Examen Seria 14

SAI

09.06.2023

② $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 4 & 6 & 5 & 2 & 1 \end{pmatrix} \in S_6$,

a)

- prod. de cicli disjuncți: $\sigma = (1\ 3\ 6)(2\ 4\ 5)$

- prod. de transpoziții: $\sigma = (1\ 3)(3\ 6)(2\ 4)(4\ 5)$

$ord(\sigma) = cmmmc(3, 3) = 3$

$\varepsilon(\sigma) = (-1)^4 = 1$

$$\sigma^{-2023} = (\sigma^{2023})^{-1} \underset{2023 = 3\cdot 674 + 1}{=\!=\!=} (\sigma^{3\cdot 674+1})^{-1} = ((\sigma^3)^{674}\cdot\sigma^1)^{-1} =$$

$$\underset{ord(\sigma)=3}{=\!=\!=} ((id)^{674}\cdot\sigma)^{-1} = (\sigma)^{-1} = ((1\,3\,6)(2\,4\,5))^{-1} =$$

$$= (1\,3\,6)^{-1}(2\,4\,5)^{-1} = (1\,6\,3)(2\,5\,4)$$

b) $\tau \in S_6$ a.î. $\tau^2 = \sigma$

τ a.î. $\tau^2 = (1\,3\,6)(2\,4\,5)$

Deoarece un ciclu de lungime impară ridicat la pătrat este egal cu un ciclu de aceeași lungime, iar un ciclu de lungime pară ridicat la pătrat este egal cu doi cicli disjuncți de lungime jumătate din lungimea ciclului inițial, având în vedere unicitatea scrierii ca produs de cicli disjuncți, rezultă că τ ~~se~~ poate scrie, ~~ca~~ ca produs de cicli disjuncți, fie ca un singur ciclu de lungime 6, fie ca doi cicli ~~de~~ disj. lungime 3.

I $\tau = (a_1\, a_2 \dots a_6) \Rightarrow \tau^2 = (a_1\, a_3\, a_5)(a_2\, a_4\, a_6) =$

$= (1\,3\,6)(2\,4\,5)$

$\xRightarrow{\text{unicitatea scrierii ca prod. de c. dij.}}$ $\begin{cases} \cancel{(a_1\, a_3\, a_5) = (1\,3\,6)} \\ \cancel{(a_2\, a_4\, a_6) = (2\,4\,5)} \end{cases}$

$\Rightarrow \tau \in \{(1\ 2\ 3\ 4\ 6\ 5), (1\ 4\ 3\ 5\ 6\ 2), (1\ 5\ 3\ 2\ 6\ 4)\}$

II $\quad \tau = (a_1\ a_2\ a_3)(a_4\ a_5\ a_6) \Rightarrow \tau^2 = (a_1\ a_3\ a_2)(a_4\ a_6\ a_5)$

$= (1\ 3\ 6)(2\ 4\ 5)$

$\Rightarrow \tau \in \{(1\ 6\ 3)(2\ 5\ 4)\}$

~~Din ridicarea la pătrat a acestor permutări, obținem (163)(254). Mai există posibilitatea de a înmulți aceste permutări cu 3 un produs disjunct de cicli disjuncți de ordin 2 (disjuncți oricare doi, dar și disjuncți față de permutările deja obținute~~

c) Este $\mathbb{Z}_3 \times \mathbb{Z}_3$ izomorf cu un subgrup al lui S_6? Dacă da, scrieți explicit un astfel de izomorfism.

Da!

Considerăm subgrupul $H \leq S_6$, $H = \langle (1\ 2\ 3), (4\ 5\ 6) \rangle =$

$= \{ id, (1\ 2\ 3), (1\ 3\ 2), (4\ 5\ 6), (4\ 6\ 5), (1\ 2\ 3)(4\ 5\ 6), (1\ 3\ 2)(4\ 5\ 6), (1\ 2\ 3)(4\ 6\ 5), (1\ 3\ 2)(4\ 6\ 5) \}$

$\mathbb{Z}_3 \times \mathbb{Z}_3$

$\oplus$	00	01	02	10	11	12	20	21	22
00	00	01	02	10	11	12	20	21	22
01	01	02	00	11	12	10	21	22	20
02	02	00	01	12	10	11	22	20	21
10	10	11	12	20	21	22	00	01	02
11	11	12	10	21	22	20	01	02	00
12	12	10	11	22	20	21	02	00	01
20	20	21	22	00	01	02	10	11	12
21	21	22	20	01	02	00	11	12	10
22	22	20							

Scriem și table de înmulțire în H

$\circledast$	id	(123)	(132)	(456)	(456)(123)	(456)(132)	(465)	(465)(123)	(465)(132)
$\vdots$									

scriem eventual tabelul

Deoarece tablele de compunere coincid după renotarea $f: \mathbb{Z}_3 \times \mathbb{Z}_3 \to \langle (123), (456) \rangle$

$f(00) = id \quad f(123) = 01 \quad f(456) = 10$

$f((123)(456)) = 11 \quad f(132) = 02 \quad f(465) = 20$

$f(456)(132) = 12 \quad f(465)(123) = 21$

$f(465)(132) = 22$

Deducem că ~~f este~~ cele două grupuri sunt izomorfe, cu izomorfismul dat de f.

Aici a fost mai mult eve de idee, am observat că ~~$\mathbb{Z}_3 \times \mathbb{Z}_3$ este~~ un grup $G = \langle x, y \rangle$ cu $xy = yx$ $x^3 = y^3 = 1$ (generat de x și y)

și $\langle x \rangle \cap \langle y \rangle = 1$ (intersecție trivială) trebuie să fie izomorf cu $\mathbb{Z}_3 \times \mathbb{Z}_3$

În $\mathbb{Z}_3 \times \mathbb{Z}_3$, putem lua $x = 10$ $y = 01$

În S_6, luăm $\langle x, y \rangle = H$ cu $x = (123)$ și $y = (456)$

Am observat că dacă duc pe 10 și 01 care sunt generatori lui $\mathbb{Z}_3 \times \mathbb{Z}_3$ în (123) și (456) (care au și aceleași ordin, adică 3) atunci

$$\mathbb{Z}_3 \times \mathbb{Z}_3 \simeq \langle (123), (456) \rangle = H$$

unde ~~te~~ orice element din $\mathbb{Z}_3 \times \mathbb{Z}_3$ se duce în H conform legii de morfism, știind că e o comb. de (10) și (01)

Sub. III $G = \mathbb{Z}_9 \times \mathbb{Z}_{18}$

a) $\text{ord}(\hat{4}, \bar{3})$ ...

$\frac{18}{\gcd(3,18)}) = ($ ... lcm

$\text{ord}(\hat{3}, \bar{5}) = \text{lcm}($ ...

$= \text{lcm}(\frac{9}{3},$ ...

b) $(\hat{4}, \bar{3})$ ...

Sol. I $\langle (\hat{3}, \bar{5}) \rangle =$ ...

$(\hat{3}, \bar{2}), (\hat{6},$ ...

$(\hat{3}, \overline{14}), (\hat{6}, \bar{1})$ ...

$(\hat{3}, \bar{8}), (\hat{6},$ ...

$(\hat{4}, \bar{3}) \notin \langle (\hat{3}$ ...

Analog $(\hat{3}, \bar{5})$ ...

Sol. II Obs ...

$\hat{a} \in \{\hat{0}, \hat{3}, \hat{6}\}$ ...

Dc. $(\hat{a}, \bar{b}) \in \langle$ ...

Dar $\bar{5} \notin \{$ ...

c) $G =$ ...

Deoarece ...

$(1,0), (0,1) \in$ ...

$(\hat{4}, \bar{3})$ ...

$6 \cdot (\hat{4}, \bar{3}) = ($ ...

(465) (465)(123) (465)(132)

d după

65) = 20

= 20

22

izomorfe, cu izomorfismul

$xy = yx \quad x^3 = y^3 = 1$

să fie izomorf cu $\mathbb{Z}_3 \times \mathbb{Z}_3$

$y = (456)$

t generatorii lui $\mathbb{Z}_3 \times \mathbb{Z}_3$

că 3) atunci

$(456)\rangle = H$

$\mathbb{Z}_3$ se duce în

amb. de (10) și (01)

Sub. III $\quad G = \mathbb{Z}_9 \times \mathbb{Z}_{18}$

a) $\operatorname{ord}(\hat{4}, \bar{3}) \overset{\text{cmmmc}}{=} \operatorname{lcm}(\operatorname{ord}(\hat{4}), \operatorname{ord}(\bar{3})) = \operatorname{lcm}\left(\frac{9}{\gcd(4,9)}, \frac{18}{\gcd(3,18)}\right) = \operatorname{lcm}\left(\frac{9}{1}, \frac{18}{3}\right) = \operatorname{lcm}(9, 6) = 18$

$\operatorname{ord}(\hat{3}, \bar{5}) = \operatorname{lcm}(\operatorname{ord}(\hat{3}), \operatorname{ord}(\bar{5})) = \operatorname{lcm}\left(\frac{9}{\gcd(9,3)}, \frac{18}{\gcd(5,18)}\right)$
$= \operatorname{lcm}\left(\frac{9}{3}, \frac{18}{1}\right) = \operatorname{lcm}(3, 18) = 18$

b) $(\hat{4}, \bar{3}) \in \langle (\hat{3}, \bar{5}) \rangle$?

Sol. I $\langle (\hat{3}, \bar{5}) \rangle = \{ (\hat{0}, \bar{0}), (\hat{3}, \bar{5}), (\hat{6}, \overline{10}), (\hat{0}, \overline{15}), (\hat{3}, \bar{2}), (\hat{6}, \bar{7}), (\hat{0}, \overline{12}), (\hat{3}, \overline{17}), (\hat{6}, \bar{4}), (\hat{0}, \bar{9}), (\hat{3}, \overline{14}), (\hat{6}, \bar{1}), (\hat{0}, \bar{6}), (\hat{3}, \overline{11}), (\hat{6}, \overline{16}), (\hat{0}, \bar{3}), (\hat{3}, \bar{8}), (\hat{6}, \overline{13}) \}$

$(\hat{4}, \bar{3}) \notin \langle (\hat{3}, \bar{5}) \rangle$?

Analog $(\hat{3}, \bar{5}) \notin \langle (\hat{4}, \bar{3}) \rangle$.

Sol. II Obs. că dacă $(\hat{a}, \bar{b}) \in \langle (\hat{3}, \bar{5}) \rangle$, atunci $\hat{a} \in \{ \hat{0}, \hat{3}, \hat{6} \}$. Dar $\hat{4} \notin \{ \hat{0}, \hat{3}, \hat{6} \}$. Deci $(\hat{4}, \bar{3}) \notin \langle (\hat{3}, \bar{5}) \rangle$.

Dc. $(\hat{a}, \bar{b}) \in \langle (\hat{4}, \bar{3}) \rangle$, atunci $\bar{b} \in \{ \bar{0}, \bar{3}, \bar{6}, \bar{9}, \overline{12}, \overline{15} \}$.
Dar $\bar{5} \notin \{ \dots \} \Rightarrow (\hat{3}, \bar{5}) \notin \langle (\hat{4}, \bar{3}) \rangle$.

c) $G = \langle (\hat{4}, \bar{3}), (\hat{3}, \bar{5}) \rangle$? $\quad H := \langle (\hat{4}, \bar{3}), (\hat{3}, \bar{5}) \rangle$

Deoarece $G = \langle (\hat{0}, \bar{1}), (\hat{1}, \bar{0}) \rangle$, e suficient să arătăm că $(1,0), (0,1) \in \langle (\hat{4}, \bar{3}), (\hat{3}, \bar{5}) \rangle$ pentru ca $G = \langle (\hat{4}, \bar{3}), (\hat{3}, \bar{5}) \rangle$.

$(\hat{4}, \bar{3}) - (\hat{3}, \bar{5}) = (\hat{1}, \overline{16}) \in H$

$6 \cdot (\hat{4}, \bar{3}) = (\hat{6}, \bar{0}) \in H$; $\quad 3 \cdot (\hat{3}, \bar{5}) = (\hat{0}, \overline{15}) \in H$

$2\cdot(\hat 0,\overline{15}) = (\hat 0,\overline{12}) \in H$

$(\hat 0,\overline{15}) = (\hat 0,\overline{-3}) \in H$

$(\hat 0,\overline{12}) - (\hat 0,\overline{-3}) = (\hat 0,\overline{9}) \in H$

$(\hat 0,\overline{9}) - (0,\overline{-3}) = (\hat 0,\overline{6}) \in H$

$\hat 4^{-1} = \widehat{-2} \qquad (\hat 4\cdot\widehat{-2} = \widehat{-8} = \hat 1)$

$-2\cdot(\hat 4,\overline 3) = (\hat 1,\overline{-6}) = (\hat 1,\overline{12}) \in H$

$(\hat 1,\overline{12}) - (\hat 0,\overline{12}) = \boxed{(\hat 1,\overline 0)\in H}$

$\cancel{3\cdot(\hat 3,\overline 5) = (\hat 0, 1}$

$6\cdot(\hat 4,\overline 3) = (\hat 6,\overline 0) \in H$

$2\cdot(\hat 6,\overline 0) = (\hat{12},\overline 0) \in H$, $\cancel{3\cdot(\hat 6,\overline 0) =}$

$\overline 5^{-1} = \overline{-7} \qquad (-7\cdot 5 + 2\cdot 18 = 1)$

$-7\cdot(\hat 3,\overline 5) = (\hat 6,\overline 1) \in H$

$(\hat 6,\overline 1) - (\hat 6,\overline 0)\ \cancel{\in H}$
$= \boxed{(\hat 0,\overline 1) \in H}$

$\Rightarrow \quad G = H = \langle(\hat 3,\overline 5),(\hat 4,\overline 3)\rangle \Rightarrow$ DA, $(\hat 3,\overline 5),(\hat 4,\overline 3)$
Sistem de generatori pt. G

d) $G/\langle(\hat 4,\overline 3)\rangle$ ciclic?

$f: G \to G/\langle(\hat 4,\overline 3)\rangle$, $(x,y)\mapsto \widetilde{(x,y)}$ morfism de grupuri $f((x,y)) = \widetilde{(\hat x,\overline y)}$

Fie $g \in G/\langle(\hat 4,\overline 3)\rangle$. Atunci $g = \widetilde{(\hat x,\overline y)}$ unde $(\hat x,\overline y)\in \underbrace{\mathbb{Z}_9\times\mathbb{Z}_{18}}_{=G}$

Cum $G = \langle(\hat 3,\overline 5),(\hat 4,\overline 3)\rangle$, $\exists m,n\in\mathbb{Z}$ a.î.

$(\hat x,\overline y) = m(\hat 3,\overline 5) + n(\hat 4,\overline 3)$

$\Rightarrow f((\hat x,\overline y)) = f(m(\hat 3,\overline 5) + n(\hat 4,\overline 3)) \underset{\text{morfism}}{=} m\cdot\widetilde{(\hat 3,\overline 5)} + n\cdot\widetilde{(\hat 4,\overline 3)}$

$\underset{}{\overset{\text{mod }(\hat 4,\overline 3)}{=}} m\cdot\widetilde{(\hat 3,\overline 5)} + n\cdot\widetilde{(\hat 0,\overline 0)} = m\cdot\widetilde{(\hat 3,\overline 5)}$

$\Rightarrow \quad g = \widetilde{(\hat x,\overline y)} = m\cdot\widetilde{(\hat 3,\overline 5)}$

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

...m de generatori pt. G

$\widehat{(x,y)} = (\hat{x},\bar{y})$

unde $(\hat{x},\bar{y}) \in \mathbb{Z}_9 \times \mathbb{Z}_{15}$ = G

...5) $+ n\cdot(\hat{1},\bar{3})$

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

Cum g a fost ales arbitrar în $G/\langle(\hat{1},\bar{3})\rangle$, rezultă că $G/\langle(\hat{1},\bar{3})\rangle$ ~~ciclic~~

și $G/\langle(\hat{1},\bar{3})\rangle = \langle \widehat{(\hat{3},\bar{5})} \rangle$ și deci ciclic.

4) $I \subseteq \mathbb{Z}[X]$ — polin. cu coef. întregi

I — polinoamele care au termenul liber un multiplu de 6

a) ex. de polinom din I de grad 9

Dem. că $I \trianglelefteq \mathbb{Z}[X]$ (I ideal al lui $\mathbb{Z}[X]$)

exemple: $X^9 + 6$; $X^9 + X + 12$

Def.: $I \trianglelefteq R$; I ideal al inelului R dacă:

(a) $I - I \subseteq I$ (I subgrup în R)

(b) $R \cdot I \subseteq I$

$\forall i, j \in I,\ i - j \in I$

$\forall r \in R,\ \forall i \in I,\ r \cdot i \in I$.

Fie $p(X), q(X) \in I$.

$\Rightarrow \begin{cases} p(X) = a_m X^m + a_{m-1} X^{m-1} + \ldots + a_1 X + a_0, \text{ unde } a_0 = 6c_0 \\ q(X) = b_m X^m + b_{m-1} X^{m-1} + \ldots + b_1 X + b_0, \text{ unde } b_0 = 6d_0 \end{cases}$

putem scrie orice două polinoame pornind cu termeni de aceeași putere maximă, egalând eventual niște coeficienți cu 0.

$\Rightarrow p(X) - q(X) = (a_m - b_m) X^m + (a_{m-1} - b_{m-1}) X^{m-1} + \ldots + (a_1 - b_1) X + (a_0 - b_0) =$

$= (a_m - b_m) X^m + \ldots + (a_1 - b_1) X + 6(c_0 - d_0)$

$\Rightarrow p(X) - q(X) \in I \Rightarrow$ (a) ✓

(b) Fie $p(X) \in I$. Fie $f(X) \in \mathbb{Z}[X]$

$p(X) = a_n X^n + \dots + a_1 X + a_0$, $a_0 = 6 d_0$

$f(X) = b_m X^m + \dots + b_1 X + b_0$

$\Rightarrow p(X) f(X) = c_{n+m} X^{n+m} + c_{n+m-1} X^{n+m-1} + \dots + c_1 X + c_0$

unde $c_k = \sum_{\substack{0 \le i, j \le k \\ i+j=k}} a_i b_j \Rightarrow c_0 = a_0 b_0 = 6 d_0 b_0 \vdots 6$

termenul liber al prod. de polinoame e produsul termenilor liberi

$\Updownarrow$

$p(X) f(X) \in I$

$\Updownarrow$

(b) ✓

$\Rightarrow I$ ideal în $\mathbb{Z}[X]$

b) $U(\mathbb{Z}[X]) \cap I$.

Despre ideale : Fie $I \trianglelefteq R$ $(R, +, \cdot)$

$U(R)$ = elemente inversabile (în rap. cu înmulțirea din inel)

Dacă $1 \in I$, atunci conform (a) $(R \cdot I \subseteq I)$, $\forall r \in R$,

$r \cdot 1 = r \in I \Rightarrow I = R \Rightarrow$ Dacă $1 \in I$, $I = R$

Mai general, dacă $u \in U(R)$ și $u \in I$, atunci, dacă $r \in R$ arbitrar din inel, atunci $\underbrace{r \cdot u^{-1}}_{\in R} \cdot \underbrace{u}_{\in I} = \underbrace{r}_{\in I} \in I$. Deci $I = R$.

(B):

Deci dacă un ideal conține un element inversabil din inel, (în particular, pe 1_R) atunci idealul este egal cu tot inelul.

~~Cum~~

Deci, în general, idealele nu conțin elemente inversabile (căci dacă ar conține, ar fi egale cu tot inelul; echivalent, dacă un ideal nu e egal cu tot inelul, atunci el nu conține elemente inversabile.)

Idealul I nu e egal cu tot inelul $I \subseteq \mathbb{Z}[X]$, dar $I \neq \mathbb{Z}[X]$.

De ex.: Păi există polin. cu coef. întregi (din $\mathbb{Z}[X]$) care nu se în I (care n-au termenul liber divizibil cu 6).

Ex.: X^5+X+2, X^4+13, $X^{10}+2X^3+5X^7+61$

De aici rezultă că $U(\mathbb{Z}[X]) \cap I = \emptyset$.

c) $\mathbb{Z}[X]/I \simeq (\mathbb{Z}_6, +, \cdot)$

$(\mathbb{Z}[X]/I, +, \cdot)$

Elementele lui $\mathbb{Z}[X]/I$ sunt clase de polinoame $\widehat{f(X)}$ a.î. $\widehat{f(X)} = \widehat{g(X)}$ dacă și numai dacă $f(X) - g(X) \in I$. În particular,

$\widehat{f(X)} = \hat{0} \iff f(X) - 0 = f(X) \in I$.

scăderea din inel / adunarea cu inversul / operație de grup, NU înmulțirea (operație de monoid a inelului)

Obs. că $I = (X, 6)$ (idealul generat de X și 6) (vezi caiet tutoriat pentru detalii ideal generat)

„$\subseteq$" Într-adevăr, orice polinom cu termenul liber div. cu 6, $f(X) = a_m X^m + \ldots + a_1 X + 6 c_0$ se scrie ca

$$f(X) = X\underbrace{(a_m X^{m-1} + \ldots + a_2 X + a_1)}_{\in \mathbb{Z}[X]} + 6 \cdot \underbrace{c_0}_{\in \mathbb{Z}[X]}$$

„$\supseteq$" Și orice element din $(X, 6)$ e un polin. cu termenul liber div. cu 6

$$X \cdot g(X) + 6 \cdot f(X) = X \cdot (a_m X^m + \ldots + a_1 X + a_0) + 6(b_m X^m + b_{m-1} X^{m-1} + \ldots + b_1 X + b_0) =$$

$$= a_m X^{m+1} + (a_{m-1} + 6b_m) X^m + \ldots + (a_0 + 6b_1) X + \underbrace{6b_0}$$

Obs.: În general $R[X]/(X-a) \simeq R$ prin morfismul $\varphi: R[X] \to R$, $\varphi(f(X)) = f(a)$

Într-adevăr φ e morfism (evaluarea unui polinom e în general morfism)

$[X]$.

1) $\varphi(1_{R[X]}) = f(1_R) = 1_R$

$\shortparallel$
1_R

polinom ct. , nu se evaluează

2) $\varphi(f(X)+g(X)) = \varphi((a_n X^n + \ldots + a_1 X + a_0) + (b_n X^n + \ldots + b_1 X + b_0))$

$= \varphi((a_n+b_n)X^n + \ldots + (a_1+b_1)X + (a_0+b_0)) =$

$= (a_n+b_n)\,a^n + \ldots + (a_1+b_1)\,a + (a_0+b_0) =$

$= (a_n a^n + \ldots + a_1 \cdot a + a_0) + (b_n \cdot a^n + \ldots + b_1 a + b_0) =$

$= \varphi(a_n X^n + \ldots + a_1 X + a_0) + \varphi(b_n X^n + \ldots + b_1 X + b_0) =$

$= \varphi(f(X)) + \varphi(g(X))$

3) $\varphi(f(X)\cdot g(X)) = \varphi((a_n X^n + \ldots + a_1 X + a_0)\cdot(b_m X^m + \ldots + b_1 X + b_0))$

$= \varphi(c_{n+m} X^{n+m} + c_{n+m-1} X^{n+m-1} + \ldots + c_1 X + c_0)$

$= c_{n+m}\, a^{n+m} + \ldots + c_1 a + c_0 = (a_n a^n + \ldots + a_1 \cdot a + a_0)\cdot$

$\cdot(b_m a^m + \ldots + b_1 a + b_0) = \varphi(a_n X^n + \ldots + a_1 X + a_0)\cdot\varphi(b_m X^m + \ldots + b_1 X + b_0)$

$= \varphi(f(X))\cdot\varphi(g(X))$

Deci morfism. (evaluare în a trece prin adunare și înmulțire de polin.)

$\mathrm{Ker}\,\varphi = \{ f(X) \in R[X] \mid \varphi(f(X)) = f(a) = 0 \}$

Deci $f \in \mathrm{Ker}\,\varphi$ dacă $f(a) = 0$

Lemă: Dacă $f(X) \in R[X]$, $f(a) = 0$, atunci $X-a$ divide $f(X)$

Împart cu rest pe $f(X) \in \mathrm{Ker}\,\varphi$ la $X-a$

$\Rightarrow f(X) = (X-a)\,q(X) + r(X)$, $q(X), r(X) \in R[X]$

și grad $r(X) <$ grad $(X-a) = 1 \Rightarrow$ grad $r(X) \in \ldots$

$\Rightarrow r(X) = c$, $c \in R$

$f(X) = g(X) \cdot (X-a) + c$

Evaluăm în a: $f(a) = g(a) \cdot (a-a) + c$

$f(a) = 0 \Rightarrow 0 = g(a) \cdot 0 + c \Rightarrow c = 0$

$\Rightarrow f(X) = (X-a) g(X)$

Deci $(X-a)$ divide $f(X)$, deci $f(X) \in (X-a)$ (idealul generat de $X-a$)

$\Rightarrow \ker \varphi \subseteq (X-a)$

"$\supseteq$" Fie $g(X) \in (X-a) \Rightarrow \exists h(X) \in R[X]$ a.î.

$g(X) = h(X)(X-a) \Rightarrow g(a) = h(a)(a-a) = 0$

$\Rightarrow g(a) = 0 \Rightarrow g(X) \in \ker \varphi \Rightarrow (X-a) \subseteq \ker \varphi$

$\Rightarrow \ker \varphi = (X-a)$

$\operatorname{Im} \varphi = R$ deci $\forall r \in R$, $r = \varphi(r)$ (φ surj.)

r privit ca un polinom constant în $R[X]$

$\Rightarrow$ teorema fundam. de izomorfism pentru inele $\Rightarrow R[X]/(X-a) \simeq R$.

<u>Obs 2</u>: $\mathbb{Z}[X] / (n) \simeq \mathbb{Z}_n[X]$

$\varphi : \mathbb{Z}[X] \to \mathbb{Z}_n[X]$ $\quad \varphi(a_m X^m + \dots + a_1 X + a_0) =$

$= \hat{a}_m X^m + \dots + \hat{a}_1 X + \hat{a}_0$

clase modulo n

Se verifică că au loc 1), 2), 3)

deci φ e morfism de inele. $\ker \varphi = ?$

$\ker \varphi = \{ f(X) \in \mathbb{Z}[X] \mid \varphi(f(X)) = \hat{0} \}$

$= \{ a_m X^m + \dots + a_1 X + a_0 \in \mathbb{Z}[X] \mid \underbrace{\hat{a}_m X^m + \dots + \hat{a}_1 X + \hat{a}_0}_{= \hat{0}} \}$

$\hat{a}_m X^m + \dots + \hat{a}_1 X + \hat{a}_0 = \hat{0} \Leftrightarrow \begin{cases} \hat{a}_m = \hat{0} \\ \vdots \\ \hat{a}_1 = \hat{0} \\ \hat{a}_0 = \hat{0} \end{cases}$

$\Leftrightarrow \begin{cases} a_m \vdots 6 \\ \vdots \\ a_1 \vdots 6 \\ a_0 \vdots 6 \end{cases} \Leftrightarrow a_m X^m + \dots + a_1 X + a_0 = 6 c_m X^m + \dots + 6 c_1 X + 6 c_0$

$\Leftrightarrow a_n X^n + \ldots + a_0 X + a_0 = 6(c_n X^n + \ldots + c_1 X + c_0)$

$\Leftrightarrow a_n X^n + \ldots + a_0 \in (6)$ în $\mathbb{Z}[X]$

$\Leftrightarrow (6) = \ker \varphi$

φ surj: $(\hat{a}_n X^n + \ldots + \hat{a}_1 X + \hat{a}_0 = \varphi(a_n X^n + \ldots + a_1 X + a_0))$

$\Rightarrow$ TFI $\Rightarrow \mathbb{Z}[X]/(n) \simeq \mathbb{Z}_n[X]$

Obs. 3: TFI

Fie φ morfism de inele $\varphi: R \to R'$.

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

$\ker \varphi$ e întotdeauna ideal în R și

$\operatorname{Im} \varphi$ e întotdeauna subinel în R'

Revenim la rezolvare

Iau $\varphi: \mathbb{Z}[x] \longrightarrow \mathbb{Z}_6$

$\varphi(f(x)) = \widehat{f(0)}$ (mod 6)

$\varphi = \varphi_2 \circ \varphi_1$

$\varphi_1: \mathbb{Z}[X] \longrightarrow \mathbb{Z}$

~~$\mathbb{Z}[X]$~~ $\varphi_1(f(x)) = f(0)$ morfism din explicații

$\varphi_2: \mathbb{Z} \to \mathbb{Z}_6$

$\varphi_2(n) = \hat{n}$ morfism

φ compunere de morfisme deci morfism.

$\ker \varphi = ?$

Fie $f(x) \in \ker \varphi \Leftrightarrow \widehat{f(0)} = \hat{0} \Leftrightarrow \widehat{b_n \cdot 0^n + b_{n-1} \cdot 0^{n-1} + \ldots + b_1 \cdot 0 + b_0} = \hat{0} \Leftrightarrow \hat{b}_0 = \hat{0} \Leftrightarrow b_0 \vdots 6 \Leftrightarrow f \in I$

$\Rightarrow \ker \varphi = I$

φ surj: căci $\hat{n} = \varphi(n)$ $\Rightarrow$ TFI $\Rightarrow \mathbb{Z}[X]/I \simeq \mathbb{Z}_6$

$n \in \mathbb{Z}[x]$ pol. ct.

d) $Y \subseteq I$, Y mulțime infinită a.î. $\forall f(X) \in Y$, $f(X)$ polinom ired. în $\mathbb{Q}[X]$ de grad 9.

Aleg $Y = \{X^9 + 3kX + 6 \mid k \in \mathbb{Z}\}$

Clar Y infinită și pol. din Y de grad 9.

$\forall f(X) \in Y$, $f(X)$ monic, $3 \mid 3k$ și 6 iar $3^2 = 9 \nmid 6$. Conform Eisenstein, f ired. în $\mathbb{Q}[X]$.

Criteriul lui Eisenstein

Fie $f(X) \in \mathbb{Z}[X]$.

Dacă:

- $f(X)$ e monic (coef. dom. $= 1$)
- $\exists\, p$ prim a.î. p divide toți ceilalți coeficienți mai puțin al dominant și p^2 nu divide termenul liber

Atunci $f(X)$ e ireductibil în $\mathbb{Q}[X]$.

(11) $A = \{a_1, \dots, a_9\}$

$\mathcal{F} : A \to \mathbb{N}$

a) care e rel. de echiv pe $\mathcal{F}$?

$f \sim_1 g \iff \exists\, a \in A$ a.î. $f(a) = g(a)$

Nu e tranz., deci nu e rel. ech.

Fie $f \in \mathcal{F}$ a.î. $f(a_1) = \dots = f(a_8) = 0$, $f(a_9) = 1$.

$g \in \mathcal{F}$ a.î. $g(a_1) = 2$, $g(a_2) = \dots = g(a_9) = 1$

$h \in \mathcal{F}$ a.î. $h(a_i) = 2$ $\forall i = \overline{1,9}$

Atunci $f \sim_1 g$ ($f(a_9) = g(a_9) = 1$) și $g \sim_1 h$ ($g(a_1) = h(a_1) = 2$)

dar $f \not\sim_1 h$ ($h(a_i) = 2$ $\forall i$, iar $f(a_i) \in \{0, 1\}$ $\forall i$ $\Rightarrow \forall i$ $h(a_i) \neq f(a_i)$)

b) $f \sim_2 g \iff \mathrm{Im}(f) \cap \mathrm{Im}(g) \neq \emptyset$

$\sim_2$ nu e tranz.

Fie $f \in \mathcal{F}$, $f(a_i) = 0$ $\forall i$

$g \in \mathcal{F}$, $g(a_1) = 0$, $g(a_2) = \dots = g(a_9) = 1$

$h \in \mathcal{F}$, $h(a_i) = 1$ $\forall i$

$f \sim_2 g$ ($\mathrm{Im}(f) \cap \mathrm{Im}(g) = \{0\} \neq \emptyset$), $g \sim_2 h$ ($\mathrm{Im}\, g \cap \mathrm{Im}\, h = \{1\} \neq \emptyset$)

dar $f \not\sim_2 h$ ($\mathrm{Im}\, f \cap \mathrm{Im}\, h = \{0\} \cap \{1\} = \emptyset$).

$f \sim_3 g \iff \sum_{a\in A} f(a) = \sum_{a\in A} g(a)$

$\boxed{R}$ $f \sim_3 f$ $\forall f \in \mathcal{F}$ căci $\sum_{a\in A} f(a) = \sum_{a\in A} f(a)$

$\boxed{S}$ $f \sim_3 g \iff \sum_{a\in A} f(a) = \sum_{a\in A} g(a) \iff \sum_{a\in A} g(a) = \sum_{a\in A} f(a) \iff g \sim_3 f$

$\boxed{T}$ $f \sim_3 g,\ g \sim_3 h \Rightarrow \sum_{a\in A} f(a) = \sum_{a\in A} g(a)$ și $\sum_{a\in A} g(a) = \sum_{a\in A} h(a)$

$\Rightarrow \sum_{a\in A} f(a) = \sum_{a\in A} h(a) \iff f \sim_3 h$

b) sistem de repr. pentru rel. de ech. de la a) (i.e. $\sim_3$)

Aleg sistemul $\mathcal{S} = \{f_i\}_{i\in\mathbb{N}}$, unde $f_i : A \to \mathbb{N}$ ← așa definim f_i-urile

$f_i(a_1) = i$

$f_i(a_2) = \dots = f_i(a_9) = 0$

• Fie $g \in \mathcal{F}$. Atunci notăm $s := \sum_{a\in A} g(a)$

Luăm f_s și observăm că $\sum_{a\in A} f_s(a) = s + \underbrace{0 + \dots + 0}_{8\text{ ori}} = s$ $\Big|\Rightarrow$

$\Rightarrow g \sim f_s \Rightarrow \forall g \in \mathcal{F}\ \exists f_i \in \mathcal{S}$ a.î. $g \sim_3 f_i$

• Fie $f_i \neq f_s$, $f_i, f_j \in \mathcal{S} \Rightarrow i \neq j$

$\sum_{a\in A} f_i(a) = i$, $\sum_{a\in A} f_j(a) = j$ $\Big| \Rightarrow \sum_{a\in A} f_i(a) \neq \sum_{a\in A} f_j(a)$

$\Updownarrow$

$f_i \nsim_3 f_j$

$\Rightarrow \forall f_i, f_j \in \mathcal{S}$ cu $f_i \neq f_j$ avem că $f_i \nsim_3 f_j$

Din •, • $\Rightarrow$ $\mathcal{S}$ sistem de repr. pentru $\sim_3$.