- Examen oral 1 teorie + 1 problemă (fără demonstrații)
  50% din nota finală
- 1 referat 10%
- La examen - un caiet de temă 10%
- Lucrare 10%
- Activitate seminar 20%
- Referat: def, enunț, obs
  1-2 probleme (carte)
  să construim o prob.

1. Operații cu mulțimi ($\cup, \cap, \setminus$...)
2. Relații binare
3. Relații de echivalență
4. Relații funcționale
5. Funcții injective
6. Funcții surjective
7. Semigrupuri. Aplicații
8. Monoizi. Aplicații
9. Subgrupurile unui grup de ordine $\leq 6$
10. Grupuri finite de ordin $\leq 8$
11. Relații de echivalență modulo un subgrup
12. Subgrup normal. Aplicații
13. Teorema fundamentală de izomorfism la grupuri. Aplicații
14. Teorema de structură a grupurilor ciclice. Aplic
15. Teorema lui Lagrange
16. Teorema lui Cosi. Ap.

17. Ordinul unui elem. într-un grup. Ap.

18. Teorema de scufundare a lui Caylay

19. Subinel. Aplicatii

20. ideal. Aplicatii

21. Morfisme de inele

22. Teorema fundamentală de izomorfism la inele Ap.

23. Lema chineza resturilor. Ap.

24. Caracteristica unui corp. Ap.

25. Corpuri finite

26. Inele de fracții Scufundări

27. Polinoame monice

28. Divizibilitatea polinoamelor $\mathbb{Q}[x]$

29. Rădăcini ale polinoamelor $\mathbb{R}[x]$

30. Teorema fundamentală a algebrei

31. Polinoam ireductibile

Sub. Examen:

I a) Definiți și exemplificați noțiunea de subgrup

Def: Fie $(G, \cdot)$ un grup și $H \subset G$, $H \neq \emptyset$

$H \leq G$ daca: 1) $(\forall)\ x, y \in H \Rightarrow x, y \in H$

2) $(\forall)\ x \in H \Rightarrow x^{-1} \in H$

$G: \{1\}$, $G \leq G$

b) Enunțați teorema lui Lagranje (la grupuri)

Fie $G$ un grup finit și $H \leq G$ Atunci $|G| = |H| \cdot |G, H|$

În part $|H| \mid |G|$

^ · Lagrange

BIBLIOGRAFIE : Dumitrescu Algebră 1.

Probleme de algebră Băiețica, ~~Mihai~~, Micu

# ELEMENTE DE TEORIE A MULȚIMILOR

## 1. Mulțimi

$X, A, B \ldots$

$a, b, c \ldots$

$a \in X$, $a \notin X$

$\{x\}$ singletonul definit de $x$

$\{x, y\}$ dublet / perechea neordonată

$(x, y)$: $\{x\}, \{x, y\}$ perechea ordonată

$(x, y, z) = ((x, y), z)$

$X, p$ $X = \{x \mid x \text{ are proprietatea } p\}$

$A, B \subset X$, $A \subset X \overset{def.}{\iff} (\forall)\, a \in A \Rightarrow a \in X$

$A \subsetneq X$

$A \not\subset X \iff \exists\, a \in A,\ a \notin X$

$A = B \iff A \subset B$ și $B \subset A$

$A \cup B = \{x \in X \mid x \in A \text{ sau } x \in B\}$

$A \cap B = \{x \in X \mid x \in A \text{ și } x \in B\}$

$A \setminus B = \{x \in X \mid x \in A \text{ și } x \notin B\}$

$(A \setminus B) \cup (B \setminus A) = A \Delta B$ ?

$X$ mulțime finită $\Rightarrow A, B$ mult. finite. $|X|$ cardinal

$X = \{a, b, c\} \Rightarrow |X| = 3$

$|A \cup B| = |A| + |B| - |A \cap B|$

$A, B, C \subset X$

$|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C|$

- $X$, $\phi_x = \{x \in X \mid x \neq x\}$

T

TEOREMĂ. Fie $X$ o mulțime și $\phi_X$ partea vidă a lui $X$.
Atunci i) $\phi_X$ nu conține niciun element
ii) Pt orice mulț $Y$, $\phi_X \subset Y$
iii) Pt orice mulț $Y$, $\phi_X = \phi_Y = \phi$

DEMONSTRAȚIE.

i) Pp. că $(\exists)\ x_0 \in \phi_X \Rightarrow x_0 \in X,\ x_0 \neq x_0 \Rightarrow 0 \neq 0$, contradicție

ii) Pp. că $(\exists)\ Y : \phi_X \not\subset Y \Rightarrow (\exists)\ x_0 \in \phi_X$ și $x_0 \notin Y$. contr.

$(\forall)\ Y : \phi_X \subset Y$

iii) Folosim ii) $\left.\begin{array}{l}(\forall)\ Y : \phi_X \subset \phi_Y \\ \phi_Y \subset \phi_X\end{array}\right| \Rightarrow \phi_X = \phi_Y = \phi$;

$\phi = \{x \mid x \neq x\}$

$A \cup \phi = A$

$A \cap \phi = \phi$

- $X$

$P(X) = \{A \mid A \subset X\}$ mulț părților lui $X$

$|X| = m,\ m \in N \Rightarrow |P(X)| = 2^m$

Ex: $\cdot\ X = \{1, 2, 3\}$, $P(X) = \{\phi, \{1\}, \{2\}, \{3\}, \{1,2\}, \{1,3\}, \{2,3\}, \{1,2,3\}\}$

$\cdot\ X = \phi$, $P_\phi = \{\phi\}$

$P(P(\phi)) = P(\{\phi\}) = \{\phi, \{\phi\}\}$

• Dați exemplu de 3 mulțimi X, Y, Z a.î. $X \subset Y \in Z$ și $X \in Y \subset Z$

$X = \emptyset$, $Y = \{\emptyset\}$, $Z = \{\emptyset, \{\emptyset\}\}$

$A, B \subset X$

a) $P(A) \cap P(B) = P(A \cap B)$

b) $P(A) \cup P(B) \subset P(A \cup B)$

$P(B) = \{\emptyset, \{1\}, \{2\}, \{4\}; \{1,2\}, \{1,4\}, \{2,4\}, \{1,2,4\}\}$

$P(A) = \{\emptyset; \{1\}; \{2\}; \{3\}, \{1,2\}, \{1,3\}, \{2,3\}, \{1,2,3\}\}$

$X = \{1,2,3,4\}$, $A = \{1,2,3\}$, $B = \{1,2,4\}$ } $A \cup B = X$

$\{3,4\} \notin P(A) \cup P(B) \neq P(A \cup B) = P(X)$

$A \subset X$, $X \setminus A = CA = C_X A$ complementara lui A în rap. cu X

$C_X A = \{x \mid x \in X, x \notin A\}$

$A, B \subset X$

$C(A \cup B) = CA \cap CB$

$C(A \cap B) = CA \cup CB$

} LEGILE LUI DE MORGEN

Prof Ex: Fie $A = \{1, 2, 3 \ldots 2019\}$

- Câte submulțimi $B \subset A$, $\{1,2\} \subset B$?

$2^{2017}$

- Câte submulțimi $B \subset A$, $\{1,2\} \subset B$, $|B| = 5$?

$|A| = n$, $n \geq 2$

$A_1 \subset A$, $|A_1| = 2$; $C_n^2 = \frac{n(n-1)}{2}$

$|A_1| = k \Rightarrow C_n^k = \frac{n!}{k!(n-k)!}$

$A = \{3, 4, \ldots 2019\}$ $|A| = 2017$

$B = \{1, 2, a, b, c\}$

$C_{2017}^3 = \frac{2017 \cdot 2016 \cdot 2015}{1 \cdot 2 \cdot 3}$

$C_{|A|}^3$

$\Downarrow$

2017 ~~st~~ $C_5$

elem 1 și 2 sunt deja folosite

$A \times B = \{(a,b) \mid a \in A, b \in B\}$ PRODUSUL CARTEZIAN

$A \times B \times C = (A \times B) \times C$

$A \times B \times C = \{(a,b,c) \mid a \in A, b \in B, c \in C\}$

$X, Y$ nevide

$\rho \subset X \times Y \leftarrow$ RELAȚIE BINARĂ DE LA $X$ LA $Y$

$\rho = \{(x,y) \in X \times Y \mid x \rho y\}$

$(x,y) \in \rho \iff x \rho y$

Dacă $X = Y \Rightarrow \rho \subset X \times X$

$\rho$ este o relație binară pe mult. $X$

$\rho \subset X \times Y$

DOM $\operatorname{Dom} \rho = \{x \in X \mid (\exists)\, y \in Y \text{ a.î. } x \rho y\}$ DOMENIUL LUI $\rho$

RANG $\operatorname{Rang} \rho = \{y \in Y \mid (\exists)\, x \in X \text{ a.î. } x \rho y\}$

$\rho^{-1} = \{(y,x) \mid (x,y) \in \rho\}$ INVERSA

Ex: $X = \{1,2,3,4\}$

$\rho \subset X \times X$ $\rho = \{(1,1), (1,2); (2,3); (2,4); (3,4)\}$

$\operatorname{Dom} \rho = \{1,2,3\}$

$\operatorname{Ram} \rho = \{1,2,3,4\}$

$\rho^{-1} = \{(1,1); (2,1); (3,2); (4,2); (4,3)\}$

$X, Y$ nevide

$\rho \subset X \times Y$, $\rho = \{(x,y) \in X \times Y \mid x \in X$ și $y \in Y\}$ $(x,y) \in \rho \Leftrightarrow x \rho y$

$\text{Dom}\, \rho = \{x \in X \mid (\exists)\, y \in Y$ a.î. $x \rho y\}$

$\text{Rar}\, \rho = \{y \in Y \mid (\exists)\, x \in X$ a.î. $x \rho y\}$

$\rho^{-1} = \{(y,x) \in Y \times X \mid x \rho y\}$

$\rho \subset X \times Y$, $s \subset Y \times Z$: $s \circ \rho \subset X \times Z$

$s \circ \rho = \{(x,z) \in X \times Z \mid (\exists)\, y \in Y$ a.î. $x \rho y$ și $y s z\}$

---

TEMA

Ex: Fie $X = \{1,2,3,4\}$ și $\rho = \{(1,2),(2,2),(2,3),(3,4)\}$

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

$\text{Dom}\, \rho = ?$ $\text{Dom}\, s = ?$ $\text{Rar}\, \rho = ?$ $\text{Rar}\, s = ?$ $s \circ \rho = ?$ $\rho^{-1} = ?$

$s^{-1} = ?$ $\rho^{-1} \circ s^{-1} = ?$ $\boxed{\text{TEMĂ}}$

---

REL DE ECHIVALENȚĂ

$\rho \subset X \times X$

(1) $\rho$ reflexivă: $x \rho x$ $(\forall)\, x \in X$ $((x,x) \in \rho, (\forall) x \in X)$

(2) $\rho$ simetrică: $x \rho y \Rightarrow y \rho x$ $((x,y) \in \rho \Rightarrow (y,x) \in \rho)$

(3) $\rho$ tranzitivă: $x \rho y, y \rho z \Rightarrow x \rho z$ $((x,y) \in \rho, (y,z) \in \rho \Rightarrow (x,z) \in \rho)$

O relație $\rho$ care este reflex, sim și tranz s.n. rel de echivalență.

---

Fie $\rho \subset X \times X$ o rel de ech. și $x_0 \in X$

- $\hat{x}_0 \overset{\text{not}}{=} C_{x_0}(\rho) = \{x \in X \mid x \rho x_0\}$ clasa de echivalență a lui $x_0$ în raport cu rel $\rho$.

- $X/_{\rho} \overset{\text{not}}{=} \{\hat{x}_0 \mid x_0 \in X\}$ mulțimea factor sau mulțimea cât în raport cu $\rho$.

TEMĂ Temă

Ex2) Dacă $\rho_1$ și $\rho_2$ sunt două rel de echivalență pe mult nevidă $X$, arătați că $\rho_1 \cap \rho_2$ este o rel de echiv.

Ex3) $X = \{1,2,3\}$

$\rho_1 = \{(1,1), (2,2), (3,3)\ (1,2), (2,1)\}$

$\rho_2 = \{(1,1); (2,2); (3,3)\ (2,3), (3,2)\}$

$\rho_1 \cup \rho_2 = \{(1,1); (2,2); (3,3); (1,2), (2,1), (2,3), (3,2)\}$

$$\left.\begin{array}{r} (\exists)(x,y) \in \rho_1 \cup \rho_2 \\ (y,z) \in \rho_1 \cup \rho_2 \\ (x,z) \notin \rho_1 \cup \rho_2 \end{array}\right| \begin{array}{l} (1,2)\ (2,3) \in \rho_1 \cup \rho_2 \\ (1,3) \notin \rho_1 \cup \rho_2 \end{array}$$

$\rho_1 \cup \rho_2$ nu este o rel. de echivalență

---

$a, b \in \mathbb{Z}$

$m \geq 2 \quad a \equiv b \pmod m \Leftrightarrow m \mid (a-b)$

$m = 1: \quad a \equiv b \pmod 1 \Leftrightarrow 1 \mid (a-b)$

$m = 0: \quad a \equiv b \pmod 0 \Leftrightarrow 0 \mid (a-b) \Leftrightarrow a = b$

$(-m): \ |-m|$

$x \mid y \Leftrightarrow (\exists)\, z : y = xz$

---

Ex 4) „$\equiv$" este rel. de ech.

$\hat{a} = \{b \in \mathbb{Z} \mid a \equiv b \pmod m\}$

$\mathbb{Z}_m = \mathbb{Z}/_{\equiv} = \{\hat{0}, \hat{1}, \dots, \widehat{m-1}\}$ mulțimea claselor de resturi mod $m$

$\hat{x} + \hat{y} = \widehat{x+y}$

$\hat{x} \cdot \hat{y} = \widehat{xy}$

$(\mathbb{Z}_n, +, \cdot)$ inel unitar comutativ

$m=4: \mathbb{Z}_4 = \{\hat{0}, \hat{1}, \hat{2}, \hat{3}\}$

$\hat{2} = \{4k+2 \mid k \in \mathbb{Z}\} = \{\dots -6, -2, 2, 6 \dots\}$

$m=7: \mathbb{Z}_7 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}\}$

$\hat{2} = \{7k+2 \mid k \in \mathbb{Z}\}$

---

(?) $U(\mathbb{Z}_n) = \{\hat{x} \in \mathbb{Z}_n^* \mid (\exists)\ \hat{y} \in \mathbb{Z}_n^*$ a.î. $\hat{x} \cdot \hat{y} = \hat{1}\}$

$(\mathbb{Z}_n^*, \cdot)$ monoid comutativ

$(U(\mathbb{Z}_n), \cdot)$ grup comutativ

Fie $\hat{x} \in U(\mathbb{Z}_m) \Leftrightarrow \exists\ \hat{y} \in \mathbb{Z}_m^* : \hat{x}\hat{y} = \hat{1} \Leftrightarrow m \mid (x, y-1) \Leftrightarrow$

$\left( x \equiv y \ (\text{mod } m) \Leftrightarrow m \mid (x-y) \Leftrightarrow \hat{x} = \hat{y} \right)$

$\Leftrightarrow (\exists)\ k \in \mathbb{Z} : xy - 1 = mk \Leftrightarrow xy + m(-k) = 1 \Leftrightarrow (x, m) = 1$

$U(\mathbb{Z}_m) = \{\hat{x} \in \mathbb{Z}_m^* \mid (x, m) = 1\}$

---

$U(\mathbb{Z}_8) = \{\hat{1}, \hat{3}, \hat{5}, \hat{7}\}$

$\mathbb{Z}_m^* = U(\mathbb{Z}_m) \Leftrightarrow m$ este nr. prim $\mathbb{Z}_2, \mathbb{Z}_3, \mathbb{Z}_5, \mathbb{Z}_7 \dots$ corpuri

---

$|U(\mathbb{Z}_m)| = |\{\hat{x} \mid 1 \le x \le m,\ (x, m) = 1\}| = \varphi(m)$ funcția lui Euler

Ex: Să se rez. ec. $3x^2 - 4x + 1 = 0$ în $\mathbb{Z}_5$ și $\mathbb{Z}_{11}$

K-corp $= ax^2 + bx + c = 0 \quad a \neq 0$

$\Delta = b^2 - 4ac = u^2, \ u \in K$

$x_{1,2} = -b \pm \sqrt{\Delta} \cdot (2a)^{-1}$

$\hat{x} \cdot \hat{y} = \hat{1}$ invers

$\hat{x} + \hat{x}' = \hat{0}$ opus

$3x^2 - 4x + 1 = 0$ în $\mathbb{Z}_5$

$\Delta = (-\hat{4})^2 - \hat{4} \cdot \hat{3} \cdot \hat{1} = \hat{1} - \hat{2} = \hat{4}$

$x_{1,2} = (\hat{4} \pm \hat{2}) \cdot \hat{1} \Rightarrow \begin{cases} x_1 = \hat{1} \\ x_2 = \hat{2} \end{cases}$

TEMĂ $\hat{3}x^2 - \hat{4}x + \hat{1} = 0$

$\Delta = (-\hat{4})^2 - \hat{4}\cdot\hat{3}\cdot\hat{1} = \hat{5} - \hat{1} = \hat{4}$

$x_{1,2} = (\hat{4} \pm \hat{2})\cdot\hat{1} \Rightarrow \begin{cases} x_1 = \hat{1} \\ x_2 = \hat{4} \end{cases}$

---

$\rho \subset X \times X$

$\rho$ este antisimetrică dacă $x \rho y$ și $y \rho x \Rightarrow x = y$

$\rho$ reflexivă și tranzitivă s.n. relație de preordine, dacă în plus este și antisimetrică s.n. rel. de ordine „$\leq$"

$x \leq y$ : $x < y$ : $x \leq y$ și $x \neq y$

$(X, \leq)$ mulț. ordonată

rel. ordine $\Rightarrow$ rel. preordine

$\not\Leftarrow$

$\mathbb{N}$; $x | y \Leftrightarrow \exists z : y = xz$

(r) $x | x$ $(\forall)$ $x \in \mathbb{N}$

(as) $x | y$ și $y | x \Rightarrow x = y$

(t) $x | y$, $y | z \Rightarrow x | z$

$\mathbb{Z}$; $2 | (-2)$ $-2 | 2$ $2 \neq -2$

$(\mathbb{Z}, |)$ este o mulț. preord., dar nu este o mulț. ordonată

---

Considerăm mulț. ordonată $(X, \leq)$.

Dacă $x \leq y$ sau $y \leq x$, $(\forall)$ $x, y \in X$, rel. „$\leq$" este total ordonată

$(X, \leq)$ este o mulț. total ordonată

$x_0 \in X$ s.n. primul elem / elem inițial al mulțimii dacă

$x_0 \leq x$ $(\forall)$ $x \in X$

$x_0 \in X$ s.n. ultimul elem / elem. final al mulțimii dacă

$x_0 \geq x$ $(\forall)$ $x \in X$

$(X, \leq)$, $(\forall)$ $A \subset X$, $A \neq \emptyset$ există un prim elem. $x_0 \in A$ s.n.

OBS: O mult. bine ordonată este total ordonată.

Def: Mult. nr. naturale este un triplet $(0, \mathbb{N}, s)$ a.î. sunt verif. ce axiomele lui Peano:

$P_1$: $0 \in \mathbb{N}$

$P_2$: $s: \mathbb{N} \to \mathbb{N}^*$ este o funcție injectivă

$P_3$: Dacă $P \subset \mathbb{N}$ a.î. i) $0 \in P$

ii) $(\forall) n \in P \Rightarrow s(n) \in P$, atunci $P = \mathbb{N}$

0 elem. inițial al mult. $s: \mathbb{N} \to \mathbb{N}^*$, $s(n) = n'$ funcția succesor

$0' = 1$, $1' = 2$, $2' = 3$ ...

$s(\mathbb{N}) = \mathbb{N}^*$

$P_3$ principiul inducției matematice

$P$ s.n. mult. inductivă

Ex) Rămân axiomele lui Peano adev. în $\mathbb{Z}$? $\boxed{NU}$

---

$\varphi: \mathbb{N} \times \mathbb{N} \to \mathbb{N}$. $\varphi(m, n) = m + n$ a.î. $A_{(1)}$ $m + 0 = m$ $(\forall) m \in \mathbb{N}$

$A_{(2)}$ $m + n' = (m + n)'$ $(\forall) m, n \in \mathbb{N}$

$(A_2)$ ÷ $m(n+1) = (m+n) + 1$

Ex) Să se arate că $2 + 2 = 4$

$2 + 2 = 2 + 1' = (2+1)' = (2 + 0')' = ((2+0)')' = (2')' = 3' = 4$

$\varphi_1: \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ $\varphi_1(m, n) = m \cdot n$ a.î. $(I_1)$ $m \cdot 0 = 0$ $(\forall) m \in \mathbb{N}$

$(I_2)$ $m \cdot n' = mn + m$ $(\forall) m, n \in \mathbb{N}$

/ $m \cdot (n+1) = mn + m$

$a, b \in \mathbb{N}$, $a \leq b \Leftrightarrow \exists\, c \in \mathbb{N}$ a.î. $a + c = b$

$b \geq a$; $a < b \Leftrightarrow a \leq b$ și $a \neq b$.

$(\mathbb{N}, \leq)$ este bine ordonată, total ordonată

(c) Nu există șiruri strict descrescătoare de nr. naturale

$x^4 + y^4 = z^4 \Rightarrow x^4 + y^4 = z^4$ nu are sol întregi nenule

(Fermat) metoda coborârii infinite

Marea Th. a lui Fermat : $x_1 > x_2 > \dots$

Ecuația $x^n + y^n = z^n$ nu are sol. nenule întregi

$n = 3$ (Euler)

18.10.2019

$X \neq \emptyset, Y \neq \emptyset$ $\quad Dom\, f = \{x \in X \mid (\exists) y \in Y \text{ a.î. } x f y\}$

$f \subset X \times Y$ s.n. rel. funcțională dacă $(\forall) x_1 \in Dom\, f$,

$(\exists!)\ y \in Y$ a.î. $x f y$

Dacă în plus $Dom\, f = X$, atunci spunem că $f$ este o funcție

$x f y \overset{not}{=\!=} y = f(x)$

OBS: $f$ funct $\Rightarrow f$ rel funcțională

$\not\Leftarrow$

$X = \{1, 2, 3\}$, $f \subset X \times X$, $f = \{(1,1), (2,3)\}$ rel funct.

$Dom\, f = \{1, 2\} \subset X$ nu este o funct.

$f : X \to Y$, $\mathcal{F}(X, Y) = Y^X = \{f \mid f : X \to Y\}$

$A \subset X$, $A \neq \emptyset$, $f_A : A \to Y$, $f_A(x) = f(x)$, $(\forall) x \in A$.

această f. s.n. restricția lui $f$ la mulț. $A$

$\Delta_X : X \to X \quad \Delta_X \overset{\text{not}}{=} 1_X \;, \; 1_X(x) = x \;, (\forall) x \in X$ funcția identi...

$$X \xrightarrow{f} Y \xrightarrow{g} Z \quad, \; g\circ f : X \to Z$$

$$(g\circ f)(x) = g(f(x))$$

① $f : X \to Y$ injectivă: $(\forall)\; x_1, x_2 \in X \;,\; \underline{f(x_1) = f(x_2) \Rightarrow x_1 = x_2}$

$\Leftrightarrow : x_1 \neq x_2 \Rightarrow f(x_1) \neq f(x_2)$

② $f$ este surjectivă : $(\forall)\; y \in Y, (\exists)\; x \in X$ a. î. $f(x) = y$

$f$ este bijectivă dacă ① $\wedge$ ②

$f$ este inversabilă : $f^{-1} : Y \to X \;,\; f^{-1}(y) = x$ este o funcție

$$X \xrightarrow{f} Y \xrightarrow{f^{-1}} X \xrightarrow{f} Y, \quad f^{-1}\circ f = 1_X \;,\; 1_X : X \to X \;,\; 1_X(x) = x$$

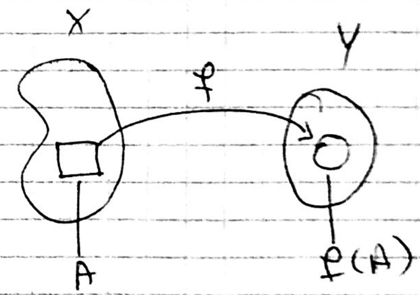
$f^{-1}\circ f \quad f\circ f^{-1}$

$$f\circ f^{-1} = 1_Y \;,\; 1_Y : Y \to Y \;,\; 1_Y(x) = x$$

---

$f : X \to X, \quad f\circ 1_X = f = 1_X \circ f$

---




Considerăm $f : X \to Y \;,\; A \subset X$

$f(A) = \{f(x) \mid x \in A\}$

$= \{y \in Y \mid (\exists)\; x \in A \text{ a. î. } f(x) = y\}$

→ imaginea directă a mulțimii A prin funcția f

$f(X) = \operatorname{Im} f \;,\; \operatorname{Im} f \subset Y$

Când $f$ e surjectivă $\operatorname{Im} f = Y$

---

$|X| = n$

$|Y| = m$ $\;,\; n, m \in \mathbb{N}^*$ finite

Câte funcții pot să construiesc de la X la Y

$|\mathcal{F}(X,Y)| = |Y^X| = |Y|^{|X|} = m^n$

---

$A_1, A_2 \subset X \;,\; f : X \to Y \;,\; f(A_1 \cap A_2) = f(A_1) \cap f(A_2)$ ?

NU

Ex: $f:\{1,2,3,4\} \to \{1,2,3,4\}$ $f(x)=\begin{cases}1 & \text{dacă } x\in\{1,2,3\}\\ 2 & \text{dacă } x=4\end{cases}$

$A_1=\{1,4\}$

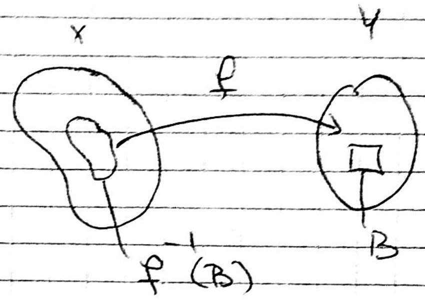
$A_2=\{2,4\}$

$f(A_1\cap A_2)=f\{4\}=2$

$f(A_1)\cap f(A_2)=\{1,2\}$

$f(A_1)=\{1,2\}$

$f(A_2)=\{1,2\}$




$f:X\to Y$, $B\subset Y$

$f^{-1}(B)=\{x\in X \mid f(x)\in B\}$

$\hookrightarrow$ imaginea inversă / reciproca a mulțimii B ~~din~~ prin f

Ex: Dați exemplu de o funcție $f: X\to X$, $B\subset X$ a.î. $f(f^{-1}(B))\neq$

## Cap 2. LEGI DE COMPOZIȚIE

$A\neq\emptyset$. $(\forall)\ f: A\times A\to A$, $(x,y)\to f(x,y)$ s.m. lege de comp. internă / operație algebrică internă

$f(x,y)\overset{\text{not}}{=} x*y$

Ex:

$\mathbb{Z}\times\mathbb{Z}\to\mathbb{Z}$, $(x,y)\to \text{cmmdc}(x,y)$ este o lege de comp

$(4,-6)=\pm 2$

NU

OBS: $|A|=n$, $n>1$ nr finit

Câte legi de comp pot să construiesc?

$|A|^{|A\times A|}=n^{n^2}$

„$*$" asociativă $(x*y)*z = x*(y*z)$ $(\forall)$ $x,y,z \in A$

Ex: „+" este asc. „+": $\mathbb{N} \times \mathbb{N} \to \mathbb{N}$ $(x,y) \to x+y$

$(x+y)+z = x+(y+z)$ $(\forall)$ $x,y,z \in \mathbb{N}$

Ex: $\mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$, $(x,y) \to x-y$ este asociativa? NU

$(x-y)-z = x-(y-z)$ „$-$" nu este asociativă pe $\mathbb{Z}$

---

„$*$" comutativă $x*y = y*x$ $(\forall)$ $x,y \in A$

$e \in A$ elem. neutru $(\forall)$ $x \in A$, $x*e = e*x = x$

OBS: Dacă există elem. neutru este unic

$x \in A$ simetrizabil (inversabil) $(\exists)$ $x' \in A$ a.î. $x*x' = x'*x = e$

$M = (A,*)$ s.n. semigrup („$*$" este asociativă)

Un semigrup cu elem. neutru s.n. monoid

grup $\Rightarrow$ monoid $\Rightarrow$ semigrup

$(\mathbb{N},+)$ $\not\Leftarrow$ $\not\Leftarrow$

Ex. $(\mathbb{N}^*,+)$

Un monoid în care orice elem este simetrizabil s.n. grup.

„$\cdot$" $(M,\cdot)$ monoid, $U(M) = \{x \in M \mid (\exists)\ x' \in M \text{ a.î. } x \cdot x' = x' \cdot x = 1\}$

mulțimea elem. inversabile / unităților

$H \neq \emptyset$

$H \subset M$ este parte stabilă: $(\forall)$ $x,y \in H \Rightarrow x \cdot y \in H$

$\cdot_H : H \times H \to H$, legea de comp indusă

(P)

Fie $(M,\cdot)$ un monoid și $a_1, a_2, \dots, a_m \in U(M)$, atunci

$a_1 a_2 \dots a_m \in U(M)$ și $(a_1 a_2 \dots a_m)^{-1} = a_m^{-1} a_{m-1}^{-1} \dots a_2^{-1} a_1^{-1}$. Dm plus $(U(M), \cdot)$ este un grup"

$(a_1 a_2 \dots a_{m-1} a_m)(a_m^{-1} a_{m-1}^{-1} \dots a_2^{-1} a_1^{-1}) = (a_1 a_2 \dots a_{m-1})(a_m a_m^{-1})(a_{m-1}^{-1} \dots a_2^{-1} a_1^{-1}) = (a_1 a_2 \dots a_{m-2})(a_{m-1} a_{m-1}^{-1}) \cdot (a_{m-2}^{-1} \dots a_2^{-1} a_1^{-1}) = \dots = a_1 a_1^{-1} = 1$

Ex: $a, b \in \mathbb{Z}$, $m \geq 2$, $a \equiv b \pmod{m} \Leftrightarrow m \mid (a-b) \Leftrightarrow \hat{a} = \hat{b}$

$\mathbb{Z}_m = \{\hat{0}, \hat{1}, \hat{2}, \dots, \widehat{m-1}\}$

$"\cdot": \mathbb{Z}_m \times \mathbb{Z}_m \to \mathbb{Z}_m$, $(\hat{x}, \hat{y}) \to \widehat{xy}$

$\hat{x} \cdot \hat{y} = \widehat{xy}$

$(\mathbb{Z}_m, \cdot)$ monoid comutativ

$(U(\mathbb{Z}_m), \cdot)$ grup ; $U(\mathbb{Z}_m) = \{\hat{x} \mid (x, m) = 1\}$

$|U(\mathbb{Z}_m)| = \varphi(m)$

$(\mathbb{Z}_m^*, \cdot)$ grup: $U(\mathbb{Z}_m) = \mathbb{Z}_m^* \Leftrightarrow m$ este prim

$(M, \cdot)$ monoid, dar devine grup $\Leftrightarrow U(M) = M^*$

Fie $(M, \cdot)$, $a \in M$, $a^0 = 1_M \Rightarrow 1_M = 1$

$a^m = \underbrace{a \cdot a \cdot a \dots a}_{m \text{ factori}}$, $m \geq 1$

$a^{-m} = (a^{-1})^m$, $m \in \mathbb{Z}$ când $a \in U(M)$

$a^m \cdot a^n = a^{m+n}$, $m, n \in \mathbb{N}^*$ $(a \in U(M);\ m, n \in \mathbb{Z}^*)$

$(a^m)^n = a^{m \cdot n}$, $m, n \in \mathbb{N}^*$

$a, b \in M$ $\quad a^m \cdot b^m = (a \cdot b)^m$ $\quad ab = ba$

$(M, \cdot)$, $(M_1, \cdot)$ monoizi

Def $\Rightarrow f: M \to M_1$, $f(xy) = f(x) \cdot f(y)$ și $f(1_M) = 1_{M_1}$ s.n. morfism de monoizi

Ex: $M \neq \emptyset$ , $P(M) = \{A \mid A \subseteq M\}$

$(P_{(M)}, \cap)$ , $(A,B) \to A \cap B$

$(P_{(M)}, \cup)$ , $(A,B) \to A \cup B$

$(P_{(M)}, \cap)$ monoid $(A \cap B) \cap C = A \cap (B \cap C)$ $(\forall)\ A,B,C \in P_{(M)}$

comutativ $A \cap B = B \cap A$

elem. neutru : $A \cap M = A$ $(\forall)\ A \in P(M)$ $\Rightarrow e = M$

$(P_{(M)}, \cup)$ monoid comutativ $(A \cup B) \cup C = A \cup (B \cup C)$, $(\forall)\ A,B,C \in$

$A \cup B = B \cup A$

elem. neutru : $A \cup \emptyset = A$ , $(\forall)\ A \in P(M)$ $\Rightarrow e = \emptyset$

$f : (P_{(M)}, \cup) \to (P_{(M)}, \cap)$ , $f(x) = Cx$

$C(A \cup B) = CA \cap CB$ C - complementa

1. $f(x \cup y) = C(x \cup y) = Cx \cap Cy = f(x) \cap f(y)$ $(\forall)\ x, y \in P_{(M)}$

2. $f(\emptyset) = C\emptyset = M$

Un monoid $(M, \cdot)$ cu toate elem. inversabile se n. grup

Fie $G$ un grup : $(G, \cdot)$ Ex: $(\mathbb{Z}, +)$, $(\mathbb{R}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{C}, +)$

$(\mathbb{Q}^*, \cdot)$, $(\mathbb{R}^*, \cdot)$, $(\mathbb{C}^*, \cdot)$

$G$ s.n. grup finit dacă $|G| < +\infty$ (cardinal de $G$ finit)

$|G| = 4$ : $(\mathbb{Z}_2 \times \mathbb{Z}_2, +)$ ; $(\mathbb{Z}_4, +)$

---

$G$, $G_1$ grupuri : $(G \times G_1, \cdot)$ produsul direct al grupurilor $G$ și $G_1$

$G \times G_1 = \{(a,b) \mid a \in G, b \in G_1\}$

$(a,b)(a_1,b_1) = (aa_1, bb_1)$

$(1_G, 1_{G_1})$ $1_G = 1$ $1_{G_1} = 1$

$(a,b)^{-1} = (a^{-1}, b^{-1})$

Tema Construiți tablele celor 2 grupuri

$G$ $(G,\cdot)$ $\mathbb{N}\subset\mathbb{Z}\subset\mathbb{Q}\subset\mathbb{R}\subset\mathbb{C}$

grup

Ex: 1) $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ și $\mathbb{C}$ „+"

2) $\mathbb{Q}^*, \mathbb{R}^*, \mathbb{C}^*$ ; „$\cdot$"

---

$A\neq\emptyset$, $A^A=\{f \mid f\ A\to A\}$ $(f,g)\to f\circ g$, $(f\circ g)(x)=f(g(x))$

$(A^A,\circ)$ monoid comutativ

$1_A \overset{\text{not}}{=} 1_A : A\to A$

$1_A(x)=x$ elem neutru

$f\circ g\neq g\circ f$

$(U(A^A),\circ)$ grup $U(A^A)\overset{\text{not}}{=} S_A$ grupul perm mult. $A$

$A=\{1,2,\dots,n\}$ $S_A \overset{\text{not}}{=} S_n$ grupul perm. de gradul $n$

$G, H$ | $(G,\cdot)$ și $(H,\circ)$

$(G\times H,\circ)$

$G\times H=\{a,b \mid a\in G, b\in H\}$ $(a,b)\cdot(a,b)=(aa,bb)$

→ produsul direct al grupului $G$ și $H$ $(1_G, 1_H)$

$G=H$, $G^2\overset{\text{not}}{=} G\times G$ $(a,b)^{-1}=(a^{-1},b^{-1})$

Ex) $(\{\pm 1\}^2,\cdot)$ grupul lui Klein

Ex $(\mathbb{Z}^{\mathbb{N}},+)$ $\mathbb{Z}^{\mathbb{N}}=\{f \mid f:\mathbb{N}\to\mathbb{Z}, f(n)=a_n\}$

$a_n=a_0a_1\dots$

## 2. MORFISME DE GRUPURI

$G, G_1$

Def: $f: G\to G_1$ s.n. morfism de grupuri dacă $f(x,y)=f(x)\cdot f(y)$

$(\forall)\ x,y\in G$

$f(xy) = f(x) \cdot f(y)$ $(\forall)\ x, y \in G$

2. $f(1_G) = 1_{G_1}$ ; $1_G, 1_{G_1}$ - elem. neutre

Ex 1. $f : G \to G_1$, $f(x) = 1_{G_1}$

2. $1_G : G \to G$, $1_G(x) = x$

3. $f_a : G \to G$ $\quad f_a(x) = a x a^{-1}$ morfismul interior definit pe a

$f$ morfism bijectiv, vom spune că $f$ este un izomorfism
$G \overset{f}{\simeq} G_1$

$f : G \to G$ izomorfism s.n. automorfism.

Ex: $(\mathbb{R}, +) \overset{f}{\simeq} (\mathbb{R}_+^*, \cdot)$ $\quad$, $f(x) = 3^x$

$f(x+y) = 3^{x+y} = 3^x \cdot 3^y = f(x) \cdot f(y)$

Ex: $(\mathbb{R}, +) \not\simeq (\mathbb{R}^*, \cdot)$ $\quad$ În general dacă $K$ este un corp comutativ, $(K, +) \not\simeq (K^*, \cdot)$

OBS:

1. Compunerea a două morfisme de grupuri este un morfism de grupuri.

2. Relația „izomorfism de grupuri" este o relație de echivalență.

$(\{\pm 1\}^2, \cdot)$, $(\mathbb{Z}_2 \times \mathbb{Z}_2, +)$, $K = \{1, a, b, c \mid a^2 = b^2 = c^2 = 1\}$
↳ grupuri Klein

## SUBGRUPURI

Fie $G$ un grup și $H \subset G$, $H \neq \emptyset$

Def: Spunem că $H$ este un subgrup al lui $G$ $(H \leq G)$ dacă $(\forall)\ x, y \in H$ avem: $xy \in H$ și $y^{-1} \in H$

1) $(\forall)\ x, y \in H \Rightarrow x \cdot y \in H$ și $y^{-1} \in H \Leftrightarrow (\forall)\ x, y \in H, (x \cdot y^{-1}) \in H$

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

2) $H \leq G \Leftrightarrow (H, \cdot)$ este un grup.

---

$G \neq \{1\}$

$\{1\}$ subgrupul trivial; $G$ subgrupul impropriu

$(\forall)\ H \leq G,\ H \neq \{1\},\ H \neq G$ s.n. subgrup ~~im~~ propriu

---

Fie $H, K \leq G$

1. Atunci $H \cap K \leq G$ ( fie $x, y \in H \cap K \Rightarrow x, y \in H$ și $x, y \in K \Rightarrow$ $\Rightarrow x^{-1}y \in H$ și $x^{-1}y \in K \Rightarrow xy^{-1} \in H \cap K$ )

$\bigcap H_i \leq G$

$H_i \leq G$ intersecția arbitrară a unei familii de subgr.

2. $H \cup K \not\leq G$ ($H \cup K \leq G \Leftrightarrow H \subset K$ sau $K \subset H$; generalizare)

? $f: G \longrightarrow G_1$ morfism de grupuri

1. $H \leq G \Rightarrow f(H) \leq G_1$
2. $H_1 \leq G_1 \Rightarrow f^{-1}(H_1) \leq G$

Proprietate:

Fie $f: G \to G_1$ morfism de grupuri.

a) Dacă $H \leq G$ atunci $f(H) \leq G_1$

$f(H) = \{f(x) \mid x \in H\}$

---

Dem: $x, y \in H$

$f(x), f(y) \in f(H) \overset{?}{\Rightarrow} f(x) \cdot f(y)^{-1} \in f(H)$

Fie $x, y \in H$ : $f(x) \cdot f(y)^{-1} = f(x) \cdot f(y^{-1}) = f(xy^{-1}) \in f(H)$

---

b) Dacă $H_1 \leq G_1$ atunci $f^{-1}(H_1) \leq G$

$\mathrm{Ker} f = f^{-1}(1_{G_1})$

↳ nucleul morfismului $f$

$\operatorname{Ker} f = \{x \in G \mid f(x) = 1_{G_1}\}$ $\quad \operatorname{Ker} f \leq G$

**Proprietate:**

Fie $f : G \to G_1$ un morfism de grupuri:

$f$ este inj $\Leftrightarrow \operatorname{Ker} f = \{1_G\}$

**Dem:** „$\Rightarrow$" Admitem că $f$ este inj. şi fie $x \in \operatorname{Ker} f$

$$\left.\begin{array}{l} f(x) = 1_{G_1} \\ f(1_G) = 1_{G_1} \end{array}\right\} \Rightarrow x = 1_G \Rightarrow \operatorname{Ker} f = \{1_G\}$$

„$\Leftarrow$" Admitem $\operatorname{Ker} f = \{1_G\}$ şi fie $x, y \in G$ a.î. $f(x) = f(y)$

$f(x) \cdot f(y)^{-1} = 1_{G_1}$

$f(x) \cdot f(y^{-1}) = 1_{G_1}$

$f(xy^{-1}) = 1_{G_1} \Rightarrow xy^{-1} = 1_G \Rightarrow x = y$

**Ex:** $\mathbb{Z}_3 = \{\hat{0}, \hat{1}, \hat{2}\}$ $\quad \mathbb{Z}_2 = \{\bar{0}, \bar{1}\}$

$f : \mathbb{Z}_3 \to \mathbb{Z}_2 \quad f(\hat{x}) = \bar{x}^2$, $\quad f(\hat{x}\hat{y}) = \overline{xy}^2 = \bar{x}^2 \cdot \bar{y}^2 = f(\hat{x}) \cdot f(\hat{y})$

morfism de monoizi

$f(\hat{0}) = \bar{0}^2 = \bar{0}$

$f(\hat{1}) = \bar{1}^2 = \bar{1}$ $\qquad \operatorname{Ker} f = \{\hat{1}\} \not\Rightarrow f$ injectivă

$f(\hat{2}) = \bar{0}$ $\qquad f$ nu este inj.

$(\mathbb{Z}, +)$ $\quad$ Pentru fiecare $n \in \mathbb{N}$, $n\mathbb{Z} = \{nk \mid k \in \mathbb{Z}\}$

**Prop:** $H$ este un subgrup al lui $(\mathbb{Z}, +) \Leftrightarrow H = n\mathbb{Z}$, $n \geq 0$

**Dem:** $n\mathbb{Z} \leq G$ : $x, y \in n\mathbb{Z}$, $x = nk$, $y = nl$, $x - y = n(k-l) \in n\mathbb{Z}$

$\Rightarrow n\mathbb{Z} \leq \mathbb{Z}$

Fie $H \leq \mathbb{Z}$

1) $H = \{0\}$, $H = 0\mathbb{Z}$

2) $H \neq \{0\}$ $\quad m \in H \Rightarrow -m \in H$, în $H$ există nr. nat. nenule,

fie $n$ cel mai mic nr. nat. nenul din $H$

$H = n\mathbb{Z}$ $\qquad n \cdot 1 = n \in H \Rightarrow n\mathbb{Z} \subset H$

$H \subset n\mathbb{Z}$

Fie $h \in H$, $h = nq + r$, $0 \leq r < n$

$h \in H, n \in H \Rightarrow h, nq \in H \Rightarrow h - nq \in H \Rightarrow r \in H \Rightarrow \underline{r = 0}$

Fie $G$ un grup, $\emptyset \neq A \subseteq G$

$<A> = \{ a_1^{\pm 1} a_2^{\pm 1} \dots a_m^{\pm 1} \mid a_1, a_2, \dots a_m \in A \}$

↳ subgrupul generat de mulțimea $A$

Fie $x, y \in <A> \Rightarrow xy \in <A>$

$x \in <A>$, $x = a_1^{\varepsilon_1} a_2^{\varepsilon_2} \dots a_m^{\varepsilon_m}$, $\varepsilon_1, \varepsilon_2 \dots \varepsilon_m \in \{-1, 1\}$

$x^{-1} = a_m^{-\varepsilon_m} \dots a_2^{-\varepsilon_2} a_1^{-\varepsilon_1} \in <A>$

$<\emptyset> = \{1\}$ ; $A \subset <A>$, $<G> = G$

$A = \{a\}$, $<A> = \{a^k \mid k \in \mathbb{Z}\}$ subgrup ciclic

$G$ este generat de mult. $A$ dacă $<A> = G$. Dacă în plus $|A| < +\infty$, atunci $G$ este finit generat

Ex $G$ grup, $A \subset G$, $<A> = \bigcap\limits_{\substack{H \leq G \\ A \subset H}} H$ $\boxed{\text{Temă!}}$

$G = <a>$ grup ciclic

Ex: $(\mathbb{Z}, +) = <1> = <-1>$

$(\mathbb{Z}_n, +) = <\hat{1}>$

$\mathbb{Z}_m = \{\hat{0}, \hat{1}, \dots, \widehat{m-1}\}$

$\widehat{x+y} = \hat{x} + \hat{y}$

OBS: Un grup ciclic $G$ este abelian

Dem: Fie $x, y \in G$ : $x = a^k$, $y = a^\ell$, $k, \ell \in \mathbb{Z}$

$xy = a^k a^\ell = a^{k+\ell} = a^{\ell+k} = a^\ell \cdot a^k = yx$

P) $H \leq \mathbb{Z} \Leftrightarrow H = m\mathbb{Z}$, $m \geq 0$

$a, b \in \mathbb{Z}$

$a \equiv b \pmod{m} \Leftrightarrow m \mid (a-b) \Leftrightarrow a - b = mk$, $k \in \mathbb{Z} \Leftrightarrow a - b \in m\mathbb{Z}$

Generalizăm: $G$ un grup, $H \leq G$

$x, y \in G$

$x \equiv_s y \pmod{H} \Leftrightarrow x^{-1}y \in H$ RELAȚIA DE CONGRUENȚĂ LA STÂNGA mod H

$x \equiv_d y \pmod{H} \Leftrightarrow xy^{-1} \in H$ RELAȚIA DE CONGRUENȚĂ LA DREAPTA mod H

P) „$\equiv_s \pmod{H}$" și „$\equiv_d \pmod{H}$" sunt relații de echivalență

Dem:

Arătăm pt „$\equiv_s \pmod{H}$"

(r) $x \equiv_s x \pmod{H} \Leftrightarrow x^{-1}x = 1 \in H$

(s) $x \equiv_s y \pmod{H} \Rightarrow x^{-1}y \in H \Rightarrow (x^{-1}y)^{-1} \in H \Rightarrow y^{-1}x \in H \Rightarrow y \equiv_s x \pmod{H}$

(t) $x \equiv_s y \pmod{H}$ și $y \equiv_s z \pmod{H} \Rightarrow x^{-1}y \in H$ și $y^{-1}z \in H \Rightarrow$

$\Rightarrow (x^{-1}y)(y^{-1}z) \in H \Rightarrow x^{-1}z \in H \Rightarrow x \equiv_s z \pmod{H}$

$x \equiv_s y \pmod{H} \Leftrightarrow x^{-1}y \in H \Rightarrow y \in xH$

$G/_{\equiv_s \pmod{H}} \overset{not}{=\!=} (G/_H)_s = \{\hat{x} = xH \mid x \in G\}$ mulțimea claselor la stânga (mod H)

$H = G$, $(G/G)_s$ - G factorizat prin G la stânga

$x \equiv_s y \pmod{G} \Leftrightarrow x^{-1}y \in G$

$(G/G)_s = G$

---

$x \equiv_s y \pmod{H} \Leftrightarrow x^{-1}y \in H \Leftrightarrow y \in xH$ ; $(G/_H)_s = \{\hat{x} \mid x \in G\}$ $\hat{x} = xH$

$\hat{x} \equiv_d y \pmod{H} \Leftrightarrow xy^{-1} \in H \Leftrightarrow x \in yH$ ; $(G/H)_d = \{\bar{x} \mid x \in G\}$ $\bar{x} = Hx$

OBS: $(G/H)_s = (G/H)_d$ ; $xH = Hx \Leftrightarrow H \subset xHx^{-1}$

$\Leftrightarrow H \trianglelefteq G$ (H este un subgrup normal)

$H \trianglelefteq G \Leftrightarrow (\forall) x \in G, h \in H \Rightarrow xhx^{-1} \in H$

$|(G/_H)_s| = |(G/_H)_d| = |G : H|$

indicele lui H în G

Ex: $|G, H| = 2$

$(G/H)_s = (G/H)_d = \{H, G \setminus H\}$

Th Lagrange

Fie $G$ un grup finit și $H \leq G$ Atunci $|G| = |H| \cdot |G : H|$

8.11.2019

$(G, \cdot)$ gr. și $H \leq G$

$x, y \in G$ $\quad x \equiv_s y \pmod H \Leftrightarrow x^{-1} y \in H \Leftrightarrow y \in xH$

$x \equiv_d y \pmod H \Leftrightarrow x y^{-1} \in H \Leftrightarrow x \in Hy$

$(G/H)_s = \{ \hat{x} = xH \mid x \in G \}$

$(G/H)_d = \{ \bar{x} = Hx \mid x \in G \}$

$x \equiv_s y \pmod H \Leftrightarrow x^{-1} y \in H \Leftrightarrow y \in xH \Leftrightarrow \hat{x} = \hat{y}$

---

(P) $G$ grup și $H \leq G$; $|(G/H)_s| \overset{\text{not}}{=} |G : H|$ (indicele lui $H$ în $G$)

$\Downarrow$

$f : G \to G$, $f(x) = x^{-1}$ bijectivă, $f \circ f^{-1} = 1_G$ ($1_G : G \to G$, $1_G(x) = x$ $\forall x \in$

$(G/H)_s \longrightarrow (G/H)_d$

$x \in G$, $f(xh) = (xh)^{-1} = h^{-1} x^{-1}$, $f(xH) = Hx^{-1}$

Cum $(G/H)_s$ și $(G/H)_d$ sunt partiții pt $G$ $\Big\} \Rightarrow |(G/H)_s| = |(G/H)_d| = |G : H|$

$(G/H)_s = (G/H)_d \Leftrightarrow xH = Hx \Leftrightarrow xHx^{-1} \subset H \Leftrightarrow H \trianglelefteq G$ ($H$ este un subgrup normal)

Th. Lagrange.

Fie $G$ un grup finit și $H$ un subgrup al lui $G$. Atunci $|G| = |H| \cdot |G : H|$

În particular $|H| \mid |G|$

Dem:

Conform proprietății anterioare este suficient să lucrăm cu clase la stânga modulo $H$

Fie $C_1 = x_1 H$, $C_2 = x_2 H$, ..., $C_s = x_s H$, $C_i \in (G/H)_s$, $i = \overline{1, s}$

$G = \bigcup_{i=1}^{s} C_i \Rightarrow |G| = \sum_{i=1}^{s} |C_i|$ (1)

$x \in H$ ... $H \to aH$, $x \to ax$ este bijectivă $(y \to ya)$

$|H| = |C_i|$ (2)

Din (1) și (2) $\Rightarrow |G| = \sum_{i=1}^{s} |H| = s\,|H| = |G:H| \cdot |H|$

$|G| = |H|\,|G:H|$, $|H|\,\big|\,|G|$ și $|G:H|\,\big|\,|G|$

<u>Ex</u>: $(\mathbb{Z}_4, +)$ $\mathbb{Z}_4 = \{\hat{0}, \hat{1}, \hat{2}, \hat{3}\}$ $\hat{x} + \hat{y} = \widehat{x+y}$

Subgrupurile lui $\mathbb{Z}_4$?

Fie $H \leq \mathbb{Z}_4$. Conf. Th. L. $\Rightarrow |H|\,\big|\,|\mathbb{Z}_4| \Rightarrow |H| \in \{1, 2, 4\}$

$|H| = 1 \Rightarrow H = \{\hat{0}\}$

$|H| = 2 \Rightarrow H = \{\hat{0}, \hat{x} \mid \hat{x} + \hat{x} = \hat{0}\} \Rightarrow H = \{\hat{0}, \hat{2}\} = \langle \hat{2} \rangle$

$\hat{2} + \hat{2} = \hat{0}$

$|H| = 4 \Rightarrow H = \mathbb{Z}_4$

<u>Ex</u>: Det. subgrupurile grupului $K = \{1, a, b, c \mid a^2 = b^2 = c^2 = 1\}$

$(G, \cdot)$

$$x \in G,\ ord(x) = \begin{cases} +\infty & \text{dacă } x^m \neq 1\ (\forall)\, m \geq 1 \\ \text{cel mai mic } m \mid x^m = 1 & \text{dacă există } m \in \mathbb{N}^* \text{ a.i. } x^m = 1 \end{cases}$$

$ord(1) = 1$

<u>Ex</u>: $(\mathbb{Z}, +)$; $ord(0) = 1$

$x \in \mathbb{Z}, x \neq 0$; $\nexists\, m \in \mathbb{N}^*$: $\underbrace{x + x + \ldots + x}_{m \text{ ori}} = 0 \Rightarrow mx = 0 \Rightarrow ord(x) = +\infty$

$\langle x \rangle = \{x^k \mid k \in \mathbb{Z}\}$

<u>OBS</u>: Dacă $G$ este un grup finit, $|G| = m$ ($m \in \mathbb{N}^*$ finit) și $x \in G$, atunci $ord(x) \mid m$ și $x^m = 1$

$ord(x) = ord\,|\langle x \rangle|$, $\langle x \rangle \leq G$ și folosind Th. Lagrange $\Rightarrow$

$\Rightarrow ord(x) \mid m$

$ord(x) = k$, $m = kq$, $q \in \mathbb{N}$

$x^m = x^{kq} = (x^k)^q$ ...

Th. ~~...~~ Cauchy

. Fie $G$ un grup finit și $p$ un nr. prim ce divide ordinul lui $G$ $(p \mid |G|)$. Atunci există un element $x \in G$ a.î. $ord(x) = p$

---

OBS: $|G| = m$, $x \in G$, $ord(x) \mid |G|$, $x^m = 1$

$(\mathbb{Z}_m, \cdot)$ $\quad (U(\mathbb{Z}_m), \cdot)$ - grup ; $U(\mathbb{Z}_m) = \{ \hat{x} \in \mathbb{Z}_m^* \mid (x, m) = 1 \}$

$|U(\mathbb{Z}_m)| = \varphi(m)$, $\varphi : \mathbb{N}^* \to \mathbb{N}^*$

$\varphi(m) = |\{ k \mid 1 \leq k < m, (k, m) = 1 \}|$

$\Downarrow$

Th. Euler. Fie $a \in \mathbb{Z}$, $m \geq 1$, $(a, m) = 1$, atunci $a^{\varphi(m)} \equiv 1 (\mathrm{mo}$

Pt $m = p$ nr. prim $\Rightarrow$ (Mica Th. a lui Fermat) : $a^{p-1} \equiv 1 (\mathrm{mod}$

$\varphi(p) = p - 1$

---

$H \leq G$

$(G/H)_s \equiv (G/H)_d \iff xH = Hx \iff xHx^{-1} \subset H$

Def: $H$ este un subgrup normal al lui $G$ dacă $(\forall) x \in G$
$h \in H \Rightarrow xhx^{-1} \in H$

OBS:

1. $G$ grup $\quad \{1\}, G \trianglelefteq G$
2. $G$ abelian , $(\forall) H \leq G \Rightarrow H \trianglelefteq G$
3. $|G : H| = 2 \Rightarrow H \trianglelefteq G$ $\quad\Big|\; 1H = H \Rightarrow H \in (G/H)_s$

   $(G/H)_s = \{ H, G \setminus H \} = (G/H)_d$ $\quad\Big|\; H1 = H$

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

---

$f : G \to G$ morfism de grupuri

$\mathrm{Ker} f = \{ x \in G \mid f(x) = 1 \}$, $1 = 1_{G'}$

$\mathrm{Im} f = f(G) = \{ f(x) \mid x \in G \}$

Proprietate: Dacă $G, G'$ sunt două grupuri și $f : G \to G'$ un morfism de grupuri, atunci $\mathrm{Ker} f \trianglelefteq G$

Dem: $\operatorname{Ker} f = \{ x \in G \mid f(x) = 1 \}$

Fie $x \in G$ şi $h \in \operatorname{Ker} f \overset{?}{\Rightarrow} x h x^{-1} \in \operatorname{Ker} f$

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

## GRUPUL FACTOR

Fie $G$ un grup şi $H$ un subgrup ~~maximal~~ al lui $G$, definim

$G/H = \{ \hat{x} \mid x \in G \}$ , $\hat{x} = \bar{x} = xH$

$\hat{x} \cdot \hat{y} = \widehat{xy}$ bine definită : $\hat{x} = \hat{x'}$ ; $\hat{y} = \hat{y'} \Rightarrow \widehat{xy} = \widehat{x'y'}$

(?) $(G/H, \cdot)$ este un grup (grupul factor al lui $G$ în raport cu ...) şi $p : G \to G/H$ , $p(x) = \hat{x}$ surjecţia canonică este un morfism de grupuri.

$(\hat{x} \cdot \hat{y}) \hat{z} = \widehat{xy} \, \hat{z} = \widehat{xyz} = \widehat{x(yz)} = \hat{x} \, \widehat{yz} = \hat{x} (\hat{y} \hat{z})$

$\hat{x} \cdot \hat{1} = \widehat{x \cdot 1} = \hat{x} = \widehat{1 \cdot x} = \hat{1} \, \hat{x}$

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

$p(xy) = \widehat{xy} = \hat{x} \, \hat{y} = p(x) \, p(y)$ $(\forall) \, x, y \in G$

$(G/H, \cdot)$ grup factor $(H \trianglelefteq G)$

$G/H$ ; $G$ abelian $\Rightarrow (\forall) \, H \leq G \Rightarrow H \trianglelefteq G$ $G/H$ $(\forall) \, H \leq G$

OBS: $G$ este abelian $\Rightarrow$ $G/H$ este abelian ($\hat{x} \hat{y} = \widehat{xy} = \widehat{yx} = \hat{y} \hat{x}$)

Ex: $(\mathbb{Z}, +)$ , $H \leq \mathbb{Z}$, $H = m\mathbb{Z} \trianglelefteq \mathbb{Z}$ , $m \geq 0$

(I) $H = \{0\}$ (pt $m = 0$) $\Rightarrow \mathbb{Z}/\{0\} = \mathbb{Z}$

(II) $H = m\mathbb{Z}$ , $m > 0$

$x, y \in \mathbb{Z}$ , $x \equiv y \pmod{m\mathbb{Z}} \Leftrightarrow x - y \in m\mathbb{Z} \Rightarrow x - y = mk$ , $k \in \mathbb{Z}$

$\Leftrightarrow x \equiv y \pmod{m}$

$\mathbb{Z}/m\mathbb{Z} = \mathbb{Z}_m$

Th. fundamentală de izomorfism la grupuri

Fie $f: G \to G'$ un morfism de grupuri, atunci există un izomorfism $\bar{f}: G/_{Ker f} \to Im f$

Dem: $\bar{f}: G/_{Ker f} \to Im f$, $\bar{f}(\hat{x}) = f(x)$

- Arătăm că $\bar{f}$ este bine definită: $\hat{x} = \hat{y} \Rightarrow \bar{f}(\hat{x}) = \bar{f}(\hat{y})$

$x \equiv_s y \pmod{Ker f} \Leftrightarrow x^{-1}y \in Ker f \ (f(x^{-1}y) = 1) \Rightarrow \hat{x} = \hat{y}$

$\hat{x} = \hat{y} \Rightarrow x^{-1}y \in Ker f \Rightarrow f(x^{-1}y) = 1 \Rightarrow f(x^{-1}) \cdot f(y) = 1 \Rightarrow$

$\Rightarrow f(x)^{-1} f(y) = 1 \Rightarrow f(x) = f(y) \Rightarrow \bar{f}(\hat{x}) = \bar{f}(\hat{y})$

- $\bar{f}$ este injectivă $\Rightarrow$ din construcție $(\forall)\ y = f(x) \in Im f$

$(\exists)\ \hat{x} \in G/_{Ker f}$ a.î. $\bar{f}(\hat{x}) = f(x)$

- $\bar{f}$ este injectivă: $\bar{f}(\hat{x}) = \bar{f}(\hat{y}) \overset{?}{\Rightarrow} \hat{x} = \hat{y}$

$\bar{f}(\hat{x}) = \bar{f}(\hat{y}) \Rightarrow f(x) = f(y) \Rightarrow f^{-1}(x) \cdot f(y) = 1 \Rightarrow f(x^{-1}y) = 1$

$\Rightarrow \underline{x^{-1}y \in Ker f} \Rightarrow \hat{x} = \hat{y}$

- $\bar{f}$ este morfism de grupuri: $\bar{f}(\hat{x} \cdot \hat{y}) = \bar{f}(\widehat{xy}) = f(xy) = f(x) f(y)$

$= \bar{f}(\hat{x}) \cdot \bar{f}(\hat{y}) \Rightarrow \bar{f}$ este izomorfism $\Rightarrow$

$\Rightarrow G/_{Ker f} \simeq Im f$

OBS: SCUFUNDARE

$f: G \to G'$ un morfism injectiv $\overset{?}{\Rightarrow} G \leq G'$

$f$ injectivă $\Leftrightarrow Ker f = \{1\}\ (f(1) = 1)$ $\Big/ \Rightarrow G/_{Ker f} \simeq Im f$

Th. f de izom. $\quad G \simeq Im f,\ Im f \leq G \Rightarrow G \leq G'$

Ex:

Fie $(\mathbb{C}^*, \cdot)$ și $(\mathbb{R}^*_+, \cdot)$ $\quad T = \{z \in \mathbb{C}^* \mid |z| = 1\}$

Să se arate că $\mathbb{C}^*/_T \simeq \mathbb{R}^*_+$

$f: \mathbb{C}^* \to \mathbb{R}^*_+$ morfism surjectiv $\xrightarrow{\underline{Th. f. izo}} \mathbb{C}^*/_{Ker f} \simeq Im f = \mathbb{R}$

$f: \mathbb{C}^* \to \mathbb{R}^*_+$, $f(z) = |z|$ surjectivă $(Im f = \mathbb{R}^*_+)$

$f(z_1 z_2) = |z_1 z_2| = |z_1| \cdot |z_2| = f(z_1) \cdot f(z_2)$ morfism

Conform Th. f. de izomor.: $\mathbb{C}^*/_{Ker f} \simeq \mathbb{R}^*_+$ $\Big\} \Rightarrow \mathbb{C}^*/_T \simeq \mathbb{R}^*_+$

$Ker f = \{z \in \mathbb{C}^* \mid f(z) = 1\} = \{z \in \mathbb{C}^* \mid |z| = 1\} = T$

15.11.2019

① $f: G \to G'$ un morfism de grupuri, atunci $(\exists)\ \bar{f}: G/_{Kerf} \to Imf$ izomorfism

$Kerf = \{x \in G \mid f(x) = 1_{G'}\} \trianglelefteq G$, $\quad Imf = \{f(x) \mid x \in G\} \trianglelefteq G'$

$G/_{Kerf} = \{\hat{x} = xKerf \mid x \in G\}$

OBS: $f: G \to G'$ scufundare (morfism injectiv)

$Kerf = \{1_G\}$ : $G/_{\{1_G\}} \simeq Imf$, $G \simeq Imf$, $Imf \leq G'$

$\therefore G \leq G'$

Ex Fie $G$ un grup $(G, \cdot)$ şi pt fiecare $g \in G$, $f_g(x^{-1}) = gxg^{-1}$;

$Im(G) = \{f_g \mid g \in G\}$

$Z(G) = \{y \in G \mid xy = yx\ (\forall) x \in G\}$ (centrul lui $G$)

Să se arate $G/_{Z(G)} \simeq Im(G)$

$T_1$ (de izomorfism)

Fie $G$ un grup şi $H, N$ subgrupuri normale ale lui $G$, a.î. $H \subset N$

Atunci $N/_H \trianglelefteq G/_H$ şi $\dfrac{G/H}{N/H} \simeq G/_N$

Fie $f: G/_H \to G/_N$, $f(\hat{x}) = \bar{x}$ : $G/H = \{\hat{x} = xH \mid x \in G\}$

$G/_N = \{\bar{x} = xN \mid x \in G\}$

$\hat{x} = \hat{y} \iff x^{-1}y \in H$

$\bar{x} = \bar{y} \iff x^{-1}y \in N$

- $f$ este bine definită : $\hat{x} = \hat{y} \Rightarrow x^{-1}y \in H \overset{H \subset N}{\Rightarrow} x^{-1}y \in N \Rightarrow$
  $\Rightarrow \bar{x} = \bar{y} \Rightarrow f(\hat{x}) = f(\hat{y})$
- $f$ este surjectivă : $\bar{x} = xN$, $(\exists)\ \hat{x} = xH$ a.î. $f(\hat{x}) = \bar{x}$
- $f$ este morfism : $f(\hat{x} \cdot \hat{y}) = f(\widehat{xy}) = \overline{xy} = \bar{x} \cdot \bar{y} = f(\hat{x}) \cdot f(\hat{y})$
  $(\forall)\ \hat{x}, \hat{y} \in G/_H$

Aplicând TR. fundamentală de izomorfism:

$G/_H/_{Kerf} \simeq Imf = G/_N$ ①

Arătăm că $Kerf = N/_H$

$\ker f = \{ \hat{x} \in G/H \mid f(\hat{x}) = \bar{1} \}$

Fie $\hat{x} \in \ker f \Rightarrow f(\hat{x}) = \bar{1} \Rightarrow \bar{x} = \bar{1} \Rightarrow x \in N \Rightarrow \hat{x} \in N/H$
Fie $\hat{x} \in N/H \Rightarrow x \in N \Rightarrow \bar{x} = \bar{1} \Rightarrow f(\hat{x}) = \bar{1} \Rightarrow \hat{x} \in \ker f$ $\Bigg\} \Rightarrow$

$\Rightarrow \ker f = N/H$ (2)

(1) + (2) $\Rightarrow \dfrac{G/H}{N/H} \simeq G/N$

---

$G$ grup, $G = \langle a \rangle$, $a \in G$, $G$ este ciclic

$G = \langle a \rangle = \{ a^k / k \in \mathbb{Z} \}$

$$(G, \cdot) \quad a^k = \begin{cases} \underbrace{a \cdot a \cdot \ldots \cdot a}_{k \text{ factori}} & k > 0 \\ 1 & k = 0 \\ \underbrace{a^{-1} \cdot a^{-1} \cdot \ldots \cdot a^{-1}}_{k^{-1} \text{ factori}} & k < 0 \end{cases}$$

Exemple:

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

$\mathbb{Z}_m = \{ \hat{0}, \hat{1}, \hat{2} \ldots \widehat{m-1} \}$ $\quad \hat{x} + \hat{y} = \widehat{x+y}$

$(\mathbb{Z}_m, +) = \langle \hat{1} \rangle$

---

Teoremă: Orice grup ciclic $G$ este izomorf cu $\mathbb{Z}$ sau cu un anumit grup $\mathbb{Z}_m$, $m \geq 1$

Dem. $G = \{ a^k / k \in \mathbb{Z} \}$

Fie $f : \mathbb{Z} \to G$, $f(k) = a^k$

$f$ este o aplicație surjectivă

$f$ este morfism: fie $k, l \in \mathbb{Z}$, $f(k+l) = a^{k+l} = a^k \cdot a^l =$
$= f(k) \cdot f(l)$

Aplicăm Teorema fundamentală de izomorfism $\Rightarrow$

$\mathbb{Z}/\ker f \simeq \operatorname{Im} f = G$

$\ker f \trianglelefteq \mathbb{Z} \Rightarrow \ker f = m\mathbb{Z}$, $m \in \mathbb{N}$

I $\ker f = \{0\}$ (pt $m = 0$) $\Rightarrow \mathbb{Z}/\{0\} \simeq G \Rightarrow G \simeq \mathbb{Z}$

II $\ker f = m\mathbb{Z}$, $m > 0 \Rightarrow \mathbb{Z}/m\mathbb{Z} \simeq G \Rightarrow \mathbb{Z}_m \simeq G$

Obs: Dacă $a \in G$ este un generator al lui $G$ : $G = \langle a \rangle$

I $ord(a) = +\infty \Rightarrow G \simeq \mathbb{Z}$

II $ord(a) = n < +\infty \Rightarrow G \simeq \mathbb{Z}_n$

Obs: Orice subgrup și grup factor al unui grup ciclic este ciclic.

Ex: Determinați subgrupurile și grupurile factor pt $(\mathbb{Z}_{12}, +)$

Fie $H \leq \mathbb{Z}_{12}$

$ord(H) \mid ord(\mathbb{Z}_{12}) \Rightarrow ord(H) = \{1, 2, 3, 4, 6, 12\}$

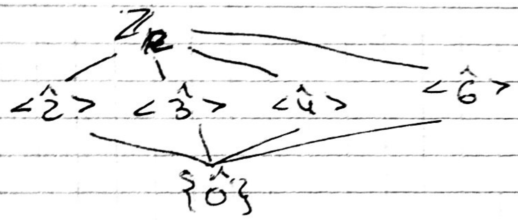
$ord(H) = 1 \Rightarrow H = \{\hat{0}\}$

$ord(H) = 2 \Rightarrow H = \{\hat{0}, \hat{x} \mid \hat{x} + \hat{x} = \hat{0}\} \Rightarrow \{\hat{0}, \hat{6}\} \quad \langle \hat{6} \rangle$

$ord(H) = 3 \Rightarrow H = \{\hat{0}, \hat{x}, \hat{x} + \hat{x} \mid \hat{x} + \hat{x} = \hat{0}\} \quad \{\hat{0}, \hat{4}, \hat{8}\} = \langle \hat{4} \rangle$

$ord(H) = 4 \Rightarrow H = \{\hat{0}, \hat{3}, \hat{6}, \hat{9}\} = \langle \hat{3} \rangle$

$ord(H) = 6 \Rightarrow H = \{\hat{0}, \hat{2}, \hat{4}, \hat{6}, \hat{8}, \hat{10}\} = \langle \hat{2} \rangle$




(T) $|G| = |H| \cdot |G;H|$

$|G/H| = |G;H| = \dfrac{|G|}{|H|}$

$\mathbb{Z}_{12}/\{\hat{0}\} = \mathbb{Z}_{12}$

$\mathbb{Z}_{12}/\mathbb{Z}_{12} = \{\hat{0}\}$

$|\mathbb{Z}_{12}/\langle \hat{2} \rangle| = \dfrac{|\mathbb{Z}_{12}|}{|\langle \hat{2} \rangle|} = 2$

$\Rightarrow \mathbb{Z}_{12}/\langle \hat{2} \rangle = \mathbb{Z}_2$

$\mathbb{Z}_{12}/\langle \hat{3} \rangle = \mathbb{Z}_3$

$\mathbb{Z}_{12}/\langle \hat{4} \rangle = \mathbb{Z}_4$

$\mathbb{Z}_{12}/\langle \hat{6} \rangle = \mathbb{Z}_6$

# GRUPURI DE PERMUTĂRI

Fie $M \neq \emptyset$, $S(M) = \{f : M \to M \mid f \text{ bijectivă}\}$, $(S(M), \circ) \overset{not}{=} S_M$ s.n. grupul de permutări al mulț. $M$

$(f, g) \to f \circ g$, $(f \circ g)(x) = f(g(x))$.

(P) Dacă $f : M \to M'$ o funcție bijectivă, atunci $S_M \simeq S_{M'}$

<u>Dem:</u>

$\theta : S_M \to S_{M'}$, $\theta(\varphi) = f \circ \varphi \circ f^{-1}$

$$\begin{tikzcd} M' \arrow[r, "f^{-1}"] \arrow[rrr, bend right, "f \circ \varphi \circ f^{-1}"'] & M \arrow[r, "\varphi"] & M \arrow[r, "f"] & M' \end{tikzcd}$$

$\theta$ morfism: fie $\varphi, \varphi_1 \in S_M$

$\theta(\varphi \circ \varphi_1) = f \circ (\varphi \circ \varphi_1) \circ f^{-1} = (f \circ \varphi) \circ (f^{-1} \circ f) \circ (\varphi_1 \circ f^{-1}) =$

$f \circ 1_M = f = 1_M \circ f$

$1_M = f \circ f^{-1}$

$= (f \circ \varphi \circ f^{-1}) \circ (f \circ \varphi_1 \circ f^{-1}) = \theta(\varphi) \circ \theta(\varphi_1)$

$\theta(\varphi \circ \varphi_1) = \theta(\varphi) \circ \theta(\varphi_1)$

injectivitatea lui $\theta$: $\theta(\varphi) = \theta(\varphi_1) \Rightarrow f \circ \varphi \circ f^{-1} = f \circ \varphi_1 \circ f^{-1} \Rightarrow \varphi = \varphi_1$

$\theta$ surjectivă: $g \in S_{M'}$, $(\exists)\ h \in S_M$ a.î. $\theta(h) = g$

$\theta(f^{-1} \circ g \circ f) = f \circ (f^{-1} \circ g \circ f) \circ f^{-1} = (f \circ f^{-1}) \circ g \circ (f \circ f^{-1}) = g$

$|M| = n$, $M = \{1, 2, \dots, n\}$ $S_M = S_n$ grupul permutărilor de ordinul $n$

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

$|S_n| = n!$

<u>OBS</u>: $S_n$ este un grup abelian $\Leftrightarrow n \leq 2$ $S_1, S_2 = \{e = \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}, \tau = \begin{pmatrix} 1 \\ 2 \end{pmatrix}$

$S_3 = \{1, \rho, \rho^2, \pi, \rho\pi, \rho^2\pi\}$ $\rho^3 = 1 = \pi^2$, $\rho^2\pi = \pi\rho$

$\sigma \in S_n$ $sg(\sigma) = \prod \frac{\sigma(j) - \sigma(i)}{j - i}$ (

$(i,j) \mid 1 \le i < j \le n$

$\tau(i) > \tau(j)$

Ex) $\tau = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$ $(1,2),(1,3)$

$inv(\tau) = 2$

$sgn(\pi) = (-1)$

$Inv(\tau) =$ nr. inversiunilor

---

$sgn : S_n \to \{-1, 1\}$ $Ker\, sgn = A_n$ (grupul altern) conține toate permutările pare

$S_n / A_n \simeq \{-1, 1\}$, $|A_n| = \frac{n!}{2}$

---

P) $f : M \to M'$ bij $\Rightarrow S_M \simeq S_{M'}$

T (Cayley) Orice grup $G$ cu $n$ elemente se poate scufunda în $S_n$.

$G \hookrightarrow S_n$ $((\exists) H \le S_n ; G \simeq H)$

$\left.\begin{array}{l} S_n \simeq S_G \end{array}\right\} \Rightarrow T : G \to S_G$ un morfism injectiv

$T(g) = t_g$, $t_g(x) = gx$

Scufundarea Cayley

? Cum arată scufundarea Cayley pt grupul lui Klein $K = \{1, a, b, c \mid a^2 = b^2 = c^2 = 1\}, \cdot)$