (chiar reale) care nu sunt numere algebrice peste câmpul numerelor raționale. Astfel de numere sunt numerele e, π.

Se poate demonstra, ca subinelul E, generat de submulțimea $F \cup \{\alpha\}$ este izomorf inelului de polinoame $F[x]$ peste F de o singură variabilă x.

Izomorfismul se stabilește în modul următor: Dacă $f(x) \in F[x]$, atunci lui $f(x)$ i se pune în corespondență elementul $f(\alpha)$ din E.

Reamintim, că polinomul $g(x) \in F[x]$ se numește ireductibil, dacă nu există două polinoame $g_1(x), g_2(x)$ de grade nenule mai mici decât gradul lui $g(x)$, încât $g(x) = g_1(x) \cdot g_2(x)$.

Fie că avem o extindere E a unui câmp F și un element algebric α al câmpului E peste F. Aceasta înseamnă, conform definiției de mai sus, că există un polinom $f(x) \in F[x]$, încât $f(\alpha) = 0$.

Este evident că acest polinom nu-i unic ce posedă proprietatea indicată. (Dacă $g(x) \neq 0$ este un polinom arbitrar, atunci $g(x)f(x) \neq 0$ și $g(\alpha)f(\alpha) \neq 0$)

În mod firesc apare întrebarea: Pot fi indicate unele restricții peste polinomul $f(x)$ pentru care elementul α este rădăcină, încât $f(x)$ să fie unic?

Vom demonstra că această întrebare se rezolvă în mod afirmativ.

Definiția 1.1 Polinomul $f(x)$ se numește polinom minimal al elementului algebric α, dacă gradul polinomului $f(x)$ este minimal în mulțimea polinoamelor pentru care este soluție.

Teorema 1.2 Fie F un câmp, E o extindere a lui, iar $\alpha \epsilon E$ un element algebric din E peste F. Dacă $f(x)$ este un polinom minimal a lui α, atunci:

1) $f(x)$ este polinom ireductibil;
2) dacă $g(x)$ este un polinom arbitrar peste F, încât $g(\alpha) = 0$, atunci $f(x)$ devide $g(x)$.

Demonstrație.

1) Presupunem prin absurd, adică fie că există două polinoame $f_1(x), f_2(x)$ de grade nenule și mai mici decât gradul lui $f(x)$, încât $f(x) =$

$f_1(x) \cdot f_2(x)$. Atunci $0 = f_1(\alpha) \cdot f_2(\alpha)$, de unde obținem că $f_1(\alpha) = 0$ ori $f_2(\alpha) = 0$, ceia ce contrazice minimialității polinomului $f(x)$.

2) Fie $g(x)$ un polinom cu coeficienții din F, încât $g(\alpha) = 0$. Conform teoremei despre împărțirea cu rest, $g(x) = q(x)f(x) + r(x)$, unde gradul lui $r(x)$ este mai mic decît gradul lui $f(x)$.

Substituim $x = 0$ și obținem $g(\alpha) = q(\alpha)f(\alpha) + r(\alpha)$, ori $r(\alpha) = 0$. Din minimalitatea lui $f(x)$ avem că $r(x)$=0. De aici $g(x) = q(x)f(x)$, adică $f(x)$ devide $g(x)$.

Corolarul 1.3. Dacă $F \subset E$ și $\alpha \in E$ este un element algebric a lui E peste F, iar $f(x)$ și $g(x)$ sunt două polinoame nimimale ale elementului α, atunci există $c \in F$, încât $f(x) = cg(x)$.

Corolarul 1.4._Dacă $F \subset E$ și $\alpha \in E$ este un element algebric a lui E peste F, atunci polinomul de forma $x^n + a_{n-1}\, x^{n-1} + \cdots + a_1 x + a_0$,$a_0 a_1, a_{n-1} \in P$ este unic.

Remarca 1.5. Polinoamele de forma $x^n + a_{x-1}x^{n-1} + \cdots + a_1 x + a_0$, $a_0, a_1, a_2 \ldots a_{a-1} \in F$ se numesc normate.

Corolarul 1.6 Dacă $F \subset E$ și $\alpha \in E$ este un element algebric a lui E peste F, iar $g(x)$ este un polinom ireductibil din $F[x]$ pentru care $g(\alpha) = 0$, atunci $g(x)$ este polinom minimal pentru α.

Exemple.

1) Pentru numărul $\sqrt{2}$ polinomul minimal peste Q este $f(x) = x^2 - 2$.

2) Pentru numărul $2 - 31$ polinomul minimal peste R este $g(x) = x^2 - 4x + 13$.

3) Pentru numărul $\sqrt{2} + \sqrt{3}$ polinomul minimal peste Q este $n(x) = x^4 - 10x^2 + 1$.

Remarca 1.7 Dacă E este un inel comutativ, P un subinel, a un element arbitrar din E, atunci subinelul T, generat de submulțimea $F \cup \{\alpha\}$, coincide cu submultimea $S = (a + a, d + \cdots .. a_k d^k; a_0, a_1 \ldots \ldots a_k, \in F$, iar k este un numar natural arbitrar.

Într-adevăr, este evident, că $S \subset T$. Invers, S este un subinel ce conține $F \cup \{\alpha\}$, de unde rezultă $T \subset S$. Am obținut că $S = T$.

Teorema 1.3 Fie $F \subset E, \alpha$ un element algebric din E, iar $f(x)$ polinomul minimal de forma $x^n + a_{n-1}x^{n-1} + \cdots + a_1 + a$. Atunci:

1) Subinelul K este generat de submulțimea $F(\alpha)$ este câmp:

2) Din $K = n$

Demonstrație.

1) Fie K subinelul generat de $F \cup (\alpha)$, iar $b_0 + b_1 a + \cdots + b_k a^k \neq 0$ un element arbitrar nenul din F. Considerăm polinomul $b(x) = b_0 + b_1 x + \cdots b_k x^k$. Avem că $b(\alpha) = 0$, deci $f(x)$ nu divide $b(x)$.

Conform *Teoremei 1* $f(x)$ este ireductibil, de unde obtinem că $f(x)$ și $b(x)$ sînt reciproc prime între ele. Atunci există polinoame $c(x)$ și $d(x)$, încît $c(x)b(x) + d(x)f(x) = 1$. Substituim $X = \alpha$ în ultima egalitate obținem $c(\alpha)b(\alpha) = 1$, adică elemental $b(\alpha) = b_0 + b_1 a + \cdots + b_k a^k$ este inversabil în K.

2) Din relația $a^n = \left(a_0 + a_{1,} a + \cdots + a_{n-1} a^{n-1}\right)$ rezultă că subinelul generat de submulțimea $F \cup \{\alpha\}$ coincide cu F – subspațiul vectorial $F + F\alpha + \cdots + Fa^{n-1}$. Submulțimea $\{1, \alpha, \ldots a^{n-1}\}$ generează spațiul vectorial K peste K. De aici avem, că din $K \leq n$.

Fie $t_0, t_1, \ldots . t_{n-1} \in F$. Încît $t_0 + t_1, a + \cdots t_{n-1} a^{n-1} = 0$. Considerăm polinomul $h(x) = t_0 + t_{n-1} a + \cdots + t_{n-1} 2^{-1} \in F[X]$. Relația scrisă mai sus ia forma $h(x) = 0$.

Din minimialitatea polinomului $f(x)$ rezulta că $h(x) = 0$.

În continuare cîmpul K se noteaza cu F(α), iar $dim\ _F E$ se noteaza cu $[K: Y]$.

Corolarul 1.9. Da $[F(\alpha): F] < \infty$ atunci elementul α este element algebric.

Corolarul 1.10. Daca α este element transcendent, atunci sistemul de elemente 1, α, α^n, ..., este liniar independent și $[F(\alpha): F] \in \infty$.

Astfel are loc urmatoarea teorema:

Teorema 1.11. Fie E o careva extindere a cîmpului F. Elementul α este element algebric dacă și numai dacă $[F(\alpha): F] < \infty$.

1.2.Unele tipuri importante de extinderi.

Fie F un subcâmp a câmpului E și $\alpha_1, \alpha_2, \ldots, \alpha_n \in E$.

Definiția 2.1. Extinderea E a câmpului F se numește extindere finită dacă orice element $\beta \leq E$ se exprimă în mod unic sub forma

$$\beta = a_1\alpha_1 + a_2\alpha_3 + \cdots + a_n\alpha_n$$

unde $a_1, a_2, \dots, a_n \in F$. Sistemul de elemente $\alpha_1, \alpha_2, \dots, \alpha_n$ se numește bază a câmpului E peste câmpul F.

Să observam că extinderea finită E a câmpului F poate fi considerată ca spațiu vectorial peste F.

Într-adevar, elementele câmpului E pot fi adunate și înmulțite cu elementele câmpului F, și evident că verific axiomele spațiului vectorial. Din acest punct de vedere extinderea E este extinderea finită dacă și numai dacă ea posedă baza finită peste F.

Definitia 2.2. Extinderea E a câmpului F se numește extinderea finită, daca dimensiunea spațiului vectorial E este finită $dim\ {}_F E = [E:F] < \infty$.

Definitia 2.3. Dimensiunea spatiului vectorial F^E se numeste gradul extinderii E peste F.

Să observam că $dim\ {}_F E = 1$ dacă și numai dacă $E = F$ (demonstrați).

Să studiem acum subcâmpurile câmpului E ce conțin F și elementele $\alpha_1, \alpha_2, \dots, \alpha_n \in E$. Este evident că intersecția acestor subcâmpuri este subcâmp și este minimal în familia subcâmpurilor cu o astfel de proprietate. Această extindere minimală se notează $F(\alpha_1, \alpha_2, \dots, \alpha_n)$.

Definiția 2.4. Câmpul $F(\alpha_1, \alpha_2, \dots, \alpha_n)$ se numește extindere generată de F și elementele $\alpha_{1,}, \alpha_2, \dots, \alpha_n$.

Afirmăm că $F(\alpha_{1,}, \alpha_2, \dots, \alpha_n) = M$, unde

$$M = \left\{ \frac{f(\alpha_{1,}, \alpha_2, \dots, \alpha_n)}{g(\alpha_{1,}, \alpha_2, \dots, \alpha_n)} \mid f(\alpha_{1,}, \alpha_2, \dots, \alpha_n), \right.$$
$$\left. g(\alpha_{1,}, \alpha_2, \dots, \alpha_n) \in F[\alpha_{1,}, \alpha_2, \dots, \alpha_n], g(\alpha_{1,}, \alpha_2, \dots, \alpha_n) \neq 0 \right\}.$$

Într-adevăr, cum $F(\alpha_{1,}, \alpha_2, \dots, \alpha_n)$ este câmp generat de F și $\alpha_{1,}, \alpha_2, \dots, \alpha_n$ atunci el conține și fracțiile $\frac{f(\alpha_{1,}, \alpha_2, \dots, \alpha_n)}{g(\alpha_{1,}, \alpha_2, \dots, \alpha_n)}$ $deci\ M \subset F(\alpha_{1,}, \alpha_2, \dots, \alpha_n)$. Invers, mulțimea fracțiilor din M formează cîmp și conține F și $\alpha_{1,}, \alpha_2, \dots, \alpha_n$, deci $F(\alpha_{1,}, \alpha_2, \dots, \alpha_n) \subset M$.

Este evident că $F(\alpha_{1,}, \alpha_2, \dots, \alpha_n) = F$ dacă și numai dacă $\alpha_{1,}, \alpha_2, \dots, \alpha_n \in F$.

Definiția 2.4 Extinderea E a câmpului F se numește algebraic generată, dacă E este generată de F și de sistemul finit de elemente algebrice $\alpha_{1,}, \alpha_2, \dots, \alpha_n$. Se notează $E = F(\alpha_{1,}, \alpha_2, \dots, \alpha_n)$.

Definiția2.5. Extinderea E generată de F și elemental algebric a se numește extindere algebrică simplă și se notează $E = F(a)$.

Definiția 2.6. Extinderea E a câmpului F se numește extindere algebrică compusă, dacă există un astfel de lanț crescător de subcâmpuri $F \subset L_0 \subset L_1 \subset \cdots \subset L_n = E$ încât pentru orice $i = 1,2,\dots,n$ subcâmpul L_i este extindere algebrică simplă a subcâmpului L_{i-1}. Dacă $L_i = L_{i-1}(a_{i,}), i = 1, \dots . . n$ atunci câmpul E se notează $F(a_{1,})(a_2) \dots . (a_{n,})$.

Să observăm, că în definiția dată elementele $\alpha_{1,}, \alpha_2, \dots, \alpha_n$ nu se presupun a fi elemente algebrice peste F.

Definiția 2.7. Extinderea E a câmpului F se numește extindere algebrică, dacă orice element din Eeste element algebric peste F .

Astfel noi am introdus următoarele tipuri de extinderi:

1° Extinderi finite;
2° Extinderi algebric generate;
3° Extinderi algebrice compuse;
4° Extinderi algebrice simple;
5° Extinderi algebrice.

În cele ce urmează vom cerceta relațiile între aceste tipuri de extinderi cît și structura fiecărei dintre extinderi cu excepția extinderilor algebrice.

1.3. Relații între tipurile de extinderi și structura extinderilor

Teorema 3.1. Orice extindere finită E a câmpului F este extindere algebrică.

*Demonstrație***.** Notăm cu n dimensiunea spațiului vectorial ${}_FE$. Dacă $n = 0$ teorema este evidentă. Considerăm acum cazul $n > 0$. Orice sistem din $n + 1$ elemente din E este liniar dependent. În caz particular, sistemul de elemente $1, \alpha, \alpha^2, \dots, \alpha^n$ este liniar dependent, pentru orice element α din E. Există astfel de elemente $c_0, c_1, \dots, c_n$ nu toate egale 0, încât $c_0 \cdot 1 + c_1 \cdot \alpha + c_1 \cdot \alpha^2 + \cdots + c_n \cdot \alpha^n = 0$. În concluzie, elementul α este element algebric peste F. *Teorema este demonstrată.*

Corolar 3.2. Orice extindere de tipul 1^0 este extindere de tipul 5^0.

Teorema 3.3. Orice extindere finită E a câmpului F este extindere algebric generată.

Demonstrație. Fie $\alpha_1, \alpha_2, \dots, \alpha_n$ o careva bază a câmpului E. După teorema 3.1 elementele $\alpha_1, \alpha_2, \dots, \alpha_n$ sînt elemente algebrice. Atunci extinderea $F(\alpha_1, \alpha_2, \dots, \alpha_n)$ este algebric generată. Cum $F(\alpha_1, \alpha_2, \dots, \alpha_n)$ este extindere minimal, $F(\alpha_1, \alpha_2, \dots, \alpha_n) \subset E$.

Pe de altă parte, $\alpha_1, \alpha_2, \dots, \alpha_n \in \mathrm{F}(\alpha_1, \alpha_2, \dots, \alpha_n)$, de unde rezultă că $\mathrm{a}_1 \cdot \alpha_1 + \mathrm{a}_2 \cdot \alpha_2 + \cdots + \mathrm{a}_n \cdot \alpha_n \in F(\alpha_1, \alpha_2, \dots, \alpha_n), \mathrm{a}_1, \mathrm{a}_2, \dots, \mathrm{a}_n \in F$. Astfel orice element a câmpului E aparține câmpului $F(\alpha_1, \alpha_2, \dots, \alpha_n)$, deci $E \subset F(\alpha_1, \alpha_2, \dots, \alpha_n)$, așa dar $E = F(\alpha_1, \alpha_2, \dots, \alpha_n)$. *Teorema este demonstrată.*

Corolar 3.4. Orice extindere de tipul 1^0 este extindere de tipul 2.

Teorema 3.5. Dacă e este extindere finită a câmpului L, iar L este extindere finită a câmpului F, atunci E este extindere finită a câmpului F și se verifică relația $[E:F] = [E:L] = [L:F]$.

Demonstrație. Considerăm baza

$$a_1, a_2, \dots, a_n \qquad (1)$$

a câmpului L peste F și

$$b_1, b_2, \dots, b_n \qquad (2)$$

baza câmpului E peste L. Orice element d din E se reprezintă sub forma

$$d = l_1 \cdot b_1 + l_2 \cdot b_2 + \cdots + l_n \cdot b_n \qquad (l_k \in L) \qquad (3)$$

Coeficienții l_k se reprezintă la rândul său prin elementele bazei (1)

$$l_k = P_{1k} \cdot a_1 + P_{2k} \cdot a_2 + \cdots + P_{mk} \cdot a_m \qquad (P_{1k} \in F) \qquad (4)$$

Substituind (4) în (3) obținem

$$d = \sum_{\substack{i \in \{1,\dots m\} \\ k \in \{1,\dots n\}}} P_{ik} a_i b_k$$

Orice element din E se reprezintă ca combinație liniară a elementelor mulțimii $B = (a_1 \cdot b_k, 1 \in \{1, \dots . m\}, k \in \{1, \dots . n\}$ iar B conține $m \cdot n$ elemente.

Afirmăm, cămulțimea B servește ca bază a câmpului E peste F.

Fie

$$\sum_{i,k} C_{i,k} Q_i b_k \qquad (5)$$

unde, $C_{i,k} \in F$. Cum sistemul (2) este linear independent peste L din (5) rezultă relația

$$c_{1k} \cdot a_{1k} + c_{1k} \cdot a_2 + \cdots + c_{mk} \cdot a_m = 0 (k = 1, \dots n) \qquad (6)$$

Deoarece elementele $a_1 \cdot a_2, \dots . a_m$ sînt liniar independente din (6) rezultă

$$c_{1k} = c_{2k} = \cdots = c_{mk} = 0 \ (k = 1, \dots n)$$

Astfel elementele mulțimii B sînt liniar independente și deci servesc ca bază. Așa dar, $[E: F] = [E: L] \cdot [L: F]$. *Teorema este demonstrată.*

Corolar 3.6. Dacă F=$L_0 \subset L_1 \subset \cdots . \subset L_{1-1} \subset L_1 \subset \cdots \subset L_n = B$ astfel încât pentru orice $i = 1, \dots, n$ câmpul L_1 este extindere finită a câmpului L_{1-1}, atunci câmpul E este extindere finită a câmpului F și are loc relația.

$$(E:F) = [E:L_{n-1}] \dots [L_1:L_{1-1}] \dots [L_1:F]$$

Teorema 3.7. Fie $E = F(\alpha_1)(\alpha_2) \dots . (\alpha_S)$ – extindere algebrică compusă. Pentru orice element β a câmpului E există un astfel de polinom $g(x_{1,\dots,}x_s) \in F(x_{1,\dots,}x_s)$, încât $\beta = g(\alpha_1 \dots . \alpha_S)$

Demonstrație. Aplicăm metoda inducției matematice dupa n.

1) $n = 1$. Atunci $E = F(\alpha)$ și teorema rezultă din teorema 1.8.
2) Presupunem că teorema este demonstrată pentru cîmpul $L = F(\alpha) \dots . (\alpha_{s-1})$.

Studiem elementul $\beta \in E$. Cum $E = L(\alpha_S)$, rezultă că există un astfel de polinom $b(x)$, încât $\beta = h(\alpha_S)$.

Fie $h(x) = \gamma_0 + \gamma_1 \cdot x + \cdots + \gamma_n \cdot x^n$, unde $\gamma_0, \dots, \gamma_n \in L$. După presupunere pentru orce $i = 0, \dots, n$ există un astfel de polinom $h(x_1, \dots, x_{s-1})$ încât $\gamma_1 = b_1(\alpha_1, \dots, \alpha_{s-1})$. Atunci substituind în precedenta obținem:

$g(x_1, \dots, x_s = h_0(x_1, \dots, x_{s-1}) + h_1(x_1, \dots, x_{s-1}) \cdot x_s + \cdots + h_n(x_1, \dots, x_{s-1}) \cdot x_s^n$, de rezultă că $\beta = g(\alpha_1, \dots, \alpha_s)$. *Teorema este demonstrată.*

Corolar 3.8. Orice extindere de tipul 4^0 este extindere de tipul 1^0.

Teorema 3.9. Orice extindere algebric generată E a câmpului F este extindere algebrică compusă.

Demonstrație. Fie $E = F(\alpha_1, \dots, \alpha_n)$, unde $\alpha_1, \dots, \alpha_n$ sînt elemente algebrice din E. Definim prin inducție cîmpurile $L_0 = F, L_1 = L_0(\alpha_1), \dots, L_n = L_{n-1}(\alpha_n)$. Cum pentru orice $i = 1, \dots, n$ elementul α_1 este algebric peste F α_1 va fi algebric și peste extindere L_{i-1}. Atunci L_1 este extindere algebrică simplă a cîmpului L_{i-1}. Așadar L_n este extindere algebrică compusă. După teorema 3.7. orice element $\beta \in L_n$ se exprimă sub forma $\beta = g(\alpha_1, \dots, \alpha_n)$ pentru un careva polinom $g(\alpha_1, \dots, \alpha_n) \in F[x_1, \dots, x_n]$. Astfel $L_n \in F(\alpha_1, \dots, \alpha_n)$. Deoarece

$\alpha_1, \dots, \alpha_n \in L_n$ rezultă că $F(\alpha_1, \dots, \alpha_n) \subset L_n$. În final $F(\alpha_1, \dots, \alpha_n) = F(\alpha_1), \dots, (\alpha_n)$. *Teorema este demonstrată.*

Corolar 3.10. Orice extindere de tipul 2^0 este extindere de tipul 3^0.

Corolar 3.11. Orice extindere de tipul 3^0 este extindere de tipul 2^0.

Corolar 3.12. Orice extindere de tipul 1^0 este extindere de tipul 3^0.

Corolar 3.13. Orice extindere de tipul 3^0 este extindere de tipul 1^0.

Din cele expuse mai sus rezultă:

Teorema 3.14. Următoarele afirmații sînt echivalente:

a) Câmpul E este extindere finită a câmpului F;
b) Câmpul E este extindere algebrică compusă a câmpului F;
c) Câmpul E este extindere algebrică generată a câmpului F;

Teorema 3.15. Extinderea algebrică simplă $E = F(\alpha)$ a câmpului F este extindere finită.

Demonstrație. Rezultă din teorema 3.14. *Teorema este demonstrată.*

Teorema 3.16. Dacă $\alpha_1, \dots, \alpha_n$ sunt elemente algebrice peste câmpul infinit F, atunci extinderea algebrică finită $F(\alpha_1, \dots, \alpha_n)$ este extindere algebrică simplă, adică există un astfel de element algebric θ, încât

$$F(\alpha_1, \dots, \alpha_n) = F(\theta)$$

Demonstrație. Aplicăm metoda inducției matematice după h.

Să arătăm mai întâi că teorema este adevărată pentru 2 elemente algebrice peste F notate cu α și β. Fie $f(x)$ și $g(x)$ polinoameleminimale pentru α și β respectiv. Fie $\alpha_1 = \alpha, \beta_1 = \beta$. Pentru $k = 1$ avem inegalitatea $\beta_1 = \beta_k$. Ecuația $\alpha_1 + x \cdot \beta_k = \alpha_I + x \cdot \beta_1$ pentru fiecare i și fiecare $k = 1$ are cel mult o rădăcină x în F. Considerăm elementul c diferit de rădăcinele acelor ecuații liniare; atunci pentru toți i și $k = 1$ se verifică $\alpha_1 + x \cdot \beta_k = \alpha_I + x \cdot \beta_1$. Notăm $\theta = \alpha_1 + c \cdot \beta_1 = \alpha + c \cdot \beta_1$. Atunci elementul θ aparține cîmpului $F(\alpha, \beta)$.

Afirmăm, că $F(\alpha_1, \dots, \alpha_n) = F(\theta)$. Într-adevăr, elementul β verifică ecuațiile $g(x) = 0, f(\theta - c \cdot x) = 0$ cu coeficienții din cîmpul $F(\theta)$. Polinoamele $g(x) = 0$ și $f(\theta - c \cdot x) = 0$ au unica rădăcină comună β, pentru că ceilalți β_k $(k = 1)$ verifică relația $\theta - c \cdot \beta_k = \alpha_1 \quad (i = 1, \dots, n)$, deci $f(\theta - c \cdot \beta_k) \neq 0$.

Elementul β este rădăcina simplă a polinomului $g(x)$, deci $x - \beta$ este cel mai mare divizor comun a polinoamelor $g(x)$ și $f(\theta - c \cdot x)$. Astfel conchidem că $\beta = F(\theta)$. Din relația $\theta - c \cdot \beta = \alpha$ rezultă că $\alpha \in F(\theta)$. În concluzie, $F(\alpha, \beta) = = F(\theta)$

Presupunem acum, că teorema este demonstrată pentru $h - 1$ elemente, adică $F(\alpha_1, \dots, \alpha_{h-1}) = F(\lambda)$.

Atunci $F(\alpha_1, \dots, \alpha_{h-1}) = F(\alpha_1, \dots, \alpha_{h-1}, \alpha_h) = F(\lambda)(\alpha_h) = F(\lambda, \alpha_h) = F(\theta)$. *Teorema este demonstrată.*

Corolar. 3.17. Orice extindere de tipul 3^0 este extindere de tipul 4^0.

În final are loc următoarea teoremă:

Teorema. 3.18. Următoarele afirmații sînt echivalente;

a) Câmpul E este extindere finită a câmpului F;
b) Câmpul E este extindere algebrică generală a câmpului F;
c) Câmpul E este extindere algebrică compusă a câmpului F;
d) Câmpul E este extindere algebrică simplă a câmpului F.

1.4. Existența extinderii algebrice simple

În această secțiune vom demonstra următoarea teoremă:

Teorema 4.1. Fie F un câmp arbitrar, iar $f(x) = x^n + a_{n-1} \cdot x^{n-1} + \cdots + a_1 \cdot x + a_0$ un polinom normat ireductibil peste F. Atunci există o extindere E a câmpului F ce conține un element pentru care $f(x)$ este polinom minimal.

Demonstrație. Considerăm inelul de polinoame $R = F[x]$ peste F și idealul $I = Rf(x)$.

Afirmăm că inelul factor R/I este câmp. Într-adevăr, fie $g(x)+I \in R/I$, unde $g(x) \in R$.

Cum $g(x)+I=0$, avem că $f(x)$ nu divide $g(x)$. Din faptul că $f(x)$ este ireductibil, rezultă ca $f(x)$ si $g(x)$ sînt prime între ele.

Există două polinoame $h(x), q(x)$, încât $f(x)\ h(x)+g(x)q(x)=1$. Atunci $(g(x)+I)(q(x)+I)=g(x)q(x)+I=g(x)q(x)+f(x)h(x)+I=1+I$, adică elementul $g(x)=I$ este inversabil.

Afirmăm că câmpul F se scufundă izomorf în câmpul R/I. Definim $\varphi: F-R/I$ în modul următor: pentru orce $a \in F$ considerăm $\varphi(x)=a+I$. Dacă $a,b \in F$, atunci $\varphi(a+b)=a+b+I=a+I+b+I=\varphi(a)+\varphi(b), \varphi(ab)=ab+I=(a+I)(b+I)=\varphi(a)\varphi(b)$. Fie $\varphi(a)=0, a \in F$. Atunci $a+I=I$ ori $a \in I \cap F=0$, adică $a=0$

Rezultă că putem identifica câmpul F cu mulțimea $\{a+I: a \in F\}$

E nevoie să demonstrăm că elementul $e=x+I$ este radăcină a polinomului $g(Y)=(a_0+I)+(a_1+I)Y+(a_2+I)Y^2+\cdots+(1+I)Y^n$. Dacă $Y=0$, atunci $(\ a_0+I)+(a_1+I)(x+I)+\ldots.+(1+I)(x+I)^n=a_0+I+a_1x+I+\cdots+x^n+I=f(x)+I=I$. Cum $g(Y)$ este polinom ireductibil al inelului $(R/I)[Y]$ din corolarul 1.6 rezultă că $g(Y)$ este polinom minimal pentru elementul $\theta=x+I$. *Teorema este demonstrată.*

Corolarul 4.2 Pentru orice polinom normat ireductibil $f(x)$ peste câmpul F există o extindere $E \supset F$ în care $f(x)$ are cel puțin o rădăcină.

Definiția 4.3. Ecuația $f(x)=0$ cu rădăcina θ se numește ecuația ce determină câmpul E.

Definiția 4.4. Elementul θ se numește element primitiv a câmpului E peste F.

1.5. Câmpul numerelor algebrice

În secțiunule anterioare am demonstrat ca tipurile de extinderi $1^0, 2^0, 3^0, 4^0$ coincid. Din teorema 3.19 și teorema 3.1 rezultă că extinderile date sînt extinderi algebrice. Să observăm însă că afirmația reciprocă în caz general nu are loc. Ca

exemplu de extindere algebrică infinită ne servește câmpul numerelor algebrice. În continuare studiem unele proprietăți a câmpului numerelor algebrice.

Să reamintim, că numărul complex $\alpha \in C$ ce este rădăcină pentru un careva polinom $f(x)$ cu coeficienți numere raționale Q, $f(\alpha) = 0$, se numește număr algebric.

Definiția 5.1. Submulțimea $V \subset C$ a numerelor complexe se numește Q-modul dacă:

a) Pentru orice $V_1, V_2 \in V, V_1 + V_2 \in V$;

b) Pentru orice $v \in V$ $și$ $r \in Q, r \cdot v \in V$;

c) Există astfel de elemente $v_1, \dots, v_n \in V$ încît orce element $v \in V$ se exprimă sub forma

$$\sum_{i=1}^{n} r_1 v_1 \ , r_1 \in Q$$

Să observăm, că mulțimea expresiilor de forma $\sum_{i=1}^{n} r_1 \lambda_1$ unde $\lambda_1 \dots \dots \lambda_n \epsilon C, r_1 \dots . . r_n \in Q$ Formează Q-modul (demonstrați).

Notăm mulțimea expresiilor de forma $\sum_{i=1}^{n} r_1 \lambda_1$ cu $\{v_1, \dots, v_n\}$

Propoziția 5.2. Fie V=$\{v_1 \dots \dots v_n\}$ și $\alpha \in C$ cu proprietatea $\alpha v \in V$ pentru orice $v \in V$. Atunci α este număr algebric .

Demonstrație. Avem că $\alpha v_1 \in V, i = 1, \dots . n$. Atunci $\alpha v_i = \sum_{j=1}^{n} a_{ij} v_j \ , a_{ij} \in Q$. De aici rezultă că $0 = \sum_{j=1}^{n} (a_{ij} - b_{ij} \alpha) vj$, unde $b_{1j} = 0$ pentru $i \neq j$ și $b_{1j} = 1$ pentru $1 = j$ .Cum $\det(a_{ij} - b_{ij} \alpha) = 0$ conchidem că α este număr algebric. *Propoziția este demonstrată.*

Teorema 5.3. Mulțimea numerelor algebrice A este câmp .

Demonstrație .Fie α_1 și $\alpha_2 \in A$. Să arătăm că $\alpha_1 + \alpha_2$ $și$ $\alpha_1 \cdot \alpha_2$ sînt numere algebrice.

Există 2 polinoame de grad n și m încît ${a_1}^n + r_1 {a_1}^{n-1} + \dots + r_n = 0$ și $a_2^m + s_1 {a_2}^{m-1} + \dots + s_m = 0, r_1, s_1 \in Q$. Notăm cu V, Q - modulul format din

mulțimea tuturor combinațiilor liniare a elementelor de forma $\alpha_1^i, \alpha_2^j, 0 \leq 1 < n$ și $0 \leq j < m$.

Fie $v \in V$. Atunci $\alpha_1 \mathrm{v} \in V$ $și$ $\alpha_2 \mathrm{v} \in V$, de unde rezultă că $(\alpha_1 + \alpha_2)\, v \in V$ și $(\alpha_1\, \alpha_2)v \in V$. După propoziția 5.2 numerele $\alpha_1 + \alpha_2$ $și$ $\alpha_1 \cdot \alpha_2$ sunt numere algebrice.

Fie $0 \in a$ -număr algebric. Atunci $a_0\alpha^n + a_1\, \alpha^{n-1} + \cdots + a_n = 0$, unde $a_i \in Q$. Cum $a \neq 0$ rezultă $\alpha^n \neq 0$. Divizăm la a^n și obținem

$a_n\, (a^{-1})^n a_{n-1}(a^{-1})^{n-1} + \cdots + a_0 = 0$. *Teorema este demonstrată.*

Este cunoscut faptul că câmpul numerelor complexe este algebric închis. Afirmația analoagă are loc și pentru câmpul numerelor algebrice A.

Teorema 5.4. Câmpul numerelor algebrice A este algebric închis.

Demonstrație. Fie $A[X]$ - inelul de polinoame peste câmpul numerelor algebrice A și

$$f(x) = a_0 + a_1\, x + \cdots + a_n\, x^n.$$

unde $a_0 \ldots . a_n \in A$, un polinom de grad pozitiv din $A[X]$.

Afirmăm că f(x) are rădăcina în A .Cum f(x) ∈ C[X] și c este algebric închis, $f(x)$ are cel puțin o rădăcină în c. Există un astfel de număr complex $c, f(c) = 0$. Fie $L = Q(a_0, \ldots, a_n)$, iar $L(c)$ extindere a câmpului $L, Q \subset I \subset L(c)$. Cum L este extindere finită a lui $Q, L(c)$ este extindere finită lui Q. După teorema 3.1 $L(c)$ este extindere algebrică a cîmpului Q,deci $c \in Q$. *Teorema este demonstrată.*

1.6. Probleme soluționate

6.1. Găsiți polinomul minimal pentu elementele.

a) $\sqrt{5}$ peste Q;
b) $2 - i$ peste R;
c) $1 + c$ peste C;
d) $\sqrt{2} + \sqrt{5}$ peste Q;

e) $1+\sqrt{3}$ peste $Q(\sqrt{2}+\sqrt{5})$;

Soluție:

a) Fie $z=\sqrt{5}$. Ridicăm la pătrat ambele părți $z^2=5$. Atunci polinomul minimal peste Q este $f(z)=z^2-5$;

b) Fie $t=2-1$. Atunci $t-2=1$. Ridicăm la pătrat ambele părți și obținem $t^2-4t+4=-1$. Polinomul minimal peste R este $h(t)=t^2-4t+5$;

c) Fie $x=1+1$. Atunci polinomul minimal peste C este $p(x)=x-1-1$.

d) Fie $y=\sqrt{2}+\sqrt{5}$. Atunci $y-\sqrt{2}=\sqrt{5}$. Ridicăm la pătrat și primim $i^2-2\sqrt{2}y+2=5$ sau $y^2-3=2\sqrt{2}y$. Ridicăm la pătrat ambele părți $(y^2-3)^2=\left(2\sqrt{2}y\right)^2$ și obținem $y^4-6y^2+9=8y^2$. Atunci polinomul minimal este Q este $\varphi(y)=y^4-14y^2+9$.

e) Polinomul minimal peste $Q(\sqrt{2}+\sqrt{3})$ este $f(u)=u-1-\sqrt{3}$.

6.2. Descrieți extinderile finite a câmpului numerelor raționale Q:

a) $Q(\sqrt{3})$;

b) $Q(\sqrt{2},\sqrt[3]{2})$;

c) $Q(\sqrt{3},\sqrt{5})$;

d) $Q(i,\sqrt[3]{5})$.

Soluție:

a) Polinomul minimal al numărului $\sqrt{3}$ peste Q este $f(x)=x^2-3$. Atunci cîmpul $E=Q(\sqrt{3})$ ca spațiu vectorial peste Q are dimensiune 2, $E=<1,\sqrt{3}>Q$. Orice element al cîmpului E se reprezintă sub forma $\alpha=a+b\sqrt{3},a,b\in Q$.

b) Observăm că elementul primitiv al extinderii $L=Q(\sqrt{2},\sqrt[3]{2})$ este $\Theta=\sqrt{2}+\sqrt[3]{2}$. Determinăm polinomul minimal al elementului $\Theta=\sqrt{2}+\sqrt[3]{2}$. Fie $x=\sqrt{2}+\sqrt[3]{2}$, de unde $x-\sqrt{2}=\sqrt[3]{2}$. Ridicăm la cub și obținem $x^3+6x-2=(2+3x^2)\sqrt{2}$. Ridicăm la pătrat ambele părți $x^6+12x^4-4x^3+36x^2+24x+4=8+24x^2+18x^4$. Atunci polinomul minimal este $f(x)=x^6-x^4-4x^3+12x^2+24x-4$. Dimensiunea spațiului vectorial $L=Q(\sqrt{2},\sqrt[3]{2})$ este 6, $L=<1,\theta,\theta^2,\theta^3,\theta^4,\theta^5>Q$. Orice elementt al câmpului L se exprimă sub forma

$$a_0 + a_1\theta + a_2\theta^2 + a_3\theta^3 + a_4\theta^4 + a_5\theta^5, a_1, a_2, a_3, a_4, a_5 \in Q$$

c) Elementul primitiv al câmpului $K = Q(\sqrt{3}, \sqrt{5})$ este $\alpha = \sqrt{3} + \sqrt{5}$. Determinăm polinomul minimal. Fie $x = \sqrt{3} + \sqrt{5}$. Atunci $x - \sqrt{3} = \sqrt{5}$. Ridicăm la pătrat ambele părți $x^2 - 2 = 2\sqrt{3}x$. Ridicăm la pătrat ambele părți $x^4 + 4x^2 + 4 = 12x^2$. Atunci polinomul minimal este $f(x) = x^4 - 16x^2 + 4$. Câmpul K ca spațiu vectorial peste Q și are dimensiunea 4. $K =< 1, \alpha, \alpha_2, \alpha_3 > Q$, deci orice element $y \in K$ se scrie sub forma $y = b_0 \cdot 1 + b_1 \cdot \alpha + b_2\alpha^2 + b_3\alpha^3, b_0, b_1, b_2, b_3 \in Q$. Găsim α^2, α^3. Avem că $\alpha^2 = \alpha \cdot \alpha = \left(\sqrt{3} + \sqrt{5}\right)^2 = 8 + 2\sqrt{15}, \alpha^3 = \alpha \cdot \alpha^2 = 18\sqrt{3} + 14\sqrt{5}$. Atunci $\sqrt{3} = \frac{1}{4}\alpha^3 - \frac{7}{2}\alpha, \sqrt{5} = \frac{9}{2}\alpha - \frac{1}{4}\alpha^3, \sqrt{15} = \frac{1}{2}\alpha^2 - 4$.

d) Elementul primitiv al extinderii $S = Q(i, \sqrt[3]{2})$ este $w = i + \sqrt[3]{2}$. Determinăm polinomul minimal. Fie $x = i + \sqrt[3]{2}$. Atunci $x - i = \sqrt[3]{2}$. Ca și mai sus obținem că polinomul minimal este $\varphi(x) = x^6 + 3x^4 - 4x^3 + 3x^2 + 12x + 5$. Câmpul S ca spațiu vectoral peste Q are dimensiuunea 6, $S =< 1, w, w_2, w_3, w_4, w_5 > Q$. Orice element din S se scrie sub forma $s \in S, s = c_0 \cdot 1 + c \cdot w + c_2 \cdot w^2 + c_3 \cdot w^3 + c_4 \cdot w^4 + c_5 \cdot w^5, c_0, c_1, c_2, c_3, c_4, c_5 \in Q$.

6.3. Demonstrați că câmpurile $Q(\sqrt{3})$ și $Q(\sqrt{5})$ nu sînt isomorfe.

Soluție: Pornim de la absurd, adică există un isomorfism: $\psi: Q(\sqrt{3}) \to Q(\sqrt{5})$. Atunci $\psi(1) = 1$ și $\psi(3) = 3$. Fie $\psi(\sqrt{3}) = a + b(\sqrt{5}), a, b \in Q$. Cum $3 = \psi\left(\sqrt{3}\right) = a^2 + 2ab\sqrt{5} + 5b^2$, rezultă $ab = 0$. Dacă $a = 0$, obținem $3 = 5b^2$ - contradicție. Dacă $b = 0$, obținem $3 = a^2$- contradicție.

6.4. Demonstrați că $R(i) \cong C$.

Soluție. Studiem extinderea simplă $R(i)$. Determinăm polinomul minimal pentru elementul i. După teorema 1.2 polinomul $f(x)$ este ireductibil.

Notăm cu $S = R[x]$, iar cu $I = f(x)R[x]$. Inelul factor S/I după teorema *4.1* este câmp. După teorema *4.1* avem $R(i) \cong S/I$.

Definim aplicația $\varphi: S/I \to C$ după regula $\varphi(a + bx + I) = a + bi, a, b \in R$. Afirmăm că φ este isomorfism. Într-adevăr. $\Phi(a + bx + I + c + dx + I) = \varphi(a + bx + I) + \varphi(c + dx + I), \varphi((a + bx + I) \cdot (c + dx + I)) = \varphi(a + bx +$

$I) \cdot \varphi(c + dx + I)$. Determinăm $Ker\,\varphi$. Fie $a + bx + I \in Ker\,\varphi$. Atunci $a = 0, b = 0$. Deci φ este aplicație injectivă. Este evident, că φ este surjectivă. După teorema despre omomorfizme de inele $S/I \cong C \cong R(i)$.

6.5. Demonstrați, că orice extindere pătratică a câmpulu numerelor reale R ce nu coincide cu R, este izomorfă câmpului numerelor complexe C.

Soluție. Fie S extinderea algebrică pătratică a cîmpului numerelor reale R, iar $\alpha \in S - R$. Cum α este element algebric există un polinom ireductibil peste R, $f(x) = x^2 + px + q$, încât $f(\alpha) = \alpha^2 + p\alpha + q = 0$, iar $\frac{p^2}{4} - q = -b^2 < 0, b \in R$. Notăm $j = \frac{\alpha}{b} + \frac{p}{2b}$. Atunci $j^2 = -1$. Este evident că $\alpha \in R(j)$. Câmpurile $R(i)$ și $R(j)$ sînt izomorfe câmpului C.

Afirmăm, că $S = R(j)$. Presupunem prin absurd, adică $S \neq R(j)$. Considerăm $\beta \in S - R(j)$. Raționând ca și mai sus se poate demonstra existența unui astfel de element $s \in S$, încât $s^2 = -1$. Atunci $\beta \in R(s)$. Cum $\beta \in R(j)$, rezultă $s \neq j, s - j \neq 0, s + j \neq 0$, dar $(s - j)(s + j) = 0$- contradicție.

6.6. Eliberați de iraționalitate la numitor fracția:

a) $\frac{3+\sqrt[3]{2}}{\sqrt[3]{4}+2\sqrt[3]{2}-1}$;

b) $\frac{1}{\alpha^2+2\alpha-1}$,unde α este rădăcina polinomului $p(x) = x^2 + 3x + 1$;

c) $\frac{z^2+1}{z^2-1}$, unde $z^3 - 2z + 2 = 0$;

d) $\frac{1}{\sqrt{2}+\sqrt{3}+1}$.

Soluție:

a) Să observăm că numărul $\sqrt[3]{2}$ este rădăcina polinomului $p(x) = x^3 - 2$, iar numitorul fracției este valoarea polinomului $p(x) = x^2 + 3x + 1$ pentru $x = \sqrt[3]{2}$. Polinoamele $f(x)$ și $g(x)$ sunt prime între ele, $(f(x), g(x)) = 1$. Există polinoamele $M(x)$ și $N(x)$ încât $f(x)\ M(x) + p(x), N(x) = 1$. Polinoamele $M(x)$ și $N(x)$ se determină pln aplicarea algoritmului Euclid. Rezultatele impărțirii se scriu astfel $p(x) = f(x)q_1(x) + r_1(x), f(x) = r_1(x)q_2(x) + r_2(x)$, unde $q_1(x) = x - 2, q_2(x) = \frac{1}{5}x + \frac{14}{25}, r_1(x) = 5x - 4, r_2(x) = \frac{31}{25}$. Din aceste relații exprimăm $r_2(x)$ prin $p(x)$ și $f(x)$. Cum $r_2(x) =$

$f(x)-r_1q_2(x)$ și $r_1(x)=p(x)-f(x)q_1(x)$ atunci $r_2(x)=f(x)-[p(x)-f(x)q_1(x)]q_2(x)=f(x)[1+q_1(x)q_2(x)]+p(x)[-q_2(x)]=\frac{31}{25}$. Substituim x cu $\sqrt[3]{2}$ și ținând seama că $p\left(\sqrt[3]{2}\right)=0$, obținem $f\left(\sqrt[3]{2}\right)\left[1+q_1\left(\sqrt[3]{2}\right)\cdot q_2\left(\sqrt[3]{2}\right)\right]=\frac{31}{25}$. Astfel, dacă înmulțim numitorul fracției cu $1+q_1\left(\sqrt[3]{2}\right)\cdot q_2\left(\sqrt[3]{2}\right)$ obținem $\frac{31}{25}$. Înmulțim numitorul și numărătorul fracției cu numărul $\frac{1}{25}\left(5\sqrt[3]{4}+4\sqrt[3]{2}-3\right)$. În final obținem

$$t=\frac{1}{25}\left(19\sqrt[3]{4}+9\sqrt[3]{2}+1\right).$$

b) Polinomul $P(x)=x^3+3x+1$ este ireductibil peste Q. Numitorul fracției t este valoarea polinomului $f(x)=x^2+2x-1$ pentru $x=\alpha$. Cum $p(x)$ este ireductibil, polinoamele $p(x)$ și $f(x)$sunt prime între ele. Există polinoamele $M(x)$ și $N(x)$ încît, $f(x)M(x)+p(x)N(x)=1$. Avem că $p(x)=f(x)q_1(x)+r_1(x), f(x)=r_1(x)q_2(x)+r_2(x), q_1(x)=x-2, r_1(x)=8x-1, q_2(x)=\frac{1}{8}x+\frac{17}{64,}, r_2(x)=-\frac{47}{64}$.

Din ultimile relații, găsim că $f(x)[1+q_1(x)q_2(x)]+p(x)[-q_2(x)]=-\frac{47}{64}$. Substituim x prin α și cum $p(\alpha)=0$ obținem $f(\alpha)[1+q_1(\alpha)q_2(\alpha)]=-\frac{47}{64}$. Trebuie să înmulțim numărătorul și numitorul fracției cu numărătorul $1+q_1(\alpha)q_2(\alpha)=1+(\alpha-2)\left(\frac{1}{18}\alpha+\frac{17}{64}\right)=\frac{1}{8}\alpha^2+\frac{1}{64}\alpha+\frac{15}{32}$.

În final obținem

$$t=-\frac{1}{47}(8\alpha^2+\alpha+30)$$

c) Polinomul $\varphi(x)=x^3-2x+2$ este ireductibil peste Q. Polinoamele $f(x)=x^2-1$ și $\varphi(x)$ sunt primele între ele. Calculînd ca și în problemele precedente, găsim că $q_1(x)=x, q_2(x)=-x-2$.

Dacă $x=z$ obținem $f(z)(1+q_1(z)q_2(z))=3$. Trebuie să înmulțim numărătorul șinumitorul fracției cu $1+q_1(z)q_2(z)=-z^2-2z+1$. Avem că $-2z^3+4z-4=0$ și $-z^4+2z^2-2z=0$ deci $-z^4-2z^3-2z+1=-2z^2-4z+5$.

În final obținem

$$\frac{z^2+1}{z^2-1}=\frac{1}{3}(-2z^2-4z+5)$$

d) Considerăm numărul algebric $\theta=\sqrt{2}+\sqrt{3}$. Polinomul minimal pentru θ este $f(x)=x^4-10x^2+1$. Calculând ca și în problemele precedente găsim că $(x^4-10x^2+1)+(x+1)(-x^3+x^2+9x-9)=-8$.

Punem $x=\theta$ și obținem $(\theta+1)(-\theta^3+\theta^2+9\theta-9)=-8$. Rezultă că trebue să înmulțim numărătorul și numitorul fracției cu $-\theta^3+\theta^2+9\theta-9$ unde $\theta^3=11\sqrt{2}+9\sqrt{3}\ \theta^2=2\sqrt{6}+5$. În final obținem

$$\frac{1}{\sqrt{2}+\sqrt{3}+1}=\frac{1}{4}\sqrt{2}-\frac{1}{4}\sqrt{6}+\frac{1}{2}.$$

§2. Câmpuri finite

2.1.Proprietăți elementare a câmpurilor finite

Fie $GF(q)$ un câmp finit din q elemente. Grupul multiplicativ $GF(q)$ constă din $q-1$ elemente. Atunci orice element $\alpha \in GF(q)$ verifică ecuția $x^{q-1}=1$.

Propoziția 1.

$$x^q - x = \prod_{\alpha \in GF(q)} (x-\alpha)$$

Demonstrație. Orice element a câmpului $GF(q)$ ese rădăcină pentru polinomul $x^q - x$. Cum câmpul $GF(q)$ are q elemente, iar gradul polinomului $x^q - x$ este q, rezultă descompunerea cerută. *Propoziția este demonstrată.*

Corolar 2. Fie $GF(q) \subset P$ un careva cîmp. Elementul $\alpha \in P$ aparține cîmpului $GF(q)$ dacă și numai dacă $\alpha^q = \alpha$.

Demonstrație. Relația $\alpha^q = \alpha$ se verifică dacă și numai dacă α este rădăcină pentru polinom $x^q = x$. După propoziția 1 rădăcinile polinomului $x^q = x$ sînt elemente cîmpului $GF(q)$. *Corolarul este demonstrat.*

Corolar 3. Dacă polinomul $f(x)$ divide $x^q = x$ și gradul lui $f(x)$ este d atunci $f(x)$ are d rădăcini diferite.

Demonstrație. Fie $f(x)g(x) = x^q - x$. Polinomul $g(x)$ are gradul egal $q-d$. Dacă $f(x)$ are mai puțin de d rădăcini diferite, atunci polinomul $f(x)g(x)$ ar avea mai puțin de $d + (q-d)$ rădăcini diferite. *Corolarul este demonstrat.*

Lema 4. Fie $GF(q)$ n cîmp finit. Multipli întregi a elementului unitate formează subcîmp ce este izomorf cu $\mathbb{Z}/p\mathbb{Z}$ pentru un careva număr simplu P.

*Demonstrație***.** Pentru a evita unele confundări notăm temporar unitatea cîmpului $GF(q)$ cu e. Studiem aplicația $\varphi: \mathbb{Z} \longrightarrow GF(q)$, $\varphi(n) = ne, n \in \mathbb{Z}$. Este evident că φ este omomorfizm de inel. Imaginea $\varphi(\mathbb{Z})$ este un subinel finit fără divizori a lui 0. Nucleul acestui omomorfism este $ker\varphi = p\mathbb{Z}$ pentru careva număr

simplu p. După teorema despre omomorfisme de inel $\varphi(\mathbb{Z}) \cong \mathbb{Z}/p\mathbb{Z}$. *Lema este demonstrată*

Propoziția 5. Numărul elementelor unui câmp fnit $GF(q)$ este puterea căruiva număr prim $p, q = p^n$.

*Demonstrație***.** Identificăm $\mathbb{Z}/p\mathbb{Z}$ cu imaginea sa în cîmpul $GF(q)$. Cîmpul $GF(q)$ este spațiu vectorial finit dimensional peste $\mathbb{Z}/p\mathbb{Z}$ de dimensiunea n. Baza spațiului $GF(q)$ peste $\mathbb{Z}/p\mathbb{Z}$ este format din elementele $V_1, V_2, \dots, V_n$. Atunci orice element $x \in GF(q)$ se scriu sub forma $x = a_1V_1 + a_2V_2 + \dots + a_nV_n, a_i \in \mathbb{Z}/p\mathbb{Z}$. De aici conchidem, că $q = p^n$. *Propoziția este demonstrată.*

Propoziția 6. Pentru orice elemene $\alpha, \beta \in GF(p^n)$ și orice număr întreg pozitiv d se verifică relația

$$(\alpha + \beta)^{p^d} = \alpha^{p^d} + \beta^{p^d}$$

Demonstrație. Aplicăm inducția după α. Dacă $d = 1$ atunci $(\alpha + \beta)^p = \alpha^p + \sum_{k=1}^{p-1} \binom{p}{k} \alpha^{p-k}\beta^k + \beta^p$. Cum $p | \binom{p}{k}$ rezultă că $\sum_{k=1}^{p-1} \binom{p}{k} \alpha^{p-k}\beta^k = 0$, deci $(\alpha + \beta)^p = \alpha^p + \beta^p$. Presupnem că $(\alpha + \beta)^{p^d} = \alpha^{p^d} + \beta^{p^d}$ substituim d cu $d + 1$ și obținem $(\alpha + \beta)^{p^{d+1}} = \left((\alpha + \beta)^{p^d}\right)^p = \left(\alpha^{p^d}\right)^p + \left(\beta^{p^d}\right)^p = \alpha^{p^{d+1}} + \beta^{p^{d+1}}$. *Propoziția este demonstrată.*

Lema 7. Fie $GF(p^n)$ un careva câmp. Poinomul $x^e - 1$ divide polinomul $x^m - 1$ în $GF(p^n)[x]$ dacă și numai dacă l divide m.

*Demonstrație***.** Fie $m = q^l + r_1, 0 \le r < l$. Atunci

$$\frac{x^m + 1}{x^l - 1} = x^r \frac{x^{q^l} - 1}{x^l - 1} + \frac{x^r - 1}{x^l - 1}$$

Cum

$$\left(x^{q^l} - 1\right) \Big| (x^l - 1) = (x^l)^{q-1} + (x^l)^{q-2} + \dots + x^l + 1,$$

partea dreaptă a relației de mai sus este polinom dacă și numai dacă $(x^r - 1)(x^l - 1)$ este polinom. Ușor se arată, că aceasta are loc dacă și numai dacă $r = 0$. *Lema este demonstrată.*

Lema 8. Fie a este un număr întreg pozitiv. Atunci $a^l - 1$ divide $a^m - 1$ dacă și numai dacă l divide m.

*Demonstrație***.** Este analog demonstrației lemei 6. *Lema este demonstrată.*

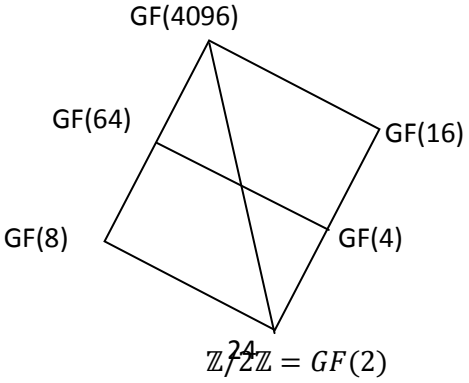
Propoziția 9. Fie $GF(p^n)$ un câmp de dimensiunea n peste câmpl $\mathbb{Z}/p\mathbb{Z}$. Subcâmpurile câmpului $GF(p^n)$ se află în corespondență biunivocă ca divizorii lui n.

Demonstrație. Fie E un careva subcâmp a cîmpului $GF(p^n)$ de dimensiunea α peste $\mathbb{Z}/p\mathbb{Z}$. Să arătăm că $d|n$. Cum E conține elemente se verifică ecuația $x^{p^d-1} - 1 = 0$ și obținem că $x^{p^d-1} - 1$ divide $x^{p^n-1} - 1$, iar după lema 7 d divide n.

Presupunem acum că $d|n$. Considerăm submulțimea $E = \left\{\alpha \in F(p^n) \middle| \alpha^{p^d} = \alpha\right\}$. Afirmăm că E este subcîmp, $(\alpha + \beta)^{p^d} = \alpha^{p^d} + \beta^{p^d}$. Dacă $\alpha \neq 0$ atunci $(\alpha^{-1})^{p^d} = \alpha^{-1}$. Submulțimea E este formată din rădăcinile ecuației $x^{p^d} - x = 0$. Cum $d|n$ rezultă că $p^d - 1 \middle| p^n - 1$ și $x^{p^d-1} - 1 \middle| x^{p^n-1} - 1$. Atunci $x^{p^d} - x \middle| x^{p^n} - x$ și după corolarul 2 E are p^d elemente, deci E are dimensiunea d peste $\mathbb{Z}/p\mathbb{Z}$.

Dacă E' este un alt subcîmp de dimensiunea d peste $\mathbb{Z}/p\mathbb{Z}$ atunci elementele sale verifică ecuația $x^{p^d} - x = 0$ și $E' = E$. *Teorema este demonstrată.*

Pentru ilustrarea propoziției 8 propunem următoarea diagramă.



Propoziția 10. Câmpul de descompunere a polinomului $f(x) = x^{p^n} - x$ din $\mathbb{Z}/p\mathbb{Z}[x]$ coincide cu mulțimea rădăcinilor acestui polinom.

Demonstrație. Fie α, β două rădăcini a acestui polinom. Atunci $(\alpha+\beta)^{p^n} - (\alpha+\beta) = \alpha^{p^n} + \beta^{p^n} - \alpha - \beta = 0$ de unde rezultă că $\alpha+\beta$ este rădăcina a acestui polinom. Analog, $(\alpha\beta)^{p^n} - \alpha\beta = \alpha\beta - \alpha\beta = 0$ de unde conchidem că $\alpha\beta$ este rădăcină. Este evident că 0,1 sunt rădăcini pentru $f(x)$. Dacă $\beta \neq 0$ atunci $(\beta^{-1})^{p^n} - \beta^{-1} = \left(\beta^{p^n}\right)^{-1} - \beta^{-1} = 0$ deci β^{-1} este rădăcină. În final, avem $(-\beta)^{p^n} - (-\beta) = (-1)^{p^n}(\beta)^{p^n} + \beta.$

Dacă p este impar, $(-1)^{p^n} = -1$ și $-\beta$ este rădăcină.

Dacî p este par $(-1)^{p^n} = 1$ în $\mathbb{Z}/2\mathbb{Z}$ și $-\beta = \beta$ este rădăcnă.

Cum derivata polinomului $f(x)$ este $p^n z^{p^n-1} - 1 = -1$ urmează că $f(x)$ nu are rădăcini multiple. Astfel câmpul de descompunere a polinomului $f(x)$ conține p^n elemente. *Propoziția este demonstrată.*

Are loc teorema:

Teorema 11. Pentru orice număr simplu p și orice număr întreg $n \geq 1$ există câmpul de ordinul $p^n, GF(p^n)$. Orice câmp finit este izomof unui și numai unui din câmpurile $GF(p^n)$.

Teorema 12. Grupul multiplicativ $GF^*(p^n)$ a câmpului finit este grup ciclic.

*Demonstrație***.** Elementele grupului $GF^*(p^n)$ sînt rădăcinile polinomului $f(x) = x^{p^n-1} - 1$. Notăm cu α elementul grupului $GF^*(p^n)$ de ordin maximal $p^n - 1, \alpha^{p^n-1} = 1.$

Afirmăm, că grupul $A = \langle\alpha\rangle$ generat de α conține $p^n - 1$ elemente. Într-adevăr, dacă $A = GF^*(p^n)$ atunci polinomul $f(x)$ are mai mult de $p^n - 1$ rădăcini – contradicție. *Teorema este demonstrată.*

2.2. O metodă de construire a câmpurilor finite.

Din afirmațiile precedente rezultă următoarea metodă de construire a câmpului finit. Procedăm în modul următor:

a) Căutăm un polinom ireductibil normat $f(x)$ de gradul n peste câmpul $GF(p^n)$ format din p elemente.

b) Notăm cu θ elementul căutat a câmpului format din p elemente. Din relația $\alpha_0 + \alpha_1\theta + \alpha_2\theta^2 + \ ... + \alpha_{n-1}\theta^{n-1} + \theta^n = 0$, obținem $\theta^n = -(\alpha_0 + \alpha_1\theta + \alpha_2\theta^2 + \ ... + \alpha_{n-1}\theta^{n-1})$. Cu ajutorul acestei relații obținem tablița de înmulțire a cîmpului din p^n elemente $GF(p^n)$.

În continuare propunem câteva exemple de aplicare a acestei metode:

i) Arătăm cum se construesc tăblițele de adunare și înmulțire pentru câmpul din 4 elemente. Demonstrăm mai întâi că polinomul $f(x) = x^2 + x + 1$ este ireductibil peste $GF(2)$.

Întra-devăr, $f(0) = 0^2 + 0 + 1 \neq 0, f(1) = 1^2 + 1 + 1 \neq 0$, deci $f(x)$ este ireductibil peste $GF(2)$. Atunci $\theta^2 + \theta + 1 = 0$, de unde $\theta^2 = -\theta - 1 = 1 + \theta$. Orice element a câmpului $GF(2^2)$ se reprezintă sub formă $c_0 + c_1\theta, c_0, c_1 \in GF(2^2)$. Atunci $GF(2^2) = \{0, 1, \theta, 1 + \theta\}$.

Să arătăm cum se face adunare și înmulțirea în $GF(2^2)$. De exemplu ,$\theta + (1 + \theta) = 1 + 2\theta = 1, \theta(1 + \theta) = \theta + \theta^2 = 1 + \theta + \theta = 1$.

Completăm acum tablițele:

+	0	1	θ	1+θ
0	0	1	θ	1+θ
	1	0	1+θ	θ
θ	θ	1+θ	1	1
1+θ	1+θ	θ	1	0

·	0	1	θ	1+θ
0	0	0	0	0
1	0	1	θ	1+θ
θ	0	θ	1+θ	1
1+θ	0	1+θ	1	0

ii) Construim acum câmpul din 8 elemente $GF(2^3)$.

Demonstrăm mai întâi că polinomul $\varphi(x) = x^3 + x + 1$ este ireductibil peste $GF(2)$. Într-adevăr, $\varphi(\theta) = \theta^3 + \theta + 1 = 1 \neq 0, \varphi(1) = 1^3 + 1 + 1 = 1 \neq 0$, deci $\varphi(x)$ este ireductibil. Atunci $\theta^3 + \theta + 1 = 0$ de unde $\theta^3 = 1 + \theta$. Orice element a câmpului $GF(2^3)$ se scrie sub forma $\alpha_0 + \alpha_1\theta + \alpha_2\theta^2, \alpha_0, \alpha_1, \alpha_2 \in GF(2)$. Atunci $GF(2^3) = \{0, 1, \theta, \theta^2, 1 + \theta, 1 + \theta^2, \theta + \theta^2, 1 + \theta + \theta^2\}$. Să arătăm cum se face adunarea și înmulțirea în $GF(2^3)$. De exemplu: $(1 + \theta^2) + (\theta + \theta^2) = 1 + \theta + 2\theta^2 = 1 + \theta, (1 + \theta^2)(\theta + \theta^2) = \theta + \theta^2 + \theta^3 + \theta^4 = \theta + \theta^2 + 1 + \theta + \theta(1 + \theta) = 1 + \theta.$

Completăm acum tablițele de adunare și înmulțire în $GF(2^3)$.

+	0	1	θ	θ^2	1+θ	$1+\theta^2$	$\theta+\theta^2$	$1+\theta+\theta^2$
0	0	1	θ	θ^2	1+θ	$1+\theta^2$	$\theta+\theta^2$	$1+\theta+\theta^2$
1	1	0	1+θ	$1+\theta^2$	θ	θ^2	$1+\theta+\theta^2$	$\theta+\theta^2$
θ	θ	1+θ	0	$\theta+\theta^2$	1	$1+\theta+\theta^2$	θ^2	$1+\theta^2$
θ^2	θ^2	$1+\theta^2$	$\theta+\theta^2$	0	$1+\theta+\theta^2$	1	θ	1+θ
1+θ	1+θ	θ	1	$1+\theta+\theta^2$	0	$\theta+\theta^2$	$1+\theta^2$	θ^2
$1+\theta^2$	$1+\theta^2$	θ^2	$1+\theta+\theta^2$	1	$\theta+\theta^2$	0	1+θ	θ
$\theta+\theta^2$	$\theta+\theta^2$	$1+\theta+\theta^2$	θ^2	θ	$1+\theta^2$	1+θ	0	1
$1+\theta+\theta^2$	$1+\theta+\theta^2$	$\theta+\theta^2$	$1+\theta^2$	1+θ	θ^2	θ	1	0

·	0	1	θ	θ^2	1+θ	$1+\theta^2$	$\theta+\theta^2$	$1+\theta+\theta^2$
0	0	0	0	0	0	0	0	0
1	0	1	θ	θ^2	1+θ	$1+\theta^2$	$\theta+\theta^2$	$1+\theta+\theta^2$
θ	0	θ	θ^2	1+θ	$\theta+\theta^2$	1	$1+\theta+\theta^2$	$1+\theta^2$
θ^2	0	θ^2	1+θ	$\theta+\theta^2$	$1+\theta+\theta^2$	θ	$1+\theta^2$	1
1+θ	0	1+θ	$\theta+\theta^2$	$1+\theta+\theta^2$	$1+\theta^2$	θ^2	1	θ
$1+\theta^2$	0	$1+\theta^2$	1	θ	θ^2	$1+\theta+\theta^2$	1+θ	$\theta+\theta^2$
$\theta+\theta^2$	0	$\theta+\theta^2$	$1+\theta+\theta^2$	$1+\theta^2$	1	1+θ	θ	θ^2
$1+\theta+\theta^2$	0	$1+\theta+\theta^2$	$1+\theta^2$	1	θ	$\theta+\theta^2$	θ^2	1+θ

iii) Construim acum câmpul din 9 elemente $GF(3^2)$

Demonstrăm mai întâi ca polinomul $g(x) = x^2 + x + 2$ este ireductibil peste $GF(3)$. Într-adevăr $g(\theta) = \theta^2 + \theta + 2 = 2, g(1) = 1^2 + 1 + 2 = 1, g(2) = 2^2 + 2 + 2 = 2$, deci $g(x)$ este ireductibil peste $GF(3^2)$. Atunci $\theta^2 + \theta + 2 = 0$ de unde $\theta^2 = -\theta - 2 = 2\theta + 1$. Orice element al cîmpului $GF(3^2)$ se scrie sub forma $\beta_0 + \beta_1\theta, \beta_0, \beta_1 \in GF(3^2)$. Atunci $GF(3^2) = \{0, 1, 2, \theta, 1 + \theta, 2 + \theta, 2\theta, 1 + 2\theta, 2 + 2\theta\}$.

Să arătăm cum se face adunarea și înmulțirea în $GF(3^2)$, de exemplu

$(1 + 2\theta) + (2 + 2\theta) = 3 + 4\theta = \theta, (1 + 2\theta)(2 + 2\theta) = 2 + 2\theta + 4\theta + 4\theta^2 = 1 + \theta$

Completăm acum tablițele de adunare și înmulțire în $GF(3^2)$.

+	0	1	2	θ	1+θ	2+θ	2θ	1+2θ	2+2θ
0	0	1	2	θ	1+θ	2+θ	2θ	1+2θ	2+2θ
1	1	2	0	1+θ	2+θ	θ	1+2θ	2+2θ	2θ
2	2	0	1	2+θ	θ	1+θ	2+2θ	2θ	1+2θ
θ	θ	1+θ	2+θ	2θ	1+2θ	2+2 θ	0	1	2
1+θ	1+θ	2+θ	θ	1+2θ	2+2θ	2 θ	1	2	0
2+θ	2+θ	θ	1+ θ	2+2θ	2θ	1+2θ	2	0	1
2θ	2θ	1+2θ	2+2θ	0	1	2	θ	1+θ	2+θ
1+2θ	1+2θ	2+2θ	2θ	1	2	0	1+θ	2+θ	θ
2+2θ	2+2θ	2 θ	1+2θ	2	0	1	2+θ	θ	1+ θ

·	0	1	2	θ	1+θ	2+θ	2θ	1+2θ	2+2θ
0	0	0	0	0	0	0	0	0	0
1	0	1	2	θ	1+θ	2+θ	2θ	1+2	2+2θ
2	0	2	1	2θ	2+2θ	1+2θ	θ	2+θ	1+θ
θ	0	θ	2θ	1+2θ	1	1+θ	2+θ	2+2θ	2
1+θ	0	1+θ	2+2θ	1	2+θ	2θ	2	θ	1+2θ
2+θ	0	2+θ	1+2θ	1+θ	2θ	2	2+2θ	1	θ
2θ	0	2θ	θ	2+θ	2	2+2θ	1+2θ	1+θ	1
1+2θ	0	1+2θ	2+θ	2+2θ	θ	1	1+θ	2	2θ
2+2θ	0	1+2θ	1+θ	2	1+2θ	θ	1	2θ	2+θ

Indicăm acum unele din polinoamele ireductibile ce pot fi folosite la construirea câmpurilor de ordinele

$$GF(2^4): x^4 + x + 1; GF(2^5): x^5 + x^2 + 1;\ GF(2^6): x^6 + x + 1;$$
$$GF(2^7): x^7 + x^3 + 1;\ GF(2^8): x^8 + x^4 + x^3 + x^2 + 1;$$
$$GF(2^9): x^9 + x^4 + 1; GF(2^{10}): x^{10} + x^4 + 1;$$
$$GF(2^{11}): x^{11} + x^2 + 1; GF(2^{12}): x^{12} + x^6 + x^4 + x + 1;$$
$$GF(2^{13}): x^{13} + x^4 + x^3 + x + 1;\ GF(2^{14}): x^{14} + x^{10} + x^6 + x + 1;$$
$$GF(2^{15}): x^{15} + x + 1;\ GF(3^3): x^3 + 2x + 1; GF(5^3): x^3 + x + 4;$$
$$GF(7^2): x^2 + 6x + 6;\ GF(7^3): x^3 + 4x + 6;$$

§ 3.Probleme propuse

3.1. Găsiți polinomul minimal pentru elementele:

a) $\sqrt{7}\ peste\ \mathbb{Q}$;

b) $1 - 2i\ peste\ \mathbb{R}$;

c) $1 + 2i\ peste\ \mathbb{C}$;

d) $\sqrt{3} + \sqrt{5}\ peste\ \mathbb{Q}$;

e) $3 + \sqrt{3}\ peste\ \mathbb{Q}(\sqrt{3} + \sqrt{5})$.

3.2. Descrieți extinderile:

a) $\mathbb{Q}(\sqrt{2})$;

b) $\mathbb{Q}(\sqrt{3};\ \sqrt[3]{3})$;

c) $\mathbb{Q}(\sqrt{2};\ \sqrt{5})$;

d) $\mathbb{Q}(i;\ \sqrt[3]{5})$.

3.3. Demonstrați, că câmpurile $\boldsymbol{Q(\sqrt{13})}$ și $\boldsymbol{Q(\sqrt{17})}$ nu sunt izomorfe.

3.4. Demonstrați, că câmpul $\boldsymbol{R(1+i)}$ este izomorf câmpului numerelor complexe $\mathbb{C}$.

3.5. Eliberați de iracționalitate la numitor fracția:

a) $\frac{7-4\sqrt[3]{25}}{2\sqrt[3]{25}+7\sqrt[3]{5}-21}$;

b) $\frac{1}{\sqrt{2}+2\sqrt[4]{2}-1}$;

c) $\frac{1}{\sqrt{3}+\sqrt{5}+1}$.

Bibliografie

1. L. Culicov, Alghebra i teoria cisel, M., 1979.
2. A. Costrichin, Vvedenie v alghebru, M., 1977.
3. S. Leng, Alghebra, M., 1976.
4. B. L. V.Waerdon, Alghebra, M., 1976.
5. M. Postincov, Teoria Galaua, M., 1963.
6. A. Costrichin, Sbornic zadaci po alghebre, M. 1962.
7. L. Snaperman, Sbornic zadaci po alghebre o teorii cisel, M., 1982