

Curs VI

ELEMENTE DE TEORIA GRUPURILOR

§ 3. RELAȚII DE ECHIVALENȚĂ PE UN GRUP ÎN RAPORT CU UN SUBGRUP AL SĂU

Fie G un grup și H un subgrup al său. Considerăm pe G relațiile binare R_H^s și R_H^d definite în modul următor: dacă $x, y \in G$, atunci

$$x R_H^s y \text{ dacă și numai dacă } x^{-1}y \in H,$$

$$x R_H^d y \text{ dacă și numai dacă } xy^{-1} \in H.$$

Aceste relații binare sunt relații de echivalență. Să demonstrăm, de exemplu, că prima relație binară este relație de echivalență, adică este reflexivă, simetrică și tranzitivă.

- 1) Dacă $x \in G$, atunci $x^{-1}x = e \in H$ și deci $x R_H^s x$ (reflexivitatea).
- 2) Dacă $x R_H^s y$, atunci $x^{-1}y \in H$ și deci $y^{-1}x = (x^{-1}y)^{-1} \in H$, de unde $y R_H^s x$ (simetria).
- 3) Dacă $x R_H^s y$ și $y R_H^s z$, atunci $x^{-1}y \in H$ și $y^{-1}z \in H$. Deci $x^{-1}z = (x^{-1}y)(y^{-1}z) \in H$, adică $x R_H^s z$ (tranzitivitatea).

Analog se demonstrează că R_H^d este relație de echivalență.

Relațiile de echivalență R_H^s și R_H^d se numesc *relații de congruență la stânga, respectiv la dreapta, în raport cu H (sau modulo H)*. Faptul că „ x este în relația R_H^s cu y ” (respectiv „ x este în relația R_H^d cu y ”) se mai citește *x este congruent cu y modulo H la stânga* (respectiv *x este congruent cu y modulo H la dreapta*) și scriem

$$x \equiv_s y \pmod{H}, \text{ respectiv } x \equiv_d y \pmod{H}.$$

Să notăm cu $[x]_s$, respectiv $[x]_d$, clasa de echivalență a elementului $x \in G$ în raport cu R_H^s , respectiv R_H^d , și o vom numi *clasa de echivalență la stânga, respectiv clasa de echivalență la dreapta a lui x modulo H* .

Fie G/R_H^s și G/R_H^d mulțimile factor (cât) corespunzătoare lui R_H^s și R_H^d , adică mulțimile claselor de echivalență la stânga, respectiv la dreapta modulo H .

Exemple.

1) Dacă G este un grup, relațiile de congruență la stânga și la dreapta modulo $\{e\}$ coincid (adică $x R_{\{e\}}^s y$ dacă și numai dacă $x R_{\{e\}}^d y$). De asemenea, relațiile R_G^s și R_G^d modulo G coincid.

2) Dacă G este un grup comutativ, iar H un subgrup oarecare al lui G , atunci relațiile de congruență la stânga și la dreapta modulo H coincid.

3) Fie S_3 grupul permutărilor de 3 elemente, adică

$$S_3 = \left\{ \begin{bmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{bmatrix}, \begin{bmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{bmatrix}, \begin{bmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{bmatrix}, \begin{bmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{bmatrix} \right\}$$

și

$$H = \left\{ \begin{bmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{bmatrix}, \begin{bmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{bmatrix} \right\}.$$

Este evident că H este un subgrup al lui S_3 .

Să construim mulțimile claselor de echivalență la stânga și la dreapta modulo H . Dacă $\sigma, \tau \in S_3$, atunci $\sigma^{-1}\tau \in H$ dacă și numai dacă $\sigma^{-1}\tau(3) = 3$, dacă și numai dacă $\sigma(3) = \tau(3)$. Deci obținem trei clase de echivalență la stânga și anume:

$$C_1^s = \left\{ \begin{bmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{bmatrix} \right\}, \quad C_2^s = \left\{ \begin{bmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{bmatrix}, \begin{bmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{bmatrix} \right\},$$

$$C_3^s = \left\{ \begin{bmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{bmatrix}, \begin{bmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{bmatrix} \right\}.$$

Dacă $\sigma, \tau \in S_3$, atunci $\sigma\tau^{-1} \in H$ dacă și numai dacă $\tau^{-1}(3) = \sigma^{-1}(3)$. Deci clasele de echivalență la dreapta sunt:

$$C_1^d = \left\{ \begin{bmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{bmatrix}, \begin{bmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{bmatrix} \right\}, \quad C_2^d = \left\{ \begin{bmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{bmatrix}, \begin{bmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{bmatrix} \right\},$$

$$C_3^d = \left\{ \begin{bmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{bmatrix}, \begin{bmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{bmatrix} \right\}.$$

Se observă că mulțimile factor $S_3 / R_H^s = \{C_1^s, C_2^s, C_3^s\}$ și $S_3 / R_H^d = \{C_1^d, C_2^d, C_3^d\}$ sunt diferite.

Notatii. Fie G un grup și fie A, B două submulțimi nevide ale sale. Notăm prin

$$AB = \{ab \mid a \in A, b \in B\}.$$

Dacă $A = \{a\}$, respectiv $B = \{b\}$, atunci în loc de AB scriem aB , respectiv Ab , adică $aB = \{ab \mid b \in B\}$, respectiv $Ab = \{ab \mid a \in A\}$.

Exercițiu. Fie G un grup și $H, K \leq G$ două subgrupuri.

(i) Arătați că HK este subgrup dacă și numai dacă $HK = KH$.

(ii) Dați un exemplu din care să rezulte că, în general, HK nu este subgrup.

Lema 3.1. Fie G un grup și H un subgrup al său. Dacă x este un element oarecare al lui G , atunci

$$[x]_s = xH \text{ și } [x]_d = Hx.$$

Demonstrație. Să arătăm doar prima egalitate, a doua demonstrându-se analog. Fie $y \in [x]_s$. Atunci $x R_H^s y$, deci $x^{-1}y \in H$, adică $x^{-1}y = h \in H$, de unde $y = xh \in xH$.

Reciproc, dacă $y \in xH$, atunci $y = xh$ cu $h \in H$, deci $x^{-1}y = h \in H$ sau $x R_H^s y$, adică $y \in [x]_s$.

Observație. Observăm că $[e]_s = eH = H$ și de asemenea $[e]_d = He = H$.

Propoziția 3.2. Dacă G este un grup și H un subgrup al său, atunci funcția

$$\varphi: G/R_H^s \rightarrow G/R_H^d$$

dată prin $\varphi(xH) = Hx^{-1}$ este o funcție bijectivă.

Demonstrație. Să arătăm mai întâi că φ este bine definită, adică nu depinde de alegerea reprezentanților. Într-adevăr, dacă $xH = yH$, adică $x R_H^s y$, atunci $x^{-1}y \in H$ sau $x^{-1}(y^{-1})^{-1} \in H$. Deci $x^{-1} R_H^d y^{-1}$, adică $Hx^{-1} = Hy^{-1}$ sau $\varphi(xH) = \varphi(yH)$, ceea ce înseamnă că φ este bine definită.

Funcția φ este injectivă căci dacă $\varphi(xH) = \varphi(yH)$, atunci $Hx^{-1} = Hy^{-1}$, adică $x^{-1} R_H^s y^{-1}$, deci $x^{-1}(y^{-1})^{-1} \in H$, de unde $x^{-1}y \in H$ sau $x R_H^s y$, deci $xH = yH$.

Faptul că φ este surjectivă este clar, deoarece $\varphi(x^{-1}H) = H(x^{-1})^{-1} = Hx$.

În particular, dacă una dintre mulțimile G/R_H^s sau G/R_H^d este finită, atunci și cealaltă este finită și au același număr de elemente. Se spune în acest caz că *H are indice finit în G* sau că *H este un subgrup de indice finit al lui G* , iar numărul de elemente al mulțimii G/R_H^s sau al mulțimii G/R_H^d , care este același, se numește *indicele lui H în G* și se notează $[G : H]$.

Exercițiu. Fie G un grup și $H, K \leq G$ subgrupuri de indice finit.

(i) Arătați că $[G : H \cap K] \leq [G : H][G : K]$.

(ii) Dacă c.m.m.d.c.([G : H], [G : K]) = 1, atunci $[G : H \cap K] = [G : H][G : K]$.

(iii) Dați un exemplu în care c.m.m.d.c.([G : H], [G : K]) > 1 și $[G : H \cap K] < [G : H][G : K]$.

(iv) Dați un exemplu din care să rezulte că reciproca proprietății (ii) este falsă.

Se spune că un grup G este finit dacă mulțimea pe care este definită structura de grup (adică mulțimea subiacentă) este finită, iar numărul de elemente ale lui G se numește ordinul său și se notează $\text{ord } G$ sau $|G|$.

Este clar că dacă G este de ordin finit, atunci orice subgrup al său este de ordin finit și, mai mult, indicele oricărui subgrup este finit.

Lema 3.3. Fie G un grup și H un subgrup al său. Atunci funcția

$$\psi : H \rightarrow xH,$$

dată de $\psi(h) = xh$, este bijectivă.

Demonstrație. Dacă $\psi(h) = \psi(h')$, atunci $xh = xh'$, de unde prin simplificare, $h = h'$; deci ψ este injectivă.

Funcția ψ este evident surjectivă și deci este bijectivă.

În particular, dacă H este un subgrup finit, atunci toate clasele de echivalență la stânga ale lui G modulo H sunt mulțimi finite și au același număr de elemente ca și H .

Observație. Afirmatia din lema precedentă referitoare la clasele de echivalență la stânga este valabilă și pentru clasele de echivalență la dreapta.

Teorema 3.4. (Lagrange) Dacă G este un grup finit și H un subgrup al său, atunci $\text{ord } G = [G : H] \text{ ord } H$.

Demonstrație. Conform propoziției de mai sus putem să facem demonstrația considerând, de exemplu, numai relația de echivalență R_H^s pe G .

Fie x_1H, \dots, x_kH clasele de echivalență la stânga modulo H ; deci $k = [G : H]$. Atunci

$$G = \bigcup_{i=1}^k x_iH \text{ și } x_iH \cap x_jH = \emptyset \text{ pentru orice } i \neq j,$$

de unde $|G| = \sum_{i=1}^k |x_iH|$. Având în vedere lema precedentă, rezultă că $|G| = k|H|$. Deci

$$\text{ord } G = [G : H] \text{ ord } H.$$

Corolarul 3.5. Dacă G este grup finit și H un subgrup al său, atunci $\text{ord } H \mid \text{ord } G$. În particular, dacă $\text{ord } G$ este un număr prim, atunci G nu are subgrupuri proprii, deci este ciclic.

Observații.

1) Dacă G este un grup finit și $d \mid \text{ord } G$, nu rezultă numai decît că există H un subgrup al lui G cu $\text{ord } H = d$.

2) Dacă G este grup *abelian* finit și $d \mid \text{ord } G$, atunci există $H \leq G$ cu $\text{ord } H = d$.

3) Pentru cazul neabelian există totuși o reciprocă parțială a teoremei lui Lagrange: Fie G un grup finit și p un număr prim cu proprietatea că $p \mid \text{ord } G$. Atunci există $H \leq G$ cu $\text{ord } H = p$. (Teorema lui Cauchy)

§ 4. ORDINUL UNUI ELEMENT

G fiind un grup și $a \in G$ un element oarecare, am numit $\langle a \rangle = \{a^k \mid k \in \mathbb{Z}\}$, *subgrupul ciclic generat de a* .

Reamintim că un grup G se numește *ciclic* dacă există $a \in G$ astfel încât $G = \langle a \rangle$. Elementul a este un *generator* al grupului ciclic G .

Am văzut că grupul aditiv \mathbb{Z} este ciclic, generat de 1 sau -1 . De asemenea, fiecare grup aditiv \mathbb{Z}_n este ciclic, un generator al său fiind, de exemplu, [1].

Definiția 4.1. Spunem că un element a al grupului G este de *ordin finit*, dacă există $i, j \in \mathbb{Z}$, $i \neq j$, astfel încât $a^i = a^j$. În caz contrar, adică dacă toate puterile lui a sunt distincte, spunem că a este element de *ordin infinit*.

Fie G un grup și $a \in G$ un element al său. Să considerăm funcția $\varphi: \mathbb{Z} \rightarrow G$ definită prin $\varphi(n) = a^n$. Avem, evident, $\text{Im } \varphi = \langle a \rangle$. Elementul a este de ordin finit dacă funcția φ nu este injectivă și este de ordin infinit dacă funcția φ este injectivă.

Fie $a \in G$ un element de ordin finit și $i < j$ astfel încât $a^i = a^j$. Atunci $a^{j-i} = e$ și deci există o putere pozitivă a lui a egală cu elementul neutru. Așadar mulțimea

$$M = \{k \in \mathbb{N}^* \mid a^k = e\}$$

este nevidă. Cum M este o submulțime nevidă de numere naturale, iar mulțimea numerelor naturale este bine ordonată, atunci M are un cel mai mic element. Numim *ordinul* elementului a și-l notăm $\text{ord}(a)$, cel mai mic număr întreg pozitiv n astfel încât $a^n = e$.

Deci $\text{ord}(a) = \min\{k \in \mathbb{N}^* \mid a^k = e\}$.

Propoziția 4.2. Fie a un element de ordin finit al unui grup G și n un număr natural nenul. Atunci $n = \text{ord}(a)$ dacă și numai dacă sunt satisfăcute condițiile:

- 1) $a^n = e$,
- 2) dacă $a^k = e$, $k \in \mathbb{Z}$, atunci $n \mid k$.

Demonstrație. Fie $n = \text{ord}(a)$. Din definiția ordinului lui a rezultă 1). Fie acum $k \in \mathbb{Z}$ astfel încât $a^k = e$. Conform teoremei împărțirii cu rest în mulțimea numerelor întregi, există $q, r \in \mathbb{Z}$ astfel încât $k = nq + r$, $0 \leq r < n$; atunci

$$a^r = a^{k-nq} = a^k a^{-nq} = a^k (a^n)^{-q} = ee^{-q} = e.$$

Cum n este cel mai mic număr natural nenul astfel încât $a^n = e$, iar $0 \leq r < n$, rezultă că $r = 0$ și deci n divide k .

Reciproc, dacă n satisface 1) și 2), iar $a^k = e$ cu $k \geq 1$, din 2) rezultă că n divide pe k , deci $n \leq k$. Așadar, n este cel mai mic dintre numerele naturale nenule k astfel încât $a^k = e$, de unde $n = \text{ord}(a)$.

Propoziția 4.3. Fie G un grup. Dacă $a \in G$ este un element de ordin n , atunci subgrupul ciclic generat de a are exact n elemente și anume:

$$\langle a \rangle = \{e, a, a^2, \dots, a^{n-1}\}.$$

Demonstrație. Să demonstrăm mai întâi că $a^i \neq a^j$ oricare ar fi $i \neq j$, $0 \leq i, j \leq n-1$. Într-adevăr, dacă am avea $a^i = a^j$ cu $0 \leq i < j \leq n-1$, atunci $a^{j-i} = e$ și $0 < j-i < n$, contradicție cu faptul că n este cel mai mic număr natural nenul astfel încât $a^n = e$.

Fie acum $n = \text{ord}(a)$ iar k un număr întreg. Din teorema împărțirii cu rest există $q, r \in \mathbb{Z}$ astfel încât $k = nq + r$ cu $0 \leq r < n$. Atunci $a^k = a^{nq+r} = (a^n)^q a^r = a^r$ și deci $a^k \in \{e, a, \dots, a^{n-1}\}$.

Corolarul 4.4. Dacă G este un grup finit, atunci ordinul oricărui element al său divide ordinul lui G .

Demonstrație. Rezultă din teorema lui Lagrange și propoziția precedentă.

Corolarul 4.5. Dacă G este un grup finit cu $\text{ord } G = n$, atunci $a^n = e$ pentru orice $a \in G$.

Demonstrație. Rezultă din corolarul precedent.

Exemple.

1) Fie (\mathbb{C}^*, \cdot) grupul multiplicativ al numerelor complexe nenule. Elementul $i \in \mathbb{C}^*$ are ordinul patru, iar $\langle i \rangle = \{1, -1, i, -i\}$.

2) Numărul complex $z_n = \cos(2\pi/n) + i \sin(2\pi/n)$ este un element de ordin n al grupului (\mathbb{C}^*, \cdot) . Mai mult, $\langle z_n \rangle = \{\cos(2k\pi/n) + i \sin(2k\pi/n) \mid k = 0, 1, \dots, n-1\}$.

3) Elementul $[3]$ din grupul aditiv $(\mathbb{Z}_6, +)$ al claselor de resturi modulo 6 este de ordin 2.

4) Numărul complex nenul $z = a + bi$ cu $a^2 + b^2 \neq 1$ este element de ordin infinit al grupului (\mathbb{C}^*, \cdot) .

Aplicație. Am văzut că dacă se consideră monoidul multiplicativ \mathbb{Z}_n , al claselor de resturi modulo n , $n \geq 1$, atunci mulțimea $U(\mathbb{Z}_n)$ a elementelor inversabile din \mathbb{Z}_n formează un grup multiplicativ. Mai mult, am demonstrat că $[a] \in U(\mathbb{Z}_n)$ dacă și numai dacă $(a, n) = 1$ și deci $|U(\mathbb{Z}_n)| = \varphi(n)$, unde φ este indicatorul lui Euler.

Dacă $a, n \in \mathbb{Z}$, $n \geq 1$ și $(a, n) = 1$, atunci $[a] \in U(\mathbb{Z}_n)$ și deci $\text{ord}(a) \mid \varphi(n)$. Prin urmare, există $m \in \mathbb{N}^*$ astfel încât $\varphi(n) = m \text{ord}([a])$, de unde rezultă că $[a]^{\varphi(n)} = [a]^{m \text{ord}([a])} = ([a]^{\text{ord}([a])})^m = [1]^m = [1]$. Deci $[a]^{\varphi(n)} = [1]$, ceea ce este echivalent cu $a^{\varphi(n)} \equiv 1 \pmod{n}$, adică am obținut o demonstrație pentru *teorema lui Euler*.

Teorema 4.6. (Cauchy) Fie G un grup finit și p un număr prim cu proprietatea că $p \mid \text{ord } G$. Atunci există $a \in G$ cu $\text{ord}(a) = p$.

Demonstrație. Fie $n = \text{ord } G$ și definim $S = \{(a_1, \dots, a_p) \mid a_i \in G \text{ și } a_1 \cdots a_p = e\}$. Avem $|S| = n^{p-1}$ și cum $p \mid n$ rezultă că $|S| \equiv 0 \pmod{p}$. Să mai observăm că o permutare ciclică a unui p -uplu $(a_1, \dots, a_p) \in S$ este tot un element al lui S .

Vom numi două p -upluri din S echivalente dacă unul este permutare ciclică a celuilalt. Astfel, $(a_1, \dots, a_p) \in S$ este echivalent cu exact p p -upluri distincte, excepție făcând cazul în care $a_1 = \dots = a_p$. Clasa de echivalență a unui p -uplu de forma (a, \dots, a) are un singur element. Evident, S conține un astfel de p -uplu, și anume pe (e, \dots, e) . Dacă acesta este singurul p -uplu de forma (a, \dots, a) din S , atunci $|S| \equiv 1 \pmod{p}$, contradicție. Așadar există un element $a \neq e$ cu proprietatea că $(a, \dots, a) \in S$, deci $a^p = e$. Se consideră acum $H = \langle a \rangle$ și demonstrația este încheiată.

Propoziția 4.7. Dacă G este un grup și $x \in G$ este un element de ordin n (finit), atunci $\text{ord}(x^k) = n/(n,k)$, pentru orice $k \in \mathbf{Z}$, $k \neq 0$.

Demonstrație. Fie $d = (n, k)$. Atunci putem scrie $n = dm$, $k = dl$, cu $(m, l) = 1$. Trebuie să arătăm că $\text{ord}(x^k) = m$.

Evident $(x^k)^m = x^{km} = x^{dlm} = x^{nl} = (x^n)^l = e^l = e$, deoarece $\text{ord}(x) = n$.

Fie $r \in \mathbf{Z}$ cu proprietatea că $(x^k)^r = e$. Atunci $x^{kr} = e$, de unde $n \mid kr$, deci $dm \mid dlr \Rightarrow m \mid lr \Rightarrow m \mid r$, deoarece $(m, l) = 1$.

O consecință imediată este faptul că $\text{ord}([k]) = n/(n,k)$ pentru orice $[k] \in \mathbf{Z}_n$.

Exercițiu. Determinați elementele de ordin 30 din \mathbf{Z}_{240} .

Exercițiu. (i) Fie G_1, G_2 două grupuri și $x_1 \in G_1, x_2 \in G_2$ elemente de ordin finit. Arătați că $\text{ord}(x_1, x_2) = [\text{ord}(x_1), \text{ord}(x_2)]$.

(ii) Determinați $\text{ord}([3], [4])$ în grupul $\mathbf{Z}_{24} \times \mathbf{Z}_{36}$.