Curs 8

24.11.2020

Reamintesc

Obs 1) $(G,\cdot)$ grup și $x\in G$, $\mathrm{ord}(x)=n<\infty \Rightarrow |\langle x\rangle| = n$

2) $(G,\cdot)$ grup finit și $x\in G \Rightarrow \mathrm{ord}(x)<\infty$ și $\mathrm{ord}(x) \mid |G|$ (Lagrange)

3) $(G,\cdot)$ grup și $x\in G$, $\mathrm{ord}(x)=n<\infty$. $x^k = 1 \iff n \mid k$.

Aplicații: ① **Teorema lui Euler** Fie $(a,n)=1$, $a,n\in\mathbb{N}$. Atunci $a^{\varphi(n)} \equiv 1 \pmod n$.

(Dem $(U(\mathbb{Z}_n),\cdot) \to$ grup cu $|U(\mathbb{Z}_n)| = \varphi(n)$. $\overset{\text{Obs 3)}}{\Longrightarrow}$ $\hat{a}^{\varphi(n)} = \hat{1}$ $(\forall)\ \hat{a}\in U(\mathbb{Z}_n)$

$\mathrm{ord}(\hat{a}) \mid \varphi(n)$ Exc!

$\Rightarrow a^{\varphi(n)} \equiv 1 \pmod n$ $((a,n)=1)$)

② (Mica Teoremă a lui Fermat) Fie p un nr. prim și $a\in\mathbb{N}$ a.î. $p\nmid a \Rightarrow a^{p-1}\equiv 1\ (p)$

(sau p-prim, $a\in\mathbb{N} \Rightarrow a^p \equiv a \pmod p$) **Dem** Euler pt $n=p$; $\varphi(p)=p-1$.

Reamintesc Def Dc $(G,\cdot)$ un grup și $H\leq G$ atunci H s.n. subgrup normal al lui G dc. $xH = Hx$ $(\forall)\ x\in G$. ($\iff (G/H)_s = (G/H)_d$). (Dc H e subgrup normal al lui G notăm $H \trianglelefteq G$)

Prop1 Fie $(G,\cdot)$ un grup și $H\leq G$. Atunci $H\trianglelefteq G \iff xHx^{-1} \subseteq H$ $(\forall)\ x\in G$

($\iff xhx^{-1}\in H$ $(\forall)\ x\in G$ $(\forall)\ h\in H$).

Exemplu 1) $G = (S_3, \circ)$, $H = \langle (13) \rangle = \{(13), e\}$ $e = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$ $(13) = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$

H nu este subgrup normal al lui G. #

$\underset{G}{\overset{\cap}{(12)}} \circ \underset{H}{\overset{\cap}{(13)}} \circ \underset{G}{\overset{\cap}{(12)^{-1}}} = (12) \circ (13) \circ (12) =$ $(12) = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$

$= \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = (23) \notin H$

$(12)^{-1} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = (12)$

$\overset{\text{Propr}}{\underset{\text{aut}}{\Longrightarrow}}$ H nu e subgrup normal al lui G.

Ream 2) $(G, \cdot)$ grup abelian $\Rightarrow (\forall)\ H \leq G$ avem $H \trianglelefteq G$.

Construcții generale de subgrupuri normale:

① Fie $(G, \cdot)$, $(G', \circ)$ 2 grupuri și $f: (G, \cdot) \to (G', \cdot)$ un morfism de grupuri.

Atunci $Ker(f) \trianglelefteq G$. ($Ker(f) = \{x \in G \mid f(x) = 1_{G'}\}$)

Dem Conform propr. aut tb. arătat că $(\forall)\ x \in G\ (\forall)\ h \in Ker(f)$ avem $xhx^{-1} \in Ker(f)$.

$f(xhx^{-1}) \overset{f}{\underset{\text{morfism}}{=}} f(x) f(h) f(x)^{-1} = f(x) f(x)^{-1} = 1_{G'}$ ∎

$h \in Ker(f) \Rightarrow \underline{f(h) = 1_{G'}}$

$xhx^{-1} \in Ker(f)$

② Orice subgrup de indice 2 este normal. ($H \leq G$, $[G:H] = |(G/H)_s|$ $(= |(G/H)_d|)$

(Dem $[G:H] = 2$; $H = 1_G H \in (G/H)_s$; mult. claselor de echivalență formează o partiție $\longrightarrow$ $(G/H)_s = \{H, G \setminus H\}$. Similar se arată că $(G/H)_d = \{H, G \setminus H\} \Rightarrow$

$|(G/H)_s| = 2$

$\Rightarrow (G/H)_s = (G/H)_d \Rightarrow H \trianglelefteq G$. ∎

Grupul factor

Fie $(G,\cdot)$ un grup, $H \trianglelefteq G$. $\quad H \trianglelefteq G \Rightarrow (G/H)_s = (G/H)_d \stackrel{\text{not}}{=} G/H$

$\hat{x} \stackrel{\text{not}}{=} xH = Hx \quad (\forall)\, x \in G$

$G/H = \{\hat{x} \mid x \in G\}$.

Pe G/H introducem operația alg.: $\quad \hat{x} \cdot \hat{y} \stackrel{\text{def}}{=} \widehat{x \cdot y} \quad (\forall)\, x, y \in G$.

$\mathbb{Z}_{12} = \{\hat{0}, \hat{1}, \dots, \widehat{11}\}$

$\hat{1} = \widehat{13} = \widehat{25}$

$\hat{2} \cdot \hat{3} = \hat{6}$

$\widehat{14} \cdot \widehat{39} = \hat{6}$

Operația e bine definită:

Fie $x', y' \in G$ a.î. $\hat{x} = \hat{x'}$; $\hat{y} = \hat{y'}$. $\Rightarrow h = x^{-1}x' \in H$. $\quad y^{-1}y' \in H$.

$x \equiv_s x' \pmod H \rightsquigarrow x^{-1}x' \in H$

$x \equiv_d x' \pmod H \rightsquigarrow x \cdot (x')^{-1} \in H$

Dar $y'H = Hy' \rightsquigarrow (\exists)\, h' \in H$ a.î. $hy' = y'h'$

Vrean $\widehat{x \cdot y} = \widehat{x'y'}$ $\left(\Leftrightarrow (xy)^{-1}x'y' \in H\right)$

$$y^{-1}\underbrace{x^{-1}x'}_{h}y' = y^{-1}(y'h') = \underbrace{(y^{-1}y')}_{\in H} \cdot \underbrace{h'}_{\in H} \in H$$

Teoremă Fie $(G,\cdot)$ un grup și $H \trianglelefteq G$. Atunci operația definită anterior este o lege de compoziție în raport cu care G/H este grup, numit grupul factor al lui G modulo H. (Aplicația $G \longrightarrow G/H$, $a \longmapsto \hat{a}$, este un morfism surjectiv de grupuri).

Obs Fie $\boxed{m\geq 2}$. Grupul factor $\mathbb{Z}/_{m\mathbb{Z}} = (\mathbb{Z}_m, +)$ (definit anterior)

$(m\mathbb{Z} \trianglelefteq (\mathbb{Z}, +)$ -abelian$)$

Teorema fundamentală de izomorfism Fie $f: G \to G'$ un morfism de grupuri. Atunci există un izomorfism între grupurile $G/_{\operatorname{Ker} f}$ și $\operatorname{Im} f$; mai precis

$$\bar{f}: G/_{\operatorname{Ker} f} \xrightarrow{\sim} \operatorname{Im} f \qquad \bar{f}(\hat{x}) = f(x) \quad (\forall)\, x \in G.$$

Aplicații ① Fie morfismul de grupuri $f: (\mathbb{R}, +) \to (\mathbb{C}^*, \cdot)$, $f(\alpha) = \cos(2\pi\alpha) + i\sin(2\pi\alpha)$ $(\forall)\, \alpha \in \mathbb{R}$. Să se arate că $\operatorname{Im}(f) = U = \{z \in \mathbb{C} \mid |z| = 1\}$, $\operatorname{Ker}(f) = \mathbb{Z}$ și $\mathbb{R}/_{\mathbb{Z}} \simeq U$.

② Arătați că $\mathbb{C}^*/_U$ este izomorf cu grupul $(\mathbb{R}_+^*, \cdot)$.

Exc ③ Arătați că $\mathbb{C}^*/_{\mathbb{R}_+^*} \simeq U$ (izomorfe ca grupuri).

(Ce tb. făcut? Tb. găsit un morf. surj. de grupuri $f: (\mathbb{C}^*, \cdot) \to (\mathbb{R}_+^*, \cdot)$ a.î. $\operatorname{Ker} f = U$)

---

① $f: (\mathbb{R}, +) \to (\mathbb{C}^*, \cdot)$ $\quad f(\alpha) = \cos(2\pi\alpha) + i\sin(2\pi\alpha)$ $\quad (\forall)\, \alpha \in \mathbb{R}$

$\operatorname{Im} f \overset{?}{=} U = \{z \in \mathbb{C} \mid |z| = 1\}$. $\quad \operatorname{Ker} f = \{\alpha \in \mathbb{R} \mid f(\alpha) = 1\}$

$\cos(2\pi\alpha) + i\sin(2\pi\alpha) = 1 \to \begin{cases} \cos(2\pi\alpha) = 1 \\ \sin(2\pi\alpha) = 0 \end{cases}$

$\Rightarrow 2\pi\alpha \in \{2k\pi \mid k\in\mathbb{Z}\} \Rightarrow \alpha\in\mathbb{Z}. \Rightarrow \operatorname{Ker} f \subseteq \mathbb{Z}$. Cum $\underset{\substack{\cap\\ \mathbb{Z}}}{f(k)} = \underset{\substack{\parallel\\ 1}}{\cos(2k\pi)+i\sin(2k\pi)} \Rightarrow$ $\supseteq$

$\Rightarrow \underline{\operatorname{Ker}(f)=\mathbb{Z}}$.

f morfism de grupuri $\left(\Leftarrow f(\alpha+\beta)=f(\alpha)\cdot f(\beta)\ (\forall)\ \alpha,\beta\in\mathbb{R}.\right.$

$f(\alpha+\beta)=\cos 2\pi(\alpha+\beta)+i\sin 2\pi(\alpha+\beta) = \left.(\cos 2\pi\alpha+i\sin 2\pi\alpha)(\cos 2\pi\beta+i\sin 2\pi\beta)\right)$

$\cos(a+b)=\cos a\cos b-\sin a\sin b$
$\sin(a+b)=\sin a\cos b+\sin b\cos a$
$a=2\pi\alpha,\ b=2\pi\beta$

Aplicând $\underline{\text{T.F.I}}$ obţin că $\mathbb{R}/\mathbb{Z}\simeq U$.

<u>Teorema de structură a grupurilor ciclice</u> Orice grup ciclic infinit este izomorf cu $(\mathbb{Z},+)$ şi orice grup ciclic finit (cu n elemente) este izomorf cu $(\mathbb{Z}_n,+)$.

<u>Dem</u> $(G,\cdot)\to$ grup ciclic $\Rightarrow (\exists)\ a\in G$ a.î. $G=\langle a\rangle=\{a^k \mid k\in\mathbb{Z}\}$.

Definesc $f:(\mathbb{Z},+)\to(G,\cdot)\quad f(k)=a^k\ (\forall)\ k\in\mathbb{Z}$

f e morfism de grupuri $\left(f(k+l)=a^{k+l}=a^k\cdot a^l=f(k)\cdot f(l)\ (\forall)\ k,l\in\mathbb{Z}\right)$

$\xrightarrow{\text{T.F.I}} \mathbb{Z}/\operatorname{Ker} f \simeq G\ (=\operatorname{Im} f)$. (1)

f e <u>surj</u>. (prin def.)

f e $\to$ injectiv $(\Leftrightarrow \operatorname{Ker} f=\{0\}=0\mathbb{Z})$; (1) devine $\mathbb{Z}\simeq G$. (G infinit)

f e $\to$ neinjectiv $(\Leftrightarrow \operatorname{Ker} f\neq\{0\}$; $\operatorname{Ker} f=n\mathbb{Z}$ cu $n\geq 1)$;(1) devine $\underset{\mathbb{Z}_n}{\mathbb{Z}/n\mathbb{Z}}\simeq G$ (finit)

Obs 1) Fie p un număr prim. Atunci orice grup finit de ordin p este ciclic, deci izomorf cu $(\mathbb{Z}_p,+)$. (Dem Fie $(G,\cdot)$ un grup de ordin p, p-prim $\Rightarrow (\exists)\, x \in G\setminus\{1\}$

$|\langle x\rangle| \,\Big|\, |G| = p \Rightarrow \underbrace{|\langle x\rangle|}_{= \mathrm{ord}(x)} = p \Rightarrow G = \langle x\rangle$.)

$\neq$ 1 $\quad$ Lagrange