

Capitole speciale de algebră

Ioan Băetu
Ciprian Băetu

*Colegiul Național „Mihai Eminescu”
Botoșani*

Editura TAIDA - 2020 -

Societatea de Științe Matematice – Filiala Botoșani

CAPITOLUL I

Grupuri finite**&1. Grupuri abeliene finite**

1.1. Definiție. Fie G un grup și $H_1, H_2, \dots, H_n \subseteq G$, n subgrupuri ale grupului G , $n \geq 1$. Numim *produsul (intern)* al acestor subgrupuri (în această ordine), submulțimea notată cu $H_1 H_2 \dots H_n \subseteq G$ și definită prin :

$$H_1 H_2 \dots H_n = \{x_1 x_2 \dots x_n \mid x_1 \in H_1, x_2 \in H_2, \dots, x_n \in H_n\}.$$

1.2. Propoziție. Dacă $H, K \subseteq G$ sunt două subgrupuri ale grupului G , atunci $|HK| = \frac{|H| \cdot |K|}{|H \cap K|}$.

Demonstrație. Fie $\varphi: H \times K \rightarrow HK$, $\varphi(h, k) = hk$. Deoarece condiția $\varphi(h, k) = \varphi(h_1, k_1)$ se scrie $hk = h_1 k_1$ sau încă $h_1^{-1} h = k_1 k^{-1} = z \in H \cap K$, deducem că $h_1 = h z^{-1}$ și $k_1 = z k$, cu z arbitrar din $H \cap K$. Cum există $|H \cap K|$ perechi de forma $(h z^{-1}, z k)$, când z descrie mulțimea $H \cap K$, rezultă că pentru orice $a \in \text{Im } \varphi$, contraimaginea lui a prin φ conține exact $|H \cap K|$ elemente. Întrucât $H \times K = \bigcup_{a \in \text{Im } \varphi} \varphi^{-1}(a)$ și $\text{Im } \varphi = HK$, găsim $|H| \cdot |K| = |H \times K| = \sum_{a \in \text{Im } \varphi} |\varphi^{-1}(a)| = |H \cap K| \cdot \sum_{a \in \text{Im } \varphi} 1 = |H \cap K| \cdot |\text{Im } \varphi| = |H \cap K| \cdot |HK|$, de unde $|HK| = \frac{|H| \cdot |K|}{|H \cap K|}$. \square

1.3. Propoziție. Dacă G este un grup comutativ, atunci produsul finit al oricărui $n \geq 1$ subgrupuri ale lui G este tot un subgrup al grupului G .

Demonstrație. Fie $H_1, H_2, \dots, H_n \subseteq G$, n subgrupuri ale grupului G . Atunci, pentru orice $x, y \in H_1 H_2 \dots H_n$ putem scrie $x = h_1 h_2 \dots h_n$, $y = r_1 r_2 \dots r_n$, cu $h_i, r_i \in H_i, \forall i \in \{1, 2, \dots, n\}$. Deoarece grupul G este comutativ, obținem: $xy^{-1} = (h_1 h_2 \dots h_n)(r_1^{-1} r_2^{-1} \dots r_n^{-1}) = (h_1 r_1^{-1})(h_2 r_2^{-1}) \dots (h_n r_n^{-1}) \in H_1 H_2 \dots H_n$. \square

Scopul acestui paragraf este acela de a stabili condiții în care să se verifice reciproca afirmației de mai sus.

Dacă G este un grup, notăm cu C submulțimea lui G definită prin

$C = \{x \in G / xa = ax, \forall a \in G\}$. Se știe că C formează un subgrup comutativ al grupului G , numit *centrul lui G* . De asemenea, pentru orice element $a \in G$, notăm cu $C(a) = \{x \in G / xa = ax\}$, care este iarăși un subgrup al grupului G , numit *centralizatorul lui a în G* . Definim în continuare relația de conjugare pe grupul G prin $a \approx b$ dacă și numai dacă există $x \in G$ astfel încât $a = x^{-1}bx$. Arătăm că " \approx " este o relație de echivalență pe G .

1) Desigur, pentru orice $a \in G$ avem $a = e^{-1}ae$, cu $e \in G$, de unde $a \approx a$.

2) Dacă $a \approx b$ din $a = x^{-1}bx$, cu $x \in G$ obținem $b = xax^{-1} = (x^{-1})^{-1}ax^{-1}$.

Cum $x^{-1} \in G$, rezultă $b \approx a$.

3) Fie $a, b, c \in G$ astfel, încât $a \approx b$ și $b \approx c$. Atunci $a = x^{-1}bx$, $b = y^{-1}cy$, cu $x, y \in G$. Din $yx \in G$ și $a = x^{-1}(y^{-1}cy)x = (yx)^{-1}c(yx)$, deducem că $a \approx c$.

Deci " \approx " este o relație de echivalență pe G .

Convenim ca pentru orice $a \in G$, să notăm cu C_a clasa de conjugare cu reprezentantul a . Avem:

$$C_a = \{b \in G / b \approx a\} = \{b \in G / b = x^{-1}ax, x \in G\} = \{x^{-1}ax / x \in G\}.$$

1.4. Propoziție. Dacă G este un grup finit, atunci numărul elementelor din clasa de conjugare a elementului $a \in G$ coincide cu indicele subgrupului $C(a)$ în G .

Demonstrație. Condiția $x^{-1}ax = y^{-1}ay$, cu $x, y \in G$, devine: $(yx^{-1})a = a(yx^{-1}) \Leftrightarrow yx^{-1} \in C(a) \Leftrightarrow C(a)x = C(a)y$. În definitiv, prin negare, găsim echivalența: $x^{-1}ax \neq y^{-1}ay \Leftrightarrow C(a)x \neq C(a)y$, de unde afirmația. \square

Firește, pentru orice $a \in C$, avem $C_a = \{x^{-1}ax / x \in G\} = \{(x^{-1}x)a / x \in G\} = \{a / x \in G\} = \{a\}$, adică orice sistem complet de reprezentanți ai claselor de conjugare pe G conține toate elementele centrului C .

1.5. Teoremă. Fie G un grup finit. Atunci,

$$\text{ord } G = \text{ord } C + \sum_a [G : C(a)] \quad (\text{ecuația claselor}),$$

unde suma de mai sus se extinde după elementele unui sistem complet de reprezentanți ai claselor de conjugare, care nu aparțin lui C .

Demonstrație. Fie a_1, a_2, \dots, a_q un sistem de reprezentanți ai claselor de conjugare pe G . Din $G = \bigcup_{i=1}^q C_{a_i}$ și $C_{a_i} \cap C_{a_j} = \emptyset, \forall i, j \in \{1, 2, \dots, q\}$, cu $i \neq j$,

CAPITOLUL II

Inele de polinoame&1. Inele de polinoame cu coeficienți într-un corp comutativ

Peste tot, inelele și subinelele le vom considera nenule și unitare.

1.1. Propoziție. (teorema împărțirii cu rest). Fie A un inel comutativ și $g = a_m X^m + \dots + a_1 X + a_0 \in A[X]$, cu $\text{grad}(g) = m, m \geq 1$. Dacă elementul a_m este inversabil în inelul A , atunci pentru orice polinom f din $A[X]$ există în mod unic polinoamele $h, r \in A[X]$ astfel încât $f = gh + r$ și $\text{grad}(r) < m$.

Demonstrație. Existența proprietății o vom demonstra prin inducție după gradul lui f . Dacă $\text{grad}(f) < m$, luăm $h = 0$ și $r = f$. Să presupunem că $\text{grad}(f) \geq m$ și afirmația adevărată pentru orice polinom din $A[X]$ de grad

mai mic decât gradul lui f . Fie $f = \sum_{i=0}^n b_i X^i \in A[X]$, cu $\text{grad}(f) = n$ și $n \geq m$. Cum $f_1 = f - a_m^{-1} b_n X^{n-m} g$ verifică condițiile presupunerii inductive, există $h_1, r \in A[X]$ astfel încât $f_1 = gh_1 + r$ și $\text{grad}(r) < m$. Punând $h = a_m^{-1} b_n X^{n-m} + h_1 \in A[X]$, găsim $f = f_1 + a_m^{-1} b_n X^{n-m} g = gh_1 + r + a_m^{-1} b_n X^{n-m} g = gh + r$, ceea ce trebuia arătat.

Unicitatea afirmației. Dacă ar exista polinoamele $h', r' \in A[X]$ încât $f = gh' + r'$ și $\text{grad}(r') < m$, din $r - r' = (f - gh) - (f - gh') = g(h' - h)$, obținem:

$$(1) \quad m > \text{grad}(r - r') = \text{grad}(g(h' - h)).$$

În presupunerea că $h' \neq h$, fie $h' - h = \sum_{i=0}^s c_i X^i \in A[X]$, unde $s \in \mathbb{N}$ și $c_s \neq 0$. Din

$$(1) \text{ și } g(h' - h) = \sum_{i=0}^{s+m} d_i X^i, \text{ cu } d_{s+m} = a_m c_s, \text{ putem scrie } a_m c_s = 0. \text{ Așadar, } c_s = a_m^{-1} (a_m c_s) = a_m^{-1} \cdot 0 = 0, \text{ absurd. Prin urmare } h' = h \text{ și totodată } r - r' = g(h' - h) = g \cdot 0 = 0, \text{ adică } r = r'. \quad \square$$

1.2. Teorema lui Bézout. Fie A un inel comutativ. Dacă $f \in A[X]$ este un polinom neconstant, atunci elementul α din A este o rădăcina a lui f dacă și numai dacă $X - \alpha$ divide f .

Demonstrație. Fie $g = X - \alpha \in A[X]$. Conform teoremei împărțirii cu

rest, există $h, r \in A[X]$ astfel încât $f = gh + r$ și $\text{grad}(r) < 1$. Demonstrația se încheie observând că $f(\alpha) = g(\alpha)h(\alpha) + r = r$. \square

Firește, dacă L este un corp comutativ, inelul de polinoame $L[X]$ este euclidian, căci în $L[X]$ are loc teorema împărțirii cu rest a polinoamelor. Prin urmare, în inelul $L[X]$ sunt verificate toate proprietățile aritmetice ale inelelor euclidiene, proprietăți știute de la inelul numerelor întregi \mathbb{Z} , cu demonstrații asemănătoare.

Fie K un corp comutativ și $g = \sum_{i=0}^n a_i X^i \in K[X]$ un polinom de grad n , $n \geq 1$. Conform teoremei împărțirii cu rest, aplicată în $K[X]$, oricărui polinom f din $K[X]$ îi corespunde în mod unic două polinoame $c, r \in K[X]$ astfel încât $f = gc + r$ și $\text{grad}(r) < \text{grad}(g)$.

Un raționament simplu arată că singurele polinoame din $K[X]$ ce dau prin împărțirea lor la g restul r sunt cele de forma $gh + r$, cu $h \in K[X]$ și numai acestea. De aceea, mulțimea $\{gh + r \mid h \in K[X]\}$ se numește clasa de resturi a lui r și-o vom nota cu \hat{r} , iar mulțimea

$$K[X]/g = \{ \hat{r} \mid r \in K[X], \text{grad}(r) < \text{grad}(g) \},$$

se numește *mulțimea claselor de resturi modulo g* .

În aplicații, este adesea util să descriem clasele de resturi și prin alte polinoame care aparțin acestora. Prin definiție vom pune:

$$\hat{f} = \widehat{f \bmod g}, \forall f \in K[X],$$

unde prin $f \bmod g$ s-a notat restul împărțirii lui f la g .

Desigur, $\hat{f} = \hat{h}$ dacă și numai dacă polinoamele f și h dau același rest prin împărțirea lor la g , adică, dacă și numai dacă g divide $f - h$. În particular, dacă $\hat{f} = \hat{h}$ și $\hat{f}_1 = \hat{h}_1$, avem: $f = h + gc$, $f_1 = h_1 + gc_1$, cu $c, c_1 \in K[X]$. Atunci,

$$f + f_1 = h + h_1 + (c + c_1) \cdot g \quad \text{și} \quad ff_1 = hh_1 + (hc_1 + ch_1 + cc_1)g,$$

de unde,

$$\widehat{f + f_1} = \widehat{h + h_1} \quad \text{și} \quad \widehat{ff_1} = \widehat{hh_1}.$$

Acest rezultat, permite definirea corectă a două operații algebrice pe mulțimea $L = K[X]/g$, notate tot aditiv și multiplicativ, și anume:

$$\hat{f} + \hat{f}_1 = \widehat{f + f_1}, \quad \hat{f} \hat{f}_1 = \widehat{ff_1}.$$

CAPITOLUL III

Inele&1. Extinderi finite de corpuri

Peste tot în acest paragraf, corpurile le vom considera comutative.

Fie $K \subseteq L$ o extindere de corpuri. Firește, se știe că intersecția tuturor corpurilor, extinderi ale lui K , care conțin elementele date $\alpha_1, \alpha_2, \dots, \alpha_n$ din L este de asemenea un corp și este cea mai mică extindere a lui K ce conține elementele $\alpha_1, \alpha_2, \dots, \alpha_n$. Îl notăm cu $K(\alpha_1, \alpha_2, \dots, \alpha_n)$ și se numește *extinderea lui K generată de elementele $\alpha_1, \alpha_2, \dots, \alpha_n$* . Punând:

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

se verifică cu destulă ușurință că:

$$1) K(\alpha_1, \dots, \alpha_n) = K, \text{ dacă și numai dacă } \alpha_1, \dots, \alpha_n \in K.$$

$$2) K(\alpha_1, \dots, \alpha_n) = K(\alpha_1, \dots, \alpha_i)(\alpha_{i+1}, \dots, \alpha_n), \forall 1 \leq i \leq n.$$

3) $K[\alpha_1, \dots, \alpha_n]$ este cel mai mic subinel al lui L care-l conține pe K și elementele $\alpha_1, \dots, \alpha_n$. În plus, $K[\alpha_1, \dots, \alpha_n] \subseteq K(\alpha_1, \dots, \alpha_n)$.

Un rol important în acest paragraf îl au extinderile finite de corpuri. Astfel, extinderea L a lui K este finită, dacă există în corpul L un număr finit de elemente nenule și distincte $\alpha_1, \alpha_2, \dots, \alpha_n$, $n \geq 1$, cu proprietatea că orice $\beta \in L$ se poate scrie în mod unic sub forma unei combinații liniare de aceste elemente și cu coeficienți din corpul K , adică:

$$\beta = a_1\alpha_1 + a_2\alpha_2 + \dots + a_n\alpha_n, \text{ cu } a_1, \dots, a_n \in K.$$

Un sistem de elemente $\alpha_1, \dots, \alpha_n$ ce verifică proprietatea de mai sus se numește *bază a extinderii lui L peste K* .

Se demonstrează imediat că sistemul $\alpha_1, \dots, \alpha_n \in L$ reprezintă o bază a lui L peste K dacă și numai dacă:

$$1) \text{ Pentru orice } \beta \in L, \text{ există } a_1, \dots, a_n \in K \text{ astfel încât } \beta = a_1\alpha_1 + \dots + a_n\alpha_n.$$

$$2) \text{ Din egalitatea } a_1\alpha_1 + \dots + a_n\alpha_n = 0, \text{ cu } a_1, \dots, a_n \in K, \text{ rezultă } a_1 = a_2 = \dots = a_n = 0.$$

Orice sistem de elemente $\alpha_1, \alpha_2, \dots, \alpha_n$ care verifică 1), desemnează un sistem de generatori ai lui L peste K .

Un sistem de elemente $\alpha_1, \alpha_2, \dots, \alpha_n$ care verifică 2), se numește liniar independent peste K . În caz contrar, sistemul se numește liniar dependent peste K .

1.1.Propoziție. Fie $K \subseteq L$ o extindere de corpuri și $\alpha_1, \dots, \alpha_n$ o bază a lui L peste K . Atunci, pentru orice $\beta_1, \dots, \beta_m \in L$, cu $m > n$, există elementele $b_1, b_2, \dots, b_m \in K$, nu toate nule, astfel încât $b_1\beta_1 + \dots + b_m\beta_m = 0$.

Demonstrație. Conform ipotezei, avem: $\beta_i = \sum_{j=1}^n a_{ij} \alpha_j$, cu $a_{ij} \in K$, $\forall i = 1, \dots, m$, $\forall j = 1, \dots, n$, ceea ce arată că sistemul liniar,

$$(1). \quad \begin{cases} a_{11}x_1 + \dots + a_{1n}x_n = \beta_1 \\ \dots \\ a_{m1}x_1 + \dots + a_{mn}x_n = \beta_m \end{cases}$$

admite soluția nenulă: $x_1 = \alpha_1, \dots, x_n = \alpha_n$. Fie,

$$A = \begin{pmatrix} a_{11} & \dots & a_{1n} \\ \dots & \dots & \dots \\ a_{m1} & \dots & a_{mn} \end{pmatrix} \quad \text{și} \quad B = \begin{pmatrix} a_{11} & \dots & a_{1n} & \beta_1 \\ \dots & \dots & \dots & \dots \\ a_{m1} & \dots & a_{mn} & \beta_m \end{pmatrix}.$$

Deoarece sistemul (1) este compatibil, rangul matricei A coincide cu rangul matricei extinse B . Fie $\text{rang}(A) = r$. Putem presupune, fără a restrânge din

generalitate, că determinantul submatricei $A_r = \begin{pmatrix} a_{11} & \dots & a_{1r} \\ \dots & \dots & \dots \\ a_{r1} & \dots & a_{rr} \end{pmatrix}$ este nenul. Cum

$$r \leq n < m, \text{ rezultă } \begin{vmatrix} a_{11} & \dots & a_{1r} & \beta_1 \\ \dots & \dots & \dots & \dots \\ a_{r1} & \dots & a_{rr} & \beta_r \\ a_{r+11} & \dots & a_{r+1r} & \beta_{r+1} \end{vmatrix} = 0 \text{ care, dezvoltat după ultima coloană,}$$

ne asigură că există elementele $b_1, b_2, \dots, b_{r+1} \in K$, unde b_{r+1} este determinantul matricei A_r , pentru care $b_1\beta_1 + \dots + b_{r+1}\beta_{r+1} = 0$ și totodată $b_{r+1} \neq 0$. Afirmția este evidentă dacă $m = r + 1$. În caz contrar, punem $b_i = 0$ pentru $i = r + 2, \dots, m$ și obținem $b_1\beta_1 + \dots + b_{r+1}\beta_{r+1} + \dots + b_m\beta_m = 0$. \square

Fie $\alpha_1, \dots, \alpha_m$ și respectiv β_1, \dots, β_n două baze ale lui L peste K . Dacă

CAPITOLUL IV

Corpuri finite**&1. Automorfismele unui corp finit**

Prezentăm fără demonstrație următorul rezultat extrem de important în teoria corpurilor finite:

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

Dacă L este un corp finit cu p^n elemente, p – prim, atunci ordinul elementului unitate în grupul aditiv $(L, +)$ este p . Deci $\mathbb{Z}_p \subseteq L$. Întrucât p este prim, rezultă p divide $C_p^k, \forall k \in \{1, 2, \dots, p-1\}$, de unde $(x+y)^p = x^p + y^p, \forall x, y \in L$. Prin generalizare, găsim:

$$(x+y)^{p^m} = x^{p^m} + y^{p^m}, \forall x, y \in L, \forall m \in \mathbb{N}.$$

1.2. Propoziție. Fie L un corp finit. Atunci orice funcție $f: L \rightarrow L$ este funcție polinomială.

Demonstrație. Fie $L = \{\alpha_1, \alpha_2, \dots, \alpha_n\}$, cu $n = |L|$ și sistemul liniar

$$(S) \begin{cases} x_0 + \alpha_1 x_1 + \dots + \alpha_1^{n-2} x_{n-2} + \alpha_1^{n-1} x_{n-1} = f(\alpha_1) \\ x_0 + \alpha_2 x_1 + \dots + \alpha_2^{n-2} x_{n-2} + \alpha_2^{n-1} x_{n-1} = f(\alpha_2) \\ \dots \dots \dots \dots \dots \dots \dots \\ x_0 + \alpha_n x_1 + \dots + \alpha_n^{n-2} x_{n-2} + \alpha_n^{n-1} x_{n-1} = f(\alpha_n) \end{cases}$$

în necunoscutele $x_0, x_1, \dots, x_{n-1} \in L$. Întrucât determinantul matricei sistemului este:

$$\Delta = \begin{vmatrix} 1 & \alpha_1 & \dots & \alpha_1^{n-2} & \alpha_1^{n-1} \\ 1 & \alpha_2 & \dots & \alpha_2^{n-2} & \alpha_2^{n-1} \\ \dots & \dots & \dots & \dots & \dots \\ 1 & \alpha_n & \dots & \alpha_n^{n-2} & \alpha_n^{n-1} \end{vmatrix} = \prod_{1 \leq j < i \leq n} (\alpha_i - \alpha_j) \neq 0,$$

rezultă că există în corpul L elementele unice b_0, b_1, \dots, b_{n-1} pentru care:

$$\begin{cases} b_0 + \alpha_1 b_1 + \dots + \alpha_1^{n-2} b_{n-2} + \alpha_1^{n-1} b_{n-1} = f(\alpha_1) \\ b_0 + \alpha_2 b_1 + \dots + \alpha_2^{n-2} b_{n-2} + \alpha_2^{n-1} b_{n-1} = f(\alpha_2) \\ \dots \dots \dots \dots \dots \dots \dots \\ b_0 + \alpha_n b_1 + \dots + \alpha_n^{n-2} b_{n-2} + \alpha_n^{n-1} b_{n-1} = f(\alpha_n) \end{cases}$$

Notând cu $g = b_{n-1}X^{n-1} + \dots + b_1X + b_0$, $g \in L[X]$, putem scrie $g(x) = f(x)$, $\forall x \in L$, ceea ce trebuia demonstrat. \square

Fie $f, g \in L[X]$ astfel încât $\text{grad}(f) = m$, $\text{grad}(g) = n$, $m \leq n$ și fie $M \subseteq L$, cu $|M| = l$, unde $n < l$. Dacă $f(x) = g(x)$, $\forall x \in M$ atunci $(f-g)(x) = 0$, $\forall x \in M$. Cum $f-g \in L[X]$ și $\text{grad}(f-g) \leq n < l$, suntem în condițiile proprietății **1.11**, capitolul II. Astfel $f = g$, de unde $f(x) = g(x)$, $\forall x \in L$.

1.3. Propoziție. Dacă L este un corp cu n elemente, $n \geq 2$ atunci orice endomorfism neconstant $f: L \rightarrow L$, de monoizi multiplicativi, este de forma $f(x) = x^m$, unde $m \in \mathbb{N}$ și $1 \leq m \leq n-1$.

Demonstrație. Conform proprietății **1.2**, există $g \in L[X]$ de forma $g = a_{n-1}X^{n-1} + \dots + a_1X + a_0$ astfel încât $g(x) = f(x)$, $\forall x \in L$. Cum endomorfismul f este neconstant, putem scrie $\text{grad}(g) \geq 1$. Fie m cel mai mare număr din mulțimea $\{1, 2, \dots, n-1\}$ pentru care $a_m \neq 0$. Atunci $1 \leq m \leq n-1$ și totodată $f(x) = a_mx^m + \dots + a_1x + a_0$, $\forall x \in L$. Întrucât:

$$(1) f(xy) = f(x)f(y), \forall x, y \in L,$$

obținem: $a_mx^m y^m + \dots + a_1xy + a_0 = f(x)(a_my^m + \dots + a_1y + a_0)$, $\forall x, y \in L \Leftrightarrow$

$$\Leftrightarrow a_m(x^m - f(x))y^m + \dots + a_1(x - f(x))y + a_0(1 - f(x)) = 0, \forall x, y \in L.$$

Menținându-l pe x fixat, conform proprietății **1.11**, capitolul II, găsim:

$$\begin{cases} a_m(x^m - f(x)) = 0 \\ \dots\dots\dots \\ a_1(x - f(x)) = 0 \\ a_0(1 - f(x)) = 0 \end{cases}, \forall x \in L.$$

Dar $a_m \neq 0$, deci $f(x) = x^m$, $\forall x \in L$. Se observă ușor că funcția f astfel definită verifică (1), adică reprezintă un endomorfism de monoizi multiplicativi. \square

1.4. Propoziție. Fie L un corp cu n elemente, $n \geq 2$. Atunci, funcția $f: L \rightarrow L$ este un izomorfism de monoizi multiplicativi dacă și numai dacă există $m \in \mathbb{N}$, cu $1 \leq m \leq n-1$ și $(m, n-1) = 1$ astfel încât $f(x) = x^m$, $\forall x \in L$.

Demonstrație. Fie $f: L \rightarrow L$ un izomorfism de monoizi multiplicativi.

CAPITOLUL V

Caracterizarea corpurilor finite folosind ecuațiile algebrice**&1. Grupul unităților unui inel finit de caracteristică p , p – prim**

Dacă L este un corp finit de caracteristică p , atunci \mathbb{Z}_p este cel mai mic subcorp (în sensul incluziunii) al corpului L . Firește, conform proprietății 3.4, cap. III, există un număr $n \in \mathbb{N}^*$ pentru care $|L| = p^n$. Deoarece înmulțirea definită pe L induce pe L^* o structură de grup cu $p^n - 1$ elemente, deducem că $x^{p^n - 1} = \hat{1}, \forall x \in L^*$, de unde $x^{p^n} = x, \forall x \in L$. Acest rezultat arată că rădăcinile în L ale polinomului $f = X^{p^n} - X \in \mathbb{Z}_p[X]$ sunt distincte două câte două și, mai mult, reprezintă cele p^n elemente ale corpului L . Așadar, L este o extindere algebrică a corpului \mathbb{Z}_p .

1.1. Propoziție Fie L un corp cu p^n elemente, p – prim, $p, n \in \mathbb{N}^*$. Atunci pentru orice $x \in L$, avem: $x + x^p + x^{p^2} + \dots + x^{p^{n-1}} \in \mathbb{Z}_p$.

Demonstrație. Pentru orice element $x \in L$, rezultă $x^{p^n} = x$. Fie $\alpha = x + x^p + x^{p^2} + \dots + x^{p^{n-1}}$. Cum corpul L este finit, deci comutativ, obținem $\alpha^p = (x + x^p + x^{p^2} + \dots + x^{p^{n-1}})^p = x^p + x^{p^2} + \dots + x^{p^{n-1}} + x^{p^n} = x + x^p + \dots + x^{p^{n-1}} = \alpha$. Așadar, α este o rădăcină în L a polinomului $f = X^p - X \in \mathbb{Z}_p[X]$. Întrucât rădăcinile în L ale acestui polinom sunt elementele lui \mathbb{Z}_p , deducem că $\alpha \in \mathbb{Z}_p$. \square

1.2. Propoziție. Dacă L este un corp cu $|L| = p^n$, unde $p, n \in \mathbb{N}, p$ – prim și $n \geq 2$, atunci există $x \in L$ astfel încât $\hat{1} + x^{p-1} + x^{p^2-1} + \dots + x^{p^{n-1}-1} = \hat{0}$.

Demonstrație. Deoarece \mathbb{Z}_p^* este un subgrup al grupului multiplicativ L^* , deducem că relația " \sim " definită pe L^* prin $x \sim y$ dacă și numai dacă $xy^{-1} \in \mathbb{Z}_p^*$ este o relație de echivalență pe L^* .

Fie polinomul $f = X^{p^{n-1}} + X^{p^{n-2}} + \dots + X^p + X - \hat{1} \in \mathbb{Z}_p[X]$. Firește, conform

proprietății 1.1, pentru orice $x \in L^*$ există $\hat{a} \in \mathbb{Z}_p$ încât $x + x^p + x^{p^2} + \dots + x^{p^{n-1}} = \hat{a}$. Dacă pentru un anumit element $x \in L^*$, rezultă $\hat{a} \neq \hat{0}$, atunci:

$$\begin{aligned} f(\hat{a}^{-1}x) &= (\hat{a}^{-1} \cdot x)^{p^{n-1}} + (\hat{a}^{-1} \cdot x)^{p^{n-2}} + \dots + (\hat{a}^{-1} \cdot x)^p + (\hat{a}^{-1} \cdot x) - \hat{1} = \\ &= \hat{a}^{-1}(x^{p^{n-1}} + x^{p^{n-2}} + \dots + x^p + x) - \hat{1} = \hat{a}^{-1} \cdot \hat{a} - \hat{1} = \hat{0}, \end{aligned}$$

ceea ce înseamnă că elementul $\hat{a}^{-1} \cdot x$ este o rădăcină în L a polinomului f . Dar $\hat{a}^{-1} \cdot x \sim x$, deci $\hat{a}^{-1} \cdot x \in C_x$, unde C_x desemnează clasa de echivalență cu reprezentantul x . Vom arăta că $\hat{a}^{-1} \cdot x$ este unica rădăcină în C_x a polinomului f .

Într-adevăr, pentru orice elemente u, v , rădăcini în C_x ale lui f , avem:

$$u + u^p + u^{p^2} + \dots + u^{p^{n-1}} = v + v^p + v^{p^2} + \dots + v^{p^{n-1}} = \hat{1}. \text{ Cum } u \sim v, \text{ rezultă } u = \hat{b}v, \text{ cu } \hat{b} \in \mathbb{Z}_p^*.$$

Din șirul de egalități: $\hat{1} = u + u^p + \dots + u^{p^{n-1}} = (\hat{b}v) + (\hat{b}v)^p + \dots + (\hat{b}v)^{p^{n-1}} = \hat{b}(v + v^p + \dots + v^{p^{n-1}}) = \hat{b}$, deducem $u = v$. În consecință, dacă există în L^* elemente x pentru care $x + x^p + x^{p^2} + \dots + x^{p^{n-1}} \in \mathbb{Z}_p^*$, atunci în clasa C_x se află exact o rădăcină a polinomului f .

Să presupunem acum că pentru orice $x \in L^*$ obținem $x + x^p + x^{p^2} + \dots + x^{p^{n-1}} \in \mathbb{Z}_p^*$. În acest caz, fiecare clasă C_x , cu $x \in L^*$ va conține câte o singură rădăcină a polinomului f .

Întrucât reuniunea tuturor claselor de echivalență, disjuncte două câte două, coincide cu L^* , deducem că numărul rădăcinilor distincte din L^* ale polinomului f coincide cu numărul acestor clase de echivalență.

Dar $|C_x| = |C_1| = |\mathbb{Z}_p^*| = p-1$ și $f(\hat{0}) = -\hat{1} \neq \hat{0}$, așa că polinomul f , de grad p^{n-1} , admite în corpul L un număr de

$$[L^* : \mathbb{Z}_p^*] = \frac{p^n - 1}{p - 1} = p^{n-1} + p^{n-2} + \dots + p + 1 \text{ rădăcini distincte, contradicție. Prin}$$

urmare, există un element $x \in L^*$ pentru care $x + x^p + x^{p^2} + \dots + x^{p^{n-1}} = \hat{0}$. Cum x este inversabil în L , rezultă $\hat{1} + x^{p-1} + \dots + x^{p^{n-1}-1} = x^{-1}(x + x^p + \dots + x^{p^{n-1}}) = \hat{0}$. \square

Firește, se pune problema de a studia dacă nu cumva egalitatea din propoziția 1.2 se verifică și în cazul unor structuri mai generale și anume ale

CAPITOLUL VI

Rădăcinile unității unor corpuri numerice**&1. Rădăcinile unității unui corp pătratic**

Fie θ un număr *liber de pătrate*, adică un număr întreg nedivizibil prin pătratul unui număr prim. Deoarece numerele $-\sqrt{\theta}$ și $\sqrt{\theta}$ reprezintă cele două rădăcini în \mathbb{C} ale polinomului $g = X^2 - \theta \in \mathbb{Q}[X]$ și $\sqrt{\theta} \notin \mathbb{Q}$, deducem că g este ireductibil peste \mathbb{Q} . Așadar, operațiile de adunare și înmulțire din \mathbb{C} induc pe $\mathbb{Q}(\sqrt{\theta}) = \{f(\sqrt{\theta}) / f \in \mathbb{Q}[X], \text{grad}(f) \leq 1\} = \{a + b\sqrt{\theta} / a, b \in \mathbb{Q}\}$ o structură de corp comutativ, numit *corp pătratic*.

Notând cu $\mathbb{Q}(\sqrt{\theta})^*$ subgrupul multiplicativ al elementelor nenule ale monoidului $\mathbb{Q}(\sqrt{\theta})$, interesează găsirea mulțimii tuturor subgrupurilor finite al acestui grup.

1.1. Definiție. Se numește *întreg algebric* orice număr complex α , pentru care există un polinom unitar $f \in \mathbb{Z}[X]$ astfel încât $f(\alpha) = 0$.

Fie $\alpha = \frac{p}{q}$, cu $p, q \in \mathbb{Z}, q \neq 0$ un întreg algebric dat. Întrucât q divide

1, rezultă $\alpha = \pm p \in \mathbb{Z}$. Prin urmare, orice întreg algebric rațional este un număr întreg.

Fie θ un număr real arbitrar. Avem:

1.2. Propoziție. Pentru orice $n \in \mathbb{N}^*$, există un polinom $f_n \in \mathbb{Z}[X]$, unitar și de grad n , astfel încât $2 \cos(n\theta) = f_n(2 \cos \theta)$.

Demonstrație. Inducție după variabila n . Scriind $S_n = 2 \cos(n\theta), n \in \mathbb{N}^*$, din $2 \cos(n-1)\theta \cos \theta = \cos(n\theta) + \cos(n-2)\theta$, rezultă $S_n = 2 \cos \theta \cdot S_{n-1} - S_{n-2}, \forall n \geq 3$. Firește, afirmația este evidentă pentru $n=1$, căci $2 \cos \theta = f_1(2 \cos \theta)$, unde $f_1 = X \in \mathbb{Z}[X]$. Din $2 \cos(2\theta) = 2(2 \cos^2 \theta - 1) = (2 \cos \theta)^2 - 2 = f_2(2 \cos \theta)$, cu $f_2 = X^2 - 2 \in \mathbb{Z}[X]$, rezultă că afirmația se verifică și pentru $n=2$.

Să presupunem $n \geq 2$ și afirmația adevărată pentru orice număr $k \in \{1, 2, \dots, n\}$. Atunci, există polinoamele $f_{n-1}, f_n \in \mathbb{Z}[X]$, unitare și de grade

CAPITOLUL VII

&1. Exerciții și probleme propuse.

1.1. Fie G un grup finit cu n elemente, $H = \{x \in G / x^2 = e\}$, unde e reprezintă elementul neutru al grupului G și fie p numărul elementelor lui H . Arătați că:

- $|H \cap xH| \geq 2p - n, \forall x \in G$.
- Dacă $p > \frac{3n}{4}$, atunci grupul G este comutativ.
- Dacă $\frac{n}{2} < p \leq \frac{3n}{4}$, atunci grupul G este necomutativ.

Olimpiada Națională / 2010

1.2 Un grup G are proprietatea (P) dacă, pentru orice automorfism f al lui G , există două automorfisme g și h ale lui G , astfel încât $f(x) = g(x) \cdot h(x)$, $\forall x \in G$. Să se arate că:

- Orice grup care are proprietatea (P) este comutativ.
- Orice grup finit comutativ de ordin impar are proprietatea (P).
- Niciun grup finit de ordin $4n+2$, $n \in \mathbb{N}$, nu are proprietatea (P).

Olimpiada Județeană / 2013

1.3. Fie A o mulțime nevidă și F o mulțime finită de funcții injective, cu domeniul și codomeniul mulțimea A . Dacă legea de compunere a funcțiilor este operație algebrică peste F , să se arate că (F, \circ) este un grup.

1.4. Fie A un inel unitar, fără divizori ai lui zero diferiți de zero și O mulțimea tuturor submulțimilor lui A^* formate cu câte m elemente, $m \geq 1$. Pentru fiecare $x \in A^*$ și $\alpha \in O$, notăm cu $\alpha x = \{ax \mid a \in \alpha\} \in O$. Să se arate că:

i) Aplicația $\bar{x}: O \rightarrow O$, $\bar{x}(\alpha) = \alpha x$ verifică $\overline{\bar{x}y} = \bar{y} \circ \bar{x}$, $\forall x, y \in A^*$.

ii) Mulțimea $G_\alpha = \{x \in A^* \mid \bar{x}(\alpha) = \alpha\}$ formează un subgrup multiplicativ având ordinul un divizor al lui m .

1.5. Fie G un grup finit cu n elemente ($n \geq 2$), m cel mai mare divizor al lui n diferit de n , iar $A \subseteq G$, $A \neq \emptyset$. Să se arate că dacă mai mult de m elemente din G comută cu toate elementele mulțimii A , atunci toate elementele lui G au aceeași proprietate. Ce se întâmplă în cazul $A = G$?

1.6. Fie G o mulțime pe care s-a definit operația algebrică asociativă " \circ " având proprietățile:

- $\exists e \in G$, e fixat astfel încât $e \circ x = x, \forall x \in G$.
- $\forall x \in G, \exists x' \in G$, astfel încât $x' \circ x = e$.

Să se arate că (G, \circ) este grup.

1.7. Fie $(G, +)$ un grup ciclic de ordinul n , $n \geq 2$. Să se arate că numărul legilor de compoziție "*" definite peste G ce-i conferă tripletului $(G, +, *)$ o structură de inel unitar este $\varphi(n)$, unde φ desemnează indicatorul lui Euler.

1.8. Fie (G, \cdot) un grup cu proprietatea că există un endomorfism $f: G \rightarrow G$, astfel încât $f(x^2 y^3) = x^3 y^2, \forall x, y \in G$. Să se arate că:

a) Grupul G este abelian.

b) $x^5 = e, \forall x \in G$, e fiind elementul neutru.

1.9. Se dau H un subgrup nenul al grupului $(\mathbb{R}, +)$ și $b \in H, b \neq 0$ fixat. Să se arate că:

i) $H_b = \{kb \mid k \in \mathbb{Z}\}$ este un subgrup al grupului $(H, +)$.

ii) $H_b = H$ dacă și numai dacă $|b|$ reprezintă cel mai mic număr pozitiv din H .

1.10. Fie $G = \{A \in M_2(\mathbb{C}) / \det(A) = \pm 1\}$ și $H = \{A \in M_2(\mathbb{C}) / \det(A) = 1\}$. Să se arate că mulțimile G și H formează două grupuri multiplicative, neizomorfe.

Olimpiada Județeană / 2006

1.11. Determinați ecuația cu coeficienți reali de forma: $x^3 + ax^2 + bx + c = 0$, ale cărei rădăcini în \mathbb{C} formează un grup în raport cu operația algebrică

$$x * y = \frac{x+y}{1-xy}.$$

1.12. Pentru un grup $(G, *)$ și $A, B \subseteq G$ submulțimi nevide, notăm cu $A * B = \{a * b / a \in A, b \in B\}$.

a) Să se arate că dacă $n \in \mathbb{N}, n \geq 3$, atunci grupul $(\mathbb{Z}_n, +)$ se poate scrie sub forma $\mathbb{Z}_n = A + B$, unde A și B sunt două submulțimi nevide ale lui \mathbb{Z}_n cu $A \neq \mathbb{Z}_n, B \neq \mathbb{Z}_n$ și $|A \cap B| = 1$.

b) Dacă $(G, *)$ este un grup finit și A, B sunt submulțimi ale lui G iar $a \in G \setminus (A * B)$, să se arate că funcția $f: A \rightarrow G \setminus B$ dată de $f(x) = x^{-1} * a$ este bine definită și injectivă. Deduceți că dacă $|A| + |B| > |G|$, atunci $G = A * B$.

Olimpiada Județeană / 2007

1.13. Fie G un grup cu m elemente și H un subgrup propriu al său cu n elemente. Pentru fiecare $x \in G$ notăm cu $H^x = \{xh x^{-1} / h \in H\}$ și presupunem că $H^x \cap H = \{e\}, \forall x \in G \setminus H$.