Reamintesc:

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

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

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

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

7.12.2021

Curs 9

Teoremă Fie $(G,\cdot)$ un grup și $H \leq G$. Atunci cele 2 congruențe modulo H anterior definite sunt relații de echivalență pe G. Clasele de echivalență ale "$\equiv_s (\mathrm{mod}\, H)$" sunt submulțimile lui G de forma $xH = \{xy \mid y \in H\}$; clasele de echivalență ale "$\equiv_d (\mathrm{mod}\, H)$" sunt submulțimile lui G de forma $Hx = \{y\cdot x \mid y \in H\}$. Mulțimea factor a lui "$\equiv_s (\mathrm{mod}\, H)$" (resp "$\equiv_d (\mathrm{mod}\, H)$") se notează cu $(G/H)_s$ (resp $(G/H)_d$) și $|(G/H)_s| = |(G/H)_d|$. Acest cardinal comun s.n. indicele lui H în G și se notează cu $[G:H]$.

Obs 1) $(G/H)_s$ și $(G/H)_d$ pot fi diferite (chiar dacă au același cardinal).

De exemplu pt $G = S_3$, $H = \langle (13) \rangle$

$(G/H)_s = \{(12)H, (13)H, (23)H\}$

Exc! $\rightarrow$ $(G/H)_d = \{H(12), H(13), H(23)\}$

2) Dacă G e abelian atunci $xH = Hx$ $(\forall)\, x \in G$; prin urmare $(G/H)_s = (G/H)_d$.

3) Fie $G = S_3$, $H = \langle (123) \rangle = \{e, (123), (132)\}$. Atunci $(G/H)_s = (G/H)_d$ (Exc!)

Exc! $(S_n, \circ) \to$ grup $\quad S_n = \{\sigma : \{1,2,\dots,n\} \to \{1,2,\dots,n\} \mid \sigma$ bijectie$\}$

$|S_n| = n!$ $\quad$ Dc $\sigma \in S_n \rightsquigarrow \sigma$ se mai scrie $\sigma = \begin{pmatrix} 1 & 2 & 3 & \dots & n \\ \sigma(1) & \sigma(2) & \sigma(3) & \dots & \sigma(n) \end{pmatrix}$

$$S_3 = \{ \underset{\substack{\text{not} \\ e}}{\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}}, \underset{\substack{\text{not} \\ (12)}}{\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}}, \underset{\substack{\text{not} \\ (13)}}{\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}}, \underset{\substack{\text{not} \\ (23)}}{\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}}, \underset{\substack{\text{not} \\ (123)}}{\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}}, \underset{\substack{\text{not} \\ (132)}}{\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}} \}$$

$$\underset{\sigma_1}{(12)} \circ \underset{\sigma_2}{(13)} = \underset{\sigma_1}{\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}} \circ \boxed{\underset{\sigma_2}{\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}}} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = (132) \quad (1)$$

$\longrightarrow$ $\sigma_2(1) = 3$, $\sigma_2(2) = 2$, $\sigma_2(3) = 1$

$(\sigma_1 \circ \sigma_2)(1) = \sigma_1(\sigma_2(1)) = \sigma_1(3) = 3$

$(\sigma_1 \circ \sigma_2)(2) = \sigma_1(\sigma_2(2)) = \sigma_1(2) = 1$

$(\sigma_1 \circ \sigma_2)(3) = \sigma_1(\sigma_2(3)) = \sigma_1(1) = 2$

$$(13) \circ (12) = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = (123) \quad (2)$$

Din (1) și (2) $\Rightarrow$ $(S_3, \circ)$ nu e grup abelian.

$(13) \circ (13) = e$

$H = \langle (13) \rangle = \{e, (13)\}$ deoarece $(13)^2 = e$

$(12)H = \{(12) \circ e, (12) \circ (13)\} = \{(12), (132)\}$

$H(12) = \{e \circ (12), (13) \circ (12)\} = \{(12), (123)\}$

$(13)H = \{(13) \circ e, (13) \circ (13)\} = \{(13), e\} = H \overset{\text{la}}{\underset{\text{fel}}{=}} H(13)$

$(23)H = \{(23) \circ e, (23) \circ (13)\} = \{(23), (123)\}$

$(23) \circ (13) = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$

$H(23) = \{e \circ (23), (13) \circ (23)\} = \{(23), (132)\}$

$(13) \circ (23) = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$

$\Rightarrow$

$(G/H)_s \neq (G/H)_d = \{H(12), H(13), H(23)\}$

$(G/H)_s = \{(12)H, (13)H, (23)H\}$

$H(12) \neq (12)H$

Teorema lui Lagrange Fie G un grup finit și $H \leq G$. Atunci
$$|G| = |H| \cdot [G:H].$$
În particular, $|H|$ divide $|G|$.

Dem "$\equiv_s (\bmod H)$" rel. de echiv. pe $G \Rightarrow |G| = \sum |C| = |H| \cdot |(G/H)_s|$

C - clasă de echiv pt "$\equiv_s (\bmod H)$"

$|(G/H)_s| = [G:H]$

$C = xH \xleftarrow[\text{bij}]{f} H = eH \rightarrow \boxed{|C| = |H|}$

$xa = f(a) \leftarrow a$

Def Fie $(G,\cdot)$ un grup și $x \in G$. Atunci

$$\text{ord}(x) \overset{\text{def}}{=} \begin{cases} \infty, & \text{dacă } x^n \neq 1\ (\forall)\, n \in \mathbb{N}^* \\ \min\{n \in \mathbb{N}^* \mid x^n = 1\} & \text{dacă } (\exists)\, t \in \mathbb{N}^* \text{ a.î. } x^t = 1. \end{cases}$$

ordinul lui x

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

2) $(G,\cdot)$ grup finit și $x \in G \Rightarrow \text{ord}(x) < \infty$ și $\text{ord}(x) \mid |G|$
(Lagrange $\Rightarrow$ $H = \langle x \rangle$; $|H| \mid |G|$), $|H| = \text{ord}\, x$

3) Dacă $(G,\cdot)$ grup finit și $x \in G \Rightarrow x^n = e$, unde $n = |G|$. ($\text{ord}(x) = t \mid n \Rightarrow$
$x^n = x^{tk} = (x^t)^k = e^k = e \mid n = tk$)

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

Dem $(U(\mathbb{Z}_n),\cdot) \rightarrow$ grup $|U(\mathbb{Z}_n)| = \varphi(n) \xRightarrow{\text{Obs2}} \text{ord}(\hat{a}) \mid |U(\mathbb{Z}_n)| = \varphi(n)$

$(a,n) = 1 \Rightarrow \hat{a} \in U(\mathbb{Z}_n)$

$\Rightarrow \text{ord}(\hat{a}) \mid \varphi(n) \Rightarrow \hat{a}^{\varphi(n)} = \hat{1} \Rightarrow a^{\varphi(n)} - 1 \equiv 0 \pmod n \Rightarrow a^{\varphi(n)} \equiv 1 \pmod n$

② **Mica teoremă a lui Fermat** Fie p un nr. prim și $a \in \mathbb{N}$ a.î. $p \nmid a$ $\Rightarrow a^{p-1} \equiv 1 \pmod p$. Mai general, dacă p e prim și $a \in \mathbb{N} \Rightarrow a^p \equiv a \pmod p$.

Dem Euler pt $n = p$ - prim și $\varphi(p) = p - 1$.

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

Propr (Cum verific că un subgrup e normal?)
Fie $(G,\cdot)$ un grup și $H \leq G$. Atunci H este subgrup normal al lui $G \iff xHx^{-1} \subseteq H$ $(\forall)$ $x \in G$. $\left(\iff xhx^{-1} \in H \ (\forall) x \in G \ (\forall) h \in H\right)$

Exemplu
1) Dc. $(G,\cdot)$ e abelian; $(\forall) H \leq G \Rightarrow H \trianglelefteq G$.

2) $G = (S_3, \circ)$ $\quad H = \langle (13) \rangle = \{e, (13)\}$
$(12)H \neq H(12)$ (vezi anterior) $\xRightarrow[\text{subgr. normal}]{\text{def}}$ H nu e subgrup normal al lui S_3

3) $G = (S_3, \circ)$ $\quad H = \langle (123) \rangle = \{e, (123), (132)\}$
$(G/H)_s = (G/H)_d$ (vezi anterior) $\xRightarrow{\text{def}} H \trianglelefteq S_3$.

Construcții generale de subgrupuri normale

① Fie $(G,\cdot)$, $(G',\cdot)$ 2 grupuri și $f : G \to G'$ un morfism de grupuri. Atunci $\operatorname{Ker} f \trianglelefteq G$. (Exc!) $\left(\operatorname{Ker} f = \{y \in G \mid f(y) = 1_{G'}\}\right)$

(Dem: $H \overset{\text{not}}{:=} \operatorname{Ker} f$. Fie $x \in G$, $h \in H (= \operatorname{Ker} f)$ $\left(\xRightarrow[\operatorname{Ker} f]{\text{def}} f(h) = 1_{G'}\right)$

Vreau $xhx^{-1} \in H (= \operatorname{Ker} f) \Longleftarrow f(xhx^{-1}) \overset{f}{\underset{\text{morf}}{=}} f(x)f(h)f(x^{-1}) \overset{f}{\underset{\text{morf}}{=}}$
$f(x) f(h) (f(x))^{-1} \underset{h \in \operatorname{Ker} f}{=} f(x) \cdot 1_{G'} (f(x))^{-1} = f(x) \cdot (f(x))^{-1} = 1_{G'} \Rightarrow$))

② Orice subgrup de indice 2 e normal. $(H \leq G \ [G:H] = 2$
$\Rightarrow H \trianglelefteq G)$ $\quad [G:H] = 2 \Rightarrow |(G/H)_s| = |(G/H)_d| = 2$

$eH = H = He$
$\quad \cap \qquad\qquad \cap$
$(G/H)_s \qquad (G/H)_d$

$$\left.\begin{array}{l} |(G/H)_s| = 2 \\ H \in (G/H)_s \end{array}\right\} \Rightarrow G \setminus H \in (G/H)_s \text{ și } (G/H)_s = \{H, G \setminus H\} \Big/ \Rightarrow$$

La fel e $(G/H)_d$

$(G/H)_s = (G/H)_d \xRightarrow[\text{subgr. normal}]{\text{def}}$

Grupul factor

Fie $(G,\cdot)$ un grup, $H \trianglelefteq G$. $\quad H \trianglelefteq G \xRightarrow{\text{def}} (G/H)_s = (G/H)_d \overset{\text{not}}{:=} G/H$
$G/H = \{\hat{x} \mid x \in G\}$ $\quad \left(\hat{x} \overset{\text{not}}{=} xH \overset{\checkmark}{=} Hx\right)$

Pe G/H introducem operația alg.

$$\hat{x} \cdot \hat{y} \overset{def}{=} \widehat{xy}.$$

(operația e bine definită) Exc!

Teoremă Fie $(G, \cdot)$ un grup și $H \trianglelefteq G$. Atunci operația în raport definită anterior este o lege de compoziție față de care G/H este grup, numit grupul factor al lui G modulo H. (Aplicația $G \xrightarrow{p} G/H$, $a \mapsto \hat{a}$ este un morf. surj. de grupuri)

Obs Dacă $G = (\mathbb{Z}, +)$ - grup abelian $(\mathbb{Z}/n\mathbb{Z}, +) = (\mathbb{Z}_n, +)$

(Fie $n \geq 2$) $n\mathbb{Z} \trianglelefteq \mathbb{Z}$

grupul factor

definit anterior

Teorema fundamentală de izomorfism Fie $f: G \to G'$ este un morfism de grupuri atunci există un izomorfism de grupuri între $G/_{\mathrm{Ker} f}$ și $\mathrm{Im} f$ ($G/_{\mathrm{Ker} f} \simeq \mathrm{Im} f$) dat de

se notează

$$\bar{f} : G/_{\mathrm{Ker} f} \longrightarrow \mathrm{Im} f \qquad \bar{f}(\hat{x}) = f(x).$$