Seminar 1

① $A = \{x \mid x = \frac{a+1}{2a+1} ; a \in \mathbb{R} \setminus \{-\frac{1}{2}\}\} = \mathbb{R} \setminus \{\frac{1}{2}\} = B$

Pp că ($\exists$) $a \in \mathbb{R}$ a.î.

„$\subseteq$" $\frac{a+1}{2a+1} = \frac{1}{2} \Leftrightarrow 2a+2 = 2a+1 \Rightarrow 0 = 1$ fals $\Rightarrow$

$\Rightarrow$ pp falsă $\Rightarrow A \subseteq B$ (i)

„$\supseteq$" Fie $b \in \mathbb{R} \setminus \{\frac{1}{2}\}$

$b = \frac{a+1}{2a+1} \Leftrightarrow a+1 = 2ab + b \Leftrightarrow 1-b = a(2b-1)$

$\Rightarrow a = \frac{1-b}{2b-1} \in \mathbb{R} \Rightarrow B \subseteq A$ (ii)

$b \neq \frac{1}{2}$

(i) (ii) $\Rightarrow A = B$

② $(3\mathbb{N}+2) \cap (5\mathbb{N}+1) = 15\mathbb{N}+11$ (Se poate face cu LMC)

$\supseteq$ Fie $a \in 15\mathbb{N}+11 \Rightarrow a = 5(3n+2)+1 \Rightarrow a \in B$

$a = 3(5n+3)+2 \Rightarrow a \in A$ $\Big| \Rightarrow$

$\Rightarrow a \in A \cap B$ (i)

$\subseteq$ Fie $a \in A \cap B \Rightarrow a = 3n+2 = 5m+1$ $n, m \in \mathbb{N}$

$3n+2 = 5m+1 \Leftrightarrow 3n = 5m-1 \Rightarrow 3 \mid 5m-1$

$m \in 3\mathbb{N}$ sau $m \in 3\mathbb{N}+1$ sau $m \in 3\mathbb{N}+2 \Rightarrow$

$m = 3k$ ✗ $m = 3k+1$ ✗ $m = 3k+2$ ✓ $(15k+9)$

$\Rightarrow m = 3k+2$ $k \in \mathbb{N}$

$5(3k+2)+1 = 15k+10-1 = 3(5k+3)$

$3n = 3(5k+3) \Rightarrow n = 5k+3$

$a = 3n+2 \Rightarrow a = 3(5k+3)+2 = 15k+11 \Rightarrow a \in C \Rightarrow$

$\Rightarrow A \cap B \subseteq$

(i) (ii) $\Big| \Rightarrow A \cap B = C$ (ii)

③ $A \cup B = \{1,2,3,4,5\}$

$A \setminus B = \{1,3\}$

$A \cap B \not\subseteq \{3,4,5\}$

$4 \notin A \setminus B$ $\Big| \Rightarrow 4 \in B$

$4 \in A \cup B$ $\quad 4 \notin A$

* Analog pentru 5

OBS $\phi \in C(A) C$ multi

$2 \in A$ ai $2 \in B$

$A = \{1,2,3\}$

$B = \{3,4,5\}$

④ $|A| = ?$ $A = \{x \in \mathbb{Q} \mid x = \frac{n^2+1}{2n^2+n+1} \mid n \in \{1, \dots, 1000\}\}$

$x \in \mathbb{Q} \Rightarrow (\exists) p, q \in \mathbb{Z}$ $q \neq 0$ a.i. $x = \frac{p}{q}$

$2n^2 + n + 1 \neq 0 \ (\forall) \ n \in \{1, \dots, 1000\}$

$|A| = 999$ (seminar 2)

Seminar 2

$A = \{1, 2, \dots, n\}$ $|A| = n$ $\Rightarrow P(A) \left(\overset{not}{=} 2^{[n]}\right)$

$|P(A)| = C_n^0 + C_n^1 + \dots + C_n^n = 2^n$

Pentru funcție: Dacă $y_1 = f(x_1)$ și $y_2 = f(x_1) \Rightarrow$
$\Rightarrow$ nu e funcție

$Im(f) = \{f(a) \mid a \in A\} \subseteq B$

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

---

① $A = \{1, 2, \dots, n\}$

a) multipli de 7 în A (în general)

$B_k = \{x \in A \mid k \mid x\}$ $|B_7| = \left[\frac{n}{7}\right]$ $B_n = \left[\frac{n}{k}\right]$

b) el din A div cu 2 și/sau 3

$= B_2 \cap B_3$

$B = \{x \in A \mid 2 \mid x \text{ și } 3 \mid x\} = \{x \in A \mid 6 \mid x\} = B_6$

sau $C = \{x \in A \mid 2 \mid x \text{ sau } 3 \mid x\} = B_2 \cup B_3$

$|C| = |B_2 \cup B_3| = |B_2| + |B_3| - |B_2 \cap B_3| =$

$= \left[\frac{n}{2}\right] + \left[\frac{n}{3}\right] - \left[\frac{n}{6}\right]$

c) el. lui A care nu sunt divizibile cu 2 și cu 3

$E = \{x \in A \mid 2 \nmid x \text{ și } 3 \nmid x\} = (A \setminus B_2) \cap (A \setminus B_3)$

$= C_A B_2 \cap C_A B_3 = C_A (B_2 \cup B_3) =$

$= n - \left[\frac{n}{2}\right] - \left[\frac{n}{3}\right] + \left[\frac{n}{6}\right]$

PIE

Fie $A_1, \dots, A_n$ mulțimi finite $n \geq 2$

$$\left|\bigcup_{i=1}^{n} A_i\right| = \sum_{i=1}^{n} |A_i| - \sum_{1 \leq i_1 < i_2 \leq n} |A_{i_1} \cap A_{i_2}| +$$

$$+ \sum_{1 \leq i_1 < i_2 < i_3 \leq n} |A_{i_1} \cap A_{i_2} \cap A_{i_3}| - \dots + (-1)^{k+1} \sum_{1 \leq i_1 < \dots < i_k \leq n} |A_{i_1} \cap \dots \cap A_{i_k}|$$

$$+ \dots + (-1)^{n+1} |A_1 \cap \dots \cap A_n|$$

Dem. **n = 3**

$|A_1 \cup A_2 \cup A_3| = |A_1| + |A_2| + |A_3| - |A_1 \cap A_2| - |A_1 \cap A_3|$

$- |A_2 \cap A_3| + |A_1 \cap A_2 \cap A_3|$

Seminar 3

$A = \{1, \dots, n\}$ $S_n = \{f \mid f: \{1,2,\dots,n\} \to \{1,2,\dots,n\}$ f bij$\}$

f o.m. perm. a mult. $\{1,2,\dots,n\}$

$|S_n| = n!$

$(S_n, \circ)$ g. neab. $(n \geq 3)$

Thm. Cayley $(\exists)$ mor. inj de la $(G, *)$ la $(S_n, \circ)$

Dacă f bij $\Rightarrow (\exists!)\ g: B \to A$ o.m. inversa not f^{-1}

Preimaginea există mereu

Def echipotente = aceeași cardinal dacă $(\exists)\ f: A \to B$ bij.

$\emptyset$ mult. echi. cu $\mathbb{N}$ o.n. numărabilă

Def $|A| \leq |B| \iff (\exists)\ f: A \to B$ inj

Seminar 4

Rel de echi: refl. $a \sim a$

sim. $a \sim b \Rightarrow b \sim a$

tranz. $\left.\begin{matrix} a \sim b \\ b \sim c \end{matrix}\right| \Rightarrow a \sim c$

OBS $|A| = n \Rightarrow 2^{n^2}$ rel binare

Seminar 5

$a \equiv b \pmod n \overset{def}{\iff} n \mid a-b$

Caz particular ① $n=0$ $a \equiv b \pmod 0 \iff$

$\iff 0 \mid a-b \iff a=b$

② $n=1$ $a \equiv b \pmod 1 \iff 1 \mid a-b \quad \forall a,b \in \mathbb{Z}$

③ $n \geq 2$ $a \equiv b \pmod n \iff n \mid a-b \iff$

$\iff a, b$ dau acelasi rest la impartirea cu n

Def $\hat{a} = \{b \in A \mid a \sim b\}$ (cls de echi)

Multimea cls. de echi. = multimea factor a lui A mod $\sim$

$A/\sim = \{\hat{a} \mid a \in A\}$

Seminar 6

Thm nr partitii = nr. rel. echi.

Def $S \subseteq A$ s.n. SCR pentru "$\sim$" daca S contine exact cate un element din fiecare cls de echi.

① $\forall a \in A \ (\exists) \ s \in S$ a.i. $a \sim s$ $(\iff [a] = [s])$

② $\forall s_1 \neq s_2, s_1, s_2 \in S$ atunci $s_1 \not\sim s_2 \iff$

$[s_1] \cap [s_2] = \emptyset$

Monoid = ax + el. n.

① $\hat{4} \pmod 5$ $\in \mathbb{Z}$ $\quad a \equiv b \pmod 5 \Leftrightarrow 5 \mid a-b$

$\hat{a} = \{b \in \mathbb{Z} \mid a \equiv b \pmod 5\}$

$\hat{0} = \{5k \mid k \in \mathbb{Z}\}$

$\hat{1} = \{5k+1 \mid k \in \mathbb{Z}\}$

$\vdots$

$\hat{4} = \{5k+4 \mid k \in \mathbb{Z}\}$

$\mathbb{Z}/_{\equiv \pmod 5} = \{\hat{0}, \hat{1}, \hat{2}, \hat{3}, \hat{4}\}$

multimea factor de SCR: $\{0,1,2,3,4\}$

~~① $A = \{4, 7, 5\}$~~

~~2 multi factori ai lui A~~

① $x \sim y \Leftrightarrow x^2 - 3x = y^2 - 3y$

Dem că $\sim$ rel de echi, $\mathbb{R}/_\sim$ + SCR

refl. $x \sim x \Leftrightarrow x^2 - 3x = x^2 - 3x$ ✓

sim. $x \sim y \Leftrightarrow y \sim x$ evident.

tranz. $\left.\begin{matrix} x \sim y \\ y \sim t \end{matrix}\right| \Rightarrow x \sim t \Rightarrow x^2 - 3x = y^2 - 3y$

$y^2 - 3y = t^2 - 3t \Rightarrow$

$\Rightarrow x^2 - 3x = t^2 - 3t$ ✓

$\Rightarrow x \sim t$ rel. de echi.

$\hat{x} = \{y \in \mathbb{R} \mid x \sim y\} = \{y \in \mathbb{R} \mid x^2 - 3x = y^2 - 3y\}$

$x^2 - 3x = y^2 - 3y$

$x^2 - y^2 = 3x - 3y$

$(x-y)(x+y) = 3(x-y)$

$(x-y)(x+y-3) = 0$ $\begin{cases} x = y \\ x = 3 - y \end{cases}$

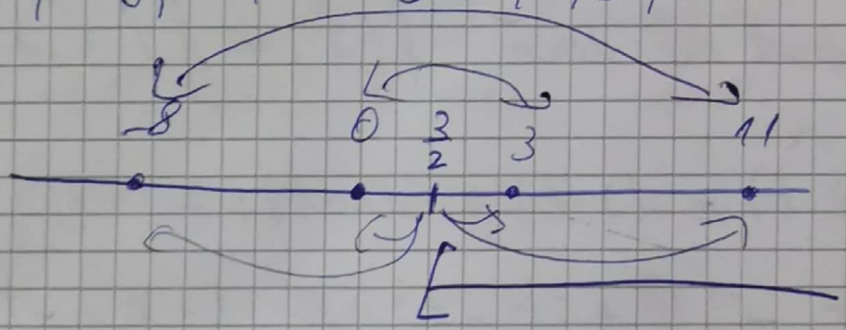
$\hat{x} = \{x, 3-x\} \in \mathcal{P}(\mathbb{R}) \setminus \{\frac{3}{2}\}$

$x = 3 - y$

$\times = \frac{3}{2}$

$\mathbb{R}/\sim = \{\hat{x} \mid x \in \mathbb{R}\} = \{\hat{x^2} \mid x \in S\}$

$-\hat{8} = \{-8, 11\}$ $\hat{0} = \{0, 3\}$



Un SCR poate fi $[\frac{3}{2}, \infty)$

Pb. dem. a.

a) $(\forall)\ a \in A(\mathbb{R})$ $b \in S$ a.i. $a \sim_\rho b$ $(\Leftrightarrow [a] = [b])$

b) $(\forall)\ b_1 \neq b_2$, $b_1, b_2 \in S$ atunci $b_1 \not\sim_\rho b_2$ $(\Leftrightarrow$

$\Leftrightarrow (\hat{b_1}] \cap [b_2] = \emptyset)$

a) $a \in \mathbb{R}$ Dacă $a \geq \frac{3}{2}$ luăm $b = a$ și $b \sim a$

$a < \frac{3}{2}$ ~~Atunci~~ $3 - a > 3 - \frac{3}{2} = \frac{3}{2}$. Luăm

$b = 3 - a$ și $a \sim_\rho b$

Se dem și b) $\Rightarrow S = [\frac{3}{2}, \infty) \subset \mathbb{R}$

Să bine def funcția $f: \mathbb{R}/_{\mathcal{N}} \to \mathbb{R}$

(i) $f(\hat{t}) = -t^2 + 3t + 7$

sau $g: \mathbb{R}/_{\mathcal{N}} \to \mathbb{R}$

(ii) $g(\hat{t}) = t^2 + t + 1$

(i) Dacă $t = \frac{3}{2}$. $\hat{\frac{3}{2}} = \{\frac{3}{2}\}$ f e bun def în $\frac{3}{2}$

Dacă $t \neq \frac{3}{2} \Rightarrow \hat{t} = \{t, 3-t\} \Rightarrow \hat{t} = \widehat{3-t}$

f coerct def dacă $f(\hat{t}) = f(\widehat{3-t})$ $(t) \hat{t} \in \mathbb{R}$

$f(\widehat{3-t}) = -(3-t)^2 + 3(3-t) + 7$

$= -9 + 6t - t^2 + 9 - 3t + 7 = -t^2 + 3t + 7$

$= f(\hat{t})$

$\Rightarrow f$ e coerct def.

(ii) $g: \mathbb{R}/_{\mathcal{N}} \to \mathbb{R}$

$g(\hat{t}) = t^2 + t + 1$

$g(\widehat{3-t}) = (3-t)^2 + 3 - t + 1$

$= 9 - 6t + t^2 + 3 - t + 1 = t^2 - 7t + 13 \neq$

$f(\hat{t})$

$\Rightarrow g$ nu e bine def.

Seminar 7

$\mathbb{Z}_n \overset{not}{=} \mathbb{Z}/_{\equiv \bmod(n)}$

$(\mathbb{Z}_n, +) \rightsquigarrow$ g a.

$(\mathbb{Z}_n, \cdot) \rightarrow$ m. c.

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

Def: $(M_1, \cdot)$ $(M_2, \cdot)$ 2 monoizi

$f: M_1 \to M_2$ morf de mon. dacă

① $f(x \cdot y) = f(x) \cdot f(y)$

② $f(1_{M_1}) = 1_{M_2}$

morfism. bij $\Rightarrow$ ~~izomorfism~~.

Prop. morf. mon.

- compunerea a 2 mon este tot mon.
- inv. unui izo. de mon. este tot ~~mon~~ izo.
- $f: M_1 \to M_2$ morf de mon.

  $a \in M_1 \Rightarrow$ • $f(a^n) = (f(a))^n$ $\forall n \geq 1$

  • dacă $a \in U(M_1) \Rightarrow f(a) \in U(M_2)$

  și $f(a^{-1}) = f(a)^{-1}$

Def $(G_1, *)$ și $(G_2, \cdot)$

$f: G_1 \to G_2$ morf de gr dacă $f(x*y) = f(x) \cdot f(y)$

morf bij $\Rightarrow$ izo.

- $f(1_{G_1}) = 1_{G_2}$ dacă $f: G_1 \to G_2$ morf.

Ex $f: (\mathbb{Z}_2, +) \to (\mathbb{Z}_4, +)$ $\quad f(\hat{0}) = \bar{0}$, $f(\hat{1}) = \bar{2}$

$f(\widehat{x+y}) = f(\hat{x}) + f(\hat{y})$

(i) $f(\widehat{0+0}) = f(\hat{0}) = \bar{0}$ $\quad (\bar{0}+\bar{0}=\bar{0})$ ✓

(ii) $f(\widehat{0+1}) = f(\hat{1}) = \bar{2}$ $\quad (\bar{0}+\bar{2}=\bar{2})$ ✓

(iii) $f(\widehat{1+1}) = f(\hat{0}) = \bar{0}$ $\quad (\bar{2}+\bar{2}=\bar{0})$ ✓

$\Rightarrow$ morf de gr.

① $\mathbb{C}$, "$\sim$" $\quad x \sim y \overset{def}{\iff} |z| = |y|$

„$\sim$" rel de echi, SCR

(i) <u>refl.</u> $\quad x \sim x \iff |x| = |x|$ ✓

(ii) <u>sim.</u> $\quad x \sim y \Rightarrow y \sim x \iff |x| = |y| \Rightarrow |y| = |x|$ ✓

(iii) <u>trans.</u> $\quad \left.\begin{matrix} x \sim y \\ y \sim z \end{matrix}\right| \Rightarrow x \sim z \quad |x| = |y| = |z| \Rightarrow |x| = |z|$ ✓

$\Rightarrow$ rel de echi.

$\hat{z} = \{x \in \mathbb{C} \mid x \sim z\} = \{x \in \mathbb{C} \mid |x| = |z|\}$

Dacă $z=0 \Rightarrow |z|=0 \quad \hat{0}=\{0\}$

Altfel $|z|=r \neq 0 \quad r \in \mathbb{R}_+^*$ $\quad \hat{z}=\{x \in \mathbb{C} \mid |x|=r\}$

$=\{r(\cos t + i \sin t) \mid t \in [0, 2\pi)\}$

$SCR \neq S = \mathbb{R}_+$

Lem SCR

1) $(\forall) z \in \mathbb{C}^* (\exists) \sigma \in S$ a.î. $z \sim \sigma$

2) $(\forall) \sigma_1, \sigma_2 \in S \quad \sigma_1 \neq \sigma_2 \Rightarrow \sigma_1 \not\sim \sigma_2$

1) $z \sim |z| \quad |z| \in S \quad (\sigma = |z|)$

2) $\sigma_1, \sigma_2 \in S \Rightarrow \sigma_1 \neq \sigma_2 \Rightarrow |\sigma_1| \neq |\sigma_2| \Rightarrow \sigma_1 \not\sim \sigma_2$

$\Rightarrow S \in SCR$

OBS A/ρ în bij cu $B \Leftrightarrow B \in SCR$ pt ρ

Seminar 8

2) morf de gr de la $(\mathbb{Z}_5, \cdot)$ la $(\mathbb{Z}_7, \cdot)$

OBS Între oricare 2 gr. există un morf de gr. (morfism Trivial) $f: (G_1, \cdot) \to (G_2, \cdot) \quad f(g) = 1_{G_2}$

Fie $f: (\mathbb{Z}_5, \cdot) \to (\mathbb{Z}_7, \cdot)$ un morf de gr

$f(\hat{a}+\hat{b}) = f(\hat{a}) + f(\hat{b}) \quad (\forall) \hat{a}, \hat{b} \in \mathbb{Z}_5$

$f(\hat{1}+\hat{1}) = 2f(\hat{1})$

$f(\hat{2}) = 2f(\hat{1})$

$f(\hat{3}) = 2f(\hat{1}) + f(\hat{1}) = 3f(\hat{1})$

$f(\hat{4}) = 4f(\hat{1})$

$f(\hat{5}) = 5f(\hat{1}) \Rightarrow 5f(\hat{1}) = \bar{0} \Rightarrow 5 \cdot \bar{4} = \bar{0}$

$7 \nmid 5 \cdot 4$, $(7,5)=1 \Rightarrow \bar{4} = \bar{0}$

$\Rightarrow f(\hat{1}) = \bar{0} \Rightarrow f(\hat{a}) = \bar{0} \ \forall \hat{a} \in \mathbb{Z}_5$

$\Rightarrow$ un singur morf (trivial)

OBS Nr de morf de la $(\mathbb{Z}_m, +)$ la $(\mathbb{Z}_n, +)$ este $d = (m, n)$. Grupul morf de la $(\mathbb{Z}_m, +)$ la $(\mathbb{Z}_n, +) \simeq (\mathbb{Z}_d, +)$

Def $(G, \cdot)$ grup. H submulțime nevidă a lui G s.n. subgrup al lui G ($H \leq G$) dacă H este p.s. a lui G închisă la luarea inversului. ($\forall x, y \in H$ avem $xy \in H$ și $x^{-1} \in H$)

SAU

Def $(G, \cdot)$. $H \leq G \Leftrightarrow \forall x, y \in H$ avem $xy^{-1} \in H$

(pentru $(G, +) \Leftrightarrow x - y \in H$

$H_1, H_2 \leq G \Rightarrow H_1 \cap H_2 \leq G$

Teorema Fie $f: G \to G'$ mor de gr

1) $H \leq G \Rightarrow f(H) \leq G'$

2) $H' \leq G' \Rightarrow f^{-1}(H') \leq G$

Def $f^{-1}(\{1_{G'}\})$ s.n. $\mathrm{Ker}(f)$ (nucleul)

Propr. $f: G \to G'$ mor de gr.

f inj $\Leftrightarrow \mathrm{Ker}(f) = \{1_G\}$

($1_G \in \mathrm{Ker}(f)$ $\forall$ mor de gr $f: G \to G'$)

① $f: (\mathbb{Z} \times \mathbb{Z}, +) \to (\mathbb{Z}, +)$

$f(x, y) = x - y$

$\mathrm{Ker}(f) = \{(x, y) \in \mathbb{Z} \times \mathbb{Z} / f(x, y) = 0\}$

$= \{(x, y) / \in \mathbb{Z} \times \mathbb{Z} / x - y = 0\}$

$= \{(x, x) \in \mathbb{Z} \times \mathbb{Z}\}$

Def $(G, \cdot)$ $A \subseteq G$

$\langle A \rangle \overset{\text{def}}{=} \{a_1^{\pm 1} a_2^{\pm 1} \cdots a_n^{\pm 1} / a_1, \ldots, a_n \in A; n \geq 1\}$

$1_G = a \cdot a^{-1}$ $\leq G$

Prim def: $\langle \phi \rangle = \{1_G\}$

OBS

① $G = \langle G \rangle$

② $A = \{a\}$ $\langle a \rangle = \{a^k / k \in \mathbb{Z}\}$ ($1_G = a^0$)

$\langle a \rangle$ = not aG

$\langle a \rangle \to$ s.m. ciclic generat de a

Ex: 1) $G = (\mathbb{Z}, +)$ $\langle n \rangle = n\mathbb{Z} = \{kn / k \in \mathbb{Z}\}$

$G = 1\mathbb{Z}$ (ciclic)

2) $G = (\mathbb{Z}_{10}, +)$

$\langle \hat{1} \rangle = \hat{1}\mathbb{Z}_{10} = \{k \cdot \hat{1} / k \in \mathbb{Z}\}$ ciclic

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

$\langle \hat{1} \rangle = \langle \hat{1}^k / k \in \mathbb{Z} \rangle = \{\hat{1}\}$

$\langle \hat{3} \rangle = \{\hat{1}, \hat{3}\}$ $\langle \hat{7} \rangle = \{\hat{1}, \hat{7}\}$

$\langle \hat{5} \rangle = \{\hat{1}, \hat{5}\}$

$\Rightarrow$ nu e ciclic

$G = \langle \{\hat{3}, \hat{5}\} \rangle = \{\hat{3}^{\pm 1} \hat{5}^{\pm 1} \cdot\}$

$= \{\hat{7}, \hat{1}, \hat{3}, \hat{5}\}$

Teorema: $(G, \cdot)$ abelian

$\langle A \rangle = \langle a_1 \dots a_n \rangle = \{a_1^{k_1} a_2^{k_2} \dots a_n^{k_n} / k_1, \dots, k_n \in \mathbb{Z}\}$

Def $\langle A \rangle = G$ G generat de A

- ciclic $G = \langle a \rangle$, $a \in G$
- finit generat $A \subseteq G$ $\quad |A| < \infty$ $\quad$ a.i. $G = \langle A \rangle$

Obs • $(\mathbb{Z}, +)$ și $(\mathbb{Z}_n, +)$ - ciclice

• ciclic $\Rightarrow$ abelian.

Def $(G, \cdot)$ grup.

$H \leq G$

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

2) $x \equiv_d y \pmod{H} \Leftrightarrow xy^{-1} \in H$

---

① $a^b \bmod c$

$2021^{2021} \pmod{22}$

$\hat{2021}^{2021} \text{ în } \mathbb{Z}_{22}$

$2021^{2021} \equiv 19^{2021} \pmod{22} \equiv (-3)^{2021} \pmod{22}$

T. Euler $(a, n) = 1$

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

$\varphi(22) = 10$

$-(3^{10})^{202} \cdot 3 \pmod{22} \equiv -3 \pmod{22} \equiv 19 \pmod{22}$

② $G = \{x \in \mathbb{R} \mid 0 \le x < 1\}$

$x * y = \{x+y\}$ ↑

$(G, *)$ abelian ↑

$\boxed{\{x\} = x - [x]}$

"$*$" - asc.

$a * (b * c) = a * \{b+c\} = \{a + \{b+c\}\}$

$= a + \{b+c\} - [a + \{b+c\}]$

$= a + b + c - [b+c] - ([a+b+c] - [b+c])$

$= \{a+b+c\} = (a * b) * c \Rightarrow$ "$*$" asc.

"$*$" e com. evident.

$x * 0 = \{x+0\} = \{x\} = x = 0 * x$ 0 el n.

$x \in [0,1)$

$U(G) = G \Rightarrow (G, *)$ g a.

③ Calc morf de gr dim:

$(\mathbb{Z}, +)$ și $(\mathbb{Z}, +)$

$f: (\mathbb{Z}, +) \to (\mathbb{Z}, +)$ morf gr.

$f(x+y) = f(x) + f(y)$ $(\Rightarrow f(0) = 0)$

$f(1+1) = f(1) + f(1) = 2f(1)$

$f(1+2) = f(1) + f(2) = f(1) + f(1+1) = 3f(1)$

$f(n) = n f(1)$

~~$f(n) = f(a) + f(-n)$~~

$f(-n) = ?$

$f(0) = f(n + (-n)) = f(n) + f(-n) \Rightarrow$

$\Rightarrow f(-n) = -f(n) = -n f(1)$

$\Rightarrow f(n) = n f(1) \ (\forall) \ n \in \mathbb{Z}$

$f_a : (\mathbb{Z}, +) \to (\mathbb{Z}, +) \quad f_a(n) = na \ (\forall) \ n \in \mathbb{Z}$

Generalizare $(G, +)$ gr. Morf de gr de la $(\mathbb{Z}, +)$ în $(G, +)$ sunt date de

$f_a (\mathbb{Z}, +) \to (G, +)$

$f_a(n) = na \quad n \in \mathbb{Z}$

Seminar 9

Teoremă

$(G, \cdot)$ gr. $H \leq G$ $\Rightarrow \begin{cases} u \equiv_s v \pmod H \Leftrightarrow xH \\ u \equiv_d v \pmod H \Leftrightarrow Hx \end{cases}$

Mulțimile factor $(G/H)_s$ și $(G/H)_d$

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

indicele lui H în G n.n. $[G:H]$

OBS G ab. $\Rightarrow xH = Hx \Rightarrow (G/H)_s = (G/H)_d$

$S_n = \{\sigma : \{1,2,\dots,n\} \to \{1,2,\dots,n\} \mid \sigma \text{ bij}\}$

$|S_n| = n!$

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

$(12)\circ(13) = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = (132)$

Thm lui Lagrange

$H \le G \Rightarrow |G| = |H| \cdot [G:H]$

Def $(G,\cdot)$ gr. $x \in G$.

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

OBS

1) $(G,\cdot)$ gr. $x \in G$

$\operatorname{ord}(x) = n < \infty \Rightarrow |\langle x \rangle| = n \ (|\langle x \rangle| = \operatorname{ord}(x))$

2) $(G,\cdot)$ gr finit $\Rightarrow \operatorname{ord}(x) < \infty$ și $\operatorname{ord}(x) \mid |G|$, $x \in G$

3) $x^n = e$; $n = |G|$

Mica teoremă a lui Fermat

p nr prim, $p \nmid a$ $\Rightarrow a^{p-1} \equiv 1 \pmod p$

Dacă p prim $\Rightarrow a^p \equiv a \pmod p$ $\forall a \in \mathbb{N}$

Def $H \leq G$ $i(G, \cdot)$

H ogn. $\Leftrightarrow xH = Hx$ $\forall x \in G$

Not $H \trianglelefteq G$

Propr (cum verificăm)

$H \trianglelefteq G \Leftrightarrow xHx^{-1} \subseteq H$

Dacă $(G, \cdot)$ abelian $\Rightarrow (\forall) H \leq G \Rightarrow H \trianglelefteq G$

① $f: G \to G'$ morf $\Rightarrow \ker f \trianglelefteq G$

② $H \leq G$ $[G:H] = 2 \Rightarrow H \trianglelefteq G$

Grup factor

$(G, \cdot)$, $H \trianglelefteq G$

$G/H = \{ \hat{x} \mid x \in G \}$ $(\hat{x} \overset{not}{=} xH = Hx)$

(OBS) Dacă $G = (\mathbb{Z}, +)$ g.a. $\Rightarrow$

$\Rightarrow \left(\frac{\mathbb{Z}}{n\mathbb{Z}}, +\right) = (\mathbb{Z}_n, +)$

TFi (Teorema fundamentală de izomorfism)

Fie $\varphi: G \to G'$ mrf de gr.

Atunci $G/\ker\varphi \simeq \operatorname{Im}\varphi$

$\bar{\varphi}: G/\ker\varphi \to \operatorname{Im}\varphi \qquad \bar{\varphi}(\hat{x}) = \varphi(x)$

$G = (\mathbb{Z}_4, +)$

+	$\hat{0}$	$\hat{1}$	$\hat{2}$	$\hat{3}$
$\hat{0}$	$\hat{0}$	$\hat{1}$	$\hat{2}$	$\hat{3}$
$\hat{1}$	$\hat{1}$	$\hat{2}$	$\hat{3}$	$\hat{0}$
$\hat{2}$	$\hat{2}$	$\hat{3}$	$\hat{0}$	$\hat{1}$
$\hat{3}$	$\hat{3}$	$\hat{0}$	$\hat{1}$	$\hat{2}$

$\operatorname{ord}(\hat{0}) = 1$

$\operatorname{ord}(\hat{1}) = 4$

$\operatorname{ord}(\hat{2}) = 2$

$\operatorname{ord}(\hat{3}) = 4$

$\Rightarrow G = \langle\hat{1}\rangle = \langle\hat{3}\rangle$

$|\langle g\rangle| = \operatorname{ord}(g)$

$(G, \cdot)$

$\operatorname{ord}(g) = n$

$\langle g\rangle = \{1, g, g^2, \dots, g^{n-1}\}$

$G = (\mathbb{Z}_2 \times \mathbb{Z}_2, +)$

$\mathbb{Z}_2 \times \mathbb{Z}_2 = \{(\hat{0},\hat{0}), (\hat{0},\hat{1}), (\hat{1},\hat{0}), (\hat{1},\hat{1})\}$

$+$	$(\hat{0},\hat{0})$	$(\hat{0},\hat{1})$	$(\hat{1},\hat{0})$	$(\hat{1},\hat{1})$
$(\hat{0},\hat{0})$	$(\hat{0},\hat{0})$	$(\hat{0},\hat{1})$	$(\hat{1},\hat{0})$	$(\hat{1},\hat{1})$
$(\hat{0},\hat{1})$	$(\hat{0},\hat{1})$	$(\hat{0},\hat{0})$	$(\hat{1},\hat{1})$	$(\hat{1},\hat{0})$
$(\hat{1},\hat{0})$	$(\hat{1},\hat{0})$	$(\hat{1},\hat{1})$	$(\hat{0},\hat{0})$	$(\hat{0},\hat{1})$
$(\hat{1},\hat{1})$	$(\hat{1},\hat{1})$	$(\hat{1},\hat{0})$	$(\hat{0},\hat{1})$	$(\hat{0},\hat{0})$

$ord((\hat{0},\hat{1})) = ord((\hat{1},\hat{0})) = 2 = ord((\hat{1},\hat{1}))$

$ord((\hat{0},\hat{0})) = 1$

G nu e ciclic

G poate fi generat minimal de 2 el.

$G = \langle (\hat{0},\hat{1}), (\hat{1},\hat{0}) \rangle = \langle (\hat{0},\hat{1}), (\hat{1},\hat{1}) \rangle =$

$= \langle (\hat{1},\hat{0}, (\hat{1},\hat{1}) \rangle$

① $U(\mathbb{Z}_{19}, \cdot)$

$(U_4 = \{z \in \mathbb{C} / z^4 = 1\}, \cdot)$

$U(\mathbb{Z}_8, \cdot)$

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

$ord(\bar{3}) = ord(\bar{5}) = ord(\bar{7}) = 2$

$= \langle \bar{3}, \bar{5} \rangle = \langle \bar{3}, \bar{7} \rangle = \langle \bar{5}, \bar{7} \rangle$

$U_4 = \{\pm 1, \pm i\}$

$U(\mathbb{Z}_8, \cdot)$

$\cdot$	$\bar{1}$	$\bar{3}$	$\bar{5}$	$\bar{7}$
$\bar{1}$	$\bar{1}$	$\bar{3}$	$\bar{5}$	$\bar{7}$
$\bar{3}$	$\bar{3}$	$\bar{1}$	$\bar{7}$	$\bar{5}$
$\bar{5}$	$\bar{5}$	$\bar{7}$	$\bar{1}$	$\bar{3}$
$\bar{7}$	$\bar{7}$	$\bar{5}$	$\bar{3}$	$\bar{1}$

$\cdot$	1	-1	i	$-i$
1	1	-1	i	$-i$
-1	-1	1	$-i$	i
i	i	$-i$	-1	1
$-i$	$-i$	i	1	-1

$U(\mathbb{Z}_8, \cdot) \simeq (\mathbb{Z}_2 \times \mathbb{Z}_2, +)$ (prin sup tabelelor)

$f(\hat{0}, \hat{1}) + (\hat{1}, \hat{0}) = f(\hat{0}, \hat{1}) \cdot f(\hat{1}, \hat{0})$

$\Downarrow$ $\qquad\qquad$ $\Downarrow$

$f(\hat{1}, \hat{1})$ $\qquad\qquad$ $\bar{3} \cdot \bar{5}$

$\Downarrow$ $\qquad\qquad$ $\Downarrow$

$\bar{7}$ $\qquad\qquad$ $\bar{7}$

OBS $\bar{3}$ 6 izo intre cele 2 gr.

$(\mathbb{Z}_4, +) \simeq (U_4, \cdot)$

OBS 2 izom intre cele 2 gr.

---

② $(\mathbb{Z}_4, +) \not\simeq (\mathbb{Z}_2 \times \mathbb{Z}_2, +)$

Pp. prin abs ca $(\mathbb{Z}_4, +) \simeq (\mathbb{Z}_2 \times \mathbb{Z}_2, +)$

$f: (\mathbb{Z}_4, +) \to (\mathbb{Z}_2 \times \mathbb{Z}_2, +)$

$f(\hat{1}) \in \mathbb{Z}_2 \times \mathbb{Z}_2$

$\text{ord}(f(\hat{1})) \begin{cases} \to 1 \\ \to 2 \end{cases}$ $f(\hat{1}) = (\bar{0},\bar{0})$ ✗ (f bij)

$f(\hat{1}) =$ oblalte 3

f izo $\Rightarrow f(\hat{0}) = (\bar{0},\bar{0})$

$f(\hat{1}) + f(\hat{1}) = (\bar{0},\bar{0})$

$f(\hat{1}+\hat{1}) = f(\hat{2})$ ✗ (f bij) $\Rightarrow$ Pr falsă.

$\Rightarrow$ nu sunt izo

OBS G grup

$|G| = p$ $p = \text{prim}$ $\Rightarrow G \cong (\mathbb{Z}_p, +)$

Prop $(G_1, \cdot)$ și $(G_2, \cdot)$ izo.

$x \in G_1$

$\text{ord}(x) = n$

$G_1 \overset{f}{\cong} G_2 \Rightarrow \text{ord}(f(x)) = n$

OBS G ab $|G| = n \cong (\mathbb{Z}_{d_1} \times \mathbb{Z}_{d_2} \times \dots \times \mathbb{Z}_{d_k}, +)$

$d_1 | d_2 | \dots | d_k$ $d_1 d_2 \dots d_k = n$

Seminar 10

① $(\mathbb{C}^*/U, \cdot) \cong (\mathbb{R}_+^*, \cdot)$ $U = \{z \in \mathbb{C} \mid |z| = 1\}$

$f: \mathbb{C}^* \to \mathbb{R}_+^*$ $f(z) = |z| > 0$

Pp f izo $\Rightarrow f(z_1 \cdot z_2) = f(z_1) \cdot f(z_2)$ $\Rightarrow \text{Im} f = \mathbb{R}_+^*$

$\ker f = U$

TFI $\Rightarrow \bar{f}: \mathbb{C}^*/U \to \mathbb{R}_+^*$ $\bar{f}(\hat{z}) = f(z)$ izo.

Teorema de str. a grp. ciclice

Orice gr ciclic { finit $\cong (\mathbb{Z}_n, +)$; infinit $\cong (\mathbb{Z}, +)$

Grupul $(S_n, \circ)$

Dacă $|A| = |B| \Rightarrow (S_A, \circ) \cong (S_B, \circ)$

Prop

$|S_n| = n!$ S_n nead $\Leftrightarrow n \geq 3$

Thm Cayley Orice grup cu n elemente este izomorf cu un sg. a lui S_n // Orice grup $G \cong$ sg S_n

Def • Cicli de lungime 2 s.n. transpoziții

• 2 cicli $(i_1 i_2 \dots i_k)$ și $(j_1 j_2 \dots j_\ell)$ s.n. disjuncți dacă $\{i_1, \dots, i_k\} \cap \{j_1, \dots, j_\ell\} = \emptyset$

• 2 cicli disjuncți comută

$(i_1 \dots i_k) \circ (j_1 \dots j_\ell) = (j_1 \dots j_\ell) \circ (i_1 \dots i_k)$

$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 2 & 4 & 7 & 1 & 5 & 6 \end{pmatrix} = (1\ 3\ 4\ 7\ 6\ 5)$

$\sigma^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 5 & 2 & 1 & 3 & 6 & 7 & 4 \end{pmatrix} = (1\ 5\ 6\ 7\ 4\ 3)$

(6) $(G, \cdot)$ gr.

$\text{ord}(x) = n \quad \forall k \in \mathbb{N} \quad \text{ord}(x^k) = \frac{n}{(n,k)}$

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

$\Rightarrow (\mathbb{Z}_{1000}, +) \quad \text{ord}(\hat{144}) = \frac{1000}{(1000,144)} = \frac{1000}{2^3} = 125$

$\Rightarrow (\mathbb{Z}_{311}, +) \quad \text{ord}(\hat{33}) = \frac{311}{(33,311)} = 311$

El de ordin n din $(\mathbb{Z}_n, +)$ sunt $\hat{44} \mid (k,n) = 1$

OBS $x \in G_1 \ ; \ y \in G_2$

$\text{ord}(x) = n$, $\text{ord}(y) = m$ $\Rightarrow \text{ord}((x,y)) = [n, m]$

Seminar 11

- Un ciclu de lungime k poate fi scris în k moduri

- $(i_1 \dots i_k)^{-1} = (i_k i_{k-1} \dots i_1)$

$\sigma = (1\ 12\ 8\ 10\ 4)(2\ 13)(5\ 11\ 7)(6\ 9)$

$\sigma^{-1} = (1\ 12\ 8\ 10\ 4)^{-1}(2\ 13)^{-1}(5\ 11\ 7)^{-1}(6\ 9)^{-1}$

$= (4\ 10\ 8\ 12\ 1)(13\ 2)(7\ 11\ 5)(9\ 6)$

Propr.

- ordinul unui ciclu este lungimea ciclului
- ordinul unei permutări $\sigma \in S_n$ este cmmmc al lungimii ciclilor
- orice permutare se scrie ca produs de transpoziții $(K-1)$

Not
- $m(\sigma)$ = nr de inversiuni
- $\operatorname{sgn}(\sigma) = (-1)^{m(\sigma)}$
- $\operatorname{sgn}((i_1 \dots i_k)) = (-1)^{k-1}$
- $\operatorname{sgn}((i\ j)) = -1$
- A_n = multime perm pare
- $\operatorname{sgn}(\sigma) = (-1)^k$; k nr de transp din desc.

①

a) el de ord 8 din $\mathbb{Z}_6 \times \mathbb{Z}_{10}$

$\{(\hat{k}, \hat{l}) \in \mathbb{Z}_6 \times \mathbb{Z}_8 \mid \operatorname{ord}((\hat{k}, \hat{l})) = 8\}$

$\operatorname{ord}((\hat{k}, \hat{l})) = [\operatorname{ord}(\hat{k}), \operatorname{ord}(\hat{l})] = 8 \Rightarrow$

$\Rightarrow \operatorname{ord}(\hat{k}) = 8$ sau ~~$\operatorname{ord}(\hat{k}) = 1$~~ $\operatorname{ord}(\hat{l}) = 8$

~~$\operatorname{ord}(\hat{k}) = 4$~~

T.L. $\Rightarrow$ $ord(\hat{4}) \mid 6$ $\Rightarrow ord(\hat{4}) \neq 8$ ✗

și

$ord(\hat{\bar{4}}) \mid 10 \Rightarrow ord(\hat{4}) \neq 8$

$\Rightarrow$ Nu ($\exists$) el de ord 8 în $\mathbb{Z}_6 \times \mathbb{Z}_{10}$

a) el de ord. 4 din $\mathbb{Z}_{12} \times \mathbb{Z}_{15}$

$\{(\hat{a}, \hat{b}) \in \mathbb{Z}_{12} \times \mathbb{Z}_{15} \mid ord((\hat{a}, \hat{b})) = 4\}$

$ord((\hat{a}, \hat{b})) = [ord(\hat{a}), ord(\hat{b})] = 4$

$\Rightarrow$ $\begin{cases} \text{~~ord}(\hat{a}) = 1\text{~~} \\ ord(\hat{b}) = 4 \end{cases}$ sau $\begin{cases} ord(\hat{a}) = 4. \\ \text{~~ord}(\hat{b}) = 1\text{~~} \end{cases}$

(I) (II)

Caz (I)

Dacă $ord(\hat{b}) = 4 \Rightarrow ord(\hat{b}) \mid 15 \Rightarrow$ ~~4~~ $4 \mid 15$ ✗

Caz (II)

$ord(\hat{a}) = 4 \mid 12$ ✓

~~ord~~ $(\hat{a}, \hat{b}) \in \{(4,1), (4,2), (4,4)\}$

✓ N

Singura variantă $ord(\hat{a}) = 4$

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

$ord(\hat{a}) = 4 \Rightarrow \frac{12}{(12,a)}$

$a = 3$ sau $a = 9$

$\Rightarrow$ Elementele de ordin 4 din $\mathbb{Z}_{12} \times \mathbb{Z}_{15}$ sunt $(\hat{3}, \bar{0})$ și $(\hat{9}, \bar{0})$

c) ord 8 din $\mathbb{Z}_{16} \times \mathbb{Z}_{64}$

$\{(\hat{a}, \bar{b}) \in \mathbb{Z}_{16} \times \mathbb{Z}_{64} \mid ord((\hat{a}, \bar{b})) = 8\}$

$ord((\hat{a}, \bar{b})) = [ord(\hat{a}), ord(\bar{b})]$

$ord((\hat{a}, \bar{b})) \in \{(1,8), (2,8), (4,8), (8,8), (8,4), (8,2), (8,1)\}$

(1,8) $\hat{a} = \hat{0}$ $\Rightarrow (\hat{0}, \bar{8})$ $(\hat{0}, \bar{12})$

$8 = \frac{64}{(64,b)} \Rightarrow \{8\}_{12}$

(2,8)

$2 = \frac{16}{(16,a)} \Rightarrow \{8\}$ $\Rightarrow (\hat{8}, \bar{8})$ $(\hat{8}, \bar{12})$

$8 \Rightarrow \{8\}_{12}$

(4,8)

$4 = \frac{16}{(16,a)} \Rightarrow \{4\}_{12} \Rightarrow (\hat{4}, \bar{8})$ $(\hat{12}, \bar{8})$ $(\hat{4}, \bar{12})$ $(\hat{12}, \bar{12})$

$8 \Rightarrow \{8\}_{12}$

(8,8) $8 = \frac{16}{(16,a)} \Rightarrow \{2\}_{16,10}$ $\Rightarrow (\hat{2}, \bar{8})$ $(\hat{10}, \bar{8})$ $(\hat{6}, \bar{8})$ $(\hat{14}, \bar{8})$ $(\hat{2}, \bar{12})$ $(\hat{6}, \bar{12})$ $(\hat{14}, \bar{12})$

$8 \Rightarrow \{8\}_{12}$

(8,4)

$8 = \frac{16}{(a,16)} \Rightarrow \{2, 6, 14\}$

$4 = \frac{64}{(a,64)} \Rightarrow \{16, 48\}$

(8,2)

8,1

② $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 2 & 9 & 5 & 7 & 10 & 3 & 4 & 6 & 1 & 8 \end{pmatrix}$

a) cicli + transp.

$\tau = (1\ 2\ 9)(3\ 5\ 10\ 8\ 6)(4\ 7)$

$\tau = (1\ 2)(2\ 9)(3\ 5)(5\ 10)(10\ 8)(8\ 6)(4\ 7)$

b) $\operatorname{sgn}(\tau) = (-1)^k$; k nr de transp.

$\operatorname{sgn}(\tau) = (-1)^7 = -1 \Rightarrow$ impar

$\operatorname{ord}(\tau) = [3, 5, 2] = 30$

$\tau^{2021} = (\tau^{30})^{67} \cdot \tau^{11} = \tau^{11}$

$\tau^{-1} = (9\ 2\ 1)(6\ 8\ 10\ 5\ 3)(7\ 4)$

$\tau^{11} = (1\ 9\ 2)(3\ 5\ 10\ 8\ 6)(4\ 7)$

c) $\beta \in S_{10}$ a.i. $\beta^2 = \tau$

$\left.\begin{array}{l} \operatorname{sgn}(\sigma^2) = 1 \\ \operatorname{sgn}(\sigma) = -1 \end{array}\right| \Rightarrow$ Nu există

d) $\rho \in S_{10}$ $\operatorname{ord}(\rho) = 10$. Poate fi ρ perm. Para?

$\operatorname{ord}(\rho) = 10 \Leftrightarrow [l_1, l_2, \dots l_k] = 10$; l_j lungimea ciclului j

$\Delta_{10}^+ = \{1, 2, 5, 10\}$

① $\rho = (k_1, \dots, k_{10})$ ciclu de lungime 10

$\operatorname{sgn}(\rho) = (-1)^9 = -1$ ⊖

② ~~$\rho = (\quad)$~~

$\rho = (k_1 k_2)(k_3 k_4 k_5 k_6 k_7)$ $\operatorname{sgn} = -1$

$\rho = (k_1 k_2)(k_3 k_4)(k_5 k_6 k_7 k_8 k_9)$

$\operatorname{sgn} = 1$

$\Rightarrow$ par $\Rightarrow$ ΔA

e) Există perm de ordin 35 în S_{10}? Dar de ord 30

ΔA → Da →

Seminar 12

$A[X] \ni f(X) = a_0 + a_1 X + \dots a_n X^n$

$(a_0, \dots, a_n)$ coef polinomiali

grad(f) = cel mai mare număr natural k a.î. $a_k \neq 0$

grad(0) = $-\infty$

a_n s.n. coeficientul dominant al lui $f(x)$

Propoziție $(A[X], +, \cdot)$

① $f, g \in A[X] \setminus \{0\} \Rightarrow \text{grad}(f+g) \leq \max\{\text{grad}(f), \text{grad}(g)\}$

$\text{grad}(f \cdot g) \leq \text{grad}(f) + \text{grad}(g)$

② $0_{A[X]} = 0$ (polinomul identic nul)

$1_{A[X]} = 1$ (Polinomul constant 1)

Notăm $(A, +, \cdot)$ inel com., nenul

Def $a \in A$ com. div. al lui zero dacă $(\exists) x \in A, x \neq 0$ a.î. $ax = 0$

- în orice inel (nenul) 0 este div. al lui 0
- un element inv. nu e div. al lui 0

Not A inel $\Rightarrow D(A)$ = div. lui 0

Def A inel, $D(A) = \{0\}$ s.n. domeniu de integritate

OBS Un corp este domeniu de integritate

Obs • $\mathcal{U}(\mathbb{Z}_n) = \mathbb{Z}_n \setminus U(\mathbb{Z}_n)$

• $(\mathbb{Z}_p, +, \cdot)$ corp $\Leftrightarrow p$ = prim

Def

• A inel
• $I \subseteq A$
• $(I,+) \leq (A,+)$
• $a \cdot x \in I$ ($\forall$) $a \in I$, $x \in A$

$\Rightarrow$ ideal al lui A

• Idealele lui $(\mathbb{Z},+,\cdot)$ sunt $n\mathbb{Z}$
• Un inel $(A,+,\cdot)$ are 2 ideale $\begin{cases} \{0\} \\ A \end{cases}$

Def Corp = inel cu 2 ideale exact.

Propr

• I, J ideale $\Rightarrow I \cap J$ & $I + J = \{a+b \mid a \in I, b \in J\}$ ideale

Def

$(A,+,\cdot)$ inel, $a \in A$

aA sau (a) idealul generat de a $= \{ax \mid x \in A\}$

(aA = idealul principal generat de $a \in A$)

$(a_1, \dots, a_n)$ $A = (a_1, \dots, a_n) = \{a_1 b_1 + \dots + a_n b_n \mid b_1, \dots, b_n \in A\}$

$\begin{cases} a\mathbb{Z} + b\mathbb{Z} = (a,b)\mathbb{Z} \\ a\mathbb{Z} \cap b\mathbb{Z} = [a,b]\mathbb{Z} \end{cases}$

Def $(A \times B, +, \cdot)$ z inele prod

- A și B inele

$f: A \to B$ morfism de inele ① $f(x+y) = f(x) + f(y)$

(unitar) ② $f(xy) = f(x)f(y)$

③ $f(1_A) = 1_B$

Inel factor

$(A, +, \cdot)$ inel

I ideal

$(I, +) \leq (A, +)$ gr ab. $\Rightarrow (I, +) \trianglelefteq (A, +)$

$\Rightarrow (A/I, +)$ gr factor

Prop. $f: A \to B$ morf de inele

a) $\exists$ ideal al lui $B \Rightarrow f^{-1}(y)$ ideal al lui A

b) $\ker f$ ideal al lui A | f inj $\Rightarrow \ker f = \{0_A\}$

c) $f(A)$ ind (subinel al lui B)

TFii $f: A \to B$ morf in.

$A/\ker f \cong \operatorname{Im}(f)$ izo.

$F: A/\ker f \to \operatorname{Im}(f)$ $F(\hat{a}) = f(a)$ izom inele

LMR

$n_1, \dots, n_k$ întregi

$(n_i, n_j) = 1 \quad \forall i \neq j$ $\Rightarrow \mathbb{Z}_{n_1 \cdots n_k} \simeq \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_k}$

① $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 4 & 9 & 7 & 2 & 3 & 1 & 8 & 5 & 6 \end{pmatrix} \in S_9$

$\sigma_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 3 & 5 & 6 & 9 & 1 & 2 & 4 & 7 & 10 & 8 \end{pmatrix} \in S_{10}$

a) descompuneri

$\sigma = (1\ 4\ 2\ 9\ 6)(3\ 7\ 8\ 5)$

$\sigma = (1\ 4)(4\ 2)(2\ 9)(9\ 6)(3\ 7)(7\ 8)(8\ 5)$

$\sigma_1 = (1\ 3\ 6\ 2\ 5)(4\ 9\ 10\ 8\ 7)$

$= (1\ 3)(3\ 6)(6\ 2)(2\ 5)(4\ 9)(9\ 10)(10\ 8)(8\ 7)$

b) $\operatorname{sgn}(\sigma)$, $\operatorname{ord}(\sigma)$, σ^{2022}

$\operatorname{sgn}(\sigma) = (-1)^7 = -1 \Rightarrow \sigma$ imp.

$\operatorname{ord}(\sigma) = [5, 4] = 20 \Rightarrow \sigma^{20} = e$

$\sigma^{2022} = (\sigma^{20})^{101} \cdot \sigma^2 = \sigma^2 = (1\ 2\ 6\ 4\ 9)(3\ 8\ 7\ 5)$

c) $\beta^3 = \sigma$ (resp. $\beta^3 = \sigma_1$)

$\beta^3 = (1\ 4\ 2\ 9\ 6)(3\ 7\ 8\ 5) = \nabla$

$\exists n$ ca $(\exists)\ \beta \in S_9$ ai $\beta^3 = \nabla$

$\beta = c_{i_1} \cdot c_{i_2} \cdot \ldots \cdot c_{i_k}$ → k cicli

$i_1 + \ldots + i_k = 9$ $\quad 1 \le k \le 9$ ($\not\exists$ nr $k = 9$)

$\beta^3 = c_{i_1}^3 \ldots c_{i_k}^3$

Algoritm

$c_\ell^3 \xrightarrow{3 \mid \ell} c_\ell^3 =$ prod de 3 cicli de lungime $\ell/3$

$\xrightarrow{3 \nmid \ell} c_\ell^3 =$ un ciclu de lungime ℓ

$\beta^3 = \nabla = (1\ 4\ 2\ 9\ 6)(3\ 7\ 8\ 5)$

$\Rightarrow k = 2$

2 cicli de $\ell_1 = 5$ $i_2 = 4$

$\beta = c_5 \cdot c_4$

$\beta^3 = c_5^3 \cdot c_4^3$

$\boxed{c_\ell^k = c_\ell \mid k = \ell}$

$c_5^3 = (1\ 4\ 2\ 9\ 6) \Rightarrow (c_5^3)^2 = c_5^6 = c_5^5 \cdot c_5$

$= c_5^2$

$c_5 = (1\ 2\ 6\ 4\ 9)$

$c_4^3 = (3\ 7\ 8\ 5) \rightarrow (c_4^3)^2 = c_4^6 = c_4^3 \Rightarrow$

$\Rightarrow c_4 = (3\ 5\ 8\ 7)$

$\Rightarrow \beta = (1\ 2\ 6\ 4\ 9)(3\ 5\ 8\ 7)$

(reciproca)

$\sigma^3 = \tau_1^4 = (1\ 3\ 6\ 2\ 5)(4\ 9\ 10\ 8\ 7)$

$\sigma = c_{i_1} \dots i_4 \Rightarrow \sigma_3 = c_{i_1}^3 \cdot c_{i_2}^3$

$\sigma^3 = (1\ 3\ 6\ 2\ 5)(4\ 9\ 10\ 8\ 7)$

$\sigma^3 = C_5^3\ C_5^3 \Rightarrow \sigma = C_5\ C_5$

$C_5^3 \Rightarrow (C_5^3)^2 = C_5^2 \Rightarrow C_{5_1} = (1\ 6\ 5\ 3\ 2)$

$C_{5_2} = (4\ 10\ 7\ 9\ 8)$

sol unică.

d) $\rho \in S_9$ $ord(\rho) = 9$. Poate fi ρ par sau impar?

Singura var pt. $ord(\rho) = 9$ [illegible]

ρ poate. $sgn(\rho) = (-1)^{9-1} = 1$

[illegible] S_n

OBS $\tau^m = e$; m = lungimea ciclului

Seminar 13

- K corp (= inel în care orice el. nenul e inversabil)
- $K[X]$ $grad(fg) = grad(f) + grad(g)$
- $(K[X], +, \cdot)$ - inel com.

Propr $K[X]$

① $K[X]$ dom de int $U(K[X]) = K \setminus \{0\}$

② Fie $f: K \to S$ morf de inele $((S, +, \cdot))$

$\tilde{f}: K[X] \to S$

$\tilde{f}(a_0 + a_1 X + \dots + a_n X^n) = f(a_0) + f(a_1) b + \dots + f(a_n) b^n$

morf de inele.

③ I i R

$f(X), g(X) \in K[X]$ $g(X) \neq 0$

$(\exists!)\ q(X), r(X) \in K[X]$ a.i.

$f(X) = g(X) \cdot q(X) + r(X)$

$$\begin{array}{r|l} X^3 - 3X + 2 & 2X + 1 \\ \hline -X^3 - \frac{1}{2}X^2 & \frac{1}{2}X^2 - \frac{1}{4}X - \frac{11}{8} \\ \hline -\frac{1}{2}X^2 - 3X + 2 & \\ \frac{1}{2}X^2 + \frac{1}{4}X & \\ \hline -\frac{11}{4}X + 2 & \\ \frac{11}{4}X + \frac{11}{8} & \\ \hline \frac{27}{8} & \end{array}$$

$f(X)$ $g(X)$ $q(X)$ $r(X)$

$$X^2 - 3X + 2 = (2X + 1) \cdot \left(\frac{1}{2}X^2 - \frac{1}{4}X - \frac{11}{8}\right) + \frac{27}{8}$$

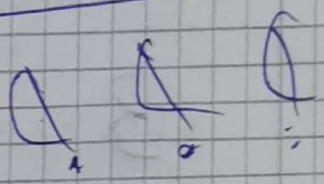
4 Teorema lui Bézout

$f(x) \in K[X]$ $a \in K$

$\frac{f(x)}{x-a} = c\hat{o}t + f(a)$

Im part., $f(a)=0 \Leftrightarrow f(x)=(x-a)g(x)$

TCR



$n_1, n_2, \dots, n_r \geq 2 \in \mathbb{N}$

$(n_i, n_j)=1 \quad \forall\, i \neq j$ și $a_1, a_2, \dots, a_n \in \mathbb{Z}$

Atunci

$$\begin{cases} x \equiv a_1 \pmod{n_1} \\ \vdots \\ x \equiv a_r \pmod{n_r} \end{cases}$$

are sol unică modulo $n_1 \cdot n_2 \cdot \dots \cdot n_r$

Alg de rez.

⊙ Consider $N = n_1 \cdot n_2 \cdot \dots \cdot n_r$

$N_i = \frac{N}{n_i} \quad \forall\, i = \overline{1,r}$

⊙⊙ Determinăm $x_1, \dots, x_r \in \mathbb{Z}$ a.î.

$N_i x_i \equiv 1 \pmod{n_i} \quad \forall\, i = \overline{1,r}$

⊙⊙ Soluția unică modulo $n_1 \cdot n_2 \cdot \dots \cdot n_r$ este $x \pmod N$

$x = a_1 N_1 x_1 + \dots a_r N_r x_r$

(9)

$$\begin{cases} x \equiv 3 \pmod 5 \\ x \equiv 2 \pmod 7 \\ x \equiv 8 \pmod 9 \end{cases}$$

$N = 5 \cdot 7 \cdot 9 = 315$

$N_1 = 63 \quad N_2 = 45 \quad N_3 = 35$

$63 x_1 \equiv 1 \pmod 5 \Rightarrow x_1 = 2$

$45 x_2 \equiv 1 \pmod 7 \Rightarrow x_2 = 5$

$35 x_3 \equiv 1 \pmod 9 \Rightarrow x_3 = 8$

$x = 3 \cdot 2 \cdot 63 + 2 \cdot 5 \cdot 45 + 8 \cdot 8 \cdot 35 \mod 315$

$x = 378 + 450 + 2240 = 3068$

$x \bmod 315 = \boxed{233}$

Seminar 14

① Calc. $7^{7^{88}} \pmod{11}$

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

$$a^P \equiv a \pmod P$$

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

$(7,11)=1 \overset{\text{Euler}}{\Rightarrow} \boxed{7^{10} \equiv 1 \pmod{11}}$

Pt. a calcula $7^{7^{8^8}} \pmod{11}$ e suficient să calc. $7^{8^8} \pmod{10}$

u.c. a lui 7^n este $\begin{cases} 7 & u \equiv 1(4) \\ 9 & u \equiv 2(4) \\ 3 & u \equiv 3(4) \\ 1 & u \equiv 0(4) \end{cases}$

Ca să aflăm ultima cifră a lui $7^{8^8} \pmod{10}$ este suf să aff $8^8 \pmod 4 \equiv 0 \pmod 4$

Deci, $8^8 \pmod 4 \equiv 0 \pmod 4 \Rightarrow 7^{8^8} \equiv 1 \pmod{10}$

$\Rightarrow 7^{8^8} = 10k+1$

$7^{7^{8^8}} \pmod{11} = 7^{10k+1} \pmod{11} = (7^{10})^k \cdot 7 \pmod{11}$

$\equiv 7 \pmod{11}$