Capitole speciale de algebră

Ioan Băetu
Ciprian Băetu

Colegiul Național „Mihai Eminescu”
Botoşani

Editura TAIDA - 2020 -

Societatea de Ştiinţe Matematice – Filiala Botoşani

CAPITOLUL I

Grupuri finite

&1. Grupuri abeliene finite

1.1. Definiţie. Fie *G* un grup şi $H_1, H_2,...,H_n \subseteq G$, n subgrupuri ale grupului G, $n \geq 1$. Numim *produsul (intern)* al acestor subgrupuri (în această ordine), submulţimea notată cu $H_1H_2...H_n \subseteq G$ şi definită prin :

$$H_1H_2...H_n = \{x_1x_2...x_n \ / \ x_1 \in H_1, x_2 \in H_2,..., x_n \in H_n\}.$$

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

Demonstraţie. Fie $\varphi : H \times K \to HK$, $\varphi(h,k) = hk$. Deoarece condiţia $\varphi(h,k) = \varphi(h_1,k_1)$ se scrie $hk = h_1k_1$ sau încă $h_1^{-1}h = k_1k^{-1} = z \in H \cap K$, deducem că $h_1 = hz^{-1}$ şi $k_1 = zk$, cu z arbitrar din $H \cap K$. Cum există $|H \cap K|$ perechi de forma (hz^{-1}, zk), când z descrie mulţimea $H \cap K$, rezultă că pentru orice $a \in \operatorname{Im}\varphi$, contraimaginea lui a prin φ conţine exact $|H \cap K|$ elemente.Întrucât $H \times K = \bigcup\limits_{a \in \operatorname{Im}\varphi} \varphi^{-1}(a)$ şi $\operatorname{Im}\varphi = HK$, găsim $|H| \cdot |K| = |H \times K| = \sum\limits_{a \in \operatorname{Im}\varphi} |\varphi^{-1}(a)| =$ $= |H \cap K| \cdot \sum\limits_{a \in \operatorname{Im}\varphi} 1 = |H \cap K| \cdot |\operatorname{Im}\varphi| = |H \cap K| \cdot |HK|$, de unde $|HK| = \dfrac{|H| \cdot |K|}{|H \cap K|}$. □

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

Demonstraţie. Fie $H_1, H_2,..., H_n \subseteq G$, n subgrupuri ale grupului G. Atunci, pentru orice $x, y \in H_1 H_2 ... H_n$ putem scrie $x = h_1h_2...h_n$, $y = r_1r_2...r_n$, cu $h_i, r_i \in H_i, \forall i \in \{1,2,...,n\}$. Deoarece grupul G este comutativ, obţinem:

$$xy^{-1} = (h_1h_2...h_n)(r_1^{-1}r_2^{-1}...r_n^{-1}) = (h_1r_1^{-1})(h_2r_2^{-1})...(h_nr_n^{-1}) \in H_1H_2...H_n . \ \square$$

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

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

$C=\{x\in G/xa=ax,\forall a\in G\}$. Se ştie 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 iarăşi un subgrup al grupului G, numit *centralizatorul lui* a *în* G. Definim în continuare relaţia de conjugare pe grupul G prin : $a\approx b$ dacă şi numai dacă există $x\in G$ astfel încât $a=x^{-1}bx$. Arătăm că "$\approx$" este o relaţie de echivalenţă 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 $x\in G$ obţinem $b=xax^{-1}=(x^{-1})^{-1}ax^{-1}$. Cum $x^{-1}\in G$, rezultă $b\approx a$.

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

Deci "$\approx$" este o relaţie de echivalenţă 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.Propoziţie. 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.

Demonstraţie. Condiţia $x^{-1}ax=y^{-1}ay$, 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 echivalenţa: $x^{-1}ax\neq y^{-1}ay\Leftrightarrow C(a)x\neq C(a)y$, de unde afirmaţia. □

Fireşte, 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 reprezentanţi ai claselor de conjugare pe G conţine toate elementele centrului C

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

$$ordG=ordC+\sum_a[G:C(a)] \quad \textit{(ecuaţia claselor)},$$

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

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

CAPITOLUL II

Inele de polinoame

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

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

1.1.Propoziţie. *(teorema împărţirii cu rest)*. Fie A un inel comutativ şi $g=a_m X^m+...+a_1 X+a_0\in A[X]$, cu $grad(g)=m, m\geq 1$. 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 $f=gh+r$ şi $grad(r)<m$.

Demonstraţie. Existenţa proprietăţii o vom demonstra prin inducţie după gradul lui f. Dacă $grad(f)<m$, luăm $h=0$ şi $r=f$. Să presupunem că $grad(f)\geq m$ şi afirmaţia 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 $grad(f)=n$ şi $n\geq m$. Cum $f_1=f-a_m^{-1}b_n X^{n-m}g$ verifică condiţiile presupunerii inductive, există $h_1, r\in A[X]$ astfel încât $f_1=gh_1+r$ şi $grad(r)<m$. 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 afirmaţiei.Dacă ar exista polinoamele $h', r'\in A[X]$ încât $f=gh'+r'$ şi $grad(r')<m$, din $r-r'=(f-gh)-(f-gh')=g(h'-h)$, obţinem:

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

În presupunerea că $h'\neq h$, fie $h'-h=\sum_{i=0}^{s} c_i X^i\in A[X]$, unde $s\in\mathbb{N}$ şi $c_s\neq 0$. Din (1) şi $g(h'-h)=\sum_{i=0}^{s+m} d_i X^i$, cu $d_{s+m}=a_m c_s$, putem scrie $a_m c_s=0$. Aşadar, $c_s=$ $=a_m^{-1}(a_m c_s)=a_m^{-1}\cdot 0=0$, absurd.Prin urmare $h'=h$ şi totodată $r-r'=g(h'-h)=$ $=g\cdot 0=0$, adică $r=r'$. □

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 şi numai dacă $X-\alpha$ divide f .

Demonstraţie. Fie $g=X-\alpha\in A[X]$. Conform teoremei împărţirii cu rest, există $h, r \in A[X]$ astfel încât $f = gh + r$ şi $grad(r) < 1$. Demonstraţia se încheie observând că $f(\alpha) = g(\alpha)h(\alpha) + r = r$. $\square$

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

Fie K un corp comutativ şi $g = \sum_{i=0}^{n} a_i X^i \in K[X]$ un polinom de grad n, $n \geq 1$. Conform teoremei împărţirii 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 $f = gc + r$ şi $grad(r) < grad(g)$.

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

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

se numeşte *mulţimea claselor de resturi modulo* g .

În aplicaţii, este adesea util să descriem clasele de resturi şi prin alte polinoame care aparţin acestora. Prin definiţie vom pune:

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

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

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

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

de unde,

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

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

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

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.Fireşte, se ştie că intersecţia tuturor corpurilor, extinderi ale lui K, care conţin elementele date $\alpha_1, \alpha_2, ..., \alpha_n$ din L este de asemenea un corp şi este cea mai mică extindere a lui K ce conţine elementele $\alpha_1, \alpha_2, ..., \alpha_n$. Îl notăm cu $K(\alpha_1, \alpha_2, .., \alpha_n)$ şi se numeşte *extinderea lui K generată de elementele $\alpha_1, \alpha_2, ..., \alpha_n$*.Punând:

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

se verifică cu destulă uşurinţă că:

1) $K(\alpha_1, ..., \alpha_n) = K$, dacă şi numai dacă $\alpha_1, ..., \alpha_n \in K$.

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

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

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 şi distincte $\alpha_1, \alpha_2, ..., \alpha_n$, $n \geq 1$, cu proprietatea că orice $\beta \in L$ se poate scrie în mod unic sub forma unei combinaţii liniare de aceste elemente şi cu coeficienţi din corpul K, adică:

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

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

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

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

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

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

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

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

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

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

admite soluţia nenulă: $x_1=\alpha_1,\ldots,x_n=\alpha_n$. Fie,

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

Deoarece sistemul (1) este compatibil, rangul matricei A coincide cu rangul matricei extinse B. Fie rang $(A)=r$. Putem presupune, fără a restrânge din generalitate, că determinantul submatricei $A_r=\begin{pmatrix} a_{11}\ldots.a_{1r} \\ a_{r1}\ldots.a_{rr} \end{pmatrix}$ este nenul. Cum $r\leq n<m$, rezultă $\begin{vmatrix} a_{11}\ldots\ldots.a_{1r} & \beta_1 \\ \ldots\ldots\ldots\ldots & \ldots \\ a_{r1}\ldots\ldots a_{rr} & \beta_r \\ a_{r+1\,1}\ldots a_{r+1\,r} & \beta_{r+1} \end{vmatrix}=0$ care, dezvoltat după ultima coloană, ne asigură că există elementele $b_1,b_2,\ldots,b_{r+1}\in K$, unde b_{r+1} este determinantul matricei A_r, pentru care $b_1\beta_1+\ldots+b_{r+1}\beta_{r+1}=0$ şi totodată $b_{r+1}\neq 0$. Afirmaţia este evidentă dacă $m=r+1$. Îm caz contrar, punem $b_i=0$ pentru $i=r+2,\ldots,m$ şi obţinem $b_1\beta_1+\ldots+b_{r+1}\beta_{r+1}+\ldots+b_m\beta_m=0$. □

Fie $\alpha_1,\ldots,\alpha_m$ şi respectiv $\beta_1,\ldots,\beta_n$ două baze ale lui L peste K. Dacă

CAPITOLUL IV

Corpuri finite

&1. Automorfismele unui corp finit

Prezentăm fără demonstraţie 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 $C_p^k, \forall k \in \{1,2,..,p-1\}$, 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.Propoziţie. Fie L un corp finit. Atunci orice funcţie $f: L \to L$ este funcţie polinomială.

Demonstraţie. Fie $L = \{\alpha_1, \alpha_2, ..., \alpha_n\}$, cu $n = |L|$ şi sistemul liniar

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

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

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

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

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

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

Fie $f,g\in L[X]$ astfel încât $grad(f)=m$, $grad(g)=n$, $m\le n$ şi 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 $f-g\in L[X]$ şi $grad(f-g)\le n<l$, suntem în condiţiile proprietăţii **1.11**, capitolul II. Astfel $f=g$, de unde $f(x)=g(x),\forall x\in L$.

1.3.Propoziţie. Dacă L este un corp cu n elemente, $n\ge 2$ atunci orice endomorfism neconstant $f:L\to L$, de monoizi multiplicativi, este de forma $f(x)=x^m$, unde $m\in\mathbb{N}$ şi $1\le m\le n-1$.

Demonstraţie. Conform proprietăţii **1.2**, există $g\in L[X]$ de forma $g=$ $=a_{n-1}X^{n-1}+\ldots+a_1X+a_0$ astfel încât $g(x)=f(x),\forall x\in L$. Cum endomorfismul f este neconstant, putem scrie $grad(g)\ge 1$. Fie m cel mai mare număr din mulţimea $\{1,2,\ldots,n-1\}$ pentru care $a_m\ne 0$. Atunci $1\le m\le n-1$ şi totodată $f(x)=$ $=a_mx^m+\ldots+a_1x+a_0,\forall x\in L$. Întrucât:

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

obţinem: $a_mx^my^m+\ldots+a_1xy+a_0=f(x)(a_my^m+\ldots+a_1y+a_0),\forall x,y\in L\Leftrightarrow$ $\Leftrightarrow a_m(x^m-f(x))y^m+\ldots+a_1(x-f(x))y+a_0(1-f(x))=0,\forall x,y\in L$.

Menţinându-l pe x fixat, conform proprietăţii **1.11**, capitolul II, găsim:

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

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

1.4. Propoziţie. Fie L un corp cu n elemente, $n\ge 2$. Atunci, funcţia $f:L\to L$ este un izomorfism de monoizi multiplicativi dacă şi numai dacă există $m\in\mathbb{N}$, cu $1\le m\le n-1$ şi $(m,n-1)=1$ astfel încât $f(x)=x^m,\forall x\in L$.

Demonstraţie. Fie $f:L\to L$ 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 proprietăţii **3.4**,cap.III, există un număr $n\in\mathbb{N}^*$ pentru care $|L|=p^n$. Deoarece înmulţirea 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 şi, mai mult, reprezintă cele p^n elemente ale corpului L. Așadar, L este o extindere algebrică a corpului $\mathbb{Z}_p$.

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

Demonstraţie. Pentru orice element $x\in L$, rezultă $x^{p^n}=x$. Fie $\alpha=$ $=x+x^p+x^{p^2}+\ldots+x^{p^{n-1}}$. Cum corpul L este finit, deci comutativ, obţinem $\alpha^p=$ $=(x+x^p+x^{p^2}+\ldots+x^{p^{n-1}})^p=x^p+x^{p^2}+..+x^{p^{n-1}}+x^{p^n}=x+x^p+..+x^{p^{n-1}}=\alpha$. Aşadar, 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 $\alpha\in\mathbb{Z}_p$. □

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

Demonstraţie. Deoarece $\mathbb{Z}_p^*$ este un subgrup al grupului multiplicativ L^*, deducem că relaţia "~" definită pe L^* prin $x\sim y$ dacă şi numai dacă $xy^{-1}\in$ $\in\mathbb{Z}_p^*$ este o relaţie de echivalenţă pe L^*.

Fie polinomul $f=X^{p^{n-1}}+X^{p^{n-2}}+\ldots+X^p+X-\hat{1}\in\mathbb{Z}_p[X]$. Firește, conform proprietății **1.1**, pentru orice $x\in L^*$ există $\hat{a}\in\mathbb{Z}_p$ încât $x+x^p+x^{p^2}+...+x^{p^{n-1}}=$ $=\hat{a}$. Dacă pentru un anumit element $x\in L^*$, rezultă $\hat{a}\neq\hat{0}$, atunci:

$$f(\hat{a}^{-1}x)=(\hat{a}^{-1}\cdot x)^{p^{n-1}}+(\hat{a}^{-1}\cdot x)^{p^{n-2}}+...+(\hat{a}^{-1}\cdot x)^p+(\hat{a}^{-1}\cdot x)-\hat{1}=$$
$$=\hat{a}^{-1}(x^{p^{n-1}}+x^{p^{n-2}}+...+x^p+x)-\hat{1}=\hat{a}^{-1}\cdot\hat{a}-\hat{1}=\hat{0},$$

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 echivalenţă 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: $u+u^p+u^{p^2}+...+u^{p^{n-1}}=v+v^p+v^{p^2}+...+v^{p^{n-1}}=\hat{1}$. Cum $u\sim v$, rezultă $u=\hat{b}v$, cu $\hat{b}\in\mathbb{Z}_p^*$. Din șirul de egalități: $\hat{1}=u+u^p+...+u^{p^{n-1}}=(\hat{b}v)+(\hat{b}v)^p+...+(\hat{b}v)^{p^{n-1}}=$ $=\hat{b}(v+v^p+...+v^{p^{n-1}})=\hat{b}$, deducem $u=v$. În consecinţă, dacă există în L^* elemente x pentru care $x+x^p+x^{p^2}+...+x^{p^{n-1}}\in\mathbb{Z}_p^*$, atunci în clasa C_x se află exact o rădăcină a polinomului f. Să presupunem acum că pentru orice $x\in$ $\in L^*$ obținem $x+x^p+x^{p^2}+...+x^{p^{n-1}}\in\mathbb{Z}_p^*$. În acest caz, fiecare clasă C_x, cu $x\in L^*$ va conţine câte o singură rădăcină a polinomului f. Întrucât reuniunea tuturor claselor de echivalenţă, disjuncte două câte două, coincide cu L^*, deducem că numărul rădăcinilor distincte din L^* ale polinomului f coincide cu numărul acestor clase de echivalenţă. Dar $|C_x|=|C_1|=|\mathbb{Z}_p^*|=p-1$ şi $f(\hat{0})=$ $=-\hat{1}\neq\hat{0}$, aşa că polinomul f, de grad p^{n-1}, admite în corpul L un număr de $[L^*:\mathbb{Z}_p^*]=\dfrac{p^n-1}{p-1}=p^{n-1}+p^{n-2}+...+p+1$ rădăcini distincte, contradicţie. Prin urmare, există un element $x\in L^*$ pentru care $x+x^p+x^{p^2}+...+x^{p^{n-1}}=\hat{0}$. Cum x este inversabil în L, rezultă $\hat{1}+x^{p-1}+...+x^{p^{n-1}-1}=x^{-1}(x+x^p+...+x^{p^{n-1}})=\hat{0}$. □

Fireşte, se pune problema de a studia dacă nu cumva egalitatea din propoziţia **1.2** se verifică şi în cazul unor structuri mai generale şi 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 $g=X^2-\theta\in\mathbb{Q}[X]$ şi $\sqrt{\theta}\notin\mathbb{Q}$, deducem că g este ireductibil peste $\mathbb{Q}$. Așadar, operaţiile de adunare şi înmulţire din $\mathbb{C}$ induc pe $\mathbb{Q}(\sqrt{\theta})=\{f(\sqrt{\theta})/f\in\mathbb{Q}[X],\operatorname{grad}(f)\leq 1\}=\{a+b\sqrt{\theta}/a,b\in\mathbb{Q}\}$ 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 mulţimii tuturor subgrupurilor finite al acestui grup.

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

Fie $\alpha=\dfrac{p}{q}$, 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 raţional este un număr întreg.

Fie θ un număr real arbitrar.Avem:

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

Demonstraţie. Inducţie după variabila n .Scriind $S_n=2\cos(n\theta), n\in\in\mathbb{N}^*$, din $2\cos(n-1)\theta\cos\theta=\cos(n\theta)+\cos(n-2)\theta$, rezultă $S_n=2\cos\theta\cdot S_{n-1}-S_{n-2}$, $\forall n\geq 3$. Fireşte, afirmaţia 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 afirmaţia se verifică şi pentru $n=2$.

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

CAPITOLUL VII

&1. Exerciţii şi 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:

a) $|H\cap xH|\geq 2p-n, \forall x\in G.$

b) Dacă $p>\frac{3n}{4}$, atunci grupul G este comutativ.

c) 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:

a) Orice grup care are proprietatea (P) este comutativ.

b) Orice grup finit comutativ de ordin impar are proprietatea (P).

c) Niciun grup finit de ordin $4n+2$, $n\in\mathbb{N}$, nu are proprietatea (P).

Olimpiada Județeană / 2013

1.3. Fie A o mulţime nevidă şi F o mulţime finită de funcţii injective, cu domeniul şi codomeniul mulţimea 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 diferiţi de zero şi O mulţimea tuturor submulţimilor lui A^* formate cu câte m elemente, $m\geq 1$. Pentru fiecare $x\in A^*$ şi $\alpha\in O$, notăm cu $\alpha x=\{ax|a\in\alpha\}\in O$. Să se arate că:

$i)$ Aplicaţia $\overline{x}:O\to O$, $\overline{x}(\alpha)=\alpha x$ verifică $\overline{xy}=\overline{y}\circ\overline{x}$, $\forall x,y\in A^*$.

$ii)$ Mulţimea $G_\alpha=\{x\in A^*|\overline{x}(\alpha)=\alpha\}$ 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 mulţimii A , atunci toate elementele lui G au aceeaşi proprietate.Ce se întâmplă în cazul $A=G$?

1.6. Fie G o mulţime pe care s-a definit operația algebrică asociativă "$\circ$" având proprietăţile:

1) $\exists e\in G, e$ fixat astfel încât $e\circ x=x, \forall x\in G$.

2) $\forall x\in G, \exists x'\in G$, 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 compoziţie "$*$" 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 $f:G\to G$, astfel încât $f(x^2y^3)=x^3y^2, \forall x,y\in G$. 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 $(\mathbb{R},+)$ şi $b\in H, b\neq 0$ 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 şi numai dacă $|b|$ reprezintă cel mai mic număr pozitiv din H.

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

Olimpiada Judeţeană / 2006

1.11. Determinaţi ecuaţia cu coeficienţi reali de forma: $x^3+ax^2+bx+c=$ $=0$, ale cărei rădăcini în $\mathbb{C}$ formează un grup în raport cu operația algebrică $x*y=\dfrac{x+y}{1-xy}$.

1.12. Pentru un grup $(G,*)$ şi $A,B\subseteq G$ submulţimi 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 şi B sunt două submulţimi nevide ale lui $\mathbb{Z}_n$ cu $A\neq\mathbb{Z}_n$, $B\neq\mathbb{Z}_n$ şi $|A\cap B|=1$.

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

Olimpiada Judeţeană / 2007

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