Legi de compoziție. Monoizi. Grupuri

Scurt istoric: Apariția conceptului de grup a fost un proces lent în secolul XIX și el s-a dezvoltat din trei direcții: teoria ecuațiilor algebrice, teoria numerelor și geometria de la începutul secolului XIX.

- teoria ecuațiilor algebrice, începută încă din antichitate a făcut un pas important în 1770 când Lagrange a studiat pentru prima dată permutările și a introdus ceea ce azi numim "rezolventa Lagrange". Ruffini în 1799 a fost primul care a încercat să demonstreze (demonstrația era greșită!) că nu orice ecuație de gradul 5 se poate rezolva prin radicali. Cauchy în 1815 a jucat un rol esențial în dezvoltarea teoriei permutărilor (el e cel care a definit semnul și ordinul unei permutări și a introdus noțiunea de ciclu). Abel în 1824 a dat o nouă demonstrație a faptului că nu orice ecuație de gradul 5 se poate rezolva prin radicali și demonstrația lui e considerată "acceptabilă". Rolul crucial l-a avut Galois în 1832 care a rezolvat complet problema și care a definit concepte de bază în teoria grupurilor (subgrupuri normale, clase de echivalență relativ la un subgrup etc.).

- teoria numerelor : Euler (1761) a studiat resturile a puterilor unui număr modulo n. Într-un caz special Euler a arătat primul că "ordinul unui element divide ordinul grupului". Gauss (1801) a continuat teoria lui Euler și a dezvoltat teoria grupurilor abeliene. El a arătat că pentru orice divizor al ordinului unui grup ciclic există un subgrup de ordin acel divizor;
- geometria : la începutul secolului XIX au apărut așa numitele "grupuri de simetrie" ale figurilor geometrice. Pionierii acestei direcții au fost Carnot, Poncelet, Lambert, Gauss (și a lui faimoasă construcție cu riglă și compasul a poligonelor ~~[illegible]~~ regulate cu 17 laturi). Aceste idei au condus la geneza "Programului de la Erlangen" (F. Klein 1872) care este, în linii mari, o metodă de a caracteriza geometria cu ajutorul teoriei grupurilor.

Rezumat : este greu de dat credit unui anume matematician care să fi definit primul conceptul de grup așa cum îl știm azi. Primul care a încercat o "definiție" abstractă a fost Cayley în 1854 care a clarificat grupurile de ordin ≤ 5. Tot Cayley, în 1878 a dat o altă definiție și anume:

"Un grup este definit de o lege de compoziție pe elementele sale".

care este extrem de vagă !

Burnside în 1897 a propus următoarea definiție pentru conceptul de grup:

"Fie A, B, C, ... o mulțime de operații care pot fi făcute pe același obiect sau mulțime de obiecte" care e la fel de vagă. Nu e clar că Cayley a impus rafinarea de "asociativitate" pentru legea de compoziție iar la Burnside (care o impune asociativitatea!) nu e clar dacă a impus condiția "elementului neutru". Kronecker în 1870 a dat o nouă definiție a noțiunii de grup din teoria algebrică a numerelor. La el grupurile erau abeliene. Hölder în 1893 a clasificat grupurile de ordin p^3, pq^2, pqr și p^4 (p, q, r = nr. prime) și a lansat celebra "problema a extinderilor" nerezolvată nici azi. Frobenius a avut contribuții majore în dezvoltarea teoriei reprezentărilor de grupuri (

Cam aceștia sunt "părinții" teoriei grupurilor și cei care au făcut ca teoria grupurilor să fie unul din cele mai studiate domenii ale matematicii în secolul XX.

• Legi de compoziție

Reamintim convenție : toate mulțimile sunt nevide în definițiile ce urmează !

Def 1) Fie A o mulțime. O funcție $\varphi : A \times A \longrightarrow A$ s.n. lege de compoziție pe A. Legea de compoziție $\varphi : A \times A \longrightarrow A$ s.n. asociativă dacă :

(A) $\varphi(a, \varphi(b,c)) = \varphi(\varphi(a,b), c)$, $(\forall)\ a,b,c \in A$

Un element $e \in A$ s.n. element neutru pentru $\varphi : A^2 \to A$ dacă

(N) $\varphi(e,a) = \varphi(a,e) = a$, $(\forall)\ a \in A$.

Notație : O lege de compoziție $\varphi : A^2 \to A$ se notează $\varphi((a,b)) \overset{not}{=} ab$ (notație multiplicativă) $\overset{not}{=} a+b$ (notație aditivă) $\overset{not}{=} a * b \overset{not}{=} a \circ b \overset{not}{=} a \perp b$ etc.

În notație multiplicativă ecuația (A) se scrie :

$a(bc) = (ab)c$, $(\forall)\ a,b,c \in A$

iar un element neutru s.n. cu 1_A sau 1 și condiție (N) se scrie : $1_A a = a 1_A = a$, $(\forall)\ a \in A$

În notație aditivă (A) se scrie $a + (b+c) = (a+b)+c$

iar elementul neutru, dacă există, s.n. cu 0_A sau 0

Exercițiu Arătați că elementul neutru pentru o lege de compoziție $\varphi : A^2 \to A$, dacă există, este unic.

Def 2: S.n. semigrup o pereche (S, φ), unde S = mulțime și $\varphi: S \times S \to S$ e o lege de comp. asociativă. S.n. monoid o pereche (M, φ), unde, M = mulțime și $\varphi: M \times M \to M$ e o lege de compoziție asociativă și care are element neutru.

Exemple: 1) $(\mathbb{N}, +)$, $(\mathbb{Z}, +)$, $(\mathbb{Q}, \cdot)$ etc sunt monoizi.

2) Fie A = mulțime. Atunci $(\mathcal{P}(A), \cup)$ și $(\mathcal{P}(A), \cap)$ sunt monoizi. Similar,

$Hom(A, A) := \{f: A \to A \mid f \text{ funcție}\}$ este monoid cu compunerea uzuală a funcțiilor și $1 = Id_A$.

• Legea asociativității generalizate (L.A.G.)

Fie $\varphi: A \times A \to A$ o lege de comp. și $n \in \mathbb{N}^*$. Definim recursiv funcțiile $\varphi_n: \underbrace{A \times A \times \ldots \times A}_{\text{de } n \text{ ori}} \to A$

astfel:

$\varphi_1 := Id_A$, $\varphi_2 := \varphi$ și presupunând că am definit φ_n, definim:

$$(1) \quad \boxed{\varphi_{n+1}(a_1, \ldots, a_{n+1}) \stackrel{def}{=} \varphi(\varphi_n(a_1, \ldots, a_n), a_{n+1})}$$

Teorema (L.A.G.) Fie $\varphi : A \times A \to A$ o lege de compoziție asociativă. Atunci, $(\forall)\, m, n \in \mathbb{N}^*$ și $(\forall)\, a_1, \dots a_{m+n} \in A$ avem:

$$(2) \quad \boxed{\varphi\left(\varphi_m(a_1, \dots, a_m), \varphi_n(a_{m+1}, \dots a_{m+n})\right) = \varphi_{m+n}(a_1, \dots a_{m+n})}$$

Dem: Inducție după n

$n=1$: O.K. $\varphi_1 = \mathrm{Id}_A$ iar formula (2) este exact definiția recursivă a lui φ_{m+1}.

$n \longmapsto n+1$: Pp. că (2) are loc pentru m și n. Atunci

$$\varphi\left(\varphi_m(a_1, \dots a_m), \varphi_{n+1}(a_{m+1}, \dots, a_{m+n+1})\right) \overset{(1)}{=\!=} (\text{def. lui } \varphi_{n+1})$$

$$= \varphi\Big(\underbrace{\varphi_m(a_1, \dots a_m)}_{a}, \varphi\big(\underbrace{\varphi_n(a_{m+1}, \dots, a_{m+n})}_{b}, \underbrace{a_{m+n+1}}_{c}\big)\Big)$$

$$\overset{\varphi \text{ e}}{\underset{\text{assoc.}}{=\!=}} \varphi\left(\varphi\left(\varphi_m(a_1, \dots a_m), \varphi_n(a_{m+1} \dots a_{m+n})\right), a_{m+n+1}\right)$$

= (pasul de inducție, i.e. (2) are loc pentru n)

$$= \varphi\left(\varphi_{m+n}(a_1, \dots, a_{m+n}), a_{m+n+1}\right) \overset{(1)}{=\!=}$$

$$= \varphi_{m+n+1}(a_1, \dots, a_{m+n+1})$$ i.e. (2) are loc

pentru m și $n+1$ ∎

Observație: 1) Fie $\varphi : A \times A \longrightarrow A$, $\varphi(a,b) \overset{not}{=} ab$

o lege de compoziție asociativă i.e. $(\forall)\, a,b,c \in A$ a

$$a(bc) = (ab)c \overset{not}{=} abc$$

Cum interpretăm L.A.G. și formula (2). Dacă

notăm $\varphi_n(a_1, \dots, a_n) \overset{not}{=} a_1 a_2 \dots a_n$ atunci (2) se

scrie:

$$\left[(a_1 \dots a_m)(a_{m+1} \dots a_{m+n}) = a_1 \dots a_{m+n} \right],$$

$(\forall)\, m, n \in \mathbb{N}^*$ și $a_1, \dots a_{m+n} \in A$ i.e. în

calculul lui $\varphi_{m+n}(a_1, \dots, a_{m+n}) = a_1 \dots a_{m+n}$

"nu contează unde punem parantezele" și deci le omitem!

De exemplu, pentru $n = 4$

$$(a_1 a_2)(a_3 a_4) = a_1(a_2(a_3 a_4)) = ((a_1 a_2) a_3) a_4 =$$

$$= a_1 (a_2 a_3) a_4 \overset{not}{=} a_1 a_2 a_3 a_4 .$$

2) (produs de funcții și reinterpretarea asociativității via diagrame).

Fie $f : A \longrightarrow B$, $g : C \longrightarrow D$ două funcții.

Atunci funcția $f \times g : A \times C \longrightarrow B \times D$,

definită prin $(f \times g)(a, c) := (f(a), g(c))$

$(\forall)\,(a,c) \in A \times C$ s.n. produsul funcțiilor f și g.

Exerciţiu O lege de compoziţie $\varphi : A\times A \to A$ este asociativă $\iff$ diagrama următoare

$$\begin{tikzcd}
A\times A\times A \arrow[r, "\varphi\times Id_A"] \arrow[d, "Id_A\times\varphi"'] \arrow[dr, phantom, "="] & A\times A \arrow[d, "\varphi"] \\
A\times A \arrow[r, "\varphi"] & A
\end{tikzcd}$$

este comutativă, i.e. $\varphi\circ(\varphi\times Id_A) = \varphi\circ(Id_A\times\varphi)$.

NOTAŢIE: O lege de compoziţie $\varphi : A\times A\to A$ va fi notată tot timpul multiplicativ, $\varphi(a,b) \overset{not}{=} ab$. Elementul neutru, dacă există, va fi notat cu 1_A sau 1.

Def: 1) Fie $(S_1,\cdot)$, $(S_2,*)$ două semigrupuri. O funcţie $f : S_1\to S_2$ s.n. morfism de semigrupuri dacă

$$f(x\cdot y) = f(x)*f(y),\quad (\forall)\ x,y\in S_1$$

2) Fie M_1 şi M_2 doi monoizi. O funcţie $f: M_1\to M_2$ s.n. morfism de monoizi dacă:

$$f(1_{M_1}) = 1_{M_2} \text{ şi } f(xy) = f(x)f(y),\ (\forall)\ x,y\in M_1$$

am renunţat deliberat la notaţiile cu $\cdot$ şi $*$ ca la 1)

Exemple 1) $(\mathbb{N},+)$ este un monoid; $(\mathbb{N}^*,+)$ e semigrup; $(\mathbb{N}^*,\cdot)$ este monoid; $(\mathbb{Z}_n,\cdot)$ e monoid cu $\hat{x}\cdot\hat{y} \overset{def}{:=} \widehat{xy}$, $(\forall)\ \hat{x},\hat{y}\in\mathbb{Z}_n$.

2) $f_a : (\mathbb{N}, +) \longrightarrow (\mathbb{N}^*, \cdot)$, $f_a(n) := a^n$ e morfism de monoizi ($a \in \mathbb{N}^*$, fixat).

Exerciții 1) Arătați că orice semigrup S se poate scufunda într-un monoid, i.e. $(\exists)$ M un monoid și $i : S \longrightarrow M$ morfism injectiv de semigrupuri.

2) $(\mathbb{Z}_4, \cdot)$ este un exemplu de monoid care nu se poate scufunda într-un grup. De ce?

Propoziție: Fie $f : M_1 \longrightarrow M_2$ morfism bijectiv de monoizi. Atunci $f^{-1} : M_2 \to M_1$ e morfism de monoizi.

Dem: Fie $x, y \in M_2$. Atunci:

$$f^{-1}(xy) = f^{-1}\left(f(f^{-1}(x))\, f(f^{-1}(y))\right) =$$

$$= f^{-1}\left(f\left(f^{-1}(x) f^{-1}(y)\right)\right) = \underbrace{(f^{-1} \circ f)}_{= \mathrm{Id}_{M_1}}\left(f^{-1}(x) f^{-1}(y)\right) =$$

$$= f^{-1}(x) f^{-1}(y) \text{ și}$$

$$f^{-1}(1_{M_2}) = f^{-1}(f(1_{M_1})) = \underbrace{(f^{-1} \circ f)}_{= \mathrm{Id}_{M_1}}(1_{M_1}) = 1_{M_1}. \quad \boxtimes$$

Def: Un morfism de monoizi $f : M_1 \to M_2$ s.n. izomorfism de monoizi dacă $(\exists)$ $g : M_2 \to M_1$ morfism de monoizi a.î. $f \circ g = \mathrm{Id}_{M_2}$ și $g \circ f = \mathrm{Id}_{M_1}$

Obs: $f : M_1 \to M_2$ este izomorfism de monoizi $\iff$ f este morfism bijectiv de monoizi. (Ex!)

Exerciții 1) Arătați că $i : (\mathbb{Z}, \cdot) \to (\mathbb{Q}, \cdot)$, $i(m) := m$, $(\forall) m \in \mathbb{Z}$ este epimorfism de monoizi care nu e surjectiv.

Doi monoizi M_1 și M_2 s.n. izomorfi dacă $(\exists)$ $f : M_1 \to M_2$ izomorfism de monoizi și în acest caz scriem $M_1 \simeq M$.

2) Sunt monoizii $(M_2(\mathbb{Z}), \cdot)$ și $(M_3(\mathbb{Z}), \cdot)$ izomorfi?

- Reguli de calcul într-un monoid.

Fie M un monoid notat multiplicativ cu elementul neutru 1. Pentru $x \in M$ și $n \in \mathbb{N}$ notăm:

$$x^0 := 1 \text{ și } x^n := \underbrace{x x \dots x}_{\text{de } n \text{ ori}}$$

(în notație aditivă, $0x := 0$, $nx = \underbrace{x + \dots + x}_{\text{de } n \text{ ori}}$!)

Atunci:

1) $x^m \cdot x^n = x^{m+n}$, $(\forall)\, m, n \in \mathbb{N}$
2) $(x^m)^n = x^{mn}$, — " —
3) Dacă $xy = yx \Rightarrow (xy)^n = x^n y^n$.

<u>Dem</u> 1) este exact L.A.G.

2) inducție după n. $n=1$ ok. $\underline{n \longmapsto n+1}$

$$(x^m)^{n+1} \stackrel{1)}{=} (x^m)^n \cdot x^m \stackrel{\text{inducție}}{=} x^{mn} \cdot x^m \stackrel{1)}{=}$$
$$= x^{mn+m} = x^{m(n+1)} \quad \text{ok.}$$

3) Temă !

• <u>Monoidul liber generat de o mulțime</u>

Fie A o mulțime nevidă; o numim "alfabet".

S.n. <u>cuvînt cu elemente din A</u> un sistem ordonat finit de elemente din A de forma

$$a_1 a_2 \dots a_n \qquad (n \in \mathbb{N})$$

Două cuvinte $x = a_1 a_2 \dots a_n$, $y = b_1 b_2 \dots b_t$ sunt <u>egale</u> $\stackrel{def}{\iff}$ $n = t$ și $a_i = b_i$, $(\forall)\ i = \overline{1,n}$.

Fie $\mathcal{L}(A) :=$ mulțimea tuturor cuvintelor cu elemente din A, incluzînd <u>cuvîntul vid</u> ϕ.

Atunci $\mathcal{L}(A)$ are o structură de monoid cu:

• $x = a_1 \dots a_n$, $y = b_1 b_2 \dots b_t$ definim

$$x \cdot y \stackrel{def}{:=} a_1 a_2 \dots a_n b_1 \dots b_t$$

numită <u>concatenarea cuvintelor</u>.

• $1_{\mathcal{L}(A)} := \phi$, i.e. $x \cdot \phi = \phi \cdot x = x$, $(\forall)\ x \in \mathcal{L}(A)$.

numit <u>monoidul liber generat de mulțimea A</u>.

Obs: 1) Dacă $A = \{a\} \Longrightarrow f : (\mathbb{N}, +) \xrightarrow{\sim} \mathcal{L}(A)$

$$f(n) := a^n = \underbrace{a\,a \dots a}_{\text{de } n \text{ ori}}$$ este izomorfism

de monoizi.

2) Dacă $A = \{a, b\}$, $a \neq b$ atunci $\mathcal{L}(A)$ e un monoid <u>necomutativ</u>, $ab \neq ba$. $\boxtimes$

<u>Teorema facultativă</u> (prop. de universalitate a monoidului liber generat). Fie A = mulțime nevidă și $\mathcal{L}(A)$ monoidul liber generat de A și $i : A \hookrightarrow \mathcal{L}(A)$ incluziunea canonică $i(a) := a \in \mathcal{L}(A)$.

$$\begin{tikzcd}
A \arrow[r, hook, "i"] \arrow[d, "(\forall) f"'] \arrow[dr, phantom, "="] & \mathcal{L}(A) \arrow[dl, dashed, "(\exists!) \overline{f}"] \\
M &
\end{tikzcd}$$

Atunci, $(\forall)$ M = monoid, $(\forall)$ $f : A \longrightarrow M$ o funcție $(\exists!)$ $\overline{f} : \mathcal{L}(A) \longrightarrow M$ morfism de monoizi a.î. $\overline{f} \circ i = f$.

<u>Dem</u> • <u>Unicitatea lui $\overline{f}$</u>. Fie $g : \mathcal{L}(A) \to M$ un morfism de monoizi a.î. $g \circ i = f \Longrightarrow$

$g(\phi) = g(1_{\mathcal{L}(A)}) = 1_M$ și pentru un cuvânt arbitrar $x = a_1 \dots a_n$ avem:

$$g(x) = \underline{g(a_1 a_2 \dots a_n)} = g(a_1) \cdot g(a_2) \cdot \dots \cdot g(a_n) =$$
$$= (g \circ i)(a_1) \cdot \dots \cdot (g \circ i)(a_n)$$
$$= \underline{f(a_1) \cdot f(a_2) \cdot \dots \cdot f(a_n)}$$, i.e. g e unic determinat de f.

• <u>Existența lui $\overline{f}$</u>. Definim $\overline{f} : \mathcal{L}(A) \longrightarrow M$ prin:

$$\overline{f}(\phi) := 1_M , \quad \overline{f}(a_1 a_2 \dots a_n) := f(a_1) \cdot \dots \cdot f(a_n)$$

$(\forall)\ a_1 a_2 \dots a_n \in \mathcal{L}(A)$ (prin „$\cdot$" am notat legea de compoziție din monoidul M). Atunci $\overline{f}$ este morfism de monoizi și $\overline{f} \circ i = f$. (Exercițiu) ☒

• <u>Elemente inversabile într-un monoid.</u>

<u>Def</u>: Fie $(M, \cdot)$ un monoid cu elementul neutru 1. Un element $a \in M$ s.n. <u>inversabil</u> dacă $(\exists)\ a' \in M$ a.î. $a a' = a' a = 1$.
<u>Notăm</u> $U(M) := \{ a \in M \mid a \text{ element inversabil} \}$.

<u>observație</u> Inversul unui element $a \in M =$ monoid, dacă există, este <u>unic</u> și se <u>notează</u> cu a^{-1}.
În adevăr, fie a' și a'' doi inverși pentru a; atunci avem:

$$a' = a' 1_A = a'(a a'') = (a' a) a'' = 1 a'' = a''$$

i.e. $a' = a''$.

<u>Exemple</u>: 1) $U((\mathbb{N}, +)) = \{0\}$; $U((\mathbb{Z}, \cdot)) = \{1, -1\}$;

2) $U((\mathbb{Z}_n, \cdot)) = \{ \hat{x} \in \mathbb{Z}_n \mid (x, n) = 1 \}$.

În adevăr, <u>$\hat{x} \in U(\mathbb{Z}_n)$</u> $\Longleftrightarrow (\exists)\ \hat{y} \in \mathbb{Z}_n$ a.î. $\hat{x} \cdot \hat{y} = \hat{1}$

$\Longleftrightarrow xy - 1 \equiv 0 (\text{mod } n) \Longleftrightarrow (\exists)\ a \in \mathbb{Z}$ a.î. $xy - 1 = an$

$\Longleftrightarrow (\exists)\ y \in \mathbb{Z}, a \in \mathbb{Z}$ a.î. $xy + an = 1 \Longleftrightarrow$

$\Longleftrightarrow$ <u>$(x, n) = 1$</u>

Propoziție Fie M un monoid și $x_1, \dots, x_n \in U(M)$ elemente inversabile. Atunci $x_1 x_2 \dots x_n \in U(M)$ și

$$(x_1 x_2 \cdots x_n)^{-1} = x_n^{-1} \cdots x_2^{-1} x_1^{-1}$$

Dem: Avem:

$$(x_1 x_2 \dots x_n)(x_n^{-1} \cdots x_2^{-1} x_1^{-1}) \overset{LAG}{=}$$

$$= x_1 x_2 \dots \underbrace{(x_n x_n^{-1})}_{=1} \dots x_2^{-1} x_1^{-1} = \dots = x_1 x_1^{-1} = 1$$

și analog $(x_n^{-1} \dots x_1^{-1})(x_1 \dots x_n) = 1$ $\boxtimes$

Observație: Dacă M e un monoid putem forma monoidul opus $(M^{op}, *)$, unde $M^{op} := M$ (ca mulțime) și legea de compoziție este

$$x * y := yx, \quad (\forall)\, x, y \in M^{op} = M.$$

Propoziția precedentă spune că funcția de luare a inversului

$$S : U(M) \xrightarrow{\sim} U(M)^{op}, \quad S(x) := x^{-1}$$

este un izomorfism de monoizi cu $S^2 = \mathrm{Id}_M$.

În adevăr, $S(xy) = (xy)^{-1} = y^{-1} x^{-1} = x^{-1} * y^{-1}$

$$= S(x) * S(y)$$

și $S(1) = 1^{-1} = 1$ i.e. S e morfism de monoizi.

$$S^2(x) = (x^{-1})^{-1} = x.$$

$\boxtimes$

• GRUPURI

Definiție S.n. grup un monoid $(G, \cdot)$ în care orice element este inversabil, i.e. $U(G) = G$.

Explicit un grup este un triplet $G = (G, \cdot, 1)$, unde G e o mulțime (nevidă), $\cdot : G \times G \longrightarrow G$ este o lege de compoziție, $1 \in G$ a.î.

a) $\cdot$ este asociativă, i.e. $x \cdot (y \cdot z) = (x \cdot y) \cdot z$, $(\forall)\ x, y, z \in G$.

b) 1 este element neutru pentru „$\cdot$" i.e. $x \cdot 1 = 1 \cdot x = x$, $(\forall)\ x \in G$

c) $(\forall)\ x \in G\ (\exists)\ y \in G$ a.î. $xy = yx = 1$.

În plus, un grup G s.n. abelian (sau comutativ) dacă legea de compoziție este comutativă i.e.

$$x \cdot y = y \cdot x, \quad (\forall)\ x, y \in G.$$

Exemple: 1) $(\mathbb{N}, +, 0)$ nu este grup, dar $(\{0\}, +, 0)$ e grup (grupul trivial: pe orice mulțime cu un element se poate defini o unică structură de grup).

2) $(\mathbb{Z}, +, 0)$, $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$ sunt grupuri abeliene.

3) $(\mathbb{Q}, \cdot, 1)$ nu este grup, dar $(\mathbb{Q}^* = \mathbb{Q} - \{0\}, \cdot, 1)$, $(\mathbb{R}^*, \cdot, 1)$ sunt grupuri.

4) M = monoid $\Longrightarrow (U(M), \cdot, 1)$ este un grup, numit grupul elementelor inversabile din M.

Notație: Ca și la monoizi legea de compoziție φ într-un grup G va fi notată multiplicativ $\varphi(x,y) \overset{not}{=} xy$ iar elementul neutru cu 1_G sau mai scurt cu 1.

Definiție Fie G_1, G_2 două grupuri. O funcție $f: G_1 \to G_2$ s.n. morfism de grupuri dacă $f(xy) = f(x)f(y)$, $(\forall)\, x, y \in G_1$. În plus, f s.n. izomorfism dacă $(\exists)\, g: G_2 \to G_1$ morfism de grupuri a.î. $f \circ g = Id_{G_2}$ și $g \circ f = Id_{G_1}$. Două grupuri G_1 și G_2 s.n. izomorfe și scriem asta $G_1 \simeq G_2$ dacă $(\exists)\, f: G_1 \to G_2$ un izomorfism de grupuri.

Exemple 1) $f: (\mathbb{Z}, +) \to (\mathbb{Z}, +)$, $f(n) = 3n$ este morfism de grupuri care nu e izomorfism.

2) $g: (\mathbb{R}, +) \xrightarrow{\sim} ((0, +\infty), \cdot)$, $g(x) := 2^x$ este izomorfism de grupuri.

3) $(\mathbb{R}, +) \not\simeq (\mathbb{R}^*, \cdot)$. În adevăr, pp. că $(\exists)$ $f: \mathbb{R}^* \to \mathbb{R}$ un izomorfism; atunci

$$0 = f(1) = f((-1)^2) = f((-1)(-1)) = f(-1) + f(-1)$$

$$= 2f(-1) \Rightarrow f(-1) = 0 = f(1)$$

$\Rightarrow$ (f e bijectivă) $-1 = 1$, fals! $\boxtimes$

Exercițiu: Arătați că inversul unui izomorfism de grupuri este tot izomorfism și compunerea a două morfisme de grupuri este tot morfism.

$\Rightarrow (Aut(G), \circ) := \{ f : G \to G \mid f$ izomorfism de grupuri$\}$ este un grup cu operația de compunere uzuală numit grupul automorfismelor grupului G; $1_{Aut(G)} = 1_G$

Exercițiu Determinați grupul $(Aut(\mathbb{Z}), \circ)$, unde $\mathbb{Z} = (\mathbb{Z}, +, 0)$ e grupul uzual.

Propoziție Fie $f : G_1 \longrightarrow G_2$ un morfism de grupuri. Atunci:
i) $f(1) = 1$; ii) $f(a^{-1}) = f(a)^{-1}$, $(\forall) a \in G_1$
iii) $f(a^n) = f(a)^n$, $(\forall) a \in G_1$, $n \in \mathbb{Z}$.

Dem: i) $f(1) = f(1 \cdot 1) = f(1) f(1) \Longrightarrow$

$\underbrace{f(1) f(1)^{-1}}_{=1} = f(1) \underbrace{f(1) f(1)^{-1}}_{=1} \Longrightarrow f(1) = 1$

ii) $f(a) f(a^{-1}) = f(a a^{-1}) = f(1) = 1$ și

$f(a^{-1}) f(a) = f(a^{-1} a) = f(1) = 1$

$\Rightarrow f(a)$ e inversabil și $f(a)^{-1} = f(a^{-1})$.

iii) $n = 0$, OK din i) Dacă $n > 0$ facem inducție după n

$n=1$ o.k. $\quad n \longmapsto n+1$

$$f(a^{n+1}) = f(a^n \cdot a) = f(a^n)\, f(a) \overset{\text{inducție}}{=} f(a)^n f(a) = f(a)^{n+1}, \text{ ok.}$$

Dacă $n<0$, atunci $n=-m$, $m>0$ și

$$f(a^n) = f\left((a^{-1})^m\right) = f(a^{-1})^m \overset{ii)}{=} \left(f(a)^{-1}\right)^m = f(a)^{-m} = f(a)^n \quad \square$$

Propoziție (transfer de structură) Fie G = grup, X = mulțime și $f: G \xrightarrow{\sim} X$ o funcție bijectivă. Atunci, $(\exists!)$ o structură de grup $*$ pe mulțimea X a.î. f este izomorfism de grupuri.

În acest caz, spunem că „$*$" se obține prin transferul structurii de grup de pe G pe X via f.

Dem: unicitatea: fie $\perp$ o structură de grup pe X a.î. $f: G \longrightarrow (X, \perp)$ e izo de grupuri, i.e. $f(gh) = f(g) \perp f(h)$, $(\forall)\ g,h \in G$

~~$\Rightarrow$ (aplic f^{-1}) $f^{-1}(f(x) \perp f(y)) = xy$~~

și $f^{-1}(x \perp y) = f^{-1}(x)\, f^{-1}(y)$, $(\forall)\ x,y \in X$

$\Rightarrow$ (aplic f peste relație și $f \circ f^{-1} = \mathrm{Id}_X$)

$$x \perp y = f\left(f^{-1}(x)\, f^{-1}(y)\right), \quad (\forall)\; x, y \in X$$

i.e. structura de grup pe X e <u>unic</u> determinată de f şi de structura de grup pe G.

<u>Existenţa</u> Definim $x * y := f\left(f^{-1}(x)\, f^{-1}(y)\right)$, $(\forall)\; x, y \in X$. Atunci, $(X, *)$ este un grup (Exerciţiu) cu $1_X := f^{-1}(1_G)$. ▨

<u>Exerciţii</u> 1) Folosind ipoteza continuumului arătaţi că pe orice mulţime $X \subseteq \mathbb{R}$ se poate defini o structură de grup (abelian). Generalizare.

2) Puneţi pe mulţimea $\mathbb{N}$ o structură de grup.

3) Puneţi pe —"— — $\mathbb{N}$ o structură de grup „$*$" a.î. $7 * 7 = 48$.

<u>Alte exemple de grupuri. (Grupuri necomutative)</u>

1) (<u>grupul simetric al unei mulţimi</u>) Fie X o mulţime nevidă şi

$$\Sigma_X := \{ f : X \longrightarrow X \mid f \text{ funcţie bijectivă} \}$$

Atunci Σ_X este un grup cu compunerea uzuală a funcţiilor cu $1_{\Sigma_X} = id_X$ numit <u>grupul simetric</u> al lui X sau <u>grupul de permutări</u> pe X. Dacă $|X| \geq 3$ atunci Σ_X este <u>necomutativ</u> (Exerciţiu!) Alte notaţii pt. el:

$$\Sigma_X \overset{not}{=} S_X \; \cancel{\overset{not}{=} Sym(X)}$$

Exercițiu: Fie $f : X \to Y$ o funcție bijectivă între două mulțimi. Arătați că $(\Sigma_X, \circ) \simeq (\Sigma_Y, \circ)$ (izomorfism de grupuri).

Dacă $X := \{1, 2, \dots n\}$ atunci $\Sigma_X \overset{not}{=} S_n$. Un s.n. <u>grupul permutărilor</u> de ordin n. Un element $\sigma \in S_n$ se notează prin valorile pe care le ia astfel:

$$\sigma = \begin{pmatrix} 1 & 2 & \dots & n \\ \sigma(1) & \sigma(2) & \dots & \sigma(n) \end{pmatrix}.$$

Un subgrup în Σ_X s.n. <u>grup de transformări</u>

2) (<u>grupuri geometrice</u>) Fie $X := \mathbb{R}^2 = \mathbb{R} \times \mathbb{R}$ mulțimea punctelor din plan.

O funcție $f : \mathbb{R}^2 \longrightarrow \mathbb{R}^2$ s.n. <u>izometrie</u> dacă păstrează distanțele dintre puncte, i.e.

$$d(f(P), f(Q)) = d(P, Q)$$

$(\forall)$ $P, Q \in \mathbb{R}^2$. Reamintim că, dacă $P = (x_1, y_1)$ și $Q = (x_2, y_2) \Rightarrow$

$$d(P, Q) := \sqrt{(x_1 - x_2)^2 + (y_1 - y_2)^2}$$

Exerciții de geometrie

1) Orice izometrie a planului este funcție bijectivă.

2) Inversa unei izometrii este tot izometrie și compunerea a două izometrii este tot izometrie

3) Orice izometrie a planului este o translație, rotație, simetrie față de o dreaptă sau o compunere dintre o translație și o simetrie.

4) Orice izometrie este compunerea a cel mult trei simetrii;

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

este un grup cu compunerea uzuală numit grupul de izometrii al planului. El este un subgrup în $\Sigma_{\mathbb{R}^2}$, i.e. $\mathrm{Isom}(\mathbb{R}^2)$ este un grup de transformări.

Caz special de izometrii : grupul rotațiilor

Fie $\theta \in [0, 2\pi)$ și $f_\theta : \mathbb{R}^2 \to \mathbb{R}^2$, $f_\theta :=$ rotație de unghi θ i.e.

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

$(\forall)\ (x, y) \in \mathbb{R}^2$. Fie

$$\mathrm{Rot}(\mathbb{R}^2) := \{ f_\theta \mid \theta \in [0, 2\pi) \} \leq \mathrm{Isom}(\mathbb{R}^2)$$

este un subgrup în $\mathrm{Isom}(\mathbb{R}^2)$ (Exercițiu!) numit grupul rotațiilor din planul $\mathbb{R}^2$.

- Grupul de simetrie a unei mulțimi $Y \subseteq \mathbb{R}^2$

Fie $Y \subseteq \mathbb{R}^2$ o submulțime fixată. Atunci

$$\underline{Sim(Y)} := \{ f \in Isom(\mathbb{R}^2) \mid f(Y) = Y \}$$

este subgrup în $Isom(\mathbb{R}^2)$ numit grupul de simetrie al lui Y.

Caz special (grupul diedral) Fie $n \geq 3$ și P_n := un poligon regulat cu n laturi fixat în plan. Atunci:

$$Sim(P_n) = \{ f \in Isom(\mathbb{R}^2) \mid f(P_n) = P_n \} \overset{not}{=} D_n \text{ grupul diedral}$$

Exerciții facultative (geometrice):
1)* Descrieți D_4 și arătați că are 8 elemente
2*) Descrieți explicit D_n și arătați că $|D_n| = 2n$.

3) ($GL_n(\mathbb{C})$ și $SL_n(\mathbb{C})$) Un rol important în matematică îl au grupurile următoare:

$$GL_n(\mathbb{C}) := \{ A \in M_n(\mathbb{C}) \mid A = \text{inversabilă} \}$$
$$SL_n(\mathbb{C}) := \{ A \in M_n(\mathbb{C}) \mid \det(A) = 1 \}$$

care sunt grupuri cu înmulțirea uzuală a matricilor și se numesc grupul general (resp. special) linear de ordin n.

Temă de REFERAT (Izometriile planului)

- Demonstrarea Exercițiilor 1)–4) pg. 47.

Bibliografie : G. Galbură, F. Radó : "Geometrie", EDP, 1979.

- Subgrupuri. Teorema de corespondență pentru subgrupuri

Def Fie $G = (G, \cdot)$ un grup și $H \subseteq G$ o submulțime. H s.n. subgrup în G (notăm $H \leq G$) dacă:

(1) H e parte stabilă a lui G; i.e. $(\forall)\ x, y \in H \Rightarrow xy \in H$.

(2) $1 \in H$

(3) Dacă $x \in H \Rightarrow x^{-1} \in H$.

Notăm $\mathcal{L}(G) \overset{def}{:=} \{ H \mid H \leq G \}$ ea este o latice (în raport cu relația de incluziune) numită laticea subgrupurilor lui G.

Exemple 1) $(\mathbb{Z}, +) \leq (\mathbb{Q}, +) \leq (\mathbb{R}, +) \leq (\mathbb{C}, +)$.

2) $\{1\} \leq G$, $G \leq G$ și ele s.n. subgrupurile triviale ale lui G. Un subgrup $H \leq G$, $H \neq \{1\}$ și $H \neq G$ s.n. subgrup propriu în G.

3) $Rot(\mathbb{R}^2) \leq Isom(\mathbb{R}^2) \leq \Sigma_{\mathbb{R}^2}$ (pg. 47)

Exercițiu Arătați că $H \leq (\mathbb{Z}, +) \Leftrightarrow (\exists!)\ n \in \mathbb{N}$ a.î. $H = n\mathbb{Z} := \{ nx \mid x \in \mathbb{Z} \}$.

Propoziție Fie $f : G_1 \longrightarrow G_2$ un morfism de grupuri.

Atunci:

a) Dacă $H \leq G_1 \Longrightarrow f(H) \leq G_2$.

b) Dacă $K \leq G_2 \Longrightarrow f^{-1}(K) \leq G_1$

Înainte de a demonstra propoziția facem următoarea:

Observație: Fie G = grup și $H \subseteq G$. Atunci

$$H \leq G \iff xy^{-1} \in H, \ (\forall)\ x, y \in H.$$

În adevăr „$\Rightarrow$" e trivială. „$\Leftarrow$" Dacă $x \in H \Rightarrow$ $1 = xx^{-1} \in H$ i.e. $1 \in H$; $x := 1$, $y \in H \Rightarrow$ $1 \cdot y^{-1} = y^{-1} \in H$. Pentru $x, y \in H$, avem că

$$xy = x(y^{-1})^{-1} \in H.$$

Demonstrația propoziției

a) Pp. că $H \leq G_1$ și fie $x, y \in f(H) \Rightarrow$ $(\exists)\ h, h' \in H$ a.î. $x = f(h)$, $y = f(h')$. Avem:

$$xy^{-1} = f(h) f(h')^{-1} = f(h) f((h')^{-1}) = f(\underbrace{h(h')^{-1}}_{\in H}) \in f(H) \Rightarrow xy^{-1} \in f(H)$$

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

b) Fie $x, y \in f^{-1}(K) \Rightarrow f(x), f(y) \in K$.

Atunci:

$$f(xy^{-1}) = f(x) f(y^{-1}) = f(x) f(y)^{-1} \in K$$

$$\Rightarrow xy^{-1} \in f^{-1}(K), \text{ i.e. } f^{-1}(K) \leq G_1$$

$\boxtimes$

COROLAR Fie $f : G_1 \longrightarrow G_2$ morfism de grupuri. Atunci:

a) $\mathrm{Im}(f) = f(G_1) \leq G_2$

b) $f^{-1}(\{1\}) = \{x \in G_1 \mid f(x) = 1\} \stackrel{not}{=} \underline{\mathrm{Ker}(f)} \leq G_1$

s.n. <u>nucleul</u> lui f.

Propoziție Fie $f : G_1 \longrightarrow G_2$ morfism de grupuri.

Atunci:

a) f e surjectiv $\Longleftrightarrow \mathrm{Im}(f) = G_2$.

b) f e injectiv $\Longleftrightarrow \mathrm{Ker}(f) = \{1\}$.

<u>Dem</u> a) Definiția surjectivității.

b) „$\Rightarrow$" Fie $\underline{x \in \mathrm{Ker}(f)} \Rightarrow f(x) = 1 = f(1) \stackrel{f\,inj}{\Longrightarrow}$

$\underline{x = 1} \Rightarrow \mathrm{Ker}(f) = \{1\}$.

„$\Leftarrow$" Pp. că $\underline{f(x) = f(y)} \Rightarrow f(x) f(y)^{-1} = 1 \Rightarrow$

$f(xy^{-1}) = 1 \Rightarrow xy^{-1} \in \mathrm{Ker}(f) = \{1\} \Rightarrow$

$xy^{-1} = 1 \Rightarrow \underline{x = y}$, i.e. f e injectivă ▨

<u>observații</u>: 1) Fie $H \leq G$ și $i : H \hookrightarrow G$ incluziunea canonică $i(h) := h$, $(\forall) h \in H$. Atunci i e morfism injectiv de grupuri și $\mathrm{Im}(i) = H$, $\mathrm{Ker}(i) = \{1\}$.

2) Fie $f : G_1 \longrightarrow G_2$ <u>morfism injectiv</u> de grupuri și fie $G_2' \stackrel{def}{:=} \mathrm{Im}(f) \leq G_2$.

Aplicație $\tilde{f} : G_1 \xrightarrow{\sim} G_2' = \mathrm{Im}(f)$,

$\tilde{f}(x) := f(x)$, $(\forall)\ x \in G_1$

este izomorfism de grupuri (corestricția lui f la imagine) și deci $\underline{G_1 \simeq \mathrm{Im}(f) \leq G_2}$

Definiție: Un grup G_1 se poate scufunda într-un grup G_2 dacă $(\exists)$ $f : G_1 \longrightarrow G_2$ morfism injectiv de grupuri (i.e. dacă G_1 este izomorf cu un subgrup al lui G_2).

Teoremă (Cayley, 1854) Orice grup se poate scufunda într-un grup de permutări.

Dem Fie G = grup arbitrar și $X := G$ ca mulțime.
Pentru fiecare $g \in G$ fie $\varphi_g : G \to G$, $\varphi_g(x) := gx$, $(\forall)\ x \in G$. Definim:

$$\varphi : G \longrightarrow \Sigma_G, \quad \varphi(g) := \varphi_g, \ (\forall) g \in G$$

- $\varphi_g : G \to G$ este bijectivă? (Exercițiu!)
- φ e morfism de grupuri? Fie $g_1, g_2 \in G$.

Atunci vrem:

$$\varphi(g_1 g_2) \overset{?}{=} \varphi(g_1) \circ \varphi(g_2).$$ Fie $x \in G$. Atunci

$$\varphi(g_1 g_2)(x) = \varphi_{g_1 g_2}(x) = (g_1 g_2)x \quad \text{și}$$

$$\left(\varphi(g_1)\circ\varphi(g_2)\right)(x) = \left(\varphi_{g_1}\circ\varphi_{g_2}\right)(x) =$$
$$= \varphi_{g_1}(g_2 x) = g_1(g_2 x) = (g_1 g_2)x \quad \text{i.e.}$$

φ e morfism de grupuri.

- φ este injectiv?

Fie $\underline{g \in \operatorname{Ker}(\varphi)} \Rightarrow \varphi(g) = \mathrm{Id}_G \Rightarrow \varphi_g = \mathrm{Id}_G$

$\Rightarrow \varphi_g(1) = \mathrm{Id}_G(1) \Rightarrow \underline{g = 1}$, i.e. $\underline{\operatorname{Ker}(\varphi) = \{1\}}$

şi deci φ e injectiv. ▨

In particular, orice grup finit cu n elemente se poate scufunda în grupul de permutări $S_n = \Sigma_{\{1,\dots}$

Exerciţiu Fie $n \in \mathbb{N}$, $n \geq 2$. Arătaţi că grupul de permutări S_n se poate scufunda în $GL(n, \mathbb{C}) := \{A \in M_n(\mathbb{C}) \mid A$ inversabilă$\}$.

Indicaţie: Fie matricile
$$\begin{array}{cc} & \\ e_{ij} := i & \begin{pmatrix} 0 & \cdots & & \cdots & 0 \\ \vdots & & \vdots & & \vdots \\ \cdots & \cdots & 1 & & \vdots \\ 0 & \cdots & \vdots & & 0 \end{pmatrix} \\ & \qquad\qquad j \end{array}$$
şi

$$f: S_n \longrightarrow GL(n, \mathbb{C})$$
$$f(\sigma) := e_{\sigma(1),1} + e_{\sigma(2),2} + \dots + e_{\sigma(n),n}$$

Atunci f e morfism injectiv de grupuri. ▨

Reamintim că pentru un grup G am notat cu
$\mathcal{L}(G) := \{ H \mid H \leq G \}$ mulțimea subgrupurilor lui

Teorema de corespondență pentru subgrupuri

Fie $f : G_1 \longrightarrow G_2$ un morfism <u>surjectiv</u> de grupuri.
Atunci funcția :

$$F : \{ H \mid H \leq G_1 ,\ H \supseteq \mathrm{Ker}(f) \} \xrightarrow{\sim} \mathcal{L}(G_2)$$
$$F(H) := f(H)$$

este bijectivă.

<u>Dem</u> : Definim funcția

$$\psi : \mathcal{L}(G_2) \longrightarrow \{ H \in \mathcal{L}(G_1) \mid H \supseteq \mathrm{Ker}(f) \}$$
$$\psi(K) := f^{-1}(K).$$

- ψ ia valori în mulțimea indicată.

În adevăr, dacă $K \leq G_2 \Rightarrow \psi(K) = f^{-1}(K) \leq G_1$ (Prop. anterioară) și avem de arătat că

$$\mathrm{Ker}(f) \overset{?}{\subseteq} f^{-1}(K).$$

$\underline{x \in \mathrm{Ker}(f)} \Rightarrow f(x) = 1 \in K \Rightarrow \underline{x \in f^{-1}(K)}$

•• Arătăm că F și ψ sunt <u>inverse</u> una alteia.

a) $(F \circ \psi)(K) \overset{?}{=} K$, $(\forall)\ K \leq G_2$ i.e.

$$f(f^{-1}(K)) \overset{?}{=} K, \quad (\forall)\ K \leq G_2.$$

„$\subseteq$" Fie $\underline{x \in f(f^{-1}(K))} \Rightarrow (\exists)\ z \in f^{-1}(K)$ a.î. $\overset{\parallel}{f(z)} \in K$

$x = f(z) \in \underline{K}$

„$\supseteq$" Fie $\underline{x \in K} \xRightarrow[\text{surj}]{f} (\exists)\ a \in G_1$ a.î. $x = f(a)$

Cum $f(a) = x \in K \Rightarrow \underline{a \in f^{-1}(K)}$ i.e.

$\underline{x \in f(f^{-1}(K))}$ și „?" e demonstrat.

b) $(\psi \circ F)(H) \overset{?}{=} H$, $(\forall)\ H \leq G_1$, $H \supseteq Ker(f)$, i.e.

$f^{-1}(f(H)) \overset{?}{=} H$, $(\forall)\ H \leq G_1$, $H \supseteq Ker(f)$

„$\subseteq$" Fie $\underline{x \in f^{-1}(f(H))} \Rightarrow f(x) \in f(H) \Rightarrow$
$\underline{(\exists)\ h \in H}$ a.î. $f(x) = f(h) \Longrightarrow f(x) f(h)^{-1} = 1$

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

$\Rightarrow x h^{-1} \in H \xRightarrow{h \in H} \underline{x \in H}$.

„$\supseteq$" Fie $\underline{h \in H} \Rightarrow f(h) \in f(H) \Rightarrow \underline{h \in f^{-1}(f(H))}$

i.e. $H \subseteq f^{-1}(f(H))$. Demonstrația e completă.

$\boxtimes$

<u>Propoziție</u> Fie G un grup și $(H_i)_{i \in I}$ o familie de subgrupuri ale lui G. Atunci:

$$\bigcap_{i \in I} H_i \leq G \text{ este } \underline{\text{subgrup}} \text{ în } G.$$

<u>Dem</u> Trivial, aplicați doar definiția. $\boxtimes$

<u>Observație</u> Dacă $H, \cancel{K} \leq G \not\Rightarrow H \cup G \leq G$

<u>Exemplu</u>: $G := (\mathbb{R} \times \mathbb{R}, +)$, $H := \mathbb{R} \times \{0\}$ și $K := \{0\} \times \mathbb{R}$ sunt subgrupuri în G dar $H \cup K$ <u>nu</u> e subgrup în G. (Exercițiu!)

Exerciții 1) Fie $H, K \leq G =$ grup. Atunci $H \cup K \leq G \iff H \subseteq K$ sau $K \subseteq H$.

2) Fie $(H_i)_{i \in I}$ o familie "filtrată" de subgrupuri în G, i.e. $(\forall)\ i, j \in I\ (\exists)\ t \in I$ a.î. $H_i \subseteq H_t$ și $H_j \subseteq H_t$.

Atunci, $\bigcup_{i \in I} H_i \leq G$.

Definiție Fie $G =$ grup și $X \subseteq G$ o submulțime nevidă. Arătarea

$$\langle X \rangle \overset{def}{:=} \bigcap_{X \subseteq H \leq G} H$$

s.n. subgrupul generat de X.

Obs: $\langle X \rangle$ este "cel mai mic subgrup al lui G" ce conține X i.e.: dacă $H \leq G$ și $H \supseteq X \Rightarrow \langle X \rangle \subseteq H$.

Propoziție Fie $G =$ grup și $X \subseteq G$. Atunci:

$$\langle X \rangle = \underbrace{\left\{ x_1^{\varepsilon_1} x_2^{\varepsilon_2} \cdots x_n^{\varepsilon_n} \;\middle|\; n \in \mathbb{N}^*,\ x_i \in X,\ \varepsilon_i \in \{-1, 1\},\ (\forall)\ i = \overline{1,n} \right\}}_{\overset{not}{=}\ H}$$

Dem Fie H mulțimea din dreapta. Atunci:

- $H \leq G$ și $X \subseteq H$? (dacă arătăm asta $\Rightarrow \langle X \rangle \subseteq H$ i.e. „$\subseteq$").

Fie $x \in X \neq \phi \Rightarrow x x^{-1} \in H \Rightarrow 1 \in H$

Fie acum $a, b \in H \Longrightarrow$

$a = x_1^{\varepsilon_1} \cdots x_n^{\varepsilon_n}$, $b = y_1^{\beta_1} \cdots y_m^{\beta_m}$, cu $x_i, y_j \in X$
şi $\varepsilon_i, \beta_j \in \{-1, 1\}$ $\Longrightarrow$

$a b^{-1} = x_1^{\varepsilon_1} \cdots x_n^{\varepsilon_n} y_m^{-\beta_m} \cdots y_1^{-\beta_1} \in H$ i.e. $\underline{H \leq G}$

evident $X \subseteq H$ şi deci $\underline{\langle X \rangle \subseteq H}$.

- $H \overset{?}{\subseteq} \langle X \rangle$. Fie $\underline{a = x_1^{\varepsilon_1} x_2^{\varepsilon_2} \cdots x_n^{\varepsilon_n} \in H}$

Pentru fiecare $i \in \{1, \dots n\}$ avem că $x_i^{\varepsilon_i} = \begin{cases} x_i \\ \text{sau} \\ x_i^{-1} \end{cases}$

Dacă $x_i^{\varepsilon_i} = x_i \in X \subseteq \langle X \rangle$.

Dacă $x_i^{\varepsilon_i} = x_i^{-1}$, cu $x_i \in X \subseteq \langle X \rangle \Longrightarrow$
$x_i^{-1} \in \langle X \rangle$ (căci $\langle X \rangle \leq G$) $\Longrightarrow x_i^{\varepsilon_i} \in \langle X \rangle$

Deci $x_i^{\varepsilon_i} \in \langle X \rangle$, $(\forall)\, i \in \{1, \dots n\} \Rightarrow a = x_1^{\varepsilon_1} \cdots x_n^{\varepsilon_n} \in$
$\in \langle X \rangle$. $\boxtimes$

<u>Exemple</u> 1) $G =$ <u>grup</u> şi $\underline{X = \{g\}}$, $g \in G \Longrightarrow$
$\underline{\langle g \rangle = \{ g^n \mid n \in \mathbb{Z} \}} \leq G$.

2) $(\mathbb{Z}, +) = \langle 1 \rangle = \langle -1 \rangle$.

3) $(\mathbb{Z} \times \mathbb{Z}, +) = \langle \{(1,0), (0,1)\} \rangle$ (Exerciţiu!)

<u>Observație</u>: Fie G un grup. Atunci $(\mathcal{L}(G), \subseteq)$ este o <u>latice</u> în care

$\inf\{H, K\} = H \cap K$ și $\sup\{H, K\} = \langle H \cup K \rangle$

$(\forall)$ $H, K \in \mathcal{L}(G)$. În plus, $\{1\}$ e <u>prim element</u> în $\mathcal{L}(G)$ și G este <u>ultim element</u> în $\mathcal{L}(G)$ ☒

Dacă G = grup și $A, B \subseteq G$ notăm

$$AB \overset{def}{:=} \{ab \mid a \in A, b \in B\}$$

$$A^{-1} \overset{def}{:=} \{a^{-1} \mid a \in A\}.$$

Dacă $A = \{a\}$, $\{a\}B \overset{not}{=} aB = \{ab \mid b \in B\}$

<u>Exerciții</u> 1) Fie $H \subseteq G$ = grup. Atunci $H \leq G \iff HH = H$ și $H^{-1} = H$.

2) Fie $H, K \leq G$. Atunci

$HK \leq G \iff HK = KH$.

În acest caz, $\langle H \cup K \rangle = HK$.

• <u>Produs direct de grupuri</u>

Fie G și H două grupuri. Atunci produsul cartezian $G \times H$ devine grup cu "înmulțirea pe componente"

$$(g_1, h_1) \cdot (g_2, h_2) := (g_1 g_2, h_1 h_2)$$

$(\forall)$ $g_1, g_2 \in G$, $h_1, h_2 \in H$ numit <u>produsul direct</u> al celor două grupuri (Exercițiu).

În plus, aplicațiile

$$\pi_1 : G \times H \longrightarrow G, \quad \pi_1(g, h) := g$$
$$\pi_2 : G \times H \longrightarrow H, \quad \pi_2(g, h) := h$$

sunt morfisme surjective de grupuri (Exercițiu!) numite proiecțiile canonice.

Mai general, fie I = mulțime nevidă și $(G_i)_{i \in I}$ o familie de grupuri. Fie $\prod_{i \in I} G_i$ produsul direct de mulțimi:

$$\prod_{i \in I} G_i := \{ x : I \longrightarrow \bigsqcup_{i \in I} G_i \mid x(i) \in G_i, (\forall) i \in I \}$$
$$= \{ (x_i)_{i \in I} \mid x_i \in G_i, (\forall) i \in I \}$$

unde reamintim notația $x_i = x(i)$, $(\forall) i \in I$, $x : I \to \bigsqcup_{i \in I} G_i$.

Propoziție: Fie I = mulțime nevidă și $(G_i)_{i \in I}$ o familie de grupuri. Atunci $\prod_{i \in I} G_i$ are o structură de grup cu:

$$(x \cdot y)(i) := x(i)\, y(i), \qquad (*)$$

$(\forall)\, x, y \in \prod_{i \in I} G_i$ și $i \in I$ cu elementul neutru

$$1 : I \longrightarrow \bigsqcup_{i \in I} G_i, \quad 1(i) := 1_{G_i}, \ (\forall) i \in I$$

numit produsul direct al familiei $(G_i)_{i \in I}$.

Dem: Exercițiu! Formula $(*)$ se scrie folosind notație cu șiruri și astfel:

$$(x_i)_{i\in I}\cdot(y_i)_{i\in I} := (x_i y_i)_{i\in I}.$$ ▨

Obs 1) Fie $(G_i)_{i\in I}$ o familie de grupuri. Pentru fiecare $j\in I$ funcția:

$$\pi_j : \prod_{i\in I} G_i \longrightarrow G_j,\quad \pi_j\left((x_i)_{i\in I}\right) := x_j$$

este morfism surjectiv de grupuri numit proiecție canonică pe componenta j.

2) Dacă $G_i = G$, $(\forall)\, i\in I$, atunci

$$\prod_{i\in I} G_i \overset{not}{=} G^I = \{x : I \longrightarrow G \mid x \text{ funcție}\}$$

care este un grup, produs de $|I|$ copii ale lui G.

3) Dacă $I = \{1, 2, \dots, n\}$, atunci

$$\prod_{i\in I} G_i = G_1 \times G_2 \times \dots \times G_n$$ și e grup cu

$$(x_1, \dots x_n)\cdot(y_1, \dots, y_n) := (x_1 y_1, \dots, x_n y_n)$$ și

$$1 = (1_{G_1}, \dots, 1_{G_n}).$$ ▨

Teoremă factorială (P.U.P.D.) Fie $(G_i)_{i\in I}$ o familie nevidă de grupuri. Atunci:

$(\forall)\, G =$ grup, $(\forall)\, f_j : G \to G_j$ o familie de morfisme de grupuri $(j\in I)$ $(\exists!)\, \overline{f} : G \to \prod_{i\in I} G_i$ un morfism de grupuri a.î.

$$\pi_j \circ \overline{f} = f_j,\ (\forall)\, j\in I$$

$$\begin{tikzcd}
 & G \arrow[dl, dashed, "(\exists!)\,\overline{f}"'] \arrow[d, "(\forall)\, f_j"] \\
\prod_{i\in I} G_i \arrow[r, "\pi_j"'] \arrow[ur, phantom, "\|"] & G_j
\end{tikzcd}$$

Dem TEMĂ, SIMILAR cu MULȚIMI!