CURS 4

Subgrupuri

20.03.2018

Def: Fie $(G,\cdot)$ un grup. Spunem că o submulțime $H \subseteq G$ este un subgrup a lui G dacă $\circ H$ este stabilă față de înmulțire (adică, $\forall x,y \in H,\ x\cdot y \in H$)
și $\circ H$ împreună cu restricția operației „$\cdot$" la H formează un grup.

Teoremă (de caracterizare a subgrupurilor)
Fie $(G,\cdot)$ grup și $H \subseteq G$. Următoarele afirmații sunt echivalente:
a) H este subgrup în G
b) i) $1 \in H$
ii) $\forall x,y \in H,\ x\cdot y \in H$
iii) $\forall x \in H,\ x^{-1} \in H$
c) i) $1 \in H$
ii) $\forall x,y \in H,\ x\cdot y^{-1} \in H$

Dem:
a) $\Rightarrow$ b)
H - subgrup în $G \Rightarrow$ ii) este adevărată (din definiție)
$\Rightarrow (H,\cdot)$ grup $\Rightarrow \exists e \in H$ element neutru în $(H,\cdot)$
$\Rightarrow e\cdot e = e$
„$\cdot$" operație din G $\Rightarrow e = 1 \Rightarrow 1 \in H \Rightarrow$ i) este adevărată
iii) Fie $x \in H$, $(H,\cdot)$ grup $\Rightarrow \exists x' \in H$ simetricul lui x față de „$\cdot$"
$\Rightarrow x\cdot x' = e = 1 \Rightarrow x' = x^{-1} \in H$

b) $\Rightarrow$ c)
i) evidentă
ii) Fie $x,y \in H \xrightarrow[b)]{iii)} x, y^{-1} \in H \xrightarrow[b)]{ii)} x\cdot y^{-1} \in H \Rightarrow$ c(ii) este adevărată

c) $\Rightarrow$ b)
Fie $x \in H$, $1 \in H$ $\xrightarrow{ii}$ $1\cdot x^{-1} \in H \Rightarrow \forall x \in H,\ x^{-1} \in H \Rightarrow$ b(iii) adevărată
Fie $x,y \in H \Rightarrow x, y^{-1} \in H \xrightarrow{c(ii)} x(y^{-1})^{-1} \in H \Rightarrow x\cdot y \in H \Rightarrow$ b(ii) adevărată
b(i) evident

b) $\Rightarrow$ a) b(ii) $\Rightarrow$ H este parte stabilă!
Fie $x,y,z \in H$, $H \subseteq G$ $\Rightarrow x,y,z \in G \Rightarrow (xy)z = x(yz) \Rightarrow$ „$\cdot$" este asociativă pe H
$1 \in H \Rightarrow H$ are element neutru
$\forall x \in H,\ x^{-1} \in H \Rightarrow$ toate elementele lui H sunt simetrizabile
$\Rightarrow (H,\cdot)$ grup $\Rightarrow H$ subgrup în G

Notație $H \leq G$ - H subgrup în G
Exemple
1) $(G,\cdot)$ grup $\Rightarrow \{1\}, G \leq G$ (numite subgrupuri triviale)
2) Față de „$+$":
$\mathbb{Z} \leq \mathbb{Q} \leq \mathbb{R} \leq \mathbb{C}$
3) $\mathbb{Q}^* \leq \mathbb{R}^* \leq \mathbb{C}^*$ (față de înmulțire)
4) $\mathbb{N}$ parte stabilă în $(\mathbb{Z},+)$, dar nu este subgrup
(b iii) nu este îndeplinită)
5) $n \in \mathbb{Z} \Rightarrow n\mathbb{Z} = \{nk \mid k \in \mathbb{Z}\} \leq (\mathbb{Z},+)$
6) $2\mathbb{Z}+1 = \{2k+1 \mid k \in \mathbb{Z}\}$ nu este subgrup (nu e parte stabilă)
7) $D_4 = \{1, r, r^2, r^3, s, sr, sr^2, sr^3\}$

Obs Relația de a fi subgrup este tranzitivă

$H \leq K$ și $K \leq G \Rightarrow H \leq G$

Propoziție

Fie $f: G \to K$ un morfism de grupuri. Atunci:

a) $\forall H \leq G$, $f(H) = \{f(h) \mid h \in H\} \leq K$

b) $\forall L \leq K$, $f^{-1}(L) = \{g \in G \mid f(g) \in L\} \leq G$

Dem:

a) Fie $H \leq G$. Dem. că $f(H) \leq K$

$H \leq G \Rightarrow 1_G \in H \Rightarrow f(1_G) \in f(H)$, $f(1_G) = 1_K$ $\Rightarrow 1_K \in f(H) \Rightarrow$ a(i) e verificată

a(ii) Fie $x_1, x_2 \in f(H) \Rightarrow \exists h_1, h_2 \in H$ a.î. $f(h_1) = x_1$, $f(h_2) = x_2$

$\Rightarrow x_1 \cdot x_2^{-1} = f(h_1)[f(h_2)]^{-1} = f(h_1) \cdot f(h_2^{-1}) = f(h_1 \cdot h_2^{-1})$

$h_1, h_2 \in H$, $H \leq G \Rightarrow h_1 \cdot h_2^{-1} \in H$

$\Rightarrow x_1 \cdot x_2^{-1} = f(h_1 \cdot h_2^{-1}) \in f(H)$

$\Downarrow$ a(ii) e verificată

$\Rightarrow f(H) \leq K$

b) $f(1_G) = 1_K$, $L \leq K \Rightarrow 1_K \in L$ $\Rightarrow f(1_G) \in L \Rightarrow 1_G \in f^{-1}(L)$

Fie $g_1, g_2 \in f^{-1}(L) \Rightarrow f(g_1), f(g_2) \in L \leq K \Rightarrow f(g_1) \cdot [f(g_2)]^{-1} \in L$

$\Rightarrow f(g_1 \cdot g_2^{-1}) \in L \Rightarrow g_1 \cdot g_2^{-1} \in f^{-1}(L)$

$\Rightarrow \forall g_1, g_2 \in f^{-1}(L)$, $g_1 \cdot g_2^{-1} \in f^{-1}(L)$

$\Rightarrow f^{-1}(L) \leq G$

Corolar

Dacă $f: G \to K$ este un morfism de grupuri, atunci:

$\ker f = \{g \in G \mid f(g) = 1_K\}$ este un subgrup al lui G.

Dem:

$\ker f = f^{-1}(\{1_K\})$, $\{1_K\} \leq K$ $\Rightarrow \ker f \leq G$

Def: Subgrupul $\ker f$ s.n. NUCLEUL LUI f

Propoziție

Fie $f: G \to K$ un morfism de grupuri. Următoarele afirmații sunt echivalente.

a) f injectivă

b) $\ker f = \{1_G\}$

Dem:

a) $\Rightarrow$ b) $f(1_G) = 1_K \Rightarrow 1_G \in \ker f \Rightarrow \{1_G\} \leq \ker f$

Fie $x \in \ker f \Rightarrow f(x) = 1_K = f(1_G)$, f injectivă $\Rightarrow x = 1_G$

$\Rightarrow \forall x \in \ker f$, $x = 1_G$

$\Rightarrow \ker f = \{1_G\}$

b) $\Rightarrow$ a)

Fie $x, y \in G$ a.î. $f(x) = f(y) \mid \cdot f(y)^{-1} \Rightarrow f(x) \cdot f(y)^{-1} = 1_K \Rightarrow f(x \cdot y^{-1}) = 1_K \Rightarrow x \cdot y^{-1} \in \ker f = \{1_G\}$

$\Rightarrow x \cdot y^{-1} = 1_G \Rightarrow x = y$

Def Un morfism $f: G \to K$ s.n. SCUFUNDABIL dacă f este injectiv.

Spunem că grupul G se scufundă în grupul K dacă $\exists$ o scufundare $f: G \to K$

Obs Dacă $f: G \to K$ este un morfism injectiv, atunci $f: G \to f(G)$ este un izomorfism.

Deci, G se scufundă în $K \iff G$ este izomorf cu un subgrup al lui K.

Exemplu:

Teorema lui Cayley: $\forall$ G grup, $\exists$ $\varphi: G \to S_G$ morfism de grupuri injectiv (vezi curs anterior)

$\Rightarrow$ Orice grup este izomorf cu un subgrup al unui grup de permutări

Teoremă

Dacă $(G, \cdot)$ grup și $(H_i)_{i \in I}$ este o familie de subgrupuri ale lui G, atunci:

$$\bigcap_{i \in I} H_i \leq G$$

Dem:

Verificăm condiția a) din T. de caracterizare

$\forall i \in I, H_i \leq G \Rightarrow \forall i \in I, 1 \in H_i \Rightarrow 1 \in \bigcap_{i \in I} H_i \Rightarrow$ c'il e verificată

Fie $x, y \in \bigcap_{i \in I} H_i \Rightarrow \forall i \in I, x, y \in H_i$ $\Rightarrow \forall i \in I, H_i \leq G$ $\Big\} \xrightarrow{c(ii)} \forall i \in I, x \cdot y^{-1} \in H_i \Rightarrow xy^{-1} \in \bigcap_{i \in I} H_i \Rightarrow$

$\Rightarrow c(ii)$ e adevărată

$\Rightarrow \bigcap_{i \in I} H_i \leq G.$

Obs: În general, reuniunea de subgrupuri nu este subgrup

Exemplu:

$(\mathbb{Z}, +)$ grup, $2\mathbb{Z}, 3\mathbb{Z} \leq \mathbb{Z}$

$L = 2\mathbb{Z} \cup 3\mathbb{Z}$ nu e parte stabilă: $2, 3 \in L$, dar $2+3 = 5 \notin L$

Corolar:

Fie $(G, \cdot)$ un grup și $X \subseteq G$. Atunci:

$\langle X \rangle \overset{not}{=} \bigcap_{\substack{H \leq G \\ X \subseteq H}} H$ este subgrup în G și $\langle X \rangle$ este cel mai mic (relativ la incluziune) subgrup al lui G care conține pe X.

Def: Dacă $(G, \cdot)$ este un grup și $X \subseteq G$, atunci $\langle X \rangle$ s.n. grupul generat de X.

Obs: $X = \{g_1, \dots, g_m\}$, $\langle X \rangle \overset{not}{=} \langle g_1, \dots, g_m \rangle$

Teoremă

Fie $(G, \cdot)$ grup și $\emptyset \neq X \subseteq G$. Atunci:

$$\langle X \rangle = \underbrace{\left\{ x_1^{\varepsilon_1} \cdot x_2^{\varepsilon_2} \cdot \dots \cdot x_k^{\varepsilon_k} \mid k \in \mathbb{N}^*, \forall i = \overline{1,k}, x_i \in X \text{ și } \varepsilon_i = \pm 1 \right\}}_{A}$$

Dem:

- demonstrăm că A este cel mai mic subgrup care îl conține pe X

1) $A \leq G$

2) $H \leq G, X \subseteq H \Rightarrow A \subseteq H$

1) $X \neq \emptyset \Rightarrow \exists x \in X \Rightarrow x x^{-1} \in A \Rightarrow 1 \in A$

Fie $x, y \in A \Rightarrow \exists k \in \mathbb{N}, \exists x_1, \dots, x_k \in X, \exists \varepsilon_1, \dots, \varepsilon_k \in \{\pm 1\}$ a.î. $x = x_1^{\varepsilon_1} \cdots x_k^{\varepsilon_k}$

$\Rightarrow \exists l \in \mathbb{N}, \exists y_1, \dots, y_l \in X, \exists \delta_1, \dots, \delta_l \in \{\pm 1\}$ a.î. $y = y_1^{\delta_1} \cdots y_l^{\delta_l}$

$$x \cdot y^{-1} = x_1^{\varepsilon_1} \cdot \dots \cdot x_k^{\varepsilon_k} \cdot y_l^{-\delta_l} \cdot \dots \cdot y_1^{-\delta_1}$$

$-\delta_l, \dots, -\delta_1 \in \{\pm 1\}$

$x_1, \dots, x_k, y_1, \dots, y_l \in X$

$\Big\} \Rightarrow xy^{-1} \in A$

$\Rightarrow A \leq G$

2) Fie $H \leq G$ a.î. $X \subseteq H$

Fie $x \in A \Rightarrow x = x_1^{\varepsilon_1} \cdot \dots \cdot x_k^{\varepsilon_k}$, $x_1, \dots, x_k \in X$, $\varepsilon_1, \dots, \varepsilon_k \in \{\pm 1\}$

$x_1, \dots, x_k \in X \overset{X \subseteq H}{\Rightarrow} x_1, \dots, x_k \in H$

$\overset{H \leq G}{\Rightarrow} x \in H$

Exemple

1) $(G,\cdot)$ grup și $g \in G \Rightarrow \langle g \rangle = \{g^k \mid k \in \mathbb{Z}\}$

Dacă ord $g = n \Rightarrow \langle g \rangle = \{1, g, g^2, \dots, g^n\}$

Pt. partea grea din examen 2) În S_n, $T = \{\tau \in S_n \mid \tau$ este transpoziție$\}$

$\langle T \rangle = S_n$ (pt. că orice permutare e produs de transpoziții)

$D = \{\gamma \in S_n \mid \gamma = (a,b,c)$ ciclu de lungime 3$\}$

$\langle D \rangle = ?$

$\langle D \rangle = A_n = \{\sigma \in S_n \mid \sigma$ permutare pară$\}$

σ-pară $\Leftrightarrow \sigma$ este produsul unui număr par de transpoziții

$\sigma \in A_n \Rightarrow \exists\, \tau_1, \dots, \tau_{2k}$ transpoziții a.î. $\sigma = \tau_1 \tau_2 \cdots \tau_{2k} = (\tau_1\tau_2)(\tau_3\tau_4)\cdots(\tau_{2k-1}\tau_{2k})$

Dem. că orice produs de 2 transpoziții e un produs de cicluri de lungime 3

$(i,j)\cdot(k,l) = (i,k,j)\cdot(i,k,l)$

$(i,j)\cdot(j,k) = (i,k,j)^2$

$\Rightarrow \forall\, \sigma \in A_n$, σ e un produs de cicluri de lungime 3

$\Rightarrow A_n \subseteq \langle D \rangle$

Dacă $\sigma \in \langle D \rangle \Rightarrow \sigma$ este un produs de permutări pare $\Rightarrow \sigma \in A_n$

$\Rightarrow \langle D \rangle = A_n$

CURS 5 27.03.2018

Grupuri ciclice

$(G,\cdot)$ grup

$\emptyset \neq X \subseteq G \Rightarrow \langle X \rangle = \{x_1^{\varepsilon_1} \dots x_n^{\varepsilon_n} \mid n \in \mathbb{N}^*, \forall i = \overline{1,n}, x_i \in X, \varepsilon_i = \pm 1\}$ – subgrupul generat de X

În particular, dacă $X = \{x\} \Rightarrow \langle X \rangle \overset{not}{=} \langle x \rangle = \{x^k \mid k \in \mathbb{Z}\}$

Def: Spunem că grupul $(G,\cdot)$ este ciclic, dacă:

$\exists\, x \in G$ a.î. $G = \langle x \rangle$

În aceste condiții, vom spune că x este un generator pentru G.

Exemple:

1) $(\mathbb{Z},+)$ este ciclic, generat de 1 sau de -1

$\mathbb{Z} = \langle 1 \rangle = \langle -1 \rangle$

2) $(\mathbb{Z}_n,+)$ este ciclic, $\mathbb{Z}_n = \langle \hat{1} \rangle$

$\hat{a} \in \mathbb{Z}_n$ cu $(a,n)=1 \Rightarrow$ ord $\hat{a} = n \Rightarrow \langle \hat{a} \rangle = \{k\cdot\hat{a} \mid k \in \mathbb{Z}\} = \{\hat{0}, \hat{a}, 2\hat{a}, \dots, (n-1)\cdot\hat{a}\}$ ($n \cdot \hat{a} = \hat{0}$)

ord $\hat{a} = n \Rightarrow \forall\, i < j$ cu $i,j \in \{0,\dots,n-1\}$, $i\cdot\hat{a} \neq j\cdot\hat{a}$

$\Rightarrow |\langle \hat{a} \rangle| = n \Rightarrow \langle \hat{a} \rangle = \mathbb{Z}_n$

$n = 9$, $\hat{a} = \hat{2}$

$\langle \hat{2} \rangle = \{\hat{0}, \hat{2}, \hat{4}, \hat{6}, \hat{1}, \hat{3}, \hat{5}, \hat{7}\} = \mathbb{Z}_9$ ($5\cdot\hat{2}$, $6\cdot\hat{2}$, $7\cdot\hat{2}$, $8\cdot\hat{2}$)

3) Dacă p – prim impar, atunci $(U(\mathbb{Z}_p), \cdot)$ grup ciclic.

($\hat{a}$ – generator pentru $U(\mathbb{Z}_p)$ – spunem că a este o rădăcină primitivă modulo p)