CURS V
ELEMENTE DE TEORIA GRUPURILOR

§ 2. SUBGRUPURI

Subgrupuri

Fie G un grup în notaţie multiplicativă ($G \times G \to G$, $(x, y) \to xy$) şi H o submulţime nevidă a sa. Dacă oricare ar fi $x, y \in H$, avem $xy \in H$ (produsul efectuat conform operaţiei algebrice din G), atunci se obţine o funcţie $H \times H \to H$, $(x, y) \to xy$, adică o operaţie algebrică pe H numită *operaţia indusă* pe H de operaţia din G. În acest caz se mai spune că operaţia din G induce o operaţie pe H.

Definiţia 2.1. Se spune că o submulţime nevidă H a grupului G este *subgrup* al lui G, dacă operaţia algebrică din G induce pe H o operaţie algebrică faţă de care H este grup.

Notaţie. $H \leq G$

Propoziţia 2.2. Fie G un grup şi H o submulţime nevidă a sa. Atunci următoarele afirmaţii sunt echivalente:

1) H este subgrup al lui G;

2) i) Oricare ar fi $x, y \in H$, produsul xy (efectuat în G) este un element din H;

ii) $e \in H$ (e fiind elementul neutru al lui G);

iii) Oricare ar fi $x \in H$, x^{-1} (inversul lui x în G) aparţine lui H;

3) Oricare ar fi $x, y \in H$, produsul xy^{-1} (efectuat în G) aparţine lui H.

Demonstraţie. 1) $\Rightarrow$ 2) Afirmaţia i) rezultă din faptul că operaţia din G induce pe H o operaţie algebrică. H fiind subgrup are un element neutru notat e'. Cum e este elementul neutru al lui G, avem în G relaţia

$$ee' = e' = e'e'.$$

Simplificând la dreapta relaţia $ee' = e'e'$ (adică o înmulţim la dreapta cu $(e')^{-1}$) obţinem $e = e'$.

Fie $x \in H$, x^{-1} inversul în G al lui x, iar x' inversul în H al lui x. Atunci, conform celor de mai înainte, avem în G

$$xx^{-1} = xx' = e.$$

Simplificând la stânga această relaţie, obţinem $x' = x^{-1}$, deci $x^{-1} \in H$.

2) $\Rightarrow$ 3) Dacă $x, y \in H$, conform cu iii), rezultă $y^{-1} \in H$ şi din i), $xy^{-1} \in H$.

3) $\Rightarrow$ 2) Dacă $x \in H$, atunci $xx^{-1} = e \in H$ şi $x^{-1} = ex^{-1} \in H$. De asemenea, dacă $y \in H$, cum $y^{-1} \in H$, se obţine

$$xy = x(y^{-1})^{-1} \in H.$$

2) $\Rightarrow$ 1) Asociativitatea operaţiei de pe H rezultă din faptul că operaţia lui G este asociativă. Restul este imediat.

Observaţie. Dacă G este un grup abelian, orice subgrup al său este abelian.

Exemple.

1) Dacă G este un grup, atunci G însuşi este un subgrup al lui G, numit *subgrupul total* al lui G. De asemenea submulţimea {e} a lui G este subgrup numit *subgrupul trivial* al lui G. Subgrupul total şi subgrupul trivial al unui grup G se numesc *subgrupuri improprii* ale lui G. Orice subgrup diferit de acestea se numeşte *subgrup propriu*.

2) Grupul aditiv **Z** al numerelor întregi este subgrup al grupului aditiv **Q** al numerelor raţionale; grupul aditiv **Q** este subgrup al grupului aditiv **R** al numerelor reale; grupul aditiv **R** este subgrup al grupului aditiv **C** al numerelor complexe.

De asemenea, grupul multiplicativ **Q*** este subgrup al grupului multiplicativ **R*** iar ambele sunt subgrupuri ale grupului multiplicativ **C***.

3) Grupul multiplicativ {–1, 1} este subgrup al grupului multiplicativ **Q***, iar grupul multiplicativ {–1, 1, – i, i} este subgrup al grupului multiplicativ **C***. Mai general, U_n este subgrup al grupului multiplicativ **C***. (De fapt, orice subgrup finit al lui **C*** este egal cu un U_n.)

4) Fie M o mulţime, $N \subset M$ o submulţime proprie a lui M, iar S(M) grupul permutărilor mulţimii M. Mulţimea $H = \{f \in S(M) \mid f(x) = x$ oricare ar fi $x \in M \setminus N\}$ este un subgrup al lui S(M).

5) Mulţimea automorfismelor interioare Int(G) ale unui grup G este subgrup al grupului automorfismelor Aut(G).

6) Fie **Z** grupul aditiv al numerelor întregi, iar $n \in \mathbf{Z}$ un număr întreg oarecare. Submulţimea $n\mathbf{Z} = \{nk \mid k \in \mathbf{Z}\}$ a lui **Z** este un subgrup al lui **Z.** Într-adevăr, dacă $x, y \in \mathbf{Z}$, $x = nh$ şi $y = nk$ cu $h, k \in \mathbf{Z}$, atunci

$$x - y = n(h - k) \in n\mathbf{Z}$$

şi conform punctului 3) al propoziţiei precedente rezultă că $n\mathbf{Z}$ este subgrup al lui **Z**. Observăm că $n\mathbf{Z} = (-n)\mathbf{Z}$. Mai mult, propoziţia următoare ne arată că orice subgrup al lui **Z** este de acest tip.

Propoziţia 2.3. Dacă H este un subgrup oarecare al grupului aditiv **Z**, atunci există $n \in \mathbf{Z}$, $n \geq 0$, astfel încât $H = n\mathbf{Z}$.

Demonstraţie. Fie $H \subseteq \mathbf{Z}$ un subgrup oarecare al grupului aditiv **Z**.

Dacă $H = \{0\}$, adică H este subgrupul nul, atunci $H = 0\mathbf{Z}$.

Dacă $H \neq \{0\}$, atunci există $x \in H$, $x \neq 0$. Datorită punctului 2) al propoziţiei precedente, $-x \in H$. Rezultă că H conţine numere întregi pozitive. Fie n cel mai mic număr întreg pozitiv din H. Avem că $0 \in H$, $n \in H$, $2n = n + n \in H$ şi, în general, $kn \in H$ oricare ar fi k număr natural, după cum rezultă din punctul 1) al propoziţiei precedente. De asemenea, din punctul 2) al aceleiaşi propoziţii, $kn \in H$ oricare ar fi k întreg negativ, deci $n\mathbf{Z} \subseteq H$.

Fie acum $x \in H$ un element oarecare. Conform teoremei împărţirii cu rest pentru numere întregi putem scrie $x = nq + r$, unde $0 \leq r < n$. Deoarece x şi nq sunt din H, rezultă că $r = x - nq$ aparţine lui H. Cum $0 \leq r < n$, iar n este cel mai mic număr natural nenul din H, rezultă că $r = 0$, deci $x = nq \in n\mathbf{Z}$.

Aşadar $H \subseteq n\mathbf{Z}$, de unde $H = n\mathbf{Z}$.

Exerciţiu. Determinaţi subgrupurile grupului lui Klein $\mathbf{Z}_2 \times \mathbf{Z}_2$.

Nucleul şi imaginea unui morfism de grupuri

Fie G şi G' două grupuri, iar $f : G \to G'$ un morfism de grupuri. Fie $H \leq G$ şi $H' \leq G'$ subgrupuri. Să considerăm

$$f(H) = \{x' \in G' \mid \text{există } x \in H \text{ astfel încât } x' = f(x)\},$$

imaginea (directă a) lui H prin f şi

$$f^{-1}(H') = \{x \in G \mid f(x) \in H'\},$$

imaginea reciprocă a lui H' prin f.

Se notează $\text{Ker } f = f^{-1}(\{e'\})$ şi se numeşte *nucleul* morfismului f. De asemenea, $\text{Im } f = f(G)$ şi se numeşte *imaginea* morfismului f. Deci

$$\text{Ker } f = \{x \in G \mid f(x) = e'\} \text{ şi}$$

$$\text{Im } f = \{x' \in G' \mid \text{există } x \in G \text{ astfel încât } x' = f(x)\} = \{f(x) \mid x \in G\}.$$

Propoziţia 2.4. Fie $f : G \to G'$ un morfism de grupuri. Avem:

1) Dacă H este subgrup al lui G, atunci f(H) este subgrup al lui G'. (În particular, Im f este un subgrup al lui G');

2) Dacă H' este subgrup al lui G', atunci $f^{-1}(H')$ este subgrup al lui G. (În particular, Ker f este un subgrup al lui G).

Demonstraţie. 1) Cum $H \neq \emptyset$ este evident că $f(H) \neq \emptyset$. Dacă $x', y' \in f(H)$, atunci există $x, y \in H$ astfel încât $x' = f(x)$, $y' = f(y)$. Avem

$$x'y'^{-1} = f(x)(f(y))^{-1} = f(x)f(y^{-1}) = f(xy^{-1})$$

şi cum H este subgrup rezultă că $xy^{-1} \in H$ şi deci $x'^{-1}y'^{-1} = f(xy^{-1}) \in f(H)$.

2) Cum $e' \in H'$, iar $f(e) = e'$, rezultă că $e \in f^{-1}(H')$, adică $f^{-1}(H') \neq \emptyset$. Dacă $x, y \in f^{-1}(H')$, atunci $f(x), f(y) \in H'$; cum H' este subgrup

$$f(xy^{-1}) = f(x)f(y)^{-1} = f(x)f(y^{-1}) \in H',$$

adică $xy^{-1} \in f(H')$.

Propoziţia 2.5. Un morfism de grupuri $f : G \to G'$ este injectiv dacă şi numai dacă nucleul său este trivial, adică $\text{Ker } f = \{e\}$.

Demonstraţie. Să presupunem că f este morfism injectiv. Avem $f(e) = e'$ şi dacă $x \in \text{Ker } f$, atunci $f(x) = e'$, adică $f(x) = f(e)$. Cum funcţia f este injectivă, rezultă $x = e$.

Reciproc, fie $f(x) = f(y)$. Atunci $f(x)(f(y))^{-1} = e'$, adică $f(x)f(y^{-1}) = e'$ sau $f(xy^{-1}) = e'$ şi deci $xy^{-1} = e$, de unde $x = y$. Rezultă că f este injectivă.

Observaţie. În mod evident avem că un morfism de grupuri $f : G \to G'$ este surjectiv dacă şi numai dacă $\text{Im } f = G'$.

Teorema 2.6. (Teorema de corespondenţă pentru subgrupuri) Fie $f : G \to G'$ un morfism *surjectiv* de grupuri. Există o corespondenţă bijectivă între mulţimea subgrupurilor lui G care conţin Ker f şi mulţimea tuturor subgrupurilor lui G', dată prin $H \to f(H)$.

Demonstraţie. Mai întâi observăm că dacă H este un subgrup al lui G care conţine Ker f, atunci $f^{-1}(f(H)) = H$. Într-adevăr, $H \subseteq f^{-1}(f(H))$ iar dacă $x \in f^{-1}(f(H))$, atunci $f(x) \in f(H)$, deci există $h \in H$ astfel încât $f(x) = f(h)$. De aici rezultă că $f(xh^{-1}) = e'$, ceea ce înseamnă că $xh^{-1} \in \text{Ker } f$. Cum însă $\text{Ker } f \subseteq H$ obţinem $xh^{-1} \in H$, deci $x \in H$.

Acum rezultă imediat că aplicaţia dată este injectivă: dacă H şi K sunt subgrupuri ale lui G care conţin Ker f şi $f(H) = f(K)$, atunci $f^{-1}(f(H)) = f^{-1}(f(K))$, deci $H = K$.

Pentru a demonstra că aplicaţia este surjectivă considerăm H' un subgrup al lui G' şi fie $H = f^{-1}(H')$. Evident $H \supseteq \text{Ker } f$ şi deoarece f este funcţie surjectivă avem că $f(H) = H'$.

Subgrupul generat de o submulţime a unui grup

Observăm mai întâi că dacă $(H_i)_{i \in I}$ este o familie de subgrupuri ale unui grup G, atunci $\bigcap_{i \in I} H_i$ este un subgrup al lui G. Într-adevăr, fie $x, y \in \bigcap_{i \in I} H_i$. Atunci $x, y \in H_i$, oricare ar fi $i \in I$, şi cum fiecare H_i este un subgrup rezultă că $xy^{-1} \in H_i$, oricare ar fi $i \in I$. Deci $xy^{-1} \in \bigcap_{i \in I} H_i$.

Definiţia 2.7. Fie G un grup şi X o submulţime a lui G. Intersecţia tuturor subgrupurilor care conţin mulţimea X (această intersecţie fiind un subgrup, conform celor precedente) se numeşte *subgrupul generat* de X în G. Vom nota acest subgrup cu $\langle X \rangle$. Deci

$$\langle X \rangle = \bigcap_{\substack{X \subseteq K \\ K \subseteq G \text{ subgrup}}} K$$

Dacă $H = \langle X \rangle$, adică H este subgrupul generat de X, se spune că X este un *sistem de generatori* pentru H sau că X *generează* pe H.

Observaţii.

1) $\langle X \rangle$ este cel mai mic subgrup al lui G care conţine pe X.

2) Dacă $X = \emptyset$, atunci subgrupul generat de X este subgrupul trivial $\{e\}$.

3) Dacă X este un subgrup al lui G, atunci printre subgrupurile lui G care conţin pe X se găseşte X însuşi şi deci subgrupul generat de X este chiar X. Cum subgrupul generat de un subgrup este subgrupul însuşi, rezultă că orice subgrup al unui grup G are cel puţin un sistem de generatori.

Un subgrup H al lui G care admite un sistem finit de generatori se spune că este un subgrup *finit generat*. Un subgrup H al lui G care admite un sistem de generatori format dintr-un singur element se spune că este un subgrup *ciclic*. În acest caz vom scrie $H = \langle a \rangle$, unde $a \in H$.

Următoarea teoremă ne dă forma elementelor subgrupului generat de o submulţime nevidă X în G.

Teorema 2.8. Fie $X \neq \emptyset$ o submulţime a lui G. Atunci $\langle X \rangle$, subgrupul generat de X în G, este format din mulţimea elementelor lui G care se pot scrie sub forma

$$x_1^{\varepsilon_1} x_2^{\varepsilon_2} \ldots x_k^{\varepsilon_k}, \text{ unde } k \geq 0, \varepsilon_i = \pm 1, x_i \in X, 1 \leq i \leq k.$$

Demonstraţie. Fie

$$H' = \{x \in G \mid x = x_1^{\varepsilon_1} x_2^{\varepsilon_2} \ldots x_k^{\varepsilon_k}, \text{ unde } k \geq 0, \varepsilon_i = \pm 1, x_i \in X, 1 \leq i \leq k\}.$$

Arătăm că H' este subgrup al lui G care conţine pe X. Într-adevăr, oricare ar fi $x \in X$, $x = x^1 \in H'$. Deci $X \subseteq H'$, de unde $H' \neq \emptyset$. Dacă $x, y \in H'$, atunci $x = x_1^{\varepsilon_1} x_2^{\varepsilon_2} \ldots x_k^{\varepsilon_k}$, $y = y_1^{\mu_1} y_2^{\mu_2} \ldots y_s^{\mu_s}$, $\varepsilon_i = \pm 1$, $\mu_j = \pm 1$, $x_i, y_j \in X$, $1 \leq i \leq k$, $1 \leq j \leq s$, şi deci $xy^{-1} = x_1^{\varepsilon_1} x_2^{\varepsilon_2} \ldots x_k^{\varepsilon_k} y_s^{-\mu_s} \ldots y_2^{-\mu_2} y_1^{-\mu_1} \in H'$.

Cum H' este un subgrup care conţine pe X, rezultă că H' include intersecţia tuturor subgrupurilor lui G care conţin pe X, adică $\langle X \rangle \subseteq H'$.

Reciproc, fie H este un subgrup al lui G care conţine pe X. Dacă $x_1, x_2, \ldots, x_k \in X \subseteq H$, rezultă că $x_1^{\varepsilon_1}, x_2^{\varepsilon_2}, \ldots, x_k^{\varepsilon_k} \in H$ şi H fiind subgrup avem că $x_1^{\varepsilon_1} x_2^{\varepsilon_2} \ldots x_k^{\varepsilon_k} \in H$. Deci H conţine pe H'. Cum H este un subgrup arbitrar care conţine pe X, rezultă că H' este conţinut în intersecţia tuturor acestor subgrupuri, adică în $\langle X \rangle$.

Observaţii. În cazul în care grupul G este comutativ avem că

$$\langle X \rangle = \{x \in G \mid x = x_1^{n_1} x_2^{n_2} \ldots x_k^{n_k}, \text{ unde } k \geq 0, n_i \in \mathbf{Z}, x_i \in X, 1 \leq i \leq k\}.$$

Dacă folosim scrierea aditivă, atunci

$$\langle X \rangle = \{x \in G \mid x = n_1x_1 + n_2x_2 + \cdots + n_kx_k, \text{ unde } k \geq 0, n_i \in \mathbf{Z}, x_i \in X, 1 \leq i \leq k\}.$$

Dacă H este subgrup ciclic generat de elementul *a*, atunci din teorema precedentă rezultă că

$$H = \langle a \rangle = \{a^n \mid n \in \mathbf{Z}\}.$$

În scriere aditivă avem

$$H = \langle a \rangle = \{na \mid n \in \mathbf{Z}\}.$$

Elementul *a* se numeşte *generator* al subgrupului ciclic H.

Exemple.

1) Grupul aditiv $(\mathbf{Z}, +)$ al numerelor întregi este ciclic generat de 1 sau de –1, adică $(\mathbf{Z}, +) = \langle 1 \rangle = \langle -1 \rangle$, iar în acest caz aceştia sunt singurii generatori posibili.

2) Dacă $m, n \in \mathbf{Z}$, atunci

(i) $m\mathbf{Z} \cap n\mathbf{Z} = [m, n]\mathbf{Z}$,

(ii) $\langle m, n \rangle = (m, n)\mathbf{Z}$,

unde $[m, n]$ = c.m.m.m.c.(m, n) şi (m, n) = c.m.m.d.c.(m, n).

Să demonstrăm (i). Dacă $x \in m\mathbf{Z} \cap n\mathbf{Z}$, adică $x \in m\mathbf{Z}$ şi $x \in n\mathbf{Z}$, atunci $m \mid x$ şi

n | x. Deci [m, n] | x, adică $x \in [m, n]\mathbf{Z}$. Reciproc, dacă $x \in [m, n]\mathbf{Z}$, atunci [m, n] | x şi deci m | x şi n | x, adică $x \in m\mathbf{Z}$ şi $x \in n\mathbf{Z}$, de unde $x \in m\mathbf{Z} \cap n\mathbf{Z}$.

Să demonstrăm (ii). Din teorema precedentă, în scriere aditivă, rezultă $<m, n> = \{x \in \mathbf{Z} \mid x = mk + nl, \text{ unde } k, l \in \mathbf{Z}\}$. Dacă $x \in <m,n>$, atunci $x = mk + nl$ cu $k, l \in \mathbf{Z}$ şi cum (m, n) | m şi (m, n) | n rezultă că (m, n) | mk + nl, adică (m, n) | x, de unde $x \in (m, n)\mathbf{Z}$. Cum $<m, n>$ este subgrup al lui **Z**, rezultă că există $d \in \mathbf{Z}$ astfel încât $<m, n> = d\mathbf{Z}$. Dar $m, n \in <m, n>$, adică $m, n \in d\mathbf{Z}$ şi deci d | m şi d | n. Fie acum $x \in (m, n)\mathbf{Z}$, adică (m, n) | x. Cum d este un divizor comun al numerelor m şi n, rezultă d | (m, n) şi deci d | x, adică $x \in d\mathbf{Z} = <m, n>$.

Observăm că din (i) rezultă că orice două numere întregi au un c.m.m.m.c. Din (ii) rezultă că orice două numere întregi m şi n au un c.m.m.d.c. şi, mai mult, există $k, l \in \mathbf{Z}$ astfel încât (m, n) = mk + nl.

3) Grupul aditiv $(\mathbf{Z}_n, +)$ al claselor de resturi modulo n este ciclic, generat de exemplu de [1], adică

$$(\mathbf{Z}_n, +) = < [1] >.$$

Să arătăm că $[a] \in \mathbf{Z}_n$ este generator al grupului $(\mathbf{Z}_n, +)$ dacă şi numai dacă a şi n sunt prime între ele, adică (a, n) = 1.

Într-adevăr, dacă a este generator al lui $\mathbf{Z}_n$, adică $\mathbf{Z}_n = <[a]>$, atunci există $b \in \mathbf{Z}$, astfel încât [1] = b[a] sau [1] = [ba] deci n | 1 – ba, adică există $k \in \mathbf{Z}$ astfel încât 1 – ba = kn sau ab + nk = 1, ceea ce arată că (a, n) = 1.

Reciproc, dacă (a, n) = 1, atunci rezultă că $[a] \in U(\mathbf{Z}_n)$ şi deci există $[b] \in \mathbf{Z}_n$ cu [a][b] = 1. Atunci, dacă $[x] \in \mathbf{Z}_n$, [x] = [x • 1] = [x][1] = [x][a][b] = [xb][a] = (xb)[a]. Cum $xb \in \mathbf{Z}$ avem $[x] \in <[a]>$. Aşadar $\mathbf{Z}_n = <[a]>$.

Exerciţiu. Să se arate că grupul $(\mathbf{Z} \times \mathbf{Z}, +)$ este finit generat, dar nu este ciclic.

Exerciţiu. (i) Să se arate că subgrupul lui $(\mathbf{Q}, +)$ generat de 1/2 şi 1/3 este ciclic şi să se determine un generator al acestuia.

(ii) Mai general, să se arate că orice subgrup finit generat al lui $(\mathbf{Q}, +)$ este ciclic.

(iii) Să se arate că grupul $(\mathbf{Q}, +)$ nu este finit generat.