Curs 8

23.11.2021

Exc (Seminar!) Să se arate că mulțimea morfismelor de grupuri de la $(\mathbb{Z}_m,+)$ la $(\mathbb{Z}_n,+)$ are cardinalul egal cu d, unde $d=(m,n)$. (De fapt, se poate arăta mai mult: grupul morf. de la $(\mathbb{Z}_m,+)$ la $(\mathbb{Z}_n,+)$ e izomorf cu $(\mathbb{Z}_d,+)$)

Exemplu Det. morfismele de grupuri de la $(\mathbb{Z}_5,+)$ în $(\mathbb{Z}_7,+)$

Obs Între orice 2 grupuri există un morfism de grupuri (numit trivial) $f:(G_1,\cdot)\to(G_2,*)$ $f(g)=1_{G_2}$ $(\forall)g\in G_1$

Fie $f:(\mathbb{Z}_5,+)\to(\mathbb{Z}_7,+)$ un morfism de grupuri. $(\Rightarrow f(\hat{0})=\bar{0})$

$f(\hat{a}+\hat{b})=f(\hat{a})+f(\hat{b})$ $(\forall)\ \hat{a},\hat{b}\in\mathbb{Z}_5$

f e det. de $f(\hat{1})$ $\quad f(\hat{1}+\hat{1})=f(\hat{1})+f(\hat{1})$ ...

$f(\hat{2})=2f(\hat{1})$, $f(\hat{3})=3f(\hat{1})$

$f(\hat{4})=4f(\hat{1})$, $f(\hat{5})=5f(\hat{1})$

$f(\hat{5})=f(\hat{0})=\bar{0}$ $\Rightarrow$

$\Rightarrow 5f(\hat{1})=\bar{0} \Rightarrow$ $f(\hat{1})=\bar{k}$ $\quad 5\cdot\bar{k}=\bar{0}$, $5\cdot\bar{k}=\overline{5k}$ $\Rightarrow 7\mid 5k$, $(7,5)=1$ $\Rightarrow 7\mid k \Rightarrow \bar{k}=\bar{0}$

$\Rightarrow f(\hat{1})=\bar{0} \Rightarrow f(\hat{a})=\bar{0}$ $(\forall)\ \hat{a}\in\mathbb{Z}_5$. $\Rightarrow$ există un singur morf. (cel trivial)

Subgrupuri

Def Fie $(G,\cdot)$ un grup. O submulțime nevidă H a lui G s.n. subgrup al lui G și notăm $H\leq G$, dacă H este parte stabilă a lui G închisă la luarea inversului, i.e. $(\forall)\ x,y\in H$ avem $x\cdot y\in H$ și $x^{-1}\in H$.

ECHIVALENT

Prop Fie $(G,\cdot)$ un grup. O submulțime nevidă H a lui G este subgrup $\Leftrightarrow$ $(\forall)\ x,y\in H$ avem $xy^{-1}\in H$ (în notație aditivă, adică pt $(G,+)$, scriem ...... $\Leftrightarrow (\forall)\ x,y\in H$ $x+(-y)\in H$, $x+(-y)=x-y$)

Exemple ① Subgrupurile lui $(\mathbb{Z},+)$ sunt toate submulțimile de forma $n\mathbb{Z}$, cu $n\in\mathbb{N}$. (Exc! seminar)

② Dacă $(G,\cdot)$ este un grup atunci G are 2 subgrupuri (dacă $|G|>1$) $\{1_G\}$ și G. (Dacă G este grup $|G|=1 \Rightarrow G=\{e\}$ elementul neutru)

③ $(\mathbb{Z},+) \leq (\mathbb{Q},+) \leq (\mathbb{R},+) \leq (\mathbb{C},+)$

④ Fie G un grup. Dacă $H_1, H_2 \leq G \Rightarrow H_1 \cap H_2 \leq G$.

(Dem: Fie $x,y \in H_1 \cap H_2 \Rightarrow x,y \in H_1$ și $x,y \in H_2$ $\xrightarrow[H_2 \leq G]{H_1 \leq G}$ $xy^{-1} \in H_1$ și $xy^{-1} \in H_2$ $\Rightarrow xy^{-1} \in H_1 \cap H_2 \Rightarrow H_1 \cap H_2 \leq G$)

(Se poate arăta (la fel) că orice intersecție de subgrupuri ale unui grup este un subgrup) (Exc! $n\mathbb{Z} \cap m\mathbb{Z} = [n,m]\mathbb{Z}$) $[n,m]$ = cmmmc(n,m)

Teoremă Fie $f: G \to G'$ un morfism de grupuri.

1) Dacă $H \leq G \rightsquigarrow f(H) \leq G'$ $\quad (f(H)=\{f(x) \mid x\in H\})$

2) Dacă $H' \leq G' \rightsquigarrow \underline{f^{-1}(H')} \leq G$ $\quad (f^{-1}(H')=\{x\in G \mid f(x)\in H'\})$

$f^{-1}(H')$ → preimaginea lui H' prin f

Dem exc! (cu definiția subgr.)

Obs În particular $\mathrm{Im}(f) \leq G'$ și $f^{-1}(\{1_{G'}\}) \leq G$

$\mathrm{Im}(f) = f(G)$ $\quad \{1_{G'}\} \leq G'$

Def $\underline{f^{-1}(\{1_{G'}\})}$ s.n. cu $\underline{\mathrm{Ker}(f)}$ și s.n. nucleul morfismului f.

Propr Fie $f: G \to G'$ un morfism de grupuri. Atunci f este injectiv $\Leftrightarrow \mathrm{Ker}(f)=\{1_G\}$.

(!! $1_G \in \mathrm{Ker}(f)$ $(\forall)$ morf. de gr. $f: G\to G'$)

Exemple ① $f: (\mathbb{Z}\times\mathbb{Z},+) \to (\mathbb{Z},+)$ $\quad f(x,y)=x-y$ → morf. de gr. (Exc!)

$\mathbb{Z}\times\mathbb{Z}$ → produsul direct al lui $(\mathbb{Z},+)$ cu $(\mathbb{Z},+)$

$\mathrm{Ker}(f)=\{(x,y)\in\mathbb{Z}\times\mathbb{Z} \mid \underbrace{f(x,y)}_{=x-y}=0\} = \{(x,x) \mid x\in\mathbb{Z}\}$ → nu e inj

$U_4=\{z\in\mathbb{C} \mid z^4=1\}=\{\pm1, \pm i\}$

② $f: (U_4,\cdot) \to (\mathbb{C}^*,\cdot)$ $\quad f(z)=z^2$ → morf. de grupuri, (Exc!)

$\mathrm{Ker} f = \{z\in U_4 \mid f(z)=1\} = \{-1,1\}$. → nu e inj

③ Să se arate că grupurile $(U_n,\cdot)$ și $(\mathbb{Z}_n,+)$ sunt izomorfe $(\forall)\, n\geq 2$. (Ex! seminar)

Subgrupul generat de o mulțime

(modul algoritmic de construcție a unui subgrup)

Def Fie $(G,\cdot)$ un grup și $\phi\neq A\subseteq G$. Subgrupul lui G generat de mulțimea A s.n. cu $\langle A\rangle$ și reprezintă:

$$\langle A\rangle \overset{def}{=} \{a_1^{\pm 1}\cdot a_2^{\pm 1}\cdot\ldots\cdot a_n^{\pm 1} \mid a_1,\ldots,a_n\in A,\ n\geq 1\}\leq G.$$

$1_G = a\cdot a^{-1}$, $a \in A$

Prin definiție $\langle\phi\rangle=\{1_G\}$.

Obs 1) $G=\langle G\rangle$

2) Dacă $A=\{a\}$ $\quad \langle\{a\}\rangle \overset{not}{=} \langle a\rangle = \{a^k \mid k\in\mathbb{Z}\}$ $\quad (1_G=a^0)$ $\quad$ (not aG)

$\langle a\rangle$ → s.n. subgrupul ciclic generat de a.

Exemple 1) $G=(\mathbb{Z},+)$ $\quad \langle n\rangle = n\mathbb{Z}=\{kn \mid k\in\mathbb{Z}\}$ $\quad G=1\mathbb{Z}$ (G e grup ciclic)

2) $G=(\mathbb{Z}_{10},+)$ $\quad \langle\hat{2}\rangle=\hat{2}\mathbb{Z}_{10}=\{k\cdot\hat{2} \mid k\in\mathbb{Z}\}=\{\hat{0},\hat{2},\hat{4},\hat{6},\hat{8}\}$

$\mathbb{Z}_{10}=\langle\hat{1}\rangle \;(=\langle\hat{3}\rangle=\langle\hat{7}\rangle=\langle\hat{9}\rangle)$ $\quad \mathbb{Z}_{10}$ – e grup ciclic

$\langle\hat{5}\rangle=\{\hat{0},\hat{5}\}$

3) $G=U(\mathbb{Z}_8,\cdot)=\{\hat{1},\hat{3},\hat{5},\hat{7}\}$ $\quad \langle\hat{5}\rangle=\{\hat{1},\hat{5}\}$ $\quad \langle\hat{3}\rangle=\{\hat{1},\hat{3}\}$

$\langle\hat{7}\rangle=\{\hat{1},\hat{7}\}$ $\quad \langle\hat{1}\rangle=\{\hat{1}\}$

G nu e ciclic

$G=\langle\{\hat{3},\hat{5}\}\rangle \ni \hat{1},\hat{3},\hat{5},\ \hat{7}=\hat{3}\cdot\hat{5}$

$G=\langle\{\hat{3},\hat{5}\}\rangle=\langle\{\hat{3},\hat{7}\}\rangle = \langle\{\hat{5},\hat{7}\}\rangle$

Teoremă Fie G un grup și $A\subseteq G$. Atunci $\langle A\rangle$ este un subgrup al lui G conținut în orice subgrup H al lui G, care-l conține pe A. Mai mult,

$$\langle A\rangle = \bigcap_{\substack{H\le G\\ H\supseteq A}} H$$

Obs ① Teorema ant. ne spune că $\langle A\rangle$ ește cel mai mic subgrup al lui G care-l conține pe A.

② $A=\{a_1,\dots,a_m\}\subseteq G$, $(G,\cdot)$ abelian (=com) $\Rightarrow$

$\Rightarrow \langle A\rangle \overset{\text{not}}{=} \langle a_1,\dots,a_m\rangle = \{a_1^{k_1}a_2^{k_2}\cdots a_m^{k_m} \mid k_1,\dots,k_m\in\mathbb{Z}\}$

Def Spunem că grupul $(G,\cdot)$ este generat de submulțimea A dacă $\langle A\rangle = G$. Grupul s.n. ciclic dacă $(\exists)\, a\in G$ a.î. $G=\langle a\rangle$. G s.n. finit generat dacă $(\exists)\, A\subseteq G$ cu $|A|<\infty$ a.î. $G=\langle A\rangle$.

Obs 1) $(\mathbb{Z},+)$ și $(\mathbb{Z}_n,+)$ – grupuri ciclice

2) Un grup ciclic e abelian.

3) Un grup finit e evident finit generat.

4) (Exc!) $(\mathbb{Q},+)$ nu e grup finit generat.

Def Fie $(G,\cdot)$ un grup și $H\le G$. Pe G def. urm. rel. binare:

1) "$\equiv_s (\text{mod } H)$": $x\equiv_s y\,(\text{mod } H) \Leftrightarrow x^{-1}y\in H$ (s.n. congruența la stânga modulo H)

2) "$\equiv_d (\text{mod } H)$": $x\equiv_d y\,(\text{mod } H) \Leftrightarrow xy^{-1}\in H$ (s.n. congruența la dreapta modulo H)

Exc! "$\equiv_s(\text{mod } H)$" și "$\equiv_d(\text{mod } H)$" sunt rel. de echivalență pe G