Curs VI
ELEMENTE DE TEORIA GRUPURILOR

§ 3. RELAŢII DE ECHIVALENŢĂ PE UN GRUP ÎN RAPORT CU UN SUBGRUP AL SĂU

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

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

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

Aceste relaţii binare sunt relaţii de echivalenţă. Să demonstrăm, de exemplu, că prima relaţie binară este relaţie de echivalenţă, adică este reflexivă, simetrică şi tranzitivă.

1) Dacă x $\in$ G, atunci $x^{-1}x = e \in H$ şi deci $x\ R_H^s\ x$ (reflexivitatea).

2) Dacă $x\ R_H^s\ y$, atunci $x^{-1}y \in H$ şi deci $y^{-1}x = (x^{-1}y)^{-1} \in H$, de unde $y\ R_H^s\ x$ (simetria).

3) Dacă $x\ R_H^s\ y$ şi $y\ R_H^s\ z$, atunci $x^{-1}y \in H$ şi $y^{-1}z \in H$. 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 relaţie de echivalenţă.

Relaţiile de echivalenţă R_H^s şi R_H^d se numesc *relaţii de congruenţă la stânga*, respectiv *la dreapta, în raport cu H* (sau *modulo H*). Faptul că „x este în relaţia R_H^s cu y” (respectiv „x este în relaţia R_H^d cu y”) se mai citeşte *x este congruent cu y modulo H la stânga* (respectiv *x este congruent cu y modulo H la dreapta*) şi 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 echivalenţă a elementului x $\in$ G în raport cu R_H^s, respectiv R_H^d, şi o vom numi *clasa de echivalenţă la stânga*, respectiv *clasa de echivalenţă la dreapta a lui x modulo H*.

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

Exemple.

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

2) Dacă G este un grup comutativ, iar H un subgrup oarecare al lui G, atunci relaţiile de congruenţă la stânga şi la dreapta modulo H coincid.

3) Fie $\mathbf{S}_3$ grupul permutărilor de 3 elemente, adică

$$\mathbf{S}_3 = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \right\}$$

şi

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

Este evident că H este un subgrup al lui $\mathbf{S}_3$.

Să construim mulţimile claselor de echivalenţă la stânga şi la dreapta modulo H. Dacă σ, $\tau \in \mathbf{S}_3$, atunci $\sigma^{-1}\tau \in H$ dacă şi numai dacă $\sigma^{-1}\tau(3) = 3$, dacă şi numai dacă $\sigma(3) = \tau(3)$. Deci obţinem trei clase de echivalenţă la stânga şi anume:

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

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

Dacă σ, $\tau \in \mathbf{S}_3$, atunci $\sigma\tau^{-1} \in H$ dacă şi numai dacă $\tau^{-1}(3) = \sigma^{-1}(3)$. Deci clasele de echivalenţă la dreapta sunt:

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

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

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

Notaţii. Fie G un grup şi fie A, B două submulţimi 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 $Ab = \{ab \mid a \in A\}$.

Exerciţiu. Fie G un grup şi H, K ≤ G două subgrupuri.

(i) Arătaţi că HK este subgrup dacă şi numai dacă HK = KH.

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

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

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

Demonstraţie. 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 $y \in [x]_s$.

Observaţie. Observăm că $[e]_s = eH = H$ şi de asemenea $[e]_d = He = H$.

Propoziţia 3.2. Dacă G este un grup şi H un subgrup al său, atunci funcţia

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

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

Demonstraţie. Să arătăm mai întâi că φ este bine definită, adică nu depinde de alegerea reprezentanţilor. 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 φ(xH) = φ(yH), ceea ce înseamnă că φ este bine definită.

Funcţia φ este injectivă căci dacă φ(xH) = φ(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 mulţimile G / R_H^s sau G / R_H^d este finită, atunci şi cealaltă este finită şi au acelaşi 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 mulţimii G / R_H^s sau al mulţimii G / R_H^d, care este acelaşi, se numeşte *indicele lui H în G* şi se notează [G : H].

Exerciţiu. Fie G un grup şi H, K ≤ G subgrupuri de indice finit.

(i) Arătaţi 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) Daţi un exemplu în care c.m.m.d.c.([G : H], [G : K]) > 1 şi $[G : H \cap K] < [G : H][G : K]$.

(iv) Daţi un exemplu din care să rezulte că reciproca proprietăţii (ii) este falsă.

Se spune că un grup G este finit dacă mulţimea pe care este definită structura de grup (adică mulţimea subiacentă) este finită, iar numărul de elemente ale lui G se numeşte *ordinul* său şi se notează ord G sau |G|.

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

Lema 3.3. Fie G un grup şi H un subgrup al său. Atunci funcţia

$$\psi : H \to xH,$$

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

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

Funcţia ψ este evident surjectivă şi deci este bijectivă.

În particular, dacă H este un subgrup finit, atunci toate clasele de echivalenţă la stânga ale lui G modulo H sunt mulţimi finite şi au acelaşi număr de elemente ca şi H.

Observaţie. Afirmaţia din lema precedentă referitoare la clasele de echivalenţă la stânga este valabilă şi pentru clasele de echivalenţă la dreapta.

Teorema 3.4. (Lagrange) Dacă G este un grup finit şi H un subgrup al său, atunci

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

Demonstraţie. Conform propoziţiei de mai sus putem să facem demonstraţia considerând, de exemplu, numai relaţia de echivalenţă R_H^s pe G.

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

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

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 şi H un subgrup al său, atunci ord H | ord G. În particular, dacă ord G este un număr prim, atunci G nu are subgrupuri proprii, deci este ciclic.

Observaţii.

1) Dacă G este un grup finit şi d | ord G, nu rezultă numaidecât că există H un subgrup al lui G cu ord H = d.

2) Dacă G este grup *abelian* finit şi d | ord G, atunci există $H \leq G$ cu ord H = d.

3) Pentru cazul neabelian există totuşi o reciprocă parţială a teoremei lui Lagrange: Fie G un grup finit şi p un număr prim cu proprietatea că p | ord G. Atunci există $H \leq G$ cu ord H = p. (Teorema lui Cauchy)

§ 4. ORDINUL UNUI ELEMENT

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

Reamintim că un grup G se numeşte *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 **Z** este ciclic, generat de 1 sau –1. De asemenea, fiecare grup aditiv $\mathbf{Z}_n$ este ciclic, un generator al său fiind, de exemplu, [1].

Definiţia 4.1. Spunem că un element *a* al grupului G este de *ordin finit*, dacă există $i, j \in \mathbf{Z}$, $i \neq j$, 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 şi $a \in G$ un element al său. Să considerăm funcţia $\varphi: \mathbf{Z} \to G$ definită prin $\varphi(n) = a^n$. Avem, evident, $\text{Im}\,\varphi = \langle a \rangle$. Elementul *a* este de ordin finit dacă funcţia φ nu este injectivă şi este de ordin infinit dacă funcţia φ este injectivă.

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

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

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

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

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

1) $a^n = e$,

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

Demonstraţie. Fie $n = \text{ord}(a)$. Din definiţia ordinului lui *a* rezultă 1). Fie acum $k \in \mathbf{Z}$ astfel încât $a^k = e$. Conform teoremei împărţirii cu rest în mulţimea numerelor întregi, există $q, r \in \mathbf{Z}$ 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 $r = 0$ şi deci n divide k.

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

Propoziţia 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 şi anume:

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

Demonstraţie. 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 $a^{j-i} = e$ şi $0 < j - i < n$, contradicţie cu faptul că n este cel mai mic număr natural nenul astfel încât $a^n = e$.

Fie acum n = ord(a) iar k un număr întreg. Din teorema împărţirii cu rest există q, $r \in \mathbf{Z}$ astfel încât $k = nq + r$ cu $0 \le r \le n - 1$. Atunci $a^k = a^{nq + r} = (a^n)^q a^r = a^r$ şi 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.

Demonstraţie. Rezultă din teorema lui Lagrange şi propoziţia precedentă.

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

Demonstraţie. Rezultă din corolarul precedent.

Exemple.

1) Fie $(\mathbf{C}^*, \bullet)$ grupul multiplicativ al numerelor complexe nenule. Elementul $i \in \mathbf{C}^*$ 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 $(\mathbf{C}^*, \bullet)$. 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 $(\mathbf{Z}_6, +)$ al claselor de resturi modulo 6 este de ordin 2.

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

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

Dacă $a, n \in \mathbf{Z}$, $n \ge 1$ şi $(a, n) = 1$, atunci $[a] \in U(\mathbf{Z}_n)$ şi deci ord(a) | φ(n). Prin urmare, există $m \in \mathbf{N}^*$ astfel încât $\varphi(n) = m \cdot \text{ord}([a])$, de unde rezultă că $[a^{\varphi(n)}] = [a]^{\varphi(n)} = ([a]^{\text{ord}([a])})^m = [1]^m = [1]$. Deci $[a]^{\varphi(n)} = [1]$, ceea ce este echivalent cu $a^{\varphi(n)} \equiv 1 \pmod n$, adică am obţinut o demonstraţie pentru *teorema lui Euler*.

Teorema 4.6. (Cauchy) Fie G un grup finit şi p un număr prim cu proprietatea că p | ord G. Atunci există $a \in G$ cu ord(a) = p.

Demonstraţie. Fie n = ord G şi definim $S = \{(a_1, \dots, a_p) \mid a_i \in G \text{ şi } a_1 \cdots a_p = e\}$. Avem $|S| = n^{p-1}$ şi cum p | 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, excepţie facând cazul în care $a_1 = \dots = a_p$. Clasa de echivalenţă a unui p-uplu de forma (a, ... , a) are un singur element. Evident, S conţine un astfel de p-uplu, şi anume pe (e, ... , e). Dacă acesta este singurul p-uplu de forma (a, ... , a) din S, atunci $|S| \equiv 1 \pmod p$, contradicţie. Aşadar există un element $a \ne e$ cu proprietatea că $(a, \dots, a) \in S$, deci $a^p = e$. Se consideră acum $H = \langle a \rangle$ şi demonstraţia este încheiată.

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

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

Evident $(x^k)^m = x^{km} = x^{dlm} = x^{nl} = (x^n)^l = e^l = e$, deoarece 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 consecinţă imediată este faptul că $ord([k]) = n/(n,k)$ pentru orice $[k] \in \mathbf{Z}_n$.

Exerciţiu. Determinaţi elementele de ordin 30 din $\mathbf{Z}_{240}$.

Exerciţiu. (i) Fie G_1, G_2 două grupuri şi $x_1 \in G_1$, $x_2 \in G_2$ elemente de ordin finit. Arătaţi că ord $(x_1, x_2) = [ord(x_1), ord(x_2)]$.

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