Consultație

3 Feb 2024

G ciclic $\iff \exists\, g \in G \quad G = \langle g \rangle$

$$\downarrow$$

$$|\langle g \rangle| = o(g)$$

$$\Updownarrow$$

$$\exists\, g \in G \quad o(g) = \underset{48}{|G|}$$

De exemplu pt $\mathbb{Z}_4 \times \mathbb{Z}_{12}$

$$\text{ord}((a, b)) = 2^{\max\{\alpha, \beta\}}\, 3^{\gamma}$$

$= 1$

$= 2$

$= 3$

$= 4$

$= 6$

$= 12$

Morfisme

G grup $\quad (G, +)$

$f : \mathbb{Z} \to G$ morfism de gr, $\quad f(x+y) = f(x) + f(y)$

$f(1) = a$

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

...

$f(n) = n a \qquad \forall n \in \mathbb{N}$

Inducție

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

$f(0) = 0$

$a \in G$

$f(n) = n \cdot a$

ex 1

Câte morfisme de grupuri sunt

$f : \mathbb{Z} \to \mathbb{Z}_9 \times \mathbb{Z}_{12}$

$\Updownarrow$

el $\quad a \in \mathbb{Z}_9 \times \mathbb{Z}_{12}$

$|\mathbb{Z}_9 \times \mathbb{Z}_{12}| = 9 \cdot 12$

ex 2

$f : \mathbb{Z}_{36} \to G$ $\qquad \boxed{\pi(i) = \hat{i}}$

$\mathbb{Z} \xrightarrow{\pi} \mathbb{Z}_{36} \xrightarrow{f}$

$f \pi : \mathbb{Z} \to G$ morf de gr

$\Rightarrow \exists\, a \in G \qquad (f \circ \pi)(n) = n a$

$f(\hat{n}) = n a$

$\underline{0} = f(\hat{0}) = f(\widehat{36}) = 36 \cdot a$

Am nevoie de el. $a \in G$ cu $36 a = 0$

$\iff \text{ord}(a) \mid 36$

morfismele de grupuri $f : \mathbb{Z}_{36} \to G$ sunt în bijecție cu el $a \in G$ cu $\text{ord}(a) = 36$

$f : \mathbb{Z}_n \to G \Rightarrow$ el $a \in G$ cu $\text{ord}(a) \mid n$

Generarea mulțimilor

ex 2

$\mathbb{Z}_{12} \times \mathbb{Z}_{15}$

generator

$\langle (\hat{3}, \bar{2}), (\hat{1}, \bar{4}) \rangle$

$\|$

$\{ i \cdot (\hat{3}, \bar{2}) + j (\hat{1}, \bar{4}) \mid i, j \in \mathbb{Z} \}$

$= \{ (\widehat{3i + j}, \overline{2i + 4j}) \}$

$\forall n, m \in \mathbb{Z}, \exists i, j \in \mathbb{Z}$ a.î. $3i + j \equiv n \pmod{12}$

$2i + 4j \equiv m \pmod{15}$

Putem prin inducție

- un n. divide un alt număr
- fără polinoame
- fără $\mathbb{Z}$ și $K[x]$

Permutări

$\sigma \in S_n, \quad \sigma^n = ?$

$\sigma = \sigma_1 \cdot \ldots \sigma_r,$ cicluri disjuncte

$\text{ord}(\sigma) = [\underbrace{\text{ord}(\sigma_1)}_{\substack{= \text{lungimea} \\ \text{ciclului } \sigma_1}}, \ldots, \text{ord}(\sigma_r)] \overset{\text{not}}{=} t$

$\sigma^t = e$ (permutarea identică)

$n = q \cdot t + r$

$(\sigma)^{qt+r} = (\sigma^t)^q \cdot \sigma^r = \sigma^r$

$\sigma^r = \sigma_1^r \cdot \sigma_2^r \cdot \ldots \cdot \sigma_r^r$

exc

$\sigma \in S_2$

$$\sigma = \underbrace{(1\ 7\ 5\ 10)}_{\sigma_1}\ \underbrace{(2\ 6)}_{\sigma_2}\ \underbrace{(3\ 9\ 12)}_{\sigma_3}\ \underbrace{(4\ 12)}_{\sigma_4}\ (8)$$

$$\text{ord}(\sigma) = [4, 2, 3, 2] = 12$$

$$\sigma^{12} = e$$

$$\sigma^{1000} = ?$$

$1000 : 12 = 83 + 4$

6

$$\sigma^{1000} = \sigma^{12 \cdot 83 + 4}$$
$$= (\sigma^{12})^{83} \cdot \sigma^4$$
$$= \sigma^4$$

$$\sigma^4 = \underset{\overset{\shortparallel}{e}}{\sigma_1^4} \cdot \underset{\overset{\shortparallel}{e}}{\sigma_2^4} \cdot \sigma_3^4 \cdot \underset{\overset{\shortparallel}{e}}{\sigma_4^4}$$

$$= \sigma_3^4 = \sigma_3^3 \cdot \sigma_3$$
$$= \sigma_3$$

$$\sigma^4 = (3\ 9\ 12)$$

exc

Fie $\sigma = (1, 5, 3) \in S_5$

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

$\sigma^2(1) = \sigma(\sigma(1)) = \sigma(5)$ compunere de funcții ex

$\sigma = (1, 2, 3, 4) \in S_4$, $\sigma^2 = ?$

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

ex

$$z^{10} = \sigma$$

Signatura

$$\begin{matrix} \varepsilon(z^{10}) & = & \varepsilon(\sigma) \\ \parallel & & \parallel \\ 1 & = & -1 \end{matrix} \Rightarrow \text{nu există}$$

ex

$$z^2 = \sigma$$

$$z = z_1 \cdot \ldots \cdot z_r$$

$$z^2 = z_1^2 \cdot \ldots \cdot z_r^2 = \sigma = \ldots\ldots$$

Dacă z_i are lungime impară $\Rightarrow$ z_i^2 are aceeași lungime

pară $\Rightarrow$ z_i^2 este produs de 2 cicluri de lungime $\frac{\ell}{2}$

Corpuri

$A = \dfrac{\mathbb{Z}_2[x]}{(x^3+x+\hat{1})}$ corp cu 8 elemente

$f \in \mathbb{Z}_2[x]$

$f = (x^3+x+\hat{1}) \cdot Cât + ax^2+bx+c \qquad a,b,c \in \mathbb{Z}_2$

$\hat{f} = \widehat{ax^2+bx+c}$

$\dfrac{\mathbb{Z}_2[x]}{(x^3+x+\hat{1})} = \{ \widehat{ax^2+bx+c} \mid a,b,c \in \mathbb{Z}_2 \}$

$a \in \{0,1\}$, $b \in \{0,1\}$, $c \in \{0,1\}$ $\Rightarrow$ 8 el.

$\widehat{ax^2+bx\,c+c} = \widehat{\alpha x^2+\beta x+\gamma}$

$\Updownarrow$

$a=\alpha, \quad b=\beta, \quad c=\gamma$

exc posibil

Fie $\widehat{x^2+x} \in \dfrac{\mathbb{Z}_2[x]}{(x^3+x+\hat{1})}$

Arătați că $\widehat{x^2+x}$ inversabil

Caut un $ax^2+bx+c \in A$ a.î.

$\widehat{ax^2+bx+c} \cdot \widehat{x^2+x} = 1$

$ax^4+ax^3+bx^3+bx^2+cx^2+cx$

$\widehat{ax^4+(a+b)x^3+(b+c)x^2+} \; cx = \hat{1}$

$$\begin{array}{l|l} ax^4 + (a+b)x^3 + (b+c)x^2 + cx & x^3 + x + 1 \\ \hline ax^4 \qquad\qquad\qquad\qquad + ax^2 \qquad + ax & ax + (a+b) \\ \hline / \quad + (a+b)x^3 + (a+b+c)x^2 + (a+c)x & \\ \quad (a+b)x^3 + \qquad\qquad (a+b)x + a+b & \\ \hline \quad / \quad (a+b+c)x^2 + (b+c)x + a+b = 1 & \end{array}$$

$$(a+b+c)\,x^2 + (b+c)x + a+b = 1$$

$$\begin{cases} a+b+c = 0 & \Rightarrow a = 0 \\ b+c = 0 & \Rightarrow b = 1 \\ a+b = 1 & \Rightarrow c = 1 \end{cases}$$

Inversul $u^{-1} = \widehat{x+1}$

Divisori dello zero

R comm

$\Downarrow$

a divisore dello zero

dato $\exists\, b \in R \setminus \{0\}$ t.c. $\underset{\neq 0}{a} \cdot \underset{\neq 0}{b} = 0$

es

Sia $A = \dfrac{\mathbb{Z}_2[x]}{(x^2+1)} = \{ \widehat{ax+b} \mid a, b \in \mathbb{Z}_2 \}$

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

$$\Downarrow$$

$$\underset{0}{\widehat{x^2 + 1}} = \widehat{x + 1}^{\,2}$$

es

$$\frac{\mathbb{R}[x]}{(x^2 - 3x + 2)} = \{ \widehat{ax+b} \mid a, b \in \mathbb{R} \}$$

$$\widehat{x^2 - 3x + 2} = 0$$

$$\underset{\neq 0}{\widehat{x-1}} \cdot \underset{\neq 0}{\widehat{x-2}}$$

ex

$$\frac{\mathbb{C}[x]}{(x^2+x+1)}$$ are divizori ai lui zero

ex

$$\frac{\mathbb{R}[x]}{(x^2+x+1)}$$ corp $\Rightarrow$ nu are divizori ai lui zero

ex

$$A = \{ d \mid d \in \mathbb{N},\ d \mid 24,\ d \neq 1,\ d \neq 24 \}$$

$$B = \mathcal{P}(\{1, 2, 3\}) \setminus \{ \emptyset, \{1, 2, 3\} \}$$

divizibilitatea

$(A, \mid)$ ordonată

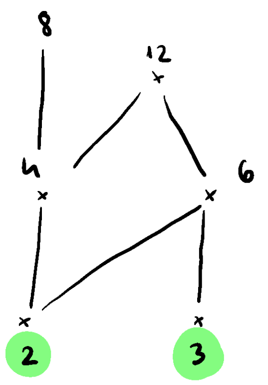
$(B, \subset)$ ordonată

$$24 = 2^3 \cdot 3 = 2^{\alpha} \cdot 3^{\beta}$$

$0 \leq \alpha \leq 3$

$0 \leq \beta \leq 1$

$$A = \{2, 3, 4, 6, 8, 12\}$$



← el. minimale

Diagrama mulțimii A

Mulțime ordonată

$(A, |) \neq \emptyset$

Axiome

1) $a \mid a$ (reflexivă)

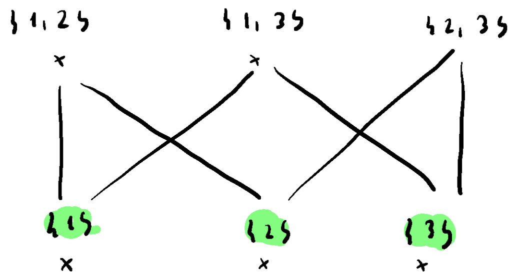
2) $a \mid b,\ b \mid c \Rightarrow a \mid c$ (tranzitivă)

3) $a \mid b,\ b \mid a \Rightarrow a = b$ (asimetrică)

$B =$

părților lui

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



$\rightarrow$ el. minimale

$(X, \subset)$ mulțime ord

$a \in X$ s.n. element minimal

dacă

$$\left.\begin{array}{l} x \leq a \\ x \in X \end{array}\right\} \Rightarrow x = a$$

$f : A \longrightarrow B$ izo pe mulțimi ordonate

$a \in A$ el minimal din A

$$\Updownarrow$$

$f(a) \in B$ el minimal în B

$\Rightarrow$ A și B nu sunt izomorfe

exc

$f : A \to B$ izo morf de gr

$a \in A \Rightarrow \underset{\text{în } B}{\text{ord}(f(a))} = \underset{\text{în } A}{\text{ord}(a)}$

Fie $n \in \mathbb{N}^*$

$$a^n = 1 \overset{f \text{ inj}}{\Leftrightarrow} f(a^n) = f(1)$$

$$\Leftrightarrow f(a)^n = 1$$

Sistem complet de repr.

Fie multimea A

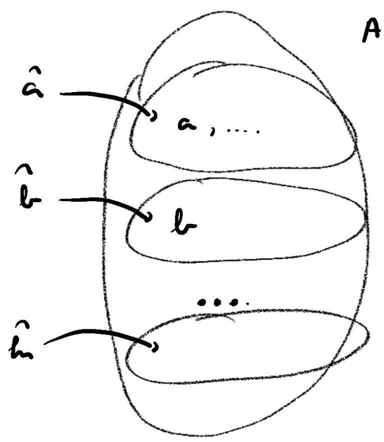
$\sim$ rel de echiv pe A

$$\begin{cases} a \sim a \\ a \sim b \Rightarrow b \sim a \\ a \sim b,\ b \sim c \Rightarrow a \sim c \end{cases}$$

$A/_\sim$ multimea factor

$a \in A$ clasa de echiv a lui a

$$\hat{a} \overset{def}{=} \{ x \in A \mid a \sim x \}$$



$$\hat{a} = \hat{b} \quad \text{sau} \quad \hat{a} \cap \hat{b} = \emptyset$$

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

$$\hat{a} = \hat{b} \iff \hat{a} \cap \hat{b} = \emptyset$$

ex

$\mathbb{C}, \sim$

$x \sim y \iff x - y \in \mathbb{R}$

S.C.R. = ?

rel de echiv

1) $x \sim x \iff \underbrace{x - x}_{=0} \in \mathbb{R}$ Adev

2) $x \sim y \Rightarrow x - y \in \mathbb{R} \Rightarrow -(y - x) \in \mathbb{R}$

$y - x \in \mathbb{R} \Rightarrow y \sim x$

3) $x \sim y,\ y \sim z \Rightarrow \begin{cases} x - y \in \mathbb{R} \\ y - z \in \mathbb{R} \end{cases}$ (+)

$x - z \in \mathbb{R} \Rightarrow x \sim z$

Dacă $z \in \mathbb{C}$

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

$\Updownarrow$

$z - x \in \mathbb{R}$

sau

$x - z = a \in \mathbb{R}$

$x = z + a, \quad a \in \mathbb{R}$

$\hat{z} = \{ z + a \mid a \in \mathbb{R} \}$

$$\hat{i} = \{ i + a \mid a \in \mathbb{R} \} = \widehat{1+i} = \widehat{7+i}$$
$$= \{ a + i \mid a \in \mathbb{R} \}$$

$$\widehat{1+2i} = \{ a + 1 + 2i \mid a \in \mathbb{R} \}$$
$$= \{ b + 2i \mid b \in \mathbb{R} \}$$

Fie $z = \alpha + \beta i, \quad \alpha, \beta \in \mathbb{R}$

$$\hat{z} = \{ c + \beta i \mid c \in \mathbb{R} \}$$

Un S.C.R. pt. rel. $\sim$ este

$$\{ \beta i \mid \beta \in \mathbb{R} \}$$

$$f : \mathbb{R} \to \mathbb{C}/\sim$$
$$f(\beta) = \widehat{\beta i}$$
f bijectivă

exc

$\mathbb{Q}, \sim$

$$x \sim y \iff x - y \in \mathbb{Z}$$

S.C.R. $[0, 1) \cap \mathbb{Q}$

$$f : [0, 1) \to \mathbb{Q}/\sim$$
$$f(a) = \hat{a}$$
$$\varphi(\hat{a}) = \{ a \}$$

Subcorpuri

Ex

$$K = \{ a + b\sqrt{3} \mid a, b \in \mathbb{Q} \}$$

K subcorp al lui $\mathbb{R}$

$$\text{subcorp} \begin{cases} \text{subinel} \begin{cases} x, y \in K \Rightarrow x - y \in K \\ \qquad\qquad\quad\; x \cdot y \in K \\ 1 \in K \end{cases} \\ x \in K \setminus \{0\} \Rightarrow x^{-1} \in K \end{cases}$$

$$x \in K \setminus \{0\} \Rightarrow x^{-1} \in K$$

<u>Dem</u>

$$\left. \begin{array}{l} a + b\sqrt{3} = 0 \\ a, b \in \mathbb{Q} \end{array} \right\} \Rightarrow a = 0 \quad b = 0$$

$$b\sqrt{3} = -a$$

$$\sqrt{3} = -\frac{a}{b} \in \mathbb{Q}$$

$$\frac{1}{a + b\sqrt{3}} = \frac{a - b\sqrt{3}}{a^2 - 3b^2} = \frac{a}{a^2 - 3b^2} + \frac{-b}{a^2 - 3b^2}\sqrt{3} \in K$$

Morfismele de corpuri

$f : K \to K$, morfism

$$\begin{cases} f(x+y) = f(x) + f(y) \\ f(xy) = f(x) \cdot f(y) \\ f(1) = 1 \end{cases}$$

$$f(x_1 + \dots + x_n) = f(x_1) + \dots + f(x_n)$$

$x_1 = x_2 = \dots = x_n$

$$f(n) = n \cdot f(1) = n \quad \forall n \in \mathbb{N}^*$$

$$f(-n) = -f(n) = -n \quad \forall n \in \mathbb{N}^*$$

$$f(n) = n, \quad \forall n \in \mathbb{Z}$$

$$f(\underbrace{\tfrac{n}{m} + \tfrac{n}{m} + \dots + \tfrac{n}{m}}_{m \text{ ori}}) = m \, f\left(\tfrac{n}{m}\right)$$

$$\| $$

$$n$$

$$\Rightarrow f\left(\tfrac{n}{m}\right) = \tfrac{n}{m}$$

$$f(a) = a \quad \forall a \in \mathbb{Q}$$

$$f(a + b\sqrt{3}) = f(a) + f(b\sqrt{3})$$

$$= \underbrace{f(a)}_{=a} + \underbrace{f(b)}_{=b} \cdot f(\sqrt{3})$$

$$\sqrt{3}^2 = 3 \quad | \ f:$$

$$\overset{f}{\Rightarrow} \quad f(\sqrt{3}^2) = f(3)$$

$$f(\sqrt{3})^2 = 3 \quad \Rightarrow f(\sqrt{3}) \in (-\sqrt{3}, \sqrt{3})$$

Avem $f(\sqrt{3}) = \sqrt{3}$ sau $f(\sqrt{3}) = -\sqrt{3}$

Dacă $f(\sqrt{3}) = \sqrt{3}$ atunci $f(a + \sqrt{3}b) = a + b\sqrt{3}$

$f = Id$ morfism

Dacă $f(\sqrt{3}) = -\sqrt{3}$ atunci $f(a + b\sqrt{3}) = a - b\sqrt{3}$

Verificăm

$$\begin{cases} f(x+y) = f(x) + f(y) \\ f(xy) = f(x) \cdot f(y) \\ f(1) = 1 \end{cases}$$

exc

$$\frac{\mathbb{R}[x]}{(x^2-1)} \simeq \mathbb{R} \times \mathbb{R}$$

$$x^2 - 1 = (x-1)(x+1)$$

$I = (x-1)$ ideale în $\mathbb{R}[x]$

$J = (x+1)$

I, J comaximale $(I + J = \mathbb{R}[x])$

$\hat{\mathbb{I}}$

$\exists\, a \in I \,,\ b \in J \qquad a + b = 1$

$\mathbb{R} \ni x$

$(x) = \{ r x \mid r \in \mathbb{R} \}$

$$\underbrace{-\tfrac{1}{2}(x-1)}_{\in I} + \underbrace{\tfrac{1}{2}(x+1)}_{\in J} = 1$$

L.C.R $\Rightarrow \quad I \cap J = I \cdot J = (x-1)\cdot(x+1) = (x^2-1)$

m;

$$\frac{\mathbb{R}[x]}{I \cap J} \simeq \frac{\mathbb{R}[x]}{I} \times \frac{\mathbb{R}[x]}{J}$$

$$\frac{\mathbb{R}[x]}{x^2-1} \simeq \frac{\mathbb{R}[x]}{x-1} \times \frac{\mathbb{R}[x]}{x+1} = \mathbb{R} \times \mathbb{R}$$

$$\boxed{\frac{A[x]}{(x-a)} \simeq A}$$

nc

$$\frac{\mathbb{Z}[x]}{(x^2-1)} \not\cong \mathbb{Z} \times \mathbb{Z}$$

$$\shortparallel$$

$$\{ \widehat{ax+b} \mid a, b \in \mathbb{Z} \}$$

mc

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 5 & 9 & 6 & 3 & 2 & 7 & 4 & 10 & 1 & 8 & 12 & 11 \end{pmatrix}$$

cicluri $= (1\ 5\ 2\ 9)\,(3\ 6\ 7\ 4)\,(8\ 10)\,(11\ 12)$

transpoziții $= \underbrace{(1\ 5)\,(5\ 2)}_{(5,\,2,\,1)}\,\underbrace{(2\ 9)\,(3\ 6)}_{(2\ 3\ 9)(2\ 3\ 6)}\,\underbrace{(6\ 7)\,(7\ 4)}_{(7\ 4\ 6)}\,\underbrace{(8\ 10)\,(11\ 12)}_{(8,\,11,\,10)\ (8,\,11,\,12)}$

$(i\ j)\,(i\ k) = (i\ k\ j)$

$(i\ j)\,(k\ l) = (i\ j\ k)\,(i\ k\ l)$

$(m, n) = 1$

$\mathbb{Z}_m \times \mathbb{Z}_n = \mathbb{Z}_{m \cdot n}$