1. Funcții injective, surjective, bijective, inversabile și monotone.

→ Funcția $f: A \to B$ se numește injectivă dacă $\forall a_1, a_2 \in A$ $a_1 \neq a_2 \Rightarrow f(a_1) \neq f(a_2)$

ddacă $f(a_1) = f(a_2) \Rightarrow a_1 = a_2$ $\forall a_1, a_2 \in A$

→ Funcția $f: A \to B$ se numește surjectivă dacă $\forall b \in B$ $\exists a \in A$ a.î. $f(a) = b$.

→ O funcție injectivă și surjectivă se numește bijectivă.

→ Dacă funcția $f: A \to B$ este inversabilă, atunci prin inversa lui f înțelegem unica funcție $g: B \to A$ cu proprietățile $g \circ f = id_A$ și $f \circ g = id_B$.

---

2. Relații: definiție, proprietăți. • Închiderea reflexivă, tranzitivă și simetrică a unei relații. Relațiile dintre aceste închideri.

→ Numim relație binară pe mulțimea nevidă A orice submulțime a lui $A \times A$.

→ Fie ρ o relație pe mulțimea A.

- spunem că ρ este reflexivă dacă $\forall a \in A$ $a \rho a$.
- spunem că ρ este ireflexivă dacă $\forall a \in A$ $a \not\rho a$.
- spunem că ρ este simetrică dacă $\forall a, b \in A$ $a \rho b \Rightarrow b \rho a$.
- spunem că ρ este antisimetrică dacă $\forall a, b \in A$ $a \rho b \wedge b \rho a \Downarrow a = b$
- spunem că ρ este tranzitivă dacă $\forall a, b, c \in A$ $a \rho b \wedge b \rho c \Downarrow a \rho c$
- spunem că ρ este totală dacă $\rho \cup \rho^{-1} = A \times A$.

→ **ÎNCHIDEREA REFLEXIVĂ**

- notație: $R(\rho)$
- $R(\rho) = \rho \cup \Delta_A$

→ **ÎNCHIDEREA SIMETRICĂ**

- notație: $S(\rho)$; $S(\rho) = \rho \cup \rho^{-1}$

→ **ÎNCHIDEREA TRANZITIVĂ**

- notație: $T(\rho)$; $T(\rho) = \bigcup\limits_{n \in \mathbb{N}^*} \rho^n$

Relațiile dintre închideri

$$\boxed{\begin{array}{l} (i)\ R(S(\rho)) = S(R(\rho)) \\ (ii)\ R(T(\rho)) = T(R(\rho)) \\ (iii)\ S(T(\rho)) \subseteq T(S(\rho)) \end{array}}$$

3. Relații de echivalență. Exemple. Mulțime factor

→ Fie ρ o relație pe mulțimea nevidă A. ρ se numește relație de echivalență dacă este reflexivă, simetrică și tranzitivă.

→ Fie ρ o relație de echivalență pe mulțimea nevidă A și $a \in A$. Prin clasă de echivalență a lui a în raport cu ρ înțelegem mulțimea $\{b \in A : b \rho a\}$

→ Notăm $\frac{A}{\rho}$ și numim mulțimea factor (cât) a lui ~~A~~ A în raport cu ρ mulțimea tuturor claselor de echivalență ale elementelor lui A în raport cu ρ.

→ EXEMPLE IMPORTANTE DE RELAȚII DE ECHIVALENȚĂ

(1) - relația de egalitate pe o mulțime nevidă.

(2) - congruența modulo n

(3) - relația de echivalență asociată unei partiții.

Fie P o partiție a mulțimii nevide A. Definim pe A relația

$a \sim_P b \overset{def}{\Longleftrightarrow} \exists B \in P \; a, b \in B$

→ de echivalență

(4) - relația de echivalență asociată unei funcții

$a_1 \rho_f a_2 \overset{def}{\Longleftrightarrow} f(a_1) = f(a_2)$

4. Relații de ordine. Tipuri importante de mulțimi ordonate.

→ Fie A o mulțime nevidă și ρ o relație pe A. Spunem că ρ este relație de ordine dacă ea este reflexivă, tranzitivă și antisimetrică.

→ Numim mulțime ordonată orice pereche alcătuită dintr-o mulțime nevidă și o relație de ordine pe ea.

→ Exemple de relații de ordine:

1) • relația de egalitate pe o mulțime nevidă

2) • relația de incluziune pe $\mathcal{P}(A)$

3) • relația de divizibilitate pe $\mathbb{N}$. (! NU și pe $\mathbb{Z}$)

4) • relația definită pe $\mathbb{Z}$ prin $x < y$ $\boxed{\text{NU}}$ este rel. de ordine.

→ Spunem că ρ este o relație de ordine strictă dacă ea este ireflexivă și tranzitivă.

→ Spunem că mulțimea $(A, \leq)$ este total ordonată dacă relația $\leq$ este totală.

→ Spunem că $(A, \leq)$ este bine ordonată dacă orice submulțime nevidă a lui A admite prim element.

→ Mulțimea ordonată $(A, \leq)$ se numește
- latice dacă pentru orice $a, b \in A$ există $\inf\{a, b\}$ și $\sup\{a, b\}$.
- latice completă dacă pentru orice submulțime nevidă B a lui A există $\inf B$ și $\sup B$.

→ $A \sim B \Leftrightarrow$ există o funcție bijectivă de la A la B. – relație de echivalență.

---

5. Legi de compoziție : def. + prop. Semigrupuri și monoizi.

→ Fie M o mulțime nevidă. Numim lege de compoziție binară pe mulțimea M orice funcție $\varphi : M \times M \to M$.

→ Fie N o submulțime a lui M. Spunem că N este parte stabilă a lui M în raport cu $*$ dacă $\forall x, y \in N$ $x * y \in N$.

→ asociativitate
→ comutativitate
→ element neutru (la stânga și la dreapta)
→ elemente care admit simetric la stânga sau la dreapta
↓
elemente care sunt simetrice

→ Semigrupuri
→ asociativitate ; morfism ($f(xy) = f(x) f(y)$)

→ Monoizi
→ asociativitate
→ admit element neutru
→ morfism ($f(xy) = f(x) f(y)$
$f(1_M) = 1_{M'}$)

6. Grupuri, subgrupuri, morfisme de grupuri: def. + ex.

→ Fie G o mulțime nevidă și „$\cdot$" o lege de compoziție pe G.
Perechea $(G, \cdot)$ s.n. grup dacă:

(1) „$\cdot$" este asociativă

(2) „$\cdot$" admite element neutru

(3) Toate elementele lui G sunt simetrizabile în raport cu „$\cdot$".

→ Exemple:

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

(2) $(\mathcal{M}_{m,n}(\mathbb{C}), +)$

(3) $(\mathbb{Z}_n, +)$

→ Grupul $\mathbb{Z}_2 \times \mathbb{Z}_2$ s.n. grupul lui Klein.

→ Fie $(M, \cdot)$ un monoid. Notăm cu $U(M)$ mulțimea tuturor elem. simetrizabile ale lui M.
$\Downarrow$
grup

→ Dacă x și y sunt elemente simetrizabile ale unui monoid $(M, \cdot)$, atunci $(xy)^{-1} = y^{-1}x^{-1}$.

→ Spunem că $H \leq G$ (subgrup al lui G) dacă
- $\forall x, y \in H \quad xy \in H$
- $\forall x \in H \quad x' \in H$

→ $H \leq G \Leftrightarrow \forall x, y \in H \quad xy' \in H$

→ Exemple: $(\mathbb{Z}, +) \leq (\mathbb{Q}, +) \leq (\mathbb{R}, +) \leq (\mathbb{C}, +)$

→ Morfism de grupuri ($f: G \to \Gamma$)
- $f(e_G) = e_\Gamma$
- $\forall x \in G \quad f(x') = f(x)'$
- $\forall x \in G \ \forall n \in \mathbb{Z} \quad f(x^n) = f(x)^n$

→ Un morfism de grupuri $f: G \to G$ s.n. endomorfism al lui G.

→ Un izomorfism de grupuri $f: G \to G$ se numește automorfism al lui G.

→ Mulțimea $\{x \in G : f(x) = e_{\Gamma}\}$ se numește nucleul lui f și se notează cu $\ker f$.

- $\ker f = f^{-1}(\{e_{\Gamma}\}) \to \ker f \leq G$

---

7. Subgrupul generat de o mulțime (def. + struct elem. + ex.). Sisteme de generatori pentru un grup.

→ Fie G un grup și $M \subset G$. Prin subgrupul lui G generat de M înțelegem cel mai mic subgrup al lui G care conține submulțimea M.

- Notăm cu $\langle M \rangle$.
- $\langle x_1, x_2, \dots, x_m \rangle$
- $\langle M \rangle = \{x_1^{\alpha_1} \cdot x_2^{\alpha_2} \cdot \ldots \cdot x_m^{\alpha_m} : m \in \mathbb{N}^*, \ x_1, x_2, \dots, x_m \in M, \ \alpha_1, \alpha_2, \dots, \alpha_m \in \mathbb{Z}\}$

→ Fie G un grup. Submulțimea M a lui G s.n. sistem de generatori al lui G dacă $\langle M \rangle = G$.

→ $\mathbb{Z}_m$, S_m, D_n sunt finit generate.

→ $\mathbb{Z}$ este finit generat.

---

8. Grupuri ciclice: definiție + prop. Teorema de structură pt. grupuri ciclice (enunț + demonstrație)

→ Grupul G se numește ciclic dacă el admite un sistem de generatori format dintr-un singur element.

- Exemplu: $\mathbb{Z}$ este ciclic, deoarece $\mathbb{Z} = \langle 1 \rangle$
- $\mathbb{Z} \times \mathbb{Z}$ nu este ciclic
- $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ nu sunt ciclice.

Teorema de structură a grupurilor ciclice

→ Orice grup ciclic cu $n \in \mathbb{N}^*$ elemente este izomorf cu $\mathbb{Z}_n$. Orice grup ciclic infinit este izomorf cu $\mathbb{Z}$.

→ $\boxed{\text{DEMONSTRAȚIE}}$

Fie G un grup ciclic și g un generator al acestuia. Considerăm $u: \mathbb{Z} \to G$, $u(n) = g^n$. Dacă $m, n \in \mathbb{Z}$ avem

$$u(m+n) = g^{m+n} = g^m g^n = u(m) u(n)$$

deci u este morfism de grupuri. În plus, u este în mod evident surjectiv. Aplicând teorema fundamentală a izomorfismului pentru grupuri, obținem $G = \operatorname{Im} u \simeq \frac{\mathbb{Z}}{\ker u}$.

Prin urmare, dacă $\ker u = n\mathbb{Z}$ cu $n \in \mathbb{N}^*$ avem $G \simeq \mathbb{Z}_n$, iar dacă $\ker u = \{0\}$ avem $G \simeq \mathbb{Z}$. $\square$

---

9. Ordinul unui element într-un grup; def. + prop.

→ Observație: dat fiind un element x al unui grup G, subgrupul $\langle x \rangle = \{x^n : n \in \mathbb{Z}\}$ al lui G este ciclic.

→ Prin ordinul elementului x înțelegem ordinul subgrupului generat de x în G.

↳ Vom nota ordinul elem. x din grupul G cu $\operatorname{ord}_G x$. Dacă G este subînțeles din context, atunci vom folosi notația $\operatorname{ord} x$.

→ Formulă:

$$\operatorname{ord}_G x = \begin{cases} \min\{n \in \mathbb{N}^* : x^n = e\}, & \text{dacă } \{n \in \mathbb{N}^* : x^n = e\} \text{ este nevidă} \\ +\infty, & \text{altfel} \end{cases}$$

→ Fie G un grup, $x \in G$ și $n \in \mathbb{N}^*$. Atunci $\operatorname{ord}_G x = n \iff x^n = e$ și $\forall m \in \mathbb{Z}\ x^m = e \Rightarrow n \mid m$.

→ Ordinul oricărui element al unui grup finit divide ordinul respectivului grup.

→ Dacă G, G_1 și G_2 sunt grupuri finite, atunci:

(i) $ord_G(x^k) = \dfrac{ord_G x}{(k, ord_G x)}$

(ii) $ord_{G_1 \times G_2}(x_1, x_2) = [ord_{G_1} x_1, ord_{G_2} x_2]$

(iii) $ord_G(xy) = ord_G(yx)$

(iv) Dacă $xy = yx$ și $(ord_G x, ord_G y) = 1$, atunci:

$$ord_G(xy) = ord_G x \cdot ord_G y$$

$$ord_G(xy) = [ord_G x, ord_G y]$$

10.+14. Subgrupuri normale: Def. + caracterizări (+ dem!), exemple
Indicele unui subgrup, inclusiv demonstrația egalității
$|(G/H)_s| = |(G/H)_d|$ pt. orice grup G și subgrup H.

→ Fie G un grup și $H \leq G$. Considerăm următoarele relații pe G:

a) $x \equiv_s y \pmod H \iff x^{-1}y \in H$

b) $x \equiv_d y \pmod H \iff xy^{-1} \in H$

$\equiv_s$ s.n. relația de echivalență la stânga modulo subgrupul H

$\equiv_d$ s.n. — " — " — " — " dreapta — " — " — " — "

→ NOTAȚIA folosită pentru mulțimea factor a lui G în raport cu
- $\equiv_s$ este $(G/H)_s$
- $\equiv_d$ este $(G/H)_d$

⇒ Fie G un grup, $H \leq G$ și $x \in G$. Atunci:

a) Clasa de echivalență a lui x în raport cu $\equiv_s \pmod H$ este xH.

b) — " — " — " — " — " — " — " $\equiv_d \pmod H$ este Hx.

Demonstrație: a) $y \in \hat{x} \Leftrightarrow x^{-1}y \in H \Leftrightarrow y \in xH$

b) $y \in \hat{x} \Leftrightarrow xy^{-1} \in H \Leftrightarrow y \in Hx$

$\to (G/H)_s = \{xH : x \in G\}$

$\to (G/H)_d = \{Hx : x \in G\}$

→ * Fie G un grup și $H \leq G$. Atunci $|(G/H)_s| = |(G/H)_d|$.

→ DEMONSTRAȚIE

Definim $f : (G/H)_s \to (G/H)_d$, $f(xH) = Hx^{-1}$

$$g : (G/H)_d \to (G/H)_s, \quad g(Hx) = x^{-1}H.$$

Dacă $xH = yH$, atunci $x^{-1}y \in H$, deci $x^{-1}(y^{-1})^{-1} \in H$, de unde $Hx^{-1} = Hy^{-1}$. Prin urmare, f este corect definită. Faptul că g este corect definită se probează analog.

Este imediat că f și g sunt inverse una celeilalte, deci ele sunt bijective, de unde concluzia. □

→ Cardinalul comun al mulțimilor $|(G/H)_s|$ și $|(G/H)_d|$ s.n. indicele lui H în G.

↳ Vom nota indicele lui H în G cu $[G : H]$

→ Prin ordinul grupului G înțelegem cardinalul lui G. Notația uzuală este $|G|$.

→ Fie G un grup, $H \leq G$ și $x \in G$. Atunci $|xH| = |H|$.

→ DEMONSTRAȚIE:

Definim $f : xH \to H$, $f(t) = x^{-1}t$ și $g : H \to xH$, $g(t) = xt$.

Este imediat că f și g sunt corect definite și inverse una celeilalte, deci ele sunt bijective, de unde concluzia. □

→ Exemplu concret:

$G = \mathbb{Z}_{12} = \{\hat{0}, \hat{1}, \hat{2}, \hat{3}, \hat{4}, \hat{5}, \hat{6}, \hat{7}, \hat{8}, \hat{9}, \hat{10}, \hat{11}\} \Rightarrow |G| = 12$

$H = \{\hat{0}, \hat{2}, \hat{4}, \hat{6}, \hat{8}, \hat{10}\}$ subgrup al lui G. $\Rightarrow |H| = 6$

$\hat{0}H = \{\hat{0}, \hat{2}, \hat{4}, \hat{6}, \hat{8}, \hat{10}\} = H\hat{0}$

$\hat{1}H = \{\hat{1}, \hat{3}, \hat{5}, \hat{7}, \hat{9}, \hat{11}\} = H\hat{1}$

$\hat{2}H = \{\hat{2}, \hat{4}, \hat{6}, \hat{8}, \hat{10}, \hat{0}\} = \hat{0}H = H\hat{2}$

Avem deci două clase de echivalență pentru $\equiv_s (\text{mod } H)$ și $\equiv_d (\text{mod } H)$:

$\{\hat{0}, \hat{2}, \hat{4}, \hat{6}, \hat{8}, \hat{10}\}$ și $\{\hat{1}, \hat{3}, \hat{5}, \hat{7}, \hat{9}, \hat{11}\}$

Deci $(G/H)_s = \{\{\hat{0}, \hat{2}, \hat{4}, \hat{6}, \hat{8}, \hat{10}\}, \{\hat{1}, \hat{3}, \hat{5}, \hat{7}, \hat{9}, \hat{11}\}\} = (G/H)_d$

$\Rightarrow |(G/H)_s| = |(G/D)_d| = 2$

→ SUBGRUPURI NORMALE

→ * Fie G un grup și $H \leq G$. Spunem că H este subgrup normal al lui G dacă îndeplinește una din condițiile echivalente de mai jos:

(i) $(G/H)_s = (G/H)_d$

(ii) $\forall x \in G \quad xH = Hx$

(iii) $\forall x \in G \quad xHx^{-1} = H$

(iv) $\forall x \in G \quad xHx^{-1} \subseteq H$

H subgrup normal al lui G NOTĂM $H \trianglelefteq G$

→ DEMONSTRAȚIE:

(iv) $\Rightarrow$ (iii)

$xHx^{-1} \subseteq H$ (1)

$H = 1_G \cdot H \cdot 1_G = x \cdot \underbrace{x^{-1} \cdot H \cdot x}_{\subseteq H} \cdot x^{-1} \subseteq xHx^{-1}$ (2)

căci $H \trianglelefteq G \Rightarrow xHx^{-1} \subseteq H, \forall x \in G \Rightarrow x^{-1}Hx \subseteq H$

Din (1) și (2) $\Rightarrow xHx^{-1} = H, \forall x \in G$ $\square$

$(iii) \Rightarrow (ii)$

$$xH = xH1_G = \underbrace{xHx^{-1}}_{H}x = Hx, \ \forall x \in G \ \square$$

$(ii) \Rightarrow (i)$ Evident

$(i) \Rightarrow (iv)$

Fie $x \in G$.

$xH \in (G/H)_s \overset{\text{ipoteză}}{=} (G/H)_d \Rightarrow xH \in (G/H)_d \Rightarrow \exists y \in G$ a.î. $xH = Hy$

$$\left.\begin{array}{l} x \in xH \\ xH = Hy \end{array}\right| \Rightarrow x \in Hy \Rightarrow x \in \hat{y}^d \Rightarrow x \equiv_d y \ (\mathrm{mod}\ H) \Rightarrow \hat{x}^d = \hat{y}^d \Rightarrow \underline{Hx = Hy}$$

obțin: $xH = Hy = Hx \iff xH = Hx \Rightarrow xHx^{-1} = Hxx^{-1} = H \Rightarrow xHx^{-1} \subseteq H$

$\Rightarrow H \trianglelefteq G.$ $\square$

→ Exemple de subgrupuri normale:

(1) – pt. orice familie $(H_i)_{i \in I}$ de subgrupuri normale ale lui G avem $\bigcap_{i \in I} H_i \trianglelefteq G$.

(2) – orice subgrup al unui grup abelian este normal.

(3) – orice subgrup ~~normal~~ de indice doi al unui grup este normal.

(4) – dacă $f: G \to G'$ morfism de grupuri, atunci $\ker f \trianglelefteq G$.

11. Teorema lui Lagrange (enunț + dem!)

→ *Fie G un grup și $H \leq G$. Atunci $|G| = |H| \cdot |G:H|$

→ $\boxed{\text{DEMONSTRAȚIE}}$

Avem $G = \bigsqcup_{xH \in (G/H)_s} xH$, deci $|G| = \sum_{xH \in (G/H)_s} |xH|$.

Dar $|xH| = |H|$, deci obținem $|G| = |H| \cdot |(G/H)_s|$.

→ COROLAR: ordinul oricărui subgrup finit divide ordinul respectivului grup.

---

12. Teoremele lui Euler și Fermat (+ dem!). Indicatorul lui Euler (def. + formulă de calcul).

→ Funcția $\varphi : \mathbb{N}^* \to \mathbb{N}^*$, $\varphi(n)$ = numărul numerelor naturale care nu-l întrec pe n și sunt prime cu n, se numește indicatorul lui Euler.

→ OBSERVAȚIE: $|U(\mathbb{Z}_n)| = \varphi(n)$

→ Dacă $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$, unde $p_1, p_2, \dots, p_r$ sunt nr. prime distincte două câte două, atunci:

$$\varphi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_r}\right)$$

→ TEOREMA LUI EULER

→ *Pentru orice $n \in \mathbb{N}^*$ și orice $a \in \mathbb{Z}$ prim cu n avem $a^{\varphi(n)} \equiv 1 \pmod{n}$

→ $\boxed{\text{DEMONSTRAȚIE}}$

a fiind prim cu n, $\hat{a}$ este element al grupului $U(\mathbb{Z}_n)$.

Dar $x^{\operatorname{ord} x} = e$

→ $\hat{a}^{\varphi(n)} = \hat{1}$ în acest grup, de unde concluzia. □

→ TEOREMA LUI FERMAT

→ Pentru orice număr prim $p \in \mathbb{N}$ și orice $a \in \mathbb{Z}$ prim cu p avem $a^{p-1} \equiv 1 \pmod p$

→ DEMONSTRAȚIE

Întrucât pentru orice număr prim p avem $\varphi(p) = p-1$, obținem concluzia aplicând teorema lui Euler. □

---

13. $\mathbb{Z}_{mn} \simeq \mathbb{Z}_m \times \mathbb{Z}_n$ dacă și numai dacă $(m,n)=1$.

→ DEMONSTRAȚIE

„$\Rightarrow$": Corespondentul $(\hat{a}, \bar{b})$ al lui $\tilde{1}$ prin izomorfism are ordinul $[\text{ord}_{\mathbb{Z}_m} \hat{a}, \text{ord}_{\mathbb{Z}_n} \bar{b}]$, dar și mn. Deci, $mn = [\text{ord}_{\mathbb{Z}_m} \hat{a}, \text{ord}_{\mathbb{Z}_n} \bar{b}] \mid [m,n]$.

Cum $mn = [m,n] \cdot (m,n)$, obținem $(m,n)=1$.

„$\Leftarrow$" Este imediat că funcția $f: \mathbb{Z}_{mn} \to \mathbb{Z}_m \times \mathbb{Z}_n$, $f(\tilde{a}) = (\hat{a}, \bar{a})$ este corect definită și morfism injectiv de grupuri. Cum atât domeniul cât și codomeniul său au mn elemente, ea este și surjectivă. Prin urmare, f este izomorfism de grupuri. □

---

15. Construcția grupului factor (+ dem.!)

→ Fie G un grup și $H \trianglelefteq G$. Atunci pe mulțimea $(G/H)_s$ este corect definită legea de compoziție $(xH) \cdot (yH) = (xy)H$.

DEMONSTRAȚIE

Vreau să arăt că $\hat{x} = \hat{x'}$ și $\hat{y} = \hat{y'} \to \widehat{xy} = \widehat{x'y'}$.

Vom lucra la stânga (similar se procedează la dreapta).

Din ipoteză: $\hat{x} = \hat{x'} \Leftrightarrow x \equiv_s x' \pmod H \Leftrightarrow x^{-1}x' \in H$.

$\hat{y} = \hat{y'} \Leftrightarrow y \equiv_s y' \pmod H \Leftrightarrow y^{-1}y' \in H$.

$$y^{-1}\underbrace{x^{-1}x'}_{\in H}y' \in y^{-1}Hy' = y^{-1}Hyy^{-1}y' = (y^{-1}Hy)y^{-1}y' \overset{H \trianglelefteq G}{=} H\underbrace{y^{-1}y'}_{\in H} \subseteq H$$

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

$\Rightarrow \widehat{xy} = \widehat{x'y'}$ □

→ Prin grupul factor al lui G în raport cu H înțelegem grupul care are mulțimea subiacentă $(G/H)_s$ și legea de compoziție $(xH)\cdot(yH) = (xy)H$.

↳ NOTAȚIA uzuală pentru grupul factor al lui G în raport cu H este $\frac{G}{H}$. Pentru elementul $xH \in \frac{G}{H}$ vom prefera uneori notația $\hat{x}$. În notație aditivă vom scrie $x+H$ în loc de xH.

↳ EXEMPLU: $\frac{\mathbb{Z}}{n\mathbb{Z}} = \mathbb{Z}_n$

---

16. TEOREMA FUNDAMENTALĂ DE IZOMORFISM PENTRU GRUPURI (enunț + dem.!)

→* Fie $f: G \to \Gamma$ un morfism de grupuri. Atunci

$$\frac{G}{\ker f} \simeq \operatorname{Im} f$$

în mod canonic via $\bar{f}(\hat{x}) = f(x)$.

→ DEMONSTRAȚIE:

Definim $\bar{f}: \frac{G}{\ker f} \to \operatorname{Im} f$, $\bar{f}(\hat{x}) = f(x)$.

- Dacă $\hat{x} = \hat{y}$, atunci $x^{-1}y \in \ker f$, deci $f(x^{-1}y) = e_\Gamma$. f fiind morfism de grupuri, obținem de aici $f(x)^{-1}f(y) = e_\Gamma$, deci $f(x) = f(y)$. Prin urmare, valorile lui $\bar{f}$ sunt independente de alegerea reprezentanților argumentelor. Cum valorile lui $\bar{f}$ sunt valori ale lui f, ele se află în $\operatorname{Im} f$. Prin urmare, $\bar{f}$ este corect definită.
- Dacă $x, y \in G$ atunci $\bar{f}(\hat{x}\hat{y}) = \bar{f}(\widehat{xy}) = f(xy) = f(x)f(y) = \bar{f}(\hat{x}) = \bar{f}(\hat{y})$. Așadar, $\bar{f}$ este morfism de grupuri.
- Este evident că $\bar{f}$ surjectivă.
- Dacă $\bar{f}(\hat{x}) = e_\Gamma$, atunci $f(x) = e_\Gamma$, deci $x \in \ker f$, de unde $\hat{x} = \hat{e}$. În consecință, $\bar{f}$ este injectivă.

Din toate faptele arătate mai sus rezultă că $\bar{f}$ este morfism bijectiv de grupuri. Prin urmare, f este izomorfism. □

---

18. Grupuri de permutări

→ Orice permutare din S_n se poate scrie ca produs de cicluri disjuncte.

→ Orice permutare din S_n se poate scrie ca produs de transpoziții.

→ *Orice transpoziție este permutare impară.

→ DEMONSTRAȚIE

Inversiunile transpoziției (i,j) unde $1 \le i < j \le n$, sunt:

(i,k), $k \in \{i+1, i+2, \dots, j\}$ și

(l,j), $l \in \{i+1, i+2, \dots, j-1\}$;

Numărul acestora este $(j-i)+(j-1-i) = 2(j-i)+1$, care este impar.

→ Demonstrații pentru: a) $S_n = \langle (1,2), (1,3), \dots, (1,n) \rangle$

b) $S_n = \langle (1,2), (2,3), \dots, (n-1, n) \rangle$

a) Observăm că $(i,j) = (1,i)(1,j)(1,i)$, $\forall\, 1 \le i < j \le n$.

Este imediată corectitudinea egalității de mai sus.

Din faptul că orice permutare din S_n se poate scrie ca produs de transpoziții, iar orice ~~permut~~ transpoziție se poate scrie ca produs de ~~permutări~~ transpoziții de forma $(1,i)$ obținem concluzia. □

De demonstrat în examen !! La b) cu inducție

b) Observăm că $(i,j) = (i,i+1)(i+1,i+2)\cdots(j-2,j-1)(j-1,j)(j-2,j-1)\cdots(i,i+1)$

$\forall\, 1 \le i < j \le n$

Este imediată corectitudinea egalității de mai sus.

Din faptul că orice permutare din S_n se poate scrie ca produs de transpoziții, iar orice transpoziție se poate scrie ca produs de transpoziții de forma $(i,i+1)$, cu $1 \le i < n$, obținem concluzia. □