• Relații de echivalență pe un grup. Teorema Lagrange

Def: Fie G un grup și $H \leq G$. Fie $x, y \in G$.

a) Spunem că x este congruent la stânga modulo H cu y, și notăm asta cu $x \equiv_s y \pmod H \overset{def}{\Longleftrightarrow}$ $x^{-1}y \in H$.

b) -II ——— II ——— congruent la dreapta modulo H cu y și notăm $x \equiv_d y \pmod H \overset{def}{\Longleftrightarrow} xy^{-1} \in H$.

Propoziție: Fie $H \leq G$ un subgrup în grupul G. Atunci relația de congruență la stânga (resp. la dreapta) modulo H este o relație de <u>echivalență</u> pe mulțimea G.

Dem • <u>reflexivitatea</u>, i.e. $x \equiv_s x \pmod H$, $(\forall)\, x \in G$.

$\Longleftrightarrow x^{-1}x = 1 \in H$, căci $H \leq G$.

• <u>simetria</u>: Fie $x, y \in G$ a.î. $x \equiv_s y \pmod H \Rightarrow$
$x^{-1}y \in H \Rightarrow (x^{-1}y)^{-1} \in H \Rightarrow y^{-1}x \in H \Rightarrow$
$y \equiv_s x \pmod H$, i.e. relația e simetrică.

• <u>tranzitivitatea</u>: Fie $x, y, z \in G$ a.î. $x \equiv_s y \pmod H$, $y \equiv_s z \pmod H \Rightarrow x^{-1}y \in H$ și $y^{-1}z \in H$
$\Rightarrow (x^{-1}y)(y^{-1}z) = x^{-1}z \in H \Rightarrow x \equiv_s z \pmod H$,
i.e. relația e tranzitivă și deci $\equiv_s$ e relație de echivalență. Analog, $\equiv_d$ e relație de echivalență.

$\boxtimes$

Notații: Mulțimile factor față de cele două relații vor fi notate:

$$\left(G/_H\right)_s \overset{not}{=} G/_{\equiv_s (\mathrm{mod}\ H)}, \quad \left(G/_H\right)_d \overset{not}{=} G/_{\equiv_d (\mathrm{mod}\ H)}$$

Dacă $x \in G$, clasa sa de echivalență la stânga este

$$\hat{x}^s = \{y \in G \mid x^{-1}y \in H\} = \{y \in G \mid y \in xH\}$$
$$= \{xh \mid h \in H\} = xH$$

Analog, pentru relația la dreapta $\hat{x}^d = Hx$

Un sistem de reprezentanți pentru $\equiv_s (\mathrm{mod}\ H)$ s.n. transversală la stânga a lui G prin H.

Exemple: 1) Fie $H := \{1\} \leq G$. Atunci

$x \equiv_s y\ (\mathrm{mod}\ 1) \iff x^{-1}y \in \{1\} \iff x = y$

i.e. $\equiv_s$ coincide cu egalitatea. În acest caz

$\hat{x}^s = \{1\}x = \{x\}$ și $\left(G/_1\right)_s = \{\{x\} \mid x \in G\} \simeq G$

2) Fie $H := G \leq G$. Atunci:

$x \equiv_s y\ (\mathrm{mod}\ G)$ $(\forall)\ x, y \in G$, i.e. orice două elemente sunt echivalente. Pentru $x \in G$,

$\hat{x}^s = xG = G$ și $\left(G/_G\right)_s = \{G\} \simeq \{*\}$.

$= \hat{1}^s$

3) Fie $G = (\mathbb{Z}, +)$, $H = n\mathbb{Z} \leq \mathbb{Z}$, $n \in \mathbb{N}^*$, $n \geq 2$

Atunci $x \equiv_s y \pmod H \iff x \equiv_d y \pmod H$

$\overset{def}{\iff} y - x \in n\mathbb{Z} \iff n \mid y - x$, ceea ce este congruența obișnuită modulo n.

Deci, congruențele la stânga / dreapta modulo un subgrup generalizează congruența modulo n din teoria numerelor.

Propoziție - Definiție Fie G un grup și $H \leq G$. Atunci mulțimile $(G/H)_s$ și $(G/H)_d$ sunt cardinal echivalente, i.e. $(\exists)$ $\varphi : (G/H)_s \xrightarrow{\sim} (G/H)_d$ o funcție bijectivă.

Numărul cardinal $|(G/H)_s| = |(G/H)_d| \overset{not}{=} |G:H|$ și s.n. indicele lui H în G.

Dem: Definim $\varphi : (G/H)_s \longrightarrow (G/H)_d$

$$\varphi(xH) \overset{def}{:=} Hx^{-1}, \quad (\forall)\ xH \in (G/H)_s$$

Afirm: φ este corect definită și bijectivă.

• φ e corect definită. Fie $xH = yH \implies$

$x \equiv_s y \pmod H \implies x^{-1}y \in H$

Vrem să arătăm că $\varphi(xH) = \varphi(yH)$ i.e. $Hx^{-1} = Hy^{-1}$

$\iff x^{-1} \equiv_d y^{-1} \pmod H \overset{def}{\iff} x^{-1}(y^{-1})^{-1} = x^{-1}y \in H$

ceea ce este, deci φ e corect definită.

Pe scurt : $x \equiv_s y \pmod H \iff x^{-1} \equiv_d y^{-1} \pmod H$. $(*)$

• φ e bijectivă şi inversa sa este

$$\psi : (G/H)_d \longrightarrow (G/H)_s, \quad \psi(Hy) := y^{-1}H,$$
$$(\forall)\ Hy \in (G/H)_d$$

ψ e și ea corect definită din $(*)$ și pentru $x \in G$ avem:

$$(\psi \circ \varphi)(\underline{xH}) = \psi(Hx^{-1}) = (x^{-1})^{-1}H = \underline{xH},$$
$$(\varphi \circ \psi)(\underline{Hx}) = \varphi(x^{-1}H) = H(x^{-1})^{-1} = \underline{Hx}$$

i.e. $\psi \circ \varphi = \mathrm{Id}$, $\varphi \circ \psi = \mathrm{Id}$. $\boxtimes$

<u>Exemple</u> : Dacă $n \in \mathbb{N}$, $n \geq 2 \Rightarrow |\mathbb{Z} : n\mathbb{Z}| = n$ şi $|\mathbb{Q} : \mathbb{Z}| = \infty$. (Exerciţiu!)

<u>Definiţie</u> : Spunem că un subgrup H într-un grup G are <u>indice finit</u> dacă $|G : H|$ este un număr natural. În caz contrar, ~~spu~~ spunem că H are <u>indice infinit</u> în G şi scriem $|G : H| = \infty$

<u>Obs</u>: Dacă ~~este~~ este un grup finit $\Rightarrow |G : H|$ este finit $(\forall)\ H \leq G$; căci mulţimea factor $(G/H)_s$ e finită. (orice mulţime factor a unei mulţimi finite este finită !).

Teorema (Lagrange, 1771)

Fie G un grup finit și $H \leq G$ un subgrup în G. Atunci

$$|G| = |H| \cdot |G:H|$$

În particular, $|H|$ divide $|G|$.

Curiozități istorice: Lagrange nu a demonstrat teorema care îi poartă numele! În 1771 nici nu exista conceptul de grup. Lagrange a arătat, ceea ce azi am putea numi caz particular, pentru $G = S_3$, grupul de permutări. Gauss în 1801 a demonstrat teorema de mai sus pentru $G = (\mathbb{Z}_p^*, \cdot)$, p = nr. prim. Cauchy în 1844 a demonstrat teorema pentru $G = S_n$. Camille Jordan în 1861 a demonstrat teorema Lagrange în forma de mai sus.

Demonstrație. Presupunem că $|G:H| = t$ și fie $\{x_1, \dots x_t\}$ o transversală la stânga a lui G prin H (i.e. un sistem de reprezentanți pentru $\equiv_s (\mathrm{mod}\, H)$).

$$\Rightarrow \left(G/_H\right)_s = \{x_1 H, \dots, x_t H\}.$$

Cum, mulțimea factor $\left(G/_H\right)_s$ formează o partiție a lui G avem că $G = \bigcup_{i=1}^{t} x_i \cdot H \Longrightarrow$

$$|G| = \sum_{i=1}^{t} |x_i \cdot H| \qquad (*)$$

- Afirm: $|x_i H| \overset{?}{=} |H|$, $(\forall)\ i = \overline{1,n}$

In adevăr, funcția $\varphi : H \xrightarrow{\sim} x_i H$,
$\varphi(h) := x_i h$, $(\forall) h \in H$ este bijectivă (Exercițiu)
$\Rightarrow |H| = |x_i H|$, $(\forall) i = \overline{1,t}$. Revenind în formula $(*)$ obținem:

$$|G| = \underbrace{|H| + \dots + |H|}_{\text{de } t \text{ ori}} = t\,|H| = |G:H| \cdot |H| \qquad \boxtimes$$

Corolar (tranzitivitatea indicelui) Fie G un grup finit și $K \leq H \leq G$. Atunci:

$$|G:K| = |G:H| \cdot |H:K|.$$

Dem. Aplicăm de ~~două~~ trei ori teorema Lagrange:

$$|G| = |H| \cdot |G:H| = \cancel{|K|} \cdot |H:K| \cdot |G:H| = \cancel{|K|} \cdot |G:K|$$

$$\Rightarrow |G:K| = |H:K| \cdot |G:H|. \qquad \boxtimes$$

Consecință: Fie p = număr prim, G un grup finit, $K \leq G$ a.î. $|G:K| = p$. Fie $H \leq G$ a.î.

$$K \leq H \leq G \Rightarrow H = K \text{ sau } H = G.$$

In adevăr, din corolar obținem:

$$p = |G:H| \cdot |H:K|.$$ Cum p e prim obținem:

- $|G:H| = 1 \Rightarrow H = G$

sau

- $|H:K| = 1 \Rightarrow H = K$. $\boxtimes$

Def: Un grup G s.n. ciclic dacă $(\exists)\ g \in G$ a.î. $G = \langle g \rangle = \{ g^n \mid n \in \mathbb{Z} \}$.

Exemple a) $(\mathbb{Z}, +)$ e grup ciclic căci $\mathbb{Z} = \langle 1 \rangle$

b) $(\mathbb{Z}_n, +)$ e ciclic, $\mathbb{Z}_n = \langle \hat{1} \rangle$.

c) $(\mathbb{Z} \times \mathbb{Z}, +)$, $(\mathbb{Q}, +)$ nu sunt ciclice (Exercițiu!)

Corolar: Fie p = număr prim și G un grup, $|G| = p$. Atunci G este ciclic.

Dem: Fie $1 \neq g \in G$ (există așa ceva căci $p \geq 2$) și $H \stackrel{def}{=} \langle g \rangle \leq G$. Atunci $H \neq \{1\}$, căci $g \in H$ și $|H| \mid p = \text{prim} \Rightarrow |H| = p \Rightarrow H = G$ i.e. $G = \langle g \rangle$, e ciclic. ☒

• Subgrupuri normale

Definiție (Galois) Fie G un grup și $H \leq G$ un subgrup al său. Atunci H s.n. subgrup normal al lui G (și notăm asta $H \trianglelefteq G$) dacă $xHx^{-1} \subseteq H$, $(\forall) x \in G$ i.e. $(\forall)\ x \in G$ și $(\forall)\ h \in H$ avem că $xhx^{-1} \in H$.

Exemple și Exerciții:

1) Dacă G = grup abelian $\Rightarrow$ orice subgrup al său este abelian.

2) $\{1\} \trianglelefteq G$ și $G \trianglelefteq G$.

3) Dacă $f : G_1 \to G_2$ e morfism de grupuri $\Longrightarrow$ $Ker(f) \trianglelefteq G_1$ (Exercițiu!)

4) Fie G un grup și $Aut(G)$ grupul automorfismelor sale (grup cu compunerea uzuală). Reamintim că

$f \in Aut(G) \overset{def}{\Longleftrightarrow} f : G \to G$ e morfism bijectiv.

Pentru $g \in G$, fie $\tau_g : G \to G$, $\tau_g(x) := g x g^{-1}$, $(\forall)\, x \in G$. Atunci, $\tau_g \in Aut(G)$, $(\forall)\, g \in G$ (Exercițiu) numit automorfism interior al lui G.

Definim funcția:

$$f : G \longrightarrow Aut(G), \quad f(g) := \tau_g, \ (\forall)\, g \in G.$$

Astfel că:

a) f este morfism de grupuri ($\tau_g \circ \tau_h = \tau_{gh}$, $(\forall)\, g, h$

b) $H \trianglelefteq G \Longleftrightarrow \tau_g(H) \subseteq H$, $(\forall)\, g \in G$.

c) $Ker(f) = \{g \in G \mid gx = xg, (\forall)\, x \in G\} \overset{not}{=} Z(G)$ s.n. centrul grupului G.

d) $Im(f) = \{\tau_g \mid g \in G\} \overset{not}{=} Inn(G)$ s.n. grupul automorfismelor interioare ale lui G.

Astfel că $Inn(G) \trianglelefteq Aut(G)$

($\sigma \in Aut(G)$ și $g \in G \Longrightarrow \sigma \circ \tau_g \circ \sigma^{-1} = \tau_{\sigma(g)}$)

5) Dacă $(H_i)_{i\in I}$ e o familie de subgrupuri normale în G = grup $\Longrightarrow \bigcap_{i\in I} H_i \trianglelefteq G$.

6) Fie $H := \{e, (1\,2)\} \leq S_3$. Atunci $H \ntrianglelefteq S_3$ căci: $(1\,3)(1\,2)(1\,3)^{-1} = (2\,3) \notin H$.

7) Fie $H \leq G$ și definim:

$$H_G := \bigcap_{g\in G} (gHg^{-1})$$

Arătați că $H_G \trianglelefteq G$ (numit inima sau interiorul normal al lui H în G) și este "cel mai mare" subgrup normal al lui G conținut în H. $\boxtimes$

Propoziție Fie G un grup și $H \leq G$ un subgrup al său. S.E.A ("sunt echivalente afirmațiile"):

a) $H \trianglelefteq G$

b) $xHx^{-1} = H$, $(\forall)\, x \in G$.

c) $xH = Hx$, $(\forall)\, x \in G$.

d) $(G/H)_s = (G/H)_d$.

Dem a) $\Rightarrow$ b) cum $H \trianglelefteq G \Rightarrow xHx^{-1} \subseteq H$, $(\forall)\, x \in G$. Mai: dar și $x^{-1}Hx \subseteq H$, $(\forall)\, x \in G$.

$$H = 1H1 = xx^{-1}Hxx^{-1} = x\underbrace{(x^{-1}Hx)}_{\subseteq H}x^{-1} \subseteq xHx^{-1}$$

i.e. $H \subseteq xHx^{-1} \subseteq H \Rightarrow xHx^{-1} = H$.

b) $\Rightarrow$ a) trivial.

b) $\Rightarrow$ c) $\underline{xH} = xH(x^{-1}x) = (xHx^{-1})x = \underline{Hx}$, $\forall x \in G$

c) $\Rightarrow$ d) trivial.

d) $\Rightarrow$ a). Fie $x \in G$. Atunci:

$xH \in (G/H)_s = (G/H)_d \Rightarrow (\exists)\, y \in G$ a.î.

$xH = Hy$. Dar,

$x = x1 \in xH = Hy \Rightarrow x \in Hy \Rightarrow Hx = Hy$

$\Rightarrow xH = Hx$. Deci:

$xHx^{-1} = (xH)x^{-1} = (Hx)x^{-1} = H1 = H$, i.e. $H \trianglelefteq G$. ☑

Corolar: Fie G = grup, $H \leq G$ cu $|G:H| = 2$

$\Rightarrow H \trianglelefteq G$.

__Dem__: Cum $|G:H| = 2$ și $H \in (G/H)_s \Rightarrow$

$(G/H)_s = \{H, G \setminus H\}$, căci $(G/H)_s$ e partiție a lui G și are două elemente. Analog

$(G/H)_d = \{H, G \setminus H\} = (G/H)_s \xRightarrow{\text{Prop.}} H \trianglelefteq G$. ☑

__Exemplu__ Cum $|S_n : A_n| = 2 \Rightarrow A_n \trianglelefteq S_n$. ☑

__Exercițiu facultativ__* Dacă $|G:H| = 3 \overset{?}{\Longrightarrow} H \trianglelefteq G$?

Propoziție Fie $f : G_1 \longrightarrow G_2$ morfism surjectiv de grupuri. Atunci, funcția:

$$F : \{ H \trianglelefteq G_1 \mid H \supseteq \ker(f) \} \xrightarrow{\sim} \{ K \mid K \trianglelefteq G_2 \}$$

$$F(H) := f(H)$$

este bijectivă.

Dem • F lucrează corect: i.e. dacă $H \trianglelefteq G_1$ $\Rightarrow f(H) \trianglelefteq G_2$. Știm deja că $f(H) \leq G_2$.

Fie $y \in G_2$ și $k \in f(H)$ $\underset{f=\text{surj}}{\Longrightarrow}$ $(\exists)\ x \in G_1$ a.î. $y = f(x)$ și $h \in H$ a.î. $k = f(h)$. Avem:

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

i.e. $f(H) \trianglelefteq G_2$.

• $K \trianglelefteq G_2 \Rightarrow f^{-1}(K) \trianglelefteq G_1$ și $f^{-1}(K) \supseteq \ker(f)$.

Știm deja că $f^{-1}(K) \leq G_1$ și $f^{-1}(K) \supseteq \ker(f)$.

Fie $x \in G_1$ și $h \in f^{-1}(K)$. Atunci

$$f(x h x^{-1}) = f(x) \underbrace{f(h)}_{\in K} f(x)^{-1} \in K, \text{ căci } K \trianglelefteq G_2$$

i.e. $x h x^{-1} \in f^{-1}(K)$.

• Faptul că F e bijectivă cu inversa $K \longrightarrow f^{-1}(K)$ se obține din teorema de corespondență pentru subgrupuri. $\boxtimes$

• Grup factor

Fie G un grup și $H \trianglelefteq G$ subgrup normal.

Notăm : $\boxed{G/_H \overset{not}{=} (G/_H)_s = (G/_H)_d}$

Fie $\hat{x} = xH$, $\hat{y} = yH \in G/_H$ și definim

$$\hat{x} \cdot \hat{y} :\overset{def}{=} \widehat{xy} \in G/_H \qquad (1)$$

• înmulțirea „·" este corect definită ? În adevăr,

Fie $\hat{x} = \widehat{x'}$ și $\hat{y} = \widehat{y'}$. Vrem : $\widehat{xy} \overset{?}{=} \widehat{x'y'}$.

$\hat{x} = \widehat{x'}$, $\hat{y} = \widehat{y'} \Rightarrow x^{-1}x' \in H$ și $y^{-1}y' \in H$

Vrem : $y^{-1}x^{-1}x'y' \overset{?}{\in} H$. În adevăr,

$$y^{-1}\underbrace{x^{-1}x'}_{\in H}y' \in y^{-1}Hy' = \underbrace{y^{-1}Hy}_{=H}y^{-1}y' =$$

$= Hy^{-1}y' \subseteq H$, i.e. forma (1) e corect defin.

În plus, pentru orice $x \in G$ avem:

•• $\hat{x} \cdot \hat{1} = \hat{1} \cdot \hat{x} = \hat{x}$, unde $\hat{1} = H$, i.e. $\hat{1}$ e element neutru pentru legea (1) și

•• $\hat{x} \cdot \widehat{x^{-1}} = \widehat{xx^{-1}} = \hat{1}$, $\widehat{x^{-1}} \cdot \hat{x} = \widehat{x^{-1}x} = \hat{1}$

i.e. $\hat{x}$ e inversabil cu inversul $\widehat{x^{-1}}$.

Rezumat; mai sus am demonstrat următoarea :

Propoziție: Fie G un grup și $H \trianglelefteq G$ subgrup normal. Atunci $G/_H$ are o structură de grup cu

$$\hat{x} \cdot \hat{y} := \widehat{xy}, \quad (\forall)\ \hat{x}, \hat{y} \in G/_H$$

numit grupul factor al lui G prin H. În plus,

$$\pi : G \longrightarrow G/_H, \quad \pi(x) := \hat{x}, \quad (\forall)\ x \in G$$

e morfism surjectiv de grupuri și $\mathrm{Ker}(\pi) = H$.

Dem: Faptul că „$\cdot$" e corect definită e demonstrat mai sus. Asociativitatea e banală, $1_{G/_H} = \hat{1} = H$ și $\hat{x}^{-1} = \widehat{x^{-1}}$, $(\forall)\ \hat{x} \in G/_H$. Pentru $x, y \in G$ avem:

$$\pi(xy) = \widehat{xy} \overset{(1)}{=} \hat{x} \cdot \hat{y} = \pi(x) \cdot \pi(y),$$ i.e. π e morfism

În final, $g \in \mathrm{Ker}(\pi) \Leftrightarrow \hat{g} = \hat{1} \Leftrightarrow g^{-1} \cdot 1 \in H$

$\Leftrightarrow g \in H$ i.e. $\mathrm{Ker}(\pi) = H$. ∎

Observații 1) Fie $H := \{1\} \trianglelefteq G$. Atunci $G/_{\{1\}} \simeq G$, căci $G/_{\{1\}} = \{\{x\} \mid x \in G\}$ iar

$$\pi : G \longrightarrow G/_{\{1\}}, \quad \pi(x) = \{x\}$$ este izo de grupuri.

Dacă $H := G \trianglelefteq G \Rightarrow G/_G \simeq \{1\}$ = grupul trivial cu un element, căci $G/_G$ are un singur element.

2) Fie $G := (\mathbb{Z}, +)$, $n \in \mathbb{N}$, $n \geq 2$ și $H := n\mathbb{Z} \leq \mathbb{Z}$.
Cum $\mathbb{Z}$ e abelian $\Rightarrow$ $H = n\mathbb{Z} \trianglelefteq \mathbb{Z}$ e subgrup normal în $\mathbb{Z}$. Grupul factor

$$\mathbb{Z}/_{n\mathbb{Z}} \overset{not}{=} \mathbb{Z}_n = \{\hat{0}, \hat{1}, \dots \widehat{n-1}\}$$

este grupul abelian al claselor de resturi modulo n cu operația:

$$\hat{a} + \hat{b} := \widehat{a+b}, \quad (\forall)\, \hat{a}, \hat{b} \in \mathbb{Z}_n.$$

3) Fie $H \trianglelefteq G$ și $\pi : G \longrightarrow G/_H$ proiecție canonică. Din teorema de corespondență pentru subgrupuri obținem:

$$\boxed{\begin{array}{l} K \leq G/_H \ (\text{resp. } K \trianglelefteq G/_H) \iff (\exists !) \\ L \leq G \ (\text{resp. } L \trianglelefteq G) \text{ cu } L \supseteq H = \mathrm{Ker}(\pi) \\ \text{a.î. } K = \pi(L) \overset{not}{=} L/_H = \{\hat{x} \mid x \in L\} \end{array}}$$

Scriem acest lucru astfel:

$$\boxed{\mathcal{L}(G/_H) = \{L/_H \mid L \leq G,\ L \supseteq H\}}$$

Caz special avem următorul:

$$\boxed{\begin{array}{l} \underline{\text{Exercițiu}} \quad \text{Fie } n \in \mathbb{N},\ n \geq 2. \text{ Arătați că:} \\ \mathcal{L}(\mathbb{Z}_n) = \{d\mathbb{Z}/_{n\mathbb{Z}} \mid d \in \mathbb{N},\ d \mid n\}. \\ \text{Listați toate subgrupurile lui } \mathbb{Z}_6, \mathbb{Z}_8, \mathbb{Z}_{12}. \end{array}}$$

Teoremă (Proprietatea de universalitate a grupului factor)

Fie G un grup, $H \trianglelefteq G$ și $\pi : G \to G/_H$ proiecția canonică, $\pi(g) = \hat{g}$, $(\forall)\, g \in G$. Atunci:

$$\begin{tikzcd} G \arrow[r, "\pi"] \arrow[d, "(\forall)\,\varphi"'] & G/_H \arrow[dl, dashed, "(\exists!)\,\overline{\varphi}"] \\ G' & \end{tikzcd}$$

$(\forall)\, G'$ un grup și $(\forall)\, \varphi : G \to G'$ morfism de grupuri cu $\underline{\ker(\varphi) \supseteq H}$

$(\exists!)\, \overline{\varphi} : G/_H \to G'$ morfism de grupuri a.î. $\overline{\varphi} \circ \pi = \varphi$, i.e. diagrama de mai sus este comutativă. În plus,

a) $\overline{\varphi}$ este surjectiv $\Longleftrightarrow$ φ este surjectiv.

b) $\overline{\varphi}$ este injectiv $\Longleftrightarrow$ $\ker(\varphi) = H$.

Dem • unicitatea lui $\overline{\varphi}$. Fie $\overline{\varphi} : G/_H \to G'$ morfism de grupuri a.î. $\overline{\varphi} \circ \pi = \varphi$ $\Longrightarrow$

$(\overline{\varphi} \circ \pi)(x) = \varphi(x)$, $(\forall)\, x \in G$ $\Longrightarrow$

$\overline{\varphi}(\hat{x}) = \varphi(x)$, $(\forall)\, x \in G$, i.e.

$\overline{\varphi}$ este unic determinat de φ.

• Existența lui $\overline{\varphi}$. Definim:

$\overline{\varphi} : G/_H \to G'$, $\underline{\overline{\varphi}(\hat{x}) := \varphi(x)}$, $(\forall)\, x \in G$.

• definiția lui $\overline{\varphi}$ este corectă:

$\hat{x} = \hat{y} \Longrightarrow x^{-1}y \in H \subseteq \ker(\varphi) \Longrightarrow$

$\varphi(x^{-1}y) = 1 \Longrightarrow \varphi(x)^{-1}\varphi(y) = 1 \Longrightarrow \underline{\varphi(x) = \varphi(y)}$, i.e. $\overline{\varphi}(\hat{x}) = \overline{\varphi}(\hat{y})$, și deci $\overline{\varphi}$ e corect definit.

- $\overline{\varphi}$ e morfism de grupuri ce închide diagrama comutativ:

$$\overline{\varphi}(\hat{x}\cdot\hat{y}) = \overline{\varphi}(\widehat{xy}) = \varphi(xy) = \varphi(x)\varphi(y)$$
$$= \overline{\varphi}(\hat{x})\,\overline{\varphi}(\hat{y})$$

i.e. $\overline{\varphi}$ e morfism și bineînț. $\overline{\varphi}\circ\pi = \varphi$.

a) „$\Rightarrow$" Pp. că $\overline{\varphi}$ e surjectiv $\Rightarrow \varphi = \overline{\varphi}\circ\pi$ este surjectivă fiind compunere de surjecții.

„$\Leftarrow$" Pp. că φ e surjectiv și fie $g' \in G' \Rightarrow$ $(\exists)\ x \in G$ a.î. $g' = \varphi(x) = \overline{\varphi}(\hat{x})$, i.e. $\overline{\varphi}$ e surjectiv.

b) „$\Rightarrow$" Pp. că $\overline{\varphi}$ e injectiv și fie $\underline{x \in Ker(\varphi)} \Rightarrow$ $\varphi(x) = 1 \Rightarrow \overline{\varphi}(\hat{x}) = 1 = \overline{\varphi}(\hat{1}) \Rightarrow$ $\hat{x} = \hat{1} \Rightarrow \underline{x \in H} \Rightarrow \underline{Ker(\varphi) = H}$.

„$\Leftarrow$" Pp. că $Ker(\varphi) = H$ și $\underline{\overline{\varphi}(\hat{x}) = \overline{\varphi}(\hat{y})} \Rightarrow$ $\varphi(x) = \varphi(y) \Rightarrow \varphi(xy^{-1}) = 1 \Rightarrow$ $xy^{-1} \in Ker(\varphi) = H \Rightarrow xy^{-1} \in H \Rightarrow \underline{\hat{x} = \hat{y}}$.

i.e. $\overline{\varphi}$ e injectiv. ∎

Teoremă (teorema fundamentală de izomorfism)

Fie $f : G \longrightarrow G'$ un morfism de grupuri. Atunci

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

este un <u>izomorfism</u> de grupuri. In particular, dacă

f e <u>surjectiv</u> $\Longrightarrow$ $G/_{Ker(f)} \simeq G'$.

<u>Dem</u>

$$\begin{tikzcd} G \arrow[r, "\pi"] \arrow[d, "u"'] & G/_{Ker(f)} \arrow[dl, dashed, "(\exists!)\, \overline{u} \overset{not}{=} \tilde{f}"] \\ Im(f) & \end{tikzcd}$$

Fie $u : G \longrightarrow Im(f)$, $u(x) \overset{def}{:=} f(x)$, corestricția lui f la $Im(f) \leq G'$.

Evident u e morfism de grupuri (căci așa este f) și u este <u>surjectiv</u>. In plus, <u>$Ker(u) = Ker(f)$</u>

Aplicând Prop. de universalitate $\Longrightarrow$
$(\exists!)\ \overline{u} \overset{not}{=} \tilde{f} : G/_{Ker(f)} \longrightarrow Im(f)$ un morfism de grupuri a.î. $\tilde{f} \circ \pi = u$, i.e.
$\tilde{f}(\hat{x}) = f(x)$, $(\forall)\ \hat{x} \in G/_{Ker(f)}$.

In plus, $\tilde{f}$ este surjectiv, căci u e surjectiv și $\tilde{f}$ e injectiv căci $Ker(u) = Ker(f)$ $\Longrightarrow$
$\tilde{f}$ este izomorfism de grupuri ■

Exemple 1) Fie $\mathbb{R} \leq (\mathbb{C}, +)$. Atunci $(\exists)$ un izomorfism de grupuri $\underline{\mathbb{C}/_{\mathbb{R}} \simeq (\mathbb{R}, +)}$.

Dem:

$$\begin{tikzcd}
\mathbb{C} \arrow[r, "\pi"] \arrow[d, "\varphi"'] \arrow[dr, phantom, "="] & \mathbb{C}/_{\mathbb{R}} \arrow[dl, dashed, "(\exists!)\ \overline{\varphi}"] \\
\mathbb{R} &
\end{tikzcd}$$

Fie $\varphi : \mathbb{C} \to \mathbb{R}$, $\varphi(a+bi) := b$, $(\forall)\ a, b \in \mathbb{R}$.

Atunci φ e morfism *surjectiv* de grupuri și $\mathrm{Ker}(\varphi) = \mathbb{R}$. Din P.U.G.F. $\Rightarrow$ $(\exists!)\ \overline{\varphi} : \mathbb{C}/_{\mathbb{R}} \to \mathbb{R}$ morfism de grupuri a.î. $\overline{\varphi}(\widehat{a+bi}) = b$, $(\forall)\ a, b \in \mathbb{R}$. În plus, $\overline{\varphi}$ este surjectiv (căci φ e surjectiv) și $\overline{\varphi}$ e injectiv căci $\mathrm{Ker}(\varphi) = \mathbb{R}$, i.e. $\overline{\varphi}$ e *izo*.

<u>Soluție alternativă</u> (folosind T.F.I.):

Fie $f : \mathbb{C} \to \mathbb{R}$, $f(a+bi) := b$ $\Rightarrow$ f e morfism *surjectiv* de grupuri cu $\mathrm{Ker}(f) = \mathbb{R}$

$\xRightarrow{\text{T.F.I.}}$ $(\exists!)\ \tilde{f} : \mathbb{C}/_{\mathbb{R}} \xrightarrow{\sim} \mathbb{R}$, $\tilde{f}(\widehat{a+bi}) = b$ un izo de grupuri.

2) Fie $\mathbb{Z} \leq (\mathbb{R}, +)$. Atunci există un izomorfism de grupuri $\underline{\mathbb{R}/_{\mathbb{Z}} \simeq (U, \cdot)}$, unde

$$U \overset{def}{:=} \{ z \in \mathbb{C} \mid |z| = 1 \} \leq (\mathbb{C}^*, \cdot)$$

Dem: $(U, \cdot) \leq (\mathbb{C}^*, \cdot)$ – temă!

Fie diagrama:

$$\begin{tikzcd} \mathbb{R} \arrow[r, "\pi"] \arrow[d, "\varphi"'] & \mathbb{R}/\mathbb{Z} \arrow[dl, dashed, "(\exists!)\overline{\varphi}"] \\ U & \end{tikzcd}$$

$\pi(r) = \hat{r}$

$\varphi : \mathbb{R} \longrightarrow U$,

$\varphi(r) := \cos(2\pi r) + i\sin(2\pi r)$

$(\forall)\ r \in \mathbb{R}$.

Atunci, φ e morfism surjectiv de grupuri și $\mathrm{Ker}(\varphi) = \mathbb{Z}$ (Exercițiu!) $\Longrightarrow$ P.U.G.F.

$(\exists!)\ \overline{\varphi} : \mathbb{R}/\mathbb{Z} \xrightarrow{\sim} U$, $\overline{\varphi}(\hat{r}) = \cos(2\pi r) + i\sin(2\pi r)$ morfism de grupuri a.î. $\overline{\varphi} \circ \pi = \varphi$. În plus, $\overline{\varphi}$ e izomorfism căci φ e surjectiv și $\mathrm{Ker}(\varphi) = \mathbb{Z}$.

Exercițiu: Arătați că există un izomorfism de grupuri

$$(\mathbb{Q}/\mathbb{Z}, +) \simeq (U_\infty, \cdot) \overset{def}{:=} \{ z \in \mathbb{C} \mid (\exists)\ n \in \mathbb{N}^*, z^n = 1 \}$$

3) Fie G un grup și $Z(G) = \{ g \in G \mid gx = xg, (\forall) x \in G \}$ centrul său. Atunci există un izomorfism de grupuri:

$$G/_{Z(G)} \simeq \mathrm{Inn}(G) = \text{grupul automorfismelor interioare ale lui } G.$$

Dem Am arătat anterior că aplicația:

$\tau : G \longrightarrow \mathrm{Inn}(G)$, $\tau(g) := \tau_g$, $(\forall) g \in G$

(unde $\tau_g : G \longrightarrow G$, $\tau_g(x) := g x g^{-1}$, $(\forall) x \in G$)

e un morfism de grupuri și $\mathrm{Im}(\tau) = \mathrm{Inn}(G)$

i.e. e surjectiv și $\mathrm{Ker}(\tau) = Z(G)$.

Din T.F.I. $\Longrightarrow$ $G/_{Z(G)} \simeq \mathrm{Inn}(G)$

$$\hat{g} \longmapsto \tau_g \qquad \blacksquare$$

· Teoreme facultative

Teoremă (teorema I de izomorfism pentru grupuri)

Fie $f : G_1 \longrightarrow G_2$ morfism surjectiv de grupuri și $H \trianglelefteq G_1$ a.î. $H \supseteq \mathrm{Ker}(f)$. Atunci $f(H) \trianglelefteq G_2$ și există un izomorfism de grupuri

$$G_2/_{f(H)} \simeq G_1/_H .$$

Dem: Faptul că $f(H) \trianglelefteq G_2$ am arătat anterior.

Fie morfismele de grupuri:

$$G_1 \xrightarrow{\ f\ } G_2 \xrightarrow{\ \pi\ } G_2/_{f(H)} \quad \text{și}$$

$f' := \pi \circ f : G_1 \longrightarrow G_2/_{f(H)}$ e morfism surjectiv de grupuri, $f'(x) = \widehat{f(x)}$, $(\forall) x \in G_1$.

Afirm: $\mathrm{Ker}(f') \overset{?}{=} H$

„$\subseteq$" Fie $x \in Ker(f')$ $\Rightarrow$ $f'(x) = \hat{1}$ $\Rightarrow$

$\widehat{f(x)} = \hat{1}$ $\Rightarrow$ $f(x) \in f(H)$ $\Rightarrow$

$(\exists)\ h \in H$ a.î. $f(x) = f(h)$ $\Rightarrow$

$f(x h^{-1}) = 1$ $\Rightarrow$ $x h^{-1} \in Ker(f) \subseteq H$

$\Rightarrow$ $x \in H$, i.e. $Ker(f') \subseteq H$.

„$\supseteq$" Fie $x \in H$ $\Rightarrow$ $f(x) \in f(H)$ $\Rightarrow$

$\widehat{f(x)} = \hat{1}$ $\Rightarrow$ $f'(x) = \hat{1}$ $\Rightarrow$ $x \in Ker(f')$

i.e. $Ker(f') = H$. Acum aplicăm T.F.I.

$\Rightarrow$ $G_1/_H \simeq G_2/_{f(H)}$. ∎

Observație Fie $H \trianglelefteq G$, $\pi : G \longrightarrow G/_H$ proiecția canonică și $K \trianglelefteq G$ a.î. $H \trianglelefteq K \trianglelefteq G$. Atunci (notăm $\pi(K) \overset{not}{=} K/_H \trianglelefteq G/_H$) există un izomorfism de grupuri:

$$\frac{G/_H}{K/_H} \simeq G/_K$$

Aplicăm efectiv Teorema 1 de izomorfism pentru

$f := \pi : G \longrightarrow G/_H$.

Caz special Fie $n, d \in \mathbb{N}^*$, $n \geq 2$ și $d \mid n$

Fie $G = (\mathbb{Z}, +)$, $H = n\mathbb{Z} \leq \mathbb{Z}$ şi $K = d\mathbb{Z} \leq \mathbb{Z}$. Avem $(d \mid n!)$

$n\mathbb{Z} \subseteq d\mathbb{Z} \trianglelefteq \mathbb{Z}$ şi există un izo de grupuri:

$$\frac{\mathbb{Z}/n\mathbb{Z}}{d\mathbb{Z}/n\mathbb{Z}} \simeq \mathbb{Z}/d\mathbb{Z}$$

$\blacksquare$

Teoremă (teorema II de izomorfism pentru grupuri)

Fie G un grup, $H, K \leq G$ a.î. $H \trianglelefteq \langle H \cup K \rangle$

Atunci:

a) $\langle H \cup K \rangle = HK$ şi $H \cap K \trianglelefteq K$.

b) Există un izomorfism de grupuri

$$HK/H \simeq K/H \cap K$$

Dem: Reamintim că $HK = \{hk \mid h \in H, k \in K\}$.

Pasul 1: $HK \leq G \overset{?}{\Longleftrightarrow} HK = KH$. În acest caz,

$\langle H \cup K \rangle = HK$.

Să demonstrăm acest pas.

"$\Rightarrow$" Pp. că $HK \leq G \Rightarrow HK = (HK)^{-1} =$

$= K^{-1}H^{-1} = KH$ i.e. $HK = KH$.

"$\Leftarrow$" Pp. că $HK = KH$. Atunci

$$(HK)(HK) = H(KH)K = H(HK)K = (HH)(KK) = HK \text{ și}$$

$$(HK)^{-1} = K^{-1}H^{-1} = KH = HK$$

$\Rightarrow HK \leq G$.

(aici am folosit o observație banală: o submulțime $L \subseteq G$ este subgrup în $G \iff LL = L$ și $L^{-1} = L$. Demonstrați această afirmație!)

A rămas de arătat că în acest caz $\langle H \cup K \rangle = HK$

Cum $HK \leq G$ și $H \subseteq HK$, $K \subseteq HK \Rightarrow H \cup K \subseteq HK \Rightarrow \langle H \cup K \rangle \subseteq HK$, căci $\langle H \cup K \rangle$ e cel mai mic subgrup în G ce conține $H \cup K$. Reciproc e banal: dacă $x = hk \in HK \Rightarrow x \in \langle H \cup K \rangle$ din propoziția care descrie elementele din subgrupul generat.

Pasul 1 este complet demonstrat.

Pasul 2: demonstrația teoremei.

a) Cum $H \trianglelefteq \langle H \cup K \rangle \Rightarrow Hk = kH$, $(\forall)\, k \in K$

$$\Rightarrow HK = \bigcup_{k \in K} Hk = \bigcup_{k \in K} kH = KH \xRightarrow{\text{Pasul 1}}$$

$HK \leq G$ și $\langle H \cup K \rangle = HK$.

Faptul că $H \cap K \trianglelefteq K$ e banal (din definiție și faptul că $H \trianglelefteq \langle H \cup K \rangle = HK$).

b) Fie morfismele de grupuri:

$$K \xrightarrow{i} HK \xrightarrow{\pi} HK/_H, \quad i(k) = 1k = k \in HK, \quad \pi(x) = \hat{x}$$

și $f := \pi \circ i : K \longrightarrow HK/_H$, $f(k) = \hat{k} = kH$

Afirm: Atunci f e morfism surjectiv de grupuri și $\mathrm{Ker}(f) = H \cap K$? ($\Rightarrow$ ok căci aplic T.F.I.)

$\underline{k \in \mathrm{Ker}(f)} \iff k \in K$ și $f(k) = \hat{1} \iff k \in K$ și $\hat{k} = \hat{1} \iff k \in K$ și $k \in H \iff \underline{k \in K \cap H}$

i.e. $\mathrm{Ker}(f) = H \cap K$.

Fie $x \in HK \Rightarrow x = hk, h \in H, k \in K \Longrightarrow$ $(\mathrm{Ker}(\pi) = H)$ $\underline{\pi(x)} = \pi(hk) = \pi(h)\pi(k) = \pi(k) = \underline{f(k)}$. Cum π e surjectiv $\Rightarrow f$ e surjectiv și deci $f : K \longrightarrow HK/_H$, $f(k) = \hat{k}$ e morfism surjectiv de grupuri cu $\mathrm{Ker}(f) = H \cap K$.

$\Longrightarrow$ T.F.I $(\exists)$ un izo de grupuri

$$K/_{H \cap K} \simeq HK/_H$$

$\blacksquare$

COMENTARII: Teorema I de izomorfism este o generalizare a "simplificării fracţiilor" din aritmetica elementară:

$$\frac{a/b}{c/b} = \frac{a}{c}$$ (vezi pag. 65, verso!)

Teorema II de izomorfism generalizează alt rezultat din aritmetica elementară şi anume: "dacă $m, n \in \mathbb{N}^*$, atunci $mn = (m,n)[m,n]$".
Să justificăm acest lucru!

Exerciţiu Fie $G = (\mathbb{Z}, +)$ şi $m, n \in \mathbb{N}^*$. Atunci

a) $m\mathbb{Z} + n\mathbb{Z} = (m,n)\mathbb{Z}$ şi $m\mathbb{Z} \cap n\mathbb{Z} = [m,n]\mathbb{Z}$

b) $\left| (m,n)\mathbb{Z}/n\mathbb{Z} \right| = \frac{n}{(m,n)}$, $\left| m\mathbb{Z}/[m,n]\mathbb{Z} \right| = \frac{[m,n]}{m}$.

Aplicăm acum teorema II de izomorfism pentru

$G := \mathbb{Z}$, $H := m\mathbb{Z}$, $K := n\mathbb{Z}$

$H + K = (m,n)\mathbb{Z}$, $H \cap K = [m,n]\mathbb{Z}$.

$$\Longrightarrow (m,n)\mathbb{Z}/n\mathbb{Z} \simeq m\mathbb{Z}/[m,n]\mathbb{Z}$$ (izo de grupuri)

$\Longrightarrow$ ele au acelaşi număr de elemente, i.e.

$$\frac{n}{(m,n)} = \frac{[m,n]}{m} \Longrightarrow mn = (m,n)[m,n].$$

$\boxtimes$

• Ordinul unui element.

Fie G = grup și $g \in G$. Fie funcție

$$\varphi_g : \mathbb{Z} \longrightarrow G, \quad \varphi_g(m) := g^m, \ (\forall) m \in \mathbb{Z}$$

Atunci φ_g e morfism de grupuri $\Longrightarrow$ $Ker(\varphi_g) \leq \mathbb{Z}$

$\Longrightarrow$ $(\exists!)\, n_g \in \mathbb{N}$ a.î.

$$Ker(\varphi_g) = \{m \in \mathbb{Z} \mid g^m = 1\} = n_g \mathbb{Z}$$

• $n_g = 0 \iff Ker(\varphi_g) = 0 \iff \varphi_g$ e injectiv

$\iff g^m \neq 1, \ (\forall) m \in \mathbb{Z} \setminus \{0\}.$

• $n_g = 1 \iff \{m \in \mathbb{Z} \mid g^m = 1\} = \mathbb{Z}$

$\iff g = 1_G.$

Definiție: Fie G un grup, $g \in G$ și

$\varphi_g : \mathbb{Z} \to G, \ \varphi_g(m) = g^m, \quad Ker(\varphi_g) = n_g \mathbb{Z}.$

a) Spunem că g are ordinul infinit și scriem $o(g) = \infty$, dacă $n_g = 0$; i.e. dacă

$g^m \neq 1, \ (\forall) m \in \mathbb{Z}, m \neq 0.$

b) Spunem că g are ordinul n_g și scriem $o(g) = n_g$, dacă $n_g \geq 1$.

Observații 1) Fie G grup, $g \in G$, a.î. $\sigma(g) = n \geq 1$. Atunci pentru $m \in \mathbb{N}$ avem:

$$\boxed{g^m = 1 \iff n \mid m}$$

În adevăr, $g^m = 1 \iff m \in \operatorname{Ker}(\varphi_g) = n\mathbb{Z} \iff (\exists)\, t \in \mathbb{Z}$ a.î. $m = nt \iff n \mid m$.

2) Cum $\sigma(g)$ este generatorul subgrupului $\operatorname{Ker}(\varphi_g)$, $\sigma(g)$ se poate redefini elementar astfel:

$$\boxed{\sigma(g) := \begin{cases} \infty, & \text{dacă } g^m \neq 1,\ (\forall)\, m \in \mathbb{Z} \setminus \{0\} \\ \min\{m \in \mathbb{N}^* \mid g^m = 1\}, & \text{dacă } (\exists)\, m \in \mathbb{Z}^* \text{ a.î. } g^m = 1. \end{cases}}$$

(**Exercițiu**: demonstrați această afirmație!)

Propoziție Fie G un grup și $g \in G$. Atunci

$$\sigma(g) = |\langle g \rangle|.$$

Dem Fie $\varphi_g : \mathbb{Z} \longrightarrow \langle g \rangle$, $\varphi_g(m) := g^m$, $(\forall)\, m \in \mathbb{Z}$. Atunci φ_g e morfism surjectiv de grupuri și fie $n \in \mathbb{N}$ a.î. $\operatorname{Ker}(\varphi_g) = n\mathbb{Z}$.

Din T.F.I. $\Longrightarrow$ există un izomorfism de grupuri

$$\mathbb{Z}/_{n\mathbb{Z}} \simeq \langle g \rangle.$$

• dacă $\underline{n=0} \Rightarrow \langle g\rangle \simeq \mathbb{Z}$, i.e. $|\langle g\rangle| = \infty = \sigma(g)$

• dacă $n>0 \Rightarrow \sigma(g)=n$ și $\langle g\rangle \simeq \mathbb{Z}/_{n\mathbb{Z}} = \mathbb{Z}_n$

i.e. $|\langle g\rangle| = n = \sigma(g)$. ▨

<u>Corolar</u> Fie G un grup <u>finit</u> și $g \in G$.
Atunci, $\underline{\sigma(g) \mid |G|}$ și $g^{|G|} = 1$.

<u>Dem</u>: $\sigma(g) = |\langle g\rangle| \mid |G|$ din teorema Lagrange
Faptul că $g^{|G|} = 1$ rezultă de aici și observația 1 ▨

• <u>Indicatorul lui Euler</u>: funcția $\varphi : \mathbb{N}^* \longrightarrow \mathbb{N}^*$,
$\varphi(n) :=$ numărul întregilor $1 \le k < n$ și primi cu n n.n. <u>indicatorul lui Euler</u>. I.e.

$$\varphi(n) := \left|\left\{ a \in \{1,2,\dots n-1\} \mid (a,n)=1\right\}\right|.$$

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

$$\varphi(n) = |U(\mathbb{Z}_n)|.$$

<u>Corolar (teorema lui Euler)</u> Fie $a, n \in \mathbb{N}^*$ numere naturale prime între ele. Atunci

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

Dem. Aplicăm corolarul precedent pentru grupul multiplicativ $G = (U(\mathbb{Z}_n), \cdot)$, $|G| = \varphi(n)$ și cum $(a, n) = 1 \Rightarrow$ $\hat{a}^{\varphi(n)} = \hat{1} \Rightarrow a^{\varphi(n)} - 1 \equiv 0 \pmod n$, i.e. $a^{\varphi(n)} \equiv 1 \pmod n$. ▨

Corolar (mica teoremă a lui Fermat)
Fie p un număr prim și $a \in \mathbb{N}$ nedivizibil cu p. Atunci

$$a^{p-1} \equiv 1 \pmod p$$

Dem: Dacă p = prim $\Rightarrow \varphi(p) = p-1$, $(a, p) = 1$ căci $p \nmid a$ și aplicăm teorema Euler. ▨

Exerciții 1) Fie $f, g \in \Sigma_{\mathbb{R}}$, $f(x) = -x+1$, $g(x) = -x$, $(\forall)\, x \in \mathbb{R}$. Arătați că în grupul permutărilor $(\Sigma_{\mathbb{R}}, \circ)$ avem că:

$$\sigma(f) = \sigma(g) = 2 \text{ și } \sigma(fg) = \sigma(gf) = \infty.$$

2) Fie $g \in G$, $\sigma(g) = n \geq 1$ și fie $k \in \mathbb{N}^*$.
Atunci: a) $\boxed{\sigma(g^k)} = \dfrac{n}{(n, k)}$.

b) g^k e generator în $\langle g \rangle \Leftrightarrow (n, k) = 1$

c) Numărul de generatori din $(\mathbb{Z}_n, +)$ este $\varphi(n)$.

- Grupuri ciclice

Reamintim că un grup G s.n. ciclic dacă $(\exists)\ g \in G$ a.î. $G = \langle g \rangle$.

Teoremă (de structură a grupurilor ciclice)

Fie G un grup ciclic. Atunci:

a) $G \simeq (\mathbb{Z}, +)$, dacă G este infinit

b) $G \simeq (\mathbb{Z}_n, +)$, dacă G e finit și $|G| = n$.

Dem. Fie $g \in G$ a.î. $G = \langle g \rangle$ și funcția

$$\varphi_g : \mathbb{Z} \longrightarrow G = \langle g \rangle, \quad \varphi_g(m) := g^m, \ (\forall) m \in$$

Atunci φ_g e morfism surjectiv de grupuri

Aplicând T.F.I $\Rightarrow$ există un izomorfism de grupuri

$$\mathbb{Z}/_{n_g \mathbb{Z}} \simeq G, \quad n_g \mathbb{Z} := \operatorname{Ker}(\varphi_g)$$

- Dacă $n_g = 0 \Rightarrow G \simeq \mathbb{Z}$.
- Dacă $n_g \geq 1 \Rightarrow G \simeq \mathbb{Z}_{n_g}$ și $n_g = o(g) = |\langle g \rangle| = |G|$. $\square$

Exercițiu Fie $p_1, \ldots p_n$ numere prime distincte și G = grup abelian, $|G| = p_1 p_2 \cdots p_n$. Atunci G este ciclic.

Propoziție (Lema chineză a resturilor)

Fie $m, n \in \mathbb{N}^*$, $(m, n) = 1$. Atunci

$$\varphi : \mathbb{Z}_{mn} \xrightarrow{\sim} \mathbb{Z}_m \times \mathbb{Z}_n$$

$$\varphi(\hat{x}) := (\bar{x}, \bar{\bar{x}}), \ (\forall)\, \hat{x} \in \mathbb{Z}_{mn}$$

este un izomorfism de grupuri.

Dem: • φ e corect definită

$\hat{x} = \hat{y} \Rightarrow mn \mid y - x \Rightarrow \left.\begin{array}{l} m \mid mn \mid y-x \\ n \mid mn \mid y-x \end{array}\right\} \Rightarrow$

$m \mid y-x$ și $n \mid y-x$ i.e. $\bar{x} = \bar{y}$ și $\bar{\bar{x}} = \bar{\bar{y}}$

$\Rightarrow \varphi(\hat{x}) = \varphi(\hat{y})$, i.e. φ e corect definită.

• φ e morfism de grupuri. (Ex!)

• φ este injectiv. Fie $\hat{x} \in Ker(\varphi) \Rightarrow$

$(\bar{x}, \bar{\bar{x}}) = (\bar{0}, \bar{\bar{0}}) \Rightarrow m \mid x, n \mid x \xRightarrow{(m,n)=1}$

$mn \mid x \Rightarrow \hat{x} = \hat{0}$, i.e. $Ker(\varphi) = \{0\}$ și deci

φ e injectiv.

Cum $|\mathbb{Z}_{mn}| = mn = |\mathbb{Z}_m \times \mathbb{Z}_n| \Rightarrow$

φ este și surjectivă i.e. φ e izo de grupuri

$\boxtimes$

Exerciții 1) Fie p = nr. prim și G un grup cu $|G| = p$. Atunci $G \simeq \mathbb{Z}_p$.

2) a) Fie $H_1 \leq G_1$, $H_2 \leq G_2 \Rightarrow H_1 \times H_2 \leq G_1 \times G_2$

b) Fie G un grup netrivial și $\mathrm{Diag}(G) = \{(g, g) \mid g \in G\}$. Atunci $\mathrm{Diag}(G) \leq G \times G$ și $\mathrm{Diag}(G) \neq H \times K$, $(\forall)\ H, K \leq G$.

3) Fie G = grup. Atunci $G \simeq H \times K \Leftrightarrow$ $(\exists)\ H_1 \trianglelefteq G$, $K_1 \trianglelefteq G$ a.î. $H_1 \simeq H$, $K_1 \simeq K$ și $G = H_1 K_1$, $H_1 \cap K_1 = 1$.

GRUPURI DE PERMUTĂRI

Dacă M e o mulțime nevidă am notat cu Σ_M sau S_M grupul de permutări pe M i.e.

$$\Sigma_M = S_M := \{ f : M \to M \mid f \text{ bijectivă} \}$$

care este grup (necomutativ dacă $|M| > 2$) cu compunerea uzuală a funcțiilor și $1_{S_M} = \mathrm{Id}_M$.

In particular, dacă $M = \{1, 2, \dots n\}$, $n \in \mathbb{N}^*$ atunci $S_{\{1,\dots,n\}} \overset{\text{not}}{\equiv} S_n$ s.n. <u>grupul permutărilor de grad n</u>. Evident $|S_n| = n!$ iar un element $\sigma \in S_n$ îl notăm ca un tabel

$$\sigma \overset{\text{not}}{=} \begin{pmatrix} 1 & 2 & \dots & n \\ \sigma(1) & \sigma(2) & & \sigma(n) \end{pmatrix}$$

Teorema lui Cayley demonstra că orice grup G (nu neapărat finit) se scufundă în grupul S_G. In particular, pentru grupuri finite avem:

Corolar Orice grup cu n elemente este izomorf cu un subgrup în S_n.

Definiție Fie $n \in \mathbb{N}$, $n \geq 2$ și $\sigma \in S_n$. O pereche (i, j), $i, j \in \{1, \dots n\}$ s.n. <u>inversiune</u> a lui σ dacă:

$$i < j \text{ și } \sigma(i) > \sigma(j)$$

Notație: $\mathrm{inv}(\sigma) \overset{\text{def}}{:=}$ numărul inversiunilor lui σ

Definiție Fie $n \geq 2$ și $\sigma \in S_n$. Numărul

$$\varepsilon(\sigma) \overset{def}{:=} \prod_{1 \leq i < j \leq n} \frac{\sigma(j) - \sigma(i)}{j - i} \qquad (1)$$

s.n. semnul (signature) lui σ.

Propoziție - Definiție Fie $n \geq 2$ și $\sigma \in S_n$. Atunci

$$\varepsilon(\sigma) = (-1)^{inv(\sigma)} \in \{-1, 1\}.$$

σ s.n. permutare pară (resp. impară) dacă $\varepsilon(\sigma) = 1$ (resp. $\varepsilon(\sigma) = -1$).

Dem: În adevăr, cum σ e bijectivă, orice factor $\sigma(j) - \sigma(i)$ cu $i < j$ de la numărătorul formulei (1) apare și la numitor, eventual cu semn schimbat. atunci când (i, j) este o inversiune.

Deci $\varepsilon(\sigma)$ este un produs de 1 și -1 și -1 apare de $inv(\sigma)$ ori. $\boxed{}$

Notăm $A_n := \{\sigma \in S_n \mid \varepsilon(\sigma) = 1\}$ s.n. grupul altern de grad n.

Definiție Fie $n \geq 2$ și $1 \leq i < j \leq n$. Permutarea $\tau_{ij} \overset{not}{=} (i\ j) \in S_n$ definită prin:

$$\tau_{ij}(k) := \begin{cases} k, & k \neq i,\ k \neq j \\ j, & k = i \\ i, & k = j \end{cases}$$

s.n. transpoziție.

Deci, o transpoziție $(i\ j)$ are forma:

$$(i\ j) = \begin{pmatrix} 1 & 2 & \dots & i & \dots & j & \dots & n \\ 1 & 2 & \dots & j & \dots & i & \dots & n \end{pmatrix}$$

Exercițiu: Arătați că $\underline{inv((i\ j)) = 2(j-i) - 1}$ și deci $\varepsilon(i\ j) = -1$.

Propoziție Fie $n \geq 2$. Atunci funcția signatură

$$\varepsilon : S_n \longrightarrow \{-1, 1\}, \quad \sigma \longmapsto \varepsilon(\sigma)$$

este un morfism surjectiv de grupuri, unde $(\{-1, 1\}, \cdot)$ este grupul cu înmulțirea uzuală. În particular, $\underline{A_n = \ker(\varepsilon) \trianglelefteq S_n}$ și $\boxed{|A_n| = \frac{n!}{2}}$.

Dem: Notăm $e \overset{not}{=} \mathrm{Id}_{\{1,\dots n\}}$ elementul unitate din grupul S_n (permutarea identică). Evident $\varepsilon(e) = (-1)^0 = 1$ și $\varepsilon(i, j) = -1$, $(\forall) i < j$ i.e. ε e funcție surjectivă. Fie acum $\sigma, \tau \in S_n$. Atunci, cum $\{\tau(1), \dots \tau(n)\} = \{1, \dots n\}$ putem scrie:

$$\varepsilon(\sigma) = \prod_{1 \leq i < j \leq n} \frac{\sigma(j) - \sigma(i)}{j - i} = \prod_{1 \leq i < j \leq n} \frac{\sigma(\tau(j)) - \sigma(\tau(i))}{\tau(j) - \tau(i)}$$

Avem:

$$\varepsilon(\sigma\tau) = \prod_{1\le i<j\le n} \frac{\sigma(\tau(j)) - \sigma(\tau(i))}{j-i} =$$

$$= \prod_{1\le i<j\le n} \frac{\sigma(\tau(j)) - \sigma(\tau(i))}{\tau(j) - \tau(i)} \cdot \prod_{1\le i<j\le n} \frac{\tau(j) - \tau(i)}{j-i} =$$

$= \varepsilon(\sigma)\,\varepsilon(\tau)$, i.e. ε e morfism de grupuri $\boxtimes$

<u>Definiție</u> Fie $n \geq 2$, $\sigma \in S_n$ și $k \in \{1, \dots n\}$.
Mulțimea

$$\mathcal{O}_\sigma(k) := \{\, \sigma^i(k) \mid i \in \mathbb{Z} \,\} =$$
$$= \{ k, \sigma(k), \sigma^{-1}(k), \sigma^2(k), \sigma^{-2}(k), \dots \}$$

s.n. <u>σ-orbita lui k</u>. $\mathcal{O}_\sigma(k)$ s.n. <u>trivială</u> dacă $\mathcal{O}_\sigma(k) = \{k\}$, i.e. dacă k e punct fix al lui σ $(\sigma(k) = k)$.

<u>Propoziție</u> Fie $n \geq 2$, $\sigma \in S_n$, $k \in \{1, \dots, n\}$. Fie $m \overset{def}{:=}$ cel mai <u>mic</u> număr natural nenul a.î. $\sigma^m(k) = k$

Atunci,

$$\mathcal{O}_\sigma(k) = \{ k, \sigma(k), \dots, \sigma^{m-1}(k) \}.$$

<u>Dem</u>: Mai întâi observăm că $(\exists)\ t \in \mathbb{N}^*$ cu $\sigma^t(k) = k$
căci mulțimea

$$\{ k, \sigma(k), \sigma^2(k), \dots, \sigma^r(k), \sigma^{r+1}(k), \dots \} \subseteq \{1, \dots n\}$$

i.e. este <u>finită</u> $\Longrightarrow (\exists)\ i < j$ a.î.

$$\sigma^i(k) = \sigma^j(k) \Longrightarrow \underline{\sigma^{j-i}(k) = k}.$$

Evident $\{k, \sigma(k), \dots, \sigma^{m-1}(k)\} \subseteq O_\sigma(k)$.

Reciproc, fie $\sigma^s(k) \in O_\sigma(k)$, cu $s \in \mathbb{Z}$.

Din împărțirea cu rest a numerelor $\Rightarrow (\exists)\ q, r \in$

a.î. $s = mq + r$, $0 \le r < m$ $\Rightarrow$

$$\sigma^s = \sigma^{mq+r} = \sigma^r \cdot (\sigma^m)^q \Rightarrow$$

$$\sigma^s(k) = \sigma^r(\sigma^m(k)^q) = \sigma^r(k) \in \{k, \dots, \sigma^{m-1}(k)\}$$

Fie acum $0 \le i < j < m$ și $\sigma^i(k) = \sigma^j(k) \Rightarrow$

$\sigma^{j-i}(k) = k \Rightarrow$ (cum e m minim) $j - i \geq m$,

fals! Deci, elementele mulțimii

$\{k, \sigma(k), \dots, \sigma^{m-1}(k)\}$ sunt diferite două câte două. ∎

<u>Exemplu</u> Fie $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 2 & 4 & 1 & 7 & 5 & 8 & 6 \end{pmatrix} \in S_8$.

σ-orbitele acestei permutări sunt:

$O_\sigma(1) = \{1, 3, 4\}$, $O_\sigma(2) = \{2\}$

$O_\sigma(5) = \{5, 7, 8, 6\} = O_\sigma(7) = O_\sigma(8) = O_\sigma(6)$

$O_\sigma(1) = O_\sigma(3) = O_\sigma(4)$, i.e. σ are <u>trei orbite</u>,

una <u>trivială</u> (cea a lui 2) și două <u>netriviale</u>. ∎

<u>Obs</u>: Fie $\sigma \in S_n$. Atunci toate orbitele sunt triviale (i.e. $O_\sigma(k) = \{k\}$, $(\forall)\ k = \overline{1,n}$)

$\Leftrightarrow \sigma = e$, permutarea identică.

Definiție Fie $n \geq 2$. O permutare $\sigma \in S_n$ s.n. ciclu dacă are o singură orbită netrivială, pe care o să o notăm cu O_σ. În acest caz, $\ell(\sigma) \overset{def}{=} |O_\sigma|$ s.n. lungimea ciclului σ.

Exemplu: Fie $\sigma \in S_n$. Atunci σ este ciclu de lungime doi $\Longleftrightarrow$ σ e o transpoziție.

Dem: „$\Leftarrow$" Pp. că $\sigma = (i\ j)$ este transpoziția (i, j). Atunci orbitele acestei permutări sunt: $O_\sigma(i) = O_\sigma(j) = \{i, j\}$ și $\sigma(k) = k$, $(\forall)\ k \neq i, j$ i.e. $\sigma = (i, j)$ are o singură orbită netrivială, și anume $\{i, j\}$ i.e. σ e ciclu de lungime 2.

σ = ciclu și $\ell(\sigma) = 2 \implies$

„$\Rightarrow$" Pp. σ are o_σ orbite: una de lungime 2, s-o notăm $\{i, j\}$, și restul sunt triviale i.e.

$O_\sigma(k) = \{k\}$, $(\forall)\ k \neq i, k \neq j$. $\implies$

$\sigma(k) = k$, $(\forall)\ j \neq k \neq i$ și $\sigma(i) = j$, $\sigma(j) = i$

i.e. $\sigma = (i\ j)$ $\square$

<u>Observație</u> Fie $\sigma \in S_n$ un <u>ciclu</u> și $\ell(\sigma) = m$.

Atunci, $O_\sigma = \{i, \sigma(i), \dots, \sigma^{m-1}(i)\}$,

unde $i \in \{1, \dots, n\}$ și $\sigma^m(i) = i$, m = minim cu prop.

Fie $i_1 := i$, $i_2 := \sigma(i)$, ... $i_m := \sigma^{m-1}(i)$

Atunci $i_\ell \neq i_k$, $(\forall)\ \ell \neq k$ și σ e dată de:

$$(*)\begin{cases} \sigma(i_1) = i_2,\ \sigma(i_2) = i_3, \dots, \sigma(i_{m-1}) = i_m,\ \sigma(i_m) = i_1 \\ \sigma(k) = k, \quad (\forall)\, k \in \{1, \dots n\} \setminus \{i_1, \dots i_m\} \end{cases}$$

<u>Reciproc</u>, dacă $\sigma \in S_n$ e dată de formule $(*) \Rightarrow$

σ e ciclu de lungime m și singura orbită netrivială este $O_\sigma = \{i_1, \dots i_m\}$.

<u>Notație</u>: vom nota ciclu dat de formule $(*)$ prin

$$\underline{\sigma = (i_1\, i_2 \dots i_m)}$$

<u>Def</u>. Doi cicli $\sigma, \tau \in S_n$ s.n. <u>disjuncți</u> dacă $O_\sigma \cap O_\tau = \phi$, i.e. dacă orbitele netriviale sunt mulțimi disjuncte.

<u>Propoziție</u> Fie $\sigma, \tau \in S_n$ doi cicli <u>disjuncți</u>.
Atunci, $\underline{\sigma\tau = \tau\sigma}$.

<u>Dem</u> Fie $i \in \{1, \dots n\}$ și vrem să arătăm $\sigma(\tau(i)) = \tau(\sigma(i))$. Avem două cazuri:

Cazul 1 : $i \notin O_\sigma \cup O_\tau \implies \sigma(i) = i$ şi $\tau(i) =$

$\implies (\sigma \circ \tau)(i) = \sigma(\tau(i)) = \sigma(i) = i$ şi

$(\tau \circ \sigma)(i) = \tau(\sigma(i)) = \tau(i) = i$ şi e ok.

Cazul 2 : $i \in O_\sigma \cup O_\tau$.

Putem presupune că $i \in O_\sigma$ (cazul celălalt e analog

$\implies i \notin O_\tau$ (căci sunt disjuncte) i.e. $\tau(i) = i$

$\sigma(\tau(i)) = \sigma(i)$ şi

$(\tau \circ \sigma)(i) = \tau(\sigma(i)) = \sigma(i)$, căci $\sigma(i) \in O_\sigma$

$\implies \sigma(i) \notin O_\tau$

i.e. şi în acest caz $(\sigma \circ \tau)(i) = (\tau \circ \sigma)(i)$. $\blacksquare$

Propoziţie : Fie $2 \leq m \leq n$ şi $\sigma = (i_1\, i_2 \ldots i_m) \in S_n$ un ciclu de lungime m. Atunci:

a) $\sigma^{-1} = (i_m\, i_{m-1} \ldots i_2\, i_1)$

b) $o(\sigma) = m = l(\sigma)$.

Dem a) Calcul direct:

$\sigma \sigma^{-1} = (i_1\, i_2 \ldots i_m)(i_m\, i_{m-1} \ldots i_2\, i_1) = e = \sigma^{-1}\sigma$.

b) $\sigma(i_1) = i_2 \neq i_1$, $\sigma^2(i_1) = i_3, \ldots, \sigma^{m-1}(i_1) = i_m$

$\implies \sigma^k \neq e$, $(\forall)\, k = 1, 2, \ldots m-1$. Arătăm

că $\sigma^m = e$ $(\implies o(\sigma) = m)$.

Dacă $j \notin \{i_1, \dots i_m\} \Rightarrow \sigma(j) = j \Rightarrow$

$\sigma^m(j) = j$.

$\sigma^m(i_1) = \sigma\left(\sigma^{m-1}(i_1)\right) = \sigma(i_m) = i_1$

i.e. $\sigma^m(i_1) = i_1$ și analog $\sigma^m(i_k) = i_k, (\forall) k$

In fapt ciclul $\sigma = (i_1 i_2 \dots i_m)$ se poate scrie și așa:

$$\sigma = (i_1 i_2 \dots i_m) = (i_2 i_3 \dots i_m i_1) = (i_3 i_4 \dots i_1 i_2) = \dots$$

$\Rightarrow o(\sigma) = m = \ell(\sigma)$. ∎

Exercițiu: Arătați că:

$$\sigma := (i_1 i_2 \dots i_m) \overset{?}{=} (i_1 i_2)(i_2 i_3) \dots (i_{m-1} i_m).$$

$$\Rightarrow \underline{\varepsilon\left((i_1 i_2 \dots i_m)\right)} = (-1)^{m-1} = \underline{(-1)^{\ell(\sigma)-1}},$$

$\Rightarrow$ ciclii de lungime $3, 5, 7, \dots$ sunt toate permutări pare.

Teoremă Fie $n \geq 2$ și $\sigma \neq e$, $\sigma \in S_n$. Atunci σ se poate descompune ca un <u>produs de cicli disjuncți</u>. Mai mult, abstracție făcând de ordinea termenilor, descompunerea e <u>unică</u>.

<u>Dem</u>: Cum $\sigma \neq e \Rightarrow \sigma$ are cel puțin o orbită <u>netrivială</u>.

Fie $O_1, O_2, \ldots, O_r$ toate orbitele netriviale ale lui σ. Conform propoziției de la pag 71 (verso) fiecare orbită netrivială O_i $(i=\overline{1,r})$ are forma

$$O_i = \{\alpha_i, \sigma(\alpha_i), \ldots, \sigma^{l_i-1}(\alpha_i)\} \overset{not}{=}$$

$$= \{\alpha_{i1}, \alpha_{i2}, \ldots, \alpha_{il_i}\}, \quad \underline{\sigma^{l_i}(\alpha_i) = \alpha_i}$$

Pentru fiecare $i=\overline{1,r}$ definim permutarea $\tau_i \in S_n$ a cărei singură orbită netrivială este O_i, astfel:

$$\tau_i(j) := \begin{cases} j, & \text{dacă } j \notin O_i \\ \sigma(j), & \text{dacă } j \in O_i \end{cases}$$

τ_i este un ciclu și $O_{\tau_i} = O_i$

Afirm: $\underline{\sigma \overset{?}{=} \tau_1\tau_2\ldots\tau_r}$. Să arătăm acest lucru:

Fie $k \in \{1, \ldots, n\}$. Avem două cazuri:

Cazul 1: Dacă $k \notin O_1 \cup \ldots \cup O_r \implies \underline{\sigma(k) = k}$.

Cum $k \notin O_1 \cup \ldots \cup O_r = O_{\tau_1} \cup \ldots \cup O_{\tau_r} \implies k \notin O_{\tau_i}$

$\implies \tau_i(k) = k$, $(\forall)\ i=\overline{1,n} \implies \underline{(\tau_1\tau_2\ldots\tau_r)(k) = k}$

Cazul 2: Dacă $k \in O_1 \cup \ldots \cup O_r \implies (\exists)\ s \in \{1, \ldots, r\}$

a.î. $k \in O_s$ și $k \notin O_t$, $(\forall)\ t \neq s$

(mulțimile $O_1, \ldots, O_r$ fiind orbitele lui σ sunt disjuncte două câte două)

Atunci avem:

$$(\tau_1\tau_2\dots\tau_r)(k) = \text{(ciclii disjuncți comută între ei)}$$

$$= (\tau_s \circ \tau_1 \circ \dots \circ \tau_{s-1} \circ \tau_{s+1} \circ \dots \tau_r)(k) = (\tau_t(k) = k,\ (\forall)\ t \neq s)$$

$$= \tau_s(k) \overset{k \in O_s}{=\!=} \sigma(k),$$ din definiția lui τ_s.

$\Rightarrow$ am arătat că $\sigma = \tau_1\tau_2\dots\tau_r$ și ciclii $\tau_1, \tau_2, \dots, \tau_r$ sunt disjuncți căci $O_{\tau_i} = O_i$, $(\forall)\ i = \overline{1,s}$ și $O_1, \dots, O_s$ sunt disjuncte două câte două.

<u>Unicitatea descompunerii</u>: Dacă $\sigma = \theta_1\theta_2\dots\theta_p$ e o altă descompunere a lui σ ca produs de <u>ciclii disjuncți</u> atunci <u>orbitele netriviale</u> ale lui σ sunt $O_{\theta_1}, \dots, O_{\theta_p}$. În adevăr, pentru

- $i \notin O_{\theta_1} \cup \dots \cup O_{\theta_p} \Rightarrow i$ e punct fix pentru fiecare ciclu $\theta_1, \dots, \theta_p \Rightarrow \sigma(i) = i$, ie $O_\sigma(i) = \{i\}$.
- $i \in O_{\theta_1} \cup \dots \cup O_{\theta_p}$. Pot presupune, eventual renumerotând, că $i \in O_{\theta_1} \Rightarrow \sigma(i) = \theta_1(i)$ (căci $\theta_g(i) = i$, $(\forall)\ g \geq 2$, ciclii fiind disjuncți)

$\Rightarrow O_\sigma(i) = O_{\theta_1}$.

Rezumat, dacă $\sigma = \zeta_1 \cdots \zeta_r = \theta_1 \cdots \theta_p$ sunt două descompuneri ale lui σ ca produse de cicli disjuncți $\Rightarrow$

$$\{ o_{\zeta_1}, \ldots, o_{\zeta_r} \} = \{ o_{\theta_1}, \ldots, o_{\theta_p} \} =$$

$= \{ o_1, \ldots, o_r \}$, căci ambele sunt orbitele netriviale ale lui σ. Rezultă că $\underline{r = p}$ și, eventual renumerotând, $\theta_i = \zeta_i$, $(\forall)\ i = \overline{1,r}$. (doi cicli, care au aceeași orbită netrivială coincid)

Teorema e complet demonstrată. $\boxtimes$

Exemple 1) Fie $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 5 & 4 & 1 & 6 & 7 & 8 & 2 \end{pmatrix} \in S_8$.

Atunci $\underline{\sigma = (1\,3\,4)(2\,5\,6\,7\,8)}$.

$o_\sigma(1) = \underline{\{1, 3, 4\}}$, $o_\sigma(2) = \underline{\{2, 5, 6, 7, 8\}}$

sunt singurele orbite netriviale.

2) Fie $\sigma' = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 3 & 5 & 1 & 4 & 7 & 10 & 8 & 2 & 6 & 9 \end{pmatrix} \in S_{10}$

Atunci $\underline{\sigma' = (1\,3)(2\,5\,7\,8)(6\,10\,9)}$. $\boxtimes$

COROLAR 1 Fie $n \geq 2$, $\sigma \in S_n$ și $\sigma = \zeta_1 \zeta_2 \cdots \zeta_r$, descompunerea ca produs de cicli disjuncți. Atunci

$o(\sigma) = [\ell(\zeta_1), \ldots, \zeta(\ell_r)]$, cel mai mic multiplu comun al lungimii ciclurilor componente.

Dem: Știm deja că $\sigma(z_i) = \ell(z_i)$, $(\forall)\ i=\overline{1,r}$.

și că $z_i z_j = z_j z_i$, $(\forall)\ i \neq j \in \{1, 2 \dots r\}$.

Fie $t := \sigma(\sigma)$ și $u := [\ell(z_1), \dots, \ell(z_r)]$.

Afirm: $t \overset{?}{=} u$. Să arătăm acest lucru.

Fie $m_i \in \mathbb{N}$ a.î. $u = \ell(z_i)\, m_i$, $(\forall)\ i=\overline{1,r}$.

Atunci:

$$\sigma^u = (z_1 \dots z_r)^u = (\text{cicli disjuncți comută între ei})$$

$$= z_1^u z_2^u \dots z_r^u = \Big(\underbrace{z_1^{\ell(z_1)}}_{e}\Big)^{m_1} \dots \Big(\underbrace{z_r^{\ell(z_r)}}_{e}\Big)^{m_r} = e,$$

permutarea identică. Deci $\sigma^u = e$ și cum $\sigma(\sigma) = t$

$\Rightarrow t \mid u$. Cum $\sigma(\sigma) = t \Rightarrow$

$$e = \sigma^t = (z_1 z_2 \dots z_r)^t = (\text{cicli disjuncți comută})$$

$$= z_1^t z_2^t \dots z_r^t \Rightarrow (\text{unicitatea descompunerii în cicli})$$

$z_i^t = e$, $(\forall)\ i=\overline{1,r} \Rightarrow \ell(z_i) = \sigma(z_i) \mid t$, $(\forall)\ i=$

$\Rightarrow u = [\ell(z_1), \dots, \ell(z_r)] \mid t \Rightarrow u \mid t$

$\boxtimes$

și deci $u = t$.

Exemple: Fie σ, σ' exemplele precedente. Atunci

$$\sigma(\sigma) = [3, 5] = 15, \quad \sigma(\sigma') = [2, 4, 3] = 12$$

$\boxtimes$

Corolar 2: Orice permutare $\sigma \in S_n$ este un produs de transpoziții (dar scrierea nu rămâne unică).

Dem: Din teorema precedentă plus descompunerea:

$$(i_1 i_2 \dots i_m) = (i_1 i_2)(i_2 i_3) \dots (i_{m-1} i_m) \qquad \boxtimes$$

Exerciții 1) Fie $n \geq 2$. Arătați că:

a) $S_n = \langle (12), (123\dots n) \rangle$

b) A_n se poate genera cu cicli de lungime 3.

Temă de referat: 1) Grupul liber generat de o mulțime.

Bibliografie: "Bazele algebrei" (C. Niță, C. Năstăsescu, C. Vraciu)

2) **Teorema Cauchy**: G = grup finit și p = nr. prim a.î. $p \mid |G| \Rightarrow (\exists)\, g \in G$ a.î. $o(g) = p$.

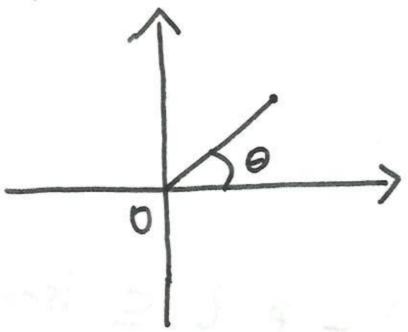
Bibliografie: "Algebră", T. Dumitrescu.

• GRUPUL DIEDRAL D_n

Fie un plan fixat pe care îl identificăm cu $\mathbb{R}^2 = \mathbb{R}\times\mathbb{R}$ și fixăm un sistem de coordonate. Am notat cu

$$\mathrm{Isom}(\mathbb{R}^2) := \{ f \in \Sigma_{\mathbb{R}^2} \mid f \text{ izometrie} \}$$

grupul de izometrii al planului (vezi 47).



Pentru $\theta \in [0, 2\pi)$ fie $f_\theta : \mathbb{R}^2 \to \mathbb{R}^2$ rotația cu centrul în O și unghi θ (în sens trigonometric), i.e.

$$f_\theta(x,y) := (x\cos\theta - y\sin\theta,\ x\sin\theta + y\cos\theta)$$

Fie $\varepsilon : \mathbb{R}^2 \to \mathbb{R}^2$ simetria (reflexia) față de axa Ox, i.e. $\varepsilon(x,y) := (x,-y)$, $(\forall)(x,y)\in\mathbb{R}^2$

Atunci: 1) $\varepsilon^2 = \mathrm{Id}_{\mathbb{R}^2}$

2) $f_\theta \circ f_{\theta'} = f_{\theta+\theta'}$ și $f_\theta^{-1} = f_{-\theta}$

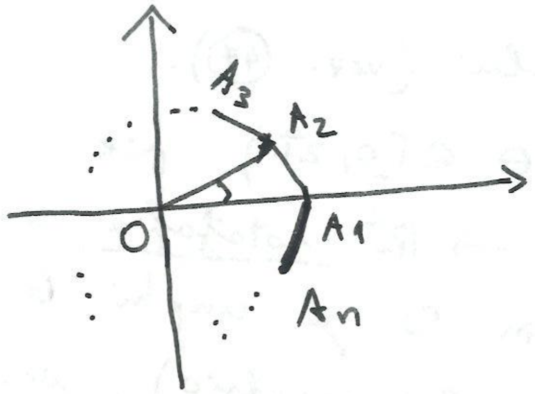
3) Fie $\rho := f_{\frac{2\pi}{n}}$, rotația de unghi $\frac{2\pi}{n}$, unde $n\in\mathbb{N}$, $n\geq 3$. Atunci:

$\rho^n = \mathrm{Id}_{\mathbb{R}^2}$, $o(\rho) = n$ și $\varepsilon\circ\rho = \rho^{n-1}\circ\varepsilon$

Exercițiu: verificați 1), 2) și 3).

Fie $P_n :=$ poligonul regulat cu n laturi. Alegând unitatea de măsură putem presupune că P_n are ~~latura~~ unul din vârfuri (A_1) este punctul $(1,0)$, i.e. $P_n = A_1A_2\dots A_n$ este

$$\sphericalangle A_1OA_2 = \frac{2\pi}{n}.$$



Teoremă Fie $n \in \mathbb{N}$, $n \geq 3$ și $D_n := \{\varphi \in \mathrm{Isom}(\mathbb{R}^2) \mid \varphi(P_n) = P_n\} \subseteq \mathrm{Isom}(\mathbb{R}^2)$.

Atunci, $(D_n, \circ)$ este un grup, $|D_n| = 2n$ și

$D_n = \{1, \rho, \dots, \rho^{n-1}, \varepsilon, \rho\varepsilon, \dots, \rho^{n-1}\varepsilon\}$, unde

ε este simetria față de axa Ox și $\rho =$ rotația cu centrul în O și unghi $2\pi/n$ i.e.

$o(\rho) = n$, $o(\varepsilon) = 2$, $\varepsilon\rho = \rho^{n-1}\varepsilon$.

În plus, $D_n \hookrightarrow S_n$ se scufundă în S_n.

Dem: Mai întâi remarcăm că

$$\{1, \rho, \rho^2, \dots \rho^{n-1}, \varepsilon, \rho\varepsilon, \dots \rho^{n-1}\varepsilon\} \subseteq D_n$$

și sunt diferite două câte două (Exercițiu!)

$\Rightarrow |D_n| \geq 2n$

Vom arăta acum că $|D_n| \overset{?}{\leq} 2n \;(\Rightarrow D_n =$ mulțimea descrisă mai sus$)$

$\boxed{\text{Afirm}}$: $\underline{\sigma \in D_n} \Rightarrow \underline{\sigma(O) = O}$.

Am presupus că $A_1 = (1,0)$, i.e. P_n e înscris în cercul unitate $\mathcal{C}(0,1) = U^1 \Rightarrow$

$$d(O, A) \leq 1, \quad (\forall)\, A \in P_n. \text{ Reciproc,}$$

dacă $O' \in \mathcal{P}$ a.î. $d(O', A) \leq 1$, $(\forall)\, A \in P_n$

$$\Rightarrow O' = O.$$

Fie acum $A' \in P_n \xRightarrow[\text{surj}]{\sigma\ \text{e}} (\exists)\, A \in P_n$ a.î. $A' = \sigma(A)$

$$\Rightarrow d(\sigma(O), A') = d(\sigma(O), \sigma(A)) = d(O, A) \leq 1$$

$$\Rightarrow d(\sigma(O), A') \leq 1, \; (\forall)\, A' \in P_n \Rightarrow \underline{\sigma(O) = O}$$

Dacă $A \in \{A_1, \dots, A_n\}$ este un vârf al poligonului

$$\Rightarrow \sigma(A) \in \{A_1, \dots A_n\}, \; (\forall)\, \sigma \in D_n \text{ căci}$$

$$d(O, \sigma(A)) = d(\sigma(O), \sigma(A)) = d(O, A) = 1$$

i.e. $\sigma(A) \in \{A_1, \dots A_n\}$, $(\forall)\, A \in \{A_1, \dots A_n\}$, $\sigma \in D_n$

Fie acum $\sigma \in D_n \Rightarrow \sigma(O) = O$ și $\sigma(A_1) \in \{A_1, \dots A_n\}$ poate fi ales în $\underline{n \text{ moduri}}$. Dacă am ales $\sigma(A_1) \Rightarrow \sigma(A_2)$ este "vecin" al lui $\sigma(A_1)$ căci σ păstrează distanțele:

$$d(\sigma(A_2), \sigma(A_1)) = d(A_2, A_1).$$

i.e. avem două moduri de a defini $\sigma(A_2)$, după ce am fixat $\sigma(A_1)$.

Acum folosim un rezultat de geometrie:
"două izometrii σ și τ ale planului sunt egale $\Leftrightarrow$ sunt egale în trei puncte necoliniare."

Cu alte cuvinte, $\sigma \in D_n$ este complet determinată de $\sigma(0)=0$, $\sigma(A_1)$ și $\sigma(A_2)$ $\Longrightarrow$ σ se poate defini în cel mult $2n$ moduri

$\Rightarrow$ $\underline{|D_n| \leq 2n.}$

$$\Longrightarrow D_n = \{1, \rho, \rho^2, \dots \rho^{n-1}, \varepsilon, \rho\varepsilon, \dots \rho^{n-1}\varepsilon\},$$

$$o(\rho)=n, \ o(\varepsilon)=2, \quad \varepsilon\rho = \rho^{n-1}\varepsilon.$$

În final, observăm că $\underline{D_3 = S_3}$ (i.e. grupul de izometrii al unui triunghi echilateral este S_3)

și în general:

$$f : D_n \longrightarrow S_n$$

$$f(\rho) := (1\,2 \dots n), \quad f(\varepsilon) := (1\,2)$$

se prelungește până la un <u>morfism injectiv</u> de grupuri prin formula:

$$f(\rho^i \varepsilon^j) := (1\,2 \dots n)^i (1\,2)^j, \quad (\forall)\ \substack{j=0,1 \\ i=0,\dots n-1}$$

$\boxtimes$