Tutoriat 1 - Rezolvari
Funcții. Relații de echivalență. S.C.I.R.

Savu Ioan Daniel, Tender Laura-Maria

- 2 noiembrie 2020 -

Exercițiul 1

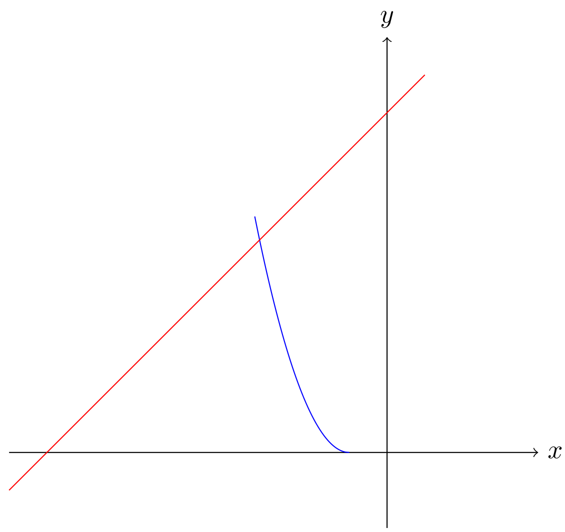
Fie f : $\mathbb{R}->\mathbb{R}$, $f(x) = \begin{cases} x^2+2x+m, x \leq -1 \\ mx-9, x > -1 \end{cases}$ cu m $\in \mathbb{R}$.

a) Realizați graficul funcției pentru m=1.
b) Determinați imaginea funției f în funcție de parametrul real m.
c) Găsiți valorile lui m pentru care funcția dată este:
  c.1 injectivă
  c.2 surjectivă
  c.3 bijectivă

Rezolvare:

a) Pentru m = 1, $f(x) = \begin{cases} x^2+2x+1, x \leq -1 \\ x-9, x > -1 \end{cases}$.

Vom studia cum se comporta funcția pe cele două ramuri: $f/_{(-\infty,-1]}$ și $f/_{(-1,\infty)}$.
Ramura superioară este de gradul al II-lea, graficul este o parabolă cu vârful în jos. Vom afla punctul de minim. Pentru ax^2+bx+c, vârful parabolei este $(-\frac{b}{2a}, -\frac{\Delta}{4a})$. Astfel obținem că punctul de minim este (-1, 0).
Ramura inferioară este liniară. $f/_{(-1,\infty)}$ este strict crescătoare. Fie $x, y \in (-1,\infty)$, $x < y$. Atunci f(x) = x - 9, f(y) = y - 9. f(x) < f(y) $\iff$ x - 9 < y - 9 $\iff$ x < y, ceea ce este adevărat. Cum $f_{/(-1,\infty)}$ este strict crescătoare minimul este atins pentru x = -1 în punctul (-1, -10).



b) Vom studia funcția similar subpunctului a) însă în funcție de parametrul real m.
Astfel, punctul de minim al primei ramuri este (-1, m-1). Iar $\lim_{x\to-\infty} f(x) = +\infty$. Deci Im$f_{(-\infty,-1]}$ este $[m-1,\,+\infty)$.
Vom studia monotonia funcției pentru $(-1,\,+\infty)$. Analog demonstrației de la subpunctul a), pentru $m > 0$ funcția este strict crescătoare.Pentru $m < 0$ funcția este strict descrescătoare. Pentru m = 0, $f/_{(-1,\,+\infty)}$ = -9, constantă.
Pentru $m > 0$, $\lim_{x\to\infty} f(x) = +\infty$. Pentru $m < 0$, $\lim_{x\to\infty} f(x) = -\infty$.
Astfel, dacă $m > 0$, Im$f_{(-1,\,+\infty)} = (-m-9,\,+\infty)$. Dacă $m < 0$, Im$f_{(-1,\,+\infty)}$ $= (-\infty,\,-m-9)$. Dacă m = 0, Im$f_{(-1,\,+\infty)}$ = -9.

În concluzie, Imf = $\begin{cases} (min(4m-4,\,-m-9),\,+\infty),\, m < 0 \\ \{-9\} \cup [-1,\,+\infty),\, m = 0 \\ (-\infty,\,-m-9] \cup [4m-4,\,+\infty),\, m > 0 \end{cases}$.

c) 1. f este injectivă dacă f(x) = f(y) => x = y. În primul rând vom studia injectivitatea pe ramuri. Cunoaștem că $f/_{(-\infty,\,-1]}$ și $f/_{(-1,\,+\infty)}$ sunt monotone, deci injective.
Caut valorile lui m pentru care funcția nu este injectivă. Fie x, y, $x \in (-\infty, -1]$, iar $y \in (-1, +\infty)$ cu proprietatea că f(x) = f(y). f(x) $\in [m-1,\,+\infty)$ => $\exists$ y f(y) $\geq$ m-1.
Pentru m > 0, funcția nu este injectivă întrucât $\forall y \in (max(4m-4, -m-9),\,+\infty)$ $\exists x_1 \in (-\infty,\,-1)$ și $x_2 \in (-1,\,+\infty)$ astfel încât $f(x_1) = f(x_2) = y$.
Pentru m = 0, funcția nu este injectivă (f(0) = f(1) = -9).
Pentru m $\leq$ 0, funcția nu este injectivă dacă m - 1 < -m - 9 $\iff$ 2m < -8 $\iff$ m < -4.
Deci, funcția este injectivă pentru m $\in [-4, 0)$.

c) 2. Funcția este surjectivă dacă $\forall$ y $\in \mathbb{R}$, $\exists x \in \mathbb{R}$ astfel încât f(x) = y.

Cu alte cuvinte, Imf = $\mathbb{R}$. Analizând cazurile obținute la b), pentru a funcția poate fi surjectivă dacă m < 0. De asemenea $(-\infty,\ -m-9] \cup [m-1,\ +\infty) = \mathbb{R}$.
m - 1 $\leq$ -m - 9 $\iff$ 2m $\leq$ -8 $\iff$ m $\leq$ -4.
Deci, f este surjectivă pentru m $\in (-\infty, -4]$.
c) 3. O funcție este bijectivă $\iff$ funcția este injectivă și surjectivă. Folosim rezultatele obținute la subpunctele anterioare și găsim că f este bijectivă pentru m $\in (-\infty, -4] \cap [-4, 0] = \{-4\}$.

Exercițiul 2

Fie E o mulțime și $A \subseteq E$. Funcția $\xi : E- > \{0, 1\}$, $\xi_A(x) = \begin{cases} 1, x \in A \\ 0, x \notin A \end{cases}$
se numește funcția caracteristică a lui A în E. (Curs 2, Seria 13, pagina 3)
Fie $A, B \subseteq E$, cunoaștem regulile lui de Morgan:
$C_E(A \cup B) = (C_E A) \cap (C_E B)$
$C_E(A \cap B) = (C_E A) \cup (C_E B)$
Demonstrați regulile lui de Morgan cu ajutorul funcției caracteristice.

Rezolvare:

Pentru doua submultimi A și B ale unei mulțimi T, funcția caracteristică are următoarele proprietăți:

1) $\xi_A = \xi_B \iff A = B$
2) $\xi_{A \cap B} = \xi_A * \xi_B$
3) $\xi_{A \cup B} = \xi_A + \xi_B - \xi_A * \xi_B$
4) $\xi_{C_T A} = 1 - \xi_A$
5) $\xi_A^2 = \xi_A$

Putem aplica proprietățile de mai sus în relațiile lui de Morgan, obținând:
$\xi_{C_E(A \cup B)} = 1 - (\xi_A + \xi_B - \xi_A * \xi_B)$
$\xi_{(C_E A) \cap (C_E B)} = 1 - (\xi_A^2 + \xi_B^2 - \xi_A * \xi_B) = 1 - (\xi_A + \xi_B - \xi_A * \xi_B)$
Din cele două relații de mai sus, împreună cu proprietatea 1, deducem:
$C_E(A \cup B) = (C_E A) \cap (C_E B)$
În mod analog,
$\xi_{C_E(A \cap B)} = 1 - \xi_A * \xi_B$
$\xi_{(C_E A) \cup (C_E B)} = (1 - \xi_A) + (1 - \xi_B) - (1 - \xi_A) * (1 - \xi_B) = 1 - \xi_A * \xi_B$
de unde:
$C_E(A \cap B) = (C_E A) \cup (C_E B)$.

Exercițiul 3

Arătați că relația de congruență modulo n este relație de echivalență.

Rezolvare:

- preluată din Tutoriat 1, anul 2019-2020, de la Gabriel Majeri

Fie $n \in \mathbb{N}^*$ fixat. Atunci spunem că $a \equiv b \mod n$ dacă $n \mid (a-b)$.

Pentru a demonstra că este relație de echivalență, trebuie să demonstrăm că este *reflexivă*, *simetrică* și *tranzitivă*.

1. Reflexivitate
   Fie $a \in \mathbb{N}$. Atunci $n \mid (a-a) = 0$. Astfel $a \equiv a \mod n$. Deci $\equiv$ este reflexivă.

2. Simetrie
   Fie $a, b \in \mathbb{N}$ cu $a \equiv b \mod n$. Din definiție, $n \mid (a-b)$. Atunci $n \mid -(a-b)$. De unde rezultă că $n \mid (b-a)$. Deci $b \equiv a \mod n$. Astfel $\equiv$ este simetrică.

3. Tranzitivitate
   Fie $a, b, c \in \mathbb{N}$ cu $a \equiv b \mod n$ și $b \equiv c \mod n$. Conform definiției $n \mid (a-b)$ și $n \mid (b-c)$. Atunci facem suma și obținem $n \mid ((a-b)+(b-c)) \implies n \mid (a-c)$. Deci $a \equiv c \mod n$. Astfel $\equiv$ este tranzitivă.

Conform celor trei proprietăți demonstrate mai sus $\equiv$ este relație de echivalență.

Exercițiul 4

Definim pe mulțimea numerelor complexe $\mathbb{C}$ următoarea relație binară:

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

a) Să se arate că ρ este relație de echivalență.
b) Aflați clasa de echivalență a lui π în raport cu ρ.
c) Aflați clasa de echivalență a lui $1+2i$ în raport cu ρ.
d) Aflați clasa de echivalență a lui $a+bi$, cu $a, b \in \mathbb{R}$, în raport cu ρ.
e) Determinați un sistem complet și independent de reprezentanți pentru ρ.
(Restanță algebră, seria 13, 04.06.2020)

Rezolvare:

a) Pentru a demonstra că ρ este relație de echivalență vom arăta că ρ este reflexivă, simetrică și tranzitivă.
ρ este reflexivă $\iff x \, \rho \, x \; \forall x \in \mathbb{R} \iff x - x \in \mathbb{R} \iff 0 \in \mathbb{R}$, ceea ce este adevarat.
ρ este simetrică $\iff \forall \, a, b \in \mathbb{R}$ astfel încât $a \, \rho \, b$ atunci $b \, \rho \, a$.
$a \, \rho \, b \iff a - b \in \mathbb{R}$. Dacă a - b $\in \mathbb{R}$, atunci -(a-b) = b-a $\in \mathbb{R} \iff b \, \rho \, a$.
ρ este tranzitivă dacă $a \, \rho \, b$ și $b \, \rho \, c$ atunci a ρ c.
a $\rho \, b \iff a - b \in \mathbb{R}$ b $\rho \, c \iff b - c \in \mathbb{R}$
Atunci a - c = (a - b) + (b - c) $\in \mathbb{R} \iff a \, \rho \, c$.

b) Clasa de echivalență a lui π în raport cu ρ este $[\pi] = \{x \mid x \, \rho \, \pi\}$,

$[\pi] = \{x \mid x\ -\ \pi \in \mathbb{R}\}$
$\pi = \pi + 0 \cdot i$
x = a + b · i
$\pi - x = \pi - a - bi \in \mathbb{R} \iff b = 0$
Deci, clasa de echivalență a lui π este $\mathbb{R}$.

c) Clasa de echivalență a lui 1 + 2i în raport cu ρ este $[1+2i] = \{x \mid x\,\rho\,(1+2i)\}$,
$[1+2i] = \{x \mid x\ -\ (1+2i) \in \mathbb{R}\}$
x = a + b · i
$x - (1+2i) = a - 1 + (b-2)i \in \mathbb{R} \iff b - 2 = 0 \iff b = 2$
Deci, clasa de echivalență a lui 1+2i este $\{a + 2i \mid a \in \mathbb{R}\}$.
d) Clasa de echivalență a lui a + bi în raport cu ρ este $[a+bi] = \{x \mid x\,\rho\,(a+bi)\}$,
$[a+bi] = \{x \mid x\ -\ (a+bi) \in \mathbb{R}\}$
x = c + d · i
$x - (a+bi) = a - c + (b-d)i \in \mathbb{R} \iff b - d = 0 \iff b = d$
Deci, clasa de echivalență a lui a+bi este $\{c + bi \mid c \in \mathbb{R}\}$.

e) O mulțime A este sistem complet și independent de reprezentanți dacă
$\forall\, x, y \in A, x \neg\rho\, y$ și $\forall\, x \in \mathbb{C}\ \exists\, y \in A$astfel încât $x\rho\, y$.
Conform d) clasa de echivalență a lui a+bi este $\{c + bi \mid c \in \mathbb{R}\}$. Un sistem de reprezentanți este $\{ai \mid a \in \mathbb{R}\}$.
$\forall\, x = a + bi \in \mathbb{C}\ \exists\, y = bi \in A$ astfel încât $x\rho\, y \iff x - y = a \in \mathbb{R}$.
$\forall\, x = ai,\ y = bi \in A,\ x \neq y,\ \ x \neg\rho\, y \iff x - y = (a-b)i \notin \mathbb{R} \iff a - b \neq 0$, ceea ce este adevărat.

Tutoriat 2 - Rezolvări
Funcții. Relații de echivalență.

Savu Ioan Daniel, Tender Laura-Maria

- 10 noiembrie 2020 -

Exercițiul 1

Fie A, B două mulțimi finite cu $|A|$ = a și $|B|$ = b. Calculați:
i) Numărul funcțiilor strict crescătoare de la A la B.
ii) Numărul funcțiilor crescătoare de la A la B.

Rezolvare:

Ținând cont de faptul ca elementele mulțimiilor sunt comparabile, pentru ușurință, le putem înlocui cu numerele lor de ordine. Astfel, $A = \{1, 2, ...a\}$ și $B =$ $= \{1, 2, ..., b\}$
i) Fie x_1, x_2, ..., x_a elementele mulțimii A cu $x_1 < x_2 < ... < x_a$. Fie y_1, y_2, ..., y_b elementele mulțimii B cu $y_1 < y_2 < ... < y_b$. f : A $\rightarrow$ B strict crescătoare $\Rightarrow$ $f(x_1) < f(x_2) < ... < f(x_a)$.
Problema ne cere să găsim în câte moduri putem să alegem $f(x_1), f(x_2), ...f(x_a)$ astfel încât să fie respectată condiția de funcțe crescătoare. Cum pentru fiecare alegere a unei mulțimi de elemente inclusă în B există o singură modalitate de a le aranja crescător, problema dată devine echivalentă cu următoarea: în câte moduri putem alege a numere din b numere. Dacă $b < a$ nu există nicio funcție strict crescătoare. Pentru $b \geq a$ răspunsul este C_b^a.

ii) Condiția de funcție crescătoare este $f(x_1) \leq f(x_2) \leq ... \leq f(x_a)$. Diferența față de punctul anterior provine din faptul că acum putem alege din mulțimea B același element de mai multe ori. Pentru a scăpa de această deosebire, putem să rescriem inegalitatea de mai sus în modul următor
$f(x_1) < f(x_2) + 1 < f(x_3) + 2 < ... < f(x_a) + a - 1$
Construim următoarea funcție $g : \{1, 2, ..., a\} \rightarrow \{1, 2, ..., b, b + 1, ..., b + a - 1\}$
$g(x_k) = f(x_k) + k - 1$. Problema inițială devine echivalentă astfel cu a determina numărul de funcții strict crescătoare de la $\{1, 2, ..., a\}$ la $\{1, 2, ..., b, b + 1, ..., b + a - 1\}$. Analog, acest număr este C_{b+a-1}^a.

Exercițiul 2

Să se determine p $\in \mathbb{N}^*$ astfel încât funcția f : $\mathbb{N} \to \mathbb{N}$, f(n) = $[\frac{n}{p}]$ + $[\frac{n+1}{p}]$ + $[\frac{n+2}{p}]$ să fie bijectivă.

Rezolvare:

f(n) = $[\frac{n}{p}]$ + $[\frac{n+1}{p}]$ + $[\frac{n+2}{p}]$
f(n+1) = $[\frac{n+1}{p}]$ + $[\frac{n+2}{p}]$ + $[\frac{n+3}{p}]$
f(n+1) - f(n) = $[\frac{n+3}{p}]$ - $[\frac{n}{p}]$ ≥ 0 $\forall n, p \Rightarrow$ funcția este crescătoare.
Pentru p = 1, f(n) = 3n + 3. f(0) = 3 și cum funcția este crescătoare nu există x $\in \mathbb{N}$ astfel încât f(x) = 0, deci funcția nu este surjectivă.
Pentru p = 2, f(0) = 1 deci nici în acest caz funcția nu este surjectivă.
Identitatea lui Hermite [a] + $[a + \frac{1}{n}]$ + [a + $\frac{2}{n}$] + ... + $[a + \frac{n-1}{n}]$ = [na] $\forall a \in \mathbb{R}, n \in \mathbb{N}$*
Pentru p = 3, alegând a = $\frac{n}{p}$, conform identității enunțate mai sus f(n) = n, care este bijectivă.
Pentru p > 3 f(0) = f(1) = 0, deci funcția nu este injectivă.
Astfel f bijectivă pentru p = 3.

Exercițiul 3

Să se arate că funcția f : $\mathbb{N} \times \mathbb{N} \to \mathbb{N}$ f(m, n) = $\frac{(m+n)(m+n+1)}{2}$ + m este o funcție bijectivă.

Rezolvare:

Funcția este surjectivă dacă $\forall x \in \mathbb{N}$ $\exists$ m, $n \in \mathbb{N}$ astfel încât f(m, n) = x.
$\frac{(m+n)(m+n+1)}{2}$ + m = x
(m+n)(m+n+1) + 2m = 2x
Fie m + n = k, relația se rescrie astfel k^2 + k + 2m = 2x
Pentru orice x căutam cel mai mare k cu proprietatea că k^2 + k $\leq$ 2x. Atunci deducem că $(k+1)^2$ + k + 1 > 2x. Atunci m = $\frac{2x-k^2+k}{2} \in \mathbb{N}$, iar n = k - m.
m $\leq$ k $\iff$ $\frac{2x-k^2+k}{2}$ $\leq$ k $\iff$ $2x - k^2 + k \leq$ 2k
$\iff$ $2x \leq k^2 + 3k$ $\iff$ $2x < k^2 + 3k + 2$ (conform alegerii k maxim).
Astfel funcția este sujectivă.
k(k+1) $\leq$ 2x < (k+1)(k+2) = k^2 + 3k + 2.
Pentru a demonstra că funcția este injectivă vom presupune ca există un alt k' care îndeplinește egalitatea.
2x = k'^2 + k' + 2m
Cum k' nu e maxim, $(k'+1)^2$ + k' + 1 $\leq$ 2x
Cum m $\leq$ k', k'^2 + 3k' + 2 = k'^2 + k' + 2k' + 2 > k^2 + k' + 2m = 2x (contradicție).

Exercițiul 4

Fie A mulțimea $\{1, 2, ..., 2000\}$. Să se determine numărul relațiilor de echivalență pe A ale căror mulțimi factor sunt formate din două clase de echivalență.

Rezolvare:

Știm că oricărei relații de echivalență pe o mulțime îi corespunde într-un mod bijectiv o partiție a mulțimii. Trebuie să determinăm în câte moduri putem să partiționăm A în două mulțimi, B și C.
Dacă B are 1 element, atunci avem C_{2000}^1 posibilități.
Dacă B are 2 elemente, atunci avem C_{2000}^1 posibilități.
...
Dacă B are 999 elemente, atunci avem C_{2000}^{999} posibilități.
Daca B are 1000 elemente, atunci avem $\frac{C_{2000}^{1000}}{2}$ posibilități (deoarce nu contează ordinea pentru B și C, iar o alegere a elementelor lui B determina elementele lui C).
Nu vom lua cazurile pentru care B are mai mult de 1000 de elemente deoarece se regăsesc in cazurile de mai sus, B C fiind echivalent cu C B.
Folosindu-ne de prorpietățiile combinăriilor, și anume
$C_n^k = C_n^{n-k}$
$C_n^0 + C_n^1 + ... + C_n^n = 2^n$ rezultatul este
$N = 2^{n-1} - 1$

Tutoriat 3 - Rezolvări
Grupuri. Teorema lui Lagrange

Savu Ioan Daniel, Tender Laura-Maria

- 17 noiembrie 2020 -

Exercițiul 1

Demonstrați că următoarele grupuri (cu adunarea) nu sunt izomorfe:

- $Z_2 \times Z_2$ și Z_4.
- **Z** și **Q**
- **Q** și **R**

Rezolvare:

Referință: Gabriel Majeri, "Rezolvări Tutoriat 6", 2019, exercițiul 1

Pentru a demonstra că două grupuri nu sunt izomorfe, putem folosi procedeul reducerii la absurd. Presupunem că ar exista un izomorfism f și ajungem la o contradicție.

- În unele cazuri ne putem gândi la ordinele elementelor. Reamintim că ordinul elementului x este cel mai mic număr natural nenul k pentru care $\underbrace{x + \cdots + x}_{k \text{ ori}} = 0$. Un izomorfism păstrează ordinul unui element: $f(\underbrace{x + \cdots + x}_{k \text{ ori}}) = \underbrace{f(x) + \cdots + f(x)}_{k \text{ ori}}$.
  - În $Z_2 \times Z_2$ toate elementele au ordin cel mult 2.
  - În Z_4 avem și un element de ordin 4 (și anume $\hat{1}$. Pentru elementul de ordin 4 nu am avea corespondent.
- O altă proprietate care trebuie păstrată de izomorfisme este cea de a fi grup ciclic. **Z** este un grup ciclic, în timp ce **Q** nu este.

  Demonstrăm prin reducere la absurd. Presupunem că **Q** ar fi ciclic. Fie a $\in$ **Q** un generator al său. Scriem a sub formă de fracție rațională ireductibilă: a = $\frac{p}{q}$, cu p, q $\in$ **Z**.

Observăm că fracția $\frac{p}{q+1}$ nu poate fi obținută din $\frac{p}{q}$. Oricum am aduna sau scădea fracțiile care sunt multiplu de $\frac{p}{q}$, nu putem ajunge la o fracție cu numitor mai mare.

- Dacă ar exista un izomorfism f, acesta ar fi funcție bijectivă. Asta ar însemna că **Q** și **R** ar avea același cardinal. Dar **Q** este mulțime numărabilă, iar **R** este nenumărabilă.

Exercițiul 2

Arătați că un grup cu 4 elemente este izomorf cu Z_4 sau cu grupul lui Klein $Z_2 \times Z_2$.

Rezolvare:

Referință: Tiberiu Dumitrescu, "Algebra 1", București, 2006, capitolul 10, exercițiul 49

$(Z_4, +)$	$\hat{0}$	$\hat{1}$	$\hat{2}$	$\hat{3}$
$\hat{0}$	$\hat{0}$	$\hat{1}$	$\hat{2}$	$\hat{3}$
$\hat{1}$	$\hat{1}$	$\hat{2}$	$\hat{3}$	$\hat{0}$
$\hat{2}$	$\hat{2}$	$\hat{3}$	$\hat{0}$	$\hat{1}$
$\hat{3}$	$\hat{3}$	$\hat{0}$	$\hat{1}$	$\hat{2}$

$(Z_2 \times Z_2, +)$	$(\hat{0}, \hat{0})$	$(\hat{0}, \hat{1})$	$(\hat{1}, \hat{0})$	$(\hat{1}, \hat{1})$
$(\hat{0}, \hat{0})$	$(\hat{0}, \hat{0})$	$(\hat{0}, \hat{1})$	$(\hat{1}, \hat{0})$	$(\hat{1}, \hat{1})$
$(\hat{0}, \hat{1})$	$(\hat{0}, \hat{1})$	$(\hat{0}, \hat{0})$	$(\hat{1}, \hat{1})$	$(\hat{1}, \hat{0})$
$(\hat{1}, \hat{0})$	$(\hat{1}, \hat{0})$	$(\hat{1}, \hat{1})$	$(\hat{0}, \hat{0})$	$(\hat{0}, \hat{1})$
$(\hat{1}, \hat{1})$	$(\hat{1}, \hat{1})$	$(\hat{1}, \hat{0})$	$(\hat{0}, \hat{1})$	$(\hat{0}, \hat{0})$

Fie G un grup cu 4 elemente. Elementele lui G au ordinul divizor al lui 4. Dacă G conține un element x de ordin 4, atunci x, x^2, x^3 și e = x^4 aparțin lui G, deci G este ciclic generat de x. Astfel G $\simeq Z_4$.
Dacă G nu conține elemente de ordin 4, atunci putem presupunem că G = $\{1, a, b, c\}$ cu $a^2 = b^2 = c^2 = 1$ Dacă ab = 1 (respectiv, ab = a, ab = b), atunci a = b (respectiv, b = 1, a = 1), contradicție. Deci ab = c, si analog ba = c, ac = ca = b, bc = cb = a. Comparând tablele de înmulțire, vedem că G $\simeq Z_2 \times Z_2$.

Exercițiul 3

Arătați că un grup cu 6 elemente este izomorf cu Z_6 sau cu S_3.

Rezolvare:

Referință: Tiberiu Dumitrescu, "Algebra 1", București, 2006, capitolul 10, exercițiul 49

Fie G un grup cu 6 elemente. G poate conține un element a de ordin 3 si un element b de ordin 2, conform teoremei lui Cauchy. Deci G = {1, a, a^2, b, ab, a^2b}.

Dacă ba = 1 (respectiv, ba = b, ba = b^2, ba = a), atunci a = b (respectiv, a = 1, a = b, b = 1), contradicție. Deci ba = ab sau ba = a^2b. Dacă ba = ab, atunci ab are ordinul 6, deci G este ciclic generat de ab, așadar G $\simeq Z_6$. Dacă ba = a^2b, atunci comparând tabelele, se vede că G $\simeq S_3$.

Exercițiul 4

Determinați dacă grupurile $Z_{28} \times Z_{29}$, $Z_{28} \times Z_{30}$, respectiv **R** sunt sau nu ciclice.

Rezolvare:

Referință: Gabriel Majeri, "Rezolvări Tutoriat 5", 2019, exercițiul 3

Pentru a simplifica demonstrațiile în problemele în care apar $Z_n \times Z_m$, ne folosim de o teoremă care ne spune că $Z_n \times Z_m$ este izomorf cu $Z_{n\times m}$ dacă și numai dacă n este prim față de m. În acest fel, se poate arăta că $Z_{n\times m}$ este ciclic dacă și numai dacă (n, m) = 1.

- Pentru $Z_{28} \times Z_{29}$, (28, 29) = 1.
- Pentru $Z_{28} \times Z_{30}$, numerele nu sunt prime între ele, deci grupul nu este izomorf cu $Z_{28\times 30}$.
- Să presupunem că **R** ar fi ciclic, și a $\in$ **R** ar fi un generator. Elementul a poate genera doar multiplii de a. Asta înseamnă că toate numerele din **R** sunt de forma na, pentru un n $\in$ **Z**. Dar **R** este o mulțime infinită nenumărabilă, deci există elemente care nu sunt generate de a.

Teorema de structură a grupurilor ciclice ne spune că orice grup ciclic este izomorf cu Z_n, dacă este finit, respectiv **Z** dacă este infinit. Deci, la un astfel de exercițiu putem arăta că un grup este/nu este izomorf cu unul dintre grupurile Z_n sau **Z**.

Exercițiul 5

Arătați că singurul morfism de grupuri (Q, +) $\to$ (Z, +) este cel nul.

Rezolvare

Considerăm un morfism $f : \mathbb{Q} \to \mathbb{Z}$. Fie un număr rațional de forma $\frac{1}{b} \in \mathbb{Q}$. Din proprietățiile morfismelor obținem următoarele două relații:
$f(0) = 0$.
$f(\underbrace{\frac{1}{b} + \cdots + \frac{1}{b}}_{b \text{ ori}}) = f(1) = b * f(\frac{1}{b}) \implies f(\frac{1}{b}) = \frac{f(1)}{b}$

Cum $f(x) \in \mathbb{Z},\ \forall x \in \mathbb{Z}$, rezultă că $\frac{f(1)}{b} \in \mathbb{Z},\ \forall b \in \mathbb{Z}$. Dacă $f(1) \neq 0$, atunci alegem $b = |f(1)| + 1$ si astfel fracția $\frac{f(1)}{b} \notin \mathbb{Z}$ deoarece $f(1)$ și b sunt prime între ele. Prin urmare $f(1) = 0$.

Din relația de mai sus avem că $f(\frac{1}{b}) = 0$, iar din relația $f(\frac{a}{b}) = f(\underbrace{\frac{1}{b} + \cdots + \frac{1}{b}}_{a \text{ ori}}) =$

$a * f(\frac{1}{b})$ rezultă că $f(\frac{a}{b}) = 0\ \forall a, b \in \mathbb{Z}$.

Tutoriat 4
Grup factor. Teorema fundamentală de izomorfism pentru grupuri

Savu Ioan Daniel, Tender Laura-Maria

- 25 noiembrie 2020 -

Exercițiul 1

Scrieți subgrupurile lui $\mathbf{Z}_{12}$ și grupurile factor ale lui $\mathbf{Z}_{12}$.

Rezolvare:

Știm din curs că orice subgrup al lui Z_n este de forma dZ_n, unde $d|n$. Această proprietate apare doarece subgrupul generat de $< a, b >=< (a, b) >$ si deci $< a_1, a_2, ..., a_k >=< (a_1, a_2, ..., a_k) >$. Cum $D_{12} = \{1, 2, 3, 4, 6, 12\}$ subgrupurile lui Z_{12} sunt: $Z_{12}, 2Z_{12}, 3Z_{12}, 4Z_{12}, 6Z_{12}, 12Z_{12}$, unde spre ex. $4Z_{12} = \{\overline{0}, \overline{4}, \overline{8}\}$.
Pentru grupul factor, vom lua ca exemplu $H = \{\overline{0}, \overline{4}, \overline{8}\}$. Grupul factor este definit ca:
$\frac{G}{H} = \{\{\overline{y}|\overline{y} - \overline{x} \in H, \overline{y} \in Z_{12}\}, \overline{x} \in Z_{12}\}$
Un element din grupul factor arata de forma :$\overline{x} + H$.
Prin urmare, $\frac{Z_{12}}{H} = \{$
$\overline{\overline{0}} = \{\overline{0}, \overline{4}, \overline{8}\}$,
$\overline{\overline{1}} = \{\overline{1}, \overline{5}, \overline{9}\}$,
$\overline{\overline{2}} = \{\overline{2}, \overline{6}, \overline{10}\}$,
$\overline{\overline{3}} = \{\overline{3}, \overline{7}, \overline{11}\}$
$\}$
În mod analog se rezolvă și pentru restul de grupuri factor.

Exercițiul 2

Fie $f : \mathbf{Q} \to \mathbf{C}^*$, definită prin $f(\frac{m}{n}) = \cos(2\pi)\frac{m}{n} + i \sin 2\pi \frac{m}{n}$ și notăm cu U mulțimea $U = \{z \in \mathbf{C}^* |\ \exists n \in \mathbf{N},\ z^n = 1\}$

1. Arătați că f este morfism de grupuri.
2. Determinați Ker$f$ și Imf.

3. Arătați că $\mathbf{Q}/\mathbf{Z} \cong U$.

Observație: Grupurile sunt $(\mathbf{Q}, +)$ și $(\mathbf{C}, \cdot)$.

Rezolvare:

1. Condiția ca f să fie morfism este ca

$$f(x+y) = f(x) \cdot f(y) \iff$$
$$\cos 2\pi(x+y) + i \sin 2\pi(x+y) = (\cos 2\pi x + i \sin 2\pi x) \cdot (\cos 2\pi y + i \sin 2\pi y)$$

   Ultima egalitate este adevărată din formulele lui de Moivre.

2. Observăm că mulțimea U este mulțimea rădăcinilor de ordin n ale unității, adică $U = \{\cos \frac{2k\pi}{n} + i \sin \frac{2k\pi}{n} \mid k \in \overline{(1, n-1)}\}$.
   $z^n = 1 \Rightarrow |z^n| = 1 \Rightarrow |z|^n = 1 \Rightarrow |z| = 1$.
   Ker $f = \{x \in \mathbf{Q} | f(x) = 1\} = \{x \in \mathbf{Q} | \cos 2\pi x + i \sin 2\pi x = 1\} = \{x \in \mathbf{Q} \mid x \in \mathbf{Z}\} = \mathbf{Z}$
   Im $f = \{y \in \mathbf{C}^* | \ \exists x \in \mathbf{Q}$, astfel incat $f(x) = y\} = \{y \in \mathbf{C}^* | \ \exists x \in \mathbf{Q}$, astfel incat $\cos 2\pi x + i \sin 2\pi x = y\} = \{y \in \mathbf{C} \mid |y| = 1\} = U$

3. Putem demonstra că grupul factor $\mathbf{Q}/\mathbf{Z}$. este izomorf cu U folosindu-ne de **teorema fundamentală de izomorfism**.

   (Teorema fundamentală de izomorfism pentru grupuri) Fie $f : G \to G'$ un morfism de grupuri. Atunci există un izomorfism de grupuri $\overline{f} : G/Kerf \to Imf$.

   Aplicând teorema pe cazul nostru obținem că există izomorfismul $\overline{f} : \mathbf{Q}/\mathbf{Z} \to U$. Deci,

$$\mathbf{Q}/\mathbf{Z} \cong U$$

Exercițiul 3

Folosind teorema de izomorfism pentru grupuri să se arate că grupul factor $(\mathbf{C}/\mathbf{R}, +)$ este izomorf cu grupul $(\mathbf{R}, +)$.

(Examen algebră, 04.06.2020, seria 13)

Rezolvare:

Fie $f : \mathbf{C} \to \mathbf{R}$, $f(a+bi) = b$. Vom demonstra că f este morfism. Fie $a+bi,\ c+di \in \mathbf{C}$, $a, b, c, d \in \mathbf{R}$.
$f(a+bi+c+di) = f(a+c+(b+d)i) = b+d = f(a+bi)+f(c+di)\ \forall a+bi,\ c+di \in \mathbf{C} \Rightarrow f$ morfism.
Im$f = \mathbf{R}$ întrucât $f(x) \in \mathbf{R}\ \forall x \in \mathbf{C}$ și $\forall\ y \in \mathbf{R}\ \exists x$ astfel încât $f(x) = y, y = z + yi, z \in \mathbf{R}$.

Ker $f = \{x \in \mathbf{C} \mid f(x) = 0\}$, $f(x) = 0 \iff f(a+bi) = 0$, unde $a + bi = x \iff b = 0 \iff x \in \mathbf{R}$. Astfel Ker $f = \mathbf{R}$.
Conform teoremei de izomorfism pentru grupuri, există un izomorfism de grupuri $\overline{f} : G/Kerf \to Imf$. $\overline{f} : \mathbf{C}/\mathbf{R} \to \mathbf{R}$. În concluzie, $(\mathbf{C}/\mathbf{R}, +) \cong (\mathbf{R}, +)$.

Exercițiul 4

Fie G grupul factor $(\mathbf{Q}/\mathbf{Z}, +)$. Arătați că:

1. dacă $a, b \in \mathbf{N}^*$ sunt prime între ele, atunci ord$\left(\widehat{\frac{a}{b}}\right) = b$
2. orice subgrup finit generat este ciclic
3. G nu este finit generat

Rezolvare:

1. În mod asemănător Exercițiului 1, putem scrie elementele grupului factor ca fiind : $\widehat{\frac{a}{b}} = \frac{a}{b} + \mathbf{Z} = \{\frac{a}{b} + n | n \in \mathbf{Z}\}$. Astfel, observăm că pentru $k \in \mathbf{Z}$, $\widehat{k} = \mathbf{Z}$ și $\widehat{0} = \mathbf{Z}$. Prin urmare, pentru a determina ordinul lui $\widehat{\frac{a}{b}}$ trebuie să vedem cel mai mic număr natural o pentru care $\frac{a}{b} * o \in \mathbf{Z}$. Cum a și b sunt prime între ele avem că o = b, deci $ord(\widehat{\frac{a}{b}}) = b$.

2. Un subgrup generat de 2 elemente este de forma $< \widehat{\frac{a}{b}}, \widehat{\frac{c}{d}} >= \{\frac{\widehat{abx+bcy}}{\widehat{bd}} | x, y \in \mathbf{Z}\}$. Se poate demonstra faptul că elementele mulțimii sunt de forma $k * \frac{\widehat{cmmdc(a,c)}}{\widehat{cmmmc(b,d)}}, k \in \mathbf{Z}$ și deci $< \widehat{\frac{a}{b}}, \widehat{\frac{c}{d}} >=< \frac{\widehat{cmmdc(a,c)}}{\widehat{cmmmc(b,d)}} >$ (această egalitate putând fi demonstrată folosind dubla incluziune). Aplicând inductiv pentru un numar arbitrar de numere relația de mai sus obținem că $< \widehat{\frac{a_1}{b_1}}, \widehat{\frac{a_2}{b_2}}, ..., \widehat{\frac{a_n}{b_n}} >=< \frac{\widehat{cmmdc(a_1,a_2,...,a_n)}}{\widehat{cmmmc(b_1,b_2,...,b_n)}} >$. Astfel, orice subgrup finit generat este ciclic.

3. Presupunem că G este finit generat. Conform subpunctului anterior, G este ciclic generat de un element de forma $\frac{a}{b}, a, b, \in \mathbf{Z}$. Fracția poate fi adusă la forma ireductibilă și conform subpunctului 1, ordinul lui G este un numar natural și deci G are un numar finit de elmente, însă G are o infinitate de elemente, contradicție. Deci G nu este finit generat.

Tutoriat 5

Savu Ioan Daniel, Tender Laura-Maria

\- 2 decembrie 2020 -

Exercițiul 1

Determinați elementele de ordin 30 din $\mathbf{Z}_{240}$.

Rezolvare:

Căutam elementele $\widehat{x}$ cu ordinul 30 în $\mathbf{Z}_{240} \iff \widehat{x}^{30} = \widehat{0}$ și nu exista $k < 30$ astfel încât $\widehat{x}^k = \widehat{0} \iff x^{30} \equiv 0 \pmod{240}$ și nu exista $k < 30$ astfel încât $x^k \equiv 0 \pmod{240}$.
Fie $\widehat{k} \in \mathbf{Z}_n$, atunci $\text{ord}(\widehat{k}) = \frac{n}{(n,k)}$.
Cum $\mathbf{Z}_{240}$ este un grup ciclic, relațiile de mai sus se pot rescrie $30x \equiv 0 \pmod{240}$. Astfel, căutăm elementele $\widehat{x}$ pentru care $\frac{240}{(240,x)} = 30 \iff (240, x) = 8$.
$240 = 2^4 \cdot 3 \cdot 5 \Rightarrow 8 \mid x$ dar $16 \nmid x, 3 \nmid x, 5 \nmid x$.
$\widehat{x} \in \{\widehat{8}, \widehat{56}, \widehat{88}, \widehat{104}, \widehat{136}, \widehat{152}, \widehat{184}, \widehat{232}\}$.

Exercițiul 2

(i) Fie G_1, G_2 două grupuri și $x_1 \in G_1$, $x_2 \in G_2$ elemente de ordin finit. Arătați că $\text{ord}(x_1, x_2) = [\text{ord}(x_1), \text{ord}(x_2)]$.
(ii) Determinați ord([3], [4]) în grupul $\mathbf{Z}_{24} \times \mathbf{Z}_{36}$.

Rezolvare:

i) Fie $m = \text{ord}\ (x_1)$ și $n = \text{ord}\ (x_2)$. $x_1^m = e_1$ (în G_1) și $x_2^n = e_2$ (în G_2).
Fie p $= \text{ord}(x_1, x_2)$, atunci $(x_1, x_2)^p = e \iff (x_1^p, x_2^p) = (e_1, e_2) \iff m \mid p$ și $n \mid p$ și p minim $\iff p = [m, n]$.

ii) Conformm i) ord([3], [4]) = [ord(3), ord(4)] în $\mathbf{Z}_{24}$, respectiv $\mathbf{Z}_{36}$.
$\text{ord}(3) = \frac{24}{(3,24)} = 8$, $\text{ord}(4) = \frac{36}{(4,36)} = 9$.
$\text{ord}([3], [4]) = 8 \cdot 9 = 72$.

Exercițiul 3

Determinați morfisemele între grupurile aditive $\mathbf{Z}_m$ și $\mathbf{Z}_n$.

Rezolvare:

Fie $\{f : \mathbf{Z}_m \to \mathbf{Z}_n |\ f(\widehat{x}+\widehat{y}) = f(\widehat{x}) + f(\widehat{y}), f(\widehat{0}) = \widehat{0}\}$ morfismele căutate.

Notăm $f(\widehat{1}) = \widehat{a}$, $a \in \mathbf{Z}_n$. Atunci f($\widehat{x}$) $= f(\widehat{1}+\widehat{1}+...\widehat{1}) = x \cdot \widehat{a}$, $x \in \mathbf{Z}_m$.

f($\widehat{m}$) $= m \cdot \widehat{a} = \widehat{0} \Rightarrow n|m \cdot a$. Notăm $(n, m) = d \Rightarrow \frac{n}{d} \mid a \Rightarrow a = \frac{n}{d} \cdot k$.
În concluzie, $\widehat{a} = \{\widehat{0}, \widehat{\frac{n}{d}}, ..., \widehat{\frac{(d-1)n}{d}}\}$.

Exercițiul 4

Fie grupul abelian $G = \mathbf{Z}_4 \times \mathbf{Z}_{10}$.

1. Se consideră elementul $x = (\widehat{2}, \widehat{2})$ al lui G. Aflați ordinul lui x și scrieți toate elementele subgrupului $H = < x >$.
2. Cu ce grup este izomorf G/H?
3. Aflați ordinul maxim al elementelor lui G și dați un exemplu de element de ordin maxim.
4. Determinați toate elementele de ordin 20 din G.

(Examen algebră, 26.01.2018, seria 10)

Rezolvare:

1. Putem alfa ordinul elementului x prin relația ord(x) = cmmmc(ord($\widehat{2}$ în $\mathbf{Z_4}$), ord($\widehat{2}$ în $\mathbf{Z_{10}}$)). Totodată, ordinul este numărul de elemente din subgrupul $H = \{(\widehat{0}, \widehat{0}), (\widehat{0}, \widehat{2}), (\widehat{0}, \widehat{4}), (\widehat{0}, \widehat{6}), (\widehat{0}, \widehat{8}), (\widehat{1}, \widehat{0}), (\widehat{1}, \widehat{2}), (\widehat{1}, \widehat{4}), (\widehat{1}, \widehat{6}), (\widehat{1}, \widehat{8})\}$.
2. Observăm că elementele din G/H sunt de forma $G/H = \{(\overline{\overline{0}}, \overline{\overline{0}}), (\overline{\overline{0}}, \overline{\overline{1}}), (\overline{\overline{1}}, \overline{\overline{0}}), (\overline{\overline{1}}, \overline{\overline{1}})\}$. Astfel, $G/H \cong Z_2 \times Z_2$. Această relație de izomorfism se poate argumenta construind tabelele legilor pentru cele două grupuri. În general, avem că $Z_n / < x > \cong Z_{n/ord(x)}$
3. Cum am precizat și la punctul 1), ordinul elementului $(\widehat{x}, \widehat{y}) \in \mathbf{Z_4} \times \mathbf{Z_{10}}$ este cmmmc(ord(x), ord(y)). Din teorema lui Lagrange știm că ord(x) | 4 și ord(y) | 10. Alegând convenabil ord(x) = 4 și ord(y) = 10, avem ordinul maxim din grup, și anume cmmmc(4, 10) = 20. Un astfel de element cu ordin maxim este $(\widehat{1}, \widehat{1})$.

4. Mai intâi trebuie să determinăm toate combinațiile de numere cu cmmmc-ul 20. Acestea sunt (4, 10) și (4, 5). Elementele corespunzătoare ordinelor 4 și 10 sunt $(\widehat{1}, \widehat{1}), (\widehat{1}, \widehat{3}), (\widehat{1}, \widehat{7}), (\widehat{1}, \widehat{9}), (\widehat{3}, \widehat{1}), (\widehat{3}, \widehat{3}), (\widehat{3}, \widehat{7}), (\widehat{3}, \widehat{9})$. Elementele corespunzătoare sunt $(\widehat{1}, \widehat{2}), (\widehat{1}, \widehat{4}), (\widehat{1}, \widehat{6}), (\widehat{1}, \widehat{8}), (\widehat{3}, \widehat{2}), (\widehat{3}, \widehat{4}), (\widehat{3}, \widehat{6}), (\widehat{3}, \widehat{8})$. Acestea sunt toate elementele pentru care ordinul lor in G este 20.

Tutoriat 6 - Rezolvări
Grupul de permutări

Savu Ioan Daniel, Tender Laura-Maria

- 9 decembrie 2020 -

Exercițiul 1

Fie permutarea $\sigma = \left(\begin{smallmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 \\ 3 & 4 & 5 & 7 & 9 & 2 & 8 & 6 & 1 & 11 & 10 \end{smallmatrix}\right) \in S_{11}$

1. Descompuneți σ în produs de cicli dijuncți.
2. Descompuneți σ în produs de transpoziții.
3. Calculați sgn(σ) și ord(σ).
4. Există permutări de ordin 35 în S_{11}
5. Rezolvați ecuația $x^{2011} = \sigma$.

Rezolvare:

1. $\sigma = (1, 3, 5, 9)(2, 4, 7, 8, 6)(10, 11)$
2. având descompusă permutarea in cicli decscompunerea în transpoziții este $\sigma = (1, 3)(3, 5)(5, 9)\ (2, 4)(4, 7)(7, 8)(8, 6)\ (10, 11)$
3. Signatura unui produs de ciclii este produsul signaturiilor ciclilor. Un ciclu de lungime n are signatura $(-1)^{n-1}$. Deci $\text{sgn}(\sigma) = (-1)^3 \cdot (-1)^4 \cdot (-1)^1 = 1$. Ordinul permutării este cel mai mic multiplu comun al lungimilor ciclilor în care acesta se descompune. $\text{ord}(\sigma) = \text{cmmmc}(4,\ 5,\ 2) = 20$.
4. Cum $35 = 7 \cdot 5$ rezultă că permutarea ar trebui să conțină cel puțin un ciclu de lungime 7 și un ciclu de lungime 5. Însă lungimea acestor cicli este $12 > 11$ și deci prin urmare nu poate exista o permutare din S_{11} cu ordinul 35.
5. Trebuie să argumentăm de unde poate proveni fiecare ciclu din permutarea σ (spre exemplu 2 2-ciclu pot proveni dintr-un ciclu de lungime 4 ridicat la pătrat). Luând pe rând ciclii din σ, cel de lungime 5 poate proveni doar dintr-un ciclu de lungime 5, cel de lungime 4 în mod analog iar

cel de lungime 2 tot dintr-un ciclu de lungime 2. Ne rămâne să vedem ce ciclu de lungime 5 ridicat la 2011 da ciclul de lungime 5 din σ. Folosindu-ne de ordinul unui ciclu, găsim pe rând ciclii și deci x = $(1, 9, 5, 3)(2, 4, 7, 8, 6)(10, 11)$

Exercițiul 2

Fie $\sigma = (1324) \in S_4$.

1. Determinați soluțiile ecuației $x^2 = \sigma, x \in S_4$
2. Determinați soluțiile ecuației $x^3 = \sigma, x \in S_4$.
3. Aflați numărul de elemente din $H =< \sigma >$ (subgrupul generat de σ în S_4.
4. Aflați indicele lui H în S_4.
5. Arătați că H nu e subgrup normal în S_4.
6. Determinați cel mai mic subgrup normal al lui S_4 care-l conține pe H.

(Examen algebră, 31.01.2020, seria 13)

Rezolvare:

1. Pentru ca ecuația $x^2 = \sigma, x \in S_4$ să aibă soluție, σ trebuie să fie o permutare pară.
   Putem scrie σ astfel
   $$\sigma = \left(\begin{smallmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 2 & 1 \end{smallmatrix}\right)$$
   ord(σ) = 2 + 3 = 5 $\Rightarrow$ sgn(σ) = -1, σ este impară deci ecuația nu are soluție.

2. Trebuie să știm că atunci când ridicăm o transpoziție la puterea a treia obținem aceeași transpoziție, când ridicăm un ciclu de lungime trei la puterea a treia obținem permutarea identică, iar când ridicăm un ciclu de lungime patru la puterea a treia obținem tot un ciclu de lungime patru. Astfel, soluția ecuației $x^3 = \sigma, x \in S_4$ poate fi doar un ciclu de patru. Fie permutarea
   $$x = \left(\begin{smallmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 1 & 2 \end{smallmatrix}\right)$$
   $$x^2 = \left(\begin{smallmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{smallmatrix}\right)$$
   $$\sigma = x^3 = \left(\begin{smallmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 2 & 1 \end{smallmatrix}\right)$$

3. σ este un ciclu de lungime patru, deci $\sigma^4 = e$. Astfel numărul de elemente din $H =< \sigma >$ este 4, $H = \{e, \sigma, (12)(34), (1423)\}$.

4. S_4 are $4! = 24$ elemente. Indicele lui H în S_4, $[S_4 : H] = \frac{\text{ord}(S_4)}{\text{ord}(H)} = 6$.

5. Dacă H ar fi subgrup normal în S_4, atunci $\forall x \in S_4, \forall y \in H \; xyx^{-1} \in H$.
Fie $x = (123)$
$$x = \left(\begin{smallmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{smallmatrix}\right)$$
$x^{-1} = (132)$
$$x = \left(\begin{smallmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{smallmatrix}\right)$$
$x\sigma x^{-1} = (123)(1324)(132) = (1342) \notin H \Rightarrow H$ nu e subgrup normal.

6. Vom demonsta la exercițiul următor că S_4 are următoarele subgrupuri normale $\{e\}, K, A_4, S_4$. Dintre acestea, cel mai mic subgrup care îl conține pe H este S_4.

Exercițiul 3

Fie $K = \{e, (12)(34), (13)(24), (14)(23)\} \subseteq S_4$. Să se arate că:

1. K este subgrup normal în S_4 (deci și în A_4).
2. S_4/K este izomorf cu S_3.
3. A_4 nu are subgrupuri de ordin 6.
4. Subgrupurile normale ale lui S_4 sunt $\{e\}, K, A_4, S_4$.

Referință: Cornel Băețică, Crina Boboc, Sorin Dăscălescu, Gabriel Mincu, "Probleme de algebră", capitolul 3, exercițiul 66

Rezolvare:

1. Fie $\sigma \in S_4$. Dacă K este subgrup normal în S_4, atunci $\sigma x \sigma^{-1} \in K$, $x \in S_4$. $\sigma(12)(34)\sigma^{-1} = (\sigma(1)\sigma(2))(\sigma(3)\sigma(4)) \in K$. Analog și pentru celelalte elemente din K, deci K subgrup normal.

2. $|S_4/K| = 6$, deci S_4/K este izomorf cu $\mathbf{Z}_6$ sau S_3 *(demonstație tutoriat 3, exercițiul 3)*. Dacă S_4/K ar fi izomorf cu $\mathbf{Z}_6$ atunci acesta ar fi grup ciclic și ar conține un element de ordin 6, pe care îl notez cu $\widehat{\sigma}$. Dar $\sigma \in S_4$ permutare deci $\mathrm{ord}(\sigma) \in \{1, 2, 3, 4\}$. Atunci $\widehat{\sigma}$ nu poate avea ordin 6. Deci S_4/K nu este izomorf cu $\mathbf{Z}_6 \Rightarrow S_4/K \cong S_3$.

3. A_4 este subgrupul permutărilor pare din S_4. $\mathrm{ord}(A_4) = 12$. $A_4 = \{e, (12)(34), (13)(24), (14)(23), (123), (132), (124), (142), (134), (143), (234), (243)\}$. A_4 are un element de ordin 1, trei elemente de ordin 2 și opt elemente de ordin 3. Dacă X este un subgrup cu 6 elemente, atunci X nu poate fi izomorf cu $\mathbf{Z}_6$ pentru că nu are niciun element de ordin 6. Deci X ar trebui să fie izomorf cu S_3. Astfel X trebuie să conțină două elemente de ordin 2, și acestea pot fi doar (12)(34), (13)(24), (14)(23). Alegând oricare dintre ele o vor genera pe cea de-a treia. Deci nu putem obține un subgrup cu 6 elemente al lui A_4.

4. Fie X subgrupurile normale al lui S_4. Vom analiza două cazuri:
   a) $X \subseteq A_4$
   b) $X \nsubseteq A_4$
   a) În acest caz, conform teoremei lui Lagrange, un subgrup propriu al lui A_4 are ordinul 2, 3, 4 sau 6. Deja am demonstrat că nu există subgrupuri cu 6 elemente. Un grup cu ordinul 4 nu are elemente de ordin 3 (nu ar respecta Langrange, $3 \nmid 4$). Deci singurul grup cu 4 elemente este K. Subgrupurile cu 3 sau 2 elemnente sunt ciclice, generate de o transpoziție sau un ciclu de trei. Acestea nu pot fi grupuri normale.
   b) În acest caz, există $\sigma \in X$ permutare impară. σ poate fi o transpoziție sau un ciclu de lungime 4. Dacă σ este transpoziție $\sigma = (ij)$, atunci $\tau\sigma\tau^{-1} = (\tau(i)\tau(j)) \in X \ \forall \ \tau \in S_4$. Deci X conține toate transpozițiile, iar acestea generează S_4 (vezi problema următoare). Dacă σ este ciclu de lungime 4, $\sigma = (ijkl)$, atunci X va conține toti ciclii de lungime 4. $\sigma^2 = (ik)(jl) \in X$, deci X va conține și toate produsele de câte două transpoziții. Dar (ijkl)(iljk) = (jlk) $\in X$, deci X conține toți ciclii de lungime 3 $\Rightarrow X = S_4$.

Exercițiul 4

Să se arate că S_n este generat de fiecare din următoarele mulțimi de permutări:

1. (12), (13), . . . , (1,n)
2. (12), (23), . . . , (n-1, n)
3. (12), (12. . . n)

Rezolvare:

Știm ca orice permutare poate fi descompusa in transpoziții. Este deci suficient să demonstrăm ca având permutările date putem forma orice transpoziție. Astfel, fiecare permutare din S_n poate fi descompusă in transpoziții iar fiecare transpoziție în permutările date.

1. Vrem să obținem în cazul general transpoziția (a, b), cu $a, b \leq n$. Având permutările de forma (1, x), se poate observa că $(a, b) = (1, a)(1, b)(1, a)$. Cum avem $(1, a)$ și $(1, b)$ pentru orice a și b în setul nostru de permutări, putem obține orice transpoziție și deci S_n este generat de acest set.

2. Observăm că în acest set de mulțimi dacă facem produsul elementelor în stilul $(1, 2)(2, 3)(3, 4)...(a - 1, a)$ vom obține o permutare circulară a primelor a elemente la stânga. $\begin{pmatrix} 1 & 2 & 3 & \dots & a-1 & a \\ 2 & 3 & 4 & \dots & a & 1 \end{pmatrix} \in S_{11}$. Vedem că dacă am permuta circular la dreapta primele a-1 elemente acum am obține permutarea (1, a) pentru orice a. Deci, am obține toate permutările de la punctul anterior iar desrpre ele știm deja că genereaza pe S_n. Pentru a permuta circular la dreapta primele a-1 elemente trebuie să permutam circular la stanga de a-1 ori primele n elemente. Deci $(1, a) =$

$(1,2)(2,3)(3,4)...(a-1,a)$ $((1,2)(2,3)(3,4)...(a-2,a-1))^{a-2}$. Prin urmare, setul dat de permutări generează S_n.

3. În mod analog ca subpunctul de mai sus, putem să incercăm să generăm elementele de forma (a-1, a) avand permutările date. Dacă le putem genera pe toate ne putem folosi de punctul anterior în a argumenta concluzia. Observăm că $(a-1,a) = (1,2,...,n)^{a-1}(1,2)(1,2,3,...,n)^{n-a+1}$. Astfel, putem genera orice element din multimea anterioară de permutări iar cum acestea generează toată mulțimea S_n, avem deci concluzia că elementele date generează toată mulțimea.

Tutoriat 7
Inele. Generalități.

Savu Ioan Daniel, Tender Laura-Maria

- 15 decembrie 2020 -

Exercițiul 1

Găsiți elementele inversabile, divizorii lui zero, elementele nilpotente și elementele idempotente din $\mathbf{Z}_{63}$.

Exercițiul 2

Se consideră numărul natural $n \geq 2$ care are r factori primi distincți în descompunerea sa. Să se arate că numărul idempotenților lui $\mathbf{Z_n}$ este 2^r. Să se determine idempotenții inelului Z_{36}.

$(R, +, \cdot)$ — operație 1, operație 2; R — mulțime

$(R,+)$ grup comutativ

$(\forall) a,b,c \in R$
$(a\cdot b)\cdot c = a\cdot(b\cdot c)$ → asociativitate

$(\forall) a,b,c \in R$
$a(b+c) = a\cdot b + a\cdot c$
$(b+c)\cdot a = b\cdot a + c\cdot a$

Dacă $\exists 1 \in R$ a.î. $(\forall) a \in R$ $a\cdot 1 = 1\cdot a = a$

R → inel unitar

0 → elem neutru pt. operația de adunare

În plus dacă $(\forall) a,b \in R$ $a\cdot b = b\cdot a$
Inel comutativ.

Exercițiul 1 $(R,+,\cdot)$ $(\mathbb{Z}_{63},+,\cdot)$
Găsiți elem inversabile, divizori lui 0, elem nilpotente și elem idempotente din $\mathbb{Z}_{63}$.

→ elemente inversabile $x \; \exists \; x'$
$x\cdot x' = 1$
$\hat{x} \; \exists \; \hat{x'}$ a.î. $\hat{x}\cdot\hat{x'} = \hat{1}$
$\mathbb{Z}_n$, $(x,n) = 1 \Leftrightarrow \hat{x}$ inversabil
$U(\mathbb{Z}_{63}) = \{\hat{1}, \hat{2}, \hat{4}, \hat{5}, \dots\}$

→ divizorii lui zero
x dacă $\exists \; x'$ a.î. $x\cdot x' = 0$
În $\mathbb{Z}_n$ toate elementele $\hat{x}$, $(x,n) \neq 1$ sunt divizorii lui 0. $63 = 3^2\cdot 7$
$\{\hat{3}, \hat{6}, \hat{7}, \hat{9}, \hat{12}, \dots\}$

→ elemente nilpotente $x \; \exists \; n \in \mathbb{N}^*$ a.î. $x^n = 0$
în $\mathbb{Z}_{63}$ $\hat{x}^n = \hat{0}$, $x^n \equiv 0 \pmod{63}$
$63 \mid x^n$
$3\cdot 7 = 21 \mid x$
$\hat{x} \in \{\hat{0}, \hat{21}, \hat{42}\}$. $x = p_1^{a_1}\cdot p_2^{a_2}\dots p_k^{a_k}$
$\hat{x} = \hat{2}_1$ $\hat{x} = \hat{3}\cdot\hat{7}$
$\exists \; n$ a.î. $\hat{x}^n = \hat{0} \Leftrightarrow \exists \; n$ a.î. $63 \mid x^n$
$63 \mid p_1^{n\cdot a_1}\cdot p_2^{n\cdot a_2}\cdot p_k^{n\cdot a_k} \dots$
$p_i = 3$ și $p_j = 7$

→ elemente idempotente x
$x^2 = x$.
Obs: 0, 1 sunt idempotente
$\mathbb{Z}_n = \mathbb{Z}_{p_1^{a_1}\cdot p_2^{a_2}\dots p_k^{a_k}} \simeq \mathbb{Z}_{p_1^{k_1}}\cdot\mathbb{Z}_{p_2^{k_2}}\dots\mathbb{Z}_{p_k^{a_k}}$
$n = p_1^{a_1}\cdot p_2^{a_2}\dots p_k^{a_k}$
$\mathbb{Z}_{p_i^{k_i}}$, $i = \overline{1,k}$ → are doar 2 (triviali)
p_i prim

$\mathbb{Z}_{63} = \mathbb{Z}_{9\cdot 7} = \mathbb{Z}_9 \times \mathbb{Z}_7$
$\hat{0} \Leftarrow (\bar{0}, \bar{\bar{0}})$ → restul 0 la împ. la 9 — 7
$\hat{1} \Leftarrow (\bar{1}, \bar{\bar{1}})$
$\hat{36} \Leftarrow (\bar{0}, \bar{\bar{1}})$ → restul 0 la împ cu 9 — 1 — 1 — cu 7 idempotenți (cei
$\hat{28} \Leftarrow (\bar{1}, \bar{\bar{0}})$

$\hat{x}$ idempotent, $1 - \hat{x}$ idempotent
$x = x^2$ $x - x^2 = 0$
$x(1-x) = 0$
$\hat{1} - \hat{36} = \widehat{-35} = \hat{28}$

② $m \geq 2$, $(\mathbb{Z}_m, +, \cdot)$

Să demonstrăm că numărul de elemente idempotente este 2^r, unde r = numărul de divizori primi al lui m

---

$m \in \mathbb{N}$

$m = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot p_3^{\alpha_3} \cdot \ldots \cdot p_r^{\alpha_r}$

$\mathbb{Z}_m \simeq \mathbb{Z}_{p_1^{\alpha_1}} \times \mathbb{Z}_{p_2^{\alpha_2}} \times \ldots \times \mathbb{Z}_{p_r^{\alpha_r}}$ pt că $(p_1^{\alpha_1}, \ldots, p_r^{\alpha_r}) = 1$

Din faptul că cele 2 inele sunt izomorfe $\Rightarrow$ nr de elemente idempotente din $\mathbb{Z}_m$ = nr de elemente idempotente din $\mathbb{Z}_{p_1^{\alpha_1}} \times \mathbb{Z}_{p_2^{\alpha_2}} \times \ldots \times \mathbb{Z}_{p_r^{\alpha_r}}$

$(\mathbb{Z}_m, +, \cdot) \cong (\mathbb{Z}_{p_1^{\alpha_1}} \times \mathbb{Z}_{p_2^{\alpha_2}} \times \ldots \times \mathbb{Z}_{p_r^{\alpha_r}}, +, \cdot)$

$\downarrow$

$(a_1, a_2, \ldots, a_r) +/\cdot (b_1, b_2, \ldots, b_r) = (a_1 +/\cdot b_1, a_2 +/\cdot b_2, \ldots, a_r +/\cdot b_r)$

Dacă p este un nr prim, atunci idem $\mathbb{Z}_{p^m}$ sunt doar $\hat{0}$ și $\hat{1}$

idem din $\mathbb{Z}_{p_1^{\alpha_1}} \times \mathbb{Z}_{p_2^{\alpha_2}} \times \ldots \times \mathbb{Z}_{p_r^{\alpha_r}} = (a_1, a_2, \ldots, a_r)$, $a_1, a_2, \ldots, a_r \in \{0, 1\}$

Nr. idem. din $\mathbb{Z}_{p_1^{\alpha_1}} \times \mathbb{Z}_{p_2^{\alpha_2}} \times \ldots \times \mathbb{Z}_{p_r^{\alpha_r}} = 2^r$

$f : \mathbb{Z}_m \to \mathbb{Z}_{p^{\alpha_1}} \times \mathbb{Z}_{p_2^{\alpha_2}} \times \ldots \times \mathbb{Z}_{p_r^{\alpha_r}}$

$f(x) = (a_1, a_2, \ldots, a_r)$

idem din $\mathbb{Z}_{36}$: $\mathbb{Z}_{36} \simeq \mathbb{Z}_{3^2} \times \mathbb{Z}_{2^2}$

idem din $\mathbb{Z}_{3^2} \times \mathbb{Z}_{2^2}$ sunt $\begin{cases} (\bar{0},\bar{\bar{0}}) \\ (\bar{0},\bar{\bar{1}}) \\ (\bar{1},\bar{\bar{0}}) \\ (\bar{1},\bar{\bar{1}}) \end{cases}$

$f(x) = (x \bmod p_1^{\alpha_1}, x \bmod p_2^{\alpha_2}, \dots, x \bmod p_r^{\alpha_r})$

$\hat{12} \in \mathbb{Z}_{36} \simeq (3,0)$ în $\mathbb{Z}_9 \times \mathbb{Z}_4$

$(0,0)$: $\begin{cases} x \bmod 9 = 0 \\ x \bmod 4 = 0 \end{cases}$ o singură soluție în $\mathbb{Z}_{36}$ $x = 0$

$(0,1)$: $\begin{cases} x \bmod 9 = 0 \\ x \bmod 4 = 1 \end{cases}$ ~~o singură soluție~~ $0, 9, 18, 27$ } o singură soluție $x = 9$

$(1,0)$: $\begin{cases} x \bmod 9 = 1 \\ x \bmod 4 = 0 \end{cases}$ $\Rightarrow 1, 10, 19, 28$ } o singură soluție $x = 28$ $(\widehat{1-9})$

$(1,1)$: $\begin{cases} x \bmod 9 = 1 \\ x \bmod 4 = 1 \end{cases}$ o singură soluție $x = 1$

$\mathbb{Z}_{30} \simeq \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_5$

30	2
15	5
3	3
1	

$30 = 2 \cdot 3 \cdot 5$

idempotenți : $(\hat{0},\bar{0},\bar{\bar{0}})$, $(\hat{0},\bar{0},\bar{\bar{1}})$, $(\hat{0},\bar{1},\bar{\bar{0}})$, $(\hat{0},\bar{1},\bar{\bar{1}})$, $(\hat{1},\bar{0},\bar{\bar{0}})$, $(\hat{1},\bar{0},\bar{\bar{1}})$, $(\hat{1},\bar{1},\bar{\bar{0}})$, $(\hat{1},\bar{1},\bar{\bar{1}})$

un elem din $(\hat{0},\bar{1},\bar{4}) \Leftrightarrow \hat{4}$ în $\mathbb{Z}_{30}$

în $\mathbb{Z}_{30}$: $(0,1,0) = \begin{cases} x \bmod 2 = 0 \\ x \bmod 3 = 1 \\ x \bmod 5 = 0 \end{cases}$ $0, 10, 20$ } $\Rightarrow x = 10 \Leftrightarrow (\hat{0},\bar{1},\bar{\bar{0}}) = 10$

Tutoriat 8 - Rezolvări

Inele. Polinoame.

Savu Ioan Daniel, Tender Laura-Maria

- 13 ianuarie 2021 -

Exercițiul 1

Arătați că:

- $\mathbf{Q}/(X^2-1) \cong \mathbf{Q} \times \mathbf{Q}$.
- $\mathbf{Z}/(X^2-X) \cong \mathbf{Z} \times \mathbf{Z}$.
- $\mathbf{Z}/(X^2-1) \ncong \mathbf{Z} \times \mathbf{Z}$.

Rezolvare

- Putem rescrie $\mathbf{Q}/(X^2-1) \cong \mathbf{Q}/((X-1)(X+1))$. Pentru a arăta că $(X-1)$ și $(X+1)$ sunt comaximale, trebuie să arătăm că suma lor generează tot $\mathbf{Q}[X]$. Este suficient să arătâm că suma idealelor conține elementul unitate.

  Observăm că $(X+1)-(X-1)=2$. Înmulțind relația cu $\frac{1}{2}$ (putem face această operație întrucât lucrăm în mulțimea numerelor raționale) obținem 1.

  $\mathbf{Q}/((X-1)(X+1)) \cong \mathbf{Q}/(X-1) \cap (X+1)$
  $\mathbf{Q}/(X-1) \cap (X+1) \cong \mathbf{Q}/(X-1) \times \mathbf{Q}/(X+1)$

  Clasele de echivalență ale lui $\mathbf{Q}/(X-1)$ sunt resturile obținute prin împărțirea oricărui polinom la $X-1$, deci sunt polinoame de grad 0, de forma $\{a \mid a \in \mathbf{Q}\}$, deci $\mathbf{Q}/(X-1) \cong \mathbf{Q}$. Analog pentru $\mathbf{Q}/(X+1) \cong \mathbf{Q}$

  În concluzie, $\mathbf{Q}/(X^2-1) \cong \mathbf{Q} \times \mathbf{Q}$.

- Demonstrația decurge asemănător pentru $\mathbf{Z}/(X^2-X)$, cu observația că $X^2-X=X(X-1)$. Sunt comaximale deoarece $X-(X-1)=1$.

- Spre deosebire de primul subpunct, aici nu mai putem înmulți relația cu $\frac{1}{2}$, întrucât lucrăm cu mulțimea numerelor întregi.

Presupunem că inelul factor ar fi izomorf cu $\mathbf{Z}\times\mathbf{Z}$. Ne uităm la elementele idempotente ale acestor două inele.
Observație: deoarece X^2-1 aparține idealului prin care factorizăm, $\widehat{X^2-1} = \widehat{0}$, de unde $\widehat{X^2} = \widehat{1}$.
Fie $\widehat{a}X + \widehat{b}$ un element indempotent.
Atunci $(\widehat{a}X+\widehat{b})^2 = \widehat{a}X+\widehat{b}$, $\widehat{a}^2X^2+2\widehat{a}\widehat{b}X+\widehat{b}^2 = \widehat{a}X+\widehat{b}$, $\widehat{a}^2+2\widehat{a}\widehat{b}X+\widehat{b}^2 = \widehat{a}X+\widehat{b}$.

$\begin{cases} \widehat{a}^2+\widehat{b}^2 = \widehat{b} \\ 2\widehat{a}\widehat{b} = \widehat{a} \end{cases}$ Singurele soluții ale ecuațiilor în $\mathbf{Z}$ sunt $a = 0$ și $b \in \{0, 1\}$.
Deci obținem 3 elemente indempotente.
În $\mathbf{Z}\times\mathbf{Z}$, sunt 4 elemente idempotente: $\{(0,0),(0,1),(1,0),(1,1)\}$. Având număr diferit de idempotenți, inelele nu sunt izomorfe.

Exercițiul 2

Fie idealul $I = (X^3, X^5)$ al inelului de polinoame $\mathbf{Q}[X]$.

1. Dați un exemplu de polinom care aparține lui I și are 4 termeni nenuli.
2. Dați un exemplu de polinom care nu aparține lui I și are 3 termeni nenuli.
3. Este adevărat că $I = (X^3)$? Dar că $I = (X^5)$? Justificați.
4. Determinați elementele nilpotente din inelul factor $\mathbf{Q}[X]/I$.
5. Determinați elementele idempotente din inelul factor $\mathbf{Q}[X]/I$.
6. Sunt izomorfe inelele $\mathbf{Q}[X]/I$ și $\mathbf{Q}\times\mathbf{Q}$?. Justificați.

Rezolvare

(1) Cum $X^5 \in I$, un astfel de polinom este $X^5+X^6+X^7+X^8$.
(2) Fie $P = X^2+X^1+1$. Presupunem ca $P \in I$. Atunci $P = X^3 * A + X^5 * B$, unde A, B sunt polinoame. Observăm că P poate fi rescris ca $P = X^3 * C$, cu C polinom. Comparând gradele posibile pentru $X^3 * C$ și pentru P, rezultă că P nu poate fi egal cu $X^3 * C$. Contradicție. Prin urmare $P \notin I$ și P are 3 termeni nenuli, deci este un polinom valid pentru cerință.
(3) Orice polinom din I poate fi scris sub forma $X^3 * A + X^5 * B$ cu A, B polinoame. Astfel, aranjând termenii, putem scrie mai departe că un polinom din I este de forma $X^3 * C$ cu C polinom. Putem observa imediat că $I = (X^3)$. De asemenea, din ultima relație, avem că $I \neq (X^5)$ deoarece $I = (X^3)$ și $X^3 \in (X^3)$ dar $X^3 \notin (X^5)$.
(4) Elementele din grupul factor sunt de forma $P = a\widehat{X^2+bX}+c = X(\widehat{b+aX})+c$, cu $a, b, c \in \mathbf{R}$. P este nilpotent daca $\exists n \in \mathbf{N}$ a.î. P^n este multiplu de X^3. Din ultima relație, daca scriem P^n folosind binomul lui Newton observăm ca acesta

este multiplu de $X^3 \iff c = 0$. Prin urmare, există o infinitate de elemente nilpotente, acestea fiind de forma $aX^2 + bX$.
(5) Analog subpunctului anterior, $P = ax^2 \widehat{+ bX} + c$. Trebuie să rezolvăm ecuația $P^2 = P$, de unde $(b^2 + 2ac)X^2 + 2bcX + c^2 = aX^2 + bX + c$. Avem două soluții, și anume 0 și 1 care sunt idempotenții triviali. Prin urmare, idempotenții inelului factor sunt idempotenții triviali.
(6) În $\mathbf{Q} \times \mathbf{Q}$ singurul element nilpotent este $(0, 0)$. În inelul factor, conform (4), există o infinitate de elemente nilpotente. Prin urmare, cele două inele nu pot fi izomorfe.

Exercițiul 3

Fie polinomul $P(X) = X^4 - X^2 + 1$ având rădăcinile complexe $\alpha_1, ..., \alpha_4$.

1. Descompuneți polinomul $P(X)$ în factori ireductibili peste fiecare dintre corpurile $\mathbf{R}$, $\mathbf{Q}$, $\mathbf{Z}_2$, $\mathbf{Z}_3$.
2. Calculați $\alpha_1^5 + ... + \alpha_4^5$.
3. Determinați explicit coeficienții unui polinom nenul care să aibă ca rădăcini pe $2\alpha_1 - 1, ..., 2\alpha_4 - 1$.

Rezolvare

1. $P(X) = X^4 - X^2 + 1 = X^4 + 1 - X^2 = X^4 + 2X^2 + 1 - 3X^2 = (X^2 + 1)^2 - 3X^2 = (X^2 + 1 - \sqrt{3}X)(X^2 + 1 + \sqrt{3}X)$.
   Știm că un polinom este ireductibil peste $\mathbf{C}$, dacă este descompus în polinoame de gradul întâi. Însă, peste $\mathbf{R}$, un polinom este ireductibil dacă este descompus în polinoame de gradul întâi sau în polinoame de gradul al doilea cu $\Delta < 0$.
   Calculăm Δ pentru cele două polinoame de gradul al doilea în care lam descompus pe $P(X)$. $\Delta_1 = \Delta_2 = 3 - 4 = -1 < 0$. Deci forma este ireductibilă peste $\mathbf{R}$.
   Vom arăta că $P(X)$ este ireductibil peste $\mathbf{Q}$. Presupunem că există $\frac{m}{n}, (m, n) = 1, m \in \mathbf{Z}, n \in \mathbf{N}^*$ astfel încât $P(\frac{m}{n}) = 0$, $\frac{m}{n}$ rădăcină a lui $P(X)$.

   TEOREMĂ

   Fie $f \in \mathbb{Z}[X]$, $f = a_0 + a_1X + \ldots + a_nX^n$, $a_0 \neq 0$, $a_n \neq 0$.

   Dacă $\frac{p}{q}$, $(p, q) = 1$, este o rădăcină rațională a polinomului f, atunci p / a_0 și q / a_n.

   Atunci $m|1$ și $n|1$, deci $\frac{m}{n} \in \{+1, -1\}$.
   $P(1) = 1 \neq 0, P(-1) = 1 \neq 0$. Astfel, presupunerea făcută este falsă, deci $P(X)$ este ireductibil peste $\mathbf{Q}$.
   Peste $\mathbf{Z}_2$, $P(X) = X^4 + X^2 + 1 = (X^2 + X + 1)^2.f(X) = (X^2 + X + 1)^2.f$

este ireductibil peste $\mathbf{Z}_2$ întrucât $f(\widehat{0}) = \widehat{1}$ și $f(\widehat{1}) = \widehat{1}$.
Peste $\mathbf{Z}_3$, $P(X) = X^4 + \widehat{2}X + \widehat{1} = (X^2 + \widehat{1})^2$. $X^2 + \widehat{1}$ este ireductibil peste $\mathbf{Z}_3$.

2. $P(\alpha_i) = 0$, $i \in \overline{(1,4)}$. Deci $\alpha_i^4 - \alpha_i^2 + 1 = 0 \iff \alpha_i^4 = \alpha_i^2 - 1$.
$\alpha_i^5 = \alpha_i^3 - \alpha_i$. $\sum_{i=1}^4 \alpha_i^5 = \sum_{i=1}^4 \alpha_i^3 - \sum_{i=1}^4 \alpha_i$
Conform relațiilor lui Viete, $s_1 = p_1 = \sum_{i=1}^4 \alpha_i = 0$. $s_2 = -1, s_3 = 0, s_4 = 1$. Dorim să aflăm $p_3 = \sum_{i=1}^4 \alpha_i^3$. Conform formulelor lui Newton
$p_3 - p_2 s_1 + p_1 s_2 - 3s_3 = 0$
$p_1 = s_1 = 0 \Rightarrow p_3 = 3s_3 = 0$
În concluzie, $\sum_{i=1}^4 \alpha_i^5 = 0$.

3. $2\alpha_i - 1 = \beta_i \iff \alpha_i = \frac{\beta_i + 1}{2}$
Răspunsul este polinomul $Q(X) = P(\frac{X+1}{2}) = (\frac{X+1}{2})^4 - (\frac{X+1}{2})^2 + 1$.

Tutoriat 9
Inele. Polinoame.

Savu Ioan Daniel, Tender Laura-Maria

- 22 ianuarie 2021 -

Exercițiul 1

Fie I submulțimea lui $\mathbf{Z}[X]$ formată din toate polinoamele care au termenul liber divizibil cu 6.
(1) Demonstrați că I este un ideal al lui $\mathbf{Z}[X]$.
(2) Dați un exemplu de polinom de grad 4 din I.
(3) Arătați că $I = (6, X)$. Este I ideal principal? Justificați.
(4) Determinați toți divizorii lui zero din inelul factor $\mathbf{Z}[X]/I$.
(5) Arătați că $\mathbf{Z}[X]/I$ este un inel finit si gasiți-i numărul de elemente.
(6) Are loc izomorfismul de inele unitare $\mathbf{Z}[X]/I \cong \mathbf{Z_2} \times \mathbf{Z_3}$? Justificați.

Exercițiul 2

1. Fie $x, y, z \in \mathbf{C}$ astfel încât $\begin{cases} x+y+z=3 \\ x^2+y^2+z^2=5 \\ x^3+y^3+z^3=6 \end{cases}$

   Calculați $x^5+y^5+z^5$.

2. Aflați polinomul monic $P \in Z[T]$ care are ca rădăcini pe x, y, z.

3. Studiați ireductibilitatea lui P peste $\mathbf{Q}, \mathbf{Z}_2, \mathbf{Z}_5$.

Examen seria 13, 31.01.2020

Exercițiul 3

Fie inelul $Z[X]$ și I submulțimea formată din toate polinoamele care au termenul liber și coeficientul lui X numere divizibile cu 3.
(1) Demonstrați că I este un ideal al lui $Z[X]$.
(2) Determinați un sistem de generatori pentru I. Este I ideal principal?
(3) Este inelul $\mathbf{Z}[X]/I$ integru? Dacă nu, determinați toți divizorii lui zero.
(4) Arătați că $\mathbf{Z}[X]/I$ este un inel finit și găsiț-i numărul n de elemente.
(5) Are loc izomorfismul de inele unitare $\mathbf{Z}[X]/I \cong \mathbf{Z_n}$?

Exercițiul 1

I submulțime pentru $\mathbb{Z}[X]$ a.î. polinoamele din I au termenul liber $\vdots 6$.

(1) I este ideal pt. $\mathbb{Z}[X]$ inel de polinoame

I este ideal $\Leftrightarrow$

1. $(\forall)\ x, y \in I,\ x-y \in I$
2. $(\forall)\ x \in I$ și $(\forall)\ a \in \mathbb{Z}[X] \Rightarrow a \cdot x \in I$

$P_1 = 6k_1 + a_1 \cdot X + a_2 \cdot X^2 + \dots + a_n X^n$

$P_2 = 6k_2 + b_1 \cdot X + b_2 \cdot X^2 + \dots + b_m \cdot X^m$

$P_1 - P_2 = 6(k_1 - k_2) + (a_1 - b_1) \cdot X + \dots$

$= \underset{\vdots 6}{6(k_1 - k_2)} + X \cdot P_3 \in I$

2. $P_0 = a_0 + a_1 \cdot X + \dots + a_k X^k \in \mathbb{Z}[X]$

$P_1 = 6 b_0 + b_1 \cdot X + \dots + b_m \cdot X^m \in I$

$P_0 \cdot P_1 = 6 b_0 \cdot P_0 + \underbrace{b_1 \cdot X \cdot P_0 + \dots + b_m \cdot X^m \cdot P_0}$

$P_0 \cdot P_1 = 6 b_0 \cdot P_0 + X \cdot P_3$

$P_0 \cdot P_1 = \underset{\vdots 6}{6 \cdot b_0 \cdot a_0} + X(P_4) + X P_3 \in I$

$1, 2 \Rightarrow$ I este ideal bilateral

(2) Polinom de gr 4 din I

$6 + X^4 \in I$ deoarece $6 \vdots 6$

$6 + X^4$ are grad 4

(3) Arătați că $I = (6, X)$. Este I ideal principal?

(1) $I \subseteq (6, X)$

$(6, X) = \{ 6 \cdot P_1 + X \cdot P_2 \mid P_1, P_2 \in \mathbb{Z}[X] \}$

Fie $P_0 = 6 \cdot a_0 + a_1 \cdot X + a_2 \cdot X^2 + \dots + a_m \cdot X^m \in I$

$a_0, a_1, a_2, \dots, a_m \in \mathbb{Z}$

Trebuie să rezolvăm ecuația

$P_0 = 6 \cdot P_1 + X P_2$, necunoscute: P_1, P_2

$6 \cdot a_0 + a_1 \cdot X + a_2 \cdot X^2 + \dots + a_m \cdot X^m = 6 \cdot P_1 + X \cdot P_2$

$6 \cdot a_0 + X(a_1 + a_2 X + \dots + a_m X^{m-1}) = 6P_1 + X P_2$

o soluție este $\begin{cases} P_1 = a_0 \\ P_2 = a_1 + a_2 X + \dots + a_m X^{m-1} \end{cases}$

$\Rightarrow$ ecuația $6P_1 + X \cdot P_2 = P_0$ are soluție

pt. $(\forall)\ P_0 \in I \Rightarrow I \subseteq (6, X)$

(2) „$\supseteq$" pt. $(\forall)\ P \in (6, X) \in I$

$P = 6 \cdot P_1 + X P_2 = 6(a_0 + a_1 X + \dots) + X(b_0 + b_1 \cdot X + \dots) =$

$= \underset{\vdots 6}{6 \cdot a_0} + X(a_1 + b_1 + (a_2 + b_2) X + \dots) \in I$

$\Rightarrow (6, X) \subseteq I$

(1)(2) $\Rightarrow I = (6, X)$

$(6, X)$ ideal principal? $\approx$ „grup ciclic"

$(6, X) \overset{?}{=} (Y)$

$X = P \cdot 6 \sim \frac{1}{6} \cdot X \notin \mathbb{Z}[X]$

$6 = P \cdot X \qquad \frac{1}{X}$

Presupunem că $(6, X)$ este principal $\Rightarrow$ este generat de un singur elem.

$(6, X) = (Y)$

$6 \in (6, X)$

$P \in \mathbb{Z}[X]$ a.î. $6 = Y \cdot P$, grad 0

$Y = \{1, 2, 3, 6\}$

$(1) \ni 1$

$(6, X) \not\ni 1$

Analog pentru $Y \in \{2, 3\}$

$\Rightarrow Y = 6$

$(6, X) = (6)$

$X \in (6, X) \Rightarrow 6 \cdot 0 + 1 \cdot X$

$6 \cdot P = X \Rightarrow P = \frac{1}{6} \cdot X \notin \mathbb{Z}[X]$

$(6, X) \neq (6)$

$Y \in \emptyset \Rightarrow (6, X)$ nu este principal

Toți divizorii lui 0 în inelul factor $\mathbb{Z}[X]/I$

$\mathbb{Z}[X]/(6, X) \simeq \dfrac{\mathbb{Z}[X]/(6)}{(6, X)/(6)} \cong \mathbb{Z}_6[X]/(X) = \{ a \mid a \in \mathbb{Z}_6 \}$

$\mathbb{Z}[X]/I \cong \dfrac{\mathbb{Z}[X]/J}{I/J}$

J, I ideale $J \subseteq I$

$\mathbb{Z}[X]/(k, P) \simeq \mathbb{Z}_k[X]/P$

Divizorii lui 0:

Sunt elem x ∃ $y \neq 0$ $x \cdot y = 0$

Pt. $\mathbb{Z}_6$ divizorii lui 0 sunt:

$\{\hat{0}, \hat{2}, \hat{3}, \hat{4}\}$

(5) $\mathbb{Z}[X]/I \cong \mathbb{Z}_6 \Rightarrow$ este finit și are 6 elemente

(6) Are loc izomorfismul de inele unitare $\mathbb{Z}[X]/I \cong \mathbb{Z}_2 \times \mathbb{Z}_3$

$\Leftrightarrow \mathbb{Z}_6 \cong \mathbb{Z}_2 \times \mathbb{Z}_3$?

$\mathbb{Z}_6 = \{\hat{0}, \hat{1}, \hat{2}, \hat{3}, \hat{4}, \hat{5}\}$ — $6, 3, 2, 3, 6$

$\mathbb{Z}_2 \times \mathbb{Z}_3 = \{(\hat{0}, \hat{0}), (\hat{0}, \hat{1}), (\hat{0}, \hat{2}), (\hat{1}, \hat{0}), (\hat{1}, \hat{1}), (\hat{1}, \hat{2})\}$ — $3, 3, 2, 6, 6$

$\hat{0}$	$\hat{1}$	$\hat{2}$	$\hat{}$	$\hat{4}$	$\hat{5}$
$(\hat{0}, \hat{0})$	$(\hat{0}, \hat{1})$	$(\hat{0}, \hat{2})$	$(\hat{1}, \hat{0})$	$(\hat{1}, \hat{1})$	$(\hat{1}, \hat{2})$

$(1, 1)$	$(0, 2)$	$(1, 0)$	$(0, 1)$	$(1, 2)$	$(0, 0)$
1	2	3	4	5	$\hat{0}$

$\mathbb{Z}_{p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \dots \cdot p_m^{\alpha_m}} \cong \mathbb{Z}_{p_1^{\alpha_1}} \times \mathbb{Z}_{p_2^{\alpha_2}} \times \dots \times \mathbb{Z}_{p_m^{\alpha_m}}$

$\mathbb{Z}_m$?

Ex: $\mathbb{Z}_8 \not\cong \mathbb{Z}_4 \times \mathbb{Z}_2$

$x, y, z \in \mathbb{C}$ $\begin{cases} x+y+z = 3 = p_1 \\ x^2+y^2+z^2 = 5 = p_2 \\ x^3+y^3+z^3 = 6 = p_3 \end{cases}$

a) $x^5+y^5+z^5 = ? = p_5$

Fie x, y, z sunt rădăcinile unui polinom P

$p_i = \alpha_1^i + \alpha_2^i + \dots + \alpha_n^i$, $\alpha_1, \alpha_2, \dots, \alpha_n$ rădăcini pt. P

P are gradul 3 $\qquad$ 3 rădăcini

s_1, s_2, s_3

$s_1 = x+y+z = p_1$

$s_2 = xy+xz+yz$

$s_3 = xyz$

$(x+y+z)^2 = x^2+y^2+z^2 + 2(xy+xz+yz)$

$p_2 - p_1 s_1 + 2s_2 = 0$

$5 - 9 + 2s_2 = 0$

$s_2 = 2$

$p_3 - p_2 s_1 + p_1 s_2 - 3s_3 = 0$

$6 - 5 \cdot 3 + 3 \cdot 2 - 3s_3 = 0$

$s_3 = -1$

$p_4 - p_3 s_1 + p_2 s_2 - p_1 s_3 = 0$

$p_4 - 18 + 10 + 3 = 0$

$p_4 = 5.$

$p_5 - p_4 s_1 + p_3 s_2 - p_2 s_3 = 0$

$p_5 - 15 + 12 + 5 = 0$

$p_5 = -2.$

$x^5+y^5+z^5 = -2$

b) $s_1 = 3 \quad s_2 = 2 \quad s_3 = -1$

$T^3 + aT^2 + bT + c$

$T^3 - s_1 T^2 + s_2 T$

$T^3 - 3T^2 + 2T + 1 \in \mathbb{Z}[T]$

are ca rădăcini x, y, z

c) ireductibilitate peste $\mathbb{Q}$, $\mathbb{Z}_2$ și $\mathbb{Z}_5$

are grad 3, dacă ar fi reductibil, s-a descompune în un polinom de gr. 1 și un polinom de gr. 2

$\frac{m}{n}$ $(m,n) = 1$ $m \in \mathbb{Z}, n \in \mathbb{N}^*$

$P\left(\frac{m}{n}\right) = 0 \quad m \mid 1 \quad n \mid 1$

$\frac{m}{n} \in \{\pm 1\}$ $\quad P(1) = 1 \neq 0$

$P(-1) = -3 \neq 0$

Nu există o rădăcină rațională a lui P, deci e ireductibil peste $\mathbb{Q}$.

$P(T) = T^3 - 3T^2 + 2T + 1.$

în $\mathbb{Z}_2$: $P(T) = T^3 + T^2 + \hat{1}$ se descompune într-un polinom gr 1 și un polinom de gr. 2.

$P(\hat{0}) = \hat{1} \quad P(\hat{1}) = \hat{1}$

Nu găsim rădăcină în $\mathbb{Z}_2$

$\Rightarrow$ ireductibil peste $\mathbb{Z}_2$

$\mathbb{Z}_5$: $P = T^3 + \hat{2}T^2 + \hat{2}T + \hat{1}$

$P(\hat{0}) \quad P(\hat{1}) \quad P(\hat{2}) \quad P(\hat{3}) \quad P(\hat{4})$

$P(-\hat{2}) \quad P(-\hat{1})$

$P(\hat{4}) = P(-\hat{1}) = \hat{0}$

$P = T^3 + T^2 + T^2 + T^2 + T + \hat{1}$

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

forma ireductibilă $\rightarrow P = (T+\hat{1})(\underbrace{T^2+T+\hat{1}}) - s_3.$

$Q = T^2 + T + \hat{1}$ $\rightarrow$ ireductibile

$Q(\hat{0}) = \hat{1}$

$Q(\hat{1}) = \hat{3}$

$Q(\hat{2}) = \hat{2}$

$Q(\hat{3}) = Q(-\hat{2}) = \bar{3}$

$Q(-\hat{1}) = Q(\hat{4}) = \hat{1}$

n-ciclu σ a.î. $\sigma^k = \tau$ 3 cicli de lungime 2

a. $\tau = (1\,2)(3\,4)(5\,6)(7\,8)(9\,10)$, $n \geq 10$.

$(a_1\ a_2 \ldots a_m)^d$ $m d | m \Rightarrow$

$\Rightarrow$ d cicli de lungime m/d

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

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

b) $\tau = (1\,2)(3\,4\,5)$, $n \geq 5$

1) în τ nu obținem cicli de aceeași lungime

2) Deoarece σ este un 5-ciclu acesta nu se sparge când este ridicat la o putere

(3) $\mathbb{Z}[X]$-inel, I-submulțimea formată din toate pol care au term. liber și coef lui $X \vdots 3$

a) I ideal $\mathbb{Z}[X]$

(1) Luăm P_1 și $P_2 \in I$ (Analog ca la Ex 1)

$P_1 - P_2 \in I$

(2) Fie $P_1 \in I$ și $P_2 \in \mathbb{Z}$ $\Rightarrow$ analog Ex 1

$P_1 \cdot P_2 \in I$

(1), (2) $\Rightarrow I$ ideal

Scanned with CamScanner

b) determ. un sist. de generatori pt I

$I = (P_1, P_2, P_3, \dots, P_k)$

$\{P_1 \cdot M_1 + P_2 \cdot M_2 + \dots + P_k \cdot M_k \mid M_1, M_2, \dots, M_k \text{ (polinoame) } \in \mathbb{Z}[X]\}$

$3 \cdot a_0 + 3a_1 X + a_2 X^2 + \dots + a_n X^n = 3(a_0 + a_1 X) + X^2 \underbrace{(a_2 + a_3 X + \dots + a_n X^{n-2})}$

$I = (3, X^2) \to$ analog ca la Ex 1

I este ideal principal?

$(3, X^2) \neq (\cdot) \to$ Analog Ex 1

c) $\mathbb{Z}[X]/I$ integru?

$\mathbb{Z}[X]/_I = \mathbb{Z}[X]/_{(3,X^2)} = \mathbb{Z}[X]/_3 \Big/ {}_{(3,X^2)/_3} = \mathbb{Z}_3[X]/_{(X^2)}\ \{a \cdot X + b \mid a, b \in \mathbb{Z}_3\}$

$(ax+b)(cx+d) = 0,\ a, b, c, d \in \mathbb{Z}_3$

~~$ac\, X + bd$~~

$\underset{\hat{0}}{a \cdot c} \cdot \underset{\hat{0}}{x^2} + \underset{\hat{0}}{a \cdot d} \cdot x + b c \cdot x + b \cdot d = \hat{0}$

$\begin{cases} ~~a \cdot c = 0~~ \\ bd = \hat{0} & \text{în } \mathbb{Z}_3 \\ a \cdot d + b \cdot c = \hat{0} \end{cases}$

~~$b = \hat{0} \Rightarrow a \cdot d = \hat{0}$, $a = \hat{0} \Rightarrow d$ poate fi oricât~~

~~$a \cdot X + b = 0$~~

~~$b \neq \hat{0} \Rightarrow a \cdot d = \hat{0}$~~

~~a poate fi oricât~~

~~$d = \hat{0}$~~

~~$a \cdot X$~~

~~$\hat{0}, \hat{X}, \hat{2X}$ ... [illegible] ... integru~~

$b = \hat{0} \Rightarrow d = \hat{0}$

$d = \hat{0} \Rightarrow b = \hat{0}$

$\Rightarrow \{\hat{0}, a\hat{X}\}$

$\Rightarrow \{\hat{0}, \hat{X}, \hat{2X}\}$

d) $\mathbb{Z}[x]/I$ este corp finit

$\{ax+b \mid a,b \in \mathbb{Z}_3\}$

$|\mathbb{Z}[x]/I| = 9 = n$

e) $\mathbb{Z}[x]/I \cong \mathbb{Z}_9$?

$\{\hat{0}, \hat{x}, \widehat{2x}\}$ $\{0, 3, 6\}$

div lui 0

$0x+0$ $\quad x+0 \to 3$ $\quad 2x+0 \to 3$

$0x+1 \to 3$ $\quad x+1 \to 3$ $\quad 2x+1 \to 3$

$0x+2 \to 3$ $\quad x+2 \to 3$ $\quad 2x+2 \to 3$

$\mathbb{Z}[x]/I \not\cong \mathbb{Z}_9$