

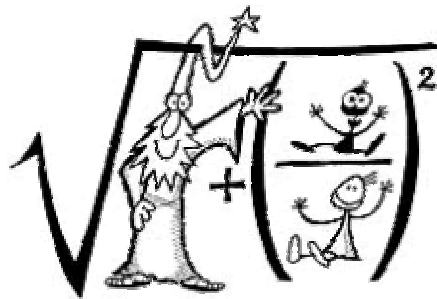
DUMITRU BUȘNEAG

FLORENTINA CHIRTEȘ DANA PICIU

PROBLEME

de

ALGEBRĂ



Dumitru BUȘNEAG

Florentina CHIRTEȘ

Dana PICIU

PROBLEME de ALGEBRĂ

Dumitru BUȘNEAG

Florentina CHIRTEȘ

Dana PICIU

PROBLEME

de

ALGEBRĂ

**Editura UNIVERSITARIA
CRAIOVA
2002**

Referenți științifici:

Prof.univ.dr.Constantin Năstăsescu,Universitatea Bucuresti

Membru corespondent al Academiei Române

Prof.univ.dr. Constantin Niță,Universitatea București

Prof.univ.dr. Alexandru Dincă,Universitatea Craiova

© 2002 EUC – CRAIOVA

All rights reserved. No part of this publication may be reproduce, stored in a retrieval system, or transmitted, in any forms or by any means, electronic, mechanical, photocopying, recording, or other wise, without the prior written permission of the publisher.

Tehnoredactare computerizată : Dana Piciu, Florentina Chirteș

Copertă: Cătălin Bușneag

Descrierea CIP a Bibliotecii Naționale

Dumitru Bușneag (coordonator),

Probleme de Algebră

Bun de tipar: 20.02.2002

Tipografia Universității din Craiova, Strada, Al. Cuza, nr.13

Craiova, România

Published in Romania by:

EDITURA UNIVERSITARIA CRAIOVA

ISBN: 973 – 8043 – 189 – 9

CUPRINS

Prefață	i
Index de notații și abrevieri	ii
Partea 1 : Enunțurile problemelor	1
§1. Operații algebrice. Semigrupuri. Monoizi. Morfisme de monoizi	1
§2. Grup. Subgrup. Subgrup generat de o mulțime. Calcule într-un grup. Grupuri de permutări	6
§3. Teorema lui Lagrange. Ordinul unui element. Indicele unui subgrup. Subgrupuri normale	17
§4. Morfisme și izomorfisme de grupuri. Grupuri factor. Teoremele de izomorfism pentru grupuri	24
§5. Produse directe de grupuri	36
§6. Inel. Subinel. Exemple. Calcule într-un inel. Elemente inversabile. Divizori ai lui zero. Elemente idempotente. Elemente nilpotente. Produse directe de inele	39
§7. Morfisme și izomorfisme de inele	50
§8. Ideale. Latticea idealelor unui inel comutativ. Anulatorul și radicalul unui inel. Factorizarea unui inel printr-un ideal bilateral. Ideale prime. Ideale maximale	54
§9. Corp. Subcorp. Caracteristica unui corp. Morfisme și izomorfisme de corpuri	61
§10. Inele de polinoame	70
Partea 2 : Soluțiile problemelor	79
§1. Operații algebrice. Semigrupuri. Monoizi. Morfisme de monoizi	79
§2. Grup. Subgrup. Subgrup generat de o mulțime. Calcule într-un grup. Grupuri de permutări	90
§3. Teorema lui Lagrange. Ordinul unui element. Indicele unui subgrup. Subgrupuri normale	119

§4. Morfisme și izomorfisme de grupuri. Grupuri factor. Teoremele de izomorfism pentru grupuri	131
§5. Produse directe de grupuri	163
§6. Inel. Subinel. Exemple. Calcule într-un inel. Elemente inversabile. Divizori ai lui zero. Elemente idempotente. Elemente nilpotente. Produse directe de inele	175
§7. Morfisme și izomorfisme de inele	208
§8. Ideale. Latticea idealelor unui inel comutativ. Anulatorul și radicalul unui inel. Factorizarea unui inel printr-un ideal bilateral. Ideale prime. Ideale maximale	225
§9. Corp. Subcorp. Caracteristica unui corp. Morfisme și izomorfisme de corpuri	244
§10. Inele de polinoame	276
Bibliografie	310

Prefață

Lucrarea de față este destinată în principal seminarizării cursurilor de algebră legate de structurile algebrice fundamentale (grup, inel, corp). Ea cuprinde probleme legate de grupuri, inele, corpuri și inele de polinoame.

Această lucrare este utilă în primul rând studenților de la facultățile de matematică - informatică dar și celor de la facultățile tehnice. Ea poate fi însă utilă în egală măsură atât profesorilor de matematică din învățământul preuniversitar (în procesul didactic și de perfecționare), ca și elevilor din ultima clasă de liceu participanți la tradiționalele concursuri de matematici de la noi.

Pentru anumite aspecte teoretice recomandăm cititorilor lucrările [4, 12, 13, 18, 19, 20, 21].

Atât tehnoredactarea cât și corectura aparțin autorilor.

Craiova, 20.02.2002

Autorii

Index de notații și abrevieri

a.î.	: astfel încât
$\Rightarrow(\Leftrightarrow)$: implicația (echivalența) logică
$(\forall) ((\exists))$: cuantificatorul universal (existențial)
$x \in A$: elementul x aparține mulțimii A
$A \subseteq B$: mulțimea A este inclusă în mulțimea B
$A \subsetneq B$: mulțimea A este inclusă strict în mulțimea B
$A \cap B$: intersecția mulțimilor A și B
$A \cup B$: reuniunea mulțimilor A și B
$A \setminus B$: diferența mulțimilor A și B
$A \Delta B$: diferența simetrică a mulțimilor A și B
$P(M)$: familia submulțimilor mulțimii M
$C_M A$: complementara în raport cu M a mulțimii A
$A \times B$: produsul cartezian al mulțimilor A și B
$ M $ (sau card M)	: cardinalul mulțimii M (dacă M este finită $ M $ reprezintă numărul elementelor lui M)
1_A	: funcția identică a mulțimii A
$\mathbb{N}(\mathbb{N}^*)$: mulțimea numerelor naturale (nenule)
$\mathbb{Z}(\mathbb{Z}^*)$: mulțimea numerelor întregi (nenule)
$\mathbb{Q}(\mathbb{Q}^*)$: mulțimea numerelor raționale (nenule)
\mathbb{Q}_+^*	: mulțimea numerelor raționale strict pozitive
$\mathbb{R}(\mathbb{R}^*)$: mulțimea numerelor reale (nenule)
\mathbb{R}_+^*	: mulțimea numerelor reale strict pozitive
$\mathbb{C}(\mathbb{C}^*)$: mulțimea numerelor complexe (nenule)
δ_{ij}	: simbolul lui Kronecker (adică 1 pentru $i = j$ și 0 pentru $i \neq j$)
$ z $: modulul numărului complex z
U_n	: mulțimea rădăcinilor complexe de ordin n ale unității
T	: mulțimea numerelor complexe de modul 1
$m \mid n$: numărul întreg m divide numărul întreg n
$[m, n]$: cel mai mic multiplu comun al numerelor naturale m și n
c.m.m.m.c.	: cel mai mic multiplu comun
(m, n)	: cel mai mare divizor comun al numerelor naturale m și n

	n
c.m.m.d.c.	: cel mai mare divizor comun
$m \equiv n \pmod{p}$: m este congruent cu n modulo p (adică $p \mid m-n$)
\mathbb{Z}_n	: mulțimea claselor de resturi modulo numărul natural n ($n \geq 2$)
$M_n(K)$: mulțimea matricelor pătratice de ordin n cu elemente din mulțimea K
$M_{m,n}(K)$: mulțimea matricelor cu m linii și n coloane, cu elemente din mulțimea K
$I_n(O_n)$: matricea unitate (nulă) de ordin n ($n \geq 2$)
$\text{Tr}(M)$: urma matricei pătratice M
$\det(M)$: determinantul matricei pătratice M
$U(M, \circ)$: mulțimea elementelor inversabile din monoidul (M, \circ)
$\varphi(n)$ ($n \in \mathbb{N}^*$)	: numărul numerelor naturale mai mici decât n și prime cu n (φ poartă numele de <i>indicatorul lui Euler</i>)
$GL_n(K)$: grupul liniar de grad n peste corpul K
$SL_n(K)$: grupul special de grad n peste corpul K
$\Sigma(X)$: grupul simetric al mulțimii X (adică grupul funcțiilor bijective $f: X \rightarrow X$ relativ la compunerea funcțiilor)
S_n	: grupul simetric al unei mulțimi cu n elemente
A_n	: grupul altern de grad n
D_n	: grupul diedral de grad n
DI_n	: grupul dicitic de grad n
Q	: grupul quaternionilor
Q_n	: grupul generalizat al quaternionilor
$o(g)$: ordinul elementului g din grupul G
$H \leq G$: H este subgrup al grupului G
$H \trianglelefteq G$: H este subgrup normal al grupului G
$ G:H $: indicele subgrupului H în grupul G
$(G/H)_d$: mulțimea claselor la dreapta ale grupului G relative la subgrupul H al grupului G
$(G/H)_s$: mulțimea claselor la stânga ale grupului G relative la subgrupul H al grupului G
G/H	: grupul factor al grupului G prin subgrupul său normal H
$L(G)$: mulțimea subgrupurilor grupului G
$L_0(G)$: mulțimea subgrupurilor normale ale grupului G
$\langle X \rangle$: subgrupul generat de mulțimea X în grupul G ($X \subseteq G$)
$H \vee K$: subgrupul generat de $H \cup K$ în grupul G ($H, K \leq G$)
$H \cdot K$: mulțimea elementelor de forma $h \cdot k$ cu $h \in H$ și $k \in K$ ($H, K \leq G$)
$H \approx K$: grupurile H și K sunt izomorfe

$H \cong K$: grupurile H și K nu sunt izomorfe
$\text{Hom}(G_1, G_2)$: mulțimea morfismelor de grup de la grupul G_1 la grupul G_2
$\text{Aut}(G)$: mulțimea automorfismelor grupului G
$\text{Inn}(G)$: mulțimea automorfismelor interioare ale grupului G
$C_M(x)$: centralizatorul în monoidul M al elementului x (adică mulțimea elementelor lui M ce comută cu x)
$Z(M)$: centrul monoidului M (mulțimea elementelor lui M ce comută cu oricare element al lui M)
$N_G(H)$: normalizatorul lui H în G (adică mulțimea elementelor $x \in G$ pentru care $xH = Hx$, $H \subseteq G$)
$[x, y]$: $x^{-1}y^{-1}xy$ (comutatorul elementelor x și y din grupul G)
$\text{ch } a = (e^a + e^{-a}) / 2$: cosinus hiperbolic
$\text{sh } a = (e^a - e^{-a}) / 2$: sinus hiperbolic
$\text{Car}(A)$: caracteristica inelului A
$U(A)$: grupul unităților inelului A
$Z(A)$: centrul inelului A
$N(A)$: mulțimea elementelor nilpotente ale inelului A
$\text{Id}(A)$: mulțimea idealelor inelului comutativ A
A / I	: inelul factor al lui A prin idealul I
$J(A)$: radicalul Jacobson al inelului comutativ A
$r(I)$: radicalul idealului I
$\text{Ann}(I)$: anulatorul idealului I
(M)	: idealul generat de submulțimea M din inelul A
$[x, y]$: comutatorul elementelor x și y din inelul A (adică $xy - yx$)
$A[[X]]$: inelul seriilor formale peste inelul A
$A[X]$: inelul polinoamelor într-o nedeterminată cu coeficienți în inelul comutativ A
$A[X_1, \dots, X_n]$: inelul polinoamelor în nedeterminatele X_1, \dots, X_n ($n \geq 2$) cu coeficienți din inelul comutativ A
\tilde{f}	: funcția polinomială atașată polinomului $f \in A[X]$

Partea 1: Enunțurile problemelor

§1. Operații algebrice. Semigrupuri. Monoizi. Morfisme de monoizi.

1.1. Fie M o mulțime cu n elemente.

(i) Câte operații algebrice se pot defini pe M ?

(ii) Câte dintre acestea sunt comutative?

(iii) Câte dintre acestea admit element neutru?

(iv) Să se arate că numărul operațiilor algebrice ce se pot defini

pe M care sunt în același timp comutative și cu element neutru este $\frac{n^2-n+2}{n-2}$.

1.2. Pe \mathbb{R} considerăm operația algebrică :

$$x \circ y = xy + ax + by + c \quad (a, b, c \in \mathbb{R}).$$

(i) Pentru ce valori ale lui a, b, c operația ” \circ ” este asociativă?

(ii) Să se demonstreze că operația ” \circ ” este asociativă \Leftrightarrow are element neutru ;

(iii) În ipoteza că operația ” \circ ” este asociativă, să se pună în evidență $U(\mathbb{R}, \circ)$.

1.3. Pe \mathbb{Z} considerăm operația algebrică :

$$x \circ y = axy + b(x + y) + c \quad (a, b, c \in \mathbb{Z}).$$

Să se demonstreze că:

(i) Operația ” \circ ” este asociativă $\Leftrightarrow b^2 - b - ac = 0$;

(ii) Dacă $b^2 - b - ac = 0$, atunci operația ” \circ ” are element neutru dacă și numai dacă $b \mid c$.

1.4. Fie M o mulțime nevidă iar ” \circ ” o operație algebrică asociativă pe M . Să se demonstreze că :

$$H = \{a \in M : (x \circ a) \circ y = x \circ (a \circ y), \text{ pentru orice } x, y \in M\}$$

este parte stabilă a lui M în raport cu operația dată.

1.5. Fie M o mulțime nevidă. Pe M se definește o operație algebrică asociativă. Arătați că dacă M este finită și există $a \in M$ a.î. funcția $f: M \rightarrow M$, $f(x) = xa$ este injectivă, atunci (M, \cdot) este monoid.

1.6. Fie S un semigrup finit și $a \in S$. Să se arate că există $m \in \mathbb{N}^*$ a.î. a^m este idempotent.

1.7. Fie A o mulțime nevidă și o operație algebrică asociativă pe A cu proprietatea că există $n \in \mathbb{N}^*$ a.î. $x^n y^n = yx$, pentru orice $x, y \in A$. Arătați că operația dată este comutativă.

1.8. Fie $M \neq \emptyset$ și o operație algebrică asociativă cu proprietatea că există $n \in \mathbb{N}^*$ a.î. $(xy)^n = yx$, pentru orice $x, y \in M$. Atunci operația algebrică este comutativă.

1.9. Pe mulțimea M se definește o operație algebrică cu proprietățile:

1) $x^2 = x$, pentru orice $x \in M$;

2) $(xy)z = (yz)x$, pentru orice $x, y, z \in M$.

Să se arate că operația este asociativă și comutativă.

1.10. Pe mulțimea S se definește o operație algebrică asociativă cu următoarele proprietăți:

1) $x^3 = x$, pentru orice $x \in S$

2) $xy^2x = yx^2y$, pentru orice $x, y \in S$.

Să se arate că operația este comutativă.

1.11. Fie $\mathbb{Z}[i] = \{x+yi : x, y \in \mathbb{Z}, i \in \mathbb{C}, i^2 = -1\}$. Să se demonstreze că $(\mathbb{Z}[i], \cdot)$ este monoid comutativ.

Să se determine $U(\mathbb{Z}[i], \cdot)$.

1.12. Fie d un număr natural liber de pătrate ($d \geq 2$) iar $\mathbb{Z}[\sqrt{d}] = \{x+y\sqrt{d} \mid x, y \in \mathbb{Z}\}$. Definim $N : \mathbb{Z}[\sqrt{d}] \rightarrow \mathbb{Z}[\sqrt{d}]$ prin $N(x+y\sqrt{d}) = x^2 - dy^2$, pentru orice $x, y \in \mathbb{Z}$. Să se demonstreze că $(\mathbb{Z}[\sqrt{d}], \cdot)$ este monoid comutativ iar $z \in U(\mathbb{Z}[\sqrt{d}], \cdot) \Leftrightarrow N(z) \in \{\pm 1\}$.

1.13. Să se demonstreze că $U(\mathbb{Z}[\sqrt{2}], \cdot)$ este o mulțime infinită.

1.14. Fie n un număr natural, $n \geq 2$ și $M_n = \{x \in \mathbb{Z} : (n, x) \neq 1\}$.

Să se demonstreze că M_n este parte stabilă a lui $(\mathbb{Z}, +) \Leftrightarrow n$ este o putere naturală a unui număr prim.

1.15. Fie $M \subseteq \mathbb{C}$ parte stabilă a lui $(\mathbb{C}, +)$ a.î. $\{z \in \mathbb{C} : |z| = 1\} \subseteq M$. Să se demonstreze că $M = \mathbb{C}$.

1.16. Pe mulțimea $M = \mathbb{Z} \times \mathbb{Z}$ definim operația algebrică :

$$(x_1, y_1) \circ (x_2, y_2) = (x_1 x_2, x_2 y_1 + y_2).$$

Să se demonstreze că (M, \circ) este monoid iar apoi să se determine $U(M, \circ)$.

1.17. Fie $M = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a, b, c, d \in \mathbb{Z} \text{ și } a + b = c + d \right\}$.

Să se demonstreze că M împreună cu înmulțirea matricelor este monoid iar apoi să se pună în evidență unitățile monoidului M .

1.18. Fie $A = \{f : \mathbb{N}^* \rightarrow \mathbb{C}\}$. Pe A definim operația algebrică $*$ astfel:
 $(f * g) = \sum_{d|n} f(n)g(n/d)$.

Să se demonstreze că $(A, *)$ este monoid comutativ și $f \in U(A, *) \Leftrightarrow f(1) \neq 0$.

Observație. Funcțiile din A se numesc *funcții aritmetice* iar operația algebrică $*$ poartă numele de *produs de convoluție* sau *produs Dirichlet*.

1.19. Fie (M, \cdot) un monoid și 1 elementul său neutru.

(i) Să se arate că dacă M este mulțime finită, atunci nu există $a, b \in M$ a.î. $ab = 1$ și $ba \neq 1$;

(ii) Să se dea un exemplu de două aplicații $f, g : \mathbb{N} \rightarrow \mathbb{N}$ a.î. $f \circ g = 1_{\mathbb{N}}$ și $g \circ f \neq 1_{\mathbb{N}}$;

(iii) Fie a și b în M a.î. $ab = 1$ și $ba \neq 1$. Să se arate că dacă $b^n a^m = b^q a^p$ cu $m, n, p, q \in \mathbb{N}^*$, atunci $n = q$ și $m = p$.

1.20. Să se demonstreze că dacă $M \subseteq \mathbb{C}$ este parte stabilă relativ la operațiile de adunare și înmulțire a numerelor complexe și $\mathbb{R} \subseteq M \subseteq \mathbb{C}$, atunci $M = \mathbb{R}$ sau $M = \mathbb{C}$.

1.21. Pentru monoidul (M, \cdot) definim

$$Z(M) = \{x \in M \mid xy = yx, \text{ pentru orice } y \in M\}.$$

Să se demonstreze că $Z(M)$ este submonoid al lui M .

Observație. $Z(M)$ poartă numele de *centrul* monoidului M .

1.22. Fie $n \in \mathbb{N}$, $n \geq 2$. Să se demonstreze că

$$Z(M_n(\mathbb{C}), \cdot) = \{a \cdot I_n \mid a \in \mathbb{C}\}.$$

1.23. Fie matricea $A = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} \in M_2(\mathbb{C})$.

- (i) Să se determine $X \in M_2(\mathbb{C})$ a.î. $AX = XA$;
- (ii) Să se rezolve în $M_2(\mathbb{C})$ ecuația $X^n = A$ ($n \in \mathbb{N}, n \geq 2$).

1.24. Fie $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\mathbb{R})$ a.î. $a+d > 2$ și $\det(A) = 1$.

Să se demonstreze că $A^n \neq I_2$, pentru orice $n \in \mathbb{N}, n \geq 1$.

1.25. Fie $n \in \mathbb{N}, n \geq 2$ și $A, B \in M_n(\mathbb{C})$ a.î. $A + B = AB$.
Să se demonstreze că $AB = BA$.

1.26. Fie $n \in \mathbb{N}, n \geq 2$ și $A, B \in M_n(\mathbb{C})$.
Să se demonstreze că

$$I_n - AB \in U(M_n(\mathbb{C}), \cdot) \Leftrightarrow I_n - BA \in U(M_n(\mathbb{C}), \cdot).$$

1.27. Fie S un semigrup. Să se arate că există un monoid M și un morfism injectiv de semigrupuri $f : S \rightarrow M$.

1.28. Fie M_1, M_2 monoizi, $f, g : M_1 \rightarrow M_2$ două morfisme de monoizi, $M_{f,g} = \{x \in M_1 : f(x) = g(x)\}$ iar $i : M_{f,g} \rightarrow M_1$ morfismul incluziune.

Să se demonstreze că :

(i) $M_{f,g}$ este submonoid al lui M_1 iar $f \circ i = g \circ i$;

(ii) Dacă M' este un alt monoid iar $i' : M' \rightarrow M_1$ este un morfism de monoizi a.î. $f \circ i' = g \circ i'$, atunci există un unic morfism de monoizi $u : M' \rightarrow M_{f,g}$ a.î. $i \circ u = i'$.

Observație. Dubletul $(M_{f,g}, i)$ îl notăm cu $\text{Ker}(f, g)$ și poartă numele de *nucleul perechii de morfisme de monoizi (f, g)* .

Dacă g este morfismul nul ($g(x) = 1, (\forall) x \in M_1$), notăm $\text{Ker}(f) = M_{f,1} = \{x \in M_1 : f(x) = 1\}$ și îl numim *nucleul* lui f .

1.29. Fie M_1, M_2 monoizi, $f : M_1 \rightarrow M_2$ un morfism de monoizi.

Considerăm următoarele afirmații :

(i) f este aplicație injectivă ;

(ii) $\text{Ker}(f) = \{1\}$.

Să se demonstreze că (i) \Rightarrow (ii) însă în general (ii) \nRightarrow (i).

1.30. Fie M_1, M_2 monoizi, $f : M_1 \rightarrow M_2$ un morfism de monoizi.

Considerăm următoarele afirmații :

(i) f este aplicație injectivă ;

(ii) Dacă M_0 este un alt monoid iar $g, h : M_0 \rightarrow M_1$ sunt morfisme de monoizi a.î. $f \circ g = f \circ h$, atunci $g = h$;

(iii) $\text{Ker}(f) = \{1\}$.

Să se demonstreze că (i) \Rightarrow (ii) și (ii) \Rightarrow (iii).

Observație. Un morfism ce verifică (ii) se numește *monomorfism de monoizi*.

1.31. Fie M_1, M_2 monoizi, $f : M_1 \rightarrow M_2$ un morfism de monoizi.

Considerăm următoarele afirmații :

(i) f este aplicație surjectivă ;

(ii) Dacă M_3 este un alt monoid iar $g, h : M_2 \rightarrow M_3$ sunt morfisme de monoizi a.î. $g \circ f = h \circ f$, atunci $g = h$.

Să se demonstreze că (i) \Rightarrow (ii) însă în general (ii) \nRightarrow (i).

Observație. Un morfism ce verifică (ii) se numește *epimorfism de monoizi*.

§2. Grup. Subgrup. Subgrup generat de o mulțime.

Calculul într-un grup. Grupuri de permutări.

2.1. Pe mulțimea \mathbb{Z} definim operația algebrică:

$$x \circ y = xy + 2(x + y + 1).$$

(i) Să se arate că dubletul (\mathbb{Z}, \circ) nu este grup ;

(ii) Să se determine cea mai mare submulțime $G \subseteq \mathbb{Z}$ (față de incluziune) a.î. dubletul (G, \circ) să fie grup comutativ.

2.2. Pe mulțimea \mathbb{Q} se definește operația algebrică :

$$x \circ y = x + y - kxy$$

($k \in \mathbb{Q}^*$ fixat). Să se arate că există $a \in \mathbb{Q}$ a.î. $(\mathbb{Q} \setminus \{a\}, \circ)$ să fie grup abelian.

2.3. Fie $a, b, c, d \in \mathbb{R}^*$ și operația algebrică : $x \circ y = xy + ax + by + c$.

Ce condiție trebuie să îndeplinească a, b și c pentru ca (\mathbb{R}, \circ) să fie grup abelian ?

2.4. Fie $G = \left\{ \begin{pmatrix} 1 & \ln a & 0 \\ 0 & 1 & 0 \\ 0 & 0 & a \end{pmatrix} : a \in \mathbb{R}, a > 0 \right\}$.

Să se demonstreze că G împreună cu înmulțirea matricelor este grup comutativ.

2.5. Fie $G = \left\{ \begin{pmatrix} 1-x & 0 & x \\ 0 & 0 & 0 \\ x & 0 & 1-x \end{pmatrix} : x \in \mathbb{R} - \{\frac{1}{2}\} \right\}$.

Să se demonstreze că G împreună cu înmulțirea matricelor este grup comutativ.

2.6. Să se determine $x \in \mathbb{R}$ a.î. mulțimea :

$$M = \left\{ \begin{pmatrix} a & 0 & b \\ 0 & x & 0 \\ c & 0 & d \end{pmatrix} : a, b, c, d \in \mathbb{R}, ad - bc = 1 \right\}$$

să fie grup în raport cu operația de înmulțire a matricelor.

2.7. Să se determine numerele reale a și b a.î.:

$$G = \left\{ \begin{pmatrix} x+ay & y-bx \\ y+bx & x-ay \end{pmatrix} : x, y \in \mathbb{R}, x^2 - 4y^2 = 1 \right\}$$

să formeze un grup în raport cu înmulțirea matricelor.

2.8. Fie n natural, $n \geq 2$ dat. Să se arate că mulțimea :

$$G = \left\{ A = \begin{pmatrix} x & 0 \\ 0 & y \end{pmatrix} : x, y \in \mathbb{C}, A^n = I_2, n \geq 2 \right\}$$

este un grup în raport cu înmulțirea matricelor.

Câte elemente are grupul G ?

2.9. Să se arate că mulțimea :

$$G = \left\{ \begin{pmatrix} x+4y & 2y \\ -2y & x-4y \end{pmatrix} : x, y \in \mathbb{R}, x^2 - 12y^2 = 1 \right\}$$

împreună cu înmulțirea matricelor formează grup comutativ.

2.10. Fie G mulțimea matricelor de forma $M(a,b) = \begin{pmatrix} a & b & b \\ b & a & b \\ b & b & a \end{pmatrix}$ cu

proprietatea că $\det M(a,b) = 1$. Să se arate că G este grup în raport cu înmulțirea matricelor.

2.11. Considerăm mulțimea $M =$

$$\left\{ \begin{pmatrix} a & b & c \\ c & a & b \\ b & c & a \end{pmatrix} \mid a, b, c \in \mathbb{R}, \text{ iar } f = a + bX + cX^2 \text{ și } g = X^3 - 1 \text{ sunt prime} \right. \\ \left. \text{intre ele} \right\}.$$

Să se arate că M este grup în raport cu înmulțirea matricelor.

2.12. Fie $E = \mathbb{R} \times \mathbb{R}$ iar pentru $t \in \mathbb{R}$, funcția $f_t: E \rightarrow E$,

$$f_t(x,y) = (x + ty + t^2/2, y + t), \text{ oricare ar fi } (x,y) \in E.$$

Să se demonstreze că mulțimea $G = \{f_t : t \in \mathbb{R}\}$ formează grup comutativ în raport cu compunerea funcțiilor.

2.13. Se consideră mulțimea :

$$G = \left\{ \begin{pmatrix} a & b & c & d \\ d & a & b & c \\ c & d & a & b \\ b & c & d & a \end{pmatrix} \in M_4(\mathbb{R}) \mid (a-c)^2 + (b-d)^2 \neq 0, |a+c| \neq |b+d| \right\}.$$

(i) Să se arate că (G, \cdot) este grup abelian ;

(ii) Pentru $n \in \mathbb{N}$ și $X \in G$, să se arate că există $a_n, b_n, c_n, d_n \in \mathbb{R}$ și $X^n = \{A, B, C, D\}$, $H \subset G$, a.î. (H, \cdot) să fie grup abelian și $= a_n A + b_n B + c_n C + d_n D$ pentru orice n număr natural.

(iii) Pentru $n \in \mathbb{N}^*$ calculați :
$$\begin{pmatrix} 2 & 0 & 0 & 3 \\ 3 & 2 & 0 & 0 \\ 0 & 3 & 2 & 0 \\ 0 & 0 & 3 & 2 \end{pmatrix}^n.$$

2.14. Fie $A = \begin{pmatrix} 2 & 1 & 1 \\ 4 & 2 & 2 \\ -8 & -4 & -4 \end{pmatrix}$ și

$$M_A = \{ x \cdot I_3 + y \cdot A \mid (x,y) \in \mathbb{R}^* \times \mathbb{R} \}.$$

Să se arate că :

- (i) $\det X$ nu depinde de y , pentru orice $X \in M_A$;
(ii) (M_A, \cdot) este un grup abelian ;
(iii) $(X^*)^n + (X^*)^{-n} \in M_A$ și $\det ((X^*)^n + (X^*)^{-n}) \geq 8$, pentru orice $n \in \mathbb{N}^*$ și orice $X \in M_A$, unde X^* este adjuncta lui X .

2.15. Fie $M = \left\{ \begin{pmatrix} a & b \\ 0 & a+b \end{pmatrix} \mid a, b \in \mathbb{Q}, a \neq 0, a \neq -b \right\}$.

- (i) Să se arate că (M, \cdot) este grup ;
(ii) Să se determine toate matricele $X \in M$ a.î. $X \cdot X^t = I_2$;
(iii) Ecuația $Y^t \cdot Y = I_2$ are soluții în M ?

2.16. Să se demonstreze că $U_n = \{z \in \mathbb{C}^* : z^n = 1\}$ și $T = \{z \in \mathbb{C}^* : |z| = 1\}$ este subgrup al grupului (\mathbb{C}^*, \cdot) ($n \in \mathbb{N}$).

2.17. Fie K o mulțime cu patru elemente $K = \{1, a, b, c\}$.
Pe K considerăm operația de înmulțire a cărei tabelă este:

\cdot	1	a	b	c
1	1	a	b	c
a	a	1	c	b
b	b	c	1	a
c	c	b	a	1

Să se demonstreze că dubletul (K, \cdot) este grup comutativ.
Observație. Grupul K poartă numele de *grupul lui Klein*.

2.18. Determinați $a, b, c \in \mathbb{R}$ a.î.

$$G = \{x \in \mathbb{R} \mid a \cos x + b \sin x + c = 0\}$$

să fie subgrup al grupului $(\mathbb{R}, +)$.

2.19. Determinați matricele $A \in M_n(\mathbb{R})$, ($n \geq 3$), pentru care mulțimea $G(A) = \{B \in M_n(\mathbb{R}) \mid \det(A+B) = \det(A) + \det(B)\}$ este grup în raport cu adunarea matricelor din $M_n(\mathbb{R})$.

2.20. Să se demonstreze că orice grup cu cel mult cinci elemente este comutativ.

2.21. Să se demonstreze că pe orice mulțime finită se poate defini o structură de grup comutativ.

2.22. Să se demonstreze că un grup nu se poate scrie ca reuniunea a două subgrupuri proprii ale sale.

2.23. Să se demonstreze că există grupuri ce se pot scrie ca reuniunea a trei subgrupuri proprii ale sale.

2.24. Să se arate că nu există nici un grup care să fie reuniunea a trei subgrupuri proprii ale sale, dintre care două au câte trei elemente.

2.25. Fie (G, \cdot) un grup și $H = \{x^2 \mid x \in G\}$. Să se arate că dacă G este comutativ, atunci H este subgrup al lui G . Reciproca este adevărată?

2.26. Fie (G, \cdot) un dublet format dintr-o mulțime și o operație algebrică asociativă. Să se arate că dacă oricare ar fi $a, b, c \in G$ există $x \in G$ a.î. $axb = c$, atunci (G, \cdot) este grup.

2.27. Fie (G, \cdot) un grup și $a, b \in G$ a.î. $ab = c^n$, cu $c \in G$ și $n \in \mathbb{N}^*$. Să se arate că există $d \in G$ a.î. $ba = d^n$.

2.28. Fie $p \geq 3$ un număr natural impar. Construiți un grup (G, \cdot) cu p^3 elemente, unde $p > 2$ este număr impar, cu proprietatea că pentru orice $x \in G$, $x^p = 1$.

2.29. Fie G o mulțime finită pe care este definită o operație algebrică asociativă, notată multiplicativ. Dacă operația are proprietatea

că :

$$xy = xz \Rightarrow y = z,$$

$yx = zx \Rightarrow y = z$, pentru orice $x, y, z \in G$,
atunci (G, \cdot) este un grup.

2.30. Fie (G, \cdot) un grup în care are loc implicația $xy^n = z^n x \Rightarrow y = z$, unde $n \in \mathbb{N}^*$. Să se arate că (G, \cdot) este grup abelian.

2.31. Fie (G, \cdot) un grup și $a, b \in G$ a.î. $aba = bab$. Să se arate că $a^n = 1$ dacă și numai dacă $b^n = 1$.

2.32. Fie $(G, +)$ un grup abelian finit cu r elemente și să considerăm două elemente fixate a și b din acest grup. Pentru m și n numere naturale date,

notăm cu $M_{m,n}(G)$ mulțimea matricelor cu m linii și n coloane având elementele din grupul G , iar cu $M(a,b)$ notăm submulțimea lui $M_{m,n}(G)$ formată din acele matrice cu proprietatea că suma elementelor de pe fiecare linie este a , iar suma elementelor de pe fiecare coloană este b .

Să se demonstreze că :

- (i) $(M_{m,n}(G), +)$ este grup abelian având r^{mn} elemente;
- (ii) Dacă $ma \neq nb$, atunci $M(a,b)$ este mulțimea vidă ;
- (iii) Dacă $ma = nb$, atunci $M(a,b)$ are $r^{(m-1)(n-1)}$ elemente.

2.33. Fie G un grup iar $A, B, C \leq G$ a.î. $A \subseteq B$, $A \cap C = B \cap C$ și $AC = BC$. Să se demonstreze că $A = B$ (unde $AC = \{ac \mid a \in A \text{ și } c \in C\}$).

2.34. Fie G un grup, $H, K \leq G$ iar $x, y \in G$ a.î. $H \cdot x = K \cdot y$. Să se demonstreze că $H = K$.

2.35. Fie G un grup iar $A, B \leq G$.

Să se demonstreze că $|AB| \cdot |A \cap B| = |A| \cdot |B|$.

2.36. Fie G un grup finit iar $A, B \subseteq G$ a.î. $|A| + |B| > |G|$.

Să se demonstreze că $G = AB$.

2.37. Fie (G, \cdot) un grup cu proprietățile:

- 1) Dacă $x^2 = 1$, atunci $x = 1$;
 - 2) $(xy)^2 = (yx)^2$, oricare ar fi $x, y \in G$.
- Să se demonstreze că grupul G este abelian.

2.38. Fie G un grup a.î. $x^2 = 1$, pentru orice $x \in G$.

Să se demonstreze că G este comutativ iar dacă G este finit, atunci $|G|$ este o putere naturală a lui 2.

2.39. Fie G un grup finit și p un număr prim care divide ordinul lui G . Atunci numărul soluțiilor ecuației $x^p = 1$ este un multiplu nenul al lui p .

2.40. Dacă G este un grup, să se demonstreze că $Z(G) \leq G$ (vezi problema. 1.21.).

2.41. Fie G un grup iar $x, y \in G$ a.î. $xy \in Z(G)$.

Să se demonstreze că $xy = yx$.

2.42. Fie (G, \cdot) un grup, $x, y \in G$ și $m, n \in \mathbb{N}^*$ a.î. $(m, n) = 1$.

Să se arate că dacă x comută cu y^m și y^n , atunci x comută și cu y .

2.43. Fie G un grup iar $H \leq G$ un subgrup propriu al său.

Să se demonstreze că $\langle G \setminus H \rangle = G$.

2.44. Fie (G, \cdot) un grup care are un subgrup H a.î. $G \setminus H$ are un număr finit de elemente. Să se arate că grupul G este finit.

2.45. Fie (G, \cdot) un grup abelian finit. Spunem că subgrupul H al lui G are proprietatea (A) dacă $G \neq H$ și produsul elementelor lui H este egal cu produsul elementelor din $G \setminus H$. Să se arate că dacă G are un subgrup cu proprietatea (A), atunci orice subgrup al lui G , diferit de G are proprietatea (A).

2.46. Pentru un grup finit G notăm cu $s(G)$ numărul de subgrupuri ale sale.

Să se arate că:

(i) Pentru orice număr real $a > 0$ există grupuri finite G a.î. $\frac{|G|}{s(G)} < a$;

(ii) Pentru orice număr real $a > 0$ există grupuri finite G a.î. $\frac{|G|}{s(G)} > a$.

2.47. Fie \cdot o operație algebrică asociativă pe mulțimea M . Să se demonstreze că (M, \cdot) este grup dacă și numai dacă oricare ar fi $a \in M$, există $n \in \mathbb{N}^*$ a.î. $f_a: M \rightarrow M$, $f_a(x) = axa^n$ să fie surjectivă.

2.48. Să se demonstreze că grupul aditiv $(\mathbb{Q}, +)$ nu este finit generat.

2.49. Fie H un subgrup al grupului aditiv $(\mathbb{Q}, +)$.

Să se arate că dacă $\mathbb{Q} = H + \mathbb{Z}$, atunci $H = \mathbb{Q}$.

2.50. Fie (G, \cdot) un grup (abelian), G' o mulțime pentru care există o bijecție $f: G \rightarrow G'$. Pentru $x, y \in G'$ definim $x \circ y = f(f^{-1}(x) \cdot f^{-1}(y))$. Să se arate că în felul acesta (G', \circ) devine grup (abelian).

2.51. Să se demonstreze că pe orice interval deschis și mărginit de numere reale se poate defini o operație algebrică ce determină pe intervalul respectiv o structură de grup.

2.52. Fie (G, \cdot) un grup. Să se arate că următoarele afirmații sunt echivalente :

(i) Orice parte stabilă a lui G este subgrup al său ;

(ii) Pentru orice $x \in G$, există $k \in \mathbb{N}^*$ a.î. $x^k = 1$.

2.53. Fie (G, \cdot) un grup, $n \in \mathbb{N}$, $n \geq 3$ și H_1, H_2, \dots, H_n subgrupuri ale lui G
a.î. :

$$1) \bigcup_{i=1}^n H_i = G$$

$$2) H_i \not\subset \bigcup_{\substack{i=1 \\ i \neq j}}^n H_j.$$

Să se arate că pentru orice $x \in G$, există $k \in \mathbb{N}^*$, $k \leq (n-1)!$ a.î. $x^k \in \bigcap_{i=1}^n H_i$.

2.54. Pentru orice $n \in \mathbb{N}^*$ considerăm $H_n = \{ \frac{k}{n!} \mid k \in \mathbb{Z} \}$.

Să se demonstreze că:

(i) H_n este subgrup al grupului $(\mathbb{Q}, +)$ și că $\mathbb{Q} = \bigcup_{n \in \mathbb{N}^*} H_n$;

(ii) Dacă G_1, G_2, \dots, G_m sunt subgrupuri ale grupului $(\mathbb{Q}, +)$ și $G_i \neq \mathbb{Q}$,
pentru orice $1 \leq i \leq m$ atunci $\bigcup_{i=1}^m G_i \neq \mathbb{Q}$.

2.55. Fie $n \in \mathbb{N}^*$ iar $U_n = \{ z \in \mathbb{C}^* : z^n = 1 \}$.

Să se demonstreze că $U_n \leq (\mathbb{C}^*, \cdot)$, $|U_n| = n$ iar U_n este grup ciclic (vezi problema **2.16.**).

2.56. Fie (G, \cdot) un grup comutativ cu elementul unitate 1 și $m, n \in \mathbb{N}^*$.

Să se arate că :

$$H_m H_n = H_{[m,n]},$$

unde am notat $H_n = \{ x \in G \mid x^n = 1 \}$, $H_m H_n = \{ xy \mid x \in H_m, y \in H_n \}$, iar $[m,n]$ = c.m.m.m.c (m,n) .

2.57. Fie (G, \cdot) un grup iar $L(G)$ mulțimea subgrupurilor lui G . Să se arate că $(L(G), \subseteq)$ este latice completă.

2.58. Să se arate că în laticea $L(\mathbb{Z})$ pentru $H = m\mathbb{Z}$ și $K = n\mathbb{Z}$, cu $m, n \in \mathbb{N}$, $H \wedge K = [m,n]\mathbb{Z}$ iar $H \vee K = (m,n)\mathbb{Z}$. Să se deducă de aici faptul că $(L(\mathbb{Z}), \subseteq)$ este latice distributivă.

2.59. Fie G un grup cu proprietatea că $(xy)^2 = x^2 y^2$, pentru orice $x, y \in G$.

Să se demonstreze că G este comutativ.

2.60. Fie G un grup cu proprietatea că există $n \in \mathbb{N}^*$ a.î. $(xy)^k = x^k y^k$, pentru $k = n, n+1, n+2$, oricare ar fi $x, y \in G$.

Să se demonstreze că G este comutativ.

2.61. Fie G un grup cu proprietatea că există $n \in \mathbb{N}^*$ a.î. $(xy)^k = x^k y^k$, pentru $k = n, n+2, n+4$, oricare ar fi $x, y \in G$.

Să se demonstreze că G este comutativ.

2.62. Fie G un grup cu proprietatea că există $m, n \in \mathbb{N}^*$, $(m, n) = 1$ a.î. oricare ar fi $x, y \in G$, $(xy)^n = (yx)^n$ și $(xy)^m = (yx)^m$.

Să se demonstreze că G este comutativ.

2.63. Fie G un grup cu proprietatea că $x^3 = 1$ și $x^2 y^2 = y^2 x^2$, oricare ar fi $x, y \in G$. Să se demonstreze că G este comutativ.

2.64. Fie G un grup iar $x, y \in G$. Notăm $[x, y] = x^{-1} y^{-1} xy$. Să se demonstreze că dacă $x, y, z \in G$, atunci:

- (i) $xy = yx \Leftrightarrow [x, y] = 1$;
- (ii) $[xy, z] = y^{-1} [x, z] y [y, z]$;
- (iii) $[x, yz] = [x, z] z^{-1} [x, y] z$;
- (iv) $y^{-1} [[x, y^{-1}], z] y z^{-1} [[y, z^{-1}], x] z x^{-1} [[z, x^{-1}], y] x = 1$.

Observație. $[x, y]$ poartă numele de *comutatorul* lui x și y .

2.65. Fie X o mulțime nevidă iar $F(X) = \{f : X \rightarrow X\}$.

Să se demonstreze că relativ la compunerea funcțiilor, $F(X)$ este un monoid iar $U(F(X), \circ) = \{f \in F(X) : f \text{ este o bijecție}\}$.

Observație. Vom nota $U(F(X), \circ) = \Sigma(X)$; grupul $(\Sigma(X), \circ)$ poartă numele de *grupul de permutări asupra mulțimii X* . Dacă X este o mulțime finită cu n elemente, vom nota $\Sigma(X)$ prin S_n .

2.66. În grupul permutărilor $\Sigma(\mathbb{R})$ considerăm elementele σ, τ definite astfel: $\sigma(x) = x + 1$ și $\tau(x) = 2x$, pentru orice $x \in \mathbb{R}$ iar $G = \langle \sigma, \tau \rangle \leq \Sigma(\mathbb{R})$.

Pentru $n \in \mathbb{N}^*$, fie $\sigma_n = \tau^{-n} \sigma \tau^n \in G$ și $H_n = \langle \sigma_n \rangle \leq G$.

Să se demonstreze că pentru orice $n \geq 1$, $H_n \leq H_{n+1}$ iar $H = \bigcup_{n \geq 1} H_n$ nu este subgrup finit generat al lui G .

2.67. Să se determine $f : \mathbb{R} \rightarrow \mathbb{R}$ care admit primitive pe \mathbb{R} , cu proprietatea că mulțimea primitivelor lui f este subgrup al grupului bijecțiilor lui \mathbb{R} (în raport cu compunerea funcțiilor).

2.68. Fie (X,d) un spațiu metric iar

$\text{Izom}(X) = \{f \in \Sigma(X) : d(f(x), f(y)) = d(x,y), \text{ pentru orice } x,y \in X\}$.

Să se demonstreze că $\text{Izom}(X) \leq \Sigma(X)$.

Observație. Elementele lui $\text{Izom}(X)$ se numesc *izometrii* ale lui X .

2.69. Fie $X = E^2$ planul euclidian înzestrat cu funcția distanță uzuală. Vom nota prin $\text{Tr}(E^2) =$ mulțimea translațiilor lui E^2 iar pentru un punct fixat $O \in E^2$, $\text{Rot}(O,E^2) =$ mulțimea rotațiilor lui E^2 în jurul lui O . Să se demonstreze că :

(i) $\text{Tr}(E^2) \leq \text{Izom}(E^2)$, $\text{Rot}(O,E^2) \leq \text{Izom}(E^2)$;

(ii) Pentru orice $f \in \text{Izom}(E^2)$, există $\rho \in \text{Rot}(O,E^2)$, $\tau \in \text{Tr}(E^2)$ a.î. $f = \rho \circ \tau$, cu $O \in E^2$.

2.70. Fie (X,d) un spațiu metric, $Y \subseteq X$ iar

$$S_X(Y) = \{f \in \text{Izom}(X) \mid f(Y) = Y\}.$$

Să se demonstreze că $S_X(Y) \leq \text{Izom}(X)$.

Observație. $S_X(Y)$ poartă numele de *grupul de simetrie al lui Y în raport cu X* .

2.71. Pentru un număr natural n și P_n un poligon regulat cu n laturi, definim $D_n = S_{E^2}(\overline{P})$ (\overline{P} fiind conturul lui P_n). Fie O centru lui P_n , ρ rotația în jurul lui O de unghi $2\pi/n$ iar ε simetria față de una din axele de simetrie ale lui P_n . Să se demonstreze că $D_n = \{1, \rho, \rho^2, \rho^3, \dots, \rho^{n-1}, \varepsilon, \rho\varepsilon, \dots, \rho^{n-1}\varepsilon\}$.

Observație. Grupul D_n de ordin $2n$ poartă numele de *grupul diedral de grad n* .

2.72. Să se demonstreze că grupul simetric S_n este generat de transpozițiile $\tau_i = (i, i+1)$, $i = 1, 2, \dots, n-1$.

2.73. Să se demonstreze că grupul simetric S_n este generat de transpozițiile $\tau_i = (1, i)$, $i = 1, 2, \dots, n$.

2.74. Să se demonstreze că pentru orice $1 \leq k \leq n$, grupul simetric S_n este generat de transpozițiile $(1, k), (2, k), \dots, (k-1, k), (k+1, k), \dots, (n, k)$.

2.75. Să se demonstreze că grupul simetric S_n este generat de transpoziția $\tau = (1, 2)$ și ciclul $\sigma = (1, 2, \dots, n)$.

2.76. Să se demonstreze că grupul altern A_n este generat de ciclul de lungime 3.

2.77. Să se demonstreze că grupul altern A_n este generat de ciclul $(1,2,3), (1,2,4), \dots, (1,2,n)$.

2.78. Să se demonstreze că în S_n avem :

$$(1,2, \dots, r) = (2,3, \dots, r,1) = \dots = (r,1,2, \dots, r-1) \quad (r \leq n).$$

2.79. Să se demonstreze că dacă α este un r -ciclu în S_n , atunci $\alpha^r = e$ ($r \leq n$) și r este cel mai mic număr natural cu această proprietate.

2.80. Fie α și β doi r -cicli în S_n ($r \leq n$).

Să se demonstreze că dacă există $i \in S_n$ a.î. $\alpha(i) \neq i$ și $\beta(i) \neq i$ iar $\alpha^k(i) = \beta^k(i)$ pentru orice k natural, atunci $\alpha = \beta$.

2.81. Două permutări $\alpha, \beta \in S_n$ se zic *disjuncte* dacă atunci când una din ele schimbă un element, cealaltă îl fixează.

Să se demonstreze că dacă $\alpha = (i_1, i_2, \dots, i_r)$, $\beta = (j_1, j_2, \dots, j_s)$, $r, s \leq n$, atunci α și β sunt disjuncte $\Leftrightarrow \{i_1, i_2, \dots, i_r\} \cap \{j_1, j_2, \dots, j_s\} = \emptyset$.

2.82. Să se demonstreze că dacă permutările $\alpha, \beta \in S_n$ sunt disjuncte, atunci $\alpha\beta = \beta\alpha$.

2.83. Să se demonstreze că S_n poate fi privit ca subgrup al lui A_{n+2} .

2.84. Să se demonstreze că pentru $n \geq 4$, $Z(A_n) = \{e\}$.

2.85. Să se demonstreze că pentru $n \geq 3$, $Z(S_n) = \{e\}$.

2.86. Să se demonstreze că în S_n două permutări sunt conjugate dacă și numai dacă au aceeași structură ciclică.

2.87. Să se rezolve în S_n ecuația $x^2 = (1,2, \dots, n)$.

2.88. Fie p un număr prim iar $\sigma \in S_n$ un ciclu de lungime m ($m \leq n$).

Să se demonstreze că :

(i) Dacă $p \nmid m$, atunci σ^p este un ciclu de lungime m , având aceeași orbită ca și σ ;

(ii) Dacă $p \mid m$, atunci σ^p este un produs de p cicli disjuncți de lungime m/p .

2.89. Fie p un număr prim. Să se demonstreze că :

(i) Dacă $\sigma \in S_n$ este un ciclu de lungime m , unde $p \nmid m$, atunci există $\tau \in S_n$ un ciclu de lungime m a.î. $\tau^p = \sigma$;

(ii) Dacă $\sigma_1, \sigma_2, \dots, \sigma_p \in S_n$ sunt cicluri disjuncte de aceeași lungime k , atunci există $\tau \in S_n$ un ciclu de lungime $m=kp$ a.î. $\tau^p = \sigma_1 \sigma_2 \dots \sigma_p$.

2.90. Fie un număr prim, $\sigma \in S_n$, $\sigma \neq e$. Să presupunem că în descompunerea în cicluri disjuncte a lui σ apar α_1 cicluri de lungime m_1 , α_2 cicluri de lungime m_2 , ..., α_t cicluri de lungime m_t (m_1, m_2, \dots, m_t fiind distincte două câte două) iar m_1, m_2, \dots, m_k ($k \leq t$) sunt divizibile cu p .

Să se demonstreze că ecuația $x^p = \sigma$ are soluție în $S_n \Leftrightarrow \alpha_1, \alpha_2, \dots, \alpha_k$ sunt divizibile prin p .

Aplicație. Să se studieze compatibilitatea ecuațiilor:

$$x^2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 & 16 & 17 & 18 & 19 \\ 5 & 6 & 7 & 8 & 1 & 2 & 3 & 11 & 12 & 19 & 13 & 16 & 4 & 15 & 17 & 9 & 18 & 14 & 10 \end{pmatrix} \text{ în } S_{19};$$

$$x^3 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 3 & 6 & 5 & 9 & 1 & 7 & 8 & 2 & 10 & 4 \end{pmatrix} \text{ în } S_{10}.$$

2.91. Dacă p este un număr prim, $p \geq n$, să se demonstreze că ecuația $x^p = \sigma$ are soluție pentru orice $\sigma \in S_n$, $\sigma \neq e$.

2.92. Fie p un număr prim. Să se demonstreze că $x \in S_n$ este soluție a ecuației $x^p = e \Leftrightarrow x$ este un produs de cicluri disjuncte de lungime p din S_n .

2.93. Fie G un grup comutativ cu n elemente. Să se demonstreze că orice subgrup al lui G poate fi generat de cel mult n elemente.

2.94. Să se demonstreze că grupul $(\mathbb{Q}, +)$ nu admite un sistem de generatori minimal.

2.95. Să se demonstreze că orice subgrup finit generat al lui $(\mathbb{Q}, +)$ este ciclic (un astfel de grup se numește *local ciclic*).

§3. Teorema lui Lagrange. Ordinul unui element.

Indicele unui subgrup. Subgrupuri normale.

3.1. Fie G un grup finit a.î. $|Z(G)| > \frac{1}{2} \cdot |G|$. Să se demonstreze că grupul G este comutativ.

3.2. Fie G un grup finit comutativ a.î. $x^2 = 1$ pentru mai mult de jumătate din elementele lui G . Să se demonstreze că $x^2 = 1$, oricare ar fi $x \in G$.

3.3. Să se demonstreze că într-un grup G cu $2n$ elemente, unde n este număr impar, există cel mult n elemente de ordin 2.

3.4. Fie G un grup iar $x \in G$ un element de ordin finit. Să se demonstreze că :

$$o(x^n) \mid o(x), \text{ oricare ar fi } n \in \mathbb{N}.$$

3.5. Să se arate că într-un grup abelian G există un element al cărui ordin este egal cu c.m.m.d.c al ordinelor tuturor elementelor $x \neq 1$ ale lui G .

3.6. Fie G un grup, $x, y \in G$ a.î. $xy = yx$ iar $x^m = y^n = 1$ ($m, n \in \mathbb{N}$).
Să se demonstreze că $(xy)^k = 1$, unde $k = [m, n]$.
Putem avea $o(xy) < k$?

3.7. Fie G un grup iar $x, y \in G$.
Să se demonstreze că $o(xy) = o(yx)$ și $o(x) = o(x^{-1})$.

3.8. Fie G un grup iar $x \in G$ un element de ordin finit n .
Să se demonstreze că pentru orice $m \in \mathbb{N}^*$, $o(x^m) = n / (m, n)$.

3.9. Fie G un grup și $x, y \in G$ cu $o(x) = n_1$, $o(y) = n_2$ finite, $(n_1, n_2) = 1$ iar $xy = yx$. Să se demonstreze că $o(xy) = o(x) \cdot o(y)$.
Dacă condiția $(n_1, n_2) = 1$ se înlocuiește cu $\langle x \rangle \cap \langle y \rangle = \{1\}$, să se arate că $o(xy) = [n_1, n_2]$.

3.10. Fie G un grup, $x \in G$ a.î. $o(x) = n_1 n_2$ cu $n_1, n_2 \in \mathbb{N}^*$, $(n_1, n_2) = 1$.
Să se demonstreze că există și sunt unic determinate elementele $y, z \in G$ a.î. $x = yz = zy$ și $o(y) = n_1$, $o(z) = n_2$.

3.11. Fie G un grup iar $x, y \in G$ a.î. $o(x) = m, o(y) = n, (m, n) \in \mathbb{N}^*$.
Să se demonstreze că dacă x și y comută cu $[x, y]$, atunci $[x, y]^d = 1$,
unde $d = (m, n)$.

3.12. Fie (G, \cdot) un grup comutativ de ordin finit.

Sunt echivalente :

(i) G este de ordin impar ;

(ii) Pentru orice $a \in G$ ecuația $x^2 = a$ are soluție unică în G .

3.13. Fie (G, \cdot) un grup finit. Dacă m și n sunt divizori ai ordinului grupului, atunci ecuațiile $x^m = 1$ și $x^n = 1$ au o singură soluție comună dacă și numai dacă $(m, n) = 1$.

3.14. Fie G un grup cu 10 elemente în care există $a, b \in G \setminus \{1\}$ distincte a.î. $a^2 = b^2 = 1$. Să se arate că G nu este abelian.

3.15. În monoidul multiplicativ $M_2(\mathbb{Z})$ considerăm matricele:

$$A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \text{ și } B = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}.$$

Să se demonstreze că $o(A) = 4, o(B) = 3$ iar $o(AB) = \infty$.

3.16. Fie G un grup, $H \leq G$ și $x \in G$ a.î. $o(x) = n$ ($n \in \mathbb{N}^*$).

Să se demonstreze că dacă $x^m \in H$ pentru orice $m \in \mathbb{N}^*$ a.î. $(m, n) = 1$, atunci $x \in H$.

3.17. Fie G un grup comutativ de ordin n .

Arătați că produsul celor n elemente ale lui G este egal cu produsul tuturor elementelor de ordin cel mult 2.

Aplicând acest rezultat grupului multiplicativ (\mathbb{Z}_p^*, \cdot) cu p prim, să se demonstreze că $p \mid (p-1)! + 1$.

Observație. Consecința de la problema **3.17.** este datorată lui *Wilson*.

3.18. Fie p un număr prim iar $n \geq 2$ un număr natural.

Să se demonstreze că:

(i) Dacă $p = 2$ și $n > 2$, atunci în grupul $U(\mathbb{Z}_{2^n}, \cdot)$ numai elementele $-\hat{1}, \hat{1}, \widehat{2^{n-1}-1}, \widehat{2^{n-1}+1}$ au ordinul cel mult 2 ;

(ii) Dacă $p > 2$, atunci în grupul $U(\mathbb{Z}_{p^n}, \cdot)$ numai elementele $\hat{1}$ și $-\hat{1}$ au ordinul cel mult 2 ;

(iii) Să se deducă de aici următoarele variante de generalizare pentru *teorema lui Wilson*:

a) Dacă p este un număr prim, $p > 2$ și $n \geq 1$ un număr natural, atunci :

$$p^n \mid \left(\prod_{\substack{1 \leq a < p^n \\ (a,p)=1}} a \right) + 1$$

b) Dacă $p = 2$ și $n > 2$, atunci : $2^n \mid \left(\prod_{\substack{1 \leq a < 2^n \\ (a,2)=1}} a \right) + 1.$

c) Dacă $p = 2$ și $n = 2$, atunci : $2^2 \mid \left(\prod_{\substack{1 \leq a < 2^2 \\ (a,2)=1}} a \right) + 1.$

3.19. Fie p un număr prim, $n \in \mathbb{N}^*$ și $U_{p^n} = \{z \in \mathbb{C}^* : z^{p^n} = 1\}$.

Să se demonstreze că:

(i) $U_{p^0} \subset U_{p^1} \subset \dots \subset U_{p^n} \subset U_{p^{n+1}} \subset \dots \subset \mathbb{C}^*$;

(ii) Dacă notăm $U_{p^\infty} = \bigcup_{n \geq 0} U_{p^n}$, atunci $U_{p^\infty} \leq (\mathbb{C}^*, \cdot)$;

(iii) Dacă $H \leq (U_{p^\infty}, \cdot)$ este propriu, atunci există $n \in \mathbb{N}$ a.î. $H =$

$$U_{p^n}.$$

3.20. Fie A un inel unitar, $n \in \mathbb{N}$, $n \geq 2$. Notăm $GL_n(A) = \{M \in M_n(A) : \det(M) \in U(A, \cdot)\}$ și $SL_n(A) = \{M \in M_n(A) : \det(M) = 1\}$.

Să se demonstreze că $GL_n(A)$ este un grup relativ la înmulțirea matricelor iar $SL_n(A) \trianglelefteq GL_n(A)$.

Observație. Grupurile $GL_n(A)$ și $SL_n(A)$ poartă numele de *grupul liniar general* (respectiv *special*) de grad n peste inelul A .

3.21. Dacă K este un corp finit cu q elemente, să se demonstreze că:

$$|GL_n(K)| = (q^n - 1)(q^n - q) \dots (q^n - q^{n-1}).$$

3.22. Fie $U, V \in M_2(\mathbb{Z})$, $U = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, $V = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$.

Să se demonstreze că $U, V \in SL_2(\mathbb{Z})$ iar $\langle U, V \rangle = SL_2(\mathbb{Z})$.

3.23. Fie $U, V, W \in M_2(\mathbb{Z})$, $U = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, $V = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$, $W = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$.

Să se demonstreze că $U, V, W \in GL_2(\mathbb{Z})$ iar $\langle \{U, V, W\} \rangle = GL_2(\mathbb{Z})$.

3.24. Fie (G, \cdot) un grup iar $L_0(G)$ mulțimea subgrupurilor normale ale lui G . Să se arate că $L_0(G)$ este sublatice modulară a lui $L(G)$.

3.25. Dacă M este un A -modul, atunci latticea $(L_A(M), \subseteq)$ a submodulelor lui M este modulară.

3.26. Fie G un grup, $H \leq G$ a.î. $H \subseteq Z(G)$.
Să se demonstreze că $H \trianglelefteq G$.

3.27. Fie G un grup iar $H \trianglelefteq G$. Să se demonstreze că $Z(H) \trianglelefteq G$.

3.28. Fie G un grup și $H \trianglelefteq G$ cu $|H| = 2$. Să se demonstreze că $H \leq Z(G)$.

3.29. Fie G un grup, $H \leq G$ a.î. $|G:H| = 2$. Să se demonstreze că $H \trianglelefteq G$.

3.30. Fie G un grup finit și $n \in \mathbb{N}^*$ a.î. $(n, |G|) = 1$.
Să se demonstreze că oricare ar fi $x \in G$ există și este unic $y \in G$ a.î. $y^n = x$.
Să se deducă de aici că dacă $y, z \in G$ și $y^n = z^n$, atunci $y = z$.

3.31. Fie G un grup a.î. $|G:Z(G)| = n$ ($n \in \mathbb{N}^*$).
Să se demonstreze că oricare ar fi $x, y \in G$ avem:
$$[x, y]^{n+1} = [x, y^2] \cdot [y^{-1}xy, y]^{n-1}.$$

3.32. Dacă orice subgrup propriu al unui grup G este comutativ, rezultă că grupul G este comutativ ?

3.33. Fie G un grup finit cu n elemente. Să se demonstreze că $x^n = 1$, pentru orice $x \in G$.

Să se deducă de aici că dacă $a, n \in \mathbb{N}^*$ a.î. $(a, n) = 1$, atunci $n \mid a^{(n)} - 1$.

Observație. Consecința acestui rezultat este datorat lui *Euler*

3.34. Fie $G = \{ a_1, a_2, \dots, a_n \}$ un subgrup al grupului (\mathbb{C}^*, \cdot) și $k \in \mathbb{N}^*$.
Să se arate că :

- (i) $G = U_n$;
- (ii) Există relația :

$$a_1^k + a_2^k + \dots + a_n^k = \begin{cases} 0, & \text{dacă } k \text{ nu este multiplu de } n \\ n, & \text{dacă } k \text{ este multiplu de } n \end{cases}.$$

3.35. Fie G un grup a.î. există $A \subset G$ finită și nevidă cu proprietatea că $G \setminus A$ este un subgrup al lui G .

- (i) Să se arate că G este finit și $|G| \leq 2|A|$;
(ii) Dacă $|A|$ este prim, atunci $|G| = 2|A|$ sau $|G| = |A| + 1$.

3.36. Să se demonstreze că cel mai mic subgrup normal al lui G ce conține pe H este subgrupul lui G generat de elementele de forma $g^{-1}hg$ cu $g \in G$ și $h \in H$.

Observație. Cel mai mic subgrup normal al lui G ce conține pe H se notează prin $N_G(H)$ și poartă numele de *închiderea normală* a lui H în G (sau *normalizatorul* lui H în G).

3.37. Fie A, B, C subgrupuri ale grupului G . Să se demonstreze că :

- (i) Dacă $A \leq B$, atunci $|B : A| \geq |(C \cap B) : (C \cap A)|$;
(ii) $|G : (A \cap B)| \leq |G : A| \cdot |G : B|$;
(iii) $|(A \vee B) : B| \geq |A : (A \cap B)|$.

3.38. Fie A, B subgrupuri ale unui grup G a.î. $|G : A|$ și $|G : B|$ sunt finite și prime între ele.

Să se demonstreze că :

- (i) $|G : (A \cap B)| = |G : A| \cdot |G : B|$;
(ii) Dacă în plus G este finit, atunci $G = AB$.

3.39. Fie G un grup finit iar A, B subgrupuri ale lui G .

Să se demonstreze că dacă $|A : (A \cap B)| > \frac{1}{2} \cdot |G : B|$, atunci $A \vee B = G$.

3.40. Fie G un grup finit generat.

Să se demonstreze că orice subgrup de indice finit în G este finit generat.

3.41. Să se demonstreze că într-un grup G intersecția unui număr finit de subgrupuri de indice finit este un subgrup de indice finit.

3.42. Fie G un grup, $x \in G$ iar $C_G(x) = \{ y \in G : xy = yx \}$. Să se demonstreze că $C_G(x) \leq G$ iar mulțimea conjugaților lui x (adică a elementelor de forma axa^{-1} cu $a \in G$) are cardinalul egal cu $|G : C_G(x)|$.

Observație. $C_G(x)$ poartă numele de *centralizatorul* lui x în G ; în general, dacă M este o submulțime a lui G , definim $C_G(M)$ ca fiind intersecția centralizatoarelor tuturor elementelor lui M .

3.43. Fie G un grup iar $K \leq G$. Să se demonstreze că $C_G(K) = \{1\} \Leftrightarrow Z(H) = \{1\}$, oricare ar fi H a.î. $K \leq H \leq G$.

3.44. Fie n un număr natural, $n \geq 2$, K un corp, $K \neq \mathbb{Z}_2$ iar D mulțimea matricelor diagonale din $GL_n(K)$.

(i) Arătați că $C_G(D) = D$. Deduceți de aici că

$$Z(GL_n(K)) = \{aI_n : a \in K\};$$

(ii) Presupunând în plus că $n \geq 3$ sau $K \neq \mathbb{Z}_3$ să se demonstreze că $C_{GL_n(K)}(D \cap SL_n(K)) = D$ și deduceți de aici că

$$Z(SL_n(K)) = SL_n(K) \cap Z(GL_n(K)).$$

3.45. Să se demonstreze că pentru $n \geq 3$, D_n are un singur subgrup de ordin n .

3.46. Fie $n \geq 3$. Să se demonstreze că dacă n este impar, atunci $|Z(D_n)| = 1$ iar dacă n este par, atunci $|Z(D_n)| = 2$.

3.47. Să se demonstreze că grupul altern A_4 (care are ordinul 12) nu are subgrupuri de ordin 6.

Observație. Acest exercițiu ne arată că *reciproca teoremei lui Lagrange* nu este adevărată.

§4. Morfisme și izomorfisme de grupuri.

Grup factor. Teorema lui Cauchy.

Teoremele de izomorfism pentru grupuri.

4.1. Fie G_1, G_2 două grupuri, $f, g : G_1 \rightarrow G_2$ morfisme de grupuri, $G = \{x \in G_1 : f(x) = g(x)\}$ iar $i : G \rightarrow G_1$ incluziunea canonică.

Să se demonstreze că $G \leq G_1$ și că dubletul (G, i) verifică următoarea proprietate de universalitate:

(i) $f \circ i = g \circ i$;

(ii) Dacă G' este un alt grup, $i' : G' \rightarrow G_1$ un morfism de grupuri a.î. $f \circ i' = g \circ i'$, atunci există un unic morfism de grupuri $u : G' \rightarrow G$ a.î. $i \circ u = i'$.

Observație. Dubletul (G, i) se notează prin $\text{Ker}(f, g)$ și poartă numele de *nucleul* perechii de morfisme (f, g) .

Dacă g este morfismul nul (adică $g(x) = 1$, pentru orice $x \in G_1$), convenim să notăm $\text{Ker}(f) = \text{Ker}(f, 1) = \{x \in G_1 : f(x) = 1\}$ (fără a mai specifica morfismul incluziune).

4.2. Fie G_1, G_2 două grupuri, $f : G_1 \rightarrow G_2$ un morfism de grupuri.

Să se demonstreze că următoarele afirmații sunt echivalente:

(i) f este aplicație injectivă;

(ii) $\text{Ker}(f) = \{1\}$.

4.3. Fie G_1, G_2 două grupuri, $f : G_1 \rightarrow G_2$ un morfism de grupuri.

Să se demonstreze că următoarele afirmații sunt echivalente:

(i) f este aplicație injectivă;

(ii) Dacă G_0 este un alt grup și $g, h : G_0 \rightarrow G_1$ sunt morfisme de grupuri

a.î. $f \circ g = f \circ h$, atunci $g = h$.

Observație. Acest exercițiu ne arată că în categoria grupurilor, *monomorfismele* sunt exact morfismele injective.

4.4. Fie G_1, G_2 două grupuri, $f : G_1 \rightarrow G_2$ un morfism de grupuri.

Să se demonstreze că următoarele afirmații sunt echivalente:

(i) f este aplicație surjectivă;

(ii) Dacă G_3 este un alt grup și $g, h : G_2 \rightarrow G_3$ sunt morfisme de grupuri

a.î. $g \circ f = h \circ f$, atunci $g = h$.

Observație. Acest exercițiu ne arată că în categoria grupurilor, *epimorfismele* sunt exact morfismele surjective.

4.5. Fie M un monoid comutativ cu proprietatea că dacă $x, y \in M$ și $xy = xz$ atunci $y = z$.

Să se demonstreze că există un grup G_M și un morfism injectiv de monoizi $i_M : M \rightarrow G_M$ a.î. pentru orice grup abelian G și orice morfism de monoizi $u : M \rightarrow G$ există un unic morfism de grupuri $u' : G_M \rightarrow G$ a.î. $u' \circ i_M = u$.

Observație. Acest rezultat este datorat lui *Malțev*.

4.6. Fie $M = (1, \infty)$ și o operație algebrică pe M , $\circ : M \times M \rightarrow M$, definită astfel: $x \circ y = xy + ax + by + c$ ($a, b, c \in \mathbb{R}$). Să se determine a, b, c știind că (M, \circ) este grup și să se arate că (M, \circ) este izomorf cu $(\mathbb{R}, +)$.

4.7. Fie G un subgrup nenul al lui grupului $(\mathbb{R}, +)$ cu proprietatea că $G \cap (-a, a)$ este mulțime finită, oricare ar fi $a \in \mathbb{R}$, $a > 0$. Să se arate că grupul $(G, +)$ este izomorf cu grupul $(\mathbb{Z}, +)$.

4.8. Într-un grup (G, \cdot) se consideră submulțimile:

$$H_n = \{x \in G \mid x^n = 1\}, n \in \mathbb{N}^*.$$

Să se arate că:

(i) H_2 este subgrup al lui $G \Leftrightarrow xy = yx$ pentru orice $x, y \in H_2$;

(ii) Dacă p este un număr prim cu proprietatea că H_p are cel mult p elemente, atunci $H_p = \{1\}$ sau H_p este subgrup al lui G izomorf cu grupul $(\mathbb{Z}_p, +)$.

4.9. Fie $G = (0, \infty) \setminus \{1\}$ și $a \in G, \alpha \in \mathbb{R}^*$. Definim pe G operația algebrică: $x \circ y = x^{\alpha \log_a y}$ și notăm cu $G_{a, \alpha} = (G, \circ)$. Să se arate că :

(i) $G_{a, \alpha}$ este grup abelian;

(ii) Dacă $b \in G, \beta \in \mathbb{R}^*$ atunci grupurile $G_{a, \alpha}$ și $G_{b, \beta}$ sunt izomorfe.

4.10. Arătați că mulțimea M a matricelor de forma $A = \begin{pmatrix} cha & sha \\ sha & cha \end{pmatrix}, a \in \mathbb{R}$, formează un grup multiplicativ izomorf cu $(\mathbb{R}, +)$.

4.11. Fie mulțimile:

$$M = \left\{ A \in M_2(\mathcal{Q}) \mid \begin{pmatrix} a+2b & 3b \\ 2b & a-2b \end{pmatrix}, a^2 - 10b^2 = 1, a, b \in \mathcal{Q} \right\} \text{ și}$$

$$G = \{ x \in \mathbb{Q}(\sqrt{10}) \mid x = a + b\sqrt{10}, a^2 - 10b^2 = 1, a, b \in \mathbb{Q} \}.$$

Să se arate că :

(i) (M, \cdot) și (G, \cdot) sunt grupuri în raport cu operațiile de înmulțire obișnuite ;

(ii) Avem izomorfismul de grupuri $(M, \cdot) \approx (G, \cdot)$.

4.12. Fie T mulțimea matricelor de forma $\begin{pmatrix} x & y \\ -y & x \end{pmatrix}$ unde x și y

parcurs mulțimea \mathbb{Z}_3 a claselor de resturi modulo 3.

(i) Determinați numărul elementelor mulțimii T ;

(ii) Să se determine mulțimea G a matricelor $\begin{pmatrix} x & y \\ -y & x \end{pmatrix}$ din T a.î.

$$x^2 + y^2 = \hat{1} ;$$

(iii) Arătați că mulțimea G formează un grup față de operația de înmulțire a matricelor ;

(iv) Arătați că grupul G este izomorf cu grupul aditiv $(\mathbb{Z}_4, +)$ al claselor de resturi modulo 4.

4.13. (i) Fie $M = \left\{ \begin{pmatrix} a & 0 & ib \\ 0 & 0 & 0 \\ ib & 0 & a \end{pmatrix} \mid a, b \in \mathbb{R}, a^2 + b^2 \neq 0, i^2 = -1 \right\}$.

Arătați că M este un grup în raport cu înmulțirea matricelor, izomorf cu grupul (\mathbb{C}^*, \cdot) ;

(ii) Dacă $A = \begin{pmatrix} 1 & 0 & i \\ 0 & 0 & 0 \\ i & 0 & 1 \end{pmatrix}$, calculați A^{2002} (folosind eventual

izomorfismul dintre grupurile (\mathbb{C}^*, \cdot) și (M, \cdot)).

4.14. Să se arate că :

(i) Mulțimea $M = \left\{ D_k = \begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix}, k \in \mathbb{Z} \right\}$ formează grup în raport cu

operația de înmulțire a matricelor, grup izomorf cu grupul $(\mathbb{Z}, +)$;

(ii) Mulțimea $M = \left\{ M_k = \begin{pmatrix} 1 & 1 & 2k+1 \\ 0 & 0 & 1 \\ 0 & 0 & 1 \end{pmatrix}, k \in \mathbb{Z} \right\}$ este grup abelian în

raport cu înmulțirea matricelor, izomorf cu $(\mathbb{Z}, +)$;

(iii) Mulțimea $M = \left\{ A_a = \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}, a \in \mathbb{R} \right\}$ este subgrup al grupului

matricelor inversabile din $M_2(\mathbb{R})$, izomorf cu $(\mathbb{R}, +)$.

4.15. Fie $M = \left\{ M(a) = \begin{pmatrix} 2-a & a-1 \\ 2(1-a) & 2a-1 \end{pmatrix}, a \in \mathbb{R}^* \right\}$.

(i) Să se arate că (M, \cdot) este grup izomorf cu (\mathbb{R}^*, \cdot) ;

(ii) Să se calculeze $[M(a)]^n$, $a \in \mathbb{R}^*$.

4.16. Să se demonstreze că mulțimea:

$$G = \left\{ \begin{pmatrix} 1 & x & y \\ 0 & 1 & z \\ 0 & 0 & 1 \end{pmatrix} \mid x, y, z \in \mathbb{R} \right\}$$

este grup în raport cu înmulțirea matricelor, iar grupul automorfismelor lui G este infinit.

4.17. Pentru $n \geq 1$ fixat, se notează cu M mulțimea matricelor $A \in M_{2n}(\mathbb{R})$ de forma :

$$A(x) = \begin{pmatrix} x & 0 & 0 & \dots & 0 & 0 & x \\ 0 & x & 0 & \dots & 0 & x & 0 \\ 0 & 0 & x & \dots & x & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & x & 0 & \dots & 0 & x & 0 \\ x & 0 & 0 & \dots & 0 & 0 & x \end{pmatrix} \text{ cu } x \neq 0.$$

Să se arate că :

- (i) M este grup abelian față de înmulțirea matricelor ;
- (ii) Grupurile (M, \cdot) și (\mathbb{R}^*, \cdot) sunt izomorfe.

4.18. Fie $\alpha \in \mathbb{R}$ fixat și $A = \begin{pmatrix} 0 & 1 & -\sin \alpha \\ -1 & 0 & \cos \alpha \\ -\sin \alpha & \cos \alpha & 0 \end{pmatrix}$.

- (i) Să se calculeze A^3 ;
- (ii) Pentru $x \in \mathbb{R}$ definim $A_x = I_3 + xA + \frac{1}{2}x^2A^2$. Să se arate că

$G = \{ A_x \mid x \in \mathbb{R} \}$ este grup abelian în raport cu înmulțirea matricelor;

- (iii) $(G, \cdot) \approx (\mathbb{R}, +)$.

4.19. Fie $M_d = \left\{ \begin{pmatrix} a & db \\ b & a \end{pmatrix} \mid a, b \in \mathbb{R}, a^2 - db^2 \neq 0 \right\}$, unde $d \in \mathbb{R}$ este un număr

real fixat. Să se determine valorile lui d pentru care (M_d, \cdot) este grup izomorf cu grupul (\mathbb{C}^*, \cdot) .

4.20. Fie G_n mulțimea matricelor pătratiche de ordin n având pe fiecare linie câte un element egal cu 1 și celelalte elemente egale cu 0 și același lucru valabil și pe coloane.

Să se demonstreze că G_n este grup relativ la operația de înmulțire a matricelor iar $G_n \approx S_n$.

4.21. Se consideră (G, \circ) și (\mathbb{R}_+^*, \cdot) unde $G = (3, \infty)$ și

$$x \circ y = xy - 3x - 3y + 12, \text{ oricare ar fi } x, y \in G.$$

Să se arate că :

- (i) (G, \circ) este un grup abelian ;

(ii) Să se determine $a, b \in \mathbb{R}$ a.î. $f: \mathbb{R}_+^* \rightarrow (3, \infty)$, $f(x) = ax + b$ să fie un izomorfism de grupuri ;

(iii) Să se calculeze x^n , unde $x \in G$ și $n \in \mathbb{N}^*$.

4.22. $G = (5, \infty)$ și legea "o" definită prin

$$x \circ y = xy - 5x - 5y + 30, \text{ oricare ar fi } x, y \in G.$$

Să se arate că :

(i) (G, \circ) este un grup abelian;

(ii) $(G, \circ) \approx (\mathbb{R}_+^*, \cdot)$;

(iii) $(G, \circ) \approx (\mathbb{R}, +)$;

(iv) Să se calculeze x^n , unde $x \in G$ și $n \in \mathbb{N}^*$.

4.23. Fie $S = \{ A \in M_2(\mathbb{R}) \mid A + I_2 \text{ este inversabilă} \}$. Pe S definim \circ astfel: $A \circ B = A + B + AB$. Să se arate că (S, \circ) este grup izomorf cu grupul matricelor de ordin 2 cu elemente reale, inversabile.

4.24. Spunem că grupul (G, \cdot) are proprietatea $g(n)$ dacă conține cel puțin $n+1$ elemente și oricare ar fi $x_1, x_2, \dots, x_n \in G \setminus \{1\}$ există $x_{n+1} \in G$ a.î. $x_1 x_2 \dots x_n = x_{n+1}^n$.

Să se arate că:

(i) Dacă (G, \cdot) are proprietatea $g(n)$, atunci, pentru orice $x \in G$, există $y \in G$ a.î. $x = y^n$;

(ii) Grupul (\mathbb{R}_+^*, \cdot) are proprietatea $g(n)$;

(iii) $(\mathbb{R}_+^*, \cdot) \not\approx (\mathbb{R}^*, \cdot)$.

4.25. Fie G un grup pentru care $f: G \rightarrow G$, $f(x) = x^3$ este un morfism de grupuri. Să se arate că :

(i) Dacă f este un morfism injectiv, atunci (G, \cdot) este abelian ;

(ii) Dacă f este un morfism surjectiv, atunci (G, \cdot) este abelian.

4.26. Fie (G, \cdot) un grup și H un subgrup propriu al său. Să se arate că funcția $f: G \rightarrow G$, $f(x) = \begin{cases} x, & x \in H \\ 1, & x \in G \setminus H \end{cases}$ are proprietatea că duce subgrupuri în subgrupuri, dar nu este morfism de grupuri.

4.27. Fie G_1, G_2 grupuri, $f: G_1 \rightarrow G_2$ morfism de grupuri și $x \in G_1$.

Să se demonstreze că :

(i) Dacă $o(x) = n \in \mathbb{N}^* \Rightarrow o(f(x)) \mid n$;

(ii) Dacă f este izomorfism de grupuri, atunci $o(f(x))=o(x)$.

4.28. Fie G_1, G_2 două grupuri, (G_2 comutativ) iar

$$\text{Hom}(G_1, G_2) = \{ f: G_1 \rightarrow G_2 \mid f \text{ morfism de grupuri} \}.$$

Pentru $f, g \in \text{Hom}(G_1, G_2)$ definim $fg: G_1 \rightarrow G_2$ prin $(fg)(x) = f(x) \cdot g(x)$.

Să se demonstreze că :

(i) Dubletul $(\text{Hom}(G_1, G_2), \cdot)$ este grup comutativ ;

(ii) Dacă $G_1 = (\mathbb{Z}, +)$, atunci $\text{Hom}(\mathbb{Z}, G_2) \approx G_2$;

(iii) Dacă $G_1 = (\mathbb{Z}_m, +)$, $G_2 = (\mathbb{Z}_n, +)$, atunci $\text{Hom}(\mathbb{Z}_m, \mathbb{Z}_n) \approx \mathbb{Z}_d$, unde $d = (m, n)$, $(m, n \in \mathbb{N}^*)$.

4.29. Fie mulțimea $G = \{ f_n : (2, \infty) \rightarrow (2, \infty), f_n(x) = 2 + (x-2)^{2n}, n \in \mathbb{Z} \}$. Să se arate că (G, \circ) este grup abelian izomorf cu grupul abelian $(\mathbb{Z}, +)$.

4.30. Fie grupul $(\mathbb{Z}, +)$. Să se arate că :

(i) Funcțiile $f_m : \mathbb{Z} \rightarrow \mathbb{Z}$ definite prin $f_m(x) = mx$ sunt morfisme de grup ;

(ii) Orice morfism de la $(\mathbb{Z}, +)$ la $(\mathbb{Z}, +)$ este de acest tip ;

(iii) Să se determine automorfismele grupului $(\mathbb{Z}, +)$.

4.31. Fie $k > 0$. Pe mulțimea $G = (-k, k)$ se definește operația algebrică $a \circ b = \frac{k^2(a+b)}{k^2+ab}$. Să se arate că:

(i) (G, \circ) este grup abelian;

(ii) Funcția $f : G \rightarrow \mathbb{R}$, $f(t) = \int_0^t \frac{1}{k^2-x^2} dx$ este un izomorfism de grupuri

de la (G, \circ) la $(\mathbb{R}, +)$.

4.32. Pe \mathbb{R} considerăm operația algebrică

$$x \circ y = x\sqrt{1+y^2} + y\sqrt{1+x^2}.$$

Să se arate că (\mathbb{R}, \circ) este grup comutativ, izomorf cu $(\mathbb{R}, +)$.

4.33. Fie $a \in \mathbb{R}^*$ fixat, $M = \{ -\arctg \frac{1}{a} + k\pi \mid k \in \mathbb{Z} \}$, grupurile $G = (\mathbb{R}, +)$

și $H = (\mathbb{R}^*, \cdot)$ iar $f : G \rightarrow H$ o funcție definită prin:

$$f(x) = \begin{cases} \text{tg}x, & x \in M \\ a \sin x + \cos x, & x \in G \setminus M \end{cases}.$$

- (i) Arătați că există un subgrup G' al lui G pentru care restricția $f_{G'}$ a lui f la G' este morfism de grupuri ;
(ii) Determinați reuniunea subgrupurilor G' cu proprietatea de la (i).

4.34. Să se demonstreze că grupul $\text{Hom}(\mathbb{Q}, \mathbb{Z})$ este nul.

4.35. Să se demonstreze că dacă $n \geq 2$, atunci grupul $\text{Hom}(\mathbb{Z}_n, \mathbb{Z})$ este nul.

4.36. Fie G un grup finit iar $f: G \rightarrow G$ un morfism de grupuri ce nu are puncte fixe netriviale (adică $f(x) = x \Leftrightarrow x = 1$) și $f \circ f = 1_G$.
Să se demonstreze că G este comutativ.

4.37. Fie G un grup comutativ a.î. singurul automorfism al său este cel identic.

Să se arate că $x^2 = 1$, oricare ar fi $x \in G$.

4.38. Fie G un grup cu proprietatea că aplicațiile $f(x) = x^4$ și $g(x) = x^8$ sunt automorfisme ale lui G . Să se arate că G este abelian.

4.39. Fie (G, \cdot) un grup și $f \in \text{End}(G)$.

(i) Dacă aplicațiile $x \rightarrow xf(x)$ și $x \rightarrow x^2f(x)$ sunt endomorfisme ale lui G , atunci G este abelian;

(ii) Dacă aplicațiile $x \rightarrow x^2f(x)$ și $x \rightarrow x^4f(x)$ sunt endomorfisme ale lui G , atunci G este abelian.

4.40. Fie (G, \cdot) un grup finit și $f \in \text{Aut}(G)$. Să se demonstreze că f are un singur punct fix dacă și numai dacă funcția $F: G \rightarrow G$, $F(x) = x^{-1}f(x)$ este bijectivă.

4.41. Fie (G, \cdot) un grup, $f, g: G \rightarrow G$ endomorfisme și $H \subset G$ un subgrup propriu. Dacă $f = g$ pe $G \setminus H$, atunci $f = g$ pe G .

4.42. Fie G un grup și presupunem că există $n \in \mathbb{N}$, $n \geq 2$ a.î. $f: G \rightarrow G$, $f(x) = x^n$, pentru orice $x \in G$ este un automorfism al lui G .

Să se demonstreze că pentru orice $x \in G \Rightarrow x^{n-1} \in Z(G)$.

4.43. Fie (G, \cdot) un grup. Dacă există $n \in \mathbb{N}^*$ astfel încât funcțiile $f, g: G \rightarrow G$, $f(x) = x^n$, $g(x) = x^{n+1}$ să fie morfisme surjective de grup, atunci grupul G este abelian.

4.44. Să se demonstreze că singurul morfism de grupuri de la grupul $(\mathbb{Q}, +)$ la grupul simetric (S_n, \circ) este cel nul ($n \in \mathbb{N}^*$).

4.45. Fie p un număr prim, $p \geq 2$. Să se demonstreze că singurul morfism de grupuri de grupul $(\mathbb{Z}_p, +)$ la grupul (\mathbb{Z}_p^*, \cdot) este cel nul.

4.46. Definiți pe $(1, 2) \subset \mathbb{R}$ o operație care să confere acestei mulțimi structură de grup izomorf cu grupul multiplicativ al numerelor reale strict pozitive $((0, \infty), \cdot)$.

4.47. Să se determine toate morfismele de grupuri de la grupul $(\mathbb{Q}, +)$ la grupul (\mathbb{Q}^*, \cdot) .

4.48. Să se arate că grupul $(\mathbb{Q}, +)$ nu este izomorf cu nici un subgrup propriu al său.

4.49. Fie G un grup și pentru $a \in G$, $\varphi_a: G \rightarrow G$, $\varphi_a(x) = axa^{-1}$.

(i) Să se demonstreze că pentru orice $a \in G$, $\varphi_a \in \text{Aut}(G)$;

(ii) Aplicația $\varphi: G \rightarrow \text{Aut}(G)$, $\varphi(a) = \varphi_a$, este morfism de grupuri iar $\text{Ker}(\varphi) = Z(G)$;

(iii) Dacă notăm $\text{Im}(\varphi) = \text{Inn}(G)$, să se arate că $|\text{Inn}(G)| = 1 \Leftrightarrow G$ este comutativ.

Observație. φ_a poartă numele de *automorfism interior* al lui G .

4.50. Fie G un grup. Să se demonstreze că dacă $Z(G) = \{1\}$, atunci și $Z(\text{Aut}(G)) = \{1\}$.

4.51. Să se determine toate grupurile care admit un singur automorfism.

4.52. Să se determine toate grupurile comutative și finite care au un număr impar de automorfisme.

4.53. Să se demonstreze că un grup ciclic este izomorf cu $(\mathbb{Z}, +)$ sau cu $(\mathbb{Z}_n, +)$, după cum grupul respectiv este infinit sau are n elemente.

4.54. Să se demonstreze că dacă un grup are un număr finit de subgrupuri, atunci și el este finit.

4.55. Arătați că orice grup infinit are o infinitate de subgrupuri distincte.

4.56. Să se demonstreze că un grup cu 4 elemente este izomorf cu \mathbb{Z}_4 sau cu grupul lui Klein, iar $\mathbb{Z}_4 \not\cong K$.

4.57. Fie G un grup cu proprietatea că G se scrie ca reuniune de trei subgrupuri diferite de G , dintre care două au câte două elemente. Să se arate că G este izomorf cu grupul lui Klein.

4.58. Să se demonstreze că un grup cu 6 elemente este izomorf cu \mathbb{Z}_6 sau cu S_3 , iar $\mathbb{Z}_6 \not\cong S_3$ (vezi problema 4.75.).

4.59. Să se demonstreze că grupurile aditive $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$ și $(\mathbb{R}, +)$ nu sunt izomorfe două câte două.

4.60. Să se demonstreze că grupurile aditive $(\mathbb{R}, +)$ și $(\mathbb{C}, +)$ sunt izomorfe.

4.61. Să se demonstreze că grupurile multiplicative (\mathbb{Q}^*, \cdot) , (\mathbb{R}^*, \cdot) și (\mathbb{C}^*, \cdot) nu sunt izomorfe două câte două.

4.62. Fie $\mathbb{Q}_+^* = \{x \in \mathbb{Q} : x > 0\}$ și $\mathbb{R}_+^* = \{x \in \mathbb{R} : x > 0\}$.

Să se demonstreze că:

(i) $\mathbb{Q}_+^* \leq (\mathbb{Q}^*, \cdot)$ și $\mathbb{R}_+^* \leq (\mathbb{R}^*, \cdot)$;

(ii) $(\mathbb{R}_+^*, \cdot) \approx (\mathbb{R}, +)$, $(\mathbb{Q}_+^*, \cdot) \approx (\mathbb{Q}, +)$.

4.63. Să se demonstreze că grupurile $(\mathbb{Z}, +)$ și (\mathbb{Q}^*, \cdot) nu sunt izomorfe.

4.64. Să se arate că $(\mathbb{Q}, +)$ nu este izomorf cu grupul $(\mathbb{Q}[i], +)$ ($\mathbb{Q}[i] = \{a + bi \in \mathbb{C} \mid a, b \in \mathbb{Q}\}$).

4.65. Să se demonstreze că grupurile $(\mathbb{Z}, +)$ și $(\mathbb{Z}[X], +)$ nu sunt izomorfe.

4.66. Să se demonstreze că grupurile aditive $(\mathbb{Q}, +)$ și $(\mathbb{Q}[X], +)$ nu sunt izomorfe.

4.67. Să se demonstreze că grupurile aditive $(\mathbb{Z}[X], +)$ și $(\mathbb{Q}[X], +)$ nu sunt izomorfe.

4.68. Determinați endomorfismele grupului $(\mathbb{R}, +)$ integrabile pe $[-b, b]$, unde $b > 0$ este un număr real fixat.

4.69. Să se arate că orice grup de matrice din $M_2(\mathbb{C})$ în raport cu înmulțirea matricelor, al cărui element neutru este diferit de I_2 , este izomorf cu un subgrup al grupului (\mathbb{C}^*, \cdot)

4.70. Fie $(K, +, \cdot)$ un corp netrivial ($0 \neq 1$). Să se demonstreze că grupurile $(K, +)$ și (K^*, \cdot) nu sunt izomorfe.

4.71. Fie G un grup a.î. $G/Z(G)$ este ciclic. Să se arate că G este grup abelian.

4.72. Fie G un grup, $H \trianglelefteq G$ și presupunem că $|H| = m \in \mathbb{N}^*$.

Considerăm de asemenea $x \in G$ și $n \in \mathbb{N}^*$ a.î. $(m, n) = 1$.

Să se demonstreze că:

(i) Dacă $o(x) = n$, atunci $o(xH) = n$ (xH privit ca element în G/H);

(ii) Dacă $o(xH) = n$ (în G/H), atunci există $y \in G$ a.î. $o(y) = n$ și $xH = yH$.

4.73. Fie G un grup comutativ iar H subgrupul elementelor de ordin finit.

Să se demonstreze că în G/H orice element diferit de 1 are ordinul infinit.

4.74. Fie G un grup finit, p un număr prim, $p \geq 2$ a.î. $p \mid |G|$. Să se demonstreze că există $x \in G$ a.î. $o(x) = p$ (echivalent cu există $H \leq G$ a.î. $|H| = p$).

Observație. Acest rezultat este datorat lui *Cauchy*.

4.75. Fie p un număr prim, $p \geq 2$. Să se demonstreze că orice grup necomutativ cu $2p$ elemente este izomorf cu grupul diedral D_p .

4.76. Fie G un grup finit iar p un număr prim, $p \geq 2$.

Să se demonstreze că următoarele afirmații sunt echivalente:

(i) Ordinul oricărui element al lui G este o putere naturală a lui p ;

(ii) $|G|$ este o putere naturală a lui p .

Observație. Un grup în care ordinul oricărui element este o putere naturală a lui p se zice p -grup.

4.77. Fie p un număr prim, $p \geq 2$. Să se demonstreze că dacă G este un p -grup finit, atunci $|Z(G)| \geq p$.

4.78. Fie p un număr prim, $p \geq 2$. Să se demonstreze că orice grup finit cu p^2 elemente este comutativ.

4.79. Să se determine toate grupurile G cu proprietatea că orice automorfism, diferit de cel identic, admite un punct fix.

4.80. Considerăm $Z \leq (\mathbb{Q}, +)$.

(i) Să se descrie grupul cât \mathbb{Q}/Z și să se demonstreze că orice element din acest grup are ordin finit ;

(ii) Să se arate că pentru orice număr natural $n \geq 2$, \mathbb{Q}/Z are un singur subgrup de ordin n iar acesta este ciclic.

4.81. Fie G un p -grup finit cu $|G| = p^m$ ($m \in \mathbb{N}$). Să se demonstreze că există subgrupurile normale G_0, G_1, \dots, G_m ale lui G a.î. $1 = G_0 < G_1 < \dots < G_m = G$ și $|G_i| = p^i$ pentru orice $0 \leq i \leq m$.

4.82. Caracterizați grupurile finite cu proprietatea că toate subgrupurile sale proprii au același număr de elemente.

4.83. Considerăm $Z \leq (\mathbb{R}, +)$ și $T = \{z \in \mathbb{C}^* : |z| = 1\}$.

Să se demonstreze că:

(i) $T \leq (\mathbb{C}^*, \cdot)$ și $\mathbb{R}/Z \approx T$;

(ii) $\mathbb{C}^*/T \approx (\mathbb{R}_+^*, \cdot)$;

(iii) $\mathbb{R}_+^* \leq (\mathbb{C}^*, \cdot)$ și $\mathbb{C}^*/\mathbb{R}_+^* \approx T$;

(iv) $\mathbb{R} \leq (\mathbb{R}, +)$ și $\mathbb{C}/\mathbb{R} \approx (\mathbb{R}, +)$.

4.84. Fie $n \in \mathbb{N}^*$ și $A = \{1, 2, \dots, n^2\}$. Construiți un izomorfism între grupurile $(P(A), \Delta)$ și $(M_n(\mathbb{Z}_2), +)$.

4.85. Fie $n \in \mathbb{N}$, $n \geq 3$ iar Q_n un grup de ordin 2^n generat de două elemente a și b ce verifică relațiile:

$$a^{2^{n-2}} = b^2 = (ab)^2.$$

Să se demonstreze că dacă G este un grup de ordin 2^n generat de două elemente a și b ce verifică relațiile $a^{2^{n-1}} = 1$, $bab^{-1} = a^{-1}$ și $b^2 = a^{2^{n-2}}$, atunci $G \approx \mathbf{Q}_n$.

Observație. \mathbf{Q}_3 (care se mai notează și prin \mathbf{Q} sau \mathbf{C}_8) poartă numele de grupul quaternionilor iar \mathbf{Q}_n ($n \geq 4$) de grupul generalizat al quaternionilor.

4.86. În monoidul multiplicativ $M_2(\mathbb{C})$ considerăm matricele:

$$j = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, k = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \text{ iar } G = \langle j, k \rangle, J = \langle j \rangle, K = \langle k \rangle.$$

Să se demonstreze că $|G| = 8$, $|J| = |K| = 4$, $J, K \trianglelefteq G$ iar $G \approx \mathbf{Q}_3$.

4.87. În monoidul multiplicativ $M_2(\mathbb{C})$ considerăm matricele:

$$A = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}, B = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \text{ iar } G = \langle A, B \rangle.$$

Să se demonstreze că $G \approx \mathbf{Q}_3$.

4.88. Considerăm mulțimea $G = \{\pm 1, \pm i, \pm j, \pm k\}$ cu următoarea regulă de multiplicare: $i^2 = j^2 = k^2 = -1$, $ij = k$, $jk = i$, $ki = j$, $ji = -k$, $kj = -i$, $ik = -j$, -1 și 1 fiind supuse multiplicării obișnuite.

Să se demonstreze că $G \approx \mathbf{Q}_3$.

4.89. Să se caracterizeze $Z(\mathbf{Q}_3)$.

4.90. Să se demonstreze că $\mathbf{Q}_3/Z(\mathbf{Q}_3)$ este comutativ.

4.91. Să se demonstreze că $\mathbf{Q}_3 \not\approx \mathbf{D}_4$.

4.92. Să se demonstreze că un grup necomutativ cu 8 elemente este izomorf cu \mathbf{Q}_3 sau cu \mathbf{D}_4 .

4.93. Să se demonstreze că dacă G este un grup, atunci $G/Z(G) \approx \text{Inn}(G)$.

4.94. Fie $n \in \mathbb{N}^*$ și K un corp.

Să se arate că aplicația $\alpha : GL_n(K) \rightarrow GL_n(K)$, $\alpha(A) = (A^t)^{-1}$, oricare ar fi $A \in GL_n(K)$ este corect definită și că $\alpha \in \text{Aut}(GL_n(K))$.

Demonstrați de asemenea că dacă K nu este \mathbb{Z}_2 sau \mathbb{Z}_3 , atunci α nu este automorfism interior al lui $GL_n(K)$.

4.95. Să se demonstreze că numărul structurilor de grup ce se pot defini pe o mulțime cu n elemente, izomorfe cu o structură de grup fixat (G, \cdot) este egal cu $n! / |\text{Aut}(G, \cdot)|$.

4.96. Să se demonstreze că numărul structurilor de grup ciclic ce se pot defini pe o mulțime cu n elemente este egal cu $n! / \varphi(n)$, unde φ este indicatorul lui Euler.

Să se deducă de aici că numărul structurilor de grup ciclic ce se poate defini pe o mulțime cu n elemente (n prim) este egal cu $(n-2)! \cdot n$.

4.97. Să se demonstreze că $(\mathbb{Q}, +)$ este divizibil.

4.98. Să se demonstreze că dacă p este un număr prim, atunci grupul (U_{p^∞}, \cdot) este divizibil (vezi problema 3.19.).

4.99. Să se demonstreze că orice grup comutativ divizibil conține un subgrup izomorf cu (\mathbb{Q}, \cdot) sau cu un grup de forma (U_{p^∞}, \cdot) cu p prim (vezi problema 3.19.).

4.100. Să se demonstreze că orice grup factor al unui grup divizibil este divizibil.

4.101. Să se demonstreze că în categoria grupurilor abeliene obiectele injective sunt exact grupurile divizibile

§5. Produse directe de grupuri

5.1. Dacă H, K sunt grupuri, să se demonstreze că $H \times \{1\} \trianglelefteq H \times K$ și $\{1\} \times K \trianglelefteq H \times K$.

5.2. Să se demonstreze că dacă $\{G_i\}_{i \in I}$ este o familie finită de grupuri, atunci $Z(\prod_{i \in I} G_i) = \prod_{i \in I} Z(G_i)$.

Să se deducă de aici că un produs direct de grupuri este comutativ dacă și numai dacă fiecare din factorii produsului este comutativ.

5.3. Fie G un grup iar $\hat{G} = \Delta_G = \{(x, x) : x \in G\}$.

Să se demonstreze că :

(i) $\hat{G} \leq G \times G$, $\hat{G} \approx G$;

(ii) $\hat{G} \trianglelefteq G \times G \Leftrightarrow G$ este comutativ;

(iii) $N_{G \times G}(\hat{G}) = \hat{G} \Leftrightarrow Z(G) = 1.$

5.4. Fie G un grup iar $H, K \trianglelefteq G$ a.î. $G = H \cdot K.$

Să se demonstreze că $G/(H \cap K) \approx G/H \times G/K.$

5.5. Fie H, K două grupuri, $J \trianglelefteq H, L \trianglelefteq K.$

Să se demonstreze că

$$(J \times L) \trianglelefteq H \times K \text{ și } (H \times K) / (J \times L) \approx H/J \times K/L.$$

5.6. Să se demonstreze că $(\mathbb{C}^*, \cdot) \approx (\mathbb{R}^*, \cdot) \times (\mathbb{T}, \cdot).$

5.7. Să se demonstreze că $(\mathbb{Q}^*, \cdot) \approx (\mathbb{Q}_+^*, \cdot) \times (\{-1, 1\}, \cdot).$

5.8. Să se demonstreze că $(\mathbb{R}^*, \cdot) \approx (\mathbb{R}_+^*, \cdot) \times (\{-1, 1\}, \cdot).$

5.9. Să se demonstreze că $(\mathbb{C}^*, \cdot) \approx (\mathbb{R}, +) \times (\mathbb{R}/\mathbb{Z}, +).$

5.10. Să se demonstreze că $(\mathbb{C}, +) \approx (\mathbb{R}, +) \times (\mathbb{R}, +).$

5.11. Să se demonstreze că :

(i) $(\mathbb{R}, +) \approx (\mathbb{R}, +) \times (\mathbb{R}, +);$

(ii) $(\mathbb{Q}, +) \not\approx (\mathbb{Q}, +) \times (\mathbb{Q}, +).$

5.12. Să se demonstreze că $(\mathbb{Q}^*, \cdot) \approx (\mathbb{Z}_2, +) \times (\mathbb{Z}[X], +).$

5.13. Să se demonstreze că grupul $(\mathbb{Z}, +) \times (\mathbb{Z}, +)$ nu este ciclic.

5.14. Să se descrie subgrupurile grupului $(\mathbb{Z}, +) \times (\mathbb{Z}, +).$

5.15. Să se demonstreze că dacă n este un număr natural, $n \geq 2$, atunci grupul $(\mathbb{Z}, +) \times (\mathbb{Z}_n, +)$ nu este ciclic.

5.16. Fie K un corp iar $H = \left\{ \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} : a, b, c \in K \right\}.$

Să se demonstreze că :

$$H \leq GL_3(K), Z(H) \approx (K, +) \text{ și } H/Z(H) \approx (K, +) \times (K, +).$$

5.17. Să se caracterizeze :

(i) grupurile abeliene finite cu p^n elemente (p prim, $p \geq 2$, $n \in \mathbb{N}^*$);

(ii) grupurile abeliene finite cu $p_1^{n_1} p_2^{n_2} \dots p_s^{n_s}$ elemente (p_1, \dots, p_s numere prime distincte două câte două iar $n_1, \dots, n_s \in \mathbb{N}^*$).

5.18. Să se caracterizeze grupurile comutative cu 8 elemente.

5.19. Să se demonstreze că un grup cu 9 elemente este izomorf cu \mathbb{Z}_9 sau cu $\mathbb{Z}_3 \times \mathbb{Z}_3$.

5.20. Să se demonstreze că un grup cu 10 elemente este izomorf cu \mathbb{Z}_{10} sau cu D_5 .

5.21. Fie $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\mathbb{Z})$ cu $\det(A) = -1$ sau 1 . Să se demonstreze

că funcția $t_A: \mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z} \times \mathbb{Z}$ definită prin $t_A(x, y) = (ax + by, cx + dy)$, este un automorfism al lui $\mathbb{Z} \times \mathbb{Z}$ și că oricare alt automorfism al lui $\mathbb{Z} \times \mathbb{Z}$ este de forma t_A .

5.22. Fie p, q numere prime distincte, $p > q$ și G un grup abelian a.î. $|G| = pq$.

Să se arate că :

(i) Dacă $q \nmid p-1$, atunci G este ciclic ;

(ii) Dacă $q \mid p-1$, atunci G este generat de două elemente a și b

satisfăcând condițiile $a^q = b^p = 1$, $a^{-1}ba = b^r$, cu $r \not\equiv 1 \pmod{p}$ însă $r^q \equiv 1 \pmod{q}$.

5.23. Să se demonstreze că un grup cu 15 elemente este ciclic (deci izomorf cu $(\mathbb{Z}_{15}, +)$).

5.24. Să se caracterizeze grupurile finite de ordin p^3 (p prim).

5.25. Să se caracterizeze grupurile cu 12 elemente.

5.26. Să se facă un tabel de caracterizare a grupurilor cu cel mult 15 elemente.

**§6. Inel. Subinel. Exemple. Calcule în inele.
 Caracteristica unui inel. Elemente inversabile.
 Divizori ai lui zero. Elemente idempotente.
 Elemente nilpotente. Produse directe de inele.**

6.1. Să se determine toate legile de compoziție $*$ de pe \mathbb{Z} pentru care $(\mathbb{Z}, *, +)$ este inel.

6.2. Fie $(A, +, \cdot)$ un inel. Definim pe A operația algebrică $*$ prin:

$$x * y = x + y - xy, \text{ oricare ar fi } x, y \in A.$$

Să se arate că $*$ este asociativă și are element neutru. Mai mult, dacă inelul A este unitar și $1-x$ este inversabil ($x \in A$), atunci și x este inversabil față de operația $*$.

6.3. Notăm cu A mulțimea funcțiilor aritmetice, adică $A = \{f: \mathbb{N}^* \rightarrow \mathbb{C}\}$. Pe mulțimea A introducem operația algebrică $*$ definită astfel $(f, g) \rightarrow f * g$, unde $(f * g)(n) = \sum_{d|n} f(d)g\left(\frac{n}{d}\right)$, oricare ar fi $n \in \mathbb{N}^*$ (vezi problema **1.18**). Se cere:

(i) Să se demonstreze că $(A, *)$ este monoid comutativ;

(ii) Notând cu $(U(A), *)$ grupul elementelor inversabile din monoidul $(A, *)$, să se demonstreze echivalența: $f \in U(A) \Leftrightarrow f(1) \neq 0$;

(iii) Notând cu M mulțimea funcțiilor aritmetice multiplicative nenule, adică $M = \{f \in A \mid f(nm) = f(n)f(m) \text{ dacă } (n, m) = 1 \text{ și există } k \in \mathbb{N}^* \text{ cu } f(k) \neq 0\}$, să se demonstreze că $(M, *)$ este subgrup al lui $(U(A), *)$;

(iv) Să se demonstreze că tripletul $(A, +, *)$ este domeniu de integritate.

6.4. Să se arate că mulțimea

$$A = \left\{ M(a) = \begin{pmatrix} a & 0 & a \\ 0 & 0 & 0 \\ a & 0 & a \end{pmatrix} \mid a \in C \right\}$$

împreună cu operațiile obișnuite de adunare și înmulțire a matricelor este un domeniu de integritate.

6.5. Pe mulțimea $\mathbb{Z} \times \mathbb{Z} = \{(x, y) \mid x, y \in \mathbb{Z}\}$ definim operațiile algebrice:

$$(x, y) + (x', y') = (x+x', y+y')$$

$$(x, y) \cdot (x', y') = (xx', xy'+x'y), \text{ oricare ar fi } (x, y), (x', y') \in \mathbb{Z} \times \mathbb{Z}.$$

Să se arate că $(\mathbb{Z} \times \mathbb{Z}, +, \cdot)$ devine inel unitar și comutativ.

6.6. Fie $M_2(\mathbb{C})$ mulțimea matricelor pătratice de ordinul al doilea cu elemente din \mathbb{C} . Dacă $A, B \in M_2(\mathbb{C})$, notăm $[A, B] = AB - BA$. Să se arate că:

(i) $[A, B]^2$ comută cu orice matrice din $M_2(\mathbb{C})$;

(ii) Dacă $A, B, C, D \in M_2(\mathbb{C})$, atunci matricea

$$[A, B] \cdot [C, D] + [C, D] \cdot [A, B]$$

comută cu orice matrice din $M_2(\mathbb{C})$.

6.7. Să se determine

(i) Matricele $X \in M_2(\mathbb{Z}_2)$ a.î. $X^2 + I_2 = O_2$;

(ii) Matricele $X \in M_2(\mathbb{Z}_3)$ a.î. $X^2 = I_2$.

6.8. Fie A un inel care conține nondivizori ai lui zero atât la stânga cât și la dreapta. Dacă A are un număr finit de elemente, să se demonstreze că inelul A este unitar.

6.9. Fie A un inel cu 5 elemente. Să se arate că A este de caracteristică 5 și pe baza acestui rezultat să se demonstreze că A este comutativ.

6.10. Fie A un inel.

(i) Dacă $\text{car}(A) = 2$ și $x \in A$, să se exprime $(x+1)^n$ ca sumă de puteri ale lui x pentru $n \in \{2, 3, 4, 5\}$;

(ii) Dacă există $n \in \mathbb{N}^*$ a.î. $x^{n+1} = x^n$ pentru orice $x \in A$, să se arate că $\text{car}(A) = 2$ și $x^2 = x$, pentru orice $x \in A$.

6.11. Fie A un inel de caracteristică 2 a.î. pentru orice $x \in A$, $x^2 = 0$ sau $x^2 = 1$.

(i) Să se demonstreze că A este comutativ;

(ii) Să se dea exemplu de inel cu 4 elemente având proprietățile de mai sus.

6.12. Fie A un inel cu proprietatea că oricare ar fi $n \in \mathbb{N}^*$ ecuația $x^n = 0$ are în A numai soluția $x = 0$. Să se arate că:

(i) Dacă $ab=0$ (cu $a, b \in A$), atunci $ba=0$ și $axb=0$ pentru orice $x \in A$;

(ii) Dacă $a_1 a_2 a_3 = 0$ (cu $a_1, a_2, a_3 \in A$), atunci $a_2 a_3 a_1 = a_3 a_1 a_2 = 0$;
 (iii) Dacă $a_1 a_2 \dots a_n = 0$ (cu $a_k \in A, 1 \leq k \leq n$), atunci $a_{i_1} a_{i_2} \dots a_{i_n} = 0$ oricare ar fi permutarea (i_1, \dots, i_n) a mulțimii $\{1, 2, \dots, n\}$.

6.13. Fie A un inel cu proprietatea că dacă $x^2 = 0$ atunci $x = 0$. Notăm $M = \{a \in A \mid a^2 = a\}$. Să se arate că:

- (i) Dacă $a, b \in M$ rezultă $a + b - 2ab \in M$;
- (ii) Dacă M este finită atunci numărul elementelor lui M este o putere naturală a lui 2.

6.14. Fie A un inel necomutativ unitar iar $a, b \in A$. Să se arate că dacă $1-ab$ este inversabil, atunci și $1-ba$ este inversabil.

6.15. Fie $(A, +, \cdot)$ un inel unitar și $a, b \in A$ cu proprietatea că există $n \in \mathbb{N}^*$ a. î. $(aba)^n = 0$. Să se demonstreze că elementele $1-a^2b$ și $1-ba^2$ sunt inversabile.

6.16. Fie $(A, +, \cdot)$ un inel cu elementul unitate 1. Spunem că elementul $x \in A$ are proprietatea (P) dacă există $a, b \in A$ care comută cu x , cu b inversabil, a. î. $x^2 - ax + b = 0$.

- (i) Să se arate că în inelul $(M_2(\mathbb{C}), +, \cdot)$ o matrice X are proprietatea (P) dacă și numai dacă ea este nesingulară;
- (ii) Dacă x are proprietatea (P), atunci oricare putere a lui x are această proprietate.

6.17. Fie A un inel unitar și $a, b \in A$ a. î. a, b și $ab-1$ sunt inversabile. Să se arate că elementele $a-b^{-1}$ și $(a-b^{-1})^{-1} - a^{-1}$ sunt inversabile.
 Mai mult, are loc egalitatea $((a-b^{-1})^{-1} - a^{-1})^{-1} = aba - a$.

6.18. Fie A un inel și $a \in A$ a. î. există $b \in A$ cu proprietatea că $a \cdot b = 1$. Atunci următoarele afirmații sunt echivalente:

- (i) $\text{card}\{x \in A \mid a \cdot x = 1\} > 1$;
- (ii) a nu este inversabil;
- (iii) există $c \in A, c \neq 0$, a. î. $a \cdot c = 0$.

6.19. Fie A un inel și $a \in A$, a neinvertibil.

Fie $X = \{x \in A \mid ax = 1\}$.

Dacă $X \neq \emptyset$, atunci X este o mulțime infinită.

6.20. Fie $(A, +, \cdot)$ un inel comutativ cu un număr finit de divizori ai lui zero. Dacă $D = \{d_1, d_2, \dots, d_n\}$ este mulțimea acestor divizori demonstrați că $d_1 + d_2 + \dots + d_n \in D \cup \{0, 1\}$.

6.21. Fie $(A, +, \cdot)$ un inel comutativ cu $1+1 \neq 0$, iar D mulțimea divizorilor lui zero. Considerăm mulțimea $G = \{x \in D \mid 2x = 0\} \cup \{0\}$.
Demonstrați că $(G, +)$ este grup abelian.

6.22. Fie $n \in \mathbb{N}$, $n \geq 2$. Să se arate că în inelul $(\mathbb{Z}_n, +, \cdot)$ numărul elementelor inversabile este egal cu cel al celor neinvertabile dacă și numai dacă $n = 2^k$, cu $k \in \mathbb{N}^*$.

6.23. Fie A mulțimea tuturor funcțiilor continue $f: [0, 1] \rightarrow \mathbb{R}$.

(i) Arătați că A formează inel comutativ în raport cu operațiile de adunare și înmulțire a funcțiilor;

(ii) Un element $f \in A$, $f \neq 0$, este divizor al lui zero dacă și numai dacă mulțimea punctelor x pentru care $f(x) = 0$ conține un interval;

(iii) Să se determine elementele $f \in A$ a.î. $f^2 = f$;

(iv) Să se determine elementele inversabile ale inelului A .

6.24. Să se demonstreze că dacă A este un inel atunci:

(i) $Z(A)$ este subinel comutativ al lui A ;

(ii) Dacă $x^2 - x \in Z(A)$, oricare ar fi $x \in A$, atunci A este comutativ.

6.25. Fie A un inel și funcția $f: A \times A \rightarrow A$, definită prin

$$f(x, y) = (xy)^2 - x^2y^2.$$

(i) Să se calculeze valoarea expresiei

$$E(x, y) = f(1+x, 1+y) - f(1+x, y) - f(x, 1+y) + f(x, y),$$

unde $1 \in A$ este elementul unitate al inelului A ;

(ii) Dacă inelul A are proprietatea că $x+x = 0$ implică $x = 0$ și dacă $(xy)^2 - (yx)^2 = x^2y^2 - y^2x^2$ oricare ar fi $x, y \in A$, atunci A este comutativ.

6.26. Să se demonstreze că orice inel unitar cu pq elemente, unde p, q sunt numere prime nu neapărat distincte, este comutativ.

6.27. Fie A un inel unitar. Arătați că dacă $x, y \in A$ sunt a.î. $x^n y = 0 = (x+1)^m y$ pentru anumiți $m, n \in \mathbb{N}$, atunci $y = 0$.

6.28. Fie A un inel unitar și $n \geq 2$ un întreg fixat. Presupunem că $(xy)^n = x^n y^n$ și $(xy)^{n+1} = x^{n+1} y^{n+1}$, pentru orice $x, y \in A$.

Arătați că $y(xy)^n = (xy)^n y$, oricare ar fi $x, y \in A$.

6.29. Fie A un inel unitar, $n \geq 1$ un număr natural fixat. Presupunem că $(xy)^n = x^n y^n$, $(xy)^{n+1} = x^{n+1} y^{n+1}$ și $(xy)^{n+2} = x^{n+2} y^{n+2}$, pentru orice $x, y \in A$.

Atunci A este comutativ.

6.30. Fie $n \geq 2$ un număr natural fixat și A un inel integru care verifică următoarele două condiții:

- 1) $x^n - x \in Z(A)$, pentru orice $x \in A$;
 - 2) centrul $Z(A)$ al lui A conține cel puțin n elemente.
- Să se demonstreze că inelul A este comutativ.

6.31. Fie A un inel unitar și $x \in A$ un element fixat. Presupunem că pentru orice $y \in A$ există întregii relativ primi $n = n(y) \geq 1$ și $m = m(y) \geq 1$ a.î. $[x, y^n] = 0 = [x, y^m]$. Atunci $x \in Z(A)$.

6.32. Fie inelul $\mathbb{Z}[\sqrt{2}] = \{m+n\sqrt{2} \mid m, n \in \mathbb{Z}\}$ (împreună cu adunarea și înmulțirea obișnuite).

Definim funcția $\varphi: \mathbb{Z}[\sqrt{2}] \rightarrow \mathbb{N}$, $\varphi(m+n\sqrt{2}) = |m^2 - 2n^2|$.

Să se arate că:

- (i) $\varphi(z) = 0 \Leftrightarrow z = 0$;
- (ii) $\varphi(zz') = \varphi(z)\varphi(z')$, oricare ar fi $z, z' \in \mathbb{Z}[\sqrt{2}]$;
- (iii) $\mathbb{Z}[\sqrt{2}]$ are o infinitate de elemente inversabile.

6.33. Fie $d \in \mathbb{Z} \setminus \{0, 1\}$ un întreg liber de pătrate. Definim funcția normă: $N: \mathbb{Z}[\sqrt{d}] \rightarrow \mathbb{Z}$ prin $N(a+b\sqrt{d}) = a^2 - db^2$, pentru orice $a, b \in \mathbb{Z}$.

Să se demonstreze că:

- (i) $N(z_1 z_2) = N(z_1) \cdot N(z_2)$, oricare ar fi $z_1, z_2 \in \mathbb{Z}[\sqrt{d}]$;
- (ii) Elementul $z \in \mathbb{Z}[\sqrt{d}]$ este inversabil în inelul $(\mathbb{Z}[\sqrt{d}], +, \cdot)$ dacă și numai dacă $N(z) \in \{\pm 1\}$;

(iii) Notând cu $U(\mathbb{Z}[\sqrt{d}])$ grupul multiplicativ al elementelor inversabile din inelul $\mathbb{Z}[\sqrt{d}]$, avem pentru $d = -1$, $U(\mathbb{Z}[i]) = \{1, -1, i, -i\}$, respectiv pentru $d \leq -2$, $U(\mathbb{Z}[\sqrt{d}]) = \{-1, 1\}$.

6.34. Fie inelul $(\mathbb{Z}[i] = \{m+ni | m, n \in \mathbb{Z}\}, +, \cdot)$.

Definim funcția $\varphi: \mathbb{Z}[i] \rightarrow \mathbb{N}$, $\varphi(m+ni) = m^2+n^2$.

Să se arate că:

(i) $\varphi(z) = 0 \Leftrightarrow z = 0$;

(ii) $\varphi(zz') = \varphi(z)\varphi(z')$, oricare ar fi $z, z' \in \mathbb{Z}[i]$;

(iii) Dacă $z, z' \in \mathbb{Z}[i]$, $z' \neq 0$, există $q, r \in \mathbb{Z}[i]$ a.î. $z = z'q + r$, unde $\varphi(r) < \varphi(z')$;

(iv) $\varphi(z) = 1 \Leftrightarrow z$ este inversabil $\Leftrightarrow z \in \{\pm 1, \pm i\}$.

Observație. Inelul $(\mathbb{Z}[i], +, \cdot)$ poartă numele de *inelul întregilor lui Gauss*.

6.35. Fie inelul $\mathbb{Z}[i\sqrt{2}] = \{m+ni\sqrt{2} | m, n \in \mathbb{Z}\}$ (împreună cu operațiile de adunare și înmulțire obișnuite).

Definim funcția $\varphi: \mathbb{Z}[i\sqrt{2}] \rightarrow \mathbb{N}$, $\varphi(m+ni\sqrt{2}) = m^2+2n^2$.

Să se arate că:

(i) $\varphi(z) = 0 \Leftrightarrow z = 0$;

(ii) $\varphi(zz') = \varphi(z)\varphi(z')$, oricare ar fi $z, z' \in \mathbb{Z}[i\sqrt{2}]$;

(iii) Dacă $z, z' \in \mathbb{Z}[i\sqrt{2}]$, $z' \neq 0$, există $q, r \in \mathbb{Z}[i\sqrt{2}]$ a.î. $z = z'q + r$, unde $\varphi(r) < \varphi(z')$;

(iv) $\varphi(z) = 1 \Leftrightarrow z$ este inversabil $\Leftrightarrow z \in \{\pm 1\}$.

6.36. Fie A un inel unitar și comutativ.

Să se arate că suma dintre un element inversabil și un element nilpotent este element inversabil în A .

Observație. Un element $x \in A$ se numește *nilpotent* dacă există $n \in \mathbb{N}$ a.î. $x^n = 0$.

6.37. Fie $A = \left\{ \begin{pmatrix} a & b & c \\ 0 & a & d \\ 0 & 0 & a \end{pmatrix} \mid a, b, c, d \text{ numere reale} \right\}$. Să se arate că

$(A, +, \cdot)$ este un inel unitar necomutativ în care orice element este inversabil sau nilpotent.

6.38. Fie $n = p_1^{\alpha_1} \dots p_k^{\alpha_k} \in \mathbb{N}^*$. Demonstrați că $\hat{m} \in \mathbb{Z}_n$ este element nilpotent dacă și numai dacă $p_1 \dots p_k$ divide m .

6.39. Fie $n = p_1^{\alpha_1} \dots p_r^{\alpha_r}$ descompunerea în factori primi distincți a numărului natural n . Să se arate că există o bijecție între mulțimea elementelor idempotente ale lui \mathbb{Z}_n ($\text{Idemp}(\mathbb{Z}_n)$) și mulțimea A a părților mulțimii $\{p_1, \dots, p_r\}$.

În particular, să se arate că \mathbb{Z}_n are 2^r elemente idempotente și pentru $n=12$ să se găsească elementele idempotente ale lui \mathbb{Z}_{12} .

6.40. În inelul $(\mathbb{Z}_n, +, \cdot)$ al claselor de resturi modulo n , să se determine mulțimea $N = \{ \hat{x} \mid \hat{x} \in \mathbb{Z}_n \text{ a.î. există } k \in \mathbb{N} \text{ și } \hat{x}^k = \hat{0} \}$.

Fie de asemenea, $I = \{ \hat{x} \mid \hat{x} \in \mathbb{Z}_n \text{ a.î. există } k \in \mathbb{N} \text{ și } \hat{x}^k = \hat{x} \}$.

Să se arate că $N \cap I = \{ \hat{0} \}$.

6.41. Fie $n \in \mathbb{N}$, $n \geq 2$. Să se arate că $\hat{a} \in \mathbb{Z}_n$ este inversabil $\Leftrightarrow (a, n) = 1$.

6.42. Fie ecuația $\hat{a}\hat{x} = \hat{b}$, cu $\hat{a}, \hat{b} \in \mathbb{Z}_n$. Să se arate că:

(i) Dacă $(a, n) = d > 1$ și $d \nmid b$ ecuația nu are nici o soluție;

(ii) Dacă $(a, n) = d > 1$ și $d \mid b$ atunci ecuația are d soluții distincte;

(iii) Dacă $(a, n) = 1$ ecuația are soluție unică.

6.43. Fie $a, b \in \mathbb{Z}_n$, $a \neq 0$, $b \neq 0$. Dacă ecuația $ax = b$ are soluții, atunci numărul soluțiilor ei este egal cu numărul de soluții ale ecuației $ax = 0$.

6.44. Să se rezolve în \mathbb{Z}_{12} următoarele sisteme de ecuații:

$$(i) \begin{cases} \hat{3}x + \hat{2}y = \hat{1} \\ \hat{4}x + \hat{3}y = \hat{2} \end{cases} \quad (ii) \begin{cases} \hat{7}x + \hat{3}y = \hat{2} \\ \hat{4}x + \hat{6}y = \hat{3} \end{cases}$$

6.45. Fie A un *inel boolean* (adică un inel cu proprietatea că $x^2 = x$ pentru orice $x \in A$). Să se arate că:

- (i) Inelul A este de caracteristică 2 (deci $x+x = 0$, pentru orice $x \in A$);
- (ii) A este comutativ.

6.46. Demonstrați că fiind dat un inel comutativ A , el este boolean dacă și numai dacă nu are elemente nilpotente nenule și pentru orice $a, b \in A$ are loc egalitatea $(a+b)ab = 0$.

6.47. Fie A un inel cu proprietatea că pentru orice $a \in A$ avem $a^3 + a = 0$. Arătați că inelul A este boolean.

6.48. Fie $(A, +, \cdot)$ un inel cu proprietățile:

- 1) Pentru orice $x \in A$, $x+x = 0$;
- 2) Pentru orice $x \in A$, există $k = k(x) \in \mathbb{N}^*$ a. î. $x^{2^k+1} = x$. Demonstrați că $x^2 = x$, pentru orice $x \in A$.

6.49. Fie $(A, +, \cdot)$ un inel boolean și $x, a, b \in A$ a. î. $a = xab$. Atunci $a = xa$. De asemenea, dacă $x = a+b+ab$ atunci $a = xa$ și $b = xb$.

Pentru $a_1, \dots, a_n \in A$ găsiți un element $x \in A$ a. î. $a_i = xa_i$, oricare ar fi $1 \leq i \leq n$.

6.50. Fie A un inel unitar a. î. $x^6 = x$, oricare ar fi $x \in A$. Demonstrați că $x^2 = x$, oricare ar fi $x \in A$.

6.51. Fie A un inel unitar cu proprietatea că $x^{12} = x$, pentru orice $x \in A$. Demonstrați că $x^2 = x$, oricare ar fi $x \in A$.

6.52. Fie A un inel a. î. $x^3 = x$, oricare ar fi $x \in A$.

- (i) Să se calculeze $(x^2yx^2-x^2y)^2$ și $(x^2yx^2-yx^2)^2$ unde $x, y \in A$;
- (ii) Să se arate că inelul A este comutativ.

6.53. Fie A un inel finit. Să se arate că există două numere naturale $m, p, m > p \geq 1$ a. î. $a^m = a^p$, oricare ar fi $a \in A$.

6.54. Fie $(A, +, \cdot)$ un inel și $a, b \in A$, a inversabil. Să se arate că dacă relația:

$$a^k \cdot b^k = (a-b)(a^{k-1} + a^{k-2}b + \dots + ab^{k-2} + b^{k-1})$$

este satisfăcută pentru $k = m, m+1, m+2$ ($m \in \mathbb{N}$), atunci $ab = ba$.

6.55. Fie $(A, +, \cdot)$ un inel cu proprietatea că există $n \in \mathbb{N}$ $n \geq 2$ a.î. $x^{n+1} = x^n$, oricare ar fi $x \in A$. Să se arate că:

(i) $x^2 = 0 \Rightarrow x = 0$;

(ii) $x^2 = x$, oricare ar fi $x \in A$.

6.56. Fie $p \geq 2$ un număr prim. Un inel A se zice *p-inel* dacă sunt verificate următoarele două condiții:

1) $px = \underbrace{x + \dots + x}_{\text{de } p \text{ ori}} = 0$, pentru orice $x \in A$,

2) $x^p = x$, pentru orice $x \in A$.

Să se demonstreze că orice *p-inel* unitar este comutativ.

6.57. Fie A un inel unitar cu proprietatea că $(xy)^2 = x^2y^2$, pentru orice $x, y \in A$. Atunci A este comutativ.

6.58. Fie A un inel care nu are elemente nilpotente nenule. Arătați că orice element idempotent din A aparține lui $Z(A)$.

6.59. Fie A un inel cu element unitate $1 \neq 0$ și $M = \{x \in A \mid x^2 = x\}$ mulțimea elementelor sale idempotente. Să se demonstreze că dacă M este mulțime finită, atunci M are un număr par de elemente.

6.60. Fie A un inel comutativ finit cu $1 \neq 0$. Să se calculeze produsul elementelor idempotente nenule din inelul A .

6.61. Pentru un inel A de caracteristică 2, notăm

$$O_A = \{x \in A \mid x^2 = 0\},$$

$$E_A = \{x \in A \mid x^2 = 1\},$$

$$I_A = \{x \in A \mid x^2 = x\}.$$

Arătați că:

(i) Dacă $x \in O_A$, atunci $1+x \in E_A$;

Dacă $x \in E_A$, atunci $1+x \in O_A$;

Dacă $x \in I_A$, atunci $1+x \in I_A$.

(ii) $|O_A| = |E_A|$.

6.62. Fie $d > 1$ un întreg liber de pătrate.

(i) Să se determine inelele A cu proprietatea $\mathbb{Z} \subseteq A \subseteq \mathbb{Z}[\sqrt{d}]$, operațiile din A fiind cele induse de adunarea și înmulțirea din $\mathbb{Z}[\sqrt{d}]$;

(ii) Să se determine inelele B cu proprietatea $\mathbb{Q} \subseteq B \subseteq \mathbb{Q}(\sqrt{d})$, operațiile din B fiind cele induse de adunarea și înmulțirea din $\mathbb{Q}(\sqrt{d})$.

6.63. Fie A un inel. Dacă

$$T = \{(a_{ij}) \in M_n(A) \mid a_{ij} = 0, \text{ oricare ar fi } i, j \in \{1, \dots, n\}, i > j\}$$

este o mulțime de matrice, atunci T este subinel al lui $(M_n(A), +, \cdot)$.

6.64. Fie A un inel și S o submulțime oarecare a lui A . Mulțimea $C(S)$ a elementelor din A care comută cu elementele lui S formează un subinel al lui A . Dacă $A = M_n(\mathbb{R})$, \mathbb{R} fiind un inel unitar oarecare și mulțimea $S \subset A$ este formată doar din matricea (a_{ij}) definită prin $a_{ij} = \delta_{j,i+1}$, atunci să se determine $C(S)$.

6.65. Fie p un număr prim. Arătați că mulțimea $\mathbb{Z}_{(p)}$ a numerelor raționale de forma $\frac{a}{b}$, cu $a, b \in \mathbb{Z}$ iar p nu divide numitorul b , formează un subinel al inelului \mathbb{Q} al numerelor raționale.

6.66. (i) Aflați subinelele inelului \mathbb{Z} al numerelor întregi;

(ii) Arătați că mulțimea $\mathbb{Z}[\frac{1}{2}]$ a numerelor raționale de forma $\frac{a}{2^n}$, cu $a \in \mathbb{Z}$ și $n \in \mathbb{N}$, formează un subinel al inelului \mathbb{Q} al numerelor raționale.

6.67. Este $\{m+n\sqrt[3]{5} \mid m, n \in \mathbb{Z}\}$ subinel al lui \mathbb{C} ?

6.68. Fie A_1 și A_2 două inele unitare și fie adunarea și înmulțirea pe $A_1 \times A_2$ definite astfel:

$$(x_1, x_2) + (y_1, y_2) = (x_1 + y_1, x_2 + y_2)$$

$$(x_1, x_2) \cdot (y_1, y_2) = (x_1 \cdot y_1, x_2 \cdot y_2).$$

Să se arate că $A_1 \times A_2$ cu aceste operații este un inel unitar care are divizori ai lui zero.

Să se determine elementele inversabile ale acestui inel în funcție de elementele inversabile ale inelelor A_1 și A_2 .

Aplicație: a) $A_1 = A_2 = \mathbb{Z}$

b) $A_1 = \mathbb{Z}, A_2 = \mathbb{Q}$

c) $A_1 = \mathbb{Z}_m, A_2 = \mathbb{Z}_n$.

6.69. Calculați caracteristica inelelor $\mathbb{Z} \times \mathbb{Z}, \mathbb{Z}_3 \times \mathbb{Z}, \text{End}(\mathbb{Z})$ și $\text{End}(\mathbb{Z}_3)$.

6.70. Pentru $m, n \in \mathbb{N}^*$ demonstrați că $\text{car}(\mathbb{Z}_m \times \mathbb{Z}_n) = [m, n]$. Generalizare.

6.71. Dați exemplu de un inel unitar, comutativ, care nu este corp având caracteristica un număr prim.

6.72. Arătați că $\mathbb{Z}_4 \times \mathbb{Z}_4$ are exact trei subinele unitare.

6.73. Fie A un inel cu 4 elemente, de caracteristică 2.

(i) Arătați că există $a \in A, a \neq 0, a \neq 1$ a.î.:

1) $A = \{0, 1, a, 1+a\}$ și $a^2 = 0$ sau

2) $A = \{0, 1, a, 1+a\}$ și $a^2 = a$ sau

3) $A = \{0, 1, a, 1+a\}$ și $a^2 = 1+a$.

(ii) Dați câte un exemplu de inel pentru fiecare din tipurile de la punctul (i).

6.74. (i) Fie A și B două inele (comutative). Determinați elementele nilpotente ale inelului $A \times B$;

(ii) Aflați numărul elementelor nilpotente din inelul \mathbb{Z}_n .

§7. Morfisme de inele. Izomorfisme de inele.

7.1. Să se dea un exemplu de inel neunitar.

Dacă A este un inel neunitar, există un inel unitar B ce conține pe A ca subinel.

7.2. Fie A un inel, S o mulțime și $f : A \rightarrow S$ o aplicație bijectivă. Să se arate că există o unică structură de inel pe S a.î. f să devină morfism de inele.

Dacă $g : S \rightarrow C$ este o aplicație, cu C inel oarecare, să se demonstreze că g este morfism de inele pentru structura introdusă pe S dacă și numai dacă $g \circ f$ este morfism de inele.

7.3. Să se determine numărul structurilor de inel neizomorfe care pot fi definite pe o mulțime cu 4 elemente.

7.4. Dacă p este un număr prim, să se demonstreze că există doar două tipuri de inel cu p elemente.

7.5. Să se arate că pe grupul aditiv $G = (\mathbb{Z}_n, +)$ există $\varphi(n)$ operații de înmulțire care înzestreză pe G cu o structură de inel unitar (φ fiind indicatorul lui Euler). Sunt ele izomorfe?

Să se descrie toate operațiile de înmulțire care se pot defini pe grupul aditiv $H = (\mathbb{Q}/\mathbb{Z}, +)$, operații pentru care H devine inel unitar.

7.6. Să se caracterizeze morfismele de inele de la \mathbb{Z} la \mathbb{Z}_n ($n \geq 2$).

7.7. Fie m, n numere naturale $m, n \geq 2$. Să se caracterizeze morfismele de inele de la \mathbb{Z}_m la \mathbb{Z}_n .

7.8. Fie A un inel comutativ și unitar și $f, g : \mathbb{Q} \rightarrow A$ două morfisme de inele unitare ($f(1) = g(1) = 1_A$). Dacă $f(n) = g(n)$, oricare ar fi $n \in \mathbb{Z}$, atunci $f = g$.

7.9. Fie A, A' două inele unitare iar $f : A \rightarrow A'$ un morfism de inele unitare.

Să se arate că f duce elemente inversabile în elemente inversabile, elemente nilpotente în elemente nilpotente iar în ipoteza că este injecție și divizori ai lui zero în divizori ai lui zero.

7.10. Fie $I = \{f : [0,1] \rightarrow \mathbb{R} \mid f \text{ continuă}\}$ și $I' = \{f : [0,1] \rightarrow \mathbb{R} \mid f \text{ derivabilă}\}$.

Să se demonstreze că inelele $(I, +, \cdot)$ și $(I', +, \cdot)$ nu sunt izomorfe (unde $+$ și \cdot sunt operațiile uzuale de adunare și înmulțire a funcțiilor reale).

7.11. Fie $f : A \rightarrow A'$ un morfism surjectiv de inele unitare și comutative. Analizați afirmația: „ $f(a)$ este divizor al lui zero dacă și numai dacă a este divizor al lui zero”.

7.12. Fie A un inel unitar și comutativ.

Să se arate că următoarele afirmații sunt echivalente:

(i) A conține cel puțin un element idempotent diferit de 0 și 1;

(ii) A este izomorf cu produsul direct $B \times C$ a două inele comutative, unitare (nenule).

7.13. Arătați că:

(i) Inelul $T_2(\mathbb{Z})$ al matricelor de ordinul doi, triunghiulare (adică au sub diagonala principală toate elementele zero), cu componente întregi, nu este comutativ ; determinați centrul acestui inel ;

(ii) Funcția $\varphi : T_2(\mathbb{Z}) \rightarrow \mathbb{Z} \times \mathbb{Z}$ ce asociază unei matrice triunghiulare oarecare $\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}$ din $T_2(\mathbb{Z})$ perechea (a, c) din $\mathbb{Z} \times \mathbb{Z}$ formată din elementele de pe diagonala principală, este morfism de inele.

7.14. Pentru fiecare $k \in \mathbb{Z}$ se consideră mulțimea de matrice $A_k = \left\{ \begin{pmatrix} a & b \\ kb & a \end{pmatrix} \mid a, b \in \mathbb{Z} \right\}$.

(i) Să se demonstreze că A_k este inel comutativ (față de adunarea și înmulțirea matricelor) ;

(ii) Pentru ce valori ale lui k , inelul A_k are divizori ai lui zero ?

(iii) Să se demonstreze că inelele A_k și A_p sunt izomorfe dacă și numai dacă $k=p$.

7.15. Fie $d \in \mathbb{Z}$ un întreg liber de pătrate.

Să se arate că:

(i) Mulțimea $\mathbb{Z}[\sqrt{d}] = \{m+n\sqrt{d} \mid m, n \in \mathbb{Z}\}$ împreună cu adunarea și înmulțirea numerelor este un inel unitar și comutativ izomorf cu inelul A_d (definit la problema 7.14.) ;

(ii) Dacă $d' \in \mathbb{Z}$ este un alt număr liber de pătrate, atunci inelele $\mathbb{Z}[\sqrt{d}]$ și $\mathbb{Z}[\sqrt{d'}]$ sunt izomorfe dacă și numai dacă $d = d'$.

7.16. Dacă M este o mulțime nevidă, atunci $(P(M), \Delta, \cap)$ este inel boolean. În cazul în care $M = \{1, 2, \dots, m\}$ cu $m \geq 1$, atunci inelul $(P(M), \Delta, \cap)$ este izomorf cu inelul $(\underbrace{\mathbb{Z}_2 \times \dots \times \mathbb{Z}_2}_{de\ m\ ori}, +, \cdot)$.

7.17. Fie A un inel boolean a.î. $|A| = n > 1$. Arătați că există $m \geq 1$ a.î. $n = 2^m$ și $(A, +, \cdot) \simeq (\underbrace{\mathbb{Z}_2 \times \dots \times \mathbb{Z}_2}_{de\ m\ ori}, +, \cdot)$.

7.18. Să se arate că:

(i) Pe o mulțime finită A cu $n \geq 2$ elemente se poate introduce o structură de inel boolean dacă și numai dacă $n = 2^k$, $k \in \mathbb{N}^*$;

(ii) Pe mulțimea numerelor naturale se poate introduce o structură de inel boolean.

7.19. Fie E o mulțime și \mathbb{Z}_2^E inelul funcțiilor definite pe E cu valori în \mathbb{Z}_2 , cu adunarea și înmulțirea induse de adunarea și înmulțirea din \mathbb{Z}_2 . Să se arate că \mathbb{Z}_2^E este izomorf cu inelul părților mulțimii E ale cărei operații sunt:

$$E_1 + E_2 = E_1 \Delta E_2 \text{ și } E_1 \cdot E_2 = E_1 \cap E_2.$$

Să se arate că toate elementele din aceste inele sunt idempotente.

În particular, deduceți că pentru două mulțimi disjuncte M și N are loc următorul izomorfism de inele $P(M \cup N) \simeq P(M) \times P(N)$ (unde $P(M)$ desemnează inelul părților lui M relativ la operațiile Δ și \cap).

7.20. Fie A un inel. Să se arate că există o corespondență bijectivă între mulțimea morfismelor de inele definite pe \mathbb{Z} cu valori în A și mulțimea idempotenților lui A . Câte morfisme de inele există de la \mathbb{Z} într-un domeniu de integritate? Dacă A este un inel unitar să se arate că există un singur morfism de inele unitare de la \mathbb{Z} în A .

7.21. (i) Fie $(G, +)$ un grup comutativ. Arătați că mulțimea $\text{End}(G) = \{f: G \rightarrow G \mid f \text{ este morfism de grupuri}\}$ este un inel în raport cu adunarea și compunerea morfismelor;

(ii) Fie $(A, +)$ grupul aditiv subiacent al unui inel (unitar) și comutativ, $(A, +, \cdot)$. Arătați că inelul $(\text{End}(A), +, \circ)$ este comutativ dacă și numai dacă este izomorf cu $(A, +, \cdot)$.

7.22. Fie G grupul subiacent inelului produs direct $(\underbrace{\mathbb{Z} \times \dots \times \mathbb{Z}}_{\text{de } n \text{ ori}}, +, \cdot)$.

Arătați că inelul $\text{End}(G)$ (definit la problema 7.21.) este izomorf cu inelul de matrice $M_n(\mathbb{Z})$.

7.23. Să se arate că grupul aditiv al unui inel integru nu este izomorf cu grupul multiplicativ al elementelor sale inversabile.

7.24. Fie A și B două inele necomutative și $f: A \rightarrow B$ cu proprietățile:

1) $f(x+y) = f(x) + f(y)$, oricare ar fi $x, y \in A$;

2) Pentru orice $x, y \in A$ avem $f(xy) = f(x)f(y)$ sau $f(xy) = f(y)f(x)$.

Să se demonstreze că f este morfism de inele sau antimorfism de inele.

Observație. Reamintim că $f : A \rightarrow B$ se numește *antimorfism* de inele dacă pentru orice $x, y \in A$ avem $f(x+y) = f(x) + f(y)$ și $f(xy) = f(y)f(x)$.

§8. Ideale. Latticea idealelor unui inel comutativ. Anulatorul și radicalul unui inel. Factorizarea unui inel printr-un ideal bilateral. Ideale prime. Ideale maximale.

8.1. Să se dea exemplu de un inel în care există subinele ce nu sunt ideale.

8.2. Să se dea exemplu de inel în care reuniunea a două ideale ale sale nu este ideal.

8.3. Arătați că mulțimea idealelor $\text{Id}(A)$ ale unui inel comutativ A formează o lattice completă.

8.4. Fie inelul comutativ $A = \{f: [-1, 1] \rightarrow \mathbb{R}\}$ împreună cu operațiile uzuale de adunare și înmulțire a funcțiilor. Care din următoarele submulțimi ale lui A sunt ideale și care doar subinele:

(i) $P = \{f \in A \mid f \text{ este funcție polinomială}\};$

(ii) $P_n = \{f \in P \mid \text{grad}(f) \leq n\};$

(iii) $Q_n = \{f \in P_n \mid \text{grad}(f) = n\};$

(iv) $B = \{f \in A \mid f(0) = 0\};$

(v) $C = \{f \in A \mid f(0) = 1\}?$

8.5. Să se arate că există inele în care divizorii lui zero nu formează un ideal.

8.6. Dați exemplu de un morfism de inele $f: A \rightarrow A'$ și de un ideal I al lui A a.î. $f(I)$ să nu fie ideal în A' .

8.7. Fie A un inel unitar și comutativ a.î. să existe $u \in A$, $u \neq 0$ și $u \neq 1$ cu $u^2 = u$. Fie $A_1 = \{ux \mid x \in A\}$.

(i) Să se demonstreze că A_1 este un subinel al lui A care are unitate.

(ii) Să se arate apoi că există un subinel A_2 al lui A a.î.:

a) A_2 este unitar;

b) Fiecare element al lui A se exprimă ca $x_1 + x_2$ cu $x_1 \in A_1$ și $x_2 \in A_2$;

c) Dacă $x_1 \in A_1$ și $x_2 \in A_2$ atunci $x_1 x_2 = 0$;
d) $A_1 \cap A_2 = \{0\}$.
(iii) Să se arate că funcția $f: A \rightarrow A_1 \times A_2$, $f(x) = (x_1, x_2)$, unde $x = x_1 + x_2$ este un izomorfism de inele.

8.8. Arătați că inelul $M_2(\mathbb{R})$ nu are ideale bilaterale netriviale.

8.9. Să se dea exemplu de inel necomutativ și de ideale stângi (drepte) care nu sunt ideale drepte (stângi).

8.10. Fie n un număr natural $n \geq 1$. Să se arate că asocierea $d \rightsquigarrow \hat{d} \in \mathbb{Z}_n$ constituie un antiizomorfism de latici între laticea divizorilor (pozitivi) ai lui n cu ordinea $d < d'$ dacă $d|d'$ și laticea idealelor lui \mathbb{Z}_n .

8.11. Să se determine forma generală a numerelor naturale $n \geq 1$ pentru care laticea idealelor lui \mathbb{Z}_n este total ordonată.

8.12. Există pentru orice latice cu un număr finit de elemente, un număr natural n a.î. ea să fie izomorfă (ca latice) cu laticea idealelor lui \mathbb{Z}_n ?

8.13. Să se stabilească o corespondență bijectivă între mulțimea idealelor bilaterale ale unui inel unitar A și mulțimea idealelor bilaterale ale lui $M_n(A)$, $n \geq 1$.

8.14. Să se arate că dacă $m, n \in \mathbb{Z}$ atunci $n\mathbb{Z} + m\mathbb{Z} = D\mathbb{Z}$, $n\mathbb{Z} \cap m\mathbb{Z} = M\mathbb{Z}$, unde prin D și M am notat cel mai mare divizor comun respectiv cel mai mic multiplu comun al numerelor m și n .

8.15. Fie I, J, K ideale în inelul comutativ A . Arătați că dacă $I \subseteq K$ atunci $(I+J) \cap K = I + (J \cap K)$.

8.16. Fie A un inel, I, J, L ideale bilaterale în A a.î. $I+J = A$ și $I \supseteq JL$. Să se arate că $L \subseteq I$.

8.17. Demonstrați că într-un inel boolean orice ideal finit generat este principal.

8.18. Fie A un inel comutativ și I un ideal finit generat al lui A a.î. $I = I^2$. Să se găsească un element idempotent $e \in A$ a.î. $I = Ae$.

8.19. Dați exemplu de un morfism de inele comutative $f:A \rightarrow A'$ și de un ideal maximal M al lui A' a.î. $f^{-1}(M) \neq A$ și $f^{-1}(M)$ nu este ideal maximal în A .

8.20. Se pot pune în evidență un număr infinit de ideale prime în inelul \mathbb{Z} ?

8.21. Să se dea exemplu de un inel în care nu orice ideal prim este maximal.

8.22. Să se arate că pentru orice număr natural $n \geq 1$ există un inel care are n ideale.

8.23. Demonstrați că $R = \left\{ \begin{pmatrix} 0 & a \\ 0 & b \end{pmatrix} \mid a, b \in \mathbb{Q} \right\}$ este un subinel necomutativ al lui $M_2(\mathbb{Q})$. Dacă $I = \{A \in R \mid A^2 = O_2\}$ atunci I este ideal și $R/I \simeq \mathbb{Q}$.

8.24. Fie $f:A \rightarrow A'$ un morfism de inele, I un ideal în A . Arătați că $f^{-1}(f(I)) = I + \text{Ker}(f)$.

8.25. În $\mathbb{Z}[i]$, inelul întregilor lui Gauss, arătați că (3) și $(1+i)$ sunt ideale prime dar (2) nu este ideal prim.

8.26. Fie A un inel (comutativ) și P un ideal al său. Următoarele afirmații sunt echivalente:

(i) P este prim;

(ii) Oricare ar fi idealele I și J ale inelului A , dacă P conține produsul IJ , atunci P conține pe I sau pe J .

8.27. Fie A un inel unitar și S un sistem multiplicativ al său (adică $S \neq \emptyset$, $1 \in S$, $0 \notin S$ și dacă $s_1, s_2 \in S \Rightarrow s_1 s_2 \in S$). Arătați că dacă I este un ideal maximal relativ la proprietatea $I \cap S = \emptyset$, atunci I este ideal prim.

8.28. Fie A un domeniu de integritate. Arătați că în $A[X]$ intersecția tuturor idealelor maximale este idealul zero.

8.29. Fie A un inel comutativ unitar finit. Atunci demonstrați că orice ideal prim în A este și ideal maximal în inelul A .

8.30. Fie A un inel comutativ și unitar a.î. pentru orice $a \in A$ există un $n \geq 1$ cu $a^n = a$. Atunci, orice ideal prim din A este și maximal.

8.31. Arătați că în inelul $\mathbb{Z}[X, Y]$ idealul (X) este prim dar nu este maximal.

8.32. Fie A un inel comutativ unitar și $a \in A$. Atunci:

(i) $A[X] / (X, a) \simeq A/(a)$;

(ii) (X, a) este ideal prim (respectiv maximal) în $A[X] \Leftrightarrow (a)$ este ideal prim (respectiv maximal) în A ;

(iii) (X) este ideal prim dar nu este maximal în $\mathbb{Z}[X]$.

8.33. Pentru un inel A notăm cu $J(A)$ intersecția tuturor idealelor maximale din A .

Să se arate că:

(i) $J(A) = \{x \in A \mid 1 - xy \in U(A), \text{ oricare ar fi } y \in A\}$;

(ii) $J(A)$ este cel mai mare ideal I din A (relativ la incluziune) cu proprietatea că dacă $x \in I$ atunci $1 - x \in U(A)$.

8.34. Fie $A = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \mid a, b, c \in \mathbb{Z} \right\}$ subinel în $M_2(\mathbb{Z})$.

Arătați că $J(A) = \left\{ \begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix} \mid b \in \mathbb{Z} \right\}$.

8.35. Dați exemplu de inel (fără unitate) a. î. nu orice ideal al său să fie inclus într-un ideal maximal.

8.36. Dacă A este un inel integru, arătați că $J(A[X]) = 0$.

8.37. Fie A un inel comutativ. Dacă I este un ideal al lui A , atunci *anulatorul* lui I se definește ca fiind

$$\text{Ann}(I) = \{x \mid x \in A \text{ și } i \cdot x = 0, \text{ pentru orice } i \in I\}$$

și *radicalul* lui I ca fiind

$$r(I) = \{x \mid x \in A \text{ și există } n \in \mathbb{N} \text{ a.î. } x^n \in I\}.$$

(i) Arătați că $\text{Ann}(I)$ și $r(I)$ sunt ideale ale inelului A ;

(ii) Dacă I și J sunt ideale ale lui A atunci

$$1) r(r(I)) = r(I),$$

- 2) $r(I \cap J) = r(I) \cap r(J)$,
 3) $r(I + J) = r(r(I) + r(J))$.

8.38. Arătați că în inelul cât $A / r(A)$ nu există elemente nilpotente nenule.

8.39. Fie $f:A \rightarrow A'$ un morfism surjectiv de inele comutative cu unitate, al cărui nucleu $\text{Ker}(f)$ este conținut în $r(A)$.

Să se arate că dacă $a' \in A'$ este un element idempotent atunci există un singur element idempotent $a \in A$ a.î. $f(a) = a'$.

Deduceți că f induce o bijecție între mulțimile elementelor idempotente ale celor două inele.

8.40. Să se determine numărul elementelor idealului $r(\mathbb{Z} / n\mathbb{Z})$, $n \geq 2$ în funcție de n . Să se deducă în particular, că $\mathbb{Z} / n\mathbb{Z}$ este un inel redus dacă și numai dacă n nu se divide prin pătratul unui număr prim.

Observație. Un inel comutativ A se numește *reduc* dacă $r(A) = 0$.

8.41. Fie inelul $A = C([0, 1], \mathbb{R}) = \{f:[0,1] \rightarrow \mathbb{R} \mid f \text{ este continuă}\}$ (față de adunarea și înmulțirea definite prin $(f+g)(x) = f(x)+g(x)$ și $(f \cdot g)(x) = f(x) \cdot g(x)$). Arătați că $I = \{f \in A \mid f(0) = 0\}$ este un ideal ce nu este principal.

8.42. Fie d un număr întreg nenul liber de pătrate și $\mathbb{Z}[\sqrt{d}]$ subinelul corpului complex \mathbb{C} format din numerele de forma $a+b\sqrt{d}$ cu $a, b \in \mathbb{Z}$.

Fie $x = a+b\sqrt{d} \in \mathbb{Z}[\sqrt{d}]$. Să se determine un generator $t > 0$ al idealului $(x) \cap \mathbb{Z}$ în funcție de a și b . Să se arate că idealul (x) este nul dacă și numai dacă $(x) \cap \mathbb{Z}$ este nul.

8.43. Determinați idealele inelului $T_2(\mathbb{Z}_2)$ al matricelor de ordinul doi, triunghiulare, cu componente în \mathbb{Z}_2 .

8.44. Notăm cu A mulțimea matricelor de forma $\begin{pmatrix} a & p \\ 0 & b \end{pmatrix}$, cu $a, b \in \mathbb{Z}$ iar $p \in \mathbb{Q}$ și cu B mulțimea matricelor de forma $\begin{pmatrix} a & p \\ 0 & q \end{pmatrix}$, cu $a \in \mathbb{Z}$ și $p, q \in \mathbb{Q}$. Arătați că B este subinel al inelului $T_2(\mathbb{Q})$ iar A este subinel al lui B . Determinați idealele bilaterale ale inelelor A și B .

8.45. Fie A un inel, J un ideal bilateral al lui A iar I un ideal stâng al lui A . Dacă I și J sunt nilpotente arătați că $I + J$ este nilpotent.

Observație. Un ideal I se numește *nilpotent* dacă există $n \in \mathbb{N}^*$ a.î. $I^n = 0$, unde $I^n = \underbrace{I \cdot \dots \cdot I}_{\text{de } n \text{ ori}}$.

8.46. Arătați că nu există nici o structură de inel unitar care să aibă ca grup subiacent pe \mathbb{Q} / \mathbb{Z} .

8.47. Fie I și J ideale într-un inel comutativ A . Arătați că morfismul canonic de inele $A / I \cap J \rightarrow A/I \times A/J$ ($x + I \cap J \rightarrow (x+I, x+J)$) este izomorfism dacă și numai dacă $I+J = A$.

Observație. Idealele I și J cu proprietatea că $I + J = A$ se zic *ideale comaximale*.

8.48. Fie A produsul direct $\prod_{i=1}^n A_i$ al inelelor unitare A_1, A_2, \dots, A_n . Să se arate că orice ideal stâng (drept sau bilateral) $I \subseteq A$ satisface identitatea $I = \prod_{i=1}^n p_i(I)$, unde $p_i: A \rightarrow A_i$ reprezintă a i -a proiecție canonică. Observați că identitatea de mai sus nu este satisfăcută în general de subgrupurile unui produs direct de grupuri. Dați exemple de subgrupuri ale grupului aditiv $\mathbb{Z} \times \mathbb{Z}$ care nu sunt ideale ale inelului $\mathbb{Z} \times \mathbb{Z}$.

8.49. Fie A produsul direct $\prod_{i=1}^n A_i$ al inelelor unitare A_1, A_2, \dots, A_n și $I = \prod_{i=1}^n I_i \subseteq A$ un ideal (vezi problema 8.48.). Să se arate că $A/I \simeq \prod_{i=1}^n A_i / I_i$.

8.50. Fie A și B două inele comutative. Determinați idealele produsului $A \times B$. Aplicație: $\mathbb{Z} \times \mathbb{Z}$ și $K \times K$, unde K este un corp necomutativ.

8.51. Fie A un inel unitar și comutativ și $a \in A$ un nondivizor al lui zero și sistemul multiplicativ $S = \{a^n\}_{n \geq 0}$. Să se arate că inelele $S^{-1}A$ și $A[X] / (aX-1)$ sunt izomorfe.

8.52. Să se arate că $\mathbb{Z}[\sqrt{d}] / (x)$ este finit dacă și numai dacă x este un element nenul în $\mathbb{Z}[\sqrt{d}]$.

8.53. Să se arate că grupul unităților inelului $\mathbb{Z} / 2^n\mathbb{Z}$ este izomorf cu grupul aditiv $\mathbb{Z} / 2\mathbb{Z} \times \mathbb{Z} / 2^{n-2}\mathbb{Z}$, pentru $n \geq 3$.

Să se arate că pentru $n = 1, 2$ grupul unităților lui $\mathbb{Z} / 2^n\mathbb{Z}$ este ciclic.

8.54. Să se arate că grupul unităților inelului $\mathbb{Z} / p^n\mathbb{Z}$ este ciclic pentru orice număr prim $p \neq 2$ și n număr natural.

§9. Corp. Subcorp. Caracteristica unui corp. Morfisme de corpuri. Izomorfisme de corpuri.

9.1. Să se arate că inelul \mathbb{Z}_n este corp dacă și numai dacă n este număr prim.

9.2. Să se rezolve în corpul \mathbb{Z}_7 sistemul:
$$\begin{cases} x + y = \hat{0} \\ xy = \hat{5} \end{cases}.$$

9.3. Să se arate că orice inel integru finit este corp.

9.4. Să se demonstreze că într-un corp K există doar două ideale, idealul nul și K care sunt ideale bilaterale.

9.5. Fie K un inel nenul care are numai două ideale (0) și K . Să se arate că K este corp.

9.6. Pe intervalul real $K = (0, +\infty)$ se definesc operațiile algebrice:

$$x \oplus y = xy \text{ și } x \odot y = x^{\ln y}, \text{ oricare ar fi } x, y \in K.$$

Să se arate că:

(i) (K, \oplus, \odot) este corp comutativ;

(ii) Corpul (K, \oplus, \odot) este izomorf cu corpul $(\mathbb{R}, +, \cdot)$ al numerelor reale.

9.7. Fie \otimes o operație algebrică pe \mathbb{Q}^* astfel încât $(\mathbb{Q}, +, \otimes)$ este inel. Să se arate că $(\mathbb{Q}, +, \otimes)$ este corp și $(\mathbb{Q}^*, \cdot) \simeq (\mathbb{Q}^*, \otimes)$.

9.8. (i) Să se demonstreze că cel mai mic subcorp al lui \mathbb{R} ce conține pe $\sqrt{2}$ este format din numerele reale de forma $a+b\sqrt{2}$ cu $a, b \in \mathbb{Q}$;

(ii) Să se arate că mulțimea $F = \mathbb{Q}(\sqrt[3]{2}) = \{a+b\sqrt[3]{2} + c\sqrt[3]{4} \mid a, b, c \in \mathbb{Q}\}$ împreună cu adunarea și înmulțirea numerelor reale este cel mai mic subcorp (comutativ) al lui \mathbb{R} ce conține pe \mathbb{Q} și pe $\sqrt[3]{2}$.

9.9. Fie A un inel unitar inclus în corpul \mathbb{C} al numerelor complexe și care include intervalul $(0, 1)$, operațiile inelului A fiind cele induse de operațiile din \mathbb{C} . Să se demonstreze că $A = \mathbb{R}$ sau $A = \mathbb{C}$.

9.10. Fie d_1 și d_2 doi întregi liberi de pătrate, $d_1 \neq d_2$. Să se demonstreze egalitățile:

(i) $\mathbb{Q}(\sqrt{d_1}) \cap \mathbb{Q}(\sqrt{d_2}) = \mathbb{Q}$;

(ii) $\mathbb{Z}[\sqrt{d_1}] \cap \mathbb{Z}[\sqrt{d_2}] = \mathbb{Z}$.

9.11. Fie $K \subset \mathbb{C}$ un subcorp. Să se demonstreze că următoarele afirmații sunt echivalente:

(i) Ecuația $x^2 = a^2 + 1$ are soluții în K , pentru orice $a \in K$;

(ii) Ecuația $x^2 = a^2 + a + 1$ are soluții în K , pentru orice $a \in K$.

Dați exemplul de un corp K pentru care una din cele două afirmații de mai înainte este adevărată.

9.12. Caracterizați subinelele unitare ale lui $(\mathbb{Q}, +, \cdot)$.

9.13. Fie K un corp necomutativ. Dacă există $a, b \in K$ și $n \in \mathbb{Z}$ a.î.

$$a^n b^n - b^{n+1} a^{n+1} = 1 \text{ și } a^{2n+1} + b^{2n+1} = 0,$$

atunci $b^n a^n - a^{n+1} b^{n+1} = 1$.

9.14. Fie K un corp, E o extindere a lui K și $x \in E \setminus K$. Arătați că pentru orice $a, b \in K$ cu $a \neq 0$ avem $K(ax+b) = K(x)$.

9.15. (i) Fie A un inel cu n elemente, $n > 0$ și 1 elementul unitate al lui A . Dacă ordinul lui 1 în grupul $(A, +)$ este egal cu n , atunci $(A, +, \cdot) \simeq (\mathbb{Z}_n, +, \cdot)$;

(ii) Fie p un număr prim iar A un inel cu p elemente. Să se arate că A este corp comutativ izomorf cu corpul $(\mathbb{Z}_p, +, \cdot)$.

9.16. Fie A un inel cu opt elemente, de caracteristică 2.

Arătați că:

(i) Pentru orice $x \in A$, $x^7 + 1 = (x + 1)(x^3 + x^2 + 1)(x^3 + x + 1)$;

(ii) A este corp dacă și numai dacă există $a \in A$ a.î. $a^3 + a + 1 = 0$.

9.17. Fie A un inel finit cu $0 \neq 1$. Să se arate că următoarele afirmații sunt echivalente:

(i) A nu este corp;

(ii) Pentru orice $n \in \mathbb{N}^*$ ecuația $x^n + y^n = z^n$ are soluții în A^* .

9.18. Fie K un corp comutativ cu 8 elemente. Să se demonstreze că există $a \in K$ a.î. $a^3 = a + 1$.

9.19. Fie K un inel cu patru elemente. Următoarele afirmații sunt echivalente:

(i) K este corp;

(ii) Există $a \in K$ a.î. $a^2 = 1 + a$.

9.20. Fie $O, E, U \in M_3(\mathbb{Z}_2)$, $O = \begin{pmatrix} \hat{0} & \hat{0} & \hat{0} \\ \hat{0} & \hat{0} & \hat{0} \\ \hat{0} & \hat{0} & \hat{0} \end{pmatrix}$, $E = \begin{pmatrix} \hat{1} & \hat{0} & \hat{0} \\ \hat{0} & \hat{1} & \hat{0} \\ \hat{0} & \hat{0} & \hat{1} \end{pmatrix}$

$$U = \begin{pmatrix} \hat{0} & \hat{0} & \hat{1} \\ \hat{1} & \hat{0} & \hat{1} \\ \hat{0} & \hat{1} & \hat{0} \end{pmatrix}.$$

(i) Arătați că $M_3(\mathbb{Z}_2)$ este inel de caracteristică 2;

(ii) $F_8 = \{O, E, U, U^2, U^3, U^4, U^5, U^6\}$ este corp cu 8 elemente în raport cu adunarea și înmulțirea matricelor;

(iii) Orice corp K cu 8 elemente este izomorf cu F_8 .

9.21. Dacă A este un inel a.î. oricare ar fi $a \in A$, $a \neq 0$ există $b \in A$ cu $ba = 1$, atunci A este corp.

9.22. Fie K un corp comutativ cu proprietatea că pentru orice $x \in K$ avem $x^2 + 1 \neq 0$. Definim adunarea și înmulțirea pe $K \times K$ prin:

$$(x_1, y_1) + (x_2, y_2) = (x_1 + x_2, y_1 + y_2)$$

$$(x_1, y_1) \cdot (x_2, y_2) = (x_1 x_2 - y_1 y_2, x_1 y_2 + x_2 y_1),$$

pentru orice $(x_1, y_1), (x_2, y_2) \in K \times K$.

Să se arate că mulțimea $K \times K$ împreună cu aceste operații este corp comutativ, corpul K fiind izomorf cu un subcorp al acestuia. Mai mult, în acest corp ecuația $x^2+1 = 0$ are soluții.

Există corpuri K finite cu proprietatea că $x^2+1 \neq 0$, oricare ar fi $x \in K$?

9.23. Fie $H = \left\{ \begin{pmatrix} \alpha & \beta \\ -\bar{\beta} & \bar{\alpha} \end{pmatrix} \mid \alpha, \beta \text{ numere complexe} \right\}$.

Arătați că H este subcorp al lui $M_2(\mathbb{C})$.

Observație. Corpul H poartă numele de *corpul quaternionilor*.

9.24. (i) Să se arate că mulțimea matricelor de forma

$$\begin{pmatrix} a & b & c & d \\ -b & a & -d & c \\ -c & d & a & -b \\ -d & -c & b & a \end{pmatrix} \text{ cu } a, b, c, d \in \mathbb{R} \text{ formează un subcorp } K \text{ al lui } M_4(\mathbb{R})$$

izomorf cu corpul quaternionilor;

(ii) Determinați centrul lui H .

9.25. Fie K un corp (comutativ sau nu). Dacă K_1, K_2, K_3 sunt subcorpuri ale lui K a.î. $K_i \neq K$, oricare ar fi $i=1, 2, 3$, atunci $\bigcup_{i=1}^3 K_i \neq K$.

9.26. (Generalizarea problemei **9.25.**) Să se arate că un corp nu poate fi scris ca reuniune a unui număr finit de subcorpuri proprii ale sale.

9.27. Fie K un corp și E o matrice din $M_n(K)$. Să se arate că E este divizor al lui zero dacă și numai dacă E nu este inversabilă. Este necesar să presupunem K corp?

9.28. Să se arate că corpul numerelor reale nu este izomorf cu corpul numerelor complexe.

9.29. Fie K un corp. Demonstrați că orice morfism unitar de la K la un inel unitar A nenul este funcție injectivă.

9.30. Să se determine endomorfismele corpului \mathbb{Q} al numerelor raționale.

9.31. Fie f un endomorfism al corpului numerelor reale .

(i) Să se determine $f(0)$, $f(1)$ și $f(-1)$;

(ii) Să se arate că pentru orice număr rațional q avem $f(q) = q$;

(iii) Să se demonstreze că pentru orice $\alpha \in \mathbb{R}$, $\alpha > 0$, rezultă $f(\alpha) > 0$.

Să se deducă de aici că f este strict crescătoare.

(iv) Folosind rezultatele stabilite la punctele precedente, să se demonstreze că singurul endomorfism al corpului numerelor reale este aplicația identică.

9.32. Fie $(K, +, \cdot)$ un corp. Pentru fiecare $a \in K$ definim $\lambda_a: K \rightarrow K$ prin $\lambda_a(x) = ax - xa$. Să se arate că dacă există un endomorfism $f: K \rightarrow K$, $f \neq 1_K$ astfel încât $f \circ \lambda_a = \lambda_a \circ f$ pentru orice $a \in K$, atunci corpul K este comutativ.

9.33. Determinați automorfismele corpurilor $\mathbb{Q}(\sqrt{2})$ și $\mathbb{Q}(\sqrt[3]{2})$.

9.34. Să se determine automorfismele f ale corpului \mathbb{C} al numerelor complexe, cu proprietatea că $f(x) = x$, oricare ar fi $x \in \mathbb{R}$.

9.35. Fie K un inel unitar și comutativ cu proprietatea că orice morfism de la K la un inel nenul este injectiv. Atunci K este corp.

9.36. Fie K și L două corpuri necomutative și $f: K \rightarrow L$ o funcție neconstantă. Să se demonstreze că funcția f este morfism sau antimorfism de corpuri (vezi problema 7.24.) dacă și numai dacă verifică condițiile următoare:

1) $f(x+y) = f(x) + f(y)$, oricare ar fi $x, y \in K$

2) $f(x^{-1}) = f(x)^{-1}$, oricare ar fi $x \in K$, $x \neq 0$

3) $f(1) = 1$.

9.37. Fie K și L două corpuri comutative de caracteristică zero și $f: K \rightarrow L$ o funcție. Să se arate că f este morfism de corpuri dacă și numai dacă are următoarele proprietăți:

1) $f(x+y) = f(x) + f(y)$, oricare ar fi $x, y \in K$;

2) $f(x^3) = [f(x)]^3$, oricare ar fi $x \in K$;

3) $f(1) = 1$.

9.38. (i) Fie K și L două corpuri necomutative și $n \geq 2$ un număr natural. Fie $f: K \rightarrow L$ o funcție cu proprietățile:

1) $f(x+y) = f(x) + f(y)$, oricare ar fi $x, y \in K$;

2) $f(x^n) = f(x)^n$, oricare ar fi $x \in K$;

3) $f(1) = 1$.

În aceste condiții, dacă L și K sunt corpuri de caracteristică zero sau de caracteristică $p > n$, să se demonstreze că: $f(x^2) = f(x)^2$, oricare ar fi $x \in K$;

(ii) În condițiile de la (i), dacă L și K sunt corpuri comutative, să se demonstreze că f este morfism de corpuri.

9.39. Fie d_1 și d_2 doi întregi liberi de pătrate și $f: \mathbb{Q}(\sqrt{d_1}) \rightarrow \mathbb{Q}(\sqrt{d_2})$ un izomorfism de corpuri.

(i) Să se demonstreze că $d_1 = d_2$;

(ii) Să se determine automorfismele corpului $\mathbb{Q}(\sqrt{d})$, unde d este un întreg liber de pătrate.

9.40. Fie \mathbb{Z}_p corpul claselor de resturi modulo p ($p > 1$, număr prim), $(\mathbb{Z}_p, +)$ grupul aditiv al corpului, iar (\mathbb{Z}_p^*, \cdot) grupul multiplicativ al elementelor sale nenule.

Să se determine morfismele de grupuri de la $(\mathbb{Z}_p, +)$ la (\mathbb{Z}_p^*, \cdot) .

9.41. Fie \mathbb{Q} corpul numerelor raționale. Să se determine toate morfismele de grupuri de la grupul $(\mathbb{Q}, +)$ la grupul (\mathbb{Q}^*, \cdot) .

9.42. Fie K un corp comutativ cu proprietatea că există $n > 0$, număr natural a.î. $n \cdot 1_K = 0_K$. Să se arate că:

(i) Dacă p este cel mai mic număr natural pozitiv a.î. $p \cdot 1_K = 0_K$, atunci p este număr prim (p se numește *caracteristica* corpului K);

(ii) Oricare ar fi $x, y \in K$, atunci $(x \pm y)^p = x^p \pm y^p$;

(iii) Există un singur morfism de grupuri de la grupul aditiv $(K, +)$ la grupul multiplicativ (K^*, \cdot) .

9.43. Definem pe $\mathbb{Z}_3 \times \mathbb{Z}_3$ următoarele operații:

$$(a, b) + (c, d) = (a+c, b+d) \text{ și } (a, b) \cdot (c, d) = (ac-bd, ad+bc).$$

Verificați că $(\mathbb{Z}_3 \times \mathbb{Z}_3, +, \cdot)$ este corp și calculați-i caracteristica.

9.44. Fie $p \geq 2$ un număr prim și K un corp cu următoarele proprietăți:

1) $px = 0$, pentru orice $x \in K$;

2) Pentru orice $x \in K$ există un întreg $n = n(x) \geq 0$ (ce depinde de x) a.î.
 $x^{p^n} \in Z(K)$.
 Atunci K este comutativ.

9.45. Fie $(K, +, \cdot)$ un corp finit. Să se determine toate morfismele de grupuri de la $(K, +)$ la (K^*, \cdot) și de la (K^*, \cdot) la $(K, +)$.

9.46. Fie K un corp cu $\text{car}(K) \neq 2$ și $a \in K$ a.î. $a^{2n+1} = 1$, pentru $n \in \mathbb{N}^*$.

Găsiți $f: K \rightarrow K$ a.î. $f(x) + f(ax) = 2x$, oricare ar fi $x \in K$.

9.47. Fie K mulțimea matricelor pătratice de ordin doi cu elemente reale formată din matricele de tipul $M(a, b) = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$.

(i) Să se arate că față de operațiile uzuale, K are structură de corp izomorf cu corpul complex \mathbb{C} ;

(ii) Folosind rezultatul precedent, să se rezolve în K sistemul de ecuații:
$$\begin{cases} X + Y = M(3,3) \\ X^3 + Y^3 = M(-9,9) \end{cases}$$

9.48. Fie $d \in \mathbb{Z}$ un număr liber de pătrate. Să se arate că:

(i) Mulțimea $\mathbb{Q}(\sqrt{d}) = \{a + b\sqrt{d} \mid a, b \in \mathbb{Q}\}$ împreună cu adunarea și înmulțirea numerelor complexe este corp comutativ;

(ii) Mulțimea $K = \left\{ \begin{pmatrix} a & b \\ db & a \end{pmatrix} \mid a, b \in \mathbb{Q} \right\}$ împreună cu adunarea și înmulțirea matricelor este corp comutativ;

(iii) Cele două corpuri de la punctele precedente sunt izomorfe.

9.49. Un corp $K \subseteq \mathbb{C}$ în care operațiile sunt cele obișnuite cu numere complexe satisface ipotezele:

i) Corpul K are exact două endomorfisme f și g ;

ii) $f(x) = g(x) \Rightarrow x \in \mathbb{Q}$.

Să se demonstreze că există un întreg liber de pătrate $d \neq 1$ a. î. $K = \mathbb{Q}(\sqrt{d})$.

9.50. Fie $q \in \mathbb{Q}$ și $A_q = \left\{ \begin{pmatrix} a & b \\ qb & a \end{pmatrix} \mid a, b \in \mathbb{Q} \right\}$. Demonstrați că A_q este un

subinel al lui $M_2(\mathbb{Q})$ și este corp (comutativ) dacă q nu este pătratul unui număr rațional.

9.51. Se consideră K mulțimea matricelor de forma $M(a, b) = \begin{pmatrix} a+b & b \\ b & a-b \end{pmatrix}$, cu $a, b \in \mathbb{Q}$. Arătați că K împreună cu adunarea și înmulțirea matricelor formează un corp izomorf cu corpul $\mathbb{Q}(\sqrt{2})$.

9.52. Arătați că $K = \left\{ \begin{pmatrix} x+2y & 3y \\ 2y & x-2y \end{pmatrix} \mid x, y \text{ numere rationale} \right\} \subseteq M_2(\mathbb{Q})$

este corp comutativ izomorf cu corpul $\mathbb{Q}(\sqrt{10})$.

9.53. Fie $p > 0$ un număr prim și $K = \left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \mid a, b \in \mathbb{Z}_p \right\}$. Să se

demonstreze că mulțimea K înzestrată cu operațiile de adunare și înmulțire a matricelor este corp dacă și numai dacă $p \equiv 3 \pmod{4}$.

9.54. Considerăm mulțimea $K \subset M_2(\mathbb{R})$ formată din toate matricele de forma $\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix}$, cu $a \in \mathbb{R}$.

(i) Să se arate că față de adunarea și înmulțirea matricelor K este corp comutativ izomorf cu corpul \mathbb{R} ;

(ii) Demonstrați că deși matricele nenule din K sunt elemente inversabile în K , ele sunt matrice singulare în $M_2(\mathbb{R})$. Explicați rezultatul.

9.55. Fie $(A, +, \cdot)$ un inel unitar cu $0 \neq 1$. Să se demonstreze că dacă orice funcție $f: A \rightarrow A$ este polinomială, atunci $(A, +, \cdot)$ este corp.

9.56. Fie $M_2(\mathbb{Q})$ și pentru d întreg liber de pătrate considerăm submulțimea K_d a lui $M_2(\mathbb{Q})$ formată din matricele de forma $\begin{pmatrix} a & bd \\ b & a \end{pmatrix}$ cu $a, b \in \mathbb{Q}$.

(i) Să se arate că mulțimea K_d este corp față de adunarea și înmulțirea matricelor și aplicația $f: \mathbb{Q}(\sqrt{d}) \rightarrow K_d$, $f(a+b\sqrt{d}) = \begin{pmatrix} a & bd \\ b & a \end{pmatrix}$ este un izomorfism de corpuri;

(ii) Considerăm grupurile multiplicative $(\mathbb{Q}(\sqrt{d})^*, \cdot)$, (K_d^*, \cdot) , (\mathbb{Q}^*, \cdot) și aplicațiile $f: \mathbb{Q}(\sqrt{d})^* \rightarrow K_d^*$, definită ca la (i), $\Delta: K_d^* \rightarrow \mathbb{Q}^*$ definită prin $\Delta(A) = \det(A)$, $N: \mathbb{Q}(\sqrt{d})^* \rightarrow \mathbb{Q}^*$ definită prin $N(a+b\sqrt{d}) = a^2 - db^2$.

Să se demonstreze că f , Δ , N sunt morfisme de grupuri și avem egalitatea $\Delta \circ f = N$.

9.57. Dacă K_1 și K_2 sunt două corpuri, să se arate că inelul produs $K_1 \times K_2$ nu este corp.

9.58. Fie K_1, K_2, K_3, K_4, K_5 corpuri nu neapărat comutative și nu neapărat distincte. Să se arate că inelele produs $K_1 \times K_2 \times K_3$ și $K_4 \times K_5$ nu sunt izomorfe.

§10. Inele de polinoame

10.1. Fie A un inel comutativ și unitar, I o mulțime nevidă și $A[X;I]$ inelul polinoamelor cu coeficienți în A în nedeterminatele $\{X_i\}_{i \in I}$. Să se arate că:

(i) Dacă I și A sunt finite atunci $A[X;I]$ este o mulțime numărabilă;

(ii) Dacă I este finită iar A este infinită atunci $A[X;I]$ are cardinalul lui

A ;

(iii) Dacă A este finită (chiar numărabilă) și I este infinită, atunci $A[X;I]$ are cardinalul lui I .

10.2. Se poate defini pe orice mulțime nevidă o structură de inel unitar?

10.3. Fie A un domeniu de integritate și $U(A)$ grupul elementelor inversabile ale lui A . Să se arate că orice subgrup finit al lui $U(A)$ este ciclic.

10.4. (i) Să se arate că produsul elementelor nenule ale unui corp finit este egal cu -1 ;

(ii) Să se deducă de aici că pentru orice număr prim p , $p|(p-1)!+1$ (vezi problema 3.17.).

10.5. Fie A un inel (comutativ), iar $f = a_0 + a_1X + \dots + a_nX^n$ un polinom din $A[X]$ de grad $n \geq 0$. Arătați că:

- (i) f este inversabil în $A[X]$ dacă și numai dacă a_0 este inversabil în A și a_1, \dots, a_n sunt nilpotente în A ;
(ii) f este nilpotent în $A[X]$ dacă și numai dacă toți coeficienții a_0, a_1, \dots, a_n sunt nilpotenți în A ;
(iii) f este divizor al lui zero în $A[X]$ dacă și numai dacă există $a \in A^*$ a.î. $a \cdot f = 0$.

10.6. Fie p un număr prim, $p \geq 3$. Să se afle numărul soluțiilor ecuației

$$x^{p-1/2} + y^{p-1/2} = \hat{0},$$

considerată în corpul \mathbb{Z}_p , al claselor de resturi modulo p .

10.7. Fie $(A_k)_{k \in \mathbb{N}^*}$ și $(B_k)_{k \in \mathbb{N}^*}$ două șiruri de matrice pătratică de ordinul n cu elemente din \mathbb{R} . Dacă pentru orice $k \in \mathbb{N}^*$, B_k este inversabilă, să se arate că există o infinitate de numere reale α a.î. $A_k + \alpha B_k$ este inversabilă, oricare ar fi $k \in \mathbb{N}^*$.

10.8. Fie A un inel unitar comutativ cu cel puțin două elemente. Să se arate că următoarele afirmații sunt echivalente:

- (i) A este corp finit;
(ii) Orice polinom $P \in A[X]$ de grad $n \geq 1$ are cel mult n rădăcini (distincte) în A și orice funcție $f: A \rightarrow A$ este funcție polinomială (adică există $Q \in A[X]$ a.î. $f = \tilde{Q}$).

10.9. Fie polinomul $f = \hat{a} + \hat{b}X \in \mathbb{Z}_n[X]$, unde $n = p^r$, cu p prim și $r \in \mathbb{N}^*$.

- (i) Să se arate că $f \in U(\mathbb{Z}_n[X])$ dacă și numai dacă $p \nmid a$ și $p \mid b$;
(ii) Câte polinoame de grad cel mult 1 din $\mathbb{Z}_n[X]$ sunt inversabile?

10.10. Fie A un inel comutativ cu $0 \neq 1$, fără divizori ai lui zero, iar $A[X]$ inelul de polinoame asociat. Pentru fiecare număr întreg $n \geq 2$ definim aplicația $\varphi_n: A[X] \rightarrow A[X]$, $\varphi_n(f) = f^n$ și presupunem că mulțimea $M = \{n \mid n \in \mathbb{Z}, n \geq 2, \varphi_n \text{ este endomorfism al inelului } A[X]\}$ este nevidă. Să se demonstreze că există și este unic un număr prim $p > 0$ a.î. $M = \{p, p^2, p^3, \dots, p^k, \dots\}$.

10.11. Să se arate că nu există inele unitare și comutative A a.î. $A[X] \simeq (\mathbb{Z}, +, \cdot)$.

10.12. Fie A un inel unitar. Să se demonstreze că inelele $A[X]$ și $\mathbb{Z}[X]$ sunt izomorfe dacă și numai dacă inelele A și \mathbb{Z} sunt izomorfe.

10.13. Fie K un corp comutativ și A un inel unitar. Să se demonstreze că inelele $K[X]$ și $A[X]$ sunt izomorfe dacă și numai dacă inelele K și A sunt izomorfe.

10.14. Fie k și K două corpuri a.î. grupurile multiplicative (k^*, \cdot) și (K^*, \cdot) nu sunt izomorfe. Să se arate că inelele $k[X]$ și $K[X]$ nu sunt izomorfe.

Folosind acest rezultat, să se demonstreze că inelele $\mathbb{Q}[X]$ și $\mathbb{R}[X]$ nu sunt izomorfe și de asemenea inelele $\mathbb{R}[X]$ și $\mathbb{C}[X]$ nu sunt izomorfe.

10.15. Arătați că inelele \mathbb{R} și $\mathbb{R}[X]$ nu sunt izomorfe, dar grupurile lor aditive $(\mathbb{R}, +)$ și $(\mathbb{R}[X], +)$ sunt izomorfe.

10.16. Fie A un inel comutativ integru și fie $A[X]$ inelul polinoamelor în X cu coeficienți din A . Determinați automorfismele inelului $A[X]$.

10.17. Fie A un domeniu de integritate. Să se arate că o funcție $\varphi: A[X] \rightarrow A[X]$ este un automorfism al lui $A[X]$ care invariază elementele lui A dacă și numai dacă există $a, b \in A$, a inversabil, a.î. $\varphi(f(X)) = f(aX + b)$, oricare ar fi $f \in A[X]$.

10.18. (i) Fie polinomul $P = X^5 \in \mathbb{R}[X]$. Arătați că pentru orice $\alpha \in \mathbb{R}^*$, polinomul $P(X+\alpha) - P(X)$ nu are rădăcini reale;

(ii) Fie $P \in \mathbb{R}[X]$ un polinom de gradul $n \geq 2$ cu rădăcini reale și distincte. Arătați că există $\alpha \in \mathbb{Q}^*$ a.î. polinomul $P(X+\alpha) - P(X)$ să aibă toate rădăcinile reale.

10.19. Să se găsească polinoamele $f \in \mathbb{R}[X]$ a.î. $f(a + b) = f(a) + f(b)$, oricare ar fi $a, b \in \mathbb{R}$.

10.20. Fie $f = a_0 + a_1X + \dots + a_nX^n \in \mathbb{Z}[X]$. Să se arate că:

(i) Dacă $a \in \mathbb{Z}$, atunci $f(a)$ divide numărul $f(a+f(a))$;

(ii) Există $a \in \mathbb{Z}$ a.î. $f(a)$ să nu fie număr prim ;

(iii) Nu există $f \in \mathbb{Z}[X]$ neconstant a.î. $f(a)$ să fie număr prim, pentru orice $a \in \mathbb{Z}$.

10.21. Să se determine polinoamele $P \in \mathbb{R}[X]$ a.î. $XP(X) = (X-3)P(X+1)$.

10.22. (i) Pentru ce valori ale lui m polinomul $(X-1)^m - X^m + 1$ este divizibil cu $X^2 - X + 1$?

(ii) Pentru ce valori ale lui m polinomul $(X-1)^m + X^m + 1$ este divizibil cu $X^2 - X + 1$?

10.23. Să se arate că restul împărțirii polinomului f din $\mathbb{R}[X]$ prin $(X-a)(X-b)$, unde $b \neq a$, este

$$r = \frac{f(b) - f(a)}{b - a} X + \frac{bf(a) - af(b)}{b - a}.$$

10.24. Fie f un polinom de gradul doi din $\mathbb{Q}[X]$. Atunci $f(n) \in \mathbb{Z}$ pentru orice $n \in \mathbb{Z}$ dacă și numai dacă f este de forma $f = \frac{1}{2}[cX^2 + (2b - c)X + 2a]$ cu $a, b, c \in \mathbb{Z}$.

10.25. Să se determine cel mai mare divizor comun al polinoamelor $X^n - 1$ și $X^m - 1$ ($m, n \in \mathbb{N}^*$).

10.26. Să se afle cel mai mare divizor comun al polinoamelor $X^n + a^n$ și $X^m + a^m$ din $\mathbb{R}[X]$ ($m, n \in \mathbb{N}^*$, $a \in \mathbb{R}$).

10.27. Să se arate că rădăcinile polinomului $f = 1 + \frac{X}{1!} + \frac{X^2}{2!} + \dots + \frac{X^n}{n!}$ sunt simple.

10.28. Fie $f \in \mathbb{R}[X]$ cu proprietatea că $\tilde{f}(\alpha) \geq 0$, pentru orice $\alpha \in \mathbb{R}$. Atunci există două polinoame $f_1, f_2 \in \mathbb{R}[X]$ a.î. $f = f_1^2 + f_2^2$.

10.29. Fie $\mathbb{Z}[X]$ mulțimea polinoamelor cu coeficienți întregi, p un număr prim și $f, g \in \mathbb{Z}[X]$. Dacă $p|fg$, atunci $p|f$ sau $p|g$.

10.30. Fie $f \in \mathbb{Z}[X]$. Notăm cu $c(f)$ = cel mai mare divizor comun al coeficienților lui f . Dacă $f, g \in \mathbb{Z}[X]$ să se arate că $c(fg) = c(f) \cdot c(g)$.

10.31. Determinați $m \in \mathbb{N}$ a.î. $X^m - 1$ este divizibil cu $X^{2n} + X^n + 1, (n \in \mathbb{N}^*)$.

10.32. Să se arate că dacă m este un număr întreg nedivizibil cu 5, atunci polinomul $P = X^5 - X + m$ este ireductibil în $\mathbb{Z}[X]$.

10.33. Studiați reductibilitatea polinoamelor $X^2 + 1$ și $X^3 + X + 2$ în $\mathbb{Z}_3[X]$, respectiv $\mathbb{Z}_5[X]$.

10.34. Există $a \in \mathbb{Z}_5$ a.î. $X^4 + aX + 1$ să fie ireductibil în $\mathbb{Z}_5[X]$?

10.35. Verificați că polinoamele $f = X^5 + X^3 + X$ și $g = X^5 + 2X \in \mathbb{Z}_3[X]$ au aceeași funcție polinomială, deși ca polinoame sunt diferite.

10.36. Fie p un număr prim, $p > 3$.

(i) Să se determine restul împărțirii numărului $\prod_{k=1}^p (k^2 + k + 1)$ la p ;

(ii) Să se arate că polinomul $X^2 + X + 1 \in \mathbb{Z}_p[X]$ este ireductibil în $\mathbb{Z}_p[X]$ dacă și numai dacă $p \equiv 2 \pmod{3}$.

10.37. Fie K un corp comutativ de caracteristică $p \neq 0$. Să se arate că polinomul $X^{p^n} - x \in K[X]$ (x fiind arbitrar în K) are cel mult o rădăcină.

10.38. Fie K un corp finit. Să se determine mulțimea numerelor naturale $n \geq 2$ care au proprietatea că orice polinom de grad n din $K[X]$ care nu are rădăcini în K este ireductibil în $K[X]$.

10.39. (i) Să se rezolve ecuația $3x^2 - 4x + 1 = 0$ în $\mathbb{Z}_5, \mathbb{Z}_7, \mathbb{Z}_{11}, \mathbb{Z}_{13}, \mathbb{Z}_{17}, \mathbb{Z}_{19}$;

(ii) Să se rezolve ecuația $x^2 - x + 5 = 0$ în $\mathbb{Z}_7, \mathbb{Z}_{11}, \mathbb{Z}_{17}, \mathbb{Z}_{19}$.

10.40. Să se demonstreze că dacă $P \in \mathbb{R}[X]$ de grad n , are n rădăcini reale, atunci oricare ar fi $a \in \mathbb{R}$ polinomul $Q = P(X+ia) + P(X-ia)$ are, de asemenea, n rădăcini reale.

10.41. Fie $K = \{k_1, k_2, \dots, k_n\}$ un corp finit cu n elemente, iar $K[X]$ inelul polinoamelor de o nedeterminată peste corpul K . Să se arate că în inelul $K[X]$ are loc identitatea: $X^n - X = \prod_{i=1}^n (X - k_i)$.

10.42. Să se găsească $a, b \in \mathbb{Z}$ știind că ecuațiile $x^3+2x^2+ax+b = 0$ și $x^3-x^2+bx+a = 0$ admit o rădăcină întregă comună.

10.43. Fie $P = a_0X^n + a_1X^{n-1} + \dots + a_n \in \mathbb{Z}[X]$ cu a_0, a_n impare. Dacă $P(1)$ este impar să se arate că P nu are rădăcini raționale.

10.44. Dacă un polinom din $\mathbb{Q}[X]$ admite rădăcina $\sqrt[3]{2}$ să se arate că polinomul este divizibil cu X^3-2 .

10.45. Să se arate că polinomul $P = (1+X+\dots+X^n)^2-X^n$ este reductibil în $\mathbb{Z}[X]$.

10.46. Să se arate că polinomul $P = (X^n-2)^n-X-2$ este reductibil în $\mathbb{Z}[X]$.

10.47. Fie p un număr prim, iar k un număr natural ≥ 1 .
Stabiliți numărul polinoamelor inversabile, de grad mai mic sau egal cu n , din inelul $\mathbb{Z}_{p^k}[X]$.

10.48. Arătați că în inelul $\mathbb{Z}_4[X]$ există polinoame inversabile ce au gradul diferit de zero.

10.49. Să se determine $a \in \mathbb{Z}_3$ a.î. polinomul
 $P = \hat{2}X^3 + (a + \hat{2})X + \hat{1} \in \mathbb{Z}_3[X]$ să fie ireductibil.

10.50. Să se arate că polinomul $X^6+aX+\hat{5} \in \mathbb{Z}_7[X]$ este reductibil, pentru orice $a \in \mathbb{Z}_7$.

10.51. Fie polinoamele:

1) $P_1 = X^3+X+\hat{1} \in \mathbb{Z}_2[X]$

2) $P_2 = X^4+X^3+\hat{1} \in \mathbb{Z}_2[X]$

3) $P_3 = X^5+\hat{1} \in \mathbb{Z}_3[X]$

4) $P_4 = X^4-\hat{1} \in \mathbb{Z}_7[X]$.

Să se decidă dacă polinoamele date sunt sau nu reductibile, iar în caz afirmativ să se descompună în factori primi.

10.52. Fie $f = a_0 + a_1X + \dots + a_nX^n \in \mathbb{Z}[X]$ un polinom de grad ≥ 1 și să presupunem că există p număr prim, $p \geq 2$, a.f. $p | a_0, a_1, \dots, a_{n-1}$, $p \nmid a_n$ și $p^2 \nmid a_0$. Atunci f este ireductibil în $\mathbb{Z}[X]$.

Observație. Criteriul de ireductibilitate de mai sus este datorat lui *Eisenstein*.

10.53. Să se arate că dacă p este un număr prim, atunci polinomul $f = X^{p-1} + X^{p-2} + \dots + X + 1$ este ireductibil în $\mathbb{Z}[X]$.

10.54. Să se arate că polinomul $X^{52} + X^{51} + X^{50} + \dots + X^2 + X + 1$ este ireductibil în $\mathbb{Z}[X]$.

10.55. Să se arate că polinomul $X^n - 120$ ($n \geq 1$) este ireductibil în $\mathbb{Z}[X]$.

10.56. Fie $p \geq 2$ un număr prim. Să se arate că polinomul $f = X^3 + pX^2 + pX + p$ este ireductibil în $\mathbb{Z}[X]$.

10.57. Să se arate că polinomul $f = X^{2^n} + 1$, ($n \in \mathbb{N}$) este ireductibil în $\mathbb{Z}[X]$.

10.58. Fie $p \geq 2$ un număr prim și $n \in \mathbb{N}$. Să se arate că polinomul $f = X^{p^n} + p - 1$ este ireductibil în $\mathbb{Z}[X]$.

10.59. Fie polinoamele $P = 1 + X + X^2 + \dots + X^{m-1}$ și $Q = X^{u_1} + X^{u_2} + \dots + X^{u_n}$, unde $0 < u_1 < u_2 < \dots < u_n$ sunt numere întregi. Pentru $k \in \{0, 1, \dots, m-1\}$ fie n_k numărul acelor i ($1 \leq i \leq n$) pentru care restul împărțirii lui u_i la m este k .

Să se demonstreze că P divide Q dacă și numai dacă $n_0 = n_1 = \dots = n_{m-1}$.

10.60. Fie $P = X^n - a_1X^{n-1} + a_2X^{n-2} - \dots + (-1)^n a_n$ un polinom cu coeficienți reali și care are toate rădăcinile reale și conținute în intervalul $[0, 1]$. Să se demonstreze inegalitatea:

$$a_k - a_{k+1} + a_{k+2} - \dots + (-1)^{n-k} a_n \geq 0, \text{ pentru orice } k, 1 \leq k \leq n.$$

10.61. Fie a_1, a_2, \dots, a_n numere complexe ($n \geq 2$). Să se arate că ecuațiile $x^n - 1 = 0$ și $a_1 + a_2x + a_3x^2 + \dots + a_nx^{n-1} = 0$ au cel puțin o rădăcină comună dacă și numai dacă

$$\begin{vmatrix} a_1 & a_2 & \dots & a_{n-1} & a_n \\ a_2 & a_3 & \dots & a_n & a_1 \\ \dots & \dots & \dots & \dots & \dots \\ a_{n-1} & a_n & \dots & a_{n-3} & a_{n-2} \\ a_n & a_1 & \dots & a_{n-2} & a_{n-1} \end{vmatrix} = 0.$$

10.62. Fie $x_1, x_2, \dots, x_n \in \mathbb{R}$. Să se demonstreze că numerele x_1, x_2, \dots, x_n sunt pozitive dacă și numai dacă numerele $\sum x_1, \sum x_1 x_2, \dots, x_1 x_2 \dots x_n$ sunt pozitive.

10.63. Fie $P \in \mathbb{R}[X]$ de grad cel mult n cu coeficientul dominant a_0 , iar x_1, x_2, \dots, x_{n+1} numere reale distincte două câte două. Să se demonstreze că:

$$\sum_{i=1}^{n+1} \frac{P(x_i)}{(x_i - x_1) \dots (x_i - x_{i-1})(x_i - x_{i+1}) \dots (x_i - x_{n+1})} = \begin{cases} 0, & \text{daca } \text{grad}(P) \leq n-1 \\ a_0, & \text{daca } \text{grad}(P) = n \end{cases}.$$

10.64. Fie p un număr prim, $P = a_0 X^n + a_1 X^{n-1} + \dots + a_n \in \mathbb{Z}[X]$ cu $1 \leq n < p$, iar a_0 nu se divide la p . Să se demonstreze că printre numerele $0, 1, 2, \dots, p-1$ există cel mult n numere y pentru care p divide pe $P(y)$.

Observație. Acest rezultat este datorat lui *Lagrange*.

10.65. Fie $P \in \mathbb{R}[X]$ un polinom de grad $n \geq 2$ care are rădăcinile reale simple x_1, \dots, x_n . Să se demonstreze că $\sum_{k=1}^n \frac{P^{(r)}(x_k)}{P'(x_k)} = 0$, pentru orice r natural, $r \geq 2$.

10.66. Dacă x_1, \dots, x_7 sunt rădăcinile ecuației $x^7 - 1 = 0$ să se calculeze suma $\sum (x_1 + x_2)^{20}$.

10.67. Fie un polinom de grad n și x_1, \dots, x_n rădăcinile sale.

Notăm cu $S_k = x_1^k + \dots + x_n^k$, $k \in \mathbb{N}$. Să se arate că:

$$(i) \sum_{i \neq j} x_i^p x_j^q = S_p \cdot S_q - S_{p+q}, \quad i, j \in \{1, \dots, n\};$$

$$(ii) \sum_{i \neq j} x_i^p x_j^p = \frac{1}{2} \cdot [(S_p)^2 - S_{2p}], \quad i, j \in \{1, \dots, n\};$$

$$(iii) \sum_{i \neq j \neq k} x_i^p x_j^q x_k^r = S_p \cdot S_q \cdot S_r - S_{p+q} \cdot S_r - S_{p+r} \cdot S_q - S_{r+q} \cdot S_p + 2S_{p+q+r},$$

$i, j, k \in \{1, \dots, n\}$.

10.68. Să se calculeze suma $\sum_{i \neq j} x_i^3 x_j^2$, unde x_i, x_j sunt rădăcinile ecuației $x^3 + 3x - 5 = 0$.

10.69. Să se rezolve în \mathbb{C} sistemul:
$$\begin{cases} x_1 + x_2 + x_3 = 2 \\ x_1^4 + x_2^4 + x_3^4 = 8 \\ x_1^5 + x_2^5 + x_3^5 = 32 \end{cases}$$

10.70. Fie $a_1, \dots, a_n \in \mathbb{Z}$ ($n \geq 1$) distincte două câte două iar $P = (X - a_1)^2 (X - a_2)^2 \dots (X - a_n)^2 + 1$ și $Q = (X - a_1)(X - a_2) \dots (X - a_n) - 1$. Să se arate că P și Q sunt ireductibile în $\mathbb{Z}[X]$.

10.71. Să se descrie idealele inelului $K[[X]]$ al seriilor formale peste corpul comutativ K .

10.72. Să se exprime ca polinom de polinoame simetrice fundamentale, polinomul simetric $f = (X_1 - X_2)^2 (X_1 - X_3)^2 (X_2 - X_3)^2$ cu coeficienți reali.

10.73. Să se exprime ca polinom de polinoame simetrice fundamentale polinomul simetric

$$f = (-X_1 + X_2 + \dots + X_n)(X_1 - X_2 + \dots + X_n) \dots (X_1 + X_2 + \dots - X_n) \in \mathbb{R}[X_1, X_2, \dots, X_n].$$

10.74. Să se arate că inelul $K[Y, Z] / (Z^2)$ este izomorf cu un subinel al inelului $K[X, Y, Z] / (X^2, XY - Z)$, K fiind corp comutativ.

10.75. Fie K un corp. Arătați că (X) este ideal maximal în $K[X]$.

10.76. Fie a_1, \dots, a_n elemente oarecare dintr-un inel A și $A[X_1, \dots, X_n]$ inelul polinoamelor în nedeterminatele X_1, \dots, X_n cu coeficienți în A . Să se arate că inelul $A[X_1, \dots, X_n] / (X_1 - a_1, \dots, X_n - a_n)$ este izomorf cu A .

10.77. Să se arate că $\mathbb{Z}[\sqrt{d}] \simeq \mathbb{Z}[X] / (X^2 - d)$ (ca inele), cu d număr întreg nenul, liber de pătrate.

10.78. Să se determine un element idempotent diferit de 0 și 1 în inelul $\mathbb{Z}_8[X] / (X^2 + X + \hat{2})$.

10.79. Fie $f:A \rightarrow A'$ un morfism surjectiv de inele unitare și comutative cu $\text{Ker}(f) \subseteq r(A)$.

Stabiliți dacă au loc afirmațiile:

- (i) Pentru $x \in A$, $f(x)$ este inversabil în $A' \Leftrightarrow x$ este inversabil în A ;
- (ii) Pentru $x \in A$, $f(x)$ este divizor al lui zero în $A' \Leftrightarrow x$ este divizor al lui zero în A ;
- (iii) Pentru $x \in A$, $f(x)$ este idempotent în $A' \Leftrightarrow x$ este idempotent în A .

Partea 2: Soluțiile problemelor

§1. Operații algebrice. Semigrupuri. Monoizi. Morfisme de monoizi

1.1. (i). O operație algebrică pe M fiind de fapt o funcție definită pe $M \times M$ cu valori în M , numărul acestora va fi egal cu n^{n^2} deoarece $|M| = n$, iar $|M \times M| = n^2$ (am folosit faptul că numărul funcțiilor definite pe o mulțime M cu m elemente, cu valori într-o mulțime N cu n elemente, este egal cu n^m).

(ii). Pe diagonala principală a tablei de compunere sunt n poziții iar deasupra ei sunt C_n^2 . Dacă operația algebrică de pe M este comutativă, atunci $n + C_n^2 = \frac{n(n+1)}{2}$ poziții se completează arbitrar iar apoi sub diagonala principală se vor pune elementele de deasupra diagonalei principale așezate însă simetric față de aceasta.

Raționând la fel ca la (i) deducem că pe M se pot defini $n^{(n(n+1))/2}$ operații algebrice comutative.

(iii). Tabela unei operații algebrice de pe M ce admite element neutru are ocupate elementele de pe prima linie și prima coloană cu elementele lui M . Restul de $(n-1)^2$ poziții putând fi ocupate arbitrar cu elementele lui M , deducem că pe M se pot defini $n \cdot n^{(n-1)^2} = n^{(n-1)^2+1}$ operații algebrice ce admit element neutru (am înmulțit pe n cu $n^{(n-1)^2}$ deoarece rolul elementului neutru poate fi jucat de oricare din cele n elemente ale lui M)

(iv). Ținând cont de (ii) și (iii) deducem că numărul căutat este egal cu $n^{(n(n-1))/2}$ (care reprezintă numărul de operații algebrice de pe M ce admit drept element neutru un element fixat al lui M) luat de n ori, adică $n \cdot n^{(n(n-1))/2} = n^{(n^2-n+2)/2}$.

1.2. (i). Operația algebrică " \circ " este asociativă $\Leftrightarrow (\forall)x, y, z \in \mathbb{R}$ avem :

$$\begin{aligned}x \circ (y \circ z) &= (x \circ y) \circ z \Leftrightarrow x(y \circ z) + ax + b(y \circ z) + c = (x \circ y)z + a(x \circ y) + bz + c \\ \Leftrightarrow x(yz + ay + bz + c) + ax + b(yz + ay + bz + c) &= (xy + ax + by + c)z + a(xy + ax + by + c) + bz \\ \Leftrightarrow (b-a)xz + (a+c-a^2)x + (b^2-b-c)z + c(b-a) &= 0.\end{aligned}$$

Cum x, y, z sunt elemente oarecare din \mathbb{R} făcând pe rând $(x = z = 0)$, $(x = 0, z = 1)$, $(x = 1, z = 0)$, $(x = z = 1)$ obținem succesiv condițiile: $c(a-b) = 0$, $a+c-a^2 = 0$ și $b-a = 0$.

Obținem astfel condițiile necesare $a = b = \lambda$ și $c = \lambda^2 - \lambda$ cu $\lambda \in \mathbb{R}$.

Suficiența acestor condiții se verifică imediat prin calcul.

(ii). " \Rightarrow ". Dacă operația algebrică " \circ " este asociativă, atunci conform cu (i) există $\lambda \in \mathbb{R}$ a.î. $a = b = \lambda$ și $c = \lambda^2 - \lambda$.

$$\text{Dacă } x \in \mathbb{R}, \text{ atunci } x \circ (1-\lambda) = (1-\lambda) \circ x = x(1-\lambda) + \lambda x + \lambda(1-\lambda) + \lambda^2 - \lambda =$$

$= x - x\lambda + \lambda x + \lambda - \lambda^2 + \lambda^2 - \lambda = x$, adică $e = 1 - \lambda$ este element neutru pentru operația " \circ ".

" \Leftarrow ". Dacă notăm cu e elementul neutru pentru operația " \circ ", atunci

$$(\forall) x \in \mathbb{R} \text{ avem } x \circ e = e \circ x = x \Leftrightarrow xe + ax + be + c = ex + ae + bx + c = x \Leftrightarrow \begin{cases} (e + a - 1)x + be + c = 0 \\ (e + b - 1)x + ae + c = 0 \end{cases}$$

Cum x este oarecare, deducem că $e + a - 1 = e + b - 1 = be + c = ae + c = 0$ de unde rezultă că $a = b = 1 - e$ și $c = -ae$.

Dacă notăm $1 - e = \lambda$ atunci $a = b = \lambda$ iar $c = -ae = -\lambda(1 - \lambda) = \lambda^2 - \lambda$, adică operația " \circ " este asociativă (conform cu (i)).

(iii). În ipoteza că operația " \circ " este asociativă, atunci conform cu (i) și (ii), $a = b = \lambda$, $c = \lambda^2 - \lambda$ iar elementul neutru este $e = 1 - \lambda$.

Dacă $x \in U(\mathbb{R}, \circ)$, atunci $(\exists) x' \in \mathbb{R}$ a.î. $x \circ x' = x' \circ x = e \Leftrightarrow xx' + ax + bx' + c = e \Leftrightarrow xx' + \lambda x + \lambda x' + \lambda^2 - \lambda = 1 - \lambda \Leftrightarrow x'(x + \lambda) = 1 - \lambda^2 - \lambda x$. Se observă că dacă $x = -\lambda$ obținem egalitatea absurdă $0 = 1 - \lambda^2 - \lambda(-\lambda) = 1 - \lambda^2 + \lambda^2 = 1$.

Deci pentru $x \neq -\lambda$ deducem $x' = (1 - \lambda^2 - \lambda x)/(x + \lambda)$, adică $U(\mathbb{R}, \circ) = \mathbb{R} \setminus \{-\lambda\}$.

1.3. (i). Prin calcul direct se arată că $(\forall) x, y, z \in \mathbb{Z}$ avem echivalențele:

$$\begin{aligned} x \circ (y \circ z) &= (x \circ y) \circ z \\ \Leftrightarrow a^2xyz + ab(xy + yz + zx) + (ac + b)x + b^2y + b^2z + (bc + c) &= \\ &= a^2xyz + ab(xy + yz + zx) + b^2x + b^2y + (ac + b)z + (bc + c) \\ \Leftrightarrow (ac + b)x + b^2z &= (ac + b)z + b^2x \Leftrightarrow (b^2 - b - ac)(x - z) = 0 \Leftrightarrow b^2 - b - ac = 0 \end{aligned}$$

(căci x și y sunt oarecari).

Deci, operația algebrică este asociativă $\Leftrightarrow b^2 - b - ac = 0$.

(ii). Presupunem că $b^2 - b - ac = 0$ și că operația din enunț are element neutru (fie acesta $e \in \mathbb{Z}$). Atunci cu necesitate $0 \circ e = 0 \Leftrightarrow be + c = 0 \Leftrightarrow c = (-e)b$, adică b divide c . Reciproc, să presupunem că $b^2 - b - ac = 0$ și că b divide c (adică există $d \in \mathbb{Z}$ a.î. $c = bd$).

Dacă operația " \circ " are element neutru e , atunci cu necesitate $x \circ e = x$,

$$(\forall) x \in \mathbb{Z} \Leftrightarrow axe + b(x + e) + c = x \Leftrightarrow e(ax + b) = (1 - b)x - c. \quad (1)$$

Din $b^2 - b - ac = 0$ deducem că $1 - b = -(ac)/b = -(ad)$, deci (1) este echivalentă cu $e(ax + b) = -adx - bd \Leftrightarrow e(ax + b) = -d(ax + b)$, de unde deducem că elementul neutru este cu necesitate $e = -d$.

1.4. Fie $a, b \in H$, adică $(x \circ a) \circ y = x \circ (a \circ y)$ și $(x \circ b) \circ y = x \circ (b \circ y)$, $(\forall) x, y \in M$.

Datorită asociativității operației " \circ " deducem imediat că:
 $(x \circ (a \circ b)) \circ y = ((x \circ a) \circ b) \circ y = (x \circ a) \circ (b \circ y) = x \circ (a \circ (b \circ y)) = x \circ ((a \circ b) \circ y)$,
 $(\forall) x, y \in M$, de unde rezultă că $a \circ b \in H$, deci H este parte stabilă a lui M relativ la operația " \circ ".

1.5. Din ipoteză operația algebrică este bine definită și asociativă. Mai trebuie să arătăm că există elementul neutru.

Deoarece M este finită și f este injectivă, atunci f este o bijecție. Din $a \in M$ și f bijecție $\Rightarrow (\exists) b \in M$ a.î. $aba = a$. Fie $e_1 = ba$ și $e_2 = ab$. Pentru $x \in M$ există $y \in M$ a.î. $f(y) = x \Rightarrow aya = x$. Atunci $xe_1 = ayaba = aya = x$ și $e_2x = abaya = aya = x \Rightarrow xe_1 = e_2x = x$, $(\forall) x \in M$. Pentru $x = e_1$ și $x = e_2$ obținem că $e_2e_1 = e_1$ și $e_2e_1 = e_2 \Rightarrow e_1 = e_2 = e$ elementul neutru al lui M .

1.6. În șirul $\{a, a^2, \dots, a^k, \dots\}$ nu toate elementele sunt distincte deoarece S este finit. Deci există $i, j \in \mathbb{N}^*$ a.î. $a^i = a^{i+j}$. Fie $m \in \mathbb{N}^*$, $m > i+j$.

Atunci $a^m = a^{m-i} \cdot a^i = a^{m-i} \cdot a^{i+j} = a^{m+j} = a^{m+j-i} \cdot a^i = a^{m+j-i} \cdot a^{i+j} = a^{m+2j}$, etc.

Deci pentru orice $k \in \mathbb{N}^*$, $a^m = a^{m+kj}$. Fie $m > i+j$, $m = k \cdot j$. Atunci $a^m = a^{2m}$, deci a^m este idempotent.

1.7. Fie $y = x^{n-1} \Rightarrow x^n y^n = x^n (x^{n-1})^n = x^n x^{n^2-n} = x^{n^2} = x^n$, $(\forall) x \in A$.

În relația din enunț înlocuim pe x cu x^n și pe y cu y^n .

Atunci $x^{n^2} y^{n^2} = y^n x^n \Leftrightarrow x^n y^n = y^n x^n \Leftrightarrow xy = yx$, $(\forall) x, y \in A$.

Observație. Dacă mulțimea (A, \cdot) este grup atunci relația nu poate avea loc decât pentru $n \geq 3$. Pentru $n = 2$, egalitatea $x^2 y^2 = yx$ devine pentru $y = 1$: $x^2 = x \Rightarrow x = 1$, deci nu poate avea loc pentru orice x din A .

1.8. Fie $xy = (yx)^n = [(xy)^n]^n = [(xy)(xy)^{n-1}]^n = (xy)^{n-1}(xy) = (xy)^n = yx$ pentru $n > 1$. Pentru $n = 1$ concluzia este evidentă.

1.9. Arătăm că operația este comutativă, Într-adevăr:

$x \cdot y = (x \cdot y) \cdot (x \cdot y) = [y(xy)]x = [(xy)x]y = [(yx)x]y = [(x \cdot x)y]y = (x \cdot y)y = (y \cdot y)x = y \cdot x$.

Operația este asociativă deoarece $(xy)z = (yz)x = x(yz) \Leftrightarrow (xy)z = x(yz)$.

1.10. În egalitatea 2) înlocuim y cu xy și obținem :

$x(xy)^2x = (xy)x^2(xy) \Rightarrow x^2yxyx = xyx^3y$ (3) $\Rightarrow x^2yxyx = xyxy \Rightarrow \Rightarrow x(xy)^3 = xyxy^2 \Rightarrow x^2y = xyxy^2 \Rightarrow x^2y^2 = xyxy \Rightarrow x^2y^2 = (xy)^2$ (4).

Relația (3) se mai scrie $x(xy)^2x = (xy)^2$ și utilizând (4) avem :

$xx^2y^2x = x^2y^2 \Rightarrow xy^2x = x^2y^2$. Substituind pe x cu y în această ultimă relație avem : $yx^2y = y^2x^2 \Rightarrow x^2y^2 = y^2x^2 \Rightarrow (xy)^2 = (yx)^2$.

Din relația $xy^2x = (xy)^2 \Rightarrow (xy)(xy^2x) = (xy)^3 \Rightarrow (xy)^2yx = (xy)^3$
 $\Rightarrow (yx)^2(yx) = (xy)^3 \Rightarrow (yx)^3 = (xy)^3 \Rightarrow xy = yx$.

1.11. Faptul că $(\mathbb{Z}[i], \cdot)$ este monoid comutativ este imediat.

Dacă $z=a+bi \in U(\mathbb{Z}[i], \cdot)$, atunci $a, b \in \mathbb{Z}$ (în mod evident $a \cdot b \neq 0$) și trebuie ca $1/z \in \mathbb{Z}[i]$.

Însă $1/z = a/(a^2+b^2) - i \cdot b/(a^2+b^2)$, deci trebuie ca $a/(a^2+b^2), b/(a^2+b^2) \in \mathbb{Z}$, de unde deducem imediat că (a, b) trebuie să fie egală cu una din perechile $(0, 1)$, $(1, 0)$, $(0, -1)$ sau $(-1, 0)$, deci $U(\mathbb{Z}[i], \cdot) = \{-1, 1, -i, i\}$.

1.12. Fie $z_i = x_i + y_i \sqrt{d}$, cu $x_i, y_i \in \mathbb{Z}$, $i=1, 2$.

Atunci $z_1 \cdot z_2 = (x_1x_2 + dy_1y_2) + (x_1y_2 + y_1x_2)\sqrt{d} \in \mathbb{Z}[\sqrt{d}]$.

Pentru a demonstra partea a doua a problemei, arătăm că $N(z_1z_2) = N(z_1) \cdot N(z_2)$. Ținând cont de expresia lui z_1z_2 de mai înainte deducem că:

$$\begin{aligned} N(z_1) \cdot N(z_2) &= (x_1^2 - dy_1^2)(x_2^2 - dy_2^2) = x_1^2 x_2^2 - dx_1^2 y_2^2 - dx_2^2 y_1^2 + \\ &+ d^2 y_1^2 y_2^2 = (x_1^2 x_2^2 + d^2 y_1^2 y_2^2) - d(x_1^2 y_2^2 + x_2^2 y_1^2) = (x_1x_2 + dy_1y_2)^2 - d(x_1y_2 + x_2y_1)^2 = \\ &= N(z_1z_2). \end{aligned}$$

Dacă $z \in U(\mathbb{Z}[\sqrt{d}], \cdot)$, atunci $(\exists) z' \in \mathbb{Z}[\sqrt{d}]$ a.î. $zz' = 1$, deci $N(zz') = N(1) = 1$, de unde $N(z) \cdot N(z') = 1$, adică $N(z) \in \{-1, 1\}$.

Reciproc, dacă $z = x + y\sqrt{d} \in \mathbb{Z}[\sqrt{d}]$ și $N(z) \in \{-1, 1\}$, atunci avem $1/z = 1/(x + y\sqrt{d}) = (x - y\sqrt{d})/(x^2 - y^2d) = (x - y\sqrt{d})/N(z) = x/N(z) - (y/N(z))\sqrt{d}$, deci $1/z \in \mathbb{Z}[\sqrt{d}]$ (deoarece $x/N(z) = \pm x \in \mathbb{Z}$ iar $y/N(z) = \pm y \in \mathbb{Z}$), de unde deducem că $z \in U(\mathbb{Z}[\sqrt{d}], \cdot)$.

1.13. Fie $z = 3 + 2\sqrt{2}$. Ținând cont de problema anterioară avem că $N(z) = 3^2 - 4 \cdot 2 = 9 - 8 = 1$, deci $z \in U(\mathbb{Z}[\sqrt{2}], \cdot)$.

Atunci $\{z^n : n \in \mathbb{N}\} \subseteq U(\mathbb{Z}[\sqrt{2}], \cdot)$, de unde deducem că $U(\mathbb{Z}[\sqrt{2}], \cdot)$ este o mulțime infinită.

1.14. " \Rightarrow ". Presupunem prin absurd că n are în descompunerea sa cel puțin doi factori primi distincți p_1, p_2 . Cum $(p_1, p_2) = 1$, $(\exists) \alpha, \beta \in \mathbb{Z}$ a.î. $\alpha p_1 + \beta p_2 = 1$.

Deoarece $p_1 = (n, \alpha p_1)$, $p_2 = (n, \beta p_2)$, deducem că $\alpha p_1, \beta p_2 \in M$.

Cum M este parte stabilă a lui $(\mathbb{Z}, +)$ ar rezulta că $\alpha p_1 + \beta p_2 = 1 \in M$, adică $(n, 1) \neq 1$ ceea ce este absurd, de unde rezultă că n este de forma p^k cu k număr natural, $k \geq 1$ iar p prim.

" \Leftarrow ". Fie $n = p^k$ cu p prim, k natural, $k \geq 1$.

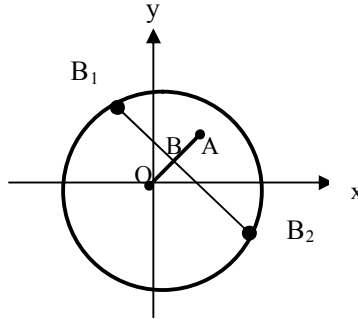
Atunci $M_n = \{x \in \mathbb{Z} : (p^k, x) \neq 1\} = \{pt : t \in \mathbb{Z}\}$ care în mod evident este parte stabilă a lui $(\mathbb{Z}, +)$.

1.15. Să arătăm la început că $D_0 = \{z \in \mathbb{C} : |z| < 1\} \subseteq M$.

Cum $|\pm 1| = 1 \Rightarrow -1, 1 \in M$, adică $0 = (-1) + 1 \in M$.

Fie $z \in \mathbb{C}$ a.î. $0 < |z| < 1$. Considerăm în planul raportat la sistemul ortogonal de axe xOy cercul de centru O și rază 1 (vezi figura) și punctul A , imaginea geometrică a lui z (care va fi situat în interiorul cercului unitate).

Dacă B este mijlocul lui OA , atunci B este imaginea geometrică a lui $z/2$.



Perpendiculara în B pe OA taie cercul unitate în B_1, B_2 . Dacă notăm cu z_1, z_2 afixele lui B_1, B_2 , atunci $z = z_1 + z_2$ (căci figura OB_1AB_2 este romb); cum $|z_1| = |z_2| = 1 \Rightarrow z_1, z_2 \in M$, deci $z \in M$, adică $D_0 \subseteq M$.

Să arătăm acum că și coroana circulară $D_1 = \{z \in \mathbb{C} : 1 < |z| \leq 2\}$ este inclusă în M . Pentru $z \in D_1$, $1 < |z| \leq 2$, deci $|z/2| < 1$ adică $z/2 \in D_0 \subseteq M$, deci $z/2 \in M$. Cum $z = 2 \cdot z/2$ iar $z/2 \in M$, rezultă că $z \in M$, adică $D_1 \subseteq M$.

Să demonstrăm acum că dacă $D_n = \{z \in \mathbb{C} : 2^{n-1} < |z| \leq 2^n\} \subseteq M$ (pentru $n \in \mathbb{N}$) atunci și $D_{n+1} \subseteq M$. Într-adevăr, dacă $z \in D_{n+1}$, atunci $2^n < |z| \leq 2^{n+1} \Rightarrow 2^{n-1} < |z/2| \leq 2^n \Rightarrow z/2 \in D_n \subseteq M \Rightarrow z \in M$ (deoarece $z = 2 \cdot z/2$), deci $D_{n+1} \subseteq M$.

Conform principiului inducției matematice deducem că $D_n \subseteq M$, $(\forall) n \in \mathbb{N}$. Cum $\mathbb{C} = \bigcup_{n \in \mathbb{N}} D_n$ deducem că $\mathbb{C} \subseteq M$ și cum $M \subseteq \mathbb{C} \Rightarrow M = \mathbb{C}$.

1.16. Dacă $z_i = (x_i, y_i) \in M$, $i=1, 2, 3$, atunci :

$(z_1 \circ z_2) \circ z_3 = (x_1 x_2, x_2 y_1 + y_2) \circ (x_3, y_3) = (x_1 x_2 x_3, x_3 (x_2 y_1 + y_2) + y_3) = (x_1 x_2 x_3, x_3 x_2 y_1 + x_3 y_2 + y_3)$ iar $z_1 \circ (z_2 \circ z_3) = (x_1, y_1) \circ (x_2 x_3, x_3 y_2 + y_3) = (x_1 x_2 x_3, x_2 x_3 y_1 + x_3 y_2 + y_3)$, de unde rezultă că $(z_1 \circ z_2) \circ z_3 = z_1 \circ (z_2 \circ z_3)$, adică operația " \circ " este asociativă. Tot prin calcul se arată imediat că elementul

neutru este elementul $e = (1,0)$ ($e \circ z = (1,0) \circ (x,y) = (1 \cdot x, 0 \cdot y + y) = (x,y)$)
 adică dubletul (M, \circ) este monoid. Dacă $z = (x,y) \in U(M, \circ)$, atunci
 $(\exists) z' = (x',y') \in M$ a.î. $zz' = z'z = e \Leftrightarrow xx'=1$ și $x'y+y' = xy'+y = 0$.

Dacă $x = 1$, atunci $x' = 1$, deci $y' = -y \in \mathbb{Z}$, iar dacă $x = -1$ atunci $x' = -1$,
 deci $y' = y \in \mathbb{Z}$.

În concluzie:

$$U(M, \circ) = \{(1, -y) : y \in \mathbb{Z}\} \cup \{(-1, y) : y \in \mathbb{Z}\}.$$

1.17. Fie $M_i = \begin{pmatrix} a_i & b_i \\ c_i & d_i \end{pmatrix} \in M$ cu $a_i, b_i, c_i, d_i \in \mathbb{Z}$ și $a_i + b_i = c_i + d_i$, $i=1,2$.

Atunci $M_1 \cdot M_2 = \begin{pmatrix} a_1 a_2 + b_1 c_2 & a_1 b_2 + b_1 d_2 \\ c_1 a_2 + d_1 c_2 & c_1 b_2 + d_1 d_2 \end{pmatrix}$, deci pentru a demonstra că

$M_1 \cdot M_2 \in M$ trebuie să arătăm că $a_1 a_2 + b_1 c_2 + a_1 b_2 + b_1 d_2 = c_1 a_2 + d_1 c_2 + c_1 b_2 + d_1 d_2 \Leftrightarrow$
 $a_1 (a_2 + b_2) + b_1 (c_2 + d_2) = c_1 (a_2 + b_2) + d_1 (c_2 + d_2)$ ceea ce este adevărat dacă ținem
 cont de faptul că $a_2 + b_2 = c_2 + d_2$ și că $a_1 + b_1 = c_1 + d_1$.

Deoarece matricea unitate $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ face în mod evident parte din M
 deducem că dubletul (M, \cdot) este monoid.

Dacă ținem cont de faptul că pentru oricare două matrice $A, B \in M_2(\mathbb{Z})$
 avem relația $\det(A \cdot B) = \det(A) \cdot \det(B)$ se deduce imediat că:

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in U(M, \cdot) \Leftrightarrow \det(A) = \pm 1 \Leftrightarrow ad - bc = \pm 1 \Leftrightarrow (a+b)(a-c) = \pm 1 \text{ (căci)}$$

$$a+b=c+d) \Leftrightarrow \begin{cases} a+b=1 \\ a-c=1 \end{cases} \text{ sau } \begin{cases} a+b=1 \\ a-c=-1 \end{cases} \text{ sau } \begin{cases} a+b=-1 \\ a-c=1 \end{cases} \text{ sau } \begin{cases} a+b=-1 \\ a-c=-1 \end{cases}.$$

Exprimând numai în funcție de a , deducem că :

$$U(M, \cdot) = \left\{ \begin{pmatrix} a & 1-a \\ a-1 & 2-a \end{pmatrix} \middle| a \in \mathbb{Z} \right\} \cup \left\{ \begin{pmatrix} a & 1-a \\ 1+a & -a \end{pmatrix} \middle| a \in \mathbb{Z} \right\} \cup \\ \cup \left\{ \begin{pmatrix} a & -1-a \\ a-1 & -a \end{pmatrix} \middle| a \in \mathbb{Z} \right\} \cup \left\{ \begin{pmatrix} a & -1-a \\ a+1 & -2-a \end{pmatrix} \middle| a \in \mathbb{Z} \right\}.$$

1.18. Plecând de la observația că pentru $f, g \in A$ și $n \in \mathbb{N}$ avem :

$$(f * g)(n) = \sum_{d_1, d_2 = n} f(d_1)g(d_2)$$

rezultă imediat comutativitatea produsului de convoluție, iar asociativitatea din
 aceea că pentru $f, g, h \in A$ și $n \in \mathbb{N}$:

$$[(f * g) * h](n) = [f * (g * h)](n) = \sum_{d_1, d_2, d_3 = n} f(d_1)g(d_2)h(d_3).$$

Să demonstrăm acum că funcția aritmetică $e: \mathbb{N}^* \rightarrow \mathbb{C}$ definită pentru $n \in \mathbb{N}$ prin $e(n)=1$ pentru $n=1$ și 0 pentru $n \geq 2$ este elementul neutru al produsului de convoluție. Într-adevăr, pentru $f \in A$ și $n \in \mathbb{N}$ avem :

$$(f * e)(n) = \sum_{d_1 d_2 = n} f(d_1) e(d_2) = f(n) e(1) = f(n), \text{ deci } f * e = f, \text{ adică dubletul}$$

$(A, *)$ este monoid comutativ.

Fie acum $f \in U(A, *)$; atunci $(\exists) f' \in A$ a.î. $f * f' = f' * f = e$, deci în particular $(f * f')(1) = e(1) \Leftrightarrow f(1) f'(1) = 1$, de unde rezultă cu necesitate $f(1) \neq 0$. Reciproc, fie $f \in A$ a.î. $f(1) \neq 0$ și să demonstrăm că $f \in U(A, *)$. Pentru aceasta definim recursiv funcția aritmetică $f': \mathbb{N}^* \rightarrow \mathbb{C}$ prin

$$f'(n) = \begin{cases} \frac{1}{f(1)} & \text{pentru } n=1 \\ -\frac{1}{f(1)} \sum_{\substack{d|n \\ d>1}} f(d) f\left(\frac{n}{d}\right) & \text{pentru } n \geq 2 \end{cases}$$

și vrem să demonstrăm că $f' = f^{-1}$ (în monoidul $(A, *)$).

Într-adevăr, $(f * f')(1) = f(1) \cdot 1/f(1) = 1 = e(1)$, iar pentru $n \geq 2$ $(f * f')(n) = \sum_{d|n} f(d) f'(n/d) = f(1) \cdot f'(n) + \sum_{\substack{d|n \\ d>1}} f(d) \cdot f'(n/d) = f(1) \cdot f'(n) = 0 = e(n)$, adică $f * f' = e$, de unde concluzia dorită ($f' = f^{-1}$).

1.19. (i). Presupunem prin absurd că există $a, b \in M$ a.î. $ab = 1$ și $ba \neq 1$. Aplicația $\varphi: M \rightarrow M$ definită prin $\varphi(x) = bx$ este injectivă (dacă $\varphi(x) = \varphi(y)$ atunci $bx = by \Rightarrow a(bx) = a(by) \Rightarrow (ab)x = (ab)y \Rightarrow 1x = 1y \Rightarrow x = y$). Cum M este finită atunci φ este surjectivă, deci există $c \in M$ a.î. $\varphi(c) = bc = 1$. Atunci $a(bc) = a \Rightarrow (ab)c = a \Rightarrow 1c = a \Rightarrow c = a \Rightarrow ba = 1$ – fals.

(ii). De exemplu putem lua $f(n) = \begin{cases} n-1, & n \geq 1 \\ 0, & n = 0 \end{cases}$ și $g(n) = n+1, (\forall) n \in \mathbb{N}$.

(iii). Să presupunem prin absurd că $n > q$. Înmulțind relația din enunț la stânga cu a^q și la dreapta cu b^p se obține: $a^q b^n a^m b^p = a^q b^q a^p b^p$ de unde $a^q b^q b^{n-q} a^m b^p = 1$ și $b^{n-q} a^m b^p = 1$. Notând cu $c = a^m b^p$ (dacă $n-q = 1$) sau $c = b^{n-q-1} a^m b^p$ (dacă $n-q > 1$), rezultă că $bc = 1$. Relațiile $ab = 1$ și $bc = 1$ implică $a = c$, deci $ba = 1$, fals.

Analog pentru $q > n$.

Așadar $q = n$, deci $b^n a^m = b^n a^p$. Presupunem prin absurd $m > p$. Înmulțim egalitatea anterioară la stânga cu a^n obținem $a^n b^n a^m = a^n b^n a^p$, de unde $a^m = a^p$ ceea ce implică $a^m b^p = a^p b^p = 1$ și deci $a^{m-p} a^p b^p = 1 \Rightarrow a^{m-p} = 1$. Dacă $m-p = 1 \Rightarrow a = 1 \Rightarrow b = 1 \Rightarrow ba = 1$ – fals. Dacă $m-p > 1$ atunci $ca = 1$ unde $c = a^{m-p-1} \Rightarrow cab = b \Rightarrow c = b \Rightarrow ba = 1$ – fals.

Analog se exclude cazul $p > m$, deci $p = m$.

1.20. Dacă $M \subseteq \mathbb{R}$, atunci și $\mathbb{R} \subseteq M$ deci $M = \mathbb{R}$; să presupunem că $M \neq \mathbb{R}$, adică $(\exists) z_0 = a_0 + i \cdot b_0 \in M$ cu $a_0, b_0 \in \mathbb{R}$ iar $b_0 \neq 0$. Atunci $ib_0 = z_0 - a_0 \in M$ și $1/b_0 \in M$ deducem că $(1/b_0) \cdot i \cdot b_0 = i \in M$. Atunci $(\forall) z = a + ib \in \mathbb{C}$ (cu $a, b \in \mathbb{R}$) rezultă că $z \in M$, adică $M = \mathbb{C}$.

1.21. Fie $x, y \in Z(M)$. Atunci, folosind faptul că înmulțirea este asociativă pe M deducem că $(xy)z = x(yz) = x(zy) = (xz)y = (zx)y = z(xy)$, $(\forall) z \in M$, deci $xy \in Z(M)$, adică $Z(M)$ este parte stabilă în raport cu înmulțirea.

Deoarece $Z(M) \subseteq M$ rezultă că înmulțirea pe $Z(M)$ este asociativă. Cum $1x = x1 = x$, $(\forall) x \in M$, atunci $1 \in Z(M)$, deci $Z(M)$ este submonoid al lui M .

1.22. Dacă $A = a \cdot I_n$, cu $a \in \mathbb{C}$, atunci în mod evident $A \cdot B = aI_n \cdot B = B \cdot aI_n = B \cdot A$, $(\forall) B \in M_n(\mathbb{C})$, adică $A \in Z(M_n(\mathbb{C}), \cdot)$.

Fie acum $A \in Z(M_n(\mathbb{C}), \cdot)$, $A = (a_{ij})_{1 \leq i, j \leq n}$ iar B_{ij} matricea pătratică de ordin n ce are pe poziția (i, j) 1 iar în rest zero ($i, j \in \{1, 2, \dots, n\}$). Deoarece matricea

$A \cdot B_{ij}$ are coloana a - j -a egală cu $\begin{pmatrix} a_{1j} \\ a_{2j} \\ \dots \\ a_{nj} \end{pmatrix}$ iar în rest toate elementele egale cu zero

pe când matricea $B_{ij} \cdot A$ are doar linia i egală cu $(a_{i1}, a_{i2}, \dots, a_{in})$, din egalitatea $B_{ij} \cdot A = A \cdot B_{ij}$ $(\forall) i, j \in \{1, 2, \dots, n\}$, deducem că $a_{ij} = 0$ pentru $i \neq j$. Scriind că $A \cdot B = B \cdot A$, B fiind de data aceasta matricea de ordin n ce are toate elementele egale cu 1, deducem că $a_{11} = a_{22} = \dots = a_{nn} = a$, $a \in \mathbb{C}$, adică $A = a \cdot I_n$.

1.23. (i). Fie $X = \begin{pmatrix} x & y \\ z & t \end{pmatrix} \in M_2(\mathbb{C})$ și scriind că $AX = XA$ deducem că

$z = 0$ și $t = x$, adică X este de forma $X = \begin{pmatrix} x & y \\ 0 & x \end{pmatrix}$, cu $x, y \in \mathbb{C}$.

(ii). Fie acum $X \in M_2(\mathbb{C})$ a.î. $X^n = A$; deoarece $AX = X^n X = X^{n+1} = XX^n = XA$, ținând cont de (i) deducem cu necesitate că X trebuie să fie de forma

$X = \begin{pmatrix} x & y \\ 0 & x \end{pmatrix}$ cu $x, y \in \mathbb{C}$.

Deoarece se verifică imediat prin inducție matematică egalitatea:

$X^n = \begin{pmatrix} x^n & nx^{n-1}y \\ 0 & x^n \end{pmatrix}$, din $X^n = A$ deducem că $x^n = 1$ și $nx^{n-1}y = 2$, de unde rezultă

că $x^n = 1$ și $2x = ny$.

În concluzie X trebuie cu necesitate să fie de forma $X = \begin{pmatrix} \varepsilon & 2\varepsilon/n \\ 0 & \varepsilon \end{pmatrix}$ cu $\varepsilon^n=1$.

$$\text{Dacă } X = \begin{pmatrix} \varepsilon & 2\varepsilon/n \\ 0 & \varepsilon \end{pmatrix} \text{ cu } \varepsilon^n=1, \text{ atunci } X^n = \begin{pmatrix} \varepsilon^n & 2\varepsilon^n \\ 0 & \varepsilon^n \end{pmatrix} = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}.$$

1.24. Să presupunem prin absurd că $(\exists) n \in \mathbb{N}, n \geq 1$ a.î. $A^n = I_2$ (se deduce imediat că $n \geq 2$). Prin inducție matematică se demonstrează că dacă $A \in M_2(\mathbb{R})$, atunci $(\forall) k \in \mathbb{N}^*$, $(\exists) x_k, y_k \in \mathbb{R}$ a.î. $A^k = x_k \cdot A + y_k \cdot I_2$ (1), cu $x_1=1, y_1=0, x_2=a+d, y_2=-\det(A)$ iar

$$\begin{cases} x_{k+1} = (a+d)x_k + y_k \\ y_{k+1} = -\det(A)x_k = -x_k \end{cases} \quad (2)$$

Cum $A^n = I_2$, din (1) deducem că $I_2 = x_n A + y_n I_2 \Leftrightarrow x_n A = (1 - y_n) I_2$.

Dacă $x_n \neq 0 \Rightarrow A = (1 - y_n) / x_n \cdot I_2$, adică $a = d = (1 - y_n) / x_n$ și cum prin ipoteză $a + d > 2 \Rightarrow (1 - y_n) / x_n > 1$. (3)

Însă $\det(A) = 1 \Leftrightarrow ad = 1 \Leftrightarrow ((1 - y_n) / x_n)^2 = 1$ care este în contradicție cu (3).

Dacă $x_n = 0$, atunci ținând cont de (1) deducem că $A^n = y_n \cdot I_2 \Leftrightarrow I_2 = y_n \cdot I_2$, adică $y_n = 1$.

Ținând cont din nou de relațiile (2) deducem că $y_n = x_{n-1}$, adică $x_{n-1} = 1$, iar $x_n = (a+d)x_{n-1} + y_{n-1}$, de unde $y_{n-1} = -(a+d)$.

Deci $x_{n-2} = a+d$ și din $x_{n-1} = (a+d)x_{n-2} + y_{n-2} \Rightarrow y_{n-2} + (a+d)^2 = 1 \Rightarrow y_{n-2} = 1 - (a+d)^2$.

Deci $A^{n-2} = (a+d)A + [1 - (a+d)^2] \cdot I_2 \Rightarrow A^n = (a+d)A^3 + [1 - (a+d)^2] \cdot A^2$ și cum $A^2 = (a+d)A - I_2$ iar $A^n = I_2$ deducem că $I_2 = (a+d)A^3 + [1 - (a+d)^2] \cdot [(a+d)A - I_2]$.

În final găsim $A^3 = [(a+d)^2 - 1]A + [2 - (a+d)^2] / (a+d) I_2$ și cum din (2) deducem că $x_3 = (a+d)x_2 + y_2 = (a+d)^2 - 1$ iar $y_3 = -x_2 = -(a+d)$, ultima egalitate matriceală devine $x_3 A + y_3 I_2 = [(a+d)^2 - 1] \cdot A + [2 - (a+d)^2] / (a+d) I_2 \Leftrightarrow -(a+d) = [2 - (a+d)^2] / (a+d) \Rightarrow 2 = 0$ ceea ce este absurd, deci $A^n \neq I_2, (\forall) n \in \mathbb{N}, n \geq 1$.

1.25. Din relația $A + B = AB$ deducem că $(I_n - A)(I_n - B) = I_n$, adică $I_n - A$ este inversabilă și $(I_n - A)^{-1} = I_n - B$, deci și $(I_n - B)(I_n - A) = I_n \Leftrightarrow A + B = BA$, adică $AB = BA$.

1.26. Evident, este suficient să probăm doar o implicație.

Fie $A, B \in M_n(\mathbb{C})$ a.î. $I_n - AB \in U(M_n(\mathbb{C}), \cdot) \Leftrightarrow (\exists) C \in M_n(\mathbb{C})$ a.î. $C(I_n - AB) = (I_n - AB)C = I_n \Leftrightarrow C - CAB = C - ABC = I_n$.

Atunci $(I_n - BA)(I_n + BCA) = I_n - BA + BCA - B(ABC)A = I_n - BA + BCA - B(C - I_n)A = I_n - BA + BCA - BCA + BA = I_n$ și analog se demonstrează că $(I_n + BCA)(I_n - BA) = I_n$, adică $I_n - BA \in U(M_n(\mathbb{C}), \cdot)$.

1.27. Dacă S este chiar monoid, adică există $1 \in S$ element neutru, considerăm $M = S$ și $f = 1_S$.

În caz contrar, fie $1 \notin S$ și $M = S \cup \{1\}$. Înzestram M cu o operație algebrică $*$ a.î. M să devină monoid, iar incluziunea lui S în M să fie un morfism.

Fie $x, y \in M$. Atunci definim : $x * y = xy$, dacă $x, y \in S$, $x * 1 = 1 * x = x$, pentru orice $x \in S$ și $1 * 1 = 1$.

Deoarece S este semigrup, înmulțirea pe S este asociativă și atunci operația $*$ este asociativă.

Deci $(M, *)$ este monoid cu 1 element neutru.

Evident, incluziunea este morfism de semigrupuri.

1.28. (i). Dacă $x, y \in M_{f,g}$, atunci $f(x) = g(x)$, $f(y) = g(y)$ și astfel $f(xy) = f(x)f(y) = g(x)g(y) = g(xy)$, adică $xy \in M_{f,g}$. Cum $f(1) = g(1)$ rezultă că $1 \in M_{f,g}$, adică $M_{f,g}$ este submonoid al lui M_1 . Evident $f \circ i = g \circ i$.

(ii). Din $f \circ i' = g \circ i'$ rezultă că $f(i'(x)) = g(i'(x))$, $(\forall) x \in M'$, adică $i'(x) \in M_{f,g}$, $(\forall) x \in M'$. Definim atunci $u: M' \rightarrow M_{f,g}$ prin $u(x) = i'(x)$, $(\forall) x \in M'$. Evident u este un morfism de monoizi (deoarece i' este un morfism) și $i \circ u = i'$. Dacă mai există $v: M' \rightarrow M_{f,g}$ a.î. $i \circ v = i'$, atunci $u(x) = i'(x) = (i \circ v)(x) = i(v(x)) = v(x)$, $(\forall) x \in M'$, deci $u = v$.

1.29. (i) \Rightarrow (ii). Deoarece $f(1) = 1 \Rightarrow 1 \in \text{Ker}(f) \Rightarrow \{1\} \subseteq \text{Ker}(f)$.

Fie $x \in \text{Ker}(f)$, adică $f(x) = 1 = f(1)$. Cum f este presupusă injectivă $\Rightarrow x = 1$, adică $\{1\} \subseteq \text{Ker}(f)$, de unde egalitatea $\text{Ker}(f) = \{1\}$.

Să demonstrăm că (ii) \nRightarrow (i).

Pentru aceasta vom considera monoizii $M_1 = (\mathbb{Z}_3, \cdot)$ și $M_2 = (\mathbb{Z}_2, \cdot)$.

Considerăm $f: \mathbb{Z}_3 \rightarrow \mathbb{Z}_2$, $f(\hat{x}) = \bar{x}^2$, pentru $x = 0, 1, 2$ (unde \hat{x} este clasa lui x în \mathbb{Z}_3 iar \bar{x} este clasa lui x în \mathbb{Z}_2). În mod evident f este morfism de monoizi iar $f(\hat{0}) = \bar{0}$, $f(\hat{1}) = \bar{1}$ și $f(\hat{2}) = \bar{0}$. Se observă că deși $\text{Ker}(f) = \{\hat{1}\}$, totuși f nu este injectivă deoarece $f(\hat{0}) = f(\hat{2})$.

1.30. (i) \Rightarrow (ii). Dacă $x \in M_0$, cum $f \circ g = f \circ h \Rightarrow f(g(x)) = f(h(x))$, $(\forall) x \in M_0 \Rightarrow g(x) = h(x)$, $(\forall) x \in M_0 \Rightarrow g = h$.

(ii) \Rightarrow (iii). Să presupunem prin absurd că $\text{Ker}(f) \neq \{1\}$. Vom nota $M_0 = \text{Ker}(f)$ (care este submonoid al lui M_1 conform problemei **1.28.**, deci și monoid) și vom considera $g, h: M_0 \rightarrow M_1$, g incluziunea iar h morfismul nul.

Atunci pentru $x \in M_0$, $(f \circ g)(x) = f(g(x)) = f(x) = 1$ iar $(f \circ h)(x) = f(h(x)) = f(1) = 1$, adică $f \circ g = f \circ h$ și totuși $g \neq h$.

1.31. (i) \Rightarrow (ii). Fie $y \in M_2$; cum f este surjectivă, $(\exists) x \in M_1$ a.î. $f(x) = y$. Atunci $g(y) = g(f(x)) = (g \circ f)(x) = (h \circ f)(x) = h(f(x)) = h(y)$, adică $g = h$.

(ii) \nRightarrow (i). Fie $M_1 = \mathbb{Z} \setminus \{0\}$ și $M_2 = \mathbb{Q} \setminus \{0\}$ monoizii multiplicativi ai numerelor întregi nenule, respectiv raționale nenule, iar $f: M_1 \rightarrow M_2$ incluziunea canonică.

Dacă M_3 este un alt monoid iar $g, h: M_2 \rightarrow M_3$ sunt morfisme de monoizi a.î. $g \circ f = h \circ f$, vom proba că $g = h$.

Fie $x = m/n \in \mathbb{Q}^*$, cu $m \in \mathbb{N}^*$ și $n \in \mathbb{Z}^*$. Atunci $1 = g(1) = g(n \cdot 1/n) = g(n) \cdot g(1/n) \Rightarrow g(1/n) = (g(n))^{-1}$ și analog $h(1/n) = (h(n))^{-1}$. Avem că $g(x) = g(m/n) = g(m \cdot 1/n) = g(m) \cdot g(1/n) = g(m) \cdot (g(n))^{-1}$ iar $h(x) = h(m/n) = h(m \cdot 1/n) = h(m) \cdot h(1/n) = h(m) \cdot (h(n))^{-1}$. Dar, deoarece f este morfismul incluziune și $g \circ f = h \circ f$, deducem că g și h coincid pe mulțimea \mathbb{Z}^* , de unde rezultă că $g(x) = h(x)$, $(\forall) x \in M_2$, adică $g = h$.

Deci f verifică (ii) fără însă a verifica și pe (i).

§ 2. Grup. Subgrup. Subgrup generat de o mulțime.

Calculul într-un grup. Grupuri de permutări.

2.1. (i). Prin calcul se probează că dubletul (\mathbb{Z}, \circ) este monoid comutativ:

-*asociativitatea*:

$$\begin{aligned} (x \circ y) \circ z &= (xy + 2(x+y+1)) \circ z = (xy + 2(x+y+1))z + 2(xy + 2(x+y+1) + z + 1) = \\ &= xyz + 2xz + 2yz + 2z + 2xy + 4x + 4y + 4 + 2z + 2 = \\ &= xyz + 2xy + 2xz + 2yz + 4x + 4y + 4z + 6 = x \circ (y \circ z) \end{aligned}$$

(din comutativitatea adunării și înmulțirii numerelor întregi)

-*comutativitatea*:

$$x \circ y = xy + 2(x+y+1) = xy + 2x + 2y + 2 = y \circ x$$

- *elementul neutru este $e = -1$* deoarece $x \circ (-1) = x(-1) + 2(x+(-1)+1) = x$

Căutăm elementele inversabile. Fie $x \in U(\mathbb{Z}, \circ)$; atunci $(\exists) x' \in \mathbb{Z}$ a.î. $x \circ x' = -1 \Leftrightarrow xx' + 2(x+x'+1) = -1 \Leftrightarrow xx' + 2x + 2x' + 4 = 1 \Leftrightarrow (x+2)(x'+2) = 1 \Leftrightarrow (x+2 = 1 \text{ și } x'+2 = 1)$ sau $(x+2 = -1 \text{ și } x'+2 = -1) \Leftrightarrow (x = -1 \text{ și } x' = -1)$ sau $(x = -3 \text{ și } x' = -3)$, deci $U(\mathbb{Z}, \circ) = \{-3, -1\}$, adică (\mathbb{Z}, \circ) nu este un grup.

(ii). Conform punctului precedent, $G = \{-3, -1\}$.

2.2. Este evident că $(\forall) x, y \in \mathbb{Q} \Rightarrow x \circ y \in \mathbb{Q}$.

Operația este asociativă și comutativă, elementul neutru este $e = 0$, iar simetricul lui $x \in \mathbb{Q} \setminus \{\frac{1}{k}\}$ este $x' = \frac{x}{kx-1} \neq \frac{1}{k}$, deci $\mathbb{Q} \setminus \{\frac{1}{k}\}$ este grup abelian față de operația algebrică definită.

2.3. $G = (d, \infty)$. Dacă G abelian, conform problemei **1.2.**, $a = b$ și atunci $x \circ y = xy + ax + ay + c = (x + a)(y + a) + c - a^2$.

$(x \circ y) \circ z = [(x + a)(y + a) + c - a^2] \circ z = [(x + a)(y + a) + c - a^2 + a] \cdot (z + a) + c - a^2$ iar $x \circ (y \circ z) = (x + a)[(y + a)(z + a) + c - a^2 + a] + c - a^2$.

Asociativitatea implică egalitatea pentru orice $x, y, z \in G$, adică

$(x + a)(y + a)(z + a) + (c - a^2 + a)(z + a) = (x + a)(y + a)(z + a) + (x + a)(c - a^2 + a) \Rightarrow c = a^2 - a \Rightarrow x \circ y = (x + a)(y + a) - a$, $(\forall) x, y > d \Rightarrow \Rightarrow x(y + a) + a(y + a) - a > d$.

Fie $f(x) = x(y + a) + a(y + a) - a$. Atunci $\lim_{x \rightarrow \infty} f(x) = \infty \Rightarrow y + a > 0$,

$(\forall) y > d \Rightarrow d + a > 0$.

$$\inf_{x \in (d, \infty)} f(x) = \lim_{x \rightarrow d} f(x) = d \Rightarrow d(y + a) + a(y + a) - a = d$$

$(d + a)(y + a) - (d + a) = 0 \Rightarrow (d + a)(y + a - 1) = 0$, $(\forall) y > d \Rightarrow -d = a \Rightarrow x \circ y = xy - dx - dy + d = (x - d)(y - d) + d - d^2$ cu care se verifică axiomele grupului. În concluzie $a = b = -d$ și $c = d$.

2.4. Verificăm mai întâi dacă înmulțirea pe G este bine definită.

Fie $A(a) = \begin{pmatrix} 1 & \ln a & 0 \\ 0 & 1 & 0 \\ 0 & 0 & a \end{pmatrix}$ și $A(b) = \begin{pmatrix} 1 & \ln b & 0 \\ 0 & 1 & 0 \\ 0 & 0 & b \end{pmatrix}$ două matrice din G , cu

$a, b \in \mathbb{R}$, $a, b > 0$. Atunci $A(a) \cdot A(b) = \begin{pmatrix} 1 & \ln a + \ln b & 0 \\ 0 & 1 & 0 \\ 0 & 0 & ab \end{pmatrix} = A(ab) \in G$, deci G este

parte stabilă în raport cu înmulțirea matricelor.

Se știe că înmulțirea matricelor este asociativă.

Din $A(a) \cdot A(b) = A(ab)$ deducem că elementul neutru este $A(1)$ (care este tocmai matricea unitate I_2) iar inversa matricei $A(a)$ este $(A(a))^{-1} = A(1/a)$ (deoarece $A(a) \cdot A(1/a) = A(1)$).

Tot din relația $A(a) \cdot A(b) = A(ab)$, ținând cont de comutativitatea înmulțirii numerelor reale deducem că $A(a) \cdot A(b) = A(b) \cdot A(a) = A(ab) = A(ba)$.

Deci G este grup comutativ.

2.5. Pentru $x \in \mathbb{R} - \{1/2\}$, notăm $A(x) = \begin{pmatrix} 1-x & 0 & x \\ 0 & 0 & 0 \\ x & 0 & 1-x \end{pmatrix}$.

Dacă și $y \in \mathbb{R} - \{1/2\}$, atunci prin calcul direct se demonstrează că :
 $A(x) \cdot A(y) = A(x+y-2xy) \in G$, deoarece $x+y-2xy=1/2 \Leftrightarrow (2x-1)(2y-1)=0 \Leftrightarrow x=1/2$
sau $y=1/2$ – absurd.

În mod evident $A(x) \cdot A(y) = A(y) \cdot A(x)$, $(\forall) x, y \in \mathbb{R} - \{1/2\}$.

Deoarece $A(x) \cdot A(0) = A(x)$, $(\forall) x \in \mathbb{R} - \{1/2\}$, deducem că $A(0)$ este elementul neutru.

Deoarece pentru $x \neq 1/2$ avem $A(x) \cdot A(\frac{x}{2x-1}) = A(0)$, deducem că $(A(x))^{-1} = A(\frac{x}{2x-1})$, deci orice element din G este inversabil.

Din cele de mai sus rezultă că G este grup comutativ.

2.6. Avem :

$$\begin{pmatrix} a_1 & 0 & b_1 \\ 0 & x & 0 \\ c_1 & 0 & d_1 \end{pmatrix} \begin{pmatrix} a_2 & 0 & b_2 \\ 0 & x & 0 \\ c_2 & 0 & d_2 \end{pmatrix} = \begin{pmatrix} a_1 a_2 + b_1 c_2 & 0 & a_1 b_2 + b_1 d_2 \\ 0 & x^2 & 0 \\ a_2 c_1 + c_2 d_1 & 0 & c_1 b_2 + d_1 d_2 \end{pmatrix}.$$

Prin calcul simplu se verifică faptul că ultima matrice este din M doar dacă $x^2 = x$, adică $x \in \{0, 1\}$.

Elementul neutru este I_3 , deci trebuie ca $x = 1$. În acest fel, M este parte stabilă în raport cu înmulțirea matricelor.

Fie $A = \begin{pmatrix} a_1 & 0 & b_1 \\ 0 & x & 0 \\ c_1 & 0 & d_1 \end{pmatrix} \in M$ și $B = \begin{pmatrix} a_2 & 0 & b_2 \\ 0 & x & 0 \\ c_2 & 0 & d_2 \end{pmatrix} \in M$ a.î. $AB = I_3$. Trebuie

să avem:
$$\begin{cases} a_1 a_2 + b_1 c_2 = 1 \\ a_1 b_2 + b_1 d_2 = 0 \\ a_2 c_1 + c_2 d_1 = 0 \\ c_1 b_2 + d_1 d_2 = 1 \end{cases}$$

Înmulțind prima ecuație cu d_1 și pe a treia cu $(-b_1)$ și adunându-le obținem $a_2(a_1 d_1 - b_1 c_1) = d_1 \Rightarrow a_2 = d_1 \Rightarrow c_2 = -c_1, d_2 = a_1, b_2 = -b_1$, deci

$B = \begin{pmatrix} d_1 & 0 & -b_1 \\ 0 & x & 0 \\ -c_1 & 0 & a_1 \end{pmatrix}$. Se observă că $B \in M$ și că $BA = I_3$, deci fiecare element

este inversabil, adică M este un grup.

2.7. Deoarece G trebuie să conțină pe I_2 , atunci:

$$\begin{cases} x_0 + ay_0 = 1 \\ x_0 - ay_0 = 1 \\ y_0 - bx_0 = 0 \\ y_0 + bx_0 = 0 \end{cases}$$

Din primele două ecuații rezultă că $x_0 = 1$ și $y_0 = 0 \Rightarrow bx_0 = 0 \Rightarrow b = 0$.

$$\text{Deci } G = \left\{ \begin{pmatrix} x+ay & y \\ y & x-ay \end{pmatrix} \mid x^2 - 4y^2 = 1, x, y \in \mathbb{R} \right\}.$$

$$\text{Fie } A(x,y) = \begin{pmatrix} x+ay & y \\ y & x-ay \end{pmatrix} \text{ și } A(x',y') = \begin{pmatrix} x'+ay' & y' \\ y' & x'-ay' \end{pmatrix}. \text{ Atunci}$$

$$A(x,y) \cdot A(x',y') = \begin{pmatrix} xx' + yy' + a^2 yy' + a(x'y + xy') & x'y + xy' \\ x'y + xy' & xx' + yy' + a^2 yy' - a(x'y + xy') \end{pmatrix}.$$

Notăm $X = xx' + yy' + a^2 yy'$ și $Y = x'y + xy'$. Atunci $A(x,y) \cdot A(x',y') = A(X,Y)$ și ca aceasta din urmă să fie din G trebuie ca $X^2 - 4Y^2 = 1 \Leftrightarrow (xx' + yy' + a^2 yy')^2 - 4(x'y + xy')^2 = 1$.

Folosind faptul că $x^2 - 4y^2 = x'^2 - 4y'^2 = 1$, ajungem la relația :

$$yy'[-15yy' - 6xx' + a^4 yy' + 2a^2 xx' + 2a^2 yy'] = 0 \Leftrightarrow$$

$$2(a^2 - 3)xx' + (a^4 + 2a^2 - 15)yy' = 0 \Leftrightarrow (a^2 - 3)[2xx' + (a^2 + 5)yy'] = 0.$$

Cum x și y , respectiv x' sau y' , sunt arbitrare rezultă că relația este satisfăcută dacă $a^2 = 3$, adică $a = \pm\sqrt{3}$.

Se arată ușor acum că pentru $a = \sqrt{3}, b=0$ sau $a = -\sqrt{3}, b=0$, (G, \cdot) este grup.

2.8. Dacă $A = \begin{pmatrix} x & 0 \\ 0 & y \end{pmatrix}$, $B = \begin{pmatrix} x' & 0 \\ 0 & y' \end{pmatrix} \in G$, se observă că $AB = BA = \begin{pmatrix} xx' & 0 \\ 0 & yy' \end{pmatrix} \in G$ deoarece $(xx')^n = x^n \cdot x'^n = 1$ și analog pentru $(yy')^n = 1$, deci $(AB)^n = I_2$, adică G este parte stabilă în raport cu înmulțirea matricelor. Evident $I_2 \in G$.

Prin inducție se arată că $A^n = \begin{pmatrix} x^n & 0 \\ 0 & y^n \end{pmatrix}$, iar din $A^n = I_2$ obținem că $x^n = y^n = 1$ ceea ce arată că x și y sunt rădăcini de ordinul n ale unității.

Dacă $A \in G$, inversa lui A este $A^{-1} = A^{n-1}$ (deoarece $A^n = I_2$). Astfel, (G, \cdot) este grup.

Numărul de elemente ale lui G este n^2 (x și y pot lua n valori distincte deoarece sunt rădăcini de ordin n ale unității)

$$2.9. \text{ Pentru } x, y \in \mathbb{R} \text{ notăm } A(x,y) = \begin{pmatrix} x+4y & 2y \\ -2y & x-4y \end{pmatrix}.$$

Prin calcul direct se arată că dacă mai considerăm $x', y' \in \mathbb{R}$, atunci:

$A(x, y) \cdot A(x', y') = A(xx' + 12yy', xy' + x'y) \in G$ (deoarece dacă notăm $x'' = xx' + 12yy'$ și $y'' = xy' + x'y$, atunci avem relația $(x'')^2 - 12(y'')^2 = 1$, ținând cont și de faptul că $x^2 - 12y^2 = (x')^2 - 12(y')^2 = 1$). Din relația de mai sus deducem că $I_2 = A(1, 0)$ este elementul neutru căutat, iar $(A(x, y))^{-1} = A(x, -y) \in G$, precum și faptul că G este comutativ.

2.10. Fie $M(a, b), M(c, d) \in G$, adică $\det M(a, b) = \det M(c, d) = 1$.

Atunci prin calcul direct se arată că $M(a, b) \cdot M(c, d) = M(e, f)$ cu $e = ac + 2bd$, $f = ad + bc + bd$. Deoarece $\det(M(a, b) \cdot M(c, d)) = \det M(a, b) \cdot \det M(c, d) = 1 \Rightarrow \det M(e, f) = 1 \Rightarrow M(e, f) \in G$, deci G este parte stabilă în raport cu înmulțirea matricelor.

Înmulțirea este asociativă, iar $I_3 = M(1, 0) \in G$.

Dacă $M(a, b) \in G \Rightarrow \det M(a, b) = 1 \neq 0$, deci $M(a, b)$ este inversabilă \Rightarrow există $M(a, b)^{-1}$ a.î. $M(a, b) \cdot M(a, b)^{-1} = I_3 \Rightarrow \det (M(a, b)^{-1}) = 1$. Prin calcul se determină $M(a, b)^{-1}$ și anume: $M(a, b)^{-1} = M(a^2 - b^2, b^2 - ab)$, deci $M(a, b)^{-1} \in G$.

Astfel, (G, \cdot) este grup.

2.11. Dacă $f = a + bX + cX^2$ și $g = X^3 - 1$ sunt prime între ele, atunci $f(1) \neq 0$ și $a + b\varepsilon + c\varepsilon^2 \neq 0$, unde ε este o rădăcină de ordin trei a unității, diferită de 1. Din prima condiție obținem $a + b + c \neq 0$, iar din a doua înmulțită

cu ε obținem $a\varepsilon + b\varepsilon^2 + c\varepsilon^3 \neq 0$. Adică $\begin{cases} c\varepsilon^2 + b\varepsilon + a \neq 0 & |b \\ b\varepsilon^2 + a\varepsilon + c \neq 0 & |-c \end{cases} \Rightarrow (b^2 - ac)\varepsilon +$

$+ab - c^2 \neq 0$. Dacă considerăm, de exemplu, $\varepsilon = \cos(2\pi/3) + i \sin(2\pi/3)$, atunci condiția de mai sus devine $(b^2 - ac) \cos(2\pi/3) + (a^2 - bc) \neq 0$ sau $(b^2 - ac) \sin(2\pi/3) \neq 0$. Deci $a^2 - bc \neq 0$ sau $b^2 - ac \neq 0$ sau $c^2 - ab \neq 0$.

Cum $\det A = (a + b + c)[a^2 - bc + b^2 - ac + c^2 - ab]$, din cele de mai sus rezultă că $\det A \neq 0$, adică A este inversabilă.

Se verifică imediat faptul că $A, B \in M \Rightarrow AB = BA \in M$, $I_3 \in M$ este elementul neutru, iar inversa lui $A \in M$ este tot o matrice din M .

Astfel, (M, \cdot) este un grup abelian.

2.12. Se observă întâi că $f_t \circ f_{t'} = f_{t+t'}$, $(\forall) t, t' \in \mathbb{R}$, astfel că verificarea axiomelor grupului rezultă mai ușor:

- *asociativitatea*: $(\forall) t, t', t'' \in \mathbb{R}: f_t \circ (f_{t'} \circ f_{t''}) = (f_t \circ f_{t'}) \circ f_{t''}$

$\Leftrightarrow f_{t+(t'+t'')} = f_{(t+t')+t''}$, $(\forall) t, t', t'' \in \mathbb{R}$, adevărat, deoarece adunarea

numerelor reale este asociativă;

- *comutativitatea* $(\forall) t, t' \in \mathbb{R}: f_t \circ f_{t'} = f_{t'} \circ f_t \Leftrightarrow f_{t+t'} = f_{t'+t}$, $(\forall) t, t' \in \mathbb{R}$

ceea ce este adevărat deoarece adunarea numerelor reale este comutativă;

- *elementul neutru* este f_0 deoarece $f_0 \circ f_t = f_t \circ f_0$, oricare ar fi $t \in \mathbb{R}$;
 - *elementele inversabile* : dacă $f_t \in G$, atunci $f_t^{-1} = f_{-t} \in G$.
- Astfel, (G, \circ) este grup comutativ.

2.13. (i). Se constată că $(\forall) X \in G$, $\det X = [(a+c)^2 - (b+d)^2] [(a-c)^2 + (b-d)^2] \neq 0$ și $(\forall) X, Y \in G \Rightarrow XY = YX \in G$.

De asemenea, $I_4 \in G$ iar dacă se calculează X^{-1} se constată că $X^{-1} \in G$.

Prin urmare (G, \cdot) este grup abelian.

(ii). Fie $A=I_4$, $B = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{pmatrix}$, $C = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}$, $D = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}$.

Făcând tabla înmulțirii pe $H = \{I_4, B, C, D\}$ se observă că $BD = DB = I_4$, $CD = DC = B$, $D^2 = C$, $B^2 = C$, de unde rezultă că $H \leq G$ și $(\forall) X \in G$ avem că $X = aI_4 + bB + cC + dD$. Prin inducție după n se deduce că $X^n = a_n I_4 + b_n B + c_n C + d_n D$, $(\forall) n \in \mathbb{N}^*$.

(iii). Notând cu Y matricea din enunț, atunci $Y = 2I_4 + 3D \Rightarrow$

$$Y^n = (2I_4 + 3D)^n = \sum_{k=0}^n C_n^k (3^k 2^{n-k}) \cdot D^k, \text{ unde } D^k = \begin{cases} I_4, & \text{dacă } k = 4m \\ D, & \text{dacă } k = 4m+1 \\ C, & \text{dacă } k = 4m+2 \\ B, & \text{dacă } k = 4m+3 \end{cases} \text{ și deci}$$

$$Y^n = 2^n I_4 + 3^n D^n + \sum_{\substack{k=1 \\ k=4m}}^n C_n^k (3^k 2^{n-k}) \cdot I_4 + \sum_{\substack{k=1 \\ k=4m+1}}^n C_n^k (3^k 2^{n-k}) \cdot D + \sum_{\substack{k=1 \\ k=4m+2}}^n C_n^k (3^k 2^{n-k}) \cdot C + \sum_{\substack{k=1 \\ k=4m+3}}^n C_n^k (3^k 2^{n-k}) \cdot B.$$

2.14. (i). Fie $X \in M_A$, $X = xI_3 + yA$, $x \in \mathbb{R}^*$, $y \in \mathbb{R} \Rightarrow \det X = x^3$, deci nu depinde de y .

(ii). Notăm $X(x,y) = xI_3 + yA$ și cum $A^2 = O_2$ avem $X(x,y) \cdot X(z,t) = X(xz, xt + yz)$ deci $X(x,y) \cdot X(z,t) \in M_A$. Din expresia lui $X(x,y) \cdot X(z,t)$ observăm că înmulțirea matricelor din M_A este comutativă. Înmulțirea matricelor este asociativă, $I_3 = X(1,0) \in M_A$ este elementul neutru, iar inversa lui $X(x,y)$ este $X(\frac{1}{x}, \frac{-y}{x^2}) \in M_A$, deci (M_A, \cdot) este grup abelian.

(iii). Avem :

- a) $aX(x,y) = X(ax, ay)$; $X(x,y) + X(z,t) = X(x+z, y+t)$;
 b) $X(x,y)^{-1} = X(\frac{1}{x}, \frac{-y}{x^2})$;
 c) $X(x,y)^* = \det X \cdot X(x,y)^{-1} = x^3 X(\frac{1}{x}, \frac{-y}{x^2}) = X(x^2, -xy)$;
 d) $X(x,y)^n = X(x^n, nx^{n-1}y)$, prin inducție după n ;
 e) $(X^*)^n = X(x^{2n}, -nx^{2n-1}y)$; $(X^*)^{-n} = X(x^{-2n}, nx^{-2n-1}y)$, de unde
 $(X^*)^n + (X^*)^{-n} = X(x^{2n} + x^{-2n}, -nx^{2n-1}y + nx^{-2n-1}y) \in M_A$ și din a) rezultă că
 $\det((X^*)^n + (X^*)^{-n}) = (x^{2n} + x^{-2n})^3 \geq 2^3 = 8$.

2.15. (i). Prin calcul direct se arată că M este parte stabilă în raport cu înmulțirea matricelor; înmulțirea matricelor este asociativă, $I_2 \in M$ este element neutru iar dacă $A \in M \Rightarrow \det A \neq 0$, deci A este inversabilă și $A^{-1} \in M$. Astfel, (M, \cdot) este grup.

$$(ii). \text{ Fie } X = \begin{pmatrix} a & b \\ 0 & a+b \end{pmatrix} \in M, X X^t = I_2 \Rightarrow \begin{cases} a^2 + b^2 = 1 \\ b(a+b) = 0 \Rightarrow 2ab = 0 \Rightarrow \\ (a+b)^2 = 1 \end{cases}$$

$$a = 0 \text{ sau } b = 0 \Rightarrow X = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \text{ sau } X = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}.$$

$$(iii). \text{ Fie } Y \in M, Y = \begin{pmatrix} a & b \\ 0 & a+b \end{pmatrix} \text{ a.î. } Y^t \cdot Y = I_2. \text{ Atunci}$$

$$\begin{cases} a^2 = 1 \\ ab = 0 \\ b^2 + (a+b)^2 = 1 \end{cases} \Rightarrow b = 0 \Rightarrow a = \pm 1 \Rightarrow Y = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \text{ sau } Y = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}.$$

2.16. Fie $z_1, z_2 \in U_n \Rightarrow z_1^n = z_2^n = 1$. Deoarece $(z_1 \cdot z_2^{-1})^n = z_1^n \cdot z_2^{-n} = 1$ deducem că $U_n \leq (\mathbb{C}^*, \cdot)$. Analog, dacă $z_1, z_2 \in T \Rightarrow |z_1| = |z_2| = 1$, atunci $|z_1 \cdot z_2^{-1}| = |z_1| \cdot |z_2^{-1}| = 1$, adică $z_1 \cdot z_2^{-1} \in T$, deci $T \leq (\mathbb{C}^*, \cdot)$.

2.17. Asociativitatea înmulțirii rezultă imediat prin calcul (de exemplu : $a(bc) = aa = 1$ iar $(ab)c = cc = 1$, e.t.c.).

Elementul neutru este 1, iar $a^{-1} = a$, $b^{-1} = b$, $c^{-1} = c$. Faptul că K este grup comutativ rezultă imediat din tabelă ($ab = ba = c$, e.t.c.).

2.18. Grupul aditiv al soluțiilor ecuației $a \cos x + b \sin x + c = 0$ fiind subgrup al lui $(\mathbb{R}, +)$ va conține pe 0, deci $a = -c$. Avem două cazuri :

1) $a = 0 \Rightarrow c = 0$ și ecuația devine $b \sin x = 0$. Considerând cazul nebanal când b nu este 0, mulțimea soluțiilor este subgrupul $G = \pi\mathbb{Z} = \{k\pi \mid k \in \mathbb{Z}\}$.

2) $a \neq 0$. Ecuația devine $\sin \frac{x}{2} (b \cos \frac{x}{2} - a \sin \frac{x}{2}) = 0$ și mulțimea soluțiilor sale este $G = G_1 \cup G_2$ unde $G_1 = \{2k\pi \mid k \in \mathbb{Z}\}$ și $G_2 = \{2 \arctg \frac{b}{a} + 2k\pi \mid k \in \mathbb{Z}\}$.

Dacă G este subgrup atunci $u = 4 \arctg \frac{b}{a} \in G$. Analizând cele două cazuri, $u \in G_1$ și $u \in G_2$, deducem că în mod necesar $b = 0$. Dar în acest caz ecuația dată este $a \cos x + c = 0 \Leftrightarrow \cos x = 1$ a cărei mulțime de soluții este subgrupul $G = 2\pi\mathbb{Z} = \{2k\pi \mid k \in \mathbb{Z}\}$.

2.19. Să presupunem că $A \in M_n(\mathbb{R})$ este o matrice pentru care $(G(A), +)$ este grup, $A = (a_{ij})_{1 \leq i, j \leq n}$. Vom nota $L_i(x_1, \dots, x_n)$ matricea din $M_n(\mathbb{R})$ care pe a i -a linie are x_1, x_2, \dots, x_n (în această ordine), restul elementelor fiind nule. Atunci $B = L_1(a_{21}, a_{22}, \dots, a_{2n}) \in G(A)$, $C = L_2(a_{11}, a_{12}, \dots, a_{1n}) \in G(A)$ și deci $B+C \in G(A)$. Avem $0 = \det(A+(B+C)) = \det A + \det(B+C) = \det A$ deci $\det A = 0$. De aici rezultă că $D_i = L_i(a_{i1}, a_{i2}, \dots, a_{in}) \in G(A)$, $(\forall) 1 \leq i \leq n$ căci $\det(A+D_i) = 2^n \det A = 0 = \det A + \det D_i$.

Deducem în continuare că pentru $i \neq j$, $-D_i + L_j(x_{j1}, x_{j2}, \dots, x_{jn}) \in G(A)$ deci și $L_j(x_{j1}, x_{j2}, \dots, x_{jn}) \in G(A)$, $(\forall) 1 \leq j \leq n$, $(\forall) x_{j1}, x_{j2}, \dots, x_{jn} \in \mathbb{R}$.

De aici deducem că $G(A) = M_n(\mathbb{R})$ căci dacă $X = (x_{ij})_{1 \leq i, j \leq n}$, atunci:

$$X = \sum_{i=1}^n L_i(x_{i1}, x_{i2}, \dots, x_{in}) \in G(A).$$

Pentru i, j arbitrare, fixate, putem alege X cu linia a i -a nulă a.î. $A+X$ să aibă pe fiecare linie diferită de a i -a câte un singur 1, fiecare situat pe câte o coloană dintre coloanele $\{1, 2, \dots, j-1, j+1, \dots, n\}$. Vom avea $\pm a_{ij} = \det(A+X) = -\det X = 0$ deci $a_{ij} = 0$, adică $A = O_n$.

2.20. Vom demonstra că în orice grup necomutativ G există cel puțin cinci elemente distincte.

Cum G este necomutativ, $(\exists) x, y \in G$ a.î. $x \neq y$ și $xy \neq yx$. Atunci $1, x, y, xy, yx$ sunt distincte două câte două.

Rezultă de aici că orice grup cu cel mult cinci elemente este comutativ.

2.21. Fie G o mulțime cu n elemente ($n \in \mathbb{N}^*$), $G = \{a_0, \dots, a_{n-1}\}$.

Dacă $i, j \in \{0, 1, 2, \dots, n-1\}$ definim $a_i \cdot a_j = a_r$, unde r este restul împărțirii lui $i+j$ la n .

Această înmulțire este evident asociativă, comutativă, elementul neutru este a_0 , iar simetricul lui a_i este a_{n-i} , $(\forall) i \in \{0, 1, \dots, n-1\}$.

2.22. Să presupunem prin absurd că există un grup G , H_1, H_2 subgrupuri proprii ale sale a.î. $G = H_1 \cup H_2$. Cum H_1, H_2 sunt presupuse proprii, $(\exists) x, y \in G$ a.î. $x \notin H_1, y \notin H_2$ (adică $x \in H_2$ și $y \in H_1$).

Considerăm elementul $z = xy \in G = H_1 \cup H_2$. Dacă $z \in H_1 \Rightarrow x = zy^{-1} \in H_1$ ceea ce este absurd, iar dacă $z \in H_2 \Rightarrow y = x^{-1}z \in H_2$ – din nou absurd.

Observație. Deducem că dacă $H_1, H_2 \leq G$, atunci $H_1 \cup H_2 \leq G \Leftrightarrow H_1 \subseteq H_2$ sau $H_2 \subseteq H_1$.

2.23. Dacă vom considera grupul lui Klein $K = \{1, a, b, c\}$ (vezi problema 2.17.) atunci :

$K = \{1, a\} \cup \{1, b\} \cup \{1, c\}$ iar $\{1, a\}, \{1, b\}, \{1, c\}$ sunt subgrupuri proprii ale lui K .

2.24. Fie $G = H \cup K \cup L$, unde H și K au trei elemente, deci sunt grupuri ciclice, adică $H = \{1, a, a^2\}$ și $K = \{1, b, b^2\}$, unde $a \neq b$. Observăm că $H \cap K$ este subgrup al lui H diferit de H (dacă am avea $H \cap K = H \Rightarrow H \subseteq K \Rightarrow H = K \Rightarrow G = H \cup L$ – absurd).

Cum $|H \cap K| \mid 3 \Rightarrow |H \cap K| = 1 \Rightarrow H \cap K = \{1\}$.

În mod analog, $H \cap L = \{1\} = L \cap K$.

Fie $c = ab$ și $d = a^2b \Rightarrow c \notin H$ și $c \notin K \Rightarrow c \in L$ (dacă de exemplu $c \in H \Rightarrow \Rightarrow b = a^{-1}c \in H \Rightarrow K \subset H \Rightarrow H = K$ – absurd).

În mod analog deducem că $d \notin H$ și $d \notin K \Rightarrow d \in L$.

Deoarece $a \in H$ și $c \in L \Rightarrow ac = d \in K$ (dacă $d \in H \Rightarrow c \in H$ – absurd, iar dacă $d \in L \Rightarrow a \in L \Rightarrow H \subset L \Rightarrow G = K \cup L$ – absurd).

Am obținut că $d \in K \cap L \Rightarrow d = 1 \Rightarrow a^2b = 1 \Rightarrow a^3b = a1 \Rightarrow a = b$, contradicție.

2.25. Fie $x \in H$, arbitrar. Atunci $(\exists) a \in G$ a.î. $x = a^2 \Rightarrow x^{-1} = (a^2)^{-1} = (a^{-1})^2 \in H$. (1)

Fie $x, y \in H \Rightarrow (\exists) a, b \in G$ a.î. $x = a^2$ și $y = b^2 \Rightarrow xy = a^2b^2 = aabb = abab = (ab)^2 \in H$. (2)

Din (1) și (2) rezultă că (H, \cdot) este subgrup al lui (G, \cdot) .

Reciproca nu este adevărată.

Fie S_3 grupul neabelian al permutărilor de ordin 3.

Fie $H = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \right\}$. Se verifică ușor că H este subgrup al

lui S_3 , $H = \{x^2 \mid x \in S_3\}$ dar S_3 nu este comutativ.

2.26. Pentru $a \in G$ fixat $\Rightarrow (\exists) x_0 \in G$ a.î. $ax_0a = a$. Notăm cu $ax_0 = e'$. Pentru $b \in G$ $(\exists) x_1 \in G$ a.î. $ax_1a = b$. Atunci $e'b = ax_0(ax_1a) = ax_1a = b \Rightarrow e'b = b$,

$(\forall) b \in G$. Analog, dacă notăm cu $x_0 a = e'' \Rightarrow be'' = b$, $(\forall) b \in G \Rightarrow e' = e'' = e$ (elementul neutru).

Fie $b \in G$ și $a = c = e \Rightarrow (\exists) x' \in G$ a.f. $ex'b = e \Rightarrow x'b = e$ și $(\exists) x'' \in G$ a.f. $bx''e = e \Rightarrow bx'' = e$.

Dar $x'' = ex'' = x'bx'' = x'e = x' \Rightarrow x' = x'' = x^{-1}$, deci orice element al lui G este inversabil. Astfel, (G, \cdot) este grup.

2.27. Din $ab = c^n \Rightarrow b = a^{-1}c^n \Rightarrow ba = a^{-1}c^n a = (a^{-1}ca)^n$, deci $d = a^{-1}ca$ verifică $ba = d^n$.

2.28. Fie \mathbb{Z}_p și $G = \left\{ \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \mid a, b, c \in \mathbb{Z}_p \right\}$. (G, \cdot) este grup necomutativ.

$$\text{Fie } A = \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \in G \Rightarrow A^2 = \begin{pmatrix} 1 & 2a & 2b + ac \\ 0 & 1 & 2c \\ 0 & 0 & 1 \end{pmatrix}$$

$$\text{Punem } A^n = \begin{pmatrix} 1 & a_n & b_n \\ 0 & 1 & c_n \\ 0 & 0 & 1 \end{pmatrix} \Rightarrow A^{n+1} = \begin{pmatrix} 1 & a + a_n & b + a_n c + b_n \\ 0 & 1 & c + c_n \\ 0 & 0 & 1 \end{pmatrix} =$$

$$= \begin{pmatrix} 1 & a_{n+1} & b_{n+1} \\ 0 & 1 & c_{n+1} \\ 0 & 0 & 1 \end{pmatrix} \Rightarrow \begin{cases} a_{n+1} = a_n + a, & a_1 = a \\ b_{n+1} = b_n + a_n c + b \\ c_{n+1} = c_n + c, & c_1 = c \end{cases} \Rightarrow a_n = na \text{ și } c_n = nc \Rightarrow$$

$$\Rightarrow b_{n+1} - b_n = b + a_n c \Rightarrow b_n = nb + \frac{na(n-1)c}{2} \Rightarrow A^p = \begin{pmatrix} 1 & pa & pb + pac \frac{p-1}{2} \\ 0 & 1 & pc \\ 0 & 0 & 1 \end{pmatrix} = I_3$$

deoarece $a, b, c \in \mathbb{Z}_p \Rightarrow G$ are p^3 elemente.

2.29. Fie $x \in G$ fixat. Definim $f_x: G \rightarrow G$ și $g_x: G \rightarrow G$ prin $f_x(y) = xy$, respectiv $g_x(y) = yx$. Din condițiile din enunț rezultă că f_x și g_x sunt injecții, și deoarece G este finită, ele vor fi bijecții. Atunci există $e_1, e_2 \in G$ a.f. $f_x(e_1) = x$ și $g_x(e_2) = x \Rightarrow xe_1 = e_2x = x$. Atunci $e = e_1 = e_2 \in G$ este element neutru. Tot din faptul că f_x și g_x sunt bijecții rezultă că există x' și x'' în G a.f. $f_x(x') = e$ și $g_x(x'') = e \Rightarrow xx' = x''x = e \Rightarrow x' = ex' = x''xx' = x''e = x''$, deci $x^{-1} = x' = x''$ este inversul lui x . Cum x a fost ales oarecare în G , atunci orice element din G este inversabil, deci G este grup.

2.30. Evident, are loc egalitatea $x(yx)^n = (xy)^n x$, $(\forall) x, y \in G$ și conform ipotezei rezultă că $xy = yx$, deci G este abelian.

2.31. Evident, $aba = bab \Leftrightarrow ab = b(ab)a^{-1} \Rightarrow ab = b(b(ab)a^{-1})a^{-1} = b^2(ab)a^{-2}$ și din aproape în aproape avem $ab = b^n (ab)a^{-n}$, de unde rezultă echivalența cerută.

2.32. (i). Evident, deoarece G este un grup abelian, se verifică ușor că $M_{m,n}(G)$ este grup abelian.

Deoarece orice matrice $A = (a_{ij})_{\substack{1 \leq i \leq m \\ 1 \leq j \leq n}} \in M_{m,n}(G)$ se identifică cu o

funcție $f: \{1,2,\dots,m\} \times \{1,2,\dots,n\} \rightarrow G$, $f(i,j) = a_{ij}$ și reciproc, deducem că numărul elementelor lui $M_{m,n}(G)$ este egal cu numărul acestor funcții, adică cu r^{mn} .

(ii). Presupunem că $ma \neq nb$ și să admitem că $M(a,b) \neq \emptyset$. Fie $A = (a_{ij}) \in M(a,b)$. Calculând suma elementelor matricei A în două moduri, și anume :

$$\sum_{\substack{1 \leq i \leq m \\ 1 \leq j \leq n}} a_{ij} = \sum_{i=1}^m \left(\sum_{j=1}^n a_{ij} \right) = \sum_{i=1}^m a = ma \quad \text{respectiv} \quad \sum_{\substack{1 \leq i \leq m \\ 1 \leq j \leq n}} a_{ij} = \sum_{j=1}^n \left(\sum_{i=1}^m a_{ij} \right) = \sum_{j=1}^n b = nb$$

rezultă că $ma = nb$, contradicție. Deci $M(a,b) = \emptyset$.

(iii). Fie $ma = nb$. Există o bijecție de la mulțimea $M_{m-1,n-1}(G)$ la mulțimea $M(a,b)$. Într-adevăr, fie $B \in M_{m-1,n-1}(G)$, $B = (b_{ij})$, $1 \leq i \leq m-1$, $1 \leq j \leq n-1$, și construim matricea

$A = (a_{ij})_{\substack{1 \leq i \leq m \\ 1 \leq j \leq n}} \in M(a,b)$ definind elementele sale în felul următor:

$$1) a_{ij} = b_{ij} \text{ pentru } 1 \leq i \leq m-1, 1 \leq j \leq n-1;$$

$$2) a_{in} = a - \sum_{1 \leq j \leq n-1} a_{ij} \text{ pentru } 1 \leq i \leq m-1$$

$$3) a_{mj} = b - \sum_{1 \leq i \leq m-1} a_{ij} \text{ pentru } 1 \leq j \leq n-1$$

$$4) a_{mn} = a - \sum_{1 \leq j \leq n-1} a_{mj} = b - \sum_{1 \leq i \leq m-1} a_{in} \quad (\text{deoarece } a - \sum_{1 \leq j \leq n-1} a_{mj} =$$

$$= a - \sum_{1 \leq j \leq n-1} (b - \sum_{1 \leq i \leq m-1} a_{ij}) = a - (n-1)b + \sum_{\substack{1 \leq i \leq m-1 \\ 1 \leq j \leq n-1}} a_{ij} = a + b - nb + S, \text{ unde}$$

$S = \sum_{\substack{1 \leq i \leq m-1 \\ 1 \leq j \leq n-1}} a_{ij}$. În baza lui 2) avem :

$$b - \sum_{1 \leq i \leq m-1} a_{in} = b - \sum_{1 \leq i \leq m-1} (a - \sum_{1 \leq j \leq n-1} a_{ij}) = b - (m-1)a + S = a + b - ma + S.$$

Cum $ma = nb$ rezultă a doua egalitate din 4.)

Din 2) rezultă că $\sum_{1 \leq j \leq n} a_{ij} = a$ pentru $1 \leq i \leq m-1$, și din 3). Avem că

$$\sum_{1 \leq i \leq m} a_{ij} = b \text{ pentru } 1 \leq j \leq n-1 \text{ iar din 4). Rezultă că } a = \sum_{1 \leq j \leq n} a_{mj} \text{ și } b = \sum_{1 \leq i \leq m} a_{in},$$

adică suma elementelor de pe linia m , respectiv coloana n , este a , respectiv b .

Așadar, matricea A construită este din $M(a,b)$ și se va obține prin bordarea matricei B cu elemente din G a.î. în noua matrice suma elementelor de pe fiecare linie să fie egală cu b , iar a_{mn} se obține datorită condiției $ma = nb$.

Funcția $\alpha : M_{m-1,n-1}(G) \rightarrow M(a,b)$ definită prin $\alpha(B) = A$ este o bijecție. Evident α este injectivă. Într-adevăr, fie $\alpha(B_1) = \alpha(B_2) = A$, unde $B_1, B_2 \in M_{m-1,n-1}(G)$ și care sunt submatrici ale lui A , obținute din A prin suprimarea ultimei linii și ultimei coloane, deci $B_1 = B_2$.

Fie $A \in M(a,b)$ și să considerăm B submatricea lui A obținută prin suprimarea liniei m și coloanei n . Avem evident $B \in M_{m-1,n-1}(G)$ și $\alpha(B) = A$, deci α este o surjecție.

Deoarece α este o bijecție, mulțimea $M(a,b)$ are același număr de elemente ca și $M_{m-1,n-1}(G)$, adică $r^{(m-1)(n-1)}$.

2.33. Demonstrăm mai întâi că dacă $A, B, C \leq G$ a.î. $A \subseteq C$, $(AB) \cap C = A(B \cap C)$.

Fie $ac \in A(B \cap C)$, cu $a \in A$ și $c \in B \cap C$. Atunci $ac \in AB$, $ac \in AC = C$, deci $ac \in (AB) \cap C$, adică $A(B \cap C) \subseteq (AB) \cap C$. Pentru cealaltă incluziune fie $ab \in (AB) \cap C$, cu $a \in A$ și $b \in B$. Atunci $b \in C$, deci $ab \in A(B \cap C)$, adică $(AB) \cap C \subseteq A(B \cap C)$, de unde egalitatea cerută.

Astfel, conform celor de mai sus, $A = A(A \cap C) = (AC) \cap B = (BC) \cap B = B$, deci $A = B$.

2.34. Din $Hx = Ky \Rightarrow H = Kyx^{-1} = Kz$, unde $z = yx^{-1} \in G$. Cum $1 \in H = Kz \Rightarrow 1 = kz$, cu $k \in K$ și deci $z = k^{-1} \in K$. Cum $Kz = K \Rightarrow H = K$.

2.35. Pe mulțimea $A \times B$ considerăm relația $(a,b) \sim (a',b') \Leftrightarrow ab = a'b'$ care este o relație de echivalență deoarece este:

-*reflexivă*: $(a,b) \sim (a,b)$, $(\forall) (a,b) \in A \times B$ deoarece $ab = ab$;
 -*simetrică* : $(a,b) \sim (a',b') \Rightarrow (a',b') \sim (a,b)$, $(\forall) (a,b),(a',b') \in A \times B$
 deoarece $ab = a'b' \Rightarrow a'b' = ab$;
 -*tranzitivă*: $(a,b) \sim (a',b')$ și $(a',b') \sim (a'',b'') \Rightarrow ab = a'b'$ și $a'b' = a''b'' \Rightarrow$
 $\Rightarrow ab = a''b'' \Rightarrow (a,b) \sim (a'',b'')$, $(\forall) (a,b),(a',b'),(a'',b'') \in A \times B$.

Clasele de echivalență corespunzătoare sunt de forma :

$$(c)_{\sim} = \{(a,b) \in A \times B : ab = c, c \in AB\}.$$

Evident aplicația $c \rightarrow (c)_{\sim}$ este o bijecție de la AB la $(A \times B) / \sim$.

Fie acum $c \in AB$ iar $a_0 \in A$, $b_0 \in B$ a.î. $a_0 b_0 = c$ și $\varphi : A \cap B \rightarrow (c)_{\sim}$,
 $\varphi(x) = (a_0 x, x^{-1} b_0)$, $(\forall) x \in A \cap B$ (deoarece $(a_0 x)(x^{-1} b_0) = a_0 b_0 = c$, deducem că
 funcția φ este bine definită). În mod evident φ este o injecție.

Pentru a proba surjectivitatea lui φ , fie $(a,b) \in (c)_{\sim}$. Atunci $ab = c = a_0 b_0$,
 deci $a_0^{-1} a = b_0 b^{-1} = x \in A \cap B$ și $\varphi(x) = (a_0 x, x^{-1} b_0) = (a,b)$. Cum $\{(c)_{\sim} : c \in AB\}$
 este o partiție a lui $A \times B$ avem:

$$|A| \cdot |B| = |A \times B| = \sum_{c \in AB} |(c)_{\sim}| = \sum_{c \in AB} |A \cap B| = |A \cap B| \cdot |AB|.$$

2.36. Fie $x \in G$ și $A' = \{xa^{-1} : a \in A\} \subseteq G$. Evident $|A'| = |A|$.

Dacă $A' \cap B = \emptyset$, atunci $|A' \cap B| = |A'| + |B| = |A| + |B| > |G|$, absurd,
 deoarece $A' \cup B \subseteq G$. Deci $(\exists) b \in A' \cap B$ a.î. $b = xa^{-1} \Rightarrow x = ab \in AB$, adică
 $G \subseteq AB$ și cum $AB \subseteq G \Rightarrow G = AB$.

2.37. Arătam că dacă $a, b \in G$ și $a^2 = b^2$, atunci $a = b$. Într-adevăr, dacă
 $a^2 = b^2 \Rightarrow b^{-1} a^2 a^{-1} = b^{-1} b^2 a^{-1} \Rightarrow b^{-1} a = b a^{-1}$.

Conform proprietății 2) avem $(ab^{-1})^2 = (b^{-1}a)^2$. Dar $(b^{-1}a)^2 = (ba^{-1})^2$ și
 $ba^{-1} = (ab^{-1})^{-1} \Rightarrow (b^{-1}a)^2 = [(ab^{-1})^{-1}]^2 = [(ab^{-1})^2]^{-1} \Rightarrow (ab^{-1})^2 = [(ab^{-1})^2]^{-1}$. Înmulțind
 egalitatea cu $(ab^{-1})^2$ obținem $[(ab^{-1})^2]^2 = 1$, de unde conform proprietății 1),
 rezultă că $(ab^{-1})^2 = 1 \Rightarrow ab^{-1} = 1 \Rightarrow a = b$.

Atunci, dacă $(xy)^2 = (yx)^2 \Rightarrow xy = yx$, adică grupul G este abelian.

2.38. Faptul că G este comutativ se probează imediat. Să presupunem că
 G este finit și fie H subgrupul lui G cu proprietatea că este cel mai mare având
 ordinul o putere a lui 2 (deci $|H| = 2^n$ iar n este cel mai mare număr natural cu
 această proprietate).

Deoarece $(\forall) x \in G, x \neq 1, x^2 = 1 \Rightarrow \{1, x\} \leq G$, deci $n \geq 1$.

Intenționăm să demonstrăm că $G = H$ și atunci va rezulta că $|G|$ este o
 putere naturală a lui 2.

Să presupunem prin absurd că $(\exists) x \in G \setminus H$. Atunci $H' = H \cup (xH) \leq G$
 (se probează imediat) și cum $H \cap (xH) = \emptyset$ deducem că $|H'| = |H| + |xH| = |H| +$
 $|H| = 2|H| = 2 \cdot 2^n = 2^{n+1}$, contrazicând astfel maximalitatea lui n . Rămâne deci
 că $G = H$, adică $|G| = 2^n$.

Observație. Pentru o altă soluție relativă la partea a doua a problemei, vezi problema 4.76..

2.39. Fie ord $G = n$ și $S = \{ (a_1, a_2, \dots, a_p) \mid a_i \in G, 1 \leq i \leq p, a_1 a_2 \dots a_p = 1 \}$. Atunci S are n^{p-1} elemente (într-adevăr, dacă $a_1, a_2, \dots, a_{p-1} \in G$ arbitrare $\Rightarrow \Rightarrow a_p = (a_1 a_2 \dots a_{p-1})^{-1}$, deci cum $a_1, \dots, a_p \in G$ și G are n elemente, rezultă că S are n^{p-1} elemente).

Definim relația de echivalență \sim pe S astfel $x \sim y \Leftrightarrow x$ este o permutare ciclică a lui y . Atunci clasa de echivalență a lui $x = (a_1, \dots, a_p)$ conține exact un singur element dacă toți a_i sunt egali, și exact p elemente în caz contrar, deoarece p este prim. Într-adevăr, fie $x = (a_1, \dots, a_p)$ și i, j primul și ultimul rang pentru care $a_i = a_j$ și $a_i = a_{i_1} = \dots = a_{i_k} = a_j$ cu $i < i_1 < \dots < i_k < j$, $k \geq 0$ (dacă $k = 0$, $i_1 = j$). Ca să obținem prin permutări circulare pe locurile i, i_1, \dots, i_k, j aceleași elemente ar trebui să avem:

$p + i - j = j - i_k = \dots = i_1 - i = n \geq k \Rightarrow j = (k+1)n + i \Rightarrow p = n + j - i = n + (k+1)n + i - i = n(k+2)$. Dar p este prim atunci $n = 1$ și $p = k+2 \Rightarrow \Rightarrow i_1 = i + 1, i_2 = i + 2, \dots, j = i + k + 1 = p - 1 + i \Rightarrow a_{i_1} = \dots = a_{i_k}$ și în acest caz rezultă că toate cele p permutări circulare sunt distincte.

Fie r numărul claselor cu un element și t numărul claselor cu p elemente. Atunci $r + tp = n^{p-1}$ și cum $p \mid n$ rezultă $p \mid r$. În plus r este diferit de zero pentru că $(1, 1, \dots, 1) \in S$, deci r este numărul soluțiilor ecuației $x^p = 1$ în G .

2.40. Cum G este în particular monoid, atunci $Z(G)$ este submonoid al lui G (vezi problema 1.21.). Fie acum $x \in Z(G)$; atunci $xy = yx, (\forall) y \in G$, deci $x^{-1}y = yx^{-1}$, de unde deducem că $x^{-1} \in Z(G)$, deci $Z(G) \leq G$.

2.41. Deoarece $xy \in Z(G)$ avem în particular că $(xy)x = x(xy) \Rightarrow xyx = xxy \Rightarrow xy = yx$.

2.42. Deoarece $(m, n) = 1$ există $u, v \in \mathbb{Z}$ astfel încât $mu + nv = 1$. Deoarece x comută cu y^m și y^n , x va comuta și cu $y^{mu} = (y^m)^u$ și $y^{nv} = (y^n)^v$, deci cu produsul lor, $y^{mu} \cdot y^{nv} = y^{mu+nv} = y$.

2.43. Fie $x \in G$; dacă $x \notin H \Rightarrow x \in G \setminus H$ și totul este clar. Dacă $x \in H$, cum $H \neq G, (\exists) y \in G$ a.î. $y \notin H$ și astfel $z = y^{-1}x \notin H$ (căci dacă $z \in H \Rightarrow y = xz^{-1} \in H$, absurd). Astfel $x = yz$ cu $y, z \in G \setminus H$, deci $\langle G \setminus H \rangle = G$.

2.44. Fie $a \in G \setminus H$ și funcția $f_a : H \rightarrow (G \setminus H), f_a(x) = ax$. Evident f_a este injectivă și deoarece $G \setminus H$ are un număr finit de elemente, rezultă că și H are un număr finit de elemente. Cum $G = H \cup (G \setminus H) \Rightarrow G$ este finit.

2.45. Fie G_1 un grup abelian finit și $p = \prod_{x \in G_1} x$. Atunci :

$$p^2 = \left(\prod_{x \in G_1} x \right)^2 = \prod_{x \in G_1} x \cdot \prod_{x \in G_1} x = \prod_{x \in G_1} x \cdot \prod_{x \in G_1} x^{-1} = \prod_{x \in G_1} (xx^{-1}) = 1. \quad (1)$$

Fie $H \leq G$ cu proprietatea (A), $p = \prod_{x \in G} x$, $\alpha = \prod_{x \in H} x$ și $\beta = \prod_{x \in G \setminus H} x$. Cum

$\alpha \cdot \beta = p$ și $\alpha = \beta$, rezultă că $\alpha^2 = p$. Considerând în (1) pe H în loc de G_1 , rezultă că $\alpha^2 = 1$, deci $p = 1$.

Fie $H_1 \leq G$, $H_1 \neq G$, $\alpha_1 = \prod_{x \in H_1} x$ și $\beta_1 = \prod_{x \in G \setminus H_1} x$. Cum $\alpha_1 \beta_1 = p = 1$, rezultă

că $\beta_1 = \alpha_1^{-1}$. Dar, din (1), $\alpha_1^2 = 1$, deci $\alpha_1^{-1} = \alpha_1$. Obținem $\beta_1 = \alpha_1$, deci H_1 are proprietatea (A).

2.46. (i). Dacă G și H sunt grupuri finite, atunci în mod evident $s(G \times H) \geq s(G) \cdot s(H)$ (căci $G' \leq G$, $H' \leq H \Rightarrow G' \times H' \leq G \times H$). Pentru grupul lui

Klein K avem $|K| = 4$, $s(K) = 5$ astfel că $\frac{|K^n|}{s(K^n)} \leq \left(\frac{|K|}{s(K)} \right)^n = \left(\frac{4}{5} \right)^n$ pentru orice

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

Fie acum $a \in \mathbb{R}$, $a > 0$. Deoarece $\left(\frac{4}{5} \right)^n \xrightarrow{n \rightarrow \infty} 0$, există $n_a \in \mathbb{N}^*$ astfel

încât $\left(\frac{4}{5} \right)^{n_a} < a$. Pentru $G = K^{n_a}$ avem $\frac{|K|}{s(K)} \leq \left(\frac{4}{5} \right)^{n_a}$ astfel că $\frac{|Z_p|}{s(Z_p)} = \frac{p}{2}$.

(ii). Fie $a \in \mathbb{R}$, $a > 0$. Există p_a prim astfel încât $\frac{p_a}{2} > a$. Alegând grupul

$G = (\mathbb{Z}_{p_a}, +)$ avem $\frac{|Z_{p_a}|}{s(Z_{p_a})} = \frac{p_a}{2} > a$.

2.47. " \Rightarrow ". (M, \cdot) este grup. Atunci $(\forall) y \in M$, $(\exists) n = 1$, $x \in M$, $x = a^{-1}y a^{-1}$ a.î. $f_a(x) = a(a^{-1}ya^{-1})a^{-1} = y$, deci f_a este surjectivă.

" \Leftarrow ". $(\forall) a \in M$, $(\exists) n \in \mathbb{N}^*$ a.î. $f_a(x) = axa^n$ este surjecție. Atunci, din $a \in M$ rezultă că $(\exists) b \in M$ a.î. $f_a(b) = a \Rightarrow aba^n = a$. Fie $e = aba^{n-1}$ și $f = ba^n$. Dacă $x \in M \Rightarrow (\exists) y \in M$ a.î. $f_a(y) = aya^n = x$. Atunci $ex = (aba^{n-1})aya^n = aba^n ya^n = x$ și $xf = (aya^n)(ba^n) = aya^n = x \Rightarrow ex = xf = x$, $(\forall) x \in M$. Pentru $x = e \Rightarrow ef = e$ iar pentru $x = f \Rightarrow ef = f \Rightarrow e = f$ și $ex = xe = x$, $(\forall) x \in M$, deci e este element neutru. Din alegerea lui $e = aba^{n-1} = f = ba^n$ rezultă că $e = a(ba^{n-1}) = (ba^{n-1})a$, adică $a^{-1} = ba^{n-1}$ este inversul lui a . Cum a a fost ales arbitrar în M , atunci orice element din M este inversabil, deci (M, \cdot) este grup.

2.48. Pentru $n \in \mathbb{N}$ considerăm $H_n = \{m/n! : m \in \mathbb{Z}\}$ deoarece $m/n! = m(n+1)/(n+1)!$ deducem că $H_n \leq H_{n+1}$ și în mod evident $H_n \leq (\mathbb{Q}, +)$.

De asemenea, $\mathbb{Q} = \bigcup_{n \geq 1} H_n$. Să presupunem acum prin absurd că $(\mathbb{Q}, +)$ ar

fi finit generat și fie x_1, x_2, \dots, x_m un sistem de generatori ai lui $(\mathbb{Q}, +)$.

Pentru fiecare $i = 1, 2, \dots, m$, $(\exists) x_i \in H_{n_i}$ și în mod evident avem incluziunea $H_{n_1}, H_{n_2}, \dots, H_{n_m} \subseteq H_n$, unde $n = \max\{n_1, n_2, \dots, n_m\}$.

Deci $\mathbb{Q} = \langle \{x_1, x_2, \dots, x_m\} \rangle \leq H_n \leq \mathbb{Q}$, adică $\mathbb{Q} = H$ ceea ce este absurd.

2.49. Dacă $H \leq (\mathbb{Q}, +) \Rightarrow H \subset \mathbb{Q}$. Vom demonstra incluziunea $\mathbb{Q} \subseteq H$.

Dacă $H = \{0\}$ atunci vom avea $\mathbb{Q} = \{0\} + \mathbb{Z} = \{0 + n \mid n \in \mathbb{Z}\} = \mathbb{Z}$ ceea ce este absurd.

Cum intersecția a două subgrupuri ale unui grup este tot un subgrup rezultă că $H \cap \mathbb{Z}$ este subgrup al lui \mathbb{Q} . Dar $H \cap \mathbb{Z}$ este subgrup al lui \mathbb{Z} și deci $H \cap \mathbb{Z} = n_1 \mathbb{Z}$, $n_1 \in \mathbb{N}^*$, deoarece $H \neq \{0\}$.

Fie $x \in \mathbb{Q} \Rightarrow x = h + n$, $h \in H$, $n \in \mathbb{Z} \Rightarrow n_1 x = n_1 h + n_1 n$. Cum $n_1 h \in H$, $n_1 n \in n_1 \mathbb{Z} \subset H \Rightarrow n_1 x \in H \Rightarrow n_1 \mathbb{Q} \subseteq H \Rightarrow \mathbb{Q} \subseteq H$ și problema este rezolvată.

2.50. Lăsăm pe seama cititorului verificarea axiomelor grupului (care nu ridică probleme deosebite).

2.51. Pe $G = (0, 1)$ operația $x \circ y = \frac{xy}{2xy - x - y + 1}$ determină un grup

abelian și cum pentru $a < b$ există o bijecție între $(0, 1)$ și (a, b) , totul rezultă acum din exercițiul precedent).

2.52. (i) \Rightarrow (ii). Fie $x \in G$, atunci submulțimea $H = \{x^n \mid n \in \mathbb{N}^*\}$ a lui G este parte stabilă a sa, deci subgrup. Rezultă că $1 \in H$, deci există $k \in \mathbb{N}^*$ astfel încât $x^k = 1$.

(ii) \Rightarrow (i). Fie H o submulțime a lui G care este parte stabilă și $x \in H$.

Din ipoteză există $k \in \mathbb{N}^*$ a.î. $x^k = 1$, deci $1 \in H$. Fie $x \in H \setminus \{1\}$. Atunci există $k \geq 2$ astfel încât $x^k = 1 \Rightarrow x^{-1} = x^{k-1}$. Dar H este parte stabilă a lui G și deci $x^{-1} = x^{k-1} \in H$.

2.53. Fie $x \in G$. Vom demonstra mai întâi că pentru orice $t \in \mathbb{N}, 1 \leq t \leq n-1$, dacă x se găsește în t dintre subgrupurile H_1, H_2, \dots, H_n , atunci $(\exists) 1 \leq u \leq n-1$, încât x^u să se găsească în $t+1$ dintre subgrupurile H_1, H_2, \dots, H_n .

Fie $x \in \bigcap_{1 \leq i \leq t} H_i$. Există $h \in H$ a.î. $h \notin \bigcup_{t+1 \leq j \leq n} H_j$. Atunci pentru orice $m \in \mathbb{N}^*$, $x^m h \notin \bigcup_{1 \leq i \leq n} H_i$, deci $x^m h \notin \bigcup_{k+1 \leq j \leq n} H_j$. Există deci $m \in \mathbb{N}$ cu $t+1 \leq m \leq n$ și există $r, s \in \{1, 2, \dots, n-t-1\}$, $r < s$, a.î. $x^r h, x^s h \in H_m$.

Prin urmare $x^{s-r} = (x^s h) \cdot (x^r h)^{-1} \in H_m$. Notăm $k = s-t$ și se observă că x^k se găsește în H_1, H_2, \dots, H_t și H_m ($t+1$ subgrupuri), $k \leq n-t$.

Folosind cele demonstrate, rezultă că există $k_1, k_2, \dots, k_{n-2} \in \mathbb{N}^*$ cu $k_i \leq n-i, 1 \leq i \leq n-2, i \in \{1, 2, \dots, n-2\}$ a.î. $x^k \in \bigcap_{1 \leq i \leq n} H_i$, unde $k = k_1 k_2 \dots k_{n-2}$.

2.54. (i). Fie $x, y \in H_n, x = \frac{k}{n!}, y = \frac{p}{n!}$, deci $x + y = \frac{k+p}{n!} \in H_n$, deci H_n este parte stabilă.

Fie $x \in H_n, x = \frac{k}{n!} \Rightarrow -x = \frac{-k}{n!} \in H_n$, deci $H_n \leq \mathbb{Q}$. Dacă $x \in \mathbb{Q}, x = \frac{p}{q}$, atunci $x \in H_q$, deci $\mathbb{Q} = \bigcup_{n \in \mathbb{N}^*} H_n$.

(ii). Considerăm $A = \{ \frac{1}{n!} \mid n \in \mathbb{N}^* \}$.

Dacă presupunem că $\mathbb{Q} = G_1 \cup \dots \cup G_m$, cum A este infinită, rezultă că există i a.î. $G_i \cap A$ să fie infinită. Se observă că $H_n \subset H_{n+1}$ și dacă $\frac{1}{n!} \in G_i$ rezultă că $H_n \subset G_i$. Fie $n < r$ a.î. $\frac{1}{r!} \in G_i \cap A$. Atunci $H_r \subset G_i \Rightarrow H_n \subset G_i$. Deci $\bigcup_{n \in \mathbb{N}^*} H_n \subset G_i$ sau $\mathbb{Q} \subset G_n$, fals.

2.55. Conform problemei 2.16., $U_n \leq (\mathbb{C}^*, \cdot)$.

Avem $U_n = \{z_0, z_1, \dots, z_{n-1}\}$, unde $z_k = \cos(2k\pi/n) + i \cdot \sin(2k\pi/n)$, $k=0, 1, \dots, n-1$, de unde rezultă că $|U_n| = n$, și cum $z_k = z_1^k, k = 0, 1, \dots, n-1$ deducem că $U_n = \langle z_1 \rangle$ adică U_n este grup ciclic.

Observație. U_n va avea $\varphi(n)$ generatori și anume elementele de forma z_k cu $(k, n) = 1, 1 \leq k \leq n$.

Un generator al lui U_n poartă numele de *rădăcină primitivă a unității de ordin n* .

2.56. Fie $x \in H_m H_n$. Atunci $x = ab, a \in H_m, b \in H_n$, deci $a^m = b^n = 1$.

Fie $[m, n] = k \Rightarrow m \mid k$ și $n \mid k$. Deoarece G este comutativ, $x^k = (ab)^k = a^k b^k = 1 \Rightarrow x \in H_k = H_{[m, n]}$, și astfel $H_m H_n \subseteq H_{[m, n]}$.

Fie $x \in H_k$, $[m,n] = k$. Dacă $d = (m,n) \Rightarrow (\exists) u, v \in \mathbb{Z}$ a.î. $d = mu + nv$.

Atunci $k \cdot d = m \cdot n \Rightarrow k(mu + nv) = m \cdot n \Rightarrow 1 = \frac{kmu}{mn} + \frac{knv}{mn} = \frac{ku}{n} + \frac{kv}{m}$ de

unde: $x = x^1 = x^{\frac{ku}{n} + \frac{kv}{m}} = x^{\frac{ku}{n}} \cdot x^{\frac{kv}{m}}$. Luând $a = x^{\frac{ku}{n}}$ și $b = x^{\frac{kv}{m}}$ vom avea :

$a^m = a^{kv} = (a^v)^k = 1$ și $b^m = b^{ku} = (b^u)^k = 1$, deci $a \in H_m$ și $b \in H_n$ și $x = ab \in H_m H_n$.

Astfel, am demonstrat și incluziunea inversă $H_{[m,n]} \subseteq H_m H_n$, de unde egalitatea cerută.

Observație. Aplicând acest rezultat grupului multiplicativ al numerelor complexe (\mathbb{C}^*, \cdot) , obținem că $U_m U_n = U_{[m,n]}$, unde $U_m = \{z \in \mathbb{C}^* \mid z^m = 1\}$.

2.57. Dacă $H, K \in L(G)$, atunci $H \cap K \in L(G)$ și astfel $H \wedge K = H \cap K$; cum reuniunea a două subgrupuri nu este în general un subgrup (vezi problema **2.22.**), atunci $H \vee K = \langle H \cup K \rangle$ (subgrupul generat de $H \cup K$, adică cel mai mic subgrup al lui G ce conține pe H și pe K).

Astfel, $(L(G), \subseteq)$ devine latices. Ea este o latices completă pentru că există infimul și supremul oricărei familii de subgrupuri ale lui A (infimul este intersecția tuturor subgrupurilor acestei familii, iar supremul este subgrupul generat de reuniunea acestor subgrupuri).

2.58. Dacă $H, K \in L(\mathbb{Z}, +)$, $H \wedge K = H \cap K$ (conform exercițiului anterior). Atunci trebuie să demonstrăm că $m\mathbb{Z} \cap n\mathbb{Z} = [m,n]\mathbb{Z}$. Notăm cu $t = [m,n]$, și atunci $t = mm_1 = nn_1$. Fie $x \in m\mathbb{Z} \cap n\mathbb{Z}$; atunci $x = mx_1 = nx_2$, cu $x_1, x_2 \in \mathbb{Z}$, deci $m \mid x$ și $n \mid x$. Cum $t = [m,n]$ rezultă că $t \mid x$, adică $x \in t\mathbb{Z}$. Invers, fie $x \in t\mathbb{Z}$; atunci $x = tx_1$, cu $x_1 \in \mathbb{Z}$, deci $x = mm_1 x_1 = nn_1 x_1$, ceea ce arată că $x \in m\mathbb{Z}$ și $x \in n\mathbb{Z}$.

Analog se demonstrează că $H \vee K = (m,n)\mathbb{Z}$.

Distributivitatea lui $(L(\mathbb{Z}, +), \subseteq)$ rezultă din faptul că (\mathbb{N}, \mid) este o latices distributivă și folosind cele demonstrate anterior.

2.59. Scriind că pentru $x, y \in G$ avem $(xy)^2 = x^2 y^2 \Rightarrow xyxy = xxyy \Rightarrow \Rightarrow yx = xy$ deci G este comutativ.

2.60. Fie $x, y \in G$; din $x^{n+1} y^{n+1} = (xy)^{n+1} \Rightarrow x^{n+1} y^{n+1} = (xy)^n xy = x^n y^n xy \Rightarrow \Rightarrow xy^n = y^n x$. (1)

Analog se deduce și relația $xy^{n+1} = y^{n+1} x$ (2).

Deoarece $(n, n+1) = 1 \Rightarrow (\exists) \alpha, \beta \in \mathbb{Z}$ a.î. $\alpha n + \beta(n+1) = 1 \Rightarrow xy = (xy)^{\alpha n + \beta(n+1)} = x(y^n)^\alpha \cdot (y^{n+1})^\beta = (y^n)^\alpha \cdot (y^{n+1})^\beta x = y^{\alpha n + \beta(n+1)} x = yx$, adică G este comutativ.

2.61. Pentru $x, y \in G$ avem $(xy)^{n+2} = (xy)^n(xy)^2 = x^n y^n xyxy = x^{n+2} y^{n+2} \Rightarrow \Rightarrow y^n xyx = x^2 y^{n+1}$ (1).

De asemenea, $(xy)^{n+4} = (xy)^{n+2}(xy)^2 = x^{n+2} y^{n+2} xyxy = x^{n+4} y^{n+4} \Rightarrow \Rightarrow y^{n+2} xyx = x^2 y^{n+3}$ (2).

Din (1) și (2) $\Rightarrow y^{n+2} xyx = y^2 x^2 y^{n+1} = x^2 y^{n+3} \Rightarrow x^2 y^2 = y^2 x^2$, $(\forall) x, y \in G$.
Ținând cont această ultimă relație, (1) devine $y^n xyx = x^2 y^2 y^{n-1} = y^2 x^2 y^{n-1} \Rightarrow \Rightarrow y^{n-1} xyx = x^2 y^{n-1}$.

Dacă n este par, continuând procedeul deducem că $xyx = x^2 y \Rightarrow \Rightarrow xy = yx$.

Dacă n este impar, cu același procedeu găsim $yxyx = x^2 y^2 = y^2 x^2 = yyxx \Rightarrow xy = yx$.

Deci G este comutativ.

2.62. Cum $(m, n) = 1$, $(\exists) \alpha, \beta \in \mathbb{Z}$ a.î. $\alpha m + \beta n = 1$. Astfel, dacă $x, y \in G$ avem $xy = (xy)^{\alpha m + \beta n} = [(xy)^m]^\alpha \cdot [(xy)^n]^\beta = [(yx)^m]^\alpha \cdot [(yx)^n]^\beta = (yx)^{\alpha m + \beta n} = yx$, adică G este comutativ.

2.63. Din $x^3 = 1 \Rightarrow x^2 = x^{-1}$, $(\forall) x \in G$. Deci pentru $x, y \in G$, din $x^2 y^2 = y^2 x^2 \Rightarrow x^{-1} y^{-1} = y^{-1} x^{-1} \Rightarrow yx = xy$, adică G este comutativ.

2.64. (i). Evident.

(ii). Avem $[xy, z] = (xy)^{-1} z^{-1} xyz = y^{-1} x^{-1} z^{-1} xyz$ iar $y^{-1} [x, z] y [y, z] = y^{-1} (x^{-1} z^{-1} x z) y (y^{-1} z^{-1} y z) = y^{-1} x^{-1} z^{-1} x z y y^{-1} z^{-1} y z = y^{-1} x^{-1} z^{-1} x z z^{-1} y z = y^{-1} x^{-1} z^{-1} x y z$, de unde egalitatea cerută.

Analog procedăm și pentru (iii).

(iv). Avem $t = y^{-1} [[x, y^{-1}], z] y = y^{-1} [x^{-1} y x y^{-1}, z] y = y^{-1} ((x^{-1} y x y^{-1})^{-1} z^{-1} (x^{-1} y x y^{-1}) z) y = y^{-1} (y x^{-1} y^{-1} x z^{-1} x^{-1} y x y^{-1} z) y = y^{-1} y x^{-1} y^{-1} x z^{-1} x^{-1} y x y^{-1} z y = x^{-1} y^{-1} x z^{-1} x^{-1} y x y^{-1} z y$ și analog :

$u = z^{-1} [[y, z^{-1}], x] z = y^{-1} z^{-1} y x^{-1} y^{-1} z y z^{-1} x z$

$v = x^{-1} [[z, x^{-1}], y] x = z^{-1} x^{-1} z y^{-1} z^{-1} x z x^{-1} y x$ și astfel

$tu = x^{-1} y^{-1} x z^{-1} x^{-1} z y z^{-1} x z = v^{-1}$, de unde egalitatea $tuv = 1$.

2.65. Prima parte a enunțului este evidentă (elementul neutru este 1_X).

Faptul că unitățile lui $F(X)$ sunt aplicațiile bijective rezultă din faptul că o funcție este bijectivă \Leftrightarrow este inversabilă.

2.66. Se arată imediat că $\tau^n(x) = 2^n x$, $(\forall) x \in \mathbb{R}$, astfel :

$\sigma_n(x) = \tau^{-n}(\sigma(\tau^n(x))) = \tau^{-n}(\sigma(2^n x)) = \tau^{-n}(2^n x + 1) = 2^{-n}(2^n x + 1) = x + 2^{-n}$

și $\sigma_n^2 = \sigma_n(x + 2^{-n}) = x + 2^{-n} + 2^{-n} = \sigma_{n-1}(x)$, $(\forall) x \in \mathbb{R}$.

Rezultă că $\sigma_{n-1} = \sigma_n^2 \in H_n$, deci $H_{n-1} = \langle \sigma_{n-1} \rangle \leq H_n$.

Pe de altă parte, $\sigma_n \notin H_{n-1}$ căci dacă $\sigma_n \in H_{n-1}$, atunci $\sigma_n = \sigma_{n-1}^k$ pentru un $k \in \mathbb{Z}$, deci $x + 2^{-n} = \sigma_n(x) = x + k \cdot 2^{-n+1}$, $(\forall) x \in \mathbb{R}$ ceea ce implică $1 = 2k$, absurd.

Ultima parte a problemei se demonstrează ca în problema 2.48.

Observație. Această problemă ne arată că într-un grup finit generat putem găsi subgrupuri ce nu sunt finit generate.

2.67. Soluția 1.

Fie $G = \{ F : \mathbb{R} \rightarrow \mathbb{R} \mid F' = f \}$. (G, \circ) fiind subgrup al grupului bijecțiilor lui \mathbb{R} , rezultă că $F \circ F \in G \Rightarrow (F \circ F)' = f \Rightarrow f(F(x)) f(x) = f(x)$, $(\forall) x \in \mathbb{R} \Rightarrow f(x) [f(F(x)) - 1] = 0$, $(\forall) x \in \mathbb{R} \Rightarrow f(\mathbb{R}) \subset \{0, 1\}$.

Dar cum f admite primitive pe \mathbb{R} și deci are proprietatea lui Darboux pe $\mathbb{R} \Rightarrow f(\mathbb{R}) = \{0\}$ sau $f(\mathbb{R}) = \{1\}$, adică $f(x) = 0$, $(\forall) x \in \mathbb{R}$, sau $f(x) = 1$, $(\forall) x \in \mathbb{R}$. Convine $f(x) = 1$, $(\forall) x \in \mathbb{R}$, caz în care $G = \{ F : \mathbb{R} \rightarrow \mathbb{R} \mid F(x) = x + k, k \in \mathbb{R} \}$ și se verifică ușor că (G, \circ) este grup.

Soluția 2.

Fie (S, \circ) grupul bijecțiilor lui \mathbb{R} și (G, \circ) subgrupul format din primitivele funcției $f : \mathbb{R} \rightarrow \mathbb{R}$.

Rezultă că elementul neutru al lui S se află în G , adică $F : \mathbb{R} \rightarrow \mathbb{R}$, $F(x) = x$. $F \in G \Rightarrow f(x) = 1$, $(\forall) x \in \mathbb{R}$. De asemenea se verifică și în acest caz că $G = \{ F : \mathbb{R} \rightarrow \mathbb{R} \mid F(x) = x + k, k \in \mathbb{R} \}$ este subgrup al grupului bijecțiilor.

2.68. Evident, $1_X \in \text{Izom}(X)$; fie $f, g \in \text{Izom}(X)$ și $x, y \in X$. Atunci, $d((f \circ g)(x), (f \circ g)(y)) = d(f(g(x)), f(g(y))) = d(g(x), g(y)) = d(x, y)$, adică $f \circ g \in \text{Izom}(X)$. De asemenea $f^{-1} \in \text{Izom}(X)$, căci dacă $x, y \in X$, $d(f^{-1}(x), f^{-1}(y)) = d(f(f^{-1}(x)), f(f^{-1}(y))) = d(x, y)$, adică $\text{Izom}(X) \leq \Sigma(X)$.

2.69. (i). Vom considera pe E^2 (planul euclidian) raportat la un sistem cartezian xOy cu originea într-un punct O . În felul acesta, fiecărui punct $A \in E^2$ îi corespunde o pereche ordonată de numere reale (x_A, y_A) (coordonatele carteziene ale lui A relative la sistemul xOy).

Astfel, o translație a lui E^2 nu este altceva decât o aplicație de forma $\tau_A : E^2 \rightarrow E^2$ (cu $A \in E^2$) definită astfel: $\tau_A(P) = A + P$, $(\forall) P \in E^2$ (punctul $A + P$ avînd drept coordonate suma coordonatelor lui A și P).

Dacă $A, B \in E^2$, atunci $(\tau_A \circ \tau_B)(P) = A + (B + P) = (A + B) + P = \tau_{A+B}(P)$, $(\forall) P \in E^2$, deci $\tau_A \circ \tau_B = \tau_{A+B} \in \text{Tr}(E^2)$.

Dacă vom considera $B = -A$ (adică punctul de coordonate $(-x_A, -y_A)$), atunci $\tau_A \circ \tau_{-A} = \tau_{-A} \circ \tau_A = 1_{E^2}$, adică τ_A este aplicație bijectivă și $\tau_A^{-1} = \tau_{-A}$.

De asemenea, dacă $A(x_A, y_A)$ și alegem două puncte oarecare $P(x_P, y_P)$, $R(x_R, y_R)$ atunci :

$$\begin{aligned} d(\tau_A(P), \tau_A(R)) &= d(A+P, A+R) = \sqrt{(x_A + x_P - x_A - x_R)^2 + (y_A + y_P - y_A - y_R)^2} = \\ &= \sqrt{(x_P - x_R)^2 + (y_P - y_R)^2} = d(P, R), \text{ adică } \tau_A \text{ este o izometrie a lui } E^2. \end{aligned}$$

Din cele de mai sus deducem că $\text{Tr}(E^2) \leq \text{Izom}(E^2)$.

Pentru a proba că și $\text{Rot}(O, E^2) \leq \text{Izom}(E^2)$, să reamintim că o rotație a lui E^2 de unghi α (măsurat în radiani) în jurul lui O este o aplicație $\rho_\alpha : E^2 \rightarrow E^2$ definită astfel: dacă $P \in E^2$ are coordonatele $(r \cos \theta, r \sin \theta)$, atunci $\rho_\alpha(P)$ va fi punctul de coordonate $(r \cos(\theta + \alpha), r \sin(\theta + \alpha))$.

Se observă imediat că $\rho_\alpha \circ \rho_\beta = \rho_{\alpha + \beta}$ și că $\rho_0 = 1_{E^2}$, de unde deducem că $\rho_\alpha \circ \rho_{-\alpha} = \rho_{-\alpha} \circ \rho_\alpha = 1_{E^2}$, adică ρ_α este o bijecție și $(\rho_\alpha)^{-1} = \rho_{-\alpha}$.

Pentru a proba că ρ_α este izometrie, să considerăm $A_1(r_1 \cos \theta_1, r_1 \sin \theta_1)$, $A_2(r_2 \cos \theta_2, r_2 \sin \theta_2)$ și să calculăm:

$$\begin{aligned} d(\rho_\alpha(A_1), \rho_\alpha(A_2)) &= \\ &= \sqrt{[r_1 \cos(\theta_1 + \alpha) - r_2 \cos(\theta_2 + \alpha)]^2 + [r_1 \sin(\theta_1 + \alpha) - r_2 \sin(\theta_2 + \alpha)]^2} \\ &= \sqrt{r_1^2 + r_2^2 - 2r_1 r_2 \cos(\theta_1 - \theta_2)} = \\ &= \sqrt{[r_1 \cos(\theta_1) - r_2 \cos(\theta_2)]^2 + [r_1 \sin(\theta_1) - r_2 \sin(\theta_2)]^2} = d(A_1, A_2), \end{aligned}$$

de unde rezultă faptul că ρ_α este o izometrie. Din cele de mai sus rezultă că $\text{Rot}(O, E^2) \leq \text{Izom}(E^2)$.

(ii). Ne bazăm pe un rezultat cunoscut din geometrie și anume: o izometrie este unic determinată de imaginile a trei puncte necoliniare din E^2 . Fie acum $\varphi \in \text{Izom}(E^2)$; alegem un punct O ca origine și fie $A, B \in E^2$ distincte a.î. $O \notin AB$. Notăm $O' = \varphi(O)$, $A' = \varphi(A)$, $B' = \varphi(B)$ și considerăm translația $\tau = \tau_{O'}$ precum și $A'' = \tau(A)$, $B'' = \tau(B)$. Deoarece φ este o izometrie, deducem că triunghiurile $O'A'B'$ și $O'A''B''$ au laturile respectiv egale, deci unghiurile $A'O'A''$ și $B'O'B''$ sunt egale, astfel că triunghiul $O'A'B'$ este imaginea lui $O'A''B''$ printr-o rotație ρ în jurul lui O de unghi $A'O'A''$.

Deoarece imaginile punctelor necoliniare O, A, B prin izometriile φ și $\rho\tau$ coincid – ținând cont de observația de la început- deducem că $\varphi = \rho\tau$.

2.70. Fie $f, g \in S_X(Y)$, adică $f(Y) = g(Y) = Y$.

Atunci $(f \circ g^{-1})(Y) = f(g^{-1}(Y)) = f(Y) = Y$, adică $f \circ g^{-1} \in S_X(Y)$, deci $S_X(Y) \leq \text{Izom}(X)$.

2.71. Fie (C) cercul circumscris poligonului P_n de centru O, r raza sa iar A_1, A_2, \dots, A_n vârfurile poligonului; avem în mod evident $d(A_i, O) = r$, $(\forall) i = 1, 2, \dots, n$ și $d(A, O) < r$ pentru orice $A \in \overline{P}_n - \{A_1, \dots, A_n\}$.

Pentru o izometrie $\varphi \in D_n$ avem: $\varphi(\overline{P}_n) = \overline{P}_n$ și $d(\varphi(A_i), \varphi(O)) = r$, $i = 1, 2, \dots, n$ iar $d(\varphi(A), \varphi(O)) < r$, $(\forall) A \in \overline{P}_n - \{A_1, \dots, A_n\}$.

Rezultă imediat că $\varphi(O) = O$ și $\varphi(A_i) \in \{A_1, \dots, A_n\}$, $(\forall) i = 1, 2, \dots, n$.

De asemenea, se deduce imediat că ρ și ε din enunț sunt elemente ale D_n .

Obținem astfel $2n$ elemente distincte ale lui D_n : $1, \rho, \rho^2, \dots, \rho^{n-1}, \varepsilon, \rho\varepsilon, \rho^2\varepsilon, \dots, \rho^{n-1}\varepsilon$.

Să demonstrăm acum că D_n are cel mult $2n$ elemente (de unde va rezulta concluzia exercițiului).

Pentru aceasta, să observăm că pentru $\varphi \in D_n$, cum $\varphi(A_i) \in \{A_1, \dots, A_n\}$, $i = 1, 2, \dots, n$, pentru alegerea lui $\varphi(A_1)$ avem cel mult n posibilități și anume $\varphi(A_1) = A_i$, $i = 1, 2, \dots, n$. Dacă $\varphi(A_1)$ este definit, atunci $\varphi(A_2)$ are numai două posibilități și anume vârfurile adiacente ale lui A_1 .

În fine, ținând cont de observația de la rezolvarea problemei **2.69.**, izometria φ este unic determinată dacă definim $\varphi(A_1)$ și $\varphi(A_2)$ (deoarece $\varphi(O) = O$), deci $|D_n| \leq 2n$ și cum D_n are deja $2n$ elemente distincte, deducem că:

$$D_n = \{1, \rho, \rho^2, \dots, \rho^{n-1}, \varepsilon, \rho\varepsilon, \rho^2\varepsilon, \dots, \rho^{n-1}\varepsilon\}.$$

2.72. Se știe că orice permutare se scrie ca un produs de transpoziții.

Total rezultă acum din faptul că orice traspoziție (i, j) cu $1 < i < j$ se scrie sub forma: $(i, j) = \tau_{j-1} \dots \tau_{i+1} \tau_i \tau_{i+1} \dots \tau_{j-1}$.

2.73. Total rezultă din faptul că orice traspoziție (i, j) cu $1 < i < j$ se scrie sub forma: $(i, j) = \tau_i \tau_j \tau_i$.

2.74. Total rezultă din faptul că orice traspoziție (i, j) cu $1 < i < j$ se scrie sub forma: $(i, j) = (i, k)(j, k)(i, k)$.

2.75. Ținând cont de problema **2.72.** este suficient să demonstrăm că orice transpoziție $\tau_i = (i, i+1)$, $i \geq 2$ face parte din grupul generat de τ și σ .

Acest lucru rezultă din relațiile :

$$\sigma^{-1} \tau \sigma = (1, n), \sigma^{-2} \tau \sigma^2 = \sigma^{-1} (1, n) \sigma = (n-1, n) = \tau_{n-1}, \sigma^{-3} \tau \sigma^3 = \sigma^{-1} \tau_{n-1} \sigma = (n-2, n-1) = \tau_{n-2}, \dots, \sigma^{-(n-1)} \tau \sigma^{n-1} = \sigma^{-1} \tau_3 \sigma = (2, 3) = \tau_2, \text{ ținând cont că } \sigma^{-1} = (n, 1, 2, \dots, n-1).$$

2.76. Se știe că orice permutare pară este produsul unui număr par de transpoziții.

Dacă două transpoziții vecine (i,j) , (k,t) au proprietatea că $\{i,j\} \cap \{k,t\} = \emptyset$, atunci $(i,j)(k,t) = (i,k_j)(i,k,t)$, iar dacă $\{i,j\} \cap \{k,t\} \neq \emptyset$ (să presupunem că $i = k$) avem $(i,j)(i,t) = (i,t,j)$.

2.77. Conform problemei 2.73. orice permutare pară este un produs de transpoziții de forma $(1,i)$, $i = 2,3,\dots,n$. Deoarece $(1,i)(1,j) = (1,j,i)$, afirmația din enunț rezultă din egalitatea $(1,j,i) = (1,2,i)(1,2,i)(1,2,j)(1,2,i)$.

2.78. Cei r - cicluri sunt egali deoarece elementele $r+1, r+2, \dots, n$ sunt lăsate pe loc iar primele r sunt schimbate între ele de fiecare r -ciclu după aceeași regulă.

2.79. Dacă $\alpha = (i_1, i_2, \dots, i_r)$ este un ciclu de lungime r ($r \leq n$), atunci $\alpha^r = 1$ deoarece, de exemplu $\alpha(i_1) = i_2, \alpha^2(i_1) = i_3, \dots, \alpha^r(i_1) = i_1$, ș.a.m.d. iar din calcule se vede că r este cel mai mic număr natural cu proprietatea $\alpha^r = e$.

2.80. Fie $\alpha = (i_1, i_2, \dots, i_r)$, $\beta = (j_1, j_2, \dots, j_r)$.

Trebuie ca $\{i_1, i_2, \dots, i_r\} \cap \{j_1, j_2, \dots, j_r\} \neq \emptyset$. Cum $\alpha(i) \neq i \Rightarrow i \in \{i_1, i_2, \dots, i_r\}$ și analog $i \in \{j_1, j_2, \dots, j_r\}$. Deci putem presupune $i = i_1 = j_1$. Avem $\alpha(i) = \beta(i)$, $\alpha(i_2) = \alpha^2(i) = \beta(i_2)$ și analog $\alpha(i_t) = \beta(i_t)$ pentru $t = 2, 3, \dots, r$.

Fie acum $j \in \{1, 2, \dots, n\} - \{i_1, i_2, \dots, i_r\}$.

Atunci $\alpha(j) = j$, iar $j \notin \{j_1, j_2, \dots, j_r\}$, căci altfel j ar fi de forma $j = \beta^k(i) = \alpha^k(i) \in \{i_1, i_2, \dots, i_r\}$ ceea ce este fals.

Analog dacă $j \notin \{j_1, j_2, \dots, j_r\} \Rightarrow j \notin \{i_1, i_2, \dots, i_r\}$, adică $\{i_1, i_2, \dots, i_r\} = \{j_1, j_2, \dots, j_r\}$ și deci $\beta(j) = j = \alpha(j)$, adică $\alpha = \beta$.

2.81. " \Rightarrow ". Fie $\alpha = (i_1, i_2, \dots, i_r)$, $\beta = (j_1, j_2, \dots, j_r)$ disjuncte și să presupunem că $\{i_1, i_2, \dots, i_r\} \cap \{j_1, j_2, \dots, j_r\} \neq \emptyset$; să presupunem de exemplu că $i_1 = j_1$. Cum $\alpha(i_1) \neq i_1$ ar trebui ca $\beta(i_1) = i_1$ ceea ce este contradictoriu, căci $\beta(i_1) = \beta(j_1) \neq j_1 = i_1$.

" \Leftarrow ". Să presupunem că $\{i_1, i_2, \dots, i_r\} \cap \{j_1, j_2, \dots, j_r\} = \emptyset$, și fie x a.î. $\alpha(x) \neq x$, adică $x \in \{i_1, i_2, \dots, i_r\}$, deci x este de forma $x = i_k$ ($k \leq r$).

Atunci $\beta(x) = x$, căci dacă $\beta(x) \neq x$, atunci $x \in \{j_1, j_2, \dots, j_r\}$, adică $x \in \{i_1, i_2, \dots, i_r\} \cap \{j_1, j_2, \dots, j_r\} = \emptyset$, absurd. Analog, dacă $\beta(x) \neq x$, atunci $\alpha(x) = x$.

2.82. Fie $x \in \{1, 2, \dots, n\}$, $\alpha = (i_1, i_2, \dots, i_r)$, $\beta = (j_1, j_2, \dots, j_r)$, cu $\{i_1, i_2, \dots, i_r\} \cap \{j_1, j_2, \dots, j_r\} = \emptyset$. Să presupunem de exemplu că $x = j_1$; atunci $\beta(x) = j_2$ iar $\alpha(\beta(x)) = \alpha(j_2) = j_2$.

De asemenea, $\beta(\alpha(x)) = \beta(x) = j_2$, de unde deducem că $(\alpha\beta)(x) = (\beta\alpha)(x)$.

Dacă $x \notin \{j_1, j_2, \dots, j_r\}$, atunci $\alpha(x) \notin \{j_1, j_2, \dots, j_r\}$, deci $\alpha(\beta(x)) = \alpha(x)$ iar $\beta(\alpha(x)) = \alpha(x)$, adică și în acest caz $\alpha(\beta(x)) = \beta(\alpha(x))$.

2.83. Fie $\sigma \in S_n$.

Dacă σ este pară, considerăm:

$$\sigma_{n+1, n+2} = \begin{pmatrix} 1 & \dots & n & n+1 & n+2 \\ \sigma(1) & \dots & \sigma(n) & n+1 & n+2 \end{pmatrix}, \text{ care este evident în } A_{n+2}.$$

Dacă σ este impară, considerăm:

$$\sigma_{n+2, n+1} = \begin{pmatrix} 1 & \dots & n & n+1 & n+2 \\ \sigma(1) & \dots & \sigma(n) & n+2 & n+1 \end{pmatrix}, \text{ care face parte tot din } A_{n+2}.$$

Să notăm prin $f: S_n \rightarrow A_{n+2}$ asocierea de mai sus și să demonstrăm că f este morfism de grupuri (în mod evident f este aplicație injectivă).

Fie deci $\sigma, \tau \in S_n$; dacă σ, τ sunt pare, atunci și $\sigma \circ \tau$ este pară, astfel că:

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

$$f(\tau) = \begin{pmatrix} 1 & \dots & n & n+1 & n+2 \\ \tau(1) & \dots & \tau(n) & n+1 & n+2 \end{pmatrix}, \text{ deci:}$$

$$f(\sigma) \circ f(\tau) = \begin{pmatrix} 1 & \dots & n & n+1 & n+2 \\ \sigma(\tau(1)) & \dots & \sigma(\tau(n)) & n+1 & n+2 \end{pmatrix} = f(\sigma \circ \tau).$$

Analog se procedează în celelalte cazuri ținând cont de faptul că prin compunerea a două permutări de aceeași paritate obținem o permutare pară iar prin compunerea a două permutări de parități diferite obținem o permutare impară. Deoarece f este morfism injectiv de grupuri deducem că S_n poate fi privit ca subgrup al lui A_{n+2} .

2.84. Vom demonstra că dacă $\sigma \in Z(A_n)$ ($n \geq 4$), atunci $\sigma = e$.

Să presupunem prin absurd că $\sigma \neq e$, atunci $(\exists) i \in \{1, 2, \dots, n\}$ a.î. $\sigma(i) \neq i$ și fie $j = \sigma(i) \neq i$.

Cum $n \geq 4$, $(\exists) k, t \in \{1, 2, \dots, n\} - \{i, j\}$.

Dacă notăm $\sigma_{jkt} = (j, k, t)$, atunci $\sigma_{jkt} \in A_n$ și astfel ar trebui ca $\sigma \sigma_{jkt} = \sigma_{jkt} \sigma$.

Scriind că în i este adevărată ultima egalitate, deducem că $j = k$ – absurd și astfel deducem că $Z(A_n) = \{e\}$.

2.85. Vom demonstra că dacă $\sigma \in Z(S_n)$ ($n \geq 3$), atunci $\sigma = e$.

Să presupunem prin absurd că $\sigma \neq e$, atunci $(\exists) i \in \{1, 2, \dots, n\}$ a.î. $\sigma(i) \neq i$ și fie $j = \sigma(i) \neq i$.

Cum $n \geq 3$, $(\exists) k \in \{1, 2, \dots, n\} - \{i, j\}$.

Dacă notăm $\sigma_{jk} = (j,k)$, atunci $\sigma_{jk}\sigma \neq \sigma\sigma_{jk}$ deoarece $(\sigma_{jk}\sigma)(i) = k$ iar $(\sigma\sigma_{jk})(i) = j$. Acest lucru este contradictoriu rezultând astfel că $Z(S_n) = \{e\}$.

2.86. " \Leftarrow ". Să presupunem că σ, σ' au aceeași structură ciclică și să considerăm descompunerile lui σ, σ' ca produse de s cicluri disjuncți de lungimi n_1, n_2, \dots, n_s cu $1 \leq n_i < n$ și $n_1 + n_2 + \dots + n_s = n$:

$$\sigma = (a_{11}, a_{12}, \dots, a_{1n_1}) \dots (a_{s1}, a_{s2}, \dots, a_{sn_s})$$

$$\sigma' = (b_{11}, b_{12}, \dots, b_{1n_1}) \dots (b_{s1}, b_{s2}, \dots, b_{sn_s}).$$

Dacă vom considera permutarea:

$$\theta = \begin{pmatrix} a_{11} & \dots & a_{1n_1} & a_{21} & \dots & a_{2n_2} & \dots & a_{s1} & \dots & a_{sn_s} \\ b_{11} & \dots & b_{1n_1} & b_{21} & \dots & b_{2n_2} & \dots & b_{s1} & \dots & b_{sn_s} \end{pmatrix}$$

atunci prin calcul direct se arată că $\theta\sigma\theta^{-1} = \sigma'$, adică σ și σ' sunt conjugate în S_n .

" \Rightarrow ". Să presupunem că $\sigma, \sigma' \in S_n$ sunt conjugate în S_n , adică $(\exists) \theta \in S_n$ a.î. $\sigma' = \theta\sigma\theta^{-1}$.

Să presupunem că σ are structura ciclică descrisă mai sus. Deoarece prin calcul direct se arată că $\sigma'(b_{ij}) = \theta(a_{i,j+1}) = b_{i,j+1}$ pentru $1 \leq i \leq s$, $1 \leq j < n_i$ și $\sigma'(b_{in_i}) = \theta(a_{i1}) = b_{i1}$ deducem că și σ' are aceeași structură ciclică precum σ .

2.87. Permutarea $\begin{pmatrix} 1 & 2 & \dots & n-1 & n \\ 2 & 3 & \dots & n & 1 \end{pmatrix}$ are $n-1$ inversiuni, deci este pară

pentru n impar și impară pentru n par. Cum pentru orice $x \in S_n$, x^2 este pară, rezultă că pentru n par ecuația respectivă nu are soluție.

Fie acum $n = 2k+1$ cu $k \in \mathbb{N}^*$.

Pentru $k = 1, 2, 3$ se verifică prin calcul că soluțiile căutate sunt respectiv:

$$x = \begin{pmatrix} 1 & 2 & 2 \\ 3 & 1 & 2 \end{pmatrix}, x = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 1 & 2 & 3 \end{pmatrix}, x = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 5 & 6 & 7 & 1 & 2 & 3 & 3 \end{pmatrix}$$

În cazul general, vom demonstra că singura soluție a ecuației:

$$x^2 = \begin{pmatrix} 1 & 2 & \dots & 2k & 2k+1 \\ 2 & 3 & \dots & 2k+1 & 1 \end{pmatrix} \text{ este permutarea}$$

$$x = \begin{pmatrix} 1 & 2 & \dots & k-1 & k & k+1 & \dots & 2k+1 \\ k+2 & k+3 & \dots & 2k & 2k+1 & 1 & \dots & k+1 \end{pmatrix}$$

Fie $x(1) = a$. Dacă $a = 1$, atunci $x^2(1) = x(1) = 1 \neq 2$ – absurd.

De asemenea, din $x(1) = 2 \Rightarrow 2 = x(2)$ – absurd, deci $a > 2$.

Dacă $a > 2$, atunci $x(2) = x(x^2(1)) = x^2(x(1)) = x^2(a) = a+1$ și prin inducție după j și t se arată că $x(j) = a+j-1$ pentru $j = 1, 2, \dots, 2k+2-a$ și $x(2k+2-a+t) = t$ pentru $t = 1, 2, \dots, a-1$.

$$\text{Deci } x = \begin{pmatrix} 1 & 2 & \dots & 2k+2-a & 2k+3-a & \dots & 2k+1 \\ a & a+1 & \dots & 2k+1 & 1 & \dots & a-1 \end{pmatrix}$$

Deoarece $x(a) = x^2(1) = 2 \Rightarrow 2k+4-a = a \Rightarrow a = k+2$, de unde rezultă forma lui x pe care am amintit-o mai sus.

2.88. (i). Fie $\sigma = (i_0, \sigma(i_0), \dots, \sigma^{m-1}(i_0))$ un ciclu de lungime m , cu $p \nmid m$. Se observă imediat că:

$$\sigma^p = (i_0, \sigma^p(i_0), \sigma^{2p}(i_0), \dots, \sigma^{(m-1)p}(i_0)).$$

Deoarece $(m,p) = 1$, resturile pe care le dau la împărțirea cu m numerele $0, p, 2p, \dots, (m-1)p$ sunt toate numerele $0, 1, 2, \dots, m-1$ (eventual într-o altă ordine). Deducem că σ^p este un ciclu de lungime m . Cum $\sigma^m = (1) = e$ deducem că $\{i_0, \sigma(i_0), \dots, \sigma^{m-1}(i_0)\} = \{i_0, \sigma^p(i_0), \dots, \sigma^{p(m-1)}(i_0)\}$, adică σ și σ^p au aceeași orbită.

(ii). Fie $m = kp$ iar $\sigma = (i_0, \sigma(i_0), \dots, \sigma^{m-1}(i_0))$ un ciclu de lungime m .

Ținând cont de egalitățile $i_0 = \sigma^{kp}(i_0), \sigma(i_0) = \sigma^{kp+1}(i_0), \dots, \sigma^{p-1}(i_0) = \sigma^{kp+p-1}(i_0)$, deducem că $\sigma^p = (i_0, \sigma^p(i_0), \dots, \sigma^{(k-1)p}(i_0)) \cdot (\sigma(i_0), \sigma^{1+p}(i_0), \dots, \sigma^{1+(k-1)p}(i_0)) \dots (\sigma^{p-1}(i_0), \dots, \sigma^{p-1+p}(i_0), \dots, \sigma^{p-1+(k-1)p}(i_0))$, adică σ^p este un produs de p cicluri disjuncți, fiecare având lungimea $k = m/p$.

2.89. (i). Fie σ un ciclu de lungime m , unde $(m,p) = 1$. Atunci există $q \in \{1, 2, \dots, m-1\}$ a.î. $pq \equiv 1 \pmod{m}$. Dacă notăm $\tau = \sigma^q$, atunci din $pq \equiv 1 \pmod{m}$ deducem că $(q,m) = 1$ și atunci, conform exercițiului precedent va rezulta că $\sigma^p = \tau$ este un ciclu de lungime m și în plus $\tau^p = \sigma^{pq} = \sigma$ (deoarece $\sigma^m = e$).

(ii). Fie cicluri disjuncți de lungime k :

$$\sigma_1 = (i_0^1, i_1^1, \dots, i_{k-1}^1)$$

.....

$$\sigma_p = (i_0^p, i_1^p, \dots, i_{k-1}^p)$$

Considerând atunci următorul ciclu de lungime kp :

$$\tau = (i_0^1, \dots, i_0^p, i_1^1, \dots, i_1^p, \dots, i_{k-1}^1, \dots, i_{k-1}^p)$$
 se constată imediat că

$$\tau = \sigma_1 \cdot \sigma_2 \dots \sigma_p.$$

2.90. " \Rightarrow ". Să presupunem că ecuația $x^p = \sigma$ are o soluție $x \in S_n$. Considerăm descompunerea lui x în cicluri disjuncți $x = x_1 x_2 \dots x_t$.

Să presupunem că dintre aceștia x_1, x_2, \dots, x_i au lungimi divizibile cu p^2 , x_{i+1}, \dots, x_j au lungimi divizibile cu p dar nu cu p^2 , iar x_{j+1}, \dots, x_t au lungimi nedivizibile cu p .

$$\text{Astfel, } \sigma = x^p = (x_1^p \dots x_i^p)(x_{i+1}^p \dots x_j^p)(x_{j+1}^p \dots x_t^p) \quad (1).$$

Conform problemei anterioare, puterile x_{j+1}^p, \dots, x_i^p sunt cicluri de lungimi egale respectiv cu lungimile ciclurilor x_{j+1}, \dots, x_i , deci nedivizibile cu p . De asemenea orbitele lor sunt respectiv egale, ceea ce ne arată că x_{j+1}^p, \dots, x_i^p sunt cicluri disjuncte.

Tot din aceeași problemă deducem că fiecare din puterile x_{i+1}^p, \dots, x_j^p este un produs de p -cicluri disjuncte de lungimi care nu se mai divid cu p și acești cicluri rămân disjuncte în totalitatea lor (au orbitele incluse în orbitele ciclurilor x_{i+1}, \dots, x_j).

De asemenea, fiecare din puterile x_1^p, \dots, x_i^p este un produs de p -cicluri disjuncte de lungimi divizibile cu p și în totalitatea lor cicluri care apar rămân disjuncte.

Să presupunem că descompunerile acestor puteri sunt :

$$x_1^p = x_{11} \cdot x_{12} \dots x_{1p}$$

.....

$$x_i^p = x_{i1} \cdot x_{i2} \dots x_{ip}$$

Ținând cont de cele de mai înainte, deducem că cicluri care au lungimi divizibile cu p sunt $x_{11}, \dots, x_{1p}, x_{21}, \dots, x_{2p}, \dots, x_{i1}, \dots, x_{ip}$ și numai aceștia; câte p dintre aceștia (și anume exact în ordinea în care sunt scriși mai înainte) au aceeași lungime.

Deducem astfel că dacă fixăm o lungime divizibilă cu p de la cicluri din descompunerea lui σ , să zicem m_s , numărul α_s al ciclurilor de lungime m_s este un multiplu de p ($s = 1, 2, \dots, k$).

" \Leftarrow ". Să presupunem că toate numerele $\alpha_1, \alpha_2, \dots, \alpha_k$ sunt divizibile cu p . Atunci cei α_1 cicluri de lungime m_1 (m_1 divizibil cu p) pot fi împărțiți în grupe de câte p cicluri și conform ex. anterior produsul ciclurilor dintr-o asemenea grupă este puterea p a unui alt ciclu (a căru orbită este reuniunea orbitelor celor p cicluri). Deducem astfel că produsul celor α_1 cicluri de lungime m_1 este un produs de puteri de p -cicluri disjuncte. Analog pentru produsul celor α_2 cicluri de lungime m_2 , ș.a.m.d. până la produsul celor α_k cicluri de lungime m_k (m_1, \dots, m_k fiind numerele divizibile cu p).

Considerăm acum și cicluri de lungime m_{k+1}, \dots, m_t (lungimi nedivizibile prin p), tot conform problemei precedente, fiecare asemenea ciclu este puterea p a unui ciclu având aceeași orbită.

Astfel, dacă notăm cu x produsul tuturor acestor noi cicluri puși în evidență obținem că $\sigma = x^p$, deci ecuația considerată are soluție în grupul S_n .

Să rezolvăm acum aplicațiile din enunț.

Pentru prima aplicație, să notăm prin σ permutarea din dreapta. Avem următoarea descompunere a lui σ în produs de cicluri disjuncte:

$$\sigma = (1\ 5)(2\ 6)(3\ 7)(10\ 9)(4\ 8\ 11\ 13)(14\ 15\ 17\ 18)(9\ 12\ 16).$$

În cazul acestei probleme avem $p = 2$ iar numărul ciclilor de lungimi divizibile prin 2 sunt cei de lungime 2 și 4. Avem $\alpha_1=4$, $\alpha_2=2$ și cum ambele numere sunt divizibile prin 2 deducem că ecuația considerată are soluție în S_{10} .

Pentru a doua ecuație, notând tot cu σ permutarea din partea dreaptă avem că $\sigma = (1\ 3\ 5)(4\ 9\ 10)(2\ 6\ 7\ 8)$. Avem $p = 3$ iar ciclul de lungime 3 sunt în număr de $\alpha_1=2$ care nefiind multiplu de 3, deducem conform celor stabilite mai înainte că a doua ecuație nu are soluție în S_{10} .

2.91. Oricum am considera o permutare $\sigma \in S_n$, $\sigma \neq e$, aceasta nu poate avea în descompunerea sa ciclul de lungime divizibilă cu p (câci $p > n$).

Deci numărul ciclilor de lungime divizibilă cu p este 0 și cum 0 este multiplu de p , totul rezultă acum din problema precedentă.

2.92. " \Rightarrow ". Fie $x \in S_n$, $x \neq e$, o soluție a ecuației $x^p = e$ și fie $x = x_1 x_2 \dots x_t$ descompunerea sa în ciclul disjuncti. Vom demonstra că x_1, \dots, x_t au, fiecare dintre ei, lungimea p .

Deoarece x_1, \dots, x_t sunt disjuncti, rezultă că acești ciclul, ca și puterile lor comută. Atunci egalitatea $x^p = e$ se scrie $x_1^p x_2^p \dots x_t^p = e$. Să demonstrăm că de aici deducem $x_1^p = x_2^p = \dots = x_t^p = e$.

Într-adevăr, dacă prin absurd $(\exists) i \in \{1, 2, \dots, t\}$ a.î. $x_i^p \neq e$, atunci $(\exists) a \in \{1, 2, \dots, t\}$ cu $x_i^p(a) \neq a$ și atunci a aparține orbitei ciclului x_i .

Deoarece astfel a nu va face parte din orbitele ciclilor disjuncti $x_1, \dots, x_{i-1}, x_{i+1}, \dots, x_t$ deducem că: $x_1^p(a) = \dots = x_{i-1}^p(a) = x_{i+1}^p(a) = \dots = x_t^p(a) = a$.

Deoarece $a = e(a) = (x_1^p x_2^p \dots x_t^p)(a) = x_i^p(a) \neq a$ rezultă contradicția $a \neq a$.

De asemenea, din cele de mai înainte deducem că ordinele permutărilor x_1, x_2, \dots, x_t în grupul S_n sunt divizori ai lui p și cum p este prim deducem că $o(x_1) = \dots = o(x_t) = p$.

Cum ordinul unui ciclu este egal cu lungimea ciclului respectiv, deducem că x_1, \dots, x_t sunt ciclul de lungime p .

" \Leftarrow ". Această implicație este evidentă deoarece orice ciclu de lungime p are ordinul p în grupul S_n , deci este o soluție a ecuației $x^p = e$.

2.93. Facem inducție după n .

Dacă $n = 1$, atunci G este ciclic și cum orice subgrup al unui grup ciclic este ciclic, totul este clar.

Presupunem acum că $G = \langle \{x_1, x_2, \dots, x_n\} \rangle$ și $H \leq G$.

Alegem $y = x_1^{m_1} x_2^{m_2} \dots x_n^{m_n}$ a.î. m_1 ia cea mai mică valoare nenulă pozitivă (dacă m_1 este negativ schimbăm rolul lui y cu y^{-1}).

Dacă x_1 nu apare la un exponent nenul în orice element al lui H , atunci $\langle \{x_2, x_3, \dots, x_n\} \rangle$ conține pe H și totul rezultă din ipoteza de inducție.

Astfel, pentru orice $z = x_1^{l_1} x_2^{l_2} \dots x_n^{l_n}$ din H putem alege $q, r \in \mathbb{Z}$ cu $0 \leq r < m_1$ și $l_1 = qm_1 + r$. Puterea la care apare x_1 în $z^{y^{-q}} \in H$ este r și ținând cont de alegerea lui m_1 deducem că $r = 0$.

Deci $H = \langle y, K \rangle$, unde $K = H \cap \langle \{x_2, x_3, \dots, x_n\} \rangle$ și conform ipotezei de inducție K este generat de o mulțime de cel mult $n-1$ elemente și acum totul este clar.

2.94. Fie M o mulțime de generatori ai grupului $(\mathbb{Q}, +)$ și $\alpha \in M$ a.î. $H = \langle M \setminus \{\alpha\} \rangle \subsetneq \mathbb{Q}$. Pentru $x \in H$, $(\exists) a, b \in \mathbb{Z}$ a.î. $a\alpha = bx$, $a \neq 0$.

Deoarece $\frac{1}{a} \cdot \alpha \in H$ și $\langle M \rangle = \mathbb{Q}$ putem scrie $\frac{1}{a} \cdot \alpha = c\alpha + y$ cu $c \in \mathbb{Z}$, $y \in H$. Rezultă că $\alpha = ac\alpha + ay = c(bx) + ay \in H$ ceea ce contrazice alegerea lui α .

2.95. După cum am arătat în soluția problemei **2.48.** avem $\mathbb{Q} = \bigcup_{m \geq 1} H_m$

unde $H_m = \langle \frac{1}{m!} \rangle$ și evident $H_{m-1} \leq H_m$, $(\forall) m \geq 1$.

Fie deci $X = \{x_1, x_2, \dots, x_n\}$ o mulțime nevidă a lui \mathbb{Q} .

Pentru orice $i = 1, 2, \dots, n$ $(\exists) m_i \in \mathbb{N}$ a.î. $x_i \in H_{m_i}$. Alegând $m = \max_{1 \leq i \leq n} m_i$

avem că $H_{m_i} \subseteq H_m$, $(\forall) i = 1, 2, \dots, n$ deci $X \subseteq H_m \Rightarrow \langle X \rangle \leq H_m$ și cum H_m este ciclic rezultă că și $\langle X \rangle$ este ciclic.

§3. Teorema lui Lagrange. Ordinul unui element. Indicele unui subgrup. Subgrupuri normale.

3.1. Din $|Z(G)| > \frac{1}{2}|G| \Rightarrow |G| < 2|Z(G)|$. Însă conform teoremei lui

Lagrange $|Z(G)|$ divide $|G|$ (căci $Z(G) \leq G$), adică $|G| = n \cdot |Z(G)|$ cu $n \in \mathbb{N}^*$, $n \geq 1$. Deci $n \cdot |Z(G)| < 2 \cdot |Z(G)| \Rightarrow n < 2$, adică $n = 1 \Rightarrow |G| = |Z(G)| \Rightarrow G$ este comutativ.

3.2. Fie $H = \{x \in G : x^2 = 1\}$. Cum G este comutativ, dacă $x, y \in H \Rightarrow x^2 = y^2 = 1 \Rightarrow (xy^{-1})^2 = x^2 y^{-2} = 1$, adică $xy^{-1} \in H$, deci $H \leq G$.

Conform problemei anterioare, punând în locul lui $Z(G)$ pe H , obținem că $|H| = |G|$, deci $H = G$, și de aici $x^2 = 1$, $(\forall) x \in G$.

3.3. Să presupunem că mulțimea $T = \{a_1, \dots, a_r\}$ a elementelor de ordin 2 are mai mult de n elemente, deci $r > n$ (atunci $r \geq n+1$). Pentru $a_i, a_j \in T$, $i \neq j$

rezultă că $a_i a_j \in G \setminus T$. Într-adevăr, dacă $a_i a_j \in T$ atunci $H = \{e, a_i, a_j, a_i a_j\}$ ar fi un subgrup în G , deci $4 \mid 2n$ (conform teoremei lui Lagrange) adică n este par, ceea ce este absurd.

În plus, $a_i a_j \neq 1$ (\forall) $i \neq j$. Din cele demonstrate rezultă că elementele $a_1 a_2, a_1 a_3, \dots, a_1 a_r$ se află în $G \setminus (T \cup \{1\})$ al cărui cardinal este $2n - r - 1 < 2n - n - 1 \Rightarrow n - 1 < r - 1$, adică există $i \neq j$ a.î. $a_i a_i = a_i a_j \Rightarrow a_i = a_j$ - absurd. Deci $r \leq n$.

Observație. Maximul se poate atinge efectiv, de exemplu în cazul grupului diedral D_n cu $2n$ elemente.

3.4. Fie $o(x) = k$ și $H = \{1, x, x^2, \dots, x^{k-1}\} \leq G$. Cum $x^n \in H$, deci $o(x^n)$ divide $|H| = k = o(x)$.

3.5. Fie $\text{ord } G = n$ și $d = \text{c.m.m.d.c}$ al ordenelor elementelor din G diferite de 1. Evident $d \mid n$. Fie $d = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \dots p_r^{\alpha_r}$. Atunci există elementele x_1, x_2, \dots, x_r a.î. $p_i^{\alpha_i} \mid o(x_i) \Leftrightarrow o(x_i) = p_i^{\alpha_i} \cdot t_i$. Se verifică ușor că $x = x_1^{t_1} x_2^{t_2} \dots x_r^{t_r}$ are ordinul d .

3.6. Putem scrie $k = mm_1 = nn_1$ cu $m_1, n_1 \in \mathbb{N}$. Atunci $(xy)^k = x^k y^k = (x^m)^{m_1} (y^n)^{n_1} = 1^{m_1} \cdot 1^{n_1} = 1$.

La cealaltă întrebare răspunsul este afirmativ căci dacă vom considera $y = x^{-1}$, atunci $xy = 1$, deci $o(xy) = 1$.

3.7. Deoarece $x^{-1}(xy)x = yx$, deducem că (\forall) $n \in \mathbb{N}$, $x^{-1}(xy)^n x = (yx)^n$, deci $(xy)^n = 1 \Leftrightarrow (yx)^n = 1$ de unde deducem că $o(xy) = o(yx)$.

Faptul că $o(x) = o(x^{-1})$ rezultă din echivalența $x^k = 1 \Leftrightarrow x^{-k} = 1$, (\forall) $k \in \mathbb{N}$.

3.8. Fie $k = o(x^m)$ iar $d = (m, n)$. Putem scrie $m = dm'$, $n = dn'$ cu $m', n' \in \mathbb{N}$ și $(m', n') = 1$ iar $mm' = nn' = dm'n'$.

Cum $n = o(x)$, avem $(x^m)^{n'} = (x^n)^{m'} = 1$, adică $o(x^m) = k \mid n'$.

Pe de altă parte, $x^{mk} = (x^m)^k = 1 \Rightarrow n = o(x) \mid mk \Rightarrow n' \mid m'k$ și cum $(m', n') = 1 \Rightarrow n' \mid k$.

Am obținut astfel că $n' \mid k$ și $k \mid n' \Rightarrow o(x^m) = k = n' = n/d = n/(m, n)$.

3.9. Avem $(xy)^{n^2} = x^{n^2} \cdot y^{n^2} = (x^n)^{n^2} \cdot (y^n)^{n^2} = 1$.

Fie acum $n \in \mathbb{N}$ a.î. $(xy)^n = 1$; atunci $x^n = y^{-n}$ și $x^{n^2} = (y^n)^{-n} = 1 \Rightarrow$

$n_1 \mid n_2$ și cum $(n_1, n_2) = 1 \Rightarrow n_1 \mid n$. Analog se demonstrează că $n_2 \mid n$, deci $n_1 n_2 \mid n$. Prin urmare avem echivalența $(xy)^n = 1 \Leftrightarrow n_1 n_2 \mid n$, deci $o(xy) = n_1 n_2 = o(x) \cdot o(y)$.

Să presupunem că $\langle x \rangle \cap \langle y \rangle = \{1\}$ și fie $n = [n_1, n_2]$. În mod evident $(xy)^n = 1$, adică $o(xy) \mid n$. Fie acum $k \in \mathbb{N}^*$ a.î. $(xy)^k = 1$. Atunci $x^k y^k = 1$, deci $x^k = y^{-k} \in \langle x \rangle \cap \langle y \rangle$, adică $x^k = y^{-k} = 1$, de unde $n_1 \mid k$ și $n_2 \mid k$, deci $n \mid k$, ceea ce arată că $o(xy) = n$.

3.10. Să probăm la început existența lui y și z . Din $(n_1, n_2) = 1 \Rightarrow (\exists) \alpha, \beta \in \mathbb{Z}$ a.î. $\alpha n_1 + \beta n_2 = 1$.

Astfel, dacă $x \in G$, $x = x^1 = x^{\alpha n_1 + \beta n_2} = x^{\alpha n_1} \cdot x^{\beta n_2}$

Alegem $y = x^{\beta n_2}$ iar $z = x^{\alpha n_1}$. Conform problemei 3.8., $o(y) = o(x^{\beta n_2}) = o(x) / (n_1 n_2, \beta n_2) = (n_1 n_2) / n_2 = n_1$ și analog deducem că $o(z) = n_2$.

Să probăm acum unicitatea scrierii lui x ; dacă $x = y_1 z_1 = z_1 y_1$ cu $o(y_1) = n_1$ și $o(z_1) = n_2$, atunci $x = yz = y_1 z_1 \Rightarrow y_1^{-1} y = z_1 z^{-1} \Rightarrow (y_1^{-1} y)^{n_1} = 1$ și $(y_1^{-1} y)^{n_2} = (z_1 z^{-1})^{n_1} = 1 \Rightarrow (y_1^{-1} y)^{\alpha n_1 + \beta n_2} = [(y_1^{-1} y)^{n_1}]^\alpha \cdot [(y_1^{-1} y)^{n_2}]^\beta = 1 \Rightarrow y = y_1$ și analog $z = z_1$.

3.11. Deoarece x comută cu $[x, y] = x^{-1}(y^{-1}xy)$ deducem că:

$[x, y]^m = x^{-m}(y^{-1}xy)^m = x^{-m}y^{-1}x^m y = [x^m, y] = [1, y] = 1$ și analog $[x, y]^n = 1$.

Deoarece $d = (m, n)$, $(\exists) u, v \in \mathbb{Z}$ a.î. $d = mu + nv$ și astfel

$[x, y]^d = [x, y]^{mu} \cdot [x, y]^{nv} = 1^u \cdot 1^v = 1$.

3.12. (i). \Rightarrow (ii). Fie $f : G \rightarrow G$, $f(x) = x^2$, $(\forall) x \in G$. Atunci f este injectivă ($x^2 = y^2 \Rightarrow (xy^{-1})^2 = 1 \Rightarrow xy^{-1} = 1 \Rightarrow x = y$ căci în caz contrar, conform teoremei lui Lagrange, ar trebui ca $2 \mid |G|$ - absurd) și cum (G, \cdot) este grup finit, se obține că f este bijecție, de unde ecuația $x^2 = a$ are o unică soluție $x_0 \in G$, pentru orice $a \in G$.

(ii) \Rightarrow (i). Evident, căci există un singur element $x \in G$ astfel încât $x^2 = 1$, și anume $x = 1$. Restul se dispun în perechi de forma (x, x^{-1}) , unde $x \neq x^{-1}$ (căci dacă $x = x^{-1} \Rightarrow x^2 = 1$). Așadar $\text{ord}(G) = 2k+1$, $k \in \mathbb{N}^*$.

3.13. $x = 1$ este o soluție comună a celor două ecuații.

" \Leftarrow ". Dacă $(m, n) = 1 \Rightarrow (\exists) u, v \in \mathbb{Z}$ a.î. $mu + nv = 1$. Dacă x_0 este o soluție comună a celor două ecuații avem $x_0^{mu} = 1$ și $x_0^{nv} = 1 \Rightarrow x_0 = x_0^{mu+nv} = 1$.

" \Rightarrow ". Dacă $d = (m, n)$, există $a, b \in \mathbb{Z}$ a.î. $ma + nb = d$. Atunci soluția comună x_0 a celor două ecuații va fi soluție și a ecuației $x^d = 1$ și reciproc.

Într-adevăr : $x_0^m = x_0^n = 1 \Rightarrow x_0^d = x_0^{ma+nb} = 1$. Reciproca este evident adevărată.

Dacă $d \geq 2 \Rightarrow d$ are cel mult un divizor prim p . Atunci orice element de ordin p din G este soluție a ecuației $x^d = 1$. Cum există astfel de elemente în G (conform teoremei lui Cauchy, vezi problema 4.74.) rezultă că ecuația $x^d = 1$ nu are soluție unică, contradicție cu ipoteza în cazul $d \geq 2$. În concluzie, rămâne doar cazul $d = 1$.

3.14. Presupunem că G este abelian, atunci $ab = ba$. Considerăm $H = \{1, a, b, ab\}$. Deoarece G este presupus abelian, $a^2 = b^2 = (ab)^2 = 1$, $a \cdot (ab) = a^2b = b$, $b \cdot (ab) = ab^2 = a$, și astfel H este subgrup în G . Din teorema lui Lagrange avem $|H| \mid |G|$, contradicție căci $|H| = 4$ și $|G| = 10$.

3.15. Se verifică imediat prin calcul că $A^4 = B^3 = I_2$ iar prin inducție matematică după n se demonstrează că $(AB)^n = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} \neq I_2$, $(\forall) n \in \mathbb{N}^*$, de unde deducem că $o(AB) = \infty$.

3.16. Din $(m, n) = 1 \Rightarrow (\exists) \alpha, \beta \in \mathbb{Z}$ a.î. $\alpha m + \beta n = 1$. Atunci, ținând cont de faptul că $x^n = 1$, deducem că $x = x^{\alpha m + \beta n} = x^{\alpha m} = (x^m)^\alpha \in H$.

3.17. Scriem $\prod_{x \in G} x = \left(\prod_{\substack{x \in G \\ o(x) > 2}} x \right) \cdot \left(\prod_{\substack{x \in G \\ o(x) \leq 2}} x \right)$ și vom demonstra că $\prod_{\substack{x \in G \\ o(x) > 2}} x = 1$ (*).

Dacă $x \in G$ cu $o(x) > 2$, atunci $o(x) = o(x^{-1}) > 2$. Dar $x \neq x^{-1}$, căci în caz contrar ar rezulta că $x^2 = 1$.

Astfel în produsul (*) dacă apare un factor x , atunci apare și factorul x^{-1} , deci în produsul (*) factorii se grupează doi câte doi (fiecare cu inversul său), de unde rezultă că produsul (*) este 1, deci $\prod_{x \in G} x = \prod_{\substack{x \in G \\ o(x) \leq 2}} x$.

Pentru a demonstra teorema lui Wilson, se ține cont de faptul că singurele elemente din \mathbb{Z}_p^* de ordin ≤ 2 (p prim) sunt $\hat{1}$ și $\hat{p-1} = -\hat{1}$, deci conform celor de mai înainte $\hat{1} \cdot \hat{2} \cdot \dots \cdot \hat{p-1} = -\hat{1} \Rightarrow p \mid (p-1)! + 1$.

3.18. Fie p prim și $n \in \mathbb{N}$, $n \geq 2$.

Avem că $U(\mathbb{Z}_{p^n}^*, \cdot) = \{ \hat{a} \in \mathbb{Z}_{p^n}^* \mid (a, p) = 1 \}$. Să determinăm în acest grup elementele $\hat{a} \in U(\mathbb{Z}_{p^n}^*, \cdot)$ a.î. $\hat{a}^2 = \hat{1}$, adică acele numere naturale a a.î. $1 \leq a < p^n$ cu $(a, p) = 1$ și $p^n \mid a^2 - 1$ (*).

Evident $a = 1$ verifică condițiile de mai sus. Dacă $a > 1$, atunci putem scrie $a - 1 = p^k u$ și $a + 1 = p^t v$ cu $k, t \geq 0$, $(p, u) = (p, v) = 1$ iar $k + t \geq n$. Dacă $k = 0 \Rightarrow t \geq n \Rightarrow p^n | a+1$ și cum $a < p^n \Rightarrow a+1 = p^n \Rightarrow a = p^n - 1$ și astfel obținem

și elementul $\hat{a} = \widehat{p^n - 1} = -\hat{1}$ ce verifică condițiile (*).

Dacă $t = 0 \Rightarrow k > n \Rightarrow p^n | a-1$ și cum $a < p^n \Rightarrow a-1 = 0 \Rightarrow a = 1$, contradicție!

Dacă $k \neq 0, t \neq 0 \Rightarrow 2 = p^t v - p^k u \Rightarrow p | 2$; pentru $p > 2$ obținem o contradicție.

Deci, dacă $p > 2$ atunci în $U(\mathbb{Z}_{p^n}^*, \cdot)$ avem numai elementele $-\hat{1} = \widehat{p^n - 1}$

și $\hat{1}$ care au ordinul cel mult 2, obținând astfel concluzia cerută de la (ii).

Dacă $p = 2$, atunci din $2 = 2^t v - 2^k u \Rightarrow t = 1$ sau $k = 1$. Dacă $t = 1 \Rightarrow k \geq n-1 \Rightarrow a-1 = 2^k u \geq 2^{n-1} u$ și cum $1 < a < 2^n \Rightarrow u = 1$ și $k = n-1$. Deci în acest caz, dacă a verifică condițiile (*) $\Rightarrow a = 2^{n-1} + 1$.

Dacă $k = 1 \Rightarrow t \geq n-1 \Rightarrow a + 1 = 2^t v \geq 2^{n-1} v$ și cum $1 < a < 2^n \Rightarrow v = 1$ sau $v = 2$ (cazul $v = 2$ este exclus deoarece $(v, 2) = 1$).

Dacă $v = 1 \Rightarrow t = n-1$ sau $t = n$. În cazul $t = n-1 \Rightarrow a = 2^{n-1} - 1$ iar $t = n \Rightarrow a = 2^n - 1$.

În concluzie: dacă $p = 2$ și $n > 2$ în $U(\mathbb{Z}_{2^n}^*, \cdot)$ numai elementele $-\hat{1}, \hat{1}, \widehat{2^{n-1} - 1}$ și $\widehat{2^{n-1} + 1}$ au ordinul cel mult 2, obținând concluzia cerută de (i).

Acum, concluziile cerute de (iii) (varianta de generalizare a teoremei lui Wilson) rezultă ținând cont de (i), (ii) și de problema 3.17.

3.19. (i). Să notăm $H_n = U_{p^n}$ și $y_n = \cos \frac{2\pi}{p^n} + i \sin \frac{2\pi}{p^n}$, $n \in \mathbb{N}$.

Dacă $z \in H_n \Rightarrow z^{p^n} = 1 \Rightarrow z^{p^{n+1}} = (z^{p^n})^p = 1^p = 1 \Rightarrow z \in H_{n+1} \Rightarrow H_n \subset H_{n+1}$ (această incluziune este strictă deoarece $y_{n+1} \in H_{n+1}$ și cum $y_{n+1} = \cos \frac{2\pi}{p} + i \sin \frac{2\pi}{p} \neq 1 \Rightarrow y_{n+1} \notin H_n$).

(ii). Rezultă imediat din (i).

(iii). Fie $H \leq U_{p^\infty}$, $H \neq U_{p^\infty}$ și n cel mai mic număr natural pentru care $y_n \in H$ și $y_{n+1} \notin H$. Vom demonstra că $H = H_n$.

Incluziunea $H_n \subseteq H$ este evidentă (deoarece $H_n = \langle y_n \rangle$ iar $y_n \in H$).

Fie $z \in H \subset U_{p^\infty} \Rightarrow (\exists) m \in \mathbb{N}$ a.î. $z \in H_m \Rightarrow o(z) | p^m \Rightarrow o(z) = p^r$ cu

$0 \leq r \leq m$. Deci z este o rădăcină de ordin r a unității $\Rightarrow z = y_r^k$ cu $(k, p^r) = 1$.

Dacă $a, b \in \mathbb{Z}$ a.î. $ak + bp^r = 1 \Rightarrow y_r = y_r^{ak+bp^r} = (y_r^k)^a = z^a \in H \Rightarrow r \leq n$ și cum $H_r \subset H_n \Rightarrow z \in H_n \Rightarrow H \subseteq H_n \Rightarrow H = H_n$.

3.20. Dacă $M, N \in GL_n(A)$, atunci $\det(M), \det(N) \in U(A^*, \cdot)$ și cum $\det(MN) = \det(M) \cdot \det(N) \Rightarrow MN \in GL_n(A)$.

Evident $I_n \in GL_n(A)$ iar dacă $M \in GL_n(A)$, cum $\det(M^{-1}) = (\det(M))^{-1}$ deducem că $M^{-1} \in U(A^*, \cdot)$, adică $M^{-1} \in GL_n(A)$.

Rezultă astfel că $(GL_n(A), \cdot)$ este grup.

Dacă $M, N \in SL_n(A)$, atunci $\det(M) = \det(N) = 1$ și deoarece $\det(MN^{-1}) = \det(M) \cdot (\det(N))^{-1} = 1 \cdot 1^{-1} = 1$ deducem că $MN^{-1} \in S_n(A)$, adică $SL_n(A) \trianglelefteq GL_n(A)$.

3.21. Dacă V este un K - spațiu vectorial de dimensiune n , atunci $|V| = q^n$ și se observă imediat că $|GL_n(K)|$ este egal cu numărul sistemelor ordonate (e_1, e_2, \dots, e_n) de elemente ale lui V ce constituie baze ale lui V peste K .

Însă pentru a alege o bază a lui V peste K , putem alege mai întâi pe e_1 ca fiind orice element al lui V (avem $q^n - 1$ posibilități), apoi pe e_2 ca fiind orice element al lui V care nu este de forma ae_1 , cu $a \in K$ (și avem $q^n - q$ posibilități); apoi pe e_3 ca fiind orice element din V care nu este de forma $a_1e_1 + a_2e_2$ cu $a_1, a_2 \in K$ (și avem $q^n - q^2$ posibilități), e.t.c.

În concluzie $|GL_n(K)| = (q^n - 1)(q^n - q) \dots (q^n - q^{n-1})$.

3.22. Cum $\det(U) = \det(V) = 1 \Rightarrow U, V \in SL_2(\mathbb{Z})$.

Prin calcul se verifică relațiile:

$$U^{-1} = \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}, \quad V^{-1} = \begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix}, \quad U^k = \begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix}, \quad V^k = \begin{pmatrix} 1 & 0 \\ k & 1 \end{pmatrix}, \quad (\forall) k \in \mathbb{Z}$$

precum și egalitatea:

$$(*) \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = U^{-1} V^2 U^{-1} V^2.$$

Fie acum $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$ (deci $ad - bc = 1$).

Vom demonstra prin inducție matematică asupra lui $|c|$ că M poate fi scrisă sub forma $M = T_1^{k_1} \dots T_n^{k_n}$, cu $T_i \in \{U, V\}$, $k_i \in \mathbb{Z}$, $1 \leq i \leq n$.

Dacă $|c| = 0 \Rightarrow c = 0 \Rightarrow ad = 1 \Rightarrow a = d = 1$ sau $a = d = -1$.

În primul caz ($a = d = 1$) avem $M = \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} = U^b$ iar în al doilea caz

($a = d = -1$) avem $M = \begin{pmatrix} -1 & b \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} 1 & -b \\ 0 & 1 \end{pmatrix} = U^{-1} V^2 U^{-1} V^2 U^{-b}$

(ținând cont de (*)).

Presupunem acum că $|c| \neq 0$ și fie $q, r \in \mathbb{Z}$ a.f. $a = c \cdot q + r$, cu $0 \leq r < c$.

Deoarece $M_1 = VU^{-q-1}M = \begin{pmatrix} r-c & b-(q-1)d \\ r & b-qd \end{pmatrix}$, conform ipotezei de inducție putem scrie $M_1 = T_1^{k_1} \dots T_m^{k_m}$, cu $T_i \in \{U, V\}$, $k_i \in \mathbb{Z}$, $1 \leq i \leq m$, de unde $M = U^{q+1}V^{-1}M_1 = U^{q+1}V^{-1}T_1^{k_1} \dots T_m^{k_m}$.

3.23. Faptul că $U, V, W \in GL_2(\mathbb{Z})$ este imediat. Dacă $M \in GL_2(\mathbb{Z})$, atunci $\det(M) = 1$ sau -1 .

Dacă $\det(M) = 1$, atunci $M \in SL_2(\mathbb{Z})$ și totul rezultă din problema anterioară, iar dacă $\det(M) = -1$, cum $\det(W) = -1$ deducem că $\det(WM) = \det(W) \cdot \det(M) = 1$, deci $WM \in SL_2(\mathbb{Z})$ și din nou afirmația rezultă din exercițiul anterior deoarece $M = W^{-1}(WM)$.

3.24. Dacă $H, K \in L_0(G)$, $H \wedge K = H \cap K \in L_0(G)$ iar $H \vee K = HK = KH \in L_0(G)$.

Pentru prima parte, fie $x \in G$ și $h \in H \cap K$; atunci $xhx^{-1} \in H$, K deci $xhx^{-1} \in H \cap K$, adică $H \cap K \in L_0(G)$

Pentru partea a doua avem $HK = \bigcup_{x \in H} xK = \bigcup_{x \in H} Kx = KH$, deoarece $Kx = xK$, oricare ar fi $x \in G$, K fiind subgrup normal al lui G .

În mod evident $H, K \subseteq HK$, iar dacă alegem $S \leq G$ a.î. $H, K \subseteq S$, atunci $HK \subseteq S$, adică $HK = KH = H \vee K$. Pentru a arăta că HK este subgrup normal în G , fie $x \in G$, $h \in H$ și $k \in K$.

Scriind $x(hk)x^{-1} = (xhx^{-1})(xkx^{-1})$, cum $xhx^{-1} \in H$ și $xkx^{-1} \in K$, deducem că $x(hk)x^{-1} \in HK$, adică $HK \trianglelefteq G$, deci $H \vee K \in L_0(G)$.

Am demonstrat că $L_0(G)$ este o sublatice a lui $L(G)$ (chiar mărginită deoarece $\{1\}$ și $G \in L_0(G)$).

Demonstrăm că este o latice modulară, adică oricare ar fi $H, K, L \in L_0(G)$ cu $H \subseteq K$, se verifică relația $K \wedge (H \vee K) = H \vee (K \wedge L)$. Cum în orice latice are loc $H \vee (K \wedge L) \leq K \wedge (H \vee K)$, este suficient să probăm $K \wedge (H \vee K) \leq H \vee (K \wedge L)$, adică $K \cap (HL) \subseteq H(K \cap L)$. Dacă $x \in K \cap (HL)$ atunci $x \in K$ și $x \in HL$, adică $x = yz$ cu $y \in H$ și $z \in L$. Avem $z = y^{-1}x \in K$ și cum $z \in L$ deducem că $z \in K \cap L$. Cum $y \in H$ rezultă că $x = yz \in H(K \cap L)$, adică $K \cap (HL) \subseteq H(K \cap L)$.

3.25. Dacă M este un A -modul, atunci este în particular un grup comutativ. Cum într-un grup comutativ subgrupurile sunt subgrupuri normale, se aplică problema anterioară ținând cont că submodulele sunt în particular subgrupuri în grupuri aditive comutative (dacă $N, S \in L_A(M)$, $N \wedge S = N \cap S$ și $N \vee S = N + S = S + N$).

3.26. Dacă $x \in G$ și $y \in H \subseteq Z(G) \Rightarrow y \in Z(G) \Rightarrow xyx^{-1} = xx^{-1}y = y \in H$, adică H este subgrup normal al lui G .

3.27. Fie $x \in Z(H)$, $g \in G$ și $h \in H$. Din $H \trianglelefteq G \Rightarrow g^{-1}hg \in H \Rightarrow g^{-1}hgx = =xg^{-1}hg \Leftrightarrow hgxg^{-1} = hgxg^{-1}h \Rightarrow gxg^{-1} \in Z(H) \Rightarrow Z(H) \trianglelefteq G$.

3.28. Avem că $H = \{1, x\}$ cu $x \in G$, $x^2 = 1$, $x \neq 1$. Atunci $(\forall) y \in G$ avem $xyx^{-1} \in H$, deci $xyx^{-1} = 1$ sau $xyx^{-1} = x$. Dacă $xyx^{-1} = 1 \Rightarrow yx = y \Rightarrow x = 1$, fals. Deci $xyx^{-1} = x$, adică $yx = xy \Rightarrow x \in Z(G) \Rightarrow H \leq Z(G)$.

3.29. Deoarece $|G:H| = 2 \Rightarrow (G/H)_s = \{H, xH\}$ cu $x \notin H$. Atunci și $(G/H)_d = \{H, Hx\}$. Din $H \cap xH = H \cap Hx = \emptyset$ și $H \cup xH = H \cup Hx = G$ deducem că $xH = Hx$, adică $H \trianglelefteq G$.

3.30. Să demonstrăm la început că dacă $y, z \in G$ și $y^n = z^n$, atunci $y = z$.

Dacă $m = |G|$, deoarece $(m, n) = 1$, există $s, t \in \mathbb{Z}$ a.î. $ms + nt = 1$. Atunci $y = y^{ms+nt} = y^{nt} = z^{nt} = z^{ms+nt} = z$, deoarece ordinea lui y și z divid pe m . Rezultă atunci că mulțimea $\{y^n \mid y \in G\}$ conține m elemente diferite ale lui G , adică coincide cu G , de unde și faptul că $x = y^n$ pentru un singur y .

3.31. Deoarece $G/Z(G)$ are ordinul n , $[x, y]^n \in Z(G)$, deci $[x, y]^{n+1} = =x^{-1}y^{-1}x[x, y]^ny = x^{-1}y^{-2}xy^2y^{-1}[x, y]^{n-1}y = [x, y^2] \cdot [y^{-1}xy, y]^{n-1}$.

3.32. Răspunsul este negativ. Considerăm S_3 grupul permutărilor de ordin 3, $S_3 = \{e, \sigma_1, \sigma_2, \sigma_3, \sigma_4, \sigma_5\}$, unde $e = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$, $\sigma_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$, $\sigma_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$, $\sigma_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$, $\sigma_4 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$, $\sigma_5 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$.

Din teorema lui Lagrange rezultă că orice subgrup propriu al lui S_3 are 2 sau 3 elemente, deci subgrupurile lui S_3 sunt $H_1 = \{e\}$, $H_2 = \{e, \sigma_1\}$, $H_3 = \{e, \sigma_2\}$, $H_4 = \{e, \sigma_3\}$, $H_5 = \{e, \sigma_4, \sigma_5\}$. Toate acestea sunt comutative, dar $\sigma_1\sigma_2 = \sigma_5$ și $\sigma_2\sigma_1 = \sigma_4$, deci $\sigma_1\sigma_2 \neq \sigma_2\sigma_1$.

3.33. Fie $x \in G$, $x \neq 1$. Dacă notăm cu $k = o(x)$, atunci conform teoremei lui Lagrange $k \mid n$, deci putem scrie $n = k \cdot p$, cu $p \in \mathbb{N}^*$. Atunci $x^n = x^{kp} = (x^k)^p = =1^p = 1$.

Iată o soluție care nu utilizează teorema lui Lagrange în cazul în care G este comutativ.

Presupunem că $G = \{x_1, x_2, \dots, x_n\}$ și fie $x \in G$.

Deoarece $\{xx_1, xx_2, \dots, xx_n\} = G \Rightarrow (xx_1)(xx_2)\dots(xx_n) = x_1x_2\dots x_n \Rightarrow x^n(x_1x_2\dots x_n) = x_1x_2\dots x_n \Rightarrow x^n = 1$.

Fie acum $a, n \in \mathbb{N}^*$, $(a, n) = 1$. Deoarece $\hat{a} \in U(\mathbb{Z}_n^*, \cdot)$ iar grupul $G = U(\mathbb{Z}_n^*, \cdot)$ are $\varphi(n)$ elemente, conform celor de mai sus deducem că $(\hat{a})^{\varphi(n)} = \hat{1} \Rightarrow n \mid a^{\varphi(n)} - 1$.

3.34. (i). Cum (G, \cdot) este un grup cu n elemente, atunci $x^n = 1$, $(\forall) x \in G$ (conform problemei **3.33.**). Aceasta înseamnă că $G \subset U_n$. Dar atât G cât și U_n au câte n elemente, ceea ce arată că $G = U_n$.

(ii). Notăm $\xi = \cos \frac{2\pi}{n} + i \sin \frac{2\pi}{n}$. Atunci $G = U_n = \{1, \xi, \dots, \xi^{n-1}\}$.

Fie $k = nq + r$ cu $0 \leq r < n$ și deci, notând cu S suma din enunț, rezultă :
 $S = a_1^k + a_2^k + \dots + a_n^k = 1 + \xi^k + \xi^{2k} + \dots + \xi^{(n-1)k} = 1 + (\xi^n)^q \cdot \xi^r + (\xi^n)^{2q} \cdot \xi^{2r} + \dots$
 $\dots + (\xi^n)^{(n-1)q} \cdot \xi^{(n-1)r} = 1 + \xi^r + \xi^{2r} + \dots + \xi^{(n-1)r}$.

Deci dacă $r = 0$, atunci $S = n$, iar dacă $r > 0$, atunci :

$$S = 1 + \xi^r + \xi^{2r} + \dots + \xi^{(n-1)r} = \frac{1 - (\xi^r)^n}{1 - \xi^r} = \frac{1 - (\xi^n)^r}{1 - \xi^r} = \frac{1 - 1}{1 - \xi^r} = 0.$$

3.35. (i). Fie $a \in A$ fixat și $x \in G \setminus A$. Atunci $ax \in A$ (dacă $ax \notin A \Rightarrow ax \in G \setminus A$, și cum $x \in G \setminus A \Rightarrow a \in G \setminus A$ - contradicție)

Fie $f : G \setminus A \rightarrow A$, $f(x) = ax$. Atunci f este injectivă.

Dacă $G \setminus A$ este infinită $\Rightarrow A$ infinită (deoarece f este injectivă) - contradicție.

Deci $G \setminus A$ este finită $\Rightarrow G = (G \setminus A) \cup A =$ finit.

Fie $|G| = m$ și $|A| = n \Rightarrow |G \setminus A| = m - n$. Deoarece $G \setminus A \leq G$, atunci $m - n \mid m \Rightarrow m - n = m \Rightarrow n = 0$ - imposibil sau $m - n \leq m/2 \Rightarrow m \leq 2n \Rightarrow |G| \leq 2|A|$.

(ii). $m - n \mid m \Rightarrow m - n \mid m - n + n \Rightarrow m - n \mid n$. Dacă n este prim $\Rightarrow m - n = 1$ sau $m - n = n$, deci $m = n + 1$ sau $m = 2n$.

3.36. Fie $H' = \langle \{g^{-1}hg : g \in G, h \in H\} \rangle$.

Să demonstrăm la început că $H \subseteq H'$ și $H' \trianglelefteq G$. Cum pentru $x \in H$ avem $x = 1^{-1}x1$ iar $1 \in G \Rightarrow H \subseteq H'$. Dacă $\alpha = g^{-1}hg$, cu $g \in G, h \in H$, atunci se verifică ușor că $\alpha^n = g^{-1}h^n g$, $(\forall) n \in \mathbb{Z}$.

Ținând cont de definiția subgrupului generat de o mulțime, deducem că un element din H' este de forma:

$$h = (g_1^{-1}h_1g_1)^{n_1} \dots (g_k^{-1}h_kg_k)^{n_k} \text{ cu } g_i \in G, h_i \in H, n_i \in \mathbb{Z}, i = 1, 2, \dots, k, k \in \mathbb{N}.$$

Astfel, dacă $g \in G$, $g^{-1}hg = g^{-1}[(g_1^{-1}h_1^{n_1}g_1) \dots (g_k^{-1}h_k^{n_k}g_k)]g = [(g_1g)^{-1}h_1^{n_1}(g_1g)] \dots$

$\dots [(g_kg)^{-1}h_k^{n_k}(g_kg)] \in H'$, deci $H' \trianglelefteq G$.

Fie acum $H'' \trianglelefteq G$ a.î. $H \subseteq H''$; atunci deoarece orice element de forma $g_i^{-1} h_i^{n_i} g_i$ cu $g_i \in H$, $n_i \in \mathbb{Z}$ este în $H'' \Rightarrow H' \subseteq H''$.

3.37. (i). Definim $f : (C \cap B / C \cap A)_d \rightarrow (B/A)_d$ prin $f((C \cap A)x) = Ax$, $(\forall) x \in C \cap B$.

Dacă $x, y \in C \cap B$ și $(C \cap A)x = (C \cap A)y$, atunci $xy^{-1} \in C \cap A \leq A$, deci $Ax = Ay$, adică f este corect definită.

Dacă $x, y \in C \cap B$ și $Ax = Ay \Rightarrow xy^{-1} \in C \cap A \Rightarrow (C \cap A)x = (C \cap A)y$, adică f este injectivă, de unde rezultă că $|(C \cap B / C \cap A)_d| \leq |(B/A)_d| \Leftrightarrow |(C \cap B) : (C \cap A)| \leq |B : A|$.

(ii). Cum $A \leq G$, conform cu (i) avem $|G : A| \geq |(G \cap B) : (B \cap A)| = |B : (A \cap B)|$, prin urmare $|G : A| \cdot |G : B| \geq |B : (A \cap B)| \cdot |G : B| = |G : (A \cap B)|$.

(iii). cum $B \leq A \vee B$, conform cu (i) avem:

$$|A \vee B| \geq |(A \vee B) \cap A : (A \cap B)| \Leftrightarrow |(A \vee B) : B| \geq |A : (A \cap B)|.$$

3.38. (i). Conform problemei anterioare avem:

$$|G : (A \cap B)| \leq |G : A| \cdot |G : B|,$$

deci $|G : (A \cap B)|$ este finit.

De asemenea, $|G : (A \cap B)| = |G : A| \cdot |A : (A \cap B)| = |G : B| \cdot |B : (A \cap B)|$. Cum $|G : A|$ și $|G : B|$ sunt prime între ele, rezultă că $|G : A|$ divide $|B : (A \cap B)|$, deci $|G : A| \leq |B : (A \cap B)|$.

Pe de altă parte, tot din exercițiul precedent ((iii)), avem că $|G : A| \geq |(A \vee B) : A| \geq |B : (A \cap B)|$. Prin urmare $|G : A| = |B : (A \cap B)|$ și $|G : (A \cap B)| = |G : A| \cdot |G : B|$.

(ii). În cazul în care G este finit, relația $|G : (A \cap B)| = |G : A| \cdot |G : B|$ se scrie $|G| / |A \cap B| = (|G| / |A|) \cdot (|G| / |B|)$, de unde rezultă că $|G| = (|A| \cdot |B|) / |A \cap B| = |AB|$ (conform problemei 2.35.) și astfel $G = AB$.

3.39. Ținând cont de problemei 3.37., ((iii)) și de ipoteză avem:

$$|(A \vee B) : B| \geq |A : (A \cap B)| > 1/2 \cdot |G : B|.$$

Cum $|G : B| = |G : (A \vee B)| \cdot |(A \vee B) : B| \Rightarrow |G : (A \vee B)| < 2$, de unde $|G : (A \vee B)| = 1 \Rightarrow G = A \vee B$.

3.40. Fie $x_1, x_2, \dots, x_n \in G$ a.î. $\langle x_1, x_2, \dots, x_n \rangle = G$ și $H \leq G$ a.î. $|G : H| = m$ ($m, n \in \mathbb{N}^*$).

Pentru fiecare $j = 1, 2, \dots, n$ notând $x_{n+j} = x_j^{-1}$, fie $g_1, g_2, \dots, g_n \in G$ a.î. $G = \bigcup_{i=1}^m Hg_i$, unde $g_1 = 1$. Atunci, pentru fiecare pereche ordonată (i, j) există un

unic element $h_{ij} \in H$ și un unic $k \in \{1, 2, \dots, m\}$ a.î. $g_i x_j = h_{ij} g_k$ $i \in \{1, 2, \dots, m\}$ și $j \in \{1, 2, \dots, 2n\}$.

Se probează acum imediat faptul că $\{h_{ij} : i = 1, 2, \dots, m, j = 1, 2, \dots, n\}$ este un sistem de generatori pentru H .

3.41. Este suficient să probăm afirmația din enunț pentru cazul a două subgrupuri H, K ale lui G .

Pentru aceasta definim $f : (G/H \cap K)_d \rightarrow (G/H)_d \times (G/K)_d$ prin $f(x(H \cap K)) = (xH, xK), (\forall) x \in G$.

Să demonstrăm acum că f este injectivă și totul va fi clar; pentru aceasta fie $x, y \in G$ a.î. $xH = yH$ și $xK = yK$. Deducem imediat că $xy^{-1} \in H \cap K$, deci $x(H \cap K) = y(H \cap K)$, adică f este injectivă (de fapt putem utiliza și problemei 3.37. (ii)).

3.42. Faptul că $C_G(x) \leq G$ este imediat. Fie acum $a, b \in G$. Din echivalențele $axa^{-1} = bxb^{-1} \Leftrightarrow b^{-1}a \in C_G(x) \Leftrightarrow a \in C_G(x) = b C_G(x)$ deducem că dacă notăm cu C_x mulțimea conjugatilor lui x din G , atunci funcția $f : C_x \rightarrow (G/C_G(x))_d$, $f(axa^{-1}) = a C_G(x), (\forall) a \in G$ este corect definită și injectivă. Cum surjectivitatea lui f este evidentă, deducem că $|C_x| = |(G/C_G(x))_d| = |G : C_G(x)|$.

3.43. Dacă alegem H a.î. $K \leq H \leq G$, deoarece $Z(H) \leq C_G(K)$, atunci în ipoteza $C_G(K) = 1$ rezultă că $Z(H) = 1$.

Reciproc, presupunem că $Z(H) = 1$ pentru orice H a.î. $K \leq H \leq G$. Dacă $x \in C_G(K)$, atunci pentru $H = \langle K \cup \{x\} \rangle$ avem $K \leq H \leq G$ și $x \in Z(H) = 1$, deci $C_G(K) = 1$.

3.44. (i). Fie $A = (a_{ij})_{1 \leq i, j \leq n} \in C_G(D)$; deoarece $K \neq Z_2$ pentru orice $1 \leq j < k \leq n$ putem alege elementele $h_i \in K^*, i = 1, 2, \dots, n$ cu $h_i \neq h_k$. Considerând matricea B ce are pe diagonala principală elementele h_1, h_2, \dots, h_n iar în rest zero, din $AB = BA \Rightarrow a_{jk} = 0 \Rightarrow A \in D$, adică $C_G(D) \leq D$ (am notat $G = GL_n(K)$).

Deoarece D este comutativ deducem că $D \leq C_G(D)$, adică $C_G(D) = D$.

Fie acum $A = (a_{ij})_{1 \leq i, j \leq n} \in Z(G) \leq C_G(D) = D$ cu $a_{jk} = 0$ pentru $j \neq k$.

Notând cu $E_{ij} \in M_n(K)$ matricea ce are pe poziția (i, j) pe 1 iar în rest zero, considerăm pentru orice (i, j) cu $1 \leq i < j \leq n$, matricea $B = I_n + E_{ij}$. Atunci $B^{-1} = I_n - E_{ij}$ iar $BAB^{-1} = B + (a_{ji} - a_{ii})E_{ij}$. Scriind că $BAB^{-1} = B \Rightarrow a_{ii} = a_{jj}$, adică $A \in \{aI_n : a \in K\}$, de unde incluziunea $Z(G) \subseteq \{aI_n : a \in K\}$. Cum cealaltă incluziune este evidentă deducem egalitatea cerută.

(ii). Să notăm $S = SL_n(K)$.

Dacă $n = 2$, cum $K \neq \mathbb{Z}_2, \mathbb{Z}_3$ putem alege $x \in K, x \neq -1$ sau 1 și considerând $x_1 = x, x_2 = x^{-1}$ avem $x_1 x_2 = 1$, deci matricea $B = x_1 E_{11} + x_2 E_{22} \in D \cap S$. Alegând acum $A \in C_G(D \cap S)$, din $AB = BA \Rightarrow a_{12} = a_{21} = 0$, adică $A \in D$.

Dacă $n > 2$, atunci $K \neq \mathbb{Z}_2$ iar pentru $1 \leq j < k \leq n$ alegem $t \in \{1, 2, \dots, n\} \setminus \{j, k\}$ și $x_k = x_t = -1$ iar $x_i = 1$ pentru $i \in \{1, 2, \dots, n\} \setminus \{k, t\}$.

Deoarece $x_1 x_2 \dots x_n = 1$ avem că $B = x_1 E_{11} + \dots + x_n E_{nn} \in D \cap S$.

Din egalitatea $AB = BA \Rightarrow a_{jk} = 0$, adică $A \in D$.

În ambele situații obținem că $C_G(D \cap S) \leq D$.

Cum D este comutativ și $D \cap S \leq D \Rightarrow D \leq C_G(D \cap S)$, adică $C_G(D \cap S) = S$.

Avem $Z(S) \leq C_G(D \cap S) = S$, deci $Z(S) \leq D \cap S$. Observăm că pentru orice i, j cu $1 \leq i < j \leq n$, matricea $B = I_n + E_{ij} \in S$.

Cu ajutorul lui B repetăm raționamentul : orice matrice din $Z(S)$ este scalară, adică $Z(S) \leq S \cap Z(G)$ și cum incluziunea $S \cap Z(G) \subseteq Z(S)$ este evidentă, deducem că $Z(S) = S \cap Z(G)$.

3.45. Fie $H = \langle \rho \rangle \leq \mathbf{D}_n$; deoarece $o(\rho) = n$ deducem că H este subgrup ciclic de ordin n .

Orice element din $\mathbf{D}_n \setminus H$ este de forma $\rho^k \varepsilon$, $k = 0, 1, \dots, n-1$. De asemenea, avem că $\varepsilon \rho = \rho^{n-1} \varepsilon = \rho^{-1} \varepsilon$. Dacă presupunem că $\varepsilon \rho^k = \rho^{-k} \varepsilon$, atunci $\varepsilon \rho^{k+1} = \varepsilon \rho \rho^k = \rho^{-1} \varepsilon \rho^k = \rho^{-1} \rho^{-k} \varepsilon = \rho^{-(k+1)} \varepsilon$, prin urmare $\varepsilon \rho^k = \rho^{-k} \varepsilon$ pentru orice $k = 0, 1, \dots, n-1$ și $(\rho^k \varepsilon)^2 = \rho^k \varepsilon \rho^k \varepsilon = \rho^k \rho^{-k} \varepsilon^2 = 1$.

Rezultă că pentru orice $x \in \mathbf{D}_n \setminus H$ avem $o(x) = 2$. Dacă $H' = \langle x \rangle$, $x \in \mathbf{D}_n$ (iar \mathbf{D}_n este grup ciclic de ordin n) atunci $o(x) = n > 2$, deci $x \in H$. Dar atunci $H' \leq H$, $|H'| = |H| = n$, deci $H = H'$.

3.46. Avem că $\mathbf{D}_n = \{\rho^k \varepsilon^t : k = 0, 1, \dots, n-1, \text{ iar } t = 0, 1\}$. Pentru $k, r \in \{0, 1, \dots, n-1\}$ avem $\rho^k (\rho^r \varepsilon) = \rho^{k+r} \varepsilon$ și $(\rho^k \varepsilon) \rho^r = \rho^{r-k} \varepsilon$, prin urmare $\rho^k (\rho^r \varepsilon) = (\rho^r \varepsilon) \rho^k \Leftrightarrow k + r \equiv r - k \pmod{n} \Leftrightarrow 2k \equiv 0 \pmod{n}$.

Rezultă că un element de forma $\rho^r \varepsilon$, $r = 0, 1, \dots, n-1$ nu face parte din $Z(\mathbf{D}_n)$. În plus, $\rho^k \in Z(\mathbf{D}_n) \Leftrightarrow 2k \equiv 0 \pmod{n}$.

Dacă n este impar, rezultă că $k = 0$, deci $|Z(\mathbf{D}_n)| = 1$, iar dacă n este par, $n = 2m$, atunci $k = 0$ sau $k = m$, adică $Z(\mathbf{D}_n) = \{1, \rho^m\}$, deci $|Z(\mathbf{D}_n)| = 2$.

3.47. Să presupunem prin absurd că $(\exists) H \leq A_4$ a.î. $|H| = 6$. Atunci $|A_4 : H| = 12 : 6 = 2$ și deci $H \trianglelefteq A_4$ (conform problemei **3.29**). Deoarece A_4 conține 8 cicluri de lungime 3, H va trebui să conțină un astfel de ciclu α . Ținând cont de problema **2.87**, deducem că în S_4 α va avea 8 conjugăți, astfel că $C_{S_4}(\alpha)$ va avea în S_4 indicele 8 (conform problemei **3.42**) iar ordinul

$24 : 8 = 3$; există deci numai 3 permutări în S_4 (cu atât mai mult în A_4) ce comută cu α . Acestea sunt α , α^{-1} și e (permutarea identică din S_4). Deoarece toate sunt în A_4 , rezultă că $C_{A_4}(\alpha)$ are ordinul 3 iar indicele în A_4 egal cu $12 : 3 = 4$. Deci α are 4 conjugați în A_4 , care vor fi de fapt în H căci $H \trianglelefteq A_4$.

De asemenea, H trebuie să conțină și un element β de ordin 2, $\beta = (ab)(cd)$. Am depistat astfel 6 elemente ale lui H și anume : 4 cicluri de lungime 3, β și e .

Dacă $\gamma = (a,b,c)$, atunci $\gamma \in A_4$, $\gamma\beta\gamma^{-1} = (c,a)(b,d) \neq \beta$ iar $\gamma\beta\gamma^{-1} \in H$. Am găsit astfel un nou element în H diferit de cele 6 (și anume pe $\gamma\beta\gamma^{-1}$), ceea ce contrazice presupunerea de existență a lui $H \leq A_4$ a.î. $|H| = 6$.

§4. Morfisme și izomorfisme de grupuri. Grupuri factor. Teorema lui Cauchy. Teoremele de izomorfism pentru grupuri.

4.1. Dacă $x, y \in G$ atunci $f(x) = g(x)$ și $f(y) = g(y)$, astfel că $f(xy^{-1}) = f(x)f(y^{-1}) = f(x)(f(y))^{-1} = g(x)(g(y))^{-1} = g(x)g(y^{-1}) = g(xy^{-1})$, adică $xy^{-1} \in G$, deci $G \leq G_1$.

Afirmațiile (i) și (ii) se demonstrează acum analog ca în cazul monoizilor (vezi problema **1.28.**).

4.2. (i) \Rightarrow (ii). Dacă $x \in \text{Ker}(f) \Rightarrow f(x) = 1 = f(1) \Rightarrow x = 1$, adică $\text{Ker}(f) = \{1\}$.

(ii) \Rightarrow (i). Dacă $x, y \in G_1$ și $f(x) = f(y) \Rightarrow f(xy^{-1}) = 1 \Rightarrow xy^{-1} \in \text{Ker}(f) \Rightarrow xy^{-1} = 1 \Rightarrow x = y$, adică f este injectivă.

4.3. (i) \Rightarrow (ii). Dacă $x \in G_0 \Rightarrow (f \circ g)(x) = (f \circ h)(x) \Rightarrow f(g(x)) = f(h(x)) \Rightarrow g(x) = h(x) \Rightarrow g = h$.

(ii) \Rightarrow (i). Să presupunem prin absurd că f nu este injectivă, adică $\text{Ker}(f) \neq \{1\}$ (conform problemei **4.2.**).

Considerăm $g, h : \text{Ker}(f) \rightarrow G_1$, g morfismul incluziune iar h morfismul nul.

Dacă $x \in \text{Ker}(f) \Rightarrow (f \circ g)(x) = f(g(x)) = f(x) = 1$ iar $(f \circ h)(x) = f(h(x)) = f(1) = 1$, adică $f \circ g = f \circ h$ și totuși $g \neq h$, ceea ce este absurd.

Deci $\text{Ker}(f) = \{1\}$, adică f este injectivă.

4.4. (i) \Rightarrow (ii). Fie $y \in G_2$; cum f este surjectivă (\exists) $x \in G_1$ a.î. $y = f(x)$.

Din $g \circ f = h \circ f \Rightarrow g(f(x)) = h(f(x)) \Rightarrow g(y) = h(y) \Rightarrow g = h$.

(ii) \Rightarrow (i). (După Eilenberg și Moore) Fie $H = f(G_1) \leq G_2$.

Dacă $H = G_2$, evident f este surjectivă; presupunem că $H \neq G_2$.

Cazul 1. $|G : H| = 2$, atunci conform problemei 3.29. avem că $H \leq G_2$ și considerând în categoria grupurilor diagrama:

$$G_1 \xrightarrow{f} G_2 \begin{array}{c} \xrightarrow{g} \\ \xrightarrow{h} \end{array} G_3 = G_2/H,$$

unde g este morfismul surjectiv canonic iar h este morfismul nul, atunci se verifică imediat că $g \circ f = h \circ f$ și totuși $g \neq h$, absurd!

Cazul 2. $|G_2 : H| > 2$. Fie $\{x_i\}_{i \in I}$ un sistem complet de reprezentanți pentru clasele de resturi la stânga ale lui G_2 relativ la subgrupul H .

Pentru clasa de resturi H alegem ca reprezentant pe 1 și fie $i_0 \in I$ a.î. $x_{i_0} = 1$.

Fie $\sigma : I \rightarrow I$ o bijecție a.î. $\sigma(i_0) = i_0$ și $\sigma(i) \neq i$, $(\forall) i \neq i_0$.

Definim $\lambda : G_2 \rightarrow G_2$, $\lambda(x) = xx_i^{-1}x_{\sigma(i)}$, dacă $x \in Hx_i$.

Dacă $\lambda(x) = \lambda(y) \Rightarrow xx_i^{-1}x_{\sigma(i)} = yx_j^{-1}x_{\sigma(j)}$, cu $x \in Hx_i$ iar $y \in Hx_j$. Cum $xx_i^{-1}, yx_j^{-1} \in H \Rightarrow x_{\sigma(i)} \in Hx_{\sigma(j)} \Rightarrow \sigma(i) = \sigma(j) \Rightarrow i = j \Rightarrow x = y$, deci λ este o funcție injectivă.

Dacă $y \in G_2$, $y \in Hx_j$ și $i \in I$ a.î. $\sigma(i) = j$, fie $h = yx_j^{-1} \in H$ și $x = hx_i$. Atunci $\lambda(x) = xx_i^{-1}x_{\sigma(i)} = h x_i x_i^{-1} x_{\sigma(i)} = hx_j = y$, deci λ este surjectivă, adică λ este bijecție.

Considerăm în categoria grupurilor diagrama:

$$G_1 \xrightarrow{f} G_2 \begin{array}{c} \xrightarrow{\alpha} \\ \xrightarrow{\beta} \end{array} G_3, \text{ unde } G_3 = \Sigma(G_2), \alpha \text{ este morfismul}$$

Cayley (adică pentru $g \in G_2$, $\alpha(g) : G_2 \rightarrow G_2$, $\alpha(g)(x) = gx$, $(\forall) x \in G_2$) iar $\beta(g) = \lambda^{-1} \circ \alpha(g) \circ \lambda$, $(\forall) g \in G_2$. Să demonstrăm că $\alpha(g) = \beta(g) \Leftrightarrow g \in H$. (*)

Dacă $\alpha(g) = \beta(g) \Rightarrow \alpha(g)(x) = \beta(g)(x)$, $(\forall) x \in G_1 \Rightarrow gx = \lambda^{-1}(g\lambda(x))$, $(\forall) x \in G_1$ atunci considerând $x = 1 \Rightarrow g = \lambda^{-1}(g)$ (pentru că $\lambda(1) = 1$). Deci $g = \lambda(g) = gx_i^{-1}x_{\sigma(i)} \Rightarrow x_i^{-1}x_{\sigma(i)} = 1 \Rightarrow x_i = x_{\sigma(i)} \Rightarrow i = \sigma(i) \Rightarrow x_i = x_{i_0} = 1 \Rightarrow g \in H$.

Dacă $h \in H$ și $x \in G_2 \Rightarrow \lambda(hx) = h\lambda(x)$ (căci $x \in Hx_i \Rightarrow \lambda(hx) = hxx_i^{-1}x_{\sigma(i)} = h(\lambda(x))$), deci dacă $g \in H \Rightarrow (\beta(g))(x) = \lambda^{-1}(g\lambda(x)) = \lambda^{-1}(\lambda(gx)) = gx = (\alpha(g))(x)$, $(\forall) x \in G \Rightarrow \alpha(g) = \beta(g)$.

Din (*) rezultă că $\alpha \circ f = \beta \circ f$ și cum $\alpha \neq \beta$ obținem contradicția ce ne arată că f este surjectivă.

4.5. Pe mulțime $M \times M$ considerăm relația $((x,y),(x',y')) \in \rho \Leftrightarrow xy' = x'y$ și se verifică imediat că este o congruență pe mulțimea produs $M \times M$.

Considerăm $G_M = (M \times M)/\rho$ și pentru $(x,y) \in M \times M$ vom nota prin $(x,y)_\rho$ clasa de echivalență a lui (x,y) modulo ρ .

Pentru $(x_i, y_i) \in M \times M$, $i = 1, 2$, definim:

$$(x_1, y_1)_\rho \cdot (x_2, y_2)_\rho = (x_1 x_2, y_1 y_2)_\rho.$$

Se probează imediat faptul că această operație este corect definită și dubletul (G_M, \cdot) devine în felul acesta grup (elementul neutru este $(1,1)_\rho$ iar $(x,y)_\rho^{-1} = (y,x)_\rho$).

Aplicația $i_M : M \rightarrow G_M$, $i_M(x) = (x,1)_\rho$, $(\forall) x \in M$ este morfismul căutat.

Într-adevăr, dacă $x,y \in M$, atunci $i_M(xy) = (xy,1)_\rho = (x,1)_\rho \cdot (y,1)_\rho = i_M(x) \cdot i_M(y)$ și $i_M(1) = (1,1)_\rho = 1$, adică i_M este morfism de monoizi.

Dacă $i_M(x) = i_M(y) \Rightarrow (x,1)_\rho = (y,1)_\rho \Rightarrow x \cdot 1 = y \cdot 1 \Rightarrow x = y$, adică i_M este morfism injectiv de monoizi.

Fie acum G un grup comutativ și $u : G \rightarrow M$ un morfism de monoizi.

Definim $u' : G_M \rightarrow G$ prin $u'((x,y)) = u(x) \cdot (u(y))^{-1}$, $(\forall) (x,y) \in M \times M$.

Evident, u' este corect definită deoarece dacă mai avem $(x',y') \in M \times M$ a.î. $(x,y)_\rho = (x',y')_\rho \Rightarrow xy' = x'y \Rightarrow u(xy') = u(x'y) \Rightarrow u(x)u(y') = u(x')u(y) \Rightarrow u(x)(u(y))^{-1} = u(x')(u(y'))^{-1} \Rightarrow u'((x,y)_\rho) = u'((x',y')_\rho)$.

De asemenea, $u'((x,y)_\rho \cdot (x',y')_\rho) = u'((xx',yy')_\rho) = u(xx') \cdot (u(yy'))^{-1} = u(x)u(x') \cdot (u(y)u(y'))^{-1} = (u(x)u(y))^{-1} \cdot (u(x')u(y'))^{-1} = u'((x,y)_\rho) \cdot u'((x',y')_\rho)$, adică u' este morfism de monoizi.

Dacă $x \in M$, atunci $(u' \circ i_M)(x) = u'(i_M(x)) = u'((x,1)_\rho) = u(x)u(1) = u(x)$, adică $u' \circ i_M = u$.

Unicitatea lui u' se verifică imediat.

4.6. Fie $e > 1$ elementul neutru al grupului (M, \circ) .

Atunci $x \circ e = xe + ax + be + c = x$ și $e \circ x = ex + ae + bx + c = x$ pentru orice $x > 1$, de unde $e + a = 1$, $be + c = 0$, $e + b = 1$ și $ae + c = 0$. Din ultimele patru relații deducem $a = b$, $e = 1 - a > 1$ și $a(1 - a) + c = 0$, deci $a = b < 0$ și $c = a^2 - a$. Operația algebrică se scrie $x \circ y = xy + a(x + y) + a^2 - a$. Cum M este stabilă relativ la " \circ " rezultă $x \circ x = x^2 + 2ax + a^2 - a > 1$ pentru orice $x > 1$. Deci $\lim_{x \rightarrow 1} (x^2 + 2ax + a^2 - a) = a^2 + a + 1 \geq 1$, de unde $a(a + 1) \geq 0$ și cum $a < 0$ rezultă $a \leq -1$.

Dacă $a < -1$, fie $x = \frac{1-a}{2} > 1$ și $y > 1$. Atunci $x \circ y = \frac{1-a}{2}y + a(1 - \frac{a}{2} + y) + a^2 - a = \frac{(1+a)y + a^2 - a}{2} > 1 \Leftrightarrow (1+a)y + a^2 - a > 2 \Leftrightarrow (1+a)(y + a - 2) > 0$.

Cum $1 + a < 0$, rezultă că $y + a - 2 < 0$ pentru orice $y > 1$, fals căci $\lim_{y \rightarrow \infty} (y + a - 2) = +\infty$. Deci $a = -1$ și operația devine $x \circ y = xy - (x + y) + 2$. Se arată cu ușurință că (M, \circ) este grup.

Fie $f : M \rightarrow \mathbb{R}$, $f(x) = \ln(x-1)$. Cum $f(x \circ y) = f(xy - (x+y) + 2) = \ln(xy - x - y + 1) = \ln((x-1)(y-1)) = \ln(x-1) + \ln(y-1) = f(x) + f(y)$, rezultă că f este morfism de grupuri. Cum f este bijectivă, rezultă că f este izomorfism de grupuri.

4.7. Cum $G \neq \{0\}$, există $a \in G, a \neq 0$. Deoarece $G \leq \mathbb{R}$, $-a \in G$, deci G conține numere reale strict pozitive. Fie $a > 0, a \in G$ și $b = a+1$. Cum $G \cap (-b, b)$ este finită și nevidă (conține numărul a), fie α cel mai mic număr real strict pozitiv al ei. Atunci α este cel mai mic număr real strict pozitiv al lui G , (într-adevăr, dacă $\beta \in G, \beta > 0, \beta < \alpha$ atunci $\beta \in (-b, b) \cap G$ ceea ce contrazice alegerea lui α).

Vom arăta că $G = \{\alpha k / k \in \mathbb{Z}\} = \alpha \mathbb{Z}$.

Incluziunea $\alpha \mathbb{Z} \subset G$ este imediată (se demonstrează prin inducție după $k > 0$ că $\alpha k \in G$ și cum $\alpha(-k) = -(\alpha k) \in G$ pentru orice $k > 0$, rezultă incluziunea dorită).

Pentru incluziunea inversă, fie $\beta > 0, \beta \in G$ și $p = [\frac{\beta}{\alpha}]$. Rezultă că $p \leq \frac{\beta}{\alpha} < p+1$ sau $p\alpha \leq \beta < p\alpha + \alpha$, de unde $0 \leq \beta - p\alpha < \alpha$. Cum $\beta \in G, p\alpha \in G$, deducem că $\beta - p\alpha \in G$ și ținând cont de alegerea lui α , avem că $\beta - p\alpha = 0$, adică $\beta = p\alpha \in \{\alpha k / k \in \mathbb{Z}\}$.

Dacă $\beta < 0, \beta \in G$ atunci $-\beta > 0, -\beta \in G$ și deci $-\beta \in \alpha \mathbb{Z}$, de unde $\beta \in \alpha \mathbb{Z}$.

Cum evident $0 = \alpha \cdot 0 \in \alpha \mathbb{Z}$, rezultă $G = \alpha \mathbb{Z}$. Grupurile $(G, +)$ și $(\mathbb{Z}, +)$ sunt izomorfe prin aplicația $f : G \rightarrow \mathbb{Z}, f(\alpha k) = k, (\forall) k \in \mathbb{Z}$.

4.8. (i). Dacă $H_2 \leq G$ și $x, y \in H_2$ atunci $xy \in H_2$ deci $x^2 y^2 = 1 = (xy)^2 = xyxy \Rightarrow x^{-1} x^2 y^2 y^{-1} = x^{-1} xyxy y^{-1} \Rightarrow xy = yx$.

Dacă $xy = yx$ pentru orice $x, y \in H_2$, atunci $(xy)^2 = xyxy = x^2 y^2 = 1$ și $(x^{-1})^2 = (x^2)^{-1} = 1$ deci $H_2 \leq G$.

(ii). Evident $1 \in H_p$. Dacă există $x \in H_p \setminus \{1\}$, fie $k \in \mathbb{N}^*$ cel mai mic cu proprietatea $x^k = 1$. Folosind teorema împărțirii cu rest, există $q, r \in \mathbb{Z}, 0 \leq r < k$ a.î. $p = kq + r \Rightarrow 1 = x^p = (x^k)^q x^r = x^r \Rightarrow r = 0$, de unde $k = p$. Rezultă că $H_p = \{1, x, x^2, \dots, x^{p-1}\}$ care este un subgrup al lui G .

Izomorfismul dintre H_p și $(\mathbb{Z}_p, +)$ este dat de $x^i \rightarrow \hat{i}, 0 \leq i \leq p-1$.

4.9. (i). Fie $x, y \in G$. Atunci $x \circ y = x^{\alpha \log_a y} > 0$. Dacă $x^{\alpha \log_a y} = 1 \Rightarrow x = 1$ sau $\alpha \log_a y = 0 \Rightarrow y = 1$ – imposibil deoarece $1 \notin G$. Atunci $x \circ y \in G$, deci G este *parte stabilă* față de operația algebrică " \circ ".

- *asociativitatea și comutativitatea* rezultă prin calcul ;

- *elementul neutru* : fie $e \in G$ a.î. $x \circ e = x, (\forall) x \in G \Rightarrow x^{\alpha \log_a e} = x \Leftrightarrow$

$$\alpha \log_a e = 1 \Leftrightarrow \log_a e = \frac{1}{\alpha} \Leftrightarrow e = a^{\frac{1}{\alpha}}.$$

- *elementele simetrizabile* : fie $x \in G$ a.î. $x \circ x' = e \Leftrightarrow x^{\alpha \log_a x'} = a^{\frac{1}{\alpha}} \Leftrightarrow$
 $\log_a x^{\alpha \log_a x'} = \log_a a^{\frac{1}{\alpha}} \Leftrightarrow \alpha \log_a x' \cdot \log_a x = \frac{1}{\alpha} \Leftrightarrow \log_a x' = \frac{1}{\alpha^2 \log_a x} \Leftrightarrow$

$x' = a^{\frac{1}{\alpha^2 \log_a x}}$ este simetricul lui x față de operația algebrică " \circ " .

Deci $G_{a,\alpha}$ este grup abelian.

(ii). Fie $f : \mathbb{R} \rightarrow G$, $f(x) = a^{\frac{x}{\alpha}}$. Arătăm că f este injectivă :

$$f(x) = f(y) \Rightarrow a^{\frac{x}{\alpha}} = a^{\frac{y}{\alpha}} \Rightarrow \frac{x}{\alpha} = \frac{y}{\alpha} \Rightarrow x = y.$$

Arătăm că f este și surjectivă : fie $y \in G$ și atunci $f(x) = y \Leftrightarrow a^{\frac{x}{\alpha}} = y \Leftrightarrow$
 $\frac{x}{\alpha} = \log_a y \Leftrightarrow x = \alpha \log_a y \in \mathbb{R}^*$.

Fie $x, y \in \mathbb{R}^*$. Atunci $f(xy) = f(x) \circ f(y) \Leftrightarrow a^{\frac{xy}{\alpha}} = f(x)^{\alpha \log_a f(y)} \Leftrightarrow$
 $a^{\frac{xy}{\alpha}} = \left(a^{\frac{x}{\alpha}}\right)^{\alpha \log_a \left(a^{\frac{y}{\alpha}}\right)} \Leftrightarrow a^{\frac{xy}{\alpha}} = \left(a^{\frac{x}{\alpha}}\right)^{\alpha \cdot \frac{y}{\alpha}} \Leftrightarrow a^{\frac{xy}{\alpha}} = a^{\frac{xy}{\alpha}}$, deci f este un morfism de grupuri.

Astfel, am demonstrat că f este un izomorfism de grupuri, adică $\mathbb{R}^* \approx G_{a,\alpha}$. Analog $\mathbb{R}^* \approx G_{b,\beta}$, deci $G_{a,\alpha} \approx G_{b,\beta}$.

4.10. Se verifică ușor axiomele grupului față de înmulțirea matricelor.

- dacă $A = \begin{pmatrix} ch a & sh a \\ sh a & ch a \end{pmatrix}$ și $B = \begin{pmatrix} ch b & sh b \\ sh b & ch b \end{pmatrix}$ atunci

$A \cdot B = \begin{pmatrix} ch(a+b) & sh(a+b) \\ sh(a+b) & ch(a+b) \end{pmatrix}$ astfel că M este *parte stabilă* în raport cu înmulțirea matricelor;

- *asociativitatea* este evidentă;

- *elementul neutru* este $I_2 = \begin{pmatrix} ch 0 & sh 0 \\ sh 0 & ch 0 \end{pmatrix}$;

- dacă $A \in M$, atunci $\det A = ch^2 a - sh^2 a = 1$, deci A este inversabilă și

inversa ei este $A^{-1} = \begin{pmatrix} ch a & -sh a \\ -sh a & ch a \end{pmatrix} = \begin{pmatrix} ch(-a) & sh(-a) \\ sh(-a) & ch(-a) \end{pmatrix}$.

Funcția $f: \mathbb{R} \rightarrow M$, $f(a) = \begin{pmatrix} ch a & sh a \\ sh a & ch a \end{pmatrix}$ este izomorfismul dorit (folosim faptul că: $ch a ch b + sh a sh b = ch(a+b)$ și $sh a ch b + ch a sh b = sh(a+b)$).

4.11. (i). Se verifică ușor axiomele grupului față de înmulțirea matricelor pentru mulțimile M și G .

Pentru mulțimea M :

- M este parte stabilă: fie $A, B \in M$, $A = \begin{pmatrix} a+2b & 3b \\ 2b & a-2b \end{pmatrix}$ și

$B = \begin{pmatrix} a'+2b' & 3b' \\ 2b' & a'-2b' \end{pmatrix}$, cu $a^2 - 10b^2 = (a')^2 - 10(b')^2 = 1$. Atunci:

$$AB = \begin{pmatrix} (aa' + 10bb') + 2(ab' + a'b) & 3(ab' + a'b) \\ 2(ab' + a'b) & (aa' + 10bb') - 2(ab' + a'b) \end{pmatrix}$$

și se verifică prin calcul că $(aa' + 10bb')^2 - 10(ab' + a'b)^2 = 1$, deci $AB \in M$.

- *asociativitatea*: se știe că înmulțirea matricelor este asociativă.

- *elementul neutru* este evident I_2 deoarece $I_2 \in M$.

- *elementele inversabile*: fie $A \in M \setminus \{I_2\}$, $A = \begin{pmatrix} a+2b & 3b \\ 2b & a-2b \end{pmatrix} \Rightarrow$

$a^2 - 10b^2 = 1 \Rightarrow \det A = 1 \Rightarrow A$ este inversabilă. Inversa lui A se calculează ușor:

$$A^{-1} = \begin{pmatrix} a+2(-b) & 3(-b) \\ 2(-b) & a-2(-b) \end{pmatrix} \in M.$$

Calcul simple sunt și pentru G .

(ii). Izomorfismul căutat este $f: M \rightarrow G$, $f\left(\begin{pmatrix} a+2b & 3b \\ 2b & a-2b \end{pmatrix}\right) = a + b\sqrt{10}$.

4.12. (i). Numărul matricelor de forma $\begin{pmatrix} x & y \\ -y & x \end{pmatrix}$ cu $x, y \in \mathbb{Z}_3$ este egal

cu numărul perechilor $(x, y) \in \mathbb{Z}_3 \times \mathbb{Z}_3$, adică $3 \cdot 3 = 9$ (deoarece la perechi distincte corespund matrice distincte).

(ii). Se observă că mulțimea soluțiilor ecuației $x^2 + y^2 = \hat{1}$, $x, y \in \mathbb{Z}_3$ conține doar următoarele perechi: $(\hat{0}, \hat{1})$, $(\hat{1}, \hat{0})$, $(\hat{2}, \hat{0})$, $(\hat{0}, \hat{2})$. Deci G va fi formată din 4 matrice:

$$e = \begin{pmatrix} \hat{1} & \hat{0} \\ \hat{0} & \hat{1} \end{pmatrix}, a = \begin{pmatrix} \hat{0} & \hat{1} \\ -\hat{1} & \hat{0} \end{pmatrix}, b = \begin{pmatrix} \hat{2} & \hat{0} \\ \hat{0} & \hat{2} \end{pmatrix}, c = \begin{pmatrix} \hat{0} & \hat{2} \\ -\hat{2} & \hat{0} \end{pmatrix}.$$

(iii). Alcătuiind tabla de înmulțire a elementelor lui G , deducem că acesta este un grup :

·	e	a	b	c
e	e	a	b	c
a	a	b	c	e
b	b	c	e	a
c	c	e	a	b

(iv). Pentru a defini morfismul $f: G \rightarrow \mathbb{Z}_4$ vom alcătui tabla adunării în \mathbb{Z}_4 :

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

Vom pune $f(e) = \hat{0}$, $f(a) = \hat{1}$, $f(b) = \hat{2}$ și $f(c) = \hat{3}$. Se verifică imediat faptul că $f(x \cdot y) = f(x) + f(y)$, (\forall) $x, y \in G$ (prin compararea celor două tabele) și se observă că f este și bijectivă. Astfel, $(G, \cdot) \approx (\mathbb{Z}_4, +)$.

4.13. (i). Se verifică axiomele grupului prin calcule simple (elementul

neutru este $E = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix} \in M$, și deoarece dacă $A \in M$, $A = \begin{pmatrix} a & 0 & ib \\ 0 & 0 & 0 \\ ib & 0 & a \end{pmatrix} \Rightarrow A$

este simetrizabilă deoarece $A' = \begin{pmatrix} \frac{a}{a^2+b^2} & 0 & i\frac{-b}{a^2+b^2} \\ 0 & 0 & 0 \\ i\frac{-b}{a^2+b^2} & 0 & \frac{a}{a^2+b^2} \end{pmatrix} \in M$ verifică faptul că

$AA' = A'A = E$).

(ii). Faptul că $(\mathbb{C}^*, \cdot) \approx (M, \cdot)$ este evident deoarece $f: \mathbb{C}^* \rightarrow M$,

$f(a + ib) = \begin{pmatrix} a & 0 & ib \\ 0 & 0 & 0 \\ ib & 0 & a \end{pmatrix}$ este izomorfism de grupuri. Atunci $f((a + ib)^n) = A^n$,

oricare ar fi $n \in \mathbb{N}$.

În cazul nostru, $A = \begin{pmatrix} 1 & 0 & i \\ 0 & 0 & 0 \\ i & 0 & 1 \end{pmatrix} = f(1+i) \Rightarrow A^{2002} = f((1+i)^{2002})$. Dar

$$\begin{aligned} 1+i &= \sqrt{2} \left(\cos \frac{\pi}{4} + i \sin \frac{\pi}{4} \right) \Rightarrow (1+i)^{2002} = \sqrt{2}^{2002} \left(\cos \frac{\pi}{4} + i \sin \frac{\pi}{4} \right)^{2002} = \\ &= 2^{1001} \left(\cos \frac{2002\pi}{4} + i \sin \frac{2002\pi}{4} \right) = 2^{1001} \left[\cos \left(500\pi + \frac{\pi}{2} \right) + i \sin \left(500\pi + \frac{\pi}{2} \right) \right] = \\ &= 2^{1001} \left(\cos \frac{\pi}{2} + i \sin \frac{\pi}{2} \right) = 2^{1001} (0+i) \Rightarrow \\ \Rightarrow A^{2002} &= f(0+i \cdot 2^{1001}) = \begin{pmatrix} 0 & 0 & i2^{1001} \\ 0 & 0 & 0 \\ i2^{1001} & 0 & 0 \end{pmatrix}. \end{aligned}$$

4.14. Se verifică axiomele grupului pentru mulțimile de matrice de la (i) și (ii) iar pentru (iii) se verifică condițiile de subgrup.

Izomorfismele căutate sunt :

- $f: \mathbb{Z} \rightarrow M, f(k) = D_k = \begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix}$ pentru (i);
- $g: \mathbb{Z} \rightarrow M, f(k) = M_k = \begin{pmatrix} 1 & 1 & 2k+1 \\ 0 & 0 & 1 \\ 0 & 0 & 1 \end{pmatrix}$ pentru (ii);
- $h: \mathbb{R} \rightarrow M, h(a) = A_a = \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}$ pentru (iii).

4.15. (i). Notăm cu $M(a) = \begin{pmatrix} 2-a & a-1 \\ 2(1-a) & 2a-1 \end{pmatrix} \in M, a \in \mathbb{R}^*$.

Dacă $a, b \in \mathbb{R}^* \Rightarrow M(a)M(b) = M(ab)$, deci M este parte stabilă în raport cu înmulțirea matricelor. Elementul unitate este $M(1) = I_2$ și $M(a)^{-1} = M(1/a)$, $(\forall) a \in \mathbb{R}^*$, deci (M, \cdot) este grup.

În mod evident $f: \mathbb{R}^* \rightarrow M, f(a) = M(a), (\forall) a \in \mathbb{R}^*$ este izomorfism de grupuri.

(ii). Prin inducție se verifică faptul că $M(a^n) = (M(a))^n$, oricare ar fi $n \in \mathbb{N}$ și $a \in \mathbb{R}^*$.

O altă posibilitate de a calcula $(M(a))^n$ este folosind izomorfismul f :

$$f(a^n) = f(a)^n = (M(a))^n \Rightarrow (M(a))^n = \begin{pmatrix} 2-a^n & a^n-1 \\ 2(1-a^n) & 2a^n-1 \end{pmatrix}$$

4.16. Se verifică cu ușurință axiomele grupului.

Funcțiile $f_{\alpha,\beta} : G \rightarrow G$, $f_{\alpha,\beta}(A) = \begin{pmatrix} 1 & \alpha x & \alpha\beta y \\ 0 & 1 & \beta z \\ 0 & 0 & 1 \end{pmatrix}$, cu $\alpha, \beta \neq 0$, oricare ar fi

matricea $A = \begin{pmatrix} 1 & x & y \\ 0 & 1 & z \\ 0 & 0 & 1 \end{pmatrix}$ din G , sunt automorfismele lui G . Cum α și β sunt

oarecare, atunci mulțimea automorfismelor este infinită.

4.17. (i). Se verifică imediat că $A(x)A(y) = A(2xy) \in M$, pentru orice $x, y \in \mathbb{R}$.

Elementul neutru se obține pentru $x = \frac{1}{2}$, deci $E = A(\frac{1}{2}) \in M$.

Inversa lui $A(x)$ este $A(\frac{1}{4x}) \in M$ și există pentru orice $x \neq 0$.

(ii). Fie $f : M \rightarrow \mathbb{R}^*$ izomorfismul cerut. Se caută $f(A(x)) = ax$ și din $f(A(\frac{1}{2})) = 1$, adică $\frac{a}{2} = 1 \Rightarrow a = 2$. Deci $f(A(x)) = 2x$ și se verifică ușor că este izomorfism de grupuri.

4.18. (i). Prin calcul direct se arată că $A^3 = O_3$.

(ii). Se verifică prin calcul că $(\forall) x, y \in \mathbb{R}$, $A_x \cdot A_y = A_{x+y} \in G$, deci G este parte stabilă în raport cu înmulțirea matricelor. Cum $x+y = y+x$ și $(x+y)+z = x+(y+z)$, $(\forall) x, y, z \in \mathbb{R} \Rightarrow A_x A_y = A_y A_x$ și $A_{(x+y)+z} = A_{x+(y+z)} \Rightarrow$ înmulțirea pe G este comutativă și asociativă.

Elementul neutru este $I_3 = A_0 \in G$ iar inversul unui element A_x din G este A_{-x} care este tot din G . Deci (G, \cdot) este grup abelian.

(iii). Definind $f : \mathbb{R} \rightarrow G$, $f(x) = A_x$, se verifică ușor că f este un izomorfism de grupuri.

4.19. Se verifică imediat că M_d este parte stabilă față de înmulțirea matricelor. Asociativitatea este evidentă, elementul neutru este I_2 (care se obține din $a = 1$ și $b = 0$) și deoarece toate matricele din M_d au determinantul nenul, ele vor fi inversabile, iar inversele lor se va observa că sunt din M_d . Astfel, (M_d, \cdot) este grup.

Considerăm că există $f : \mathbb{C}^* \rightarrow M_d$ un izomorfism de grupuri. Acesta va duce un element $a + bi$ într-o matrice din M_d , și anume : $f(a + bi) = \begin{pmatrix} a & db \\ b & a \end{pmatrix}$.

Se deduce imediat că $f(1) = I_2$. Condiția $f((a+bi)(a'+b'i)) = f(a+bi)f(a'+b'i)$ este echivalentă cu :

$$\begin{pmatrix} aa' - bb' & d(ab' + a'b) \\ ab' + a'b & aa' - bb' \end{pmatrix} = \begin{pmatrix} a & db \\ b & a \end{pmatrix} \begin{pmatrix} a' & db' \\ b' & a' \end{pmatrix} = \begin{pmatrix} aa' + dbb' & d(ab' + a'b) \\ ab' + a'b & aa' + dbb' \end{pmatrix} \text{ ceea ce}$$

este posibil doar dacă $d = -1$, deci $f(a + bi) = \begin{pmatrix} a & -b \\ b & a \end{pmatrix}$ (faptul că f în această formă este o bijecție se verifică imediat).

4.20. Deoarece elementele lui G_n se pot caracteriza și prin aceea că suma elementelor de pe linie și de pe fiecare coloană este egală cu 1, se deduce imediat că (G_n, \cdot) este grup (pentru $A \in G_n, A^{-1} = A^t \in G_n$).

Fie acum $A \in G_n$. Fixând coloana i în matricea A , există o unică linie j în această matrice cu proprietatea că elementul de la intersecția lor este 1, adică $a_{ji} = 1$. Definim atunci permutarea $\sigma_A \in S_n$ asociind fiecărui element $i \in \{1, 2, \dots, n\}$ elementul $j \in \{1, 2, \dots, n\}$ definit ca mai sus, adică $\sigma_A(i) = j \Leftrightarrow a_{ji} = 1$. Se probează acum imediat că asocierea $A \rightarrow \sigma_A$ este izomorfismul căutat.

4.21. (i). Se verifică axiomele grupului ($e = 4 \in G$ este elementul neutru; dacă $x \in G \setminus \{4\}$, atunci simetricul lui x este $x' = \frac{3x-8}{x-3} = 3 + \frac{1}{x-3} \in G$).

(ii). Se impune ca $f(1) = 4$ și $f(xy) = f(x) \circ f(y)$, ($\forall x, y \in G \Leftrightarrow a + b = 4$ și $axy + b = (ax + b) \circ (ay + b) \Leftrightarrow a + b = 4$ și $a = a^2 \Rightarrow a = 1$ și $b = 3 \Rightarrow f(x) = x + 3$).

(iii). Se procedează prin inducție și se obține $x^n = (x-3)^n + 3$ (deoarece $f^{-1}(x) = x - 3$ și $f^{-1} : G \rightarrow \mathbb{R}_+^*$ este izomorfism și deci $f^{-1}(x^n) = (f^{-1}(x))^n \Rightarrow (f^{-1}(x))^n = (x-3)^n \Rightarrow x^n - 3 = (x-3)^n$).

4.22. (i). Deoarece ($\forall x, y \in G \ x \circ y = (x-5)(y-5) + 5 > 5$, G este parte stabilă în raport cu " \circ "; asociativitatea rezultă prin calcul . Comutativitatea rezultă din comutativitatea înmulțirii și adunării numerelor reale. Elementul neutru este $e = 6 \in G$ iar dacă $x \in G \setminus \{6\}$, atunci $x^{-1} = \frac{5x-24}{x-5} = 5 + \frac{1}{x-5} \in G$.

Deci (G, \circ) este grup comutativ.

(ii). Căutăm un izomorfism $f : (\mathbb{R}_+^*, \cdot) \rightarrow (G, \circ)$, de forma $f(x) = ax + b$.

Din $f(xy) = f(x) \circ f(y) \Rightarrow axy + b = (ax + b) \circ (ay + b) = 5(ax + b) - 5(ay + b) + 30 \Rightarrow a = 1$ și $b = 5 \Rightarrow f(x) = x + 5$ (se verifică $f(1) = 6$). Evident f este bijectivă, astfel avem izomorfismul dorit.

(iii). Cum $(\mathbb{R}_+^*, \cdot) \approx (\mathbb{R}, +)$ ($h : (0, \infty) \rightarrow \mathbb{R}, h(x) = \ln x$ este izomorfism sau inversul acestuia $g : \mathbb{R} \rightarrow (0, \infty), g(x) = e^x$ este izomorfism) $\Rightarrow (\mathbb{R}, +) \approx (G, \circ)$.

(iv). Fie $t = f \circ g : \mathbb{R} \rightarrow G \Rightarrow t(x) = e^x + 5, (\forall) x \in \mathbb{R}$. Cum f și g sunt bijecții, rezultă că și t este bijecție, adică există $t^{-1} : (G, \circ) \rightarrow (\mathbb{R}, +)$, $t^{-1}(x) = \ln(x-5)$.

Atunci $t^{-1}(x^n) = n t^{-1}(x) \Leftrightarrow \ln(x^n - 5) = n \ln(x - 5) \Leftrightarrow x^n - 5 = (x - 5)^n$ de unde rezultă că $x^n = (x - 5)^n + 5$.

4.23. Observăm că " \circ " se poate scrie astfel: $A \circ B = (A+I_2)(B+I_2) - I_2$.

Dacă $A, B \in S \Rightarrow A+I_2, B+I_2$ sunt inversabile $\Rightarrow A \circ B + I_2$ este inversabilă, deci $A \circ B \in S$, adică S este parte stabilă în raport cu " \circ ". Se observă că $O_2 \in S$ (deoarece $O_2+I_2 = I_2$ este inversabilă) iar $A \circ O_2 = A = O_2 \circ A$, deci O_2 este elementul neutru.

Dacă $A \in S, A \neq O_2$ și $A \circ B = O_2 \Rightarrow (A+I_2)(B+I_2) = I_2 \Rightarrow B+I_2$ este inversabilă în $M_2(\mathbb{R}) \Rightarrow B \in S$ și $B+I_2$ este inversul la dreapta al lui $A+I_2$ în $M_2(\mathbb{R})$. Analog, din $C \circ A = O_2 \Rightarrow C \in S$ și $C+I_2$ este inversul la stânga al lui $A+I_2$ în $M_2(\mathbb{R})$. Atunci $B+I_2 = C+I_2$, de unde $B = C$, deci A este inversabilă în raport cu legea " \circ " și $A^{-1} = (A+I_2)^{-1} - I_2$.

Astfel, (S, \circ) este grup.

Fie $f : (S, \circ) \rightarrow U(M_2(\mathbb{R}), \cdot)$ definită prin $f(A) = A+I_2$; se verifică ușor faptul că f este un izomorfism de grupuri.

4.24. (i). Fie $x \in G$ și $x_2, \dots, x_n \in G \setminus \{1\}$ a.î. $x \cdot x_2 \cdot \dots \cdot x_n \neq 1 \Rightarrow (\exists) x_{n+1} \in G$ cu $x \cdot x_2 \cdot \dots \cdot x_n = x_{n+1}^n \Rightarrow x = x_{n+1}^n \cdot x_n^{-1} \cdot \dots \cdot x_2^{-1}$. Cum $x_{n+1}^n, x_n^{-1}, \dots, x_2^{-1} \in G \setminus \{1\} \Rightarrow (\exists) y \in G, x = x_{n+1}^n \cdot x_n^{-1} \cdot \dots \cdot x_2^{-1} = y^n$.

(ii). $(\forall) x_1, x_2, \dots, x_n \in \mathbb{R}_+^* \setminus \{1\}, (\exists) x_{n+1} = \sqrt[n]{x_1 \cdot \dots \cdot x_n} \in \mathbb{R}_+^*$ a.î. $x_1 x_2 \cdot \dots \cdot x_n = x_{n+1}^n$.

(iii). (\mathbb{R}_+^*, \cdot) nu are proprietatea $g(n), (\forall) n \in \mathbb{N}$, deci $(\mathbb{R}_+^*, \cdot) \not\cong (\mathbb{R}^*, \cdot)$.

4.25. (i). Fie $x, y \in G$. Atunci $f(xy) = f(x)f(y)$ implică $(xy)^3 = x^3 y^3$, de unde, înmulțind la stânga cu x^{-1} și la dreapta cu y^{-1} , obținem $(yx)^2 = x^2 y^2$. Dar $x^4 y^4 = (y^2 x^2)^2 = [(xy)^2]^2$ și $(xy)^4 = x(yx)^3 y \Rightarrow x^3 y^3 = (yx)^3$. Atunci $(xy)^3 = (yx)^3 \Rightarrow f(xy) = f(yx)$ și cum f este injectivă, rezultă că $xy = yx, (\forall) x, y \in G$, adică G este abelian.

(ii). Conform celor de mai sus $(xy)^2 = y^2 x^2$ și $(yx)^2 = x^2 y^2, (\forall) x, y \in G$. Atunci, $y(xy)^2 = y^3 x^2 \Rightarrow (yx)^2 y = y^3 x^2$. Dar $(yx)^2 y = x^2 y^3$, de unde rezultă că $y^3 x^2 = x^2 y^3, (\forall) x, y \in G$. Deoarece f este surjectivă, $(\forall) z \in G$ există $y \in G$ a.î. $f(y) = z$, adică $y^3 = z$. Atunci $x^2 z = z x^2, (\forall) x, z \in G \Rightarrow x^2 \in Z(G)$ și $z^2 x^2 = z x^2 z \Rightarrow (xz)^2 = z x^2 z \Leftrightarrow x z x z = z x^2 z \Leftrightarrow z x = x z, (\forall) x, z \in G$, adică G este abelian.

4.26. Fie H_1 un subgrup propriu al lui G . Atunci $f(H_1) = f(H \cap H_1)$, deci $f(H_1)$ este subgrup al lui G . Pentru a arăta că f nu este morfism, fie $a \in H \setminus \{1\}$ și $b \in G \setminus H$. Atunci $ab \in G \setminus H$ și $f(ab) = 1 \neq a \cdot 1 = f(a) f(b)$, deci f nu este un morfism de grupuri.

4.27. (i). Din $x^n = 1 \Rightarrow (f(x))^n = 1 \Rightarrow o(f(x)) \mid n$.

(ii). Dacă $o(x) = \infty \Rightarrow x^n \neq 1, (\forall) n \in \mathbb{N}^* \Rightarrow (f(x))^n \neq 1, (\forall) n \in \mathbb{N}^* \Rightarrow o(f(x)) = \infty$. Dacă $o(x) = n \Rightarrow d = o(f(x)) \mid n$ (conform cu (i)).

Pe de altă parte, $f(x^d) = (f(x))^d = 1 = f(1) \Rightarrow x^d = 1 \Rightarrow n \mid d$, adică $n = d$.

4.28. (i). Dacă $f, g \in H = \text{Hom}(G_1, G_2)$ și $x, y \in G_1$, atunci $(fg)(xy) = f(xy)g(xy) = f(x)f(y)g(x)g(y) = f(x)g(x)f(y)g(y) = (fg)(x)(fg)(y)$, adică $fg \in H$.

Asociativitatea înmulțirii este imediată; elementul neutru este morfismul nul $1: G_1 \rightarrow G_2, 1(x) = 1, (\forall) x \in G_1$.

Pentru $f \in H$, definind $f': G_1 \rightarrow G_2, f'(x) = (f(x))^{-1}, (\forall) x \in G_1$ se probează imediat că f' este simetricul lui f în H , de unde deducem că H este grup.

Deoarece G_2 este comutativ rezultă că H este comutativ.

(ii). Pentru $x \in G_2$ definind $f_x: \mathbb{Z} \rightarrow G_2, f_x(n) = nx, (\forall) n \in \mathbb{Z}$, se verifică imediat că $f_x \in \text{Hom}(\mathbb{Z}, G_2)$.

De asemenea, se probează ușor că $\varphi: G_2 \rightarrow \text{Hom}(\mathbb{Z}, G_2), \varphi(x) = f_x, (\forall) x \in G_2$ este izomorfism de grupuri.

(iii). Fie $f \in \text{Hom}(\mathbb{Z}_m, \mathbb{Z}_n)$. Cum $(\mathbb{Z}_m, +)$ este grup ciclic generat de $\hat{1}$, atunci f este determinat de fapt de $f(\hat{1})$ (mai precis, dacă $\hat{x} \in \mathbb{Z}_m \Rightarrow f(\hat{x}) = x f(\hat{1})$).

Dacă notăm $f(\hat{1}) = \bar{b}$ (clasa lui b în \mathbb{Z}_n), atunci $\bar{0} = f(\hat{0}) = f(m\hat{1}) = m\bar{b}$, adică $\bar{0} = m\bar{b}$.

Reciproc, dacă alegem $\bar{a} \in \mathbb{Z}_n$ a.î. $\bar{0} = m\bar{a}$, atunci $g: \mathbb{Z}_m \rightarrow \mathbb{Z}_n, g(\hat{x}) = x\bar{a}$ este morfism de grupuri.

Să găsim acum numărul claselor $\bar{a} \in \mathbb{Z}_n$ a.î. $\bar{0} = m\bar{a}$ (putem presupune că $a < n$).

Din $\bar{0} = m\bar{a} \Rightarrow ma \equiv 0 \pmod{n} \Rightarrow (\exists) b \in \mathbb{Z}$ a.î. $ma = nb$.

Dacă $d = (m, n)$, atunci dacă $d = 1 \Rightarrow ma = nb \Rightarrow \bar{0} = \bar{a}$.

Dacă $d > 1$, tot din $ma = nb$, cum $(m/d, n/d) = 1 \Rightarrow a = \text{multiplu de } n/d$.

Reciproc, dacă a este multiplu de n/d cu $a < n$, atunci $\bar{0} = m\bar{a}$.

Deci $\bar{a} \in \{ \bar{0}, \overline{(n/d)}, \overline{(2n/d)}, \dots, \overline{((d-1)n/d)} \}$.

Rezultă că $\text{Hom}(\mathbb{Z}_m, \mathbb{Z}_n)$ este ciclic, generat de morfismul corespunzător clasei lui (n/d) și cum are d elemente el va fi izomorf cu $(\mathbb{Z}_d, +)$.

4.29. Evident, $f_n \circ f_m = f_m \circ f_n = f_{m+n} \in G$. Elementul neutru este $f_0 = 1_{(\mathbb{Z}, +)}$ iar inversa funcției f_n este f_n . Operația de compunere a funcțiilor fiind asociativă rezultă că (G, \circ) este grup.

Se verifică fără dificultate că $F: (\mathbb{Z}, +) \rightarrow (G, \circ)$, $F(n) = f_n$ este un izomorfism de grupuri.

4.30. (i). Se verifică imediat.

(ii). Fie $\varphi: \mathbb{Z} \rightarrow \mathbb{Z}$ un morfism. Notăm cu $n = \varphi(1)$. Se arată ușor prin inducție matematică: $\varphi(m) = nm$, $(\forall) m \in \mathbb{Z} \Rightarrow \varphi(m) = f_n(m) \Rightarrow \varphi = f_n$.

(iii). Evident, $f_1 = 1_{\mathbb{Z}}$ și $f_{-1} = -1_{\mathbb{Z}}$ sunt izomorfisme. Orice morfism $f_m(x) = mx$ cu $m \neq \pm 1$ nu este surjectiv deoarece $\text{Im } f_m = \{mk \mid k \in \mathbb{Z}\} \neq \mathbb{Z}$.

4.31. (i). Dacă $a, b \in (-k, k)$ atunci se verifică imediat că $a \circ b \in (-k, k)$ și că \circ este asociativă.

Elementul neutru este 0, opusul lui x este $-x$, deci $(-k, k)$ este grup abelian.

(ii). $f(t) = \int_0^t \frac{dx}{k^2 - x^2} = \frac{1}{2} \ln \frac{k+t}{k-t}$ și se verifică faptul că $f(x \circ y) = f(x) + f(y)$, deci f este morfism de grupuri de la (G, \circ) la $(\mathbb{R}, +)$. Pentru $x \in (-k, k)$, $f'(x) = \frac{1}{k^2 - x^2} > 0$, adică f este strict crescătoare, deci injectivă. Cum f este continuă pe acest interval și $\lim_{x \rightarrow -\infty} f(x) = -\infty$ și $\lim_{x \rightarrow \infty} f(x) = \infty$, rezultă că f este surjectivă, deci bijectivă. Deci f este un izomorfism de grupuri.

4.32. Fie $f: (\mathbb{R}, +) \rightarrow (\mathbb{R}, \circ)$, $f(x) = \text{sh } x$. Avem $f(0) = 0$, $f(x + y) = \text{sh}(x + y) = \text{sh } x \text{ ch } y + \text{sh } y \text{ ch } x$. Cum $\text{ch}^2 x - \text{sh}^2 x = 1 \Rightarrow \text{ch}^2 x = 1 + \text{sh}^2 x$ și cum cosinusul hiperbolic este o funcție pozitivă $\Rightarrow \text{ch } x = \sqrt{1 + \text{sh}^2 x}$.

Deci $\text{sh } x \circ \text{sh } y = \text{sh } x \sqrt{1 + \text{sh}^2 y} + \text{sh } y \sqrt{1 + \text{sh}^2 x} = \text{sh } x \text{ ch } y + \text{sh } y \text{ ch } x = \text{sh}(x + y)$, astfel că f verifică condițiile unui morfism de grupuri și este și o bijecție (deoarece funcția sh este o bijecție). Astfel (\mathbb{R}, \circ) este imaginea printr-un izomorfism a unui grup, deci va fi și el un grup.

4.33. (i). Fie $G' = \{0\}$. Atunci $f_{G'}(0) = 1$ verifică condiția din enunț.

(ii). Fie $G' \leq G = (\mathbb{R}, +)$, $G' \neq \{0\}$.

Fie $\alpha \in G' \setminus \{0\}$, $\alpha \in M$. Atunci $f(\alpha) = \operatorname{tg} \alpha = -\frac{1}{a}$. Cum $f_{G'}$ este morfism avem $f(0) = 1 \Rightarrow f(\alpha - \alpha) = 1 \Rightarrow f(\alpha) \cdot f(-\alpha) = 1$.

Dacă $-\alpha \in M \Rightarrow \operatorname{tg}(-\alpha) = -\frac{1}{a} \Rightarrow -\operatorname{tg} \alpha = -\frac{1}{a} \Rightarrow \frac{1}{a} = -\frac{1}{a}$, fals. Deci $-\alpha \notin M \Rightarrow f(-\alpha) = -a \sin \alpha + \cos \alpha \Rightarrow 1 = f(\alpha) \cdot f(-\alpha) = -\frac{1}{a}(-a \sin \alpha + \cos \alpha) \Rightarrow \sin \alpha - \frac{1}{a} \cos \alpha = 1$ și înlocuind pe $-\frac{1}{a}$ cu $\operatorname{tg} \alpha$, obținem $2 \sin \alpha = 1 \Rightarrow \sin \alpha = \frac{1}{2} \Rightarrow \cos \alpha = -\frac{a}{2}$. Înlocuind în relația $\sin^2 \alpha + \cos^2 \alpha = 1$, obținem $(-\frac{a}{2})^2 + (\frac{1}{2})^2 = 1 \Rightarrow a = \pm \sqrt{3}$.

$$G' \leq \mathbb{R} \text{ și } \alpha \in G' \Rightarrow 2\alpha \in G' \text{ și } \operatorname{tg} 2\alpha = \frac{2\operatorname{tg} \alpha}{1 - \operatorname{tg}^2 \alpha} = \frac{-\frac{2}{a}}{1 - \frac{1}{a^2}} = \frac{-2a}{a^2 - 1} \quad \text{Dacă}$$

$2\alpha \in M \Rightarrow f(2\alpha) = \operatorname{tg} 2\alpha = -\frac{1}{a} \Rightarrow 2a^2 = a^2 - 1 \Rightarrow a^2 = -1$, absurd, deci $2\alpha \notin M$, și

atunci $f(2\alpha) = a \sin 2\alpha + \cos 2\alpha$. Dacă $-2\alpha \in M$ atunci $\operatorname{tg}(-2\alpha) = -\frac{1}{a} \Rightarrow \frac{2a}{a^2 - 1} =$

$= -\frac{1}{a} \Rightarrow 3a^2 = 1 \Rightarrow a = \pm \frac{1}{\sqrt{3}}$ - absurd. Atunci $-2\alpha \notin M \Rightarrow f(-2\alpha) = -a \sin 2\alpha +$

$\cos 2\alpha \Rightarrow -a^2 \sin^2 2\alpha + \cos^2 2\alpha = 1$ (din $f(2\alpha) \cdot f(-2\alpha) = 1$) $\Rightarrow -a^2 \sin^2 2\alpha = \sin^2 2\alpha \Rightarrow (1 + a^2) \sin^2 2\alpha = 0$ - fals.

Deci $M \cap G' = \emptyset$. Fie $x \in G' \setminus \{0\}$, atunci $-x \in G'$ și $f(x) \cdot f(-x) = 1 \Rightarrow (a^2 + 1) \sin^2 x = 0 \Rightarrow x = k\pi \Rightarrow G' \subset \pi\mathbb{Z} \Rightarrow \cup G' \subset \pi\mathbb{Z}$. Deoarece $\pi\mathbb{Z}$ este subgrup al lui $(\mathbb{R}, +)$, considerând atunci restricția lui f la $\pi\mathbb{Z}$, $f_{\pi\mathbb{Z}}: \pi\mathbb{Z} \rightarrow H$, avem $f_{\pi\mathbb{Z}}(n\pi + k\pi) = (-1)^{n+k} = f(n\pi) \cdot f(k\pi) \Rightarrow \cup G' = \pi\mathbb{Z}$.

4.34. Fie $f: \mathbb{Q} \rightarrow \mathbb{Z}$ un morfism de grupuri, adică $f(x+y) = f(x) + f(y)$, $(\forall) x, y \in \mathbb{Q}$.

Dacă $n \in \mathbb{N}^*$, $nf(1/n) = f(n \cdot 1/n) = f(1) \Rightarrow f(1/n) = (1/n) \cdot f(1) \in \mathbb{Z} \Rightarrow f(1) = 0$. Însă $f(m/n) = mf(1/n) = (m/n) \cdot f(1) = 0$, $(\forall) m/n \in \mathbb{Q} \Rightarrow f = 0$, adică $\operatorname{Hom}(\mathbb{Q}, \mathbb{Z})$ este format numai din morfismul nul.

4.35. Dacă $f : \mathbb{Z}_n \rightarrow \mathbb{Z}_n$ este un morfism de grupuri, atunci $(\forall) \hat{x} \in \mathbb{Z}_n$, avem $f(\hat{x}) = x \cdot f(\hat{1})$.

Însă $0 = f(\hat{0}) = f(\hat{n}) = nf(\hat{1})$, deci $f(\hat{1}) = 0$, adică f este morfismul nul.

4.36. Fie $g : G \rightarrow G$, $g(x) = x^{-1}f(x)$, $(\forall) x \in G$. Să demonstrăm că g este o aplicație injectivă.

Dacă $x, y \in G$ și $g(x) = g(y) \Rightarrow x^{-1}f(x) = y^{-1}f(y) \Rightarrow yx^{-1} = f(x) \cdot (f(y))^{-1} \Rightarrow yx^{-1} = f(y) \cdot f(x^{-1}) = f(yx^{-1})$ și cum f nu are punct fix decât pe 1, deducem că $yx^{-1} = 1$, adică $x = y$, deci g este injectivă. Deoarece G este mulțime finită, atunci g va fi și surjectivă.

Deci orice element al lui G este de forma $x^{-1}f(x)$ cu $x \in G$.

Fie acum $y \in G$, $y = x^{-1}f(x)$ cu $x \in G$. Atunci $f(y) = f(x^{-1}f(x)) = f(x^{-1})f(f(x)) = (f(x))^{-1}x = (x^{-1}f(x))^{-1} = y^{-1}$, adică $f(y) = y^{-1}$.

Cum f este morfism de grupuri, $(\forall) y, z \in G$ va trebui să avem $f(yz) = f(y)f(z) \Leftrightarrow (yz)^{-1} = y^{-1}z^{-1} \Leftrightarrow yz = zy$, adică G este abelian.

4.37. Evident, există două automorfisme ale lui $G : f(x) = x$, $(\forall) x \in G$ și $g(x) = x^{-1}$. Deoarece în G există un singur automorfism $\Rightarrow f = g \Rightarrow f(x) = g(x)$, $(\forall) x \in G \Rightarrow x = x^{-1}$, $(\forall) x \in G \Rightarrow x^2 = 1$, $(\forall) x \in G$.

4.38. Deoarece f și g sunt morfisme rezultă că $f(xy) = f(x)f(y)$ și $g(xy) = g(x)g(y)$, $(\forall) x, y \in G \Rightarrow (xy)^4 = x^4y^4$ și $(xy)^8 = x^8y^8$, $(\forall) x, y \in G$.

Din prima relație rezultă că $(yx)^3 = x^3y^3 \Rightarrow (yx)^4 = (yx)(x^3y^3) = yx^4y^3$ și cum $(yx)^4 = y^4x^4 (= f(yx)) \Rightarrow x^4y^3 = y^3x^4$, $(\forall) x, y \in G$. (1)

Din a doua relație $(xy)^8 = x^8y^8 \Rightarrow (yx)^7 = x^7y^7 \Rightarrow (yx)^8 = (yx)(x^7y^7) = yx^8y^7$ și cum $(yx)^8 = y^8x^8 (= g(yx)) \Rightarrow x^8y^7 = y^7x^8$, $(\forall) x, y \in G$. (2)

Din (1) și (2) $\Rightarrow x^8$ comută cu y^3 și $y^7 \Rightarrow x^8$ comută cu y (deoarece $(3,7) = 1$, $(\forall) y \in G$). Cum g este surjectivă, $(\forall) z \in G (\exists) x \in G$ a.î. $g(x) = x^8 = z \Rightarrow zy = yz$, $(\forall) z, y \in G$, deci G este comutativ.

4.39. (i). Fie $g(x) = xf(x)$. Cum g este morfism (din ipoteză) $\Rightarrow g(xy) = g(x)g(y)$, $(\forall) x, y \in G \Rightarrow xyf(xy) = xf(x)yf(y)$, $(\forall) x, y \in G \Rightarrow xyf(x)f(y) = xf(x)yf(y)$, $(\forall) x, y \in G \Rightarrow yf(x) = f(x)y$, $(\forall) x, y \in G \Rightarrow f(x) \in Z(G)$. (1)

Dacă notăm $h(x) = x^2f(x) \Rightarrow h(x) = xg(x)$. Cum $g \in \text{End}(G)$ rezultă ca mai sus că $g(x) \in Z(G) \Leftrightarrow xf(x) \in Z(G)$. (2)

Din (1) și (2) $\Rightarrow x \in Z(G)$, $(\forall) x \in G$ deoarece $Z(G) \leq G \Rightarrow G$ este abelian.

(ii). Fie $g(x) = x^2f(x)$. Deoarece g este morfism (din ipoteză) $\Rightarrow g(xy) = g(x)g(y)$, $(\forall) x, y \in G \Rightarrow (xy)^2f(xy) = x^2f(x)y^2f(y)$, $(\forall) x, y \in G \Rightarrow xyxyf(x)f(y) = x^2f(x)y^2f(y)$, $(\forall) x, y \in G \Rightarrow yxyf(x) = xf(x)y^2$, $(\forall) x, y \in G$. (*)

Deoarece $h(x) = x^4 f(x)$ este morfism $\Rightarrow h(xy) = h(x)h(y)$, $(\forall) x, y \in G \Rightarrow (xy)^4 f(xy) = x^4 f(x) y^4 f(y)$, $(\forall) x, y \in G$. Cum $h(x) = x^2 g(x) \Rightarrow xyg(x) = xg(x)y^2$, $(\forall) x, y \in G \Leftrightarrow yxyx^2 f(x) = x^3 f(x)y^2$, $(\forall) x, y \in G$. (**)

Din (*) pentru $x = y \Rightarrow x^3 f(x) = xf(x)x^2 \Rightarrow x^2 f(x) = f(x)x^2$, $(\forall) x \in G$.

Tot din (*) avem $(f(x))^{-1}(yxy)^{-1} = y^{-2}(f(x))^{-1}x^{-1}$, $(\forall) x, y \in G$, iar cu (**) avem $(f(x))^{-1}(yxy)^{-1} yxyx^2 f(x) = y^{-2}(f(x))^{-1}x^{-1}x^3 f(x)y^2$, $(\forall) x, y \in G \Rightarrow (f(x))^{-1}x^2 f(x) = y^{-2} (f(x))^{-1}x^2 f(x)$, $(\forall) x, y \in G$, și cum $f(x)$ comută cu x^2 , deci comută și cu $(f(x))^{-1} \Rightarrow x^2 = y^{-2} x^2 y^2$, $(\forall) x, y \in G \Rightarrow y^2 x^2 = x^2 y^2$, $(\forall) x, y \in G$.

Punând în (*) x^2 în locul lui x rezultă că $yx^2 y f(x) = x^2 f(x)y^2$, $(\forall) x, y \in G \Rightarrow yx^2 y f(x) = x^2 y^2 f(x)$, $(\forall) x, y \in G \Rightarrow yx^2 = x^2 y$, $(\forall) x, y \in G \Rightarrow x^2 \in Z(G)$, $(\forall) x \in G \Rightarrow yxyf(x) = y^2 xf(x)$, $(\forall) x, y \in G \Rightarrow xy = yx$, $(\forall) x, y \in G$, deci G este comutativ.

4.40. Presupunem că f are un singur punct fix (acesta este 1 elementul neutru al lui G , deoarece $f(1) = 1$).

Fie $F(x) = F(y) \Rightarrow x^{-1}f(x) = y^{-1}f(y) \Rightarrow f(x)(f(y))^{-1} = xy^{-1} \Rightarrow f(xy^{-1}) = xy^{-1} \Rightarrow xy^{-1} = 1 \Rightarrow x = y \Rightarrow F$ este injectivă. Dar cum G este finit $\Rightarrow F$ este surjecție $\Rightarrow F$ este bijecție.

Reciproc, fie F bijecție.

Dacă $x \in G \setminus \{1\}$ este un punct fix al lui $f \Rightarrow f(x) = x \Rightarrow x^{-1}f(x) = 1 = =^{-1}f(1) \Rightarrow F(x) = F(1) \Rightarrow x = 1$ deoarece F este injectivă (vezi problema 4.36.).

4.41. Fie $a \in G \setminus H \Rightarrow a^{-1} \in G \setminus H$. Fie $x \in H$, arbitrar. Rezultă imediat că $a^{-1}x = b \in G \setminus H \Rightarrow x = ab$.

Avem $f(x) = f(ab) = f(a)f(b) = g(a)g(b) = g(ab) = g(x)$, $(\forall) x \in H$.

Deci $f = g$ pe $H \Rightarrow f = g$ pe G (în esență totul rezultă din problema 2.34.).

4.42. Fie $x, y \in G$ iar $z = x^{-1}y \Leftrightarrow y = xz$. Cum f este surjecție $(\exists) t \in G$ a.î. $z = t^n$.

Atunci avem $x^{n-1}y = x^{n-1}xz = x^{n-1}x t^n = x^n t^n = f(x)f(t) = f(xt) = (xt)^n = = (xt)(xt) \dots (xt)(xt) = x(tx)(tx) \dots (tx)t = x(tx)^{n-1} t x x^{-1} = x(tx)^n x^{-1} = x t^n x^n x^{-1} = y x^{n-1}$, adică $x^{n-1} \in Z(G)$.

4.43. Fie $a, c \in G$ elemente arbitrare. Deoarece f și g sunt morfisme atunci $f(ac) = f(a)f(c)$ și $g(ac) = g(a)g(c) \Rightarrow (ac)^n = a^n c^n$ și $(ac)^{n+1} = a^{n+1} c^{n+1}$. Dar $(ac)^{n+1} = (ac)^n (ac) = a^n c^n ac \Rightarrow a^n c^n ac = a^{n+1} c^{n+1} \Rightarrow (a^n)^{-1} (a^n c^n ac) c^{-1} = = (a^n)^{-1} (a^{n+1} c^{n+1}) c^{-1} \Rightarrow c^n a = ac^n$.

Fie $a, b \in G$ arbitrare. Deoarece f este surjectivă, există $c \in G$ a.î. $f(c) = b$, deci $b = c^n$. Atunci, folosind relația de mai sus, obținem : $ab = ba$, $(\forall) a, b \in G$, deci G este abelian.

4.44. Fie $f : (\mathbb{Q}, +) \rightarrow (S_n, \circ)$ un morfism de grupuri și $x \in \mathbb{Q}$ iar $\sigma = f\left(\frac{x}{n!}\right) \in S_n$.

Atunci putem scrie $f(x) = f\left(n! \cdot \frac{x}{n!}\right) = \left(f\left(\frac{x}{n!}\right)\right)^{n!} = e$ (conform problemei

3.33., deoarece S_n are $n!$ elemente), adică f este morfismul nul.

4.45. Fie $f : (\mathbb{Z}_p, +) \rightarrow (\mathbb{Z}_p^*, \cdot)$ un morfism de grupuri iar $f(\hat{1}) = \hat{a}$.

Avem $\hat{1} = f(\hat{0}) = f(\hat{p}) = (f(\hat{1}))^p = (\hat{a})^p$. Însă conform teoremei lui Fermat, $\hat{a}^p = \hat{a}$, adică $\hat{a} = \hat{1}$ deci $f(\hat{1}) = \hat{1}$.

Atunci $(\forall) x \in \{0, 1, \dots, p-1\}$, $f(\hat{x}) = (f(\hat{1}))^x = \hat{1}^x = \hat{1}$, deci f este morfismul nul.

4.46. Să presupunem că am definit operația algebrică "*" pe $(1, 2)$ a.î. $((1, 2), *) \approx ((0, \infty), \cdot)$.

Fie $f : (1, 2) \rightarrow (0, \infty)$ acest izomorfism $\Rightarrow f$ este o bijecție și $f(x * y) = f(x)f(y)$ $(\forall) x, y \in (1, 2) \Rightarrow x * y = f^{-1}(f(x)f(y))$, $(\forall) x, y \in (1, 2)$.

Fie $f : (1, 2) \rightarrow (0, \infty)$, $f(x) = \frac{x-1}{2-x}$, $(\forall) x \in (1, 2)$. Se observă că f este

bine definită deoarece $\frac{x-1}{2-x} > 0$, $(\forall) x \in (1, 2)$.

Dacă $y = \frac{x-1}{2-x} \Rightarrow y(2-x) = x-1 \Rightarrow x(y+1) = 2y+1 \Rightarrow x = \frac{2y+1}{y+1}$.

Deci $f^{-1}(y) = \frac{2y+1}{y+1}$, $(\forall) y \in (0, \infty)$. Atunci definim :

$x * y = f^{-1}(f(x)f(y)) = \frac{3xy - 4(x+y) + 6}{2xy - 3(x+y) + 5}$, $(\forall) x, y \in (1, 2)$.

4.47. Dacă $f : (\mathbb{Q}, +) \rightarrow (\mathbb{Q}^*, \cdot)$ este un morfism de grupuri, atunci pentru orice $x, y \in \mathbb{Q}$ avem $f(x+y) = f(x) \cdot f(y)$. Evident $f(-x) = 1/f(x)$, $f(0) = 1$ iar $f(x) = f\left(\frac{x}{2} + \frac{x}{2}\right) = \left(f\left(\frac{x}{2}\right)\right)^2 \geq 0$.

Notând $f(1) = a$ ($a \in \mathbb{Q}$, $a > 0$), avem $f(2) = a^2$ și inductiv $f(n) = a^n$, $(\forall) n \in \mathbb{N}$.

Dacă $n \in \mathbb{N} \Rightarrow f(-n) = 1/f(n) = 1/a^n = a^{-n}$, deci $f(x) = a^x$, $(\forall) x \in \mathbb{Z}$.

De asemenea, $f\left(\underbrace{\frac{1}{n} + \dots + \frac{1}{n}}_{n \text{ ori}}\right) = \left(f\left(\frac{1}{n}\right)\right)^n \Rightarrow a = \left(f\left(\frac{1}{n}\right)\right)^n \Rightarrow f\left(\frac{1}{n}\right) = a^{\frac{1}{n}}$.

Rezultă imediat că dacă și $m \in \mathbb{Z}$, atunci $f\left(\frac{m}{n}\right) = \left(a^{\frac{1}{n}}\right)^m = a^{\frac{m}{n}}$, adică $f(x) = a^x$, $(\forall) x \in \mathbb{Q}$.

4.48. Fie $H < \mathbb{Q}$ un subgrup propriu al lui $(\mathbb{Q}, +)$. Presupunem că $H \approx \mathbb{Q}$ și fie $f: \mathbb{Q} \rightarrow H$ un izomorfism. Acesta va avea forma $f(x) = ax$, $a = f(1) \neq 0$, $(\forall) x \in \mathbb{Q}$. Evident, există $b \in \mathbb{Q} \setminus H$ și deci $f(x) \neq b$, $(\forall) x \in \mathbb{Q} \Rightarrow ax \neq b$, $(\forall) x \in \mathbb{Q} \Rightarrow x \neq b/a$, $(\forall) x \in \mathbb{Q} \Rightarrow b/a \notin \mathbb{Q}$, absurd.

4.49. (i). Dacă $a, x, y \in G$, atunci $\varphi_a(xy) = a(xy)a^{-1} = (axa^{-1})(aya^{-1}) = \varphi_a(x) \cdot \varphi_a(y)$, adică φ_a este morfism de grupuri. Bijectivitatea lui φ_a este imediată, deci $\varphi_a \in \text{Aut}(G)$.

(ii). Dacă $a, b, x \in G \Rightarrow (\varphi_a \circ \varphi_b)(x) = \varphi_a(\varphi_b(x)) = \varphi_a(bxb^{-1}) = abxb^{-1}a^{-1} = (ab)x(ab)^{-1} = \varphi_{ab}(x) \Rightarrow \varphi_a \circ \varphi_b = \varphi_{ab}$ de unde deducem imediat că φ este morfism de grupuri.

(iii). Avem $|\text{Inn}(G)| = 1 \Rightarrow (\forall) a \in G, \varphi_a = 1_G \Rightarrow axa^{-1} = x$, $(\forall) x \in G \Rightarrow ax = xa$, $(\forall) x \in G \Rightarrow Z(G) = G \Rightarrow G$ este comutativ.

4.50. Dacă $f \in Z(\text{Aut}(G))$, în particular $f \in C_{\text{Aut}(G)}(\text{Inn}(G))$, deci $f \circ \varphi_a = \varphi_a \circ f$, $(\forall) a \in G$ (φ_a fiind automorfismul interior) $\Rightarrow f(axa^{-1}) = af(x)a^{-1}$, $(\forall) x \in G \Rightarrow a^{-1}f(a)f(x) = f(x)a^{-1}f(a)$, $(\forall) a, x \in G$.

Deoarece $f(G) = G$ rezultă că $a^{-1}f(a) \in Z(G)$, $(\forall) a \in G \Rightarrow a^{-1}f(a) = 1 \Rightarrow f(a) = a$, $(\forall) a \in G \Rightarrow Z(\text{Aut}(G)) = 1$.

4.51. Excluzând grupurile cu un singur element care satisfac proprietatea din enunț, considerăm un grup (G, \cdot) cu cel puțin două elemente și care au un singur automorfism (acesta va fi în mod necesar morfismul identic).

Pentru fiecare $a \in G$, aplicația $\varphi_a: G \rightarrow G$, $\varphi_a(x) = axa^{-1}$ este un automorfism al lui G , deci trebuie să avem $\varphi_a = 1_G \Leftrightarrow \varphi_a(x) = x \Leftrightarrow axa^{-1} = x \Leftrightarrow ax = xa$, $(\forall) x \in G$. Cum a este arbitrar, rezultă că G este comutativ.

Dar și aplicația $\psi: G \rightarrow G$, $\psi(x) = x^{-1}$ este tot un automorfism al lui G , deci $\psi = 1_G \Leftrightarrow x = x^{-1}$, $(\forall) x \in G \Leftrightarrow x^2 = 1$, $(\forall) x \in G$. Vom demonstra că pe G se poate organiza o structură de \mathbb{Z}_2 -spațiu vectorial. Pentru aceasta vom considera notația aditivă în grupul G și definim operația algebrică externă pe G cu domeniul de operatori în \mathbb{Z}_2 :

$$\lambda x = \begin{cases} 0, & \text{dacă } \lambda = \hat{0} \\ x, & \text{dacă } \lambda = \hat{1} \end{cases}, (\forall) \lambda \in \mathbb{Z}_2 \text{ și } x \in G.$$

Se verifică faptul că sunt îndeplinite axiomele spațiului vectorial.

Evident $(\hat{1} + \hat{1})x = \hat{1}x + \hat{1}x$ deoarece $x + x = 0$ în G , ș.a.m.d.

Fie $B = (x_i)_{i \in I}$ o bază a spațiului vectorial G peste corpul \mathbb{Z}_2 .

Dacă $u : B \rightarrow B$ este o bijecție a bazei B , aplicația $\bar{u} : G \rightarrow G$, $\bar{u}(\sum_{i \in I} \lambda_i x_i) = \sum_{i \in I} \lambda_i u(x_i)$ este un automorfism al spațiului vectorial G (este o

aplicație liniară bijectivă). În particular, \bar{u} este un automorfism al grupului abelian G . Prin urmare, fiecare bijecție a bazei B generează un automorfism al grupului G . Cum G are un singur automorfism, este necesar să existe o singură bijecție a mulțimii B în ea însăși, ceea ce înseamnă că B trebuie să aibă un singur element. Atunci avem izomorfismul de \mathbb{Z}_2 spații vectoriale: $G \approx \mathbb{Z}_2$, ceea ce arată că G este un grup izomorf cu grupul aditiv \mathbb{Z}_2 . Această condiție apărută ca necesară, este și suficientă, căci grupul \mathbb{Z}_2 are un singur automorfism. În concluzie, grupurile cu un singur automorfism sunt grupurile cu un element și grupurile cu două elemente.

4.52. Fie G un grup abelian. Dacă $(\exists) x \in G \setminus \{1\}$ cu $x^2 \neq 1$, rezultă $|\text{Aut}(G)|$ este număr par.

Rămâne să analizăm cazul în care $x^2 = 1$, $(\forall) x \in G$. Atunci, conform problemei anterioare, G este un \mathbb{Z}_2 - spațiu vectorial.

Fie $\{x_1, x_2, \dots, x_k\}$ o bază în G . Atunci pentru $x \in G$ există în mod unic $\alpha_1, \dots, \alpha_k \in \{\hat{0}, \hat{1}\}$ a.î. $x = x_1^{\alpha_1} \cdot x_2^{\alpha_2} \cdot \dots \cdot x_k^{\alpha_k}$.

Cazul 1. $k \geq 2$.

Definim $f : G \rightarrow G$ astfel $f(x_1^{\alpha_1} \cdot x_2^{\alpha_2} \cdot \dots \cdot x_k^{\alpha_k}) = x_1^{\alpha_2} \cdot x_2^{\alpha_1} \cdot x_3^{\alpha_3} \cdot \dots \cdot x_k^{\alpha_k}$. Se arată cu ușurință că $f \in \text{Aut}(G)$ și $f \circ f = 1_G$. Obținem că grupul $(\text{Aut}(G), \circ)$ conține un element de ordin 2, deci $|\text{Aut}(G)|$ este număr par.

Cazul 2. $k=1 \Rightarrow G \approx \mathbb{Z}_2$ și $\text{Aut}(\mathbb{Z}_2) = \{1_{\mathbb{Z}_2}\}$.

Cazul 3. $k=0 \Rightarrow G = \{e\}$ și $\text{Aut}(G) = \{1_G\}$.

Deci grupurile căutate sunt $\{1\}$ și $(\mathbb{Z}_2, +)$.

4.53. Considerăm că $G = \{a^k : k \in \mathbb{Z}\}$. Dacă $o(a) = \infty$, atunci se probează imediat că $f : G \rightarrow (\mathbb{Z}, +)$, $f(a^k) = k$, $(\forall) k \in \mathbb{Z}$ este izomorfism de grupuri iar dacă $o(a) = |G| = n$, atunci $f : G \rightarrow (\mathbb{Z}_n, +)$, $f(a^k) = \hat{k}$, $(\forall) k \in \mathbb{Z}$ este izomorfism de grupuri.

4.54. Dacă (G, \cdot) are un număr finit de subgrupuri, vom arăta mai întâi că orice element din G are ordin finit.

Într-adevăr, dacă presupunem că în G există un element de ordin infinit, acesta generează un subgrup ciclic infinit, deci izomorf cu $(\mathbb{Z}, +)$, dar acest grup are o infinitate de subgrupuri, de unde rezultă că (G, \cdot) ar avea o infinitate de subgrupuri, contradicție.

Fie $x_1 \in G \setminus \{1\}$ și H_1 subgrupul ciclic generat de x_1 . Dacă $G = H_1$, rezultă că G finit.

Dacă $G \neq H_1$, rezultă că există $x_2 \in G \setminus H_1$ și fie H_2 subgrupul ciclic generat de x_2 . Dacă $G = H_1 \cup H_2$, rezultă că G este finit.

Dacă $G \neq H_1 \cup H_2$, atunci există $x_3 \in G \setminus (H_1 \cup H_2)$ și considerăm subgrupul ciclic generat de x_3 , ș.a.m.d. Nu putem continua la nesfârșit căci am obține o infinitate de subgrupuri ale lui G (se observă că subgrupurile H_1, H_2, \dots sunt distincte două câte două datorită modului de alegere a generatorilor). Prin urmare există $n \in \mathbb{N}^*$ cu proprietatea că $G = H_1 \cup H_2 \cup \dots \cup H_n$. Deoarece subgrupurile H_1, H_2, \dots, H_n sunt finite, rezultă că (G, \cdot) este finit.

4.55. Dacă există $x \in G$ de ordin infinit, rezultă că subgrupul ciclic generat de x , $\langle x \rangle$, este izomorf cu $(\mathbb{Z}, +)$ (vezi problema 4.53.), iar $(\mathbb{Z}, +)$ admite o infinitate de subgrupuri de forma $(n\mathbb{Z}, +)$ cu $n \in \mathbb{N}$.

Dacă orice $x \in G$ este de ordin finit, construim inductiv un șir de subgrupuri distincte ale lui G . Fie $x = x_1 \in G$ și $H_1 = \langle x_1 \rangle \Rightarrow H_1$ este finit $\Rightarrow (\exists) x_2 \in G \setminus H_1$. Analog se construiesc $x_3, \dots, x_n \in G$ a.î. $\langle x_2 \rangle = H_2, \langle x_3 \rangle = H_3, \dots, \langle x_n \rangle = H_n$ și $H_1 \cup H_2 \cup \dots \cup H_n$ este finit, deci $(\exists) x_{n+1} \in G \setminus \bigcup_{k=1}^n H_k$ și $\langle x_{n+1} \rangle = H_{n+1}$.

4.56. Fie $G = \{1, a, b, c\}$ (conform problemei 2.20., G este comutativ).

Dacă $(\exists) x \in G$ a.î. $o(x) = 4$, atunci în mod evident $G \approx (\mathbb{Z}_4, +)$.

Dacă toate elementele lui G au ordin 2, atunci $a^2 = b^2 = c^2 = 1$ și se probează imediat că $ab = c, bc = a$ și $ca = b$, adică $G \approx K$ (grupul lui Klein).

Evident $\mathbb{Z}_4 \not\approx K$ deoarece în K toate elementele diferite de 1 au ordinul 2 pe când în \mathbb{Z}_4 nu se întâmplă lucrul acesta.

4.57. Fie $H_i \leq G, i = 1, 2, 3$ a.î. $G = H_1 \cup H_2 \cup H_3$. Fie $H_1 = \{1, a\}$ și $H_2 = \{1, b\}$ cu $a \neq b, a \neq 1, b \neq 1$. Evident $a^2 \in H_1$ implică $a^2 = 1$ (dacă $a^2 = a \Rightarrow a = 1$ – absurd) și analog $b^2 = 1$.

Fie $c \in H_3 \setminus \{1, a, b\}$. Dacă $ac \in H_3 \Rightarrow a \in H_3 \Rightarrow b \notin H_3$ (dacă $b \in H_3 \Rightarrow G = H_3) \Rightarrow bc \notin H_3 \Rightarrow bc \in H_2$.

Dacă $bc = b \Rightarrow c = 1$, contradicție. Dacă $bc = 1 \Rightarrow b \in H_3$, contradicție. Deducem că $a, b \notin H_3 \Rightarrow ca, cb \notin H_3 \Rightarrow ca = b$ și $cb = a$ (nu putem avea $ca = a$

sau $cb = b$). Ținând cont că $a^2 = b^2 = 1$ rezultă că $c = ab = ba$ și prin urmare $H_3 = \{1, ab\}$. Evident $(ab)^2 = 1$. Deoarece $(\forall) x \in G, x^2 = 1$ rezultă că G este abelian. Tabla grupului arată astfel:

\cdot	1	a	b	c
1	1	a	b	c
a	a	1	c	b
b	b	c	1	a
c	c	b	a	1

Deci G este izomorf cu grupul lui Klein.

4.58. Conform teoremei lui Lagrange ordinul unui element diferit de 1 dintr-un grup G cu 6 elemente poate fi 2,3 sau 6.

Dacă în G avem un element de ordin 6, atunci în mod evident $G \approx (\mathbb{Z}_6, +)$.

Dacă toate elementele lui $G \setminus \{1\}$ ar avea ordinul 2, atunci $|G|$ ar trebui să fie o putere a lui 2 – absurd.

Deci $(\exists) x \in G \setminus \{1\}$ a.î. $o(x) = 3$. Fie acum $y \in G - \{1, x, x^2\}$; dacă $o(y) = 3$, atunci în G ar apare 9 elemente distincte și anume : 1, $x, x^2, y, xy, x^2y, xy^2, x^2y^2$ ceea ce este fals.

Deci $o(y) = 2$ (cazul $o(y) = 6$ nu mai interesează). În acest caz în G am identificat 6 elemente distincte și anume 1, x, x^2, y, xy, x^2y . Cum $yx \in G \Rightarrow yx \in \{xy, x^2y\}$.

Dacă $yx = xy \Rightarrow o(xy) = o(x)o(y) = 2 \cdot 3 = 6$ și în acest caz $G \approx (\mathbb{Z}_6, +)$.

Dacă $yx = x^2y$ atunci considerând $f : G \rightarrow S_3$ definit prin $f(x) = \begin{pmatrix} 123 \\ 231 \end{pmatrix}$ și

$f(y) = \begin{pmatrix} 123 \\ 213 \end{pmatrix}$, obținem un izomorfism de grupuri, deci în acest caz $G \approx (S_3, \circ)$.

Deoarece S_3 nu este comutativ iar \mathbb{Z}_6 este, deducem că $S_3 \not\approx \mathbb{Z}_6$.

4.59. Deoarece \mathbb{R} este o mulțime nenumărabilă iar \mathbb{Z}, \mathbb{Q} sunt numărabile deducem că grupurile $(\mathbb{Z}, +)$ sau $(\mathbb{Q}, +)$ nu pot fi izomorfe cu $(\mathbb{R}, +)$.

Mai avem de demonstrat că $(\mathbb{Z}, +) \not\approx (\mathbb{Q}, +)$. Să presupunem prin absurd că există un izomorfism de grupuri $f : (\mathbb{Z}, +) \rightarrow (\mathbb{Q}, +)$.

Notând $f(1) = \frac{p}{q} \in \mathbb{Q}$ cu $p, q \in \mathbb{Z}, (p, q) = 1, q \neq 0$, se verifică imediat că

$$f(x) = \frac{p}{q} \cdot x, (\forall) x \in \mathbb{Z}.$$

Pentru ca f să fie injectivă, cu necesitate $p \neq 0$. Să demonstrăm că dacă $p \neq 0$ atunci f nu este surjectivă.

Dacă f este surjectivă $(\exists) x \in \mathbb{Z}$ a.î. $f(x) = p+1 \Leftrightarrow px = (p+1)q \Leftrightarrow p \mid (p+1) \Rightarrow p = 1$ sau $-1 \Rightarrow f(x) = \frac{x}{q}$ sau $f(x) = -\frac{x}{q}, (\forall) x \in \mathbb{Z}$.

Scriind în ambele cazuri că $(\exists) x \in \mathbb{Z}$ a.î. $f(x) = \frac{1}{q+1}$ deducem că $q = 0$, ceea ce este absurd.

4.60. Considerând pe \mathbb{R} și \mathbb{C} ca spații vectoriale peste \mathbb{Q} , atunci $(\mathbb{R}, +)$ și $(\mathbb{C}, +)$ sunt grupuri aditive ale acestor spații vectoriale.

Fie B o bază a lui \mathbb{R} peste \mathbb{Q} și fie c cardinalul său. Atunci $\mathbb{C} = \mathbb{R} \times \mathbb{R}$ va avea o bază de cardinal $c \cdot c = c$, deci \mathbb{R} și \mathbb{C} au baze echipotente, rezultând că \mathbb{R} și \mathbb{C} sunt \mathbb{Q} - spații vectoriale izomorfe, adică $(\mathbb{R}, +) \approx (\mathbb{C}, +)$.

4.61. Grupul (\mathbb{Q}^*, \cdot) nu poate fi izomorf nici cu (\mathbb{R}^*, \cdot) și nici cu (\mathbb{C}^*, \cdot) deoarece mulțimea \mathbb{Q}^* este numărabilă, pe când \mathbb{R}^* și \mathbb{C}^* sunt nenumărabile.

Să demonstrăm că (\mathbb{R}^*, \cdot) și (\mathbb{C}^*, \cdot) nu sunt izomorfe.

Dacă prin absurd ar fi izomorfe, atunci ecuația $x^3 = 1$ (ce are în \mathbb{C}^* trei soluții distincte) ar trebui să aibă și în \mathbb{R}^* tot atâtea soluții ceea ce nu este adevărat (căci are doar soluția $x = 1$ în \mathbb{R}^*).

4.62. (i). Evident.

(ii). Funcția $f: \mathbb{R}_+^* \rightarrow \mathbb{R}, f(x) = \ln(x), (\forall) x > 0$ este un izomorfism de grupuri de la (\mathbb{R}_+^*, \cdot) la $(\mathbb{R}, +)$.

Să presupunem acum prin absurd că există un izomorfism de grupuri $f: (\mathbb{Q}_+^*, \cdot) \rightarrow (\mathbb{Q}, +)$.

Atunci $r = \frac{f(2)}{2} \in \mathbb{Q}$, și fie $x \in \mathbb{Q}_+^*$ a.î. $r = f(x)$.

Deducem că $f(2) = 2r = 2f(x) = f(x^2) \Rightarrow x^2 = 2$, cu $x \in \mathbb{Q}$ - absurd.

4.63. Grupurile $(\mathbb{Z}, +)$ și (\mathbb{Q}^*, \cdot) nu sunt izomorfe deoarece $(\mathbb{Z}, +)$ este ciclic pe când (\mathbb{Q}^*, \cdot) nu este ciclic (acest fapt se probează imediat prin reducere la absurd).

4.64. Presupunem prin absurd că există un izomorfism de grupuri $f: (\mathbb{Q}, +) \rightarrow (\mathbb{Q}[i], +)$. Atunci $f(x) = ax$, $(\forall) x \in \mathbb{Q}$, unde $a = f(1)$. Deoarece $a \in \mathbb{Q}[i]$, atunci $a = m + ni$ cu $m, n \in \mathbb{Q}^*$ (nu putem avea $m = 0$ sau $n = 0$ căci atunci f nu ar mai fi surjectiv).

Deoarece f este morfism surjectiv, considerând elementul $m+(n+1)i$ din $\mathbb{Q}[i]$, deducem existența lui $x \in \mathbb{Q}$ a.î. $f(x) = m + (n+1)i$. Această egalitate se mai scrie $xf(1) = m + (n+1)i \Leftrightarrow x(m + ni) = m + (n+1)i \Leftrightarrow mx = m$ și $nx = n + 1$. Cum $m \neq 0$, din prima egalitate deducem că $x = 1$ și atunci cea de-a doua egalitate devine $n = n+1$, contradicție.

4.65. Același raționament ca la problema **4.64**.

4.66. Dacă prin absurd $(\mathbb{Q}, +) \approx (\mathbb{Q}[X], +)$, atunci notând un astfel de izomorfism cu $f: \mathbb{Q} \rightarrow \mathbb{Q}[X]$, se arată ușor că $f(x) = f(1) \cdot x$, $(\forall) x \in \mathbb{Q}$.

Acest lucru este absurd deoarece ar rezulta că toate polinoamele din $\mathbb{Q}[X]$ sunt de forma $X \cdot p(X)$ unde $p(X) = f(1) \in \mathbb{Q}[X]$ (evident, în $\mathbb{Q}[X]$ sunt polinoame de grad mai mare decât gradul lui $p(X)$).

4.67. Presupunem prin absurd că există un izomorfism de grupuri $f: \mathbb{Q}[X] \rightarrow \mathbb{Z}[X]$. Fie $P \in \mathbb{Q}[X]$ un polinom nenul și să considerăm polinomul $f(P) = a_0 + a_1X + \dots + a_nX^n \in \mathbb{Z}[X]$ care va fi de asemenea nenul.

Dacă alegem $k \in \mathbb{N}^*$, $k > \max\{|a_0|, \dots, |a_n|\}$ și considerăm polinomul $S \in \mathbb{Q}[X]$, $S = \frac{1}{k} \cdot P \Rightarrow kS = P \Rightarrow f(S) = \frac{1}{k} \cdot f(P) \Rightarrow f(S) \in \mathbb{Z}[X]$ – absurd.

4.68. Se știe că restricția morfismului f la \mathbb{Q} este de forma $f(x) = ax$, unde $a \in \mathbb{R}$. Dacă se cunoaște că pentru $x_0 \in [-b, b]$, $f(x_0) = ax_0$, atunci și $f(x_1) = ax_1$, $(\forall) x_1 \in \mathbb{R}$. Într-adevăr, $f(x_1) = f(x_1 - x_0) + f(x_0) = f(x_1 - 2x_0) + 2f(x_0) = \dots = f(x_1 - nx_0) + nf(x_0)$ și putem alege $n \in \mathbb{Z}$ a.î. $x_1 - nx_0 \in [-b, b]$.

Deci $f(x_1) = a(x_1 - nx_0) + nax_0 = ax_1$.

Se știe că f este o funcție impară. Deci este suficient să o cunoaștem pe intervalul $[0, b]$ iar pentru aceasta, fie $x_0 \in (\mathbb{R} \setminus \mathbb{Q}) \cap [0, b]$. Funcția f fiind integrabilă pe $[-b, b]$ este integrabilă și pe $[0, x_0] \subset [-b, b]$, $x_0 \in (\mathbb{R} \setminus \mathbb{Q}) \cap [0, b]$.

$$\sigma_{\Delta}(f, \alpha^n) = \sum_{i=0}^{n-1} f(\alpha_i) (x_i - x_{i-1}) \text{ și alegând o diviziune cu intervale de}$$

$$\text{lungimi egale, iar } \alpha_i \in \mathbb{Q}, \text{ obținem } \sigma_{\Delta}(f, \alpha^n) = \frac{ax_0}{n} (\alpha_1 + \dots + \alpha_n) \rightarrow \int_0^{x_0} ax \, dx =$$

$$= \frac{ax_0^2}{2}. \text{ Astfel } \int_0^{x_0} af(x) \, dx = \frac{ax_0^2}{2} \Rightarrow \int_0^{x_0} f(x) \, dx = \frac{x_0^2}{2}, (\forall) x_0 \in [0, b] \Rightarrow f(x_0) = ax_0.$$

În concluzie, f este de forma $f(x) = ax$ cu $a \in \mathbb{R}$.

4.69. Fie $G \subset M_2(\mathbb{C})$ un grup ca în ipoteza problemei și $E \in G$ elementul neutru. Atunci $E^2 = E$ și cum $E \neq I_2$ rezultă că $\det E = 0$.

Fie $A \in G \Rightarrow AE = A \Rightarrow \det A = 0, (\forall) A \in G$.

Dar $A \in M_2(\mathbb{C})$, deci $A^2 - (\text{Tr } A) A + \det A \cdot I_2 = 0_2 \Rightarrow A^2 = \alpha A$, $\alpha = \text{Tr } A$.

Fie A' simetricul lui A în $G \Rightarrow A^2 A' = \alpha AA' \Rightarrow A(AA') = \alpha E \Rightarrow AE = \alpha E \Rightarrow A = \alpha E$. Deci, orice matrice $A \in G$ este de forma $A = \alpha E$ cu $\alpha \in \mathbb{C}$.

Dacă $O_2 \in G \Rightarrow E = O_2 (E = AA', (\forall) A \in G) \Rightarrow G = \{O_2\}$. În acest caz $G = (\{O_2\}, \cdot)$.

Dacă $O_2 \notin G$, fie $f: G \rightarrow \mathbb{C}^*$, $f(A) = \alpha$, dacă $A = \alpha E$. Funcția f este bine definită pentru că $E \neq O_2$, deci $\alpha E = \beta E \Rightarrow \alpha = \beta$. În plus, dacă $A = \alpha E$ și $B = \beta E \Rightarrow AB = \alpha\beta E^2 = \alpha\beta E$, deci $f(AB) = f(A)f(B)$. Rezultă că f este morfism de grupuri. Fie $f(A) = 1 \Rightarrow A = E \Rightarrow f$ este morfism injectiv. Așadar $G \approx f(G)$ care este subgrup în (\mathbb{C}^*, \cdot) .

4.70. Să presupunem prin absurd că există un izomorfism de grupuri $f: (K, +) \rightarrow (K^*, \cdot)$ și fie $a \in K$ a.î. $f(a) = -1$.

Atunci $f(a + a) = f(a) \cdot f(a) = 1 = f(0) \Rightarrow a + a = 0$. Deducem imediat că K este corp de caracteristică 2.

Atunci $(f(1)-1)^2 = (f(1))^2 + 1 = f(1+1) + 1 = f(0) + 1 = 1 + 1 = 0 \Rightarrow f(1) = 1 = f(0) \Rightarrow 0 = 1$ -absurd.

4.71. Fie $x \in G$ a.î. $G/Z(G) = \langle xZ(G) \rangle$ și $y, z \in G$.

Avem că $yZ(G) = (xZ(G))^m$ și $zZ(G) = (xZ(G))^n$ cu $m, n \in \mathbb{Z}$.

Deducem imediat că $yx^{-m}, zx^{-n} \in Z(G) \Leftrightarrow yx^{-m} = z_1, zx^{-n} = z_2$ cu $z_1, z_2 \in Z(G) \Leftrightarrow y = z_1 x^m$ și $z = z_2 x^n$. Rezultă astfel că $yz = zy = z_1 z_2 x^{m+n}$, adică G este comutativ.

4.72. (i). În grupul G/H avem $(xH)^n = x^n H = 1 \cdot H = H$.

Dacă $k \in \mathbb{N}^*$ și $(xH)^k = H \Rightarrow (xH)^k = x^k H = H \Rightarrow x^k \in H$ și deoarece $|H| = m \Rightarrow x^{km} = (x^k)^m = 1$ adică $n = o(x) \mid km$.

Deoarece $(m, n) = 1 \Rightarrow n \mid k$, deci $(xH)^k = 1 \Leftrightarrow n \mid k$, adică $o(xH) = n$.

(ii). Deoarece $(m, n) = 1 \Rightarrow (\exists) \alpha, \beta \in \mathbb{Z}$ a.î. $\alpha m = \beta n + 1$.

Din $o(xH) = n \Rightarrow (xH)^n = H \Rightarrow x^n H = H \Rightarrow x^n \in H$ și luând $y = x^{m\alpha}$ avem $y = x^{m\alpha} = x^{n\beta+1} = x(x^n)^\beta \in xH$, adică $yH = xH$.

Deoarece $|H| = m$ și $x^n \in H \Rightarrow x^{mn} = 1$ și $y^n = (x^{m\alpha})^n = (x^{mn})^\alpha = 1 \Rightarrow o(y) \mid n$.

Fie acum $k = o(y)$; deoarece $(m, n) = 1 = (m, k)$, atunci conform cu (i), $o(yH) = k$. Dar $xH = yH$ și $o(xH) = n$, deci $o(y) = k = n$.

4.73. Fie $x \in G$, $n \in \mathbb{N}^*$ a.î. $x \notin H$ și $(xH)^n = H \Leftrightarrow x^n \in H \Rightarrow (\exists) m \in \mathbb{N}^*$ a.î. $(x^n)^m = 1 \Rightarrow x^{mn} = 1 \Rightarrow x \in H$ – absurd.

4.74. Cazul 1. G este comutativ.

Facem inducție după $|G|$. Dacă $|G| = p$ este evident.

Presupunem afirmația adevărată pentru orice grup H de cardinal mai mic decât $|G|$ ce este multiplu de p și fie $x \in G$, $x \neq 1$.

Dacă $o(x)$ este multiplu de p , afirmația din enunț este în mod evident adevărată.

Să presupunem că $(o(x), p) = 1$ și să considerăm grupul $H = G / \langle x \rangle$ ce are cardinalul $|H| = |G| / o(x) < |G|$ și cum $p \mid |G|$ iar $(o(x), p) = 1 \Rightarrow p \mid |H|$, deci putem aplica ipoteza de inducție lui H și găsim $y \in H$ a.î. $o(y) = p$. Dar $y \in H \Rightarrow y = z \langle x \rangle$, cu $z \in G \Rightarrow y^p = z^p \langle x \rangle = 1 = \langle x \rangle$ (în $G / \langle x \rangle$) $\Leftrightarrow z^p \in \langle x \rangle \Rightarrow (z^p)^{o(x)} = 1 \Rightarrow (z^{o(x)})^p = 1$, deci alegând $x_1 = z^{o(x)}$ avem că $o(x_1) = p$.

Cazul 2. G este necomutativ.

În acest caz folosim ecuația claselor:

$$|G| = |Z(G)| + \sum_{x \notin Z(G)} |G : C_G(x)|.$$

Dacă pentru un $x \notin Z(G)$, $p \mid |C_G(x)|$, atunci ca și în cazul 1 putem face inducție după $|G|$ (aplicând ipoteza de inducție pentru $C_G(x)$).

Deci putem presupune că $p \nmid |C_G(x)|$, $(\forall) x \notin Z(G)$ și cum $|G : C_G(x)| = |G| / |C_G(x)|$, iar $p \mid |G|$, putem presupune că $(\forall) x \notin Z(G)$, $p \mid |G : C_G(x)|$.

Din ecuația claselor rezultă că $p \mid |Z(G)|$ și cum $Z(G)$ este comutativ deducem că există $x \in Z(G)$ a.î. $o(x) = p$.

4.75. Fie G un grup necomutativ a.î. $|G| = 2p$. Conform problemei **4.74.** există $s, t \in G$ a.î. $o(s) = p$ și $o(t) = 2$. Dacă $H = \langle s \rangle$, atunci $|G:H| = 2p/p = 2$, deci $H \trianglelefteq G$ (conform problemei **3.29.**).

Astfel, $tst = tst^{-1} \in H$ ($o(t) = 2$ implică $t^2 = 1$, adică $t = t^{-1}$), deci există $i \in \mathbb{Z}$ a.î. $tst = s^i$.

Deducem imediat că $s = t^2 s t^2 = t (tst) t = t s^i t = (s^i)^t = s^{i^2} \Rightarrow p \mid (i^2 - 1) \Rightarrow p \mid (i+1)$ sau $p \mid (i-1) \Rightarrow tst = s$ sau $tst = s^{-1}$. Dacă $tst = s$ atunci $ts = st \Rightarrow G$ este comutativ – absurd. Avem deci $tst = s^{-1}$ adică $G \approx D_p$.

4.76. (i) \Rightarrow (ii). Dacă în descompunerea în factori primi a lui $|G|$ avem puterea naturală a unui număr prim $q \neq p$, atunci conform problemei **4.74.** $(\exists) x \in G$ a.î. $o(x) = q$ contrazicându-se (i).

(ii) \Rightarrow (i). Rezultă din teorema lui Lagrange.

4.77. Din ecuația claselor:

$$|G| = |Z(G)| + \sum_{x \notin Z(G)} |G:C_G(x)|$$

și din problema precedentă deducem că $p \mid |Z(G)|$, adică $|Z(G)| \geq p$.

4.78. Dacă $Z(G) = G$ totul este clar (conform problemei **4.77.**, $Z(G) \neq \{1\}$).

Să considerăm că $Z(G) \neq G$. Din teorema lui Lagrange deducem că $|Z(G)| = p$.

Atunci $|G/Z(G)| = p^2/p = p$, adică $G/Z(G)$ este ciclic și atunci conform problemei **4.71.** rezultă că G este comutativ.

4.79. Fie G un grup cu proprietatea din enunț și $x \in G \setminus \{1\}$. Definim $f_x: G \rightarrow G$, $f_x(y) = xyx^{-1}$, $(\forall) y \in G$. Se arată cu ușurință că $f_x \in \text{Aut}(G)$, $(\forall) x \in G$.

Cum $f_x(x) = x$ și $f_x(1) = 1 \Rightarrow f_x$ are două puncte fixe, deci $f = 1_G \Rightarrow f_x(y) = y$, $(\forall) y \in G \Rightarrow xyx^{-1} = y \Rightarrow xy = yx$, $(\forall) x, y \in G \Rightarrow (G, \cdot)$ este grup abelian.

Fie $|G| = n$ și p cel mai mic număr prim care divide pe n .

Cazul 1. Dacă $p = 2$, fie $g: G \rightarrow G$, $g(x) = x^{-1}$, $(\forall) x \in G$. Cum $2 \mid n$, există $x_0 \in G$ a.î. $x_0^2 = 1$. Atunci $g(x_0) = x_0$, $g(1) = 1$, $g \in \text{Aut}(G)$ și deci $g = 1_G$. Deci $g(x) = x$, $(\forall) x \in G$, adică $x^2 = 1$, $(\forall) x \in G$.

Cazul 2. Din alegerea lui p obținem că $p+1 \nmid n$ pentru $p > 2$.

Definim $h: G \rightarrow G$, $h(x) = x^{p+1}$. Cum $p \mid n$, din teorema lui Cauchy (vezi problema **4.74.**) există $x_0 \in G \setminus \{1\}$ a.î. $x_0^p = 1$. Atunci $h(x_0) = x_0$ și $h(1) = 1$, $h \in \text{Aut}(G)$ și deci $h = 1_G$. Obținem că $h(x) = x$, $(\forall) x \in G$ și deci $x^p = 1$, $(\forall) x \in G$.

Astfel există, în orice situație, un număr prim p a.î. $x^p = 1$, $(\forall) x \in G$. Cum G este abelian rezultă că G este un \mathbb{Z}_p -spațiu vectorial.

Fie $\{x_1, x_2, \dots, x_k\}$ o bază a lui G și deci orice element $x \in G$ admite o scriere unică sub forma $x = x_1^{\alpha_1} x_2^{\alpha_2} \dots x_k^{\alpha_k}$, cu $\alpha_i \in \{0, \dots, p-1\}$, $1 \leq i \leq k$.

Dacă $k \geq 2$, definim $f: G \rightarrow G$ astfel $f(x_1^{\alpha_1} x_2^{\alpha_2} \dots x_k^{\alpha_k}) = x_1^{\alpha_2} x_2^{\alpha_1} \dots x_k^{\alpha_k}$. Evident $f \in \text{Aut}(G)$, $f(x_1) = x_2$, $f(x_2) = x_1$, $f(x_1 x_2) = x_1 x_2$. Cum $x_1 x_2 \neq 1$ (în caz contrar $x_2 = x_1^{-1} = x_1^{p-1}$, adică x_1 și x_2 sunt liniar dependente - contradicție) rezultă că f are două puncte fixe $x_1 x_2$ și 1 ceea ce este fals.

Deci $k \in \{0, 1\}$. Dacă $k = 1$ atunci $G = \langle x_1 \rangle = \{1, x_1, \dots, x_1^{p-1}\} \approx (\mathbb{Z}_p, +)$.

Dacă $k = 0$, atunci $G = \{1\}$.

Rămîne să arătăm că grupul $(\mathbb{Z}_p, +)$ îndeplinește condiția din enunț.

Fie $f \in \text{Aut}(\mathbb{Z}_p)$. Atunci $f(\hat{k}) = a\hat{k}$ cu $a \in \{1, 2, \dots, p-1\}$. Dacă f are cel puțin două puncte fixe, atunci există $\hat{k} \neq \hat{0}$ astfel încât $f(\hat{k}) = \hat{k} \Rightarrow a\hat{k} = \hat{k} \Rightarrow (a-1)\hat{k} = \hat{0} \Rightarrow p \mid a-1 \Rightarrow a = 1$ ($a \leq p-1$) $\Rightarrow f(\hat{k}) = \hat{k} \Rightarrow f = 1_{\mathbb{Z}_p}$, deci $(\mathbb{Z}_p, +)$ îndeplinește condiția din enunț.

Deci grupurile căutate sunt grupurile $(\mathbb{Z}_p, +)$ cu p prim și grupul trivial $\{1\}$.

4.80. (i). Orice element din \mathbb{Q}/\mathbb{Z} este clasa unui număr rațional de forma m/n cu $0 \leq m < n$, $(m, n) = 1$.

Dacă $x = \frac{m}{n} + \mathbb{Z}$ este un astfel de element, atunci $nx = m + n\mathbb{Z} = 0$ (în \mathbb{Q}/\mathbb{Z}).

(ii). Este ușor de demonstrat că singurul subgrup de ordin n al lui \mathbb{Q}/\mathbb{Z} este: $\{\mathbb{Z}, \frac{1}{n} + \mathbb{Z}, \dots, \frac{n-1}{n} + \mathbb{Z}\}$.

4.81. Facem inducție matematică după m (afirmația din enunț fiind trivială pentru $m = 0, 1$). Să presupunem că afirmația este adevărată pentru subgrupurile de ordin p^{m-1} și fie G un p -grup de ordin p^m . Deoarece $Z(G) \neq \{1\}$ (conform problemei 4.77.) există un element $x \in Z(G)$, $x \neq 1$ cu $o(x) = p^n$ ($n \geq 1$). Atunci $(x^{\frac{p}{n-1}})^p = x^p = 1$ și $x^{\frac{p}{n-1}} \neq 1$, de unde deducem că $o(x^{\frac{p}{n-1}}) = p$ iar $G_1 = \langle x^{\frac{p}{n-1}} \rangle$ este un subgrup de ordin p al lui G . Deoarece $x \in Z(G)$, atunci $G_1 \leq Z(G)$, astfel că $G_1 \trianglelefteq G$ ($|G_1| = p$ - prim) și grupul factor $\bar{G} = G / G_1$ are ordinul p^{m-1} . Conform ipotezei de inducție, grupul \bar{G} are subgrupurile normale $\bar{G}_0, \bar{G}_1, \dots, \bar{G}_{m-1}$ a.î. $1 = \bar{G}_0 < \bar{G}_1 < \dots < \bar{G}_{m-1} = \bar{G}$ și $|\bar{G}_i| = p^i$ pentru orice $i \in \{1, 2, \dots, m-1\}$. Conform teoremei de corespondență, fiecare \bar{G}_i este de forma $\bar{G}_i = G_{i+1} / G_1$, unde G_{i+1} este un subgrup normal al lui G și

$G_1 \leq G_{i+1}$. În plus, $p^i = |G_i| = |G_{i+1}| / |G_1| = |G_{i+1}| / p$, deci $|G_{i+1}| = p^{i+1}$. Ținând cont de principiul inducției matematice deducem că afirmația din enunț este adevărată pentru orice $m \in \mathbb{N}$.

Observație. Din acest exercițiu tragem concluzia că pentru p – grupuri finite este adevărată reciproca teoremei lui Lagrange (vezi și problema 3.47.).

4.82. Vom demonstra că grupul G are proprietatea din enunț $\Leftrightarrow |G| = p^2$ cu p prim ($p \geq 2$).

Într-adevăr, dacă în descompunerea în factori primi a lui $|G|$ ar apărea două numere prime distincte p și q atunci, conform teoremei lui Cauchy pentru grupuri finite (problema 4.74.), există $x, y \in G$ a.f. $o(x) = p$ și $o(y) = q$. Atunci considerând $H_1 = \langle x \rangle$ și $H_2 = \langle y \rangle$, avem că $H_1, H_2 \leq G$ și $|H_1| = p \neq q = |H_2|$, contradicție. În concluzie $|G| = p^k$, $k \geq 1$ și p prim.

Utilizând exercițiul anterior, deducem că există pentru fiecare $i = 0, 1, 2, \dots, k$ $H_i \leq G$ cu $|H_i| = p^i$, ceea ce contrazice ipoteza. Deci cu necesitate $k = 2$.

Reciproc, dacă $|G| = p^2$, atunci conform teoremei lui Lagrange, toate eventualele sale subgrupuri proprii au p elemente.

4.83. (i). Dacă $z_1, z_2 \in T \Rightarrow |z_1| = |z_2| = 1 \Rightarrow |z_1 \cdot z_2^{-1}| = |z_1| \cdot |z_2| = 1 \cdot 1 = 1 \Rightarrow z_1 \cdot z_2^{-1} \in T \Rightarrow T \leq (\mathbb{C}^*, \cdot)$.

Considerând acum $f : (\mathbb{R}, +) \rightarrow (\mathbb{C}^*, \cdot)$, $f(t) = \cos(2\pi t) + i \cdot \sin(2\pi t)$, ($\forall t \in \mathbb{R}$, se arată ușor că f este morfism de grupuri, $\text{Ker}(f) = \mathbb{Z}$, $\text{Im}(f) = T$ și atunci conform teoremei fundamentale de izomorfism pentru grupuri avem $\mathbb{R}/\text{Ker}(f) \approx \text{Im}(f) \Leftrightarrow \mathbb{R}/\mathbb{Z} \approx (T, \cdot)$).

(ii). Se consideră $f : \mathbb{C}^* \rightarrow \mathbb{R}_+^*$, $f(z) = |z|$ și se arată ușor că f este morfism de grupuri, $\text{Ker}(f) = T$ și acum totul rezultă din teorema fundamentală de izomorfism pentru grupuri.

(iii). Faptul că $\mathbb{R}_+^* \leq (\mathbb{C}^*, \cdot)$ rezultă imediat.

Dacă definim $f : \mathbb{C}^* \rightarrow \mathbb{C}^*$, $f(z) = \frac{z}{|z|}$, ($\forall z \in \mathbb{C}^*$, atunci se arată imediat

că f este morfism de grupuri, $\text{Ker}(f) = \mathbb{R}_+^*$, iar $\text{Im}(f) = T$ și totul rezultă din teorema fundamentală de izomorfism pentru grupuri.

(iv). Se arată imediat că $f : \mathbb{C} \rightarrow \mathbb{R}$, $f(z) = \text{Im}(z)$ este morfism surjectiv de grupuri, $\text{Ker}(f) = \mathbb{R}$ și totul rezultă din teorema fundamentală de izomorfism pentru grupuri.

4.84. Definim $\alpha : P(A) \rightarrow M_n(\mathbb{Z}_2)$ prin $\alpha(X) = (a_{ij})_{1 \leq i, j \leq n}$ unde:

$$a_{ij} = \begin{cases} \hat{1}, & \text{dacă } ni - i + j \in X \\ \hat{0}, & \text{dacă } ni - i + j \notin X, \end{cases}$$

și se verifică ușor că α este izomorfism de grupuri.

4.85. Să presupunem că a și b verifică relațiile $a^{2^{n-2}} = b^2 = (ab)^2$.

Din $b^2 = (ab)^2 \Rightarrow b^2 = abab \Rightarrow b = aba \Rightarrow bab^{-1} = a^{-1}$.

Din $a^{2^{n-2}} = b^2 \Rightarrow b a^{2^{n-2}} b^{-1} = b^2 \Rightarrow (bab^{-1})^{2^{n-2}} = b^2 \Rightarrow a^{-2^{n-2}} = b^2 \Rightarrow a^{2^{n-2}} = b^{-2}$ și cum $a^{2^{n-2}} = b^2 \Rightarrow b^2 = b^{-2} \Rightarrow b^4 = 1 \Rightarrow (a^{2^{n-2}})^2 = 1 \Rightarrow a^{2^{n-1}} = 1$.

Reciproc, dacă a și b verifică relațiile $a^{2^{n-1}} = 1$, $bab^{-1} = a^{-1}$ și $b^2 = a^{2^{n-2}}$, atunci din $bab^{-1} = a^{-1} \Rightarrow (ab)^2 = b^2 = a^{2^{n-2}}$.

Din echivalența de relații probată mai sus deducem că $G \approx \mathbf{Q}_n$.

4.86. Prin calcul direct se arată că $o(j) = o(k) = 4$, deci $|J| = |K| = 4$ iar dacă notăm prin $t = jk$, atunci $kj = -t$ și astfel $G = \{\pm I_2, \pm j, \pm k, \pm t\}$, deci $|G| = 8$.

Deoarece $|G : J| = |G : K| = 8:4 = 2$, atunci $J, K \trianglelefteq G$.

Cum $|G| = 2^3$ și $j^2 = k^2 = (jk)^2$ deducem că $G \approx \mathbf{Q}_3$.

4.87. Deoarece $A^2 = B^2 = (AB)^2 = -I_2$, atunci analog ca la problema precedentă deducem că $G \approx \mathbf{Q}_3$.

4.88. Făcând tabla de compunere constatăm că G este grup și deoarece $|G| = 2^3$ iar $j^2 = k^2 = (jk)^2 = -1$, deducem că $G \approx \mathbf{Q}_3$.

4.89. Din studiul tablei de compunere de la problema precedentă deducem că $Z(\mathbf{Q}_3) = \{\pm 1\}$.

4.90. Fie $H = Z(\mathbf{Q}_3)$; cum $|H| = 2 \Rightarrow |\mathbf{Q}_3 / H| = 8 : 2 = 4$ și ținând cont de exercițiul precedent deducem că $\mathbf{Q}_3/H = \{H, iH, jH, kH\}$ (folosind notațiile de la problema **4.86.**). Știm că $i^{-1} = -i$, $j^{-1} = -j$, $k^{-1} = -k$; de asemenea $(iH)(jH) = (ij)H = kH$ iar $(jH)(iH) = (ji)H = (-k)H = k^{-1}H$ și deoarece $k(k^{-1})^{-1} = k^2 = -1 \in H \Rightarrow kH = k^{-1}H$, adică $(iH)(jH) = (jH)(iH)$.

Analog se arată că și celelalte elemente din \mathbf{Q}_3/H comută între ele, de unde deducem că \mathbf{Q}_3/H este comutativ.

4.91. Deoarece \mathbf{Q}_3 nu are elemente de ordin 2 iar D_4 are astfel de elemente (de ex. pe ε) deducem că ele nu pot fi izomorfe.

4.92. Deoarece G este necomutativ de ordin 8, atunci în G nu avem elemente de ordin 8 și nu toate elementele au ordin 2 (în caz contrar se deduce

imediat că G este comutativ, vezi problema 2.38.). Deci $(\exists) a \in G$ a.î. $o(a) = 4$ și fie $b \in G$ a.î. $b \notin \langle a \rangle$. Deoarece $\langle a \rangle \leq G$ (căci $|\langle a \rangle| = 4$ și $4 \mid 8$), deducem că $|G / \langle a \rangle| = 2$, deci $b^2 \in \langle a \rangle$.

Cum $b^2 = a$ sau $b^2 = a^3$ nu se poate (în caz contrar ar rezulta că $o(b) = 8$) deducem că $b^2 = 1$ sau $b^2 = a^2$. Mai mult, cum $\langle a \rangle \trianglelefteq G \Rightarrow b^{-1}ab \in \langle a \rangle$.

Cum $o(a^2) = 2 \Rightarrow b^{-1}ab = a$ sau $b^{-1}ab = a^3$ (rămâne numai cazul $b^{-1}ab = a^3$ căci în cazul $b^{-1}ab = a$ ar rezulta $ab = ba$, adică G ar fi comutativ, fals).

Avem deci posibilitățile:

(i) $a^4 = 1, b^2 = a^2$ și $b^{-1}ab = a^3 = a^{-1}$

(ii) $a^4 = 1, b^2 = 1$ și $b^{-1}ab = a^3 = a^{-1}$

Cazul (i) ne arată că $G \approx \mathbf{Q}_3$ iar cazul (ii) că $G \approx \mathbf{D}_4$.

4.93. Considerăm $f : G \rightarrow \text{Aut}(G)$, $f(a) = \varphi_a$ (automorfismul interior). Din problema 4.49. rezultă că f este un morfism de grupuri, $\text{Ker}(f) = Z(G)$, $\text{Im}(f) = \text{Inn}(G)$ și acum totul rezultă din teorema fundamentală de izomorfism pentru grupuri.

4.94. Fie $A \in \text{GL}_n(K) \Rightarrow \det(A) \neq 0 \Rightarrow \det((A^t)^{-1}) = (\det(A))^{-1} \neq 0$, adică $(A^t)^{-1} \in \text{GL}_n(K)$, deci α este corect definită.

Dacă $A, B \in \text{GL}_n(K) \Rightarrow ((AB)^t)^{-1} = (B^t A^t)^{-1} = (A^t)^{-1} (B^t)^{-1} \Rightarrow \alpha(AB) = \alpha(A) \cdot \alpha(B)$ adică α este morfism de grupuri.

În plus, deoarece pentru $A \in \text{GL}_n(K)$, $(A^t)^{-1} = (A^{-1})^t \Rightarrow (\alpha \circ \alpha)(A) = \alpha(\alpha(A)) = \alpha((A^t)^{-1}) = (((A^t)^{-1})^t)^{-1} = (A^{-1})^{-1} = A$, adică $\alpha \circ \alpha = 1_{\text{GL}_n(K)}$, deci α este o bijecție, de unde deducem că $\alpha \in \text{Aut}(\text{GL}_n(K))$.

Să presupunem prin absurd că α este automorfism interior. Atunci există $B \in \text{GL}_n(K)$ a.î. $(\forall) A \in \text{GL}_n(K)$ să avem $(A^t)^{-1} = \alpha(A) = BAB^{-1}$. Rezultă că $\det(A^{-1}) = \det((A^t)^{-1}) = \det(BAB^{-1}) = \det(A)$, $(\forall) A \in \text{GL}_n(K)$.

Deoarece aplicația $\det : \text{GL}_n(K) \rightarrow K^*$ este surjectivă deducem că $(\forall) a \in K^*$ avem $a = a^{-1} \Rightarrow a^2 = 1 \Rightarrow a = 1$ sau $-1 \Rightarrow K = \mathbb{Z}_2$ sau \mathbb{Z}_3 – absurd; deci α nu este (în condițiile enunțului) automorfism interior.

4.95. Fie $(G, *)$ un grup și $\Sigma(G)$ grupul permutărilor lui G . Pentru $\sigma \in \Sigma(G)$ notăm cu σ^* operația algebrică de pe G definită astfel:

$$x \sigma^* y = \sigma(\sigma^{-1}(x) * \sigma^{-1}(y)), (\forall) x, y \in G.$$

Se verifică imediat că dubletul (G, σ^*) devine grup izomorf cu grupul $(G, *)$, izomorfismul fiind $\sigma : (G, *) \rightarrow (G, \sigma^*)$ (spunem că noua structură σ^* este obținută din structura de grup inițială $(G, *)$ prin transportul dat de σ) (vezi și problema 2.50.).

Pe de altă parte, să observăm că orice structură de grup (G, \circ) izomorfă cu structura inițială $(G, *)$ provine prin transportul dat de o bijecție.

Într-adevăr, dacă $\sigma : (G, \circ) \rightarrow (G, *)$ este izomorfism de grupuri, atunci pentru orice $x, y \in G$ avem:

$x \circ y = \sigma(\sigma^{-1}(x \circ y)) = \sigma(\sigma^{-1}(x) * \sigma^{-1}(y)) = x \sigma^* y$, adică operația algebrică " \circ " coincide cu operația algebrică " σ^* ".

Dacă $\sigma, \xi \in \Sigma(G)$, atunci se probează imediat că $\sigma^* = \xi^* \Leftrightarrow \sigma^{-1}\xi \in \text{Aut}(G, *)$, deci dacă fixăm o bijecție $\sigma \in \Sigma(G)$, atunci toate bijecțiile care transportă structura lui $(G, *)$ în aceeași structură (G, σ^*) sunt de forma $\sigma\varphi$ cu $\varphi \in \text{Aut}(G, *)$, și sunt în număr egal cu $|\text{Aut}(G, *)|$.

Cum în $\Sigma(G)$ există $n!$ bijecții și $|\text{Aut}(G, *)|$ dintre acestea dau aceeași structură de grup pe G izomorfă cu $(G, *)$, deducem că numărul structurilor ce se pot induce pe G și care sunt izomorfe cu $(G, *)$ este egal $n!/|\text{Aut}(G, *)|$.

4.96. Să observăm la început că două grupuri ciclice cu același număr de elemente sunt izomorfe (conform problemei 4.53.).

Dacă $G = \{1, a, a^2, \dots, a^{n-1}\}$ este un grup ciclic fixat, atunci un endomorfism al lui G este perfect determinat dacă definim $f(a) = a^k$, $0 \leq k \leq n-1$.

Să demonstrăm că un astfel de endomorfism este automorfism $\Leftrightarrow (n, k) = 1$. Într-adevăr, notând cu r_0, r_1, \dots, r_{n-1} resturile la împărțirea cu n a numerelor $0, 2k, \dots, (n-1)k$, atunci ținând cont de faptul că f este morfism de grupuri și că $a^n = 1$ deducem că:

$$\text{Im}(f) = G \Leftrightarrow \{r_0, r_1, \dots, r_{n-1}\} = \{0, 1, \dots, n-1\} \Leftrightarrow (k, n) = 1.$$

Deducem că $|\text{Aut}(G)| = \varphi(n)$ și atunci conform problemei 4.95. pe G putem defini $n!/\varphi(n)$ structuri de grup ciclic. Pentru ultima afirmație se ține cont de faptul că dacă n este prim, atunci $\varphi(n) = n-1$.

4.97. Evident, dacă $y \in \mathbb{Q}$ și $n \in \mathbb{N}^*$ atunci ecuația $nx = y$ are soluție în \mathbb{Q} .

4.98. Fie $y \in U_{p^\infty}$. Pentru fiecare $n \in \mathbb{N}$ putem alege câte un generator ξ_n al lui U_{p^∞} a.î. $\xi_{n+1}^p = \xi_n$.

Avem deci un $n \in \mathbb{N}$ a.î. $y \in U_{p^n}$, deci $y = \xi_n^l$, $l \geq 0$. Fie acum $m \in \mathbb{N}^*$, $m = p^k t$, cu $(t, p) = 1$ iar $k \in \mathbb{N}$. Cum și $(t, p^n) = 1$, $(\exists) u, v \in \mathbb{Z}$ a.î. $up^n + vt = 1$. Atunci ecuația $x^m = y$ are în U_{p^∞} soluția $x = \xi_{n+k}^{vl}$ deoarece $x^m = (\xi_{n+k}^{vl})^m = \xi_{n+k}^{vlm} = \xi_{n+k}^{vp^k t l} = y^{vt} = y^{1-up^n} = y$, deci (U_{p^∞}, \cdot) este grup divizibil.

4.99. Fie G un astfel de grup și $y \in G$, $y \neq 0$ (folosim notația aditivă). Dacă y are ordinul infinit, atunci definim (folosim faptul G este divizibil) șirul recursiv $(y_n)_{n \geq 1}$ de elemente din G prin $(n+1)y_{n+1} = y_n$, $n = 1, 2, \dots$. În acest caz

se verifică imediat că grupul generat de elementele y_1, y_2, \dots este izomorf cu grupul aditiv $(\mathbb{Q}, +)$.

Dacă y are ordinul finit m , atunci elementul $y_1 = (m/p)y$, unde p este un divizor prim al lui m , are ordinul p . Cum G este divizibil, definim șirul y_1, y_2, \dots de elemente din G prin $py_{n+1} = y_n$, $n = 1, 2, \dots$. În acest caz subgrupul lui G generat de elementele y_1, y_2, \dots este izomorf cu (U_{p^∞}, \cdot) .

4.100. Să demonstrăm de exemplu că dacă G este un grup divizibil iar $H \leq G$, atunci G/H este divizibil (pe G îl considerăm grup aditiv). Fie deci $m \in \mathbb{N}^*$ și $y + H \in G/H$. Cum G este divizibil, există $x \in G$ a.î. $mx = y$. Atunci $m(x+H) = y + H$, adică G/H este divizibil.

4.101. Deoarece categoria grupurilor abeliene este echivalentă cu categoria \mathbb{Z} -modulelor, putem folosi testul de injectivitate al lui Baer: "*Un A -modul Q este injectiv $\Leftrightarrow (\forall I$ un ideal stâng al lui A și $(\forall f : I \rightarrow Q$ un morfism de A -module, $(\exists) y \in Q$ a.î. $(\forall a \in I, f(a) = ay$."*

" \Rightarrow ". Fie deci G un grup injectiv, $y \in G$, $m \in \mathbb{N}^*$ și $f : m\mathbb{Z} \rightarrow G$, $f(a) = ay$, $(\forall a = bm \in m\mathbb{Z})$. Se arată imediat că f este un morfism de grupuri.

Conform testului de injectivitate al lui Baer $(\exists) x \in G$ a.î. $f(a) = ax$, $(\forall a \in m\mathbb{Z})$.

Pentru $a = m = 1 \cdot m$ avem $y = 1 \cdot y = f(1 \cdot m) = mx$, cu $x = f(1)$, adică G este divizibil.

" \Leftarrow ". Fie acum G un grup abelian divizibil. Conform aceluiași test al lui Baer, pentru a proba injectivitatea lui G este suficient să o probăm pentru idealele $I \neq \{0\}$ ale lui \mathbb{Z} .

Avem că $(\exists) m \in \mathbb{N}^*$ a.î. $I = m\mathbb{Z}$. Fie $f : I \rightarrow G$ un morfism de grupuri și $y = f(m)$. Cum G este divizibil $(\exists) x \in G$ a.î. $mx = y$. Atunci $(\forall a \in m\mathbb{Z}, a = bm)$ avem $f(a) = f(bm) = bf(m) = by = ax$, adică G este un \mathbb{Z} -modul injectiv.

§5. Produse directe de grupuri

5.1. Să demonstrăm de exemplu că $H \times \{1\} \trianglelefteq H \times K$.

Fie deci $(x, 1) \in H \times \{1\}$ și $(y, z) \in H \times K$ ($x, y \in H$ iar $z \in K$).

Atunci $(y, z)^{-1}(x, 1)(y, z) = (y^{-1}, z^{-1})(x, 1)(y, z) = (y^{-1}xy, z^{-1}z) = (y^{-1}xy, 1) \in H \times \{1\}$ (căci $y^{-1}xy \in H$). Analog se probează că $\{1\} \times K \trianglelefteq H \times K$.

5.2. Fie de exemplu $G = G_1 \times G_2$.

Se verifică imediat că $Z(G) = Z(G_1) \times Z(G_2)$.

Deci, dacă G_1 și G_2 sunt comutative, atunci $Z(G_1) = G_1$ și $Z(G_2) = G_2$, și astfel $Z(G) = G_1 \times G_2 = G$, adică G este comutativ.

Reciproc, să presupunem că G este comutativ și să probăm că G_1 și G_2 sunt comutative. Fie de exemplu $x, y \in G_1$. Avem că $(x, 1), (y, 1) \in G$ și din $(x, 1)(y, 1) = (y, 1)(x, 1) \Rightarrow (xy, 1) = (yx, 1) \Rightarrow xy = yx$, adică G_1 este comutativ. Analog se probează că G_2 este comutativ.

5.3. (i). Fie $z_i = (x_i, x_i) \in \hat{G}$, $i = 1, 2$. Atunci $z_1 z_2^{-1} = (x_1, x_1)(x_2, x_2)^{-1} = (x_1 x_2^{-1}, x_1 x_2^{-1})$ este din \hat{G} , deci $\hat{G} \leq G \times G$.

Se probează imediat că $f: G \rightarrow \hat{G}$, $f(x) = (x, x)$, $(\forall) x \in G$ este un izomorfism de grupuri, deci $G \approx \hat{G}$.

(ii). " \Leftarrow ". Presupunem că G este comutativ și fie $z = (x, x) \in \hat{G}$ iar $y = (t, u) \in G \times G$. Atunci $zyz^{-1} = (t, u)(x, x)(t^{-1}, u^{-1}) = (txt^{-1}, uxu^{-1}) = (x, x) \in \hat{G}$, $\hat{G} \trianglelefteq G \times G$.

" \Rightarrow ". Presupunem că $\hat{G} \trianglelefteq G \times G$ și să demonstrăm că G este comutativ.

Fie $x, y \in G$. Atunci $(x, y)(x, x)(x^{-1}, y^{-1}) \in \hat{G} \Leftrightarrow (xxx^{-1}, yxy^{-1}) \in \hat{G} \Leftrightarrow (x, yxy^{-1}) \in \hat{G} \Leftrightarrow x = yxy^{-1} \Leftrightarrow xy = yx$, adică G este comutativ.

(iii). " \Rightarrow ". Fie $t \in Z(G)$; atunci $(\forall) a \in G$ avem $ta = at$ și $(t, 1)(a, a) = (ta, a) = (a, a)(t, 1)$, adică $(t, 1) \in C_{G \times G}(\hat{G}) \leq N_{G \times G}(\hat{G}) = \hat{G}$, deci $t = 1$, adică $Z(G) = \{1\}$.

" \Leftarrow ". Fie $(x, y) \in N_{G \times G}(\hat{G})$. Avem $(x, y) \hat{G} (x, y)^{-1} = \hat{G}$, deci pentru orice $a \in G$, $(x, y)(a, a)(x, y)^{-1} \in \hat{G}$. Însă $(x, y)(a, a)(x, y)^{-1} = (xax^{-1}, yay^{-1})$ deci avem $xax^{-1} = yay^{-1} \Leftrightarrow (y^{-1}x)a = a(y^{-1}x)$, $(\forall) a \in G \Rightarrow y^{-1}x \in Z(G) = 1 \Rightarrow x = y$ și astfel $(x, y) \in \hat{G}$, deci $N_{G \times G}(\hat{G}) = \hat{G}$.

5.4. Definim $f: G/(H \cap K) \rightarrow (G/H) \times (G/K)$ prin $f(x(H \cap K)) = (xH, xK)$, $(\forall) x \in G$.

Dacă $x, y \in G$ și $x(H \cap K) = y(H \cap K) \Leftrightarrow xy^{-1} \in H \cap K \Leftrightarrow xy^{-1} \in H$ și $xy^{-1} \in K \Leftrightarrow xH = yH$ și $xK = yK$, adică f este corect definită și injectivă.

Se probează imediat că f este morfism de grupuri. Pentru a arăta că f este izomorfism de grupuri mai trebuie probată surjectivitatea sa.

Fie deci $(xH, yK) \in (G/H) \times (G/K)$, cu $x, y \in G$. Deoarece $G = H \cdot K$ putem scrie $x = h_1 k_1$, $y = h_2 k_2$ cu $h_i \in H$ și $k_i \in K$, $i = 1, 2$. Considerând $z = h_2 k_1 \in HK = G$ avem $xz^{-1} = h_1 k_1 k_1^{-1} h_2^{-1} \in H$ iar $yz^{-1} = h_2 k_2 k_1^{-1} h_2^{-1} \in K$ (deoarece $K \trianglelefteq G$), adică $zH = xH$ și $zK = yK$, deci $f(z(H \cap K)) = (zH, zK) = (xH, yK)$, adică f este și surjectivă.

5.5. Considerăm surjecțiile canonice $p : H \rightarrow H/J$ și $q : K \rightarrow K/L$. Cum p și q sunt morfisme surjective de grupuri, atunci și $f : H \times K \rightarrow (H/J) \times (K/L)$, $f(x,y) = (p(x),q(y)) = (xJ,yL)$, $(\forall) (x,y) \in H \times K$ este un morfism surjectiv de grupuri. Deoarece $(x,y) \in \text{Ker}(f) \Leftrightarrow f(x,y) = (1,1) \Leftrightarrow p(x)=1$ și $q(y)=1 \Leftrightarrow x \in J$ și $y \in L \Leftrightarrow (x,y) \in J \times L \Rightarrow \text{Ker}(f) = J \times L$.

Astfel, $J \times L = \text{Ker}(f) \trianglelefteq H \times K$ și conform teoremei fundamentale de izomorfism pentru grupuri avem că $(H \times K)/(J \times L) = (H \times K)/\text{Ker}(f) \approx \text{Im}(f) = (H/J) \times (K/L)$.

5.6. Se probează imediat că $f : \mathbb{C}^* \rightarrow \mathbb{R}^* \times T$, $f(z) = (|z|, z/|z|)$ este un izomorfism de grupuri, unde $T = \{z \in \mathbb{C} \mid |z| = 1\}$.

5.7. Considerăm $f : \mathbb{Q}^* \rightarrow \mathbb{Q}_+^* \times \{-1,1\}$, $f(x) = (|x|, x/|x|)$. Avem că $x/|x| \in \{-1,1\}$, $(\forall) x \in \mathbb{Q}^*$. Se verifică imediat că f este izomorfism de grupuri.

5.8. Analog ca la problema 5.7.

5.9. Conform problemei 5.6., $(\mathbb{C}^*, \cdot) \approx (\mathbb{R}_+^*, \cdot) \times (T, \cdot)$.

Dar $(\mathbb{R}_+^*, \cdot) \approx (\mathbb{R}, +)$ (vezi problema 4.62.), iar $(\mathbb{R}/\mathbb{Z}, +) \approx (T, \cdot)$ (vezi problema 4.83.), de unde deducem imediat izomorfismul căutat.

5.10. Dacă $z \in \mathbb{C}$, $z = a + bi$ cu $a, b \in \mathbb{R}$, atunci se verifică imediat că $f : \mathbb{C} \rightarrow \mathbb{R} \times \mathbb{R}$, $f(z) = (a, b)$ este izomorfism de grupuri.

5.11. (i). Ținem cont de exercițiul anterior și de faptul că $(\mathbb{R}, +) \approx (\mathbb{C}, +)$ (vezi problema 4.60.).

(ii). Ținem cont de faptul că orice subgrup finit generat al lui $(\mathbb{Q}, +)$ este ciclic (vezi problema 2.95.).

Astfel, pentru a proba că $(\mathbb{Q}, +) \not\approx (\mathbb{Q}, +) \times (\mathbb{Q}, +)$ este suficient să construim un subgrup finit generat al lui $\mathbb{Q} \times \mathbb{Q}$ care să nu fie ciclic.

Vom considera $H = \langle \{(1,0), (0,1)\} \rangle$ și dacă prin absurd este ciclic, atunci există $(x,y) \in \mathbb{Q} \times \mathbb{Q}$ a.î. $H = \langle (x,y) \rangle$, deci $(\exists) n_1, n_2 \in \mathbb{Z}$ a.î. $(1,0) = n_1(x,y) = (n_1x, n_1y)$ și $(0,1) = n_2(x,y) = (n_2x, n_2y)$. Deducem că $1 = n_1x = n_2y$ și $0 = n_1y = n_2x$ care sunt contradictorii.

5.12. Fie $p_0 = 2, p_1 = 3, p_2 = 5, \dots$ șirul numerelor naturale prime. Se știe că orice rațional se scrie în mod unic sub forma $\alpha = (-1)^a \cdot p_0^{k_0} p_1^{k_1} \dots p_n^{k_n} \dots$ unde $a \in \{0, 1\}, k_i \in \mathbb{Z}, i = 0, 1, \dots$ și $k_i \neq 0$ pentru un număr finit de indici i .

Definim $f: \mathbb{Q}^* \rightarrow \mathbb{Z}_2 \times \mathbb{Z}[X]$ prin $f(\alpha) = (\hat{a}, k_0 + k_1X + \dots + k_nX^n + \dots)$. Se probează imediat că f este izomorfism de grupuri.

5.13. Cum $\mathbb{Z} \times \mathbb{Z}$ este infinit, dacă presupunem prin absurd că este ciclic, atunci cu necesitate avem un izomorfism $f: \mathbb{Z} \rightarrow \mathbb{Z} \times \mathbb{Z}$.

Dacă $f(1) = (a, b)$, atunci $f(2) = (2a, 2b), \dots, f(n) = (na, nb), (\forall) n \in \mathbb{Z}$.

Deoarece f este surjectivă, $(\exists) n \in \mathbb{Z}$ a.î. $f(n) = (1, 1)$, deci $na = 1$ și $nb = 1 \Rightarrow a = b = 1$ sau $a = b = -1$ și $n = 1$ sau -1 .

Dacă însă $f(1) = (1, 1)$, atunci $(\forall) m \in \mathbb{Z}, f(m) = (m, m)$ și astfel f nu mai este surjectivă (de exemplu $(1, 0)$ nu mai este imaginea nici unui element din \mathbb{Z}). Analog în celelalte cazuri.

5.14. Vom proba că subgrupurile lui $(\mathbb{Z}, +) \times (\mathbb{Z}, +)$ sunt de forma :

$(x_1, y_1)\mathbb{Z} + (0, y_2)\mathbb{Z}$ cu $0 \leq y_1 < y_2$ și $x_1 \geq 0$ (evident, toate numere naturale)

Fie $H \leq \mathbb{Z} \times \mathbb{Z}$; atunci notând cu $p_1: \mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z}$ prima proiecție, avem că $p_1(H) \leq \mathbb{Z}$, deci $p_1(H) = x_1\mathbb{Z}$ cu $x_1 \in \mathbb{N}$. Avem atunci un y_1 (nu neapărat unic) a.î. $(x_1, y_1) \in H$. Fie H' subgrupul generat de elementele de forma $(0, y)$. Atunci notând cu p_2 a doua proiecție a lui $\mathbb{Z} \times \mathbb{Z}$ avem că $p_2(H)$ este de forma $y_2\mathbb{Z}$. Deci elementul $(0, y_2) \in H$ și avem $(x_1, y_1)\mathbb{Z} + (0, y_2)\mathbb{Z} \subseteq H$.

Fie acum $(x, y) \in H$. În mod evident $x_1 \mid x$ și deci există $t \in \mathbb{Z}$ cu $x = tx_1$.

Elementul $(0, y - y_1t) = (x, y) - t(x_1, y_1) \in H'$ și deci $y_2 \mid y - y_1t$, adică $(\exists) s \in \mathbb{Z}$ a.î. $y - y_1t = sy_2$. Așadar, $(x, y) = t(x_1, y_1) + s(0, y_2)$ ceea ce ne arată că $H \subseteq (x_1, y_1)\mathbb{Z} + (0, y_2)\mathbb{Z}$, de unde egalitatea $(x_1, y_1)\mathbb{Z} + (0, y_2)\mathbb{Z} = H$.

Acum putem înlocui pe y_1 cu restul împărțirii lui y_1 prin y_2 și astfel identitatea de mai sus nu se schimbă.

5.15. Presupunem prin absurd că $\mathbb{Z} \times \mathbb{Z}_n$ este ciclic și fie $f: \mathbb{Z} \rightarrow \mathbb{Z} \times \mathbb{Z}_n$ un izomorfism de grupuri. Trebuie ca $f(1) = (1, \hat{1})$ și analog ca la soluția de la problema **5.13.** se ajunge la contradicția că f nu este surjectivă (elementul $(0, \hat{1})$ nefiind imaginea nici unui element din \mathbb{Z}).

5.16. Fie $A = \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \in H$, atunci cum $\det(A) = 1 \neq 0 \Rightarrow A \in GL_3(K)$,

deci $H \subseteq GL_3(K)$. Prin calcul se deduce că $A^{-1} = \begin{pmatrix} 1 & a' & b' \\ 0 & 1 & c' \\ 0 & 0 & 1 \end{pmatrix} \in H$, unde $a' = -a$,

$b' = ac - b$ și $c' = -c$.

Dacă $B = \begin{pmatrix} 1 & x & y \\ 0 & 1 & z \\ 0 & 0 & 1 \end{pmatrix} \in H$, atunci $AB = \begin{pmatrix} 1 & x+a & y+b+az \\ 0 & 1 & c+z \\ 0 & 0 & 1 \end{pmatrix} \in H$, deci,

din cele de mai sus rezultă că $H \leq GL_3(K)$.

Să presupunem că $A \in Z(H)$; scriind că $AB = BA$ pentru B de forma

$B = \begin{pmatrix} 1 & 0 & z \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$ și $B = \begin{pmatrix} 1 & 1 & z \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$ deducem că $a = c = 0$, de unde rezultă imediat că

$$Z(H) = \left\{ \begin{pmatrix} 1 & 0 & b \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} : b \in K \right\}.$$

Se verifică acum imediat că $f : K \rightarrow Z(H)$, $f(b) = \begin{pmatrix} 1 & 0 & b \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$ este

izomorfism de grupuri.

De asemenea, se verifică imediat că $g : H \rightarrow K \times K$, $g\left(\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}\right) =$

(a, c) este morfism surjectiv de grupuri cu $\text{Ker}(g) = Z(H)$, de unde $H/\text{Ker}(g) \approx \text{Im}(g) \Leftrightarrow H/Z(H) \approx K \times K$.

5.17. (i). Fie n un număr natural. O *partiție* a lui n este un sistem ordonat (m_1, m_2, \dots, m_n) de n numere naturale a.î. $m_1 \geq m_2 \geq \dots \geq m_n$ și $m_1 + m_2 + \dots + m_n = n$.

Există un mod prescurtat de a scrie partițiile unui număr natural n . Fie (m_1, m_2, \dots, m_n) o partiție a lui n . Mai întâi, se omit zerourile, deci, dacă $m_k \neq 0$ și $m_{k+1} = \dots = m_n = 0$, atunci vom scrie (m_1, m_2, \dots, m_k) în loc de (m_1, m_2, \dots, m_n) . Apoi dacă s dintre numerele m_1, m_2, \dots, m_k coincid cu un număr dat m , vom nota

cu m^s sistemul acestor numere, adică $m^s = \underbrace{(m, m, \dots, m)}_{s \text{ componente}}$. Notăm cu k_n numărul

partițiilor lui n . (funcția $n \mapsto k_n$ este una dintre cele mai importante funcții ale aritmeticii, comparabilă, din acest punct de vedere, cu funcția $n \mapsto \pi_n =$ numărul numerelor prime mai mici ca n).

Vom descrie, spre exemplificare, pentru $n \leq 6$, toate partițiile distincte ale lui n și vom indica numărul lor k_n :

$$n = 1 ; (1) ; k_1 = 1.$$

$$n = 2 ; (2), (1) ; k_2 = 2.$$

$$n = 3 ; (3), (2,1), (1^3) ; k_3 = 3.$$

$$n = 4 ; (4), (3,1), (2^2), (2,1^2), (1^4) ; k_4 = 5.$$

$$n = 5 ; (5), (4,1), (3,2), (3,1^2), (2^2,1), (2,1^3), (1^5) ; k_5 = 7.$$

$$n = 6 ; (6), (5,1), (4,2), (4,1^2), (3^2), (3,2,1), (3,1^3), (2^3), (2^2,1^2), (2,1^4), (1^6) ; k_6 = 11.$$

Fie acum p un număr prim și n un număr natural. Din teorema de structură a grupurilor abeliene finite (vezi [18]) se deduce că numărul grupurilor abeliene finite cu p^n elemente este egal cu k_n .

Astfel, de exemplu, există cinci tipuri de grupuri abeliene de ordin $16 = 2^4$:

$$\mathbb{Z}_{16} \quad - \text{corespunzător partiției (4) ;}$$

$$\mathbb{Z}_8 \times \mathbb{Z}_2 \quad - \text{corespunzător partiției (3,1) ;}$$

$$\mathbb{Z}_4 \times \mathbb{Z}_4 \quad - \text{corespunzător partiției (2^2) ;}$$

$$\mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \quad - \text{corespunzător partiției (2,1^2) ;}$$

$$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \quad - \text{corespunzător partiției (1^4).}$$

(ii). În general, fie n un număr întreg pozitiv și $n = p_1^{n_1} p_2^{n_2} \dots p_s^{n_s}$

descompunerea lui n în produs de numere prime (deci p_1, p_2, \dots, p_s sunt prime distincte și n_1, n_2, \dots, n_s sunt numere naturale). Numărul tipurilor de grupuri abeliene de ordin n este $k_{n_1} k_{n_2} \dots k_{n_s}$ (vezi [9]).

Astfel, de exemplu, există nouă tipuri de grupuri abeliene de ordin $216 = 2^3 \cdot 3^3$:

$$\mathbb{Z}_8 \times \mathbb{Z}_{27} ;$$

$$\mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_{27} ;$$

$$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_{27} ;$$

$$\mathbb{Z}_8 \times \mathbb{Z}_9 \times \mathbb{Z}_3 ;$$

$$\mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_9 \times \mathbb{Z}_3 ;$$

$$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_9 \times \mathbb{Z}_3 ;$$

$$\mathbb{Z}_8 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3 ;$$

$$\mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3 ;$$

$$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3.$$

5.18. Ca o consecință a problemei **5.17.** deducem că un grup comutativ cu 8 elemente este de forma \mathbb{Z}_8 , $\mathbb{Z}_2 \times \mathbb{Z}_4$ sau $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$.

5.19. Același argument ca la exercițiul anterior (grupurile cu 9 elemente fiind comutative, conform problemei **4.78.**).

5.20. Fie G un grup cu 10 elemente. Dacă G este necomutativ, scriind că $10 = 2 \cdot 5$, atunci $G \approx \mathbf{D}_5$ (conform problemei **4.75.**).

Dacă G este comutativ, $G \approx \mathbb{Z}_2 \times \mathbb{Z}_5$ (conform problemei **5.17.**).

5.21. Deoarece $\det(A) = \pm 1 \Rightarrow A$ este inversabilă și $A^{-1} \in M_2(\mathbb{Z})$, mai precis $A^{-1} = \det(A) \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$.

Prin calcul se verifică faptul că $t_{A^{-1}} \circ t_A = 1_{\mathbb{Z} \times \mathbb{Z}}$, adică t_A este bijectivă. Cum faptul că t_A este morfism de grupuri se probează imediat, deducem că $t_A \in \text{Aut}(\mathbb{Z} \times \mathbb{Z})$.

Reciproc, fie $t \in \text{Aut}(\mathbb{Z} \times \mathbb{Z})$ și să notăm $t(1,0) = (a,c)$, $t(0,1) = (b,d)$. Atunci $t(x,y) = t(x,0) + t(0,y) = x \cdot t(1,0) + y \cdot t(0,1) = x \cdot (a,c) + y \cdot (b,d) = (ax + by, cx + dy) = t_A(x,y)$.

Mai rămâne de demonstrat că $\det(A) = \pm 1$.

Cum t este bijecție, $(\exists)!$ $(x,y) \in \mathbb{Z} \times \mathbb{Z}$ a.î. $t(x,y) = (1,0) \Leftrightarrow ax + by = 1$ și $cx + dy = 0$. Datorită unicității soluției sistemului de mai sus $\Rightarrow \det(A) \neq 0$. Aplicând pentru rezolvarea sistemului formula lui Cramer, rezultă că $\det(A) \mid c$ și $\det(A) \mid d$.

Analog, considerând unicul dublet $(z,u) \in \mathbb{Z} \times \mathbb{Z}$ a.î. $t(z,u) = (0,1) \Rightarrow \det(A) \mid a$ și $\det(A) \mid b$.

Deci, notând $D = \det(A) \Rightarrow a = Da'$, $b = Db'$, $c = Dc'$, $d = Dd'$ cu $a', b', c', d' \in \mathbb{Z}$. Rezultă imediat că $D = ad - bc = D^2(a'd' - b'c')$. Cum $D \neq 0 \Rightarrow 1 = D(a'd' - b'c') \Rightarrow D = \det(A) = \pm 1$.

5.22. (i). Conform teoremei lui Cauchy pentru grupuri finite, (vezi problema **4.74.**), G conține un element b de ordin p ; fie $H = \langle b \rangle$. Cum H este un p -subgrup Sylow, atunci conform celei de-a treia teoreme a lui Sylow, numărul conjugăților lui H (adică a subgrupurilor de forma gHg^{-1} cu $g \in G$) este de forma

$1 + up$ cu $u \in \mathbb{N}$. Însă $1 + up = |G : N_G(H)|$ și trebuie să dividă $|G| = pq$. Cum $(1+up, p) = 1$ atunci $1+up \mid q$ iar cum $q < p$ deducem că $u = 0$, deci $H \trianglelefteq G$.

De asemenea, există un element $a \in G$ al cărui ordin este q ; fie $K = \langle a \rangle$. Ca și mai înainte, K este q -subgrup Sylow al lui G , astfel că $|G : N_G(H)| = 1+kq$ cu $k \in \mathbb{N}$. Cum $1 + kq \mid p$ iar prin ipoteză $q \nmid p-1$ deducem că $k = 0$.

Astfel, $K \trianglelefteq G$, deci $G \approx H \times K \approx \mathbb{Z}_p \times \mathbb{Z}_q \approx \mathbb{Z}_{pq}$, deci G este ciclic în acest caz.

(ii). Să presupunem că $q \mid p-1$. Atunci K nu mai este subgrup normal în G . Cum $H \trianglelefteq G$, $a^{-1}ba = b^r$ cu $r \in \mathbb{N}$.

Putem presupune $r \not\equiv 1 \pmod{p}$ (căci în caz contrar ne reîntoarcem la cazul comutativ). Prin inducție se arată ușor că $a^j b a^j = b^{r^j}$. În particular pentru $j=q$ avem $b = b^{r^q}$, adică $r^q \equiv 1 \pmod{p}$.

5.23. Rezultă din problema 5.22. pentru $p = 5$, $q = 3$ observând că $q \nmid p-1$.

5.24. ([18]) Fie p un număr prim. Conform problemei 5.17. numărul tipurilor de grupuri abeliene de ordin p^3 coincide cu numărul partițiilor lui 3. Deoarece $k_3 = 3$ și partițiile lui 3 sunt (3) , $(2,1)$, (1^3) , rezultă următoarele grupuri abeliene \mathbb{Z}_{p^3} , $\mathbb{Z}_{p^2} \times \mathbb{Z}_p$, $\mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_p$.

Căutăm și grupurile neabeliene de ordin p^3 , cazurile $p = 2$ (vezi și problema 4.92.) și p impar tratându-se separat.

Considerăm mai întâi cazul $p = 2$ și fie G un grup neabelian de ordin 8 (vezi problema 5.18.). Deoarece G nu este ciclic, G nu conține nici un element de ordin 8. Dacă toate elementele netriviabile ale lui G au ordinul 2, atunci pentru orice $x, y \in G$ avem $xy = (xy)^{-1} = y^{-1}x^{-1} = yx$ și rezultă că G este abelian. Prin urmare, există un element $a \in G$ cu $o(a) = 4$. Fie $H = \langle a \rangle$. Deoarece $|G:H| = 8/4 = 2$, avem $G = H \cup Hb$, unde b este un element din $G \setminus H$ și $H \trianglelefteq G$. Avem $Hb \in G/H$ și $|G/H| = 2$, deci $H = 1 = (Hb)^2 = Hb^2$ și rezultă $b^2 \in H$. Dacă $b^2 = a$ sau $b^2 = a^3$ se constată imediat că $o(b) = 8$, ceea ce nu se poate. Deci $b^2 = 1$ sau $b^2 = a^2$. Deasemenea, $bab^{-1} \in H$ deoarece H este normal. Deoarece $o(bab^{-1}) = o(a) = 4$, avem $bab^{-1} = a$ sau $bab^{-1} = a^3$. Dacă $bab^{-1} = a$, atunci $ab = ba$ și rezultă că G este abelian deoarece $G = \langle a, b \rangle$. Prin urmare $bab^{-1} = a^3$. Avem astfel:

$$G = \langle a, b \rangle \text{ cu } a^4 = 1, b^2 = 1, bab^{-1} = a^3$$

sau

$$G = \langle a, b \rangle \text{ cu } a^4 = 1, b^2 = a^2, bab^{-1} = a^3.$$

Este ușor de verificat în primul caz că $G \approx \mathbf{D}_4$ (grupul diedral de grad 4) și în al doilea caz, $G \approx \mathbf{Q}$ (grupul quaternionilor). Deoarece grupurile \mathbf{D}_4 și \mathbf{Q} , evident, nu sunt izomorfe, rezultă că există exact două tipuri de grupuri neabeliene de ordin 8.

Considerăm acum că p este un număr prim impar și G un grup neabelian de ordin p^3 . Deoarece G nu este ciclic, G nu conține nici un element de ordin p^3 . Rezultă că elementele netriviale din G au un ordinul p sau p^2 .

Presupunem mai întâi că există $a \in G$ a.î. $o(a) = p^2$. Fie $H = \langle a \rangle$. Deoarece $|G:H| = p$ avem $H \trianglelefteq G$. Deoarece $|G/H| = p$, G/H este ciclic, deci există $b \in G$ a.î. $G/H = \langle Hb \rangle$. În acest caz $H = (Hb)^p = Hb^p$ și rezultă $b^p \in H$. De asemenea, $bab^{-1} \in H$, deoarece H este normal, deci $bab^{-1} = a^r$ cu $r = 0, 1, \dots, p^2-1$. Nu putem avea $r = 0$ sau $r = 1$ deoarece $r = 0$ implică $bab^{-1} = 1$, deci $a = 1$, iar $r = 1$ implică $bab^{-1} = a$, adică $ba = ab$ și deoarece $G = \langle a, b \rangle$, rezultă că G este abelian. Prin inducție matematică după j , se demonstrează imediat că $b^j ab^{-j} = a^{r^j}$ pentru orice număr natural j . În particular, $b^p ab^{-p} = a^{r^p}$.

Pe de altă parte, avem $b^p \in H$ și H este abelian, deci $b^p ab^{-p} = a$. Rezultă $a^{r^p} = a$, deci $r^p \equiv 1 \pmod{p^2}$. Conform teoremei lui Fermat avem $r^p \equiv r \pmod{p}$ și rezultă $r \equiv 1 \pmod{p}$. Scriem $r = 1 + sp$, unde s este un număr întreg. Deoarece $1 < r < p^2$ nu putem avea $s \equiv 0 \pmod{p}$ și prin urmare $(s, p) = 1$, deci există un număr întreg j a.î. $js \equiv 1 \pmod{p}$. Atunci $spj \equiv p \pmod{p^2}$, deci $(1 + sp)^j \equiv 1 + spj \equiv 1 + p \pmod{p^2}$ și $b^j ab^{-j} = a^{r^j} = a^{(1+sp)^j} = a^{1+p}$. Deoarece $(j, p) = 1$, avem $\langle Hb^j \rangle = \langle Hb \rangle = G/H$ și prin urmare putem înlocui b cu b^j , deci putem presupune că $bab^{-1} = a^{1+p}$. Avem $b^p \in H$, deci $b^p = a^t$ pentru un număr întreg t . Deoarece b nu este de ordin p^3 avem $a^{pt} = b^{p^2} = 1$, deci $pt \equiv 0 \pmod{p^2}$, $t \equiv 0 \pmod{p}$. Fie $t = up$, $u \in \mathbb{Z}$. Din relația $ba = a^{1+p}b$ rezultă $ba^i = a^{i(1+p)}b$ pentru orice număr întreg i și, în particular, $ba^{-u} = a^{-u(1+p)}b$. Prin inducție după i rezultă imediat că $b^i a^{-u} = a^{-u(1+p)^i} b$. Avem :

$$(a^{-u}b)^2 = a^{-u} (b a^{-u}) b = a^{-u[1+(1+p)]} b^2,$$

$$(a^{-u}b)^3 = a^{-u[1+(1+p)]} (b^2 a^{-u}) b = a^{-u[1+(1+p)+(1+p)^2]} b^3,$$

și continuând în acest mod, rezultă :

$$(a^{-u}b)^p = a^{-u[1+(1+p)+\dots+(1+p)^{p-1}]} b^p.$$

Avem $1 + (1+p) + \dots + (1+p)^{p-1} \equiv 1 + (1+p) + 1 + 2p + \dots + 1 + (p-1)p = p + pp(p-1)/2 \equiv p \pmod{p^2}$ (deoarece p fiind impar $(p-1)/2$ este întreg), deci

$$a^{-u[1+(1+p)+\dots+(1+p)^{p-1}]} = b^{-p} \quad (\text{deoarece } a^{up} = a^t = b^{p^2} = 1, \text{ adică}$$

$a^{-up} = b^{-p^2} = b^{-p}$) și astfel $(a^{-u}b)^p = b^{-p}b^p = 1$. Deoarece $Ha^{-u}b = Hb$ și $(a^{-u}b)a(a^{-u}b)^{-1} = a^{-u}bab^{-1}a^u = a^{-u}a^{1+p}a^u = a^{1+p}$, îl putem înlocui pe b cu $a^{-u}b$.

Rezultă $G = \langle a, b \rangle$, cu $a^{p^2} = 1$, $b^p = 1$, $bab^{-1} = a^{1+p}$.

Prin urmare există un unic tip de grup neabelian de ordin p^3 care conține un element de ordin p^2 .

Presupunem acum că G nu conține elemente de ordin p^2 . Prin urmare, toate elementele netriviiale din G au ordinul p . Fie $H = Z(G)$ centrul lui G . Atunci H este netrivial, deci $|H| = p$ sau p^2 . Nu putem avea $|H| = p^2$ deoarece în acest caz $|G/H| = p$, ceea ce implică că G/H este ciclic, deci G este abelian (conform problemei 4.71.). Prin urmare $|H| = p$ și $|G/H| = p^2$. Deoarece G/H nu este ciclic, avem, conform problemei 5.17. (i), $G/H \approx \mathbb{Z}_p \times \mathbb{Z}_p$. Aceasta înseamnă că $G/H = \langle x, y \rangle$ cu $x^p = y^p = 1$ și $xy = yx$.

Fie $a, b \in G$ a.î. $Ha = x$ și $Hb = y$. Avem $a^p = b^p = 1$ și $Hab = xy = yx = Hba$, adică $ab = bac$ cu $c \in H$. Dacă $c = 1$ atunci $ab = ba$ și, deoarece $G = \langle H \cup \{a, b\} \rangle$, rezultă G abelian. Deci $c \neq 1$, în care caz $H = \langle c \rangle$ și $G = \langle a, b, c \rangle$. Rezultă că:

$$G = \langle a, b, c \rangle \text{ cu } a^p = b^p = c^p \text{ și } ab = bac.$$

Există deci un unic tip de grup neabelian de ordin p^3 care nu conține elemente de ordin p^2 .

În concluzie, există exact două tipuri de grupuri neabeliene de ordin p^3 .

5.25. Dacă $n \in \mathbb{N}$, $n \geq 2$, prin grup *diciclic de ordin $4n$* (notat \mathbf{DI}_n) înțelegem un grup cu $4n$ elemente :

$$\mathbf{DI}_n = \{1, x, \dots, x^{2n-1}, y, xy, \dots, x^{2n-1}y\}$$

ale cărui elemente le multiplicăm astfel:

$$\begin{aligned} x^a x^b &= x^{a+b} \\ x^a (x^b y) &= x^{a+b} y \\ (x^a y) x^b &= x^{a-b} y \\ (x^a y) (x^b y) &= x^{a-b+n} \end{aligned}$$

unde $0 \leq a, b \leq 2n-1$ iar puterile lui x sunt considerate modulo $2n$.

Se observă că pentru $n = 2$, $\mathbf{DI}_2 = \mathbf{Q}$ (grupul cuaternionilor).

Fie G un grup cu $|G| = 12$.

Dacă G este comutativ, totul rezultă din problema 5.17. (adică $G \approx Z_{12}$ sau $G \approx \mathbb{Z}_4 \times \mathbb{Z}_3$).

Considerăm acum cazul când G este necomutativ. Fie t numărul subgrupurilor Sylow distincte ale lui G cu 3 elemente. Conform teoremelor lui Sylow $t \equiv 1 \pmod{3}$ și $t \mid 4$.

Astfel, G are fie un singur subgrup de ordin 3 (care trebuie să fie subgrup normal) fie 4 subgrupuri (conjugate). Tot conform teoremelor lui Sylow deducem că G trebuie să aibă unul sau 3 subgrupuri de ordin 4.

Cazul 1. Presupunem că G conține un singur subgrup (normal) H de ordin 3 generat de x .

Dacă K este un subgrup al lui G de ordin 4, atunci K este ciclic ($K \approx \mathbb{Z}_4$) sau K este izomorf cu grupul lui Klein ($K \approx \mathbb{Z}_2 \times \mathbb{Z}_2$).

(a) Să analizăm cazul când K este ciclic, $K = \langle y \rangle$.

Cum $H \cap K = \{1\}$, atunci clasele H, Hy, Hy^2, Hy^3 sunt toate distincte și $HK = G$.

Cum $H \trianglelefteq G$ deducem că $xyx^{-1} \in H$.

(1) Dacă $xyx^{-1} = x$, atunci $xy = yx$, deci G este comutativ și avem

$$G \approx H \times K \approx \mathbb{Z}_3 \times \mathbb{Z}_4 \approx \mathbb{Z}_{12}.$$

(2) Dacă $xyx^{-1} = x^2$, atunci $yx = x^2y$, de unde $y^2x = yx^2y = x^2yxy = x^4y^2 = xy^2$.

Astfel, $xy^2 = y^2x$ și dacă considerăm $z = xy^2$ avem că $o(z) = 6$.

De asemenea $z^3 = x^3y^6 = y^2$ și $yz = yxy^2 = y^3x = y^2x^2y = z^{-1}y$.

Cum $o(y) = 4$, $y \notin \langle z \rangle$ și deci clasele $\langle z \rangle, \langle z \rangle y$ dau o partiție a lui G .

Multiplicând în acest caz elementele lui G ca în cazul grupului dicitic și anume $z^a z^b = z^{a+b}$, $z^a (z^b y) = z^{a+b} y$, $(z^a y) z^b = z^{a+b} y$, $(z^a y) (z^b y) = z^{a+b} y^2 = z^{a-b+3}$ (unde puterile lui z se reduc modulo 6) obținem în acest caz că $G \approx DI_3$.

(b) Să presupunem că K este grupul lui Klein (deci $K \approx \mathbb{Z}_2 \times \mathbb{Z}_2$) și să notăm elementele sale cu $1, u, v, w$ unde $w = uv$ și $u^2 = v^2 = 1$. Atunci $H \cap K = \{1\}$ iar clasele H, Hu, Hv, Hw partiționează pe G , de unde $HK = G$. Cum $H \trianglelefteq G$ avem $uxu^{-1} = x^a$, $v xv^{-1} = x^b$, $w x w^{-1} = x^{ab}$ unde $a, b, ab \in \{\pm 1\}$.

(3) Dacă $a = b = ab = 1$, cum G este abelian,

$$G \approx H \times K \approx \mathbb{Z}_3 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \approx \mathbb{Z}_6 \times \mathbb{Z}_2.$$

(4) Să considerăm cazul când două dintre a, b, ab sunt egale cu -1 iar al treilea egal cu 1 .

Renumerotând u, v, w (dacă este necesar) putem presupune că $a = 1$ și $b = -1$. Atunci $ux = xu$ iar $z = ux$ are ordinul 6. Astfel, $G = \langle z, v \rangle$ iar $z^6 = 1$, $v^2 = 1$ iar $vz = z^{-1}v \Leftrightarrow vzv = z^{-1}$ de unde concluzia că $G \approx D_6$.

Cazul 2. Să presupunem că G conține 4 subgrupuri (conjugate) de ordin 3.

Elementele nenule (diferite de 1) ale celor 4 subgrupuri de ordin 3 ne dau 8 elemente diferite de 1 ale lui G , restul de 4 urmând a forma singurul subgrup K de ordin 4 al lui G .

(c) Să arătăm că grupul K nu poate fi ciclic.

Presupunem prin absurd că totuși K este ciclic, $K = \langle y \rangle$ și fie $x \in G \setminus K$.

Atunci $o(x) = 3$ iar clasele K, Kx și Kx^2 dau o partiție a lui G . Cum $K \trianglelefteq G$ avem că $xyx^{-1} \in K$. Dacă $xyx^{-1} = y$, atunci ar rezulta că G este comutativ (în contradicție cu faptul că G conține 4 subgrupuri conjugate distincte de ordin 3).

De asemenea $xyx^{-1} \neq y^2$ (căci y și y^2 au ordine diferite).

În sfârșit, dacă am avea $xyx^{-1} = y^3$, atunci $y = x^3yx^{-3} = y^{27} = y^3$ – absurd, de unde concluzia că grupul K nu este ciclic.

(d) Atunci K trebuie să fie grupul lui Klein. Considerând ca mai sus $K = \{1, u, v, w\}$, fie $x \in G$ a.î. $o(x) = 3$. Atunci clasele K, Kx, Kx^2 sunt toate distincte astfel că $G = \langle u, v, x \rangle$. Conjugarea prin x permută cele 3 elemente u, v, w între ele (căci $K \leq G$) iar permutarea este sau identică sau un 3-ciclu (deoarece $x^3 = 1$).

(5) Nu putem avea permutarea identică căci în acest caz G ar deveni comutativ (caz studiat deja).

(6) Renumerotând eventual, putem presupune că $xux^{-1} = v, xv x^{-1} = w, xwx^{-1} = u$ și atunci considerând asocierile $u \leftrightarrow (12)(34), v \leftrightarrow (13)(24), x \leftrightarrow (234)$ obținem un izomorfism între G și A_4 .

În concluzie avem 5 tipuri de grupuri cu 12 elemente, 2 comutative ($\mathbb{Z}_{12}, \mathbb{Z}_4 \times \mathbb{Z}_3 \approx \mathbb{Z}_6 \times \mathbb{Z}_2$) și 3 necomutative (D_6, DI_3 și A_4).

5.26. Suntem acum în măsură să prezentăm tabelul de caracterizare a grupurilor finite cu cel mult 15 elemente:

Ordin grup	Nr. tipuri	Reprezentanți	Rezultatul care dă caracterizarea
2	1	\mathbb{Z}_2	Problema 4.53.
3	1	\mathbb{Z}_3	Problema 4.53.
4	2	$\mathbb{Z}_4, \mathbb{Z}_2 \times \mathbb{Z}_2$ ($\approx K$)	Problema 4.56.
5	1	\mathbb{Z}_5	Problema 4.53.
6	2	\mathbb{Z}_6, D_3 ($\approx S_3$)	Problema 4.58., 4.75.
7	1	\mathbb{Z}_7	Problema 4.53.
8	5	3 tipuri comutative : $\mathbb{Z}_8, \mathbb{Z}_4 \times \mathbb{Z}_2, \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ 2 tipuri necomutative: Q, D_4	Problema 4.92., 5.18.
9	2	$\mathbb{Z}_9, \mathbb{Z}_3 \times \mathbb{Z}_3$	Problema 5.19.
10	2	\mathbb{Z}_{10}, D_5	Problema 4.75., 5.17.
11	1	\mathbb{Z}_{11}	Problema 4.53.

12	5	2 comutative: $\mathbb{Z}_{12}, \mathbb{Z}_4 \times \mathbb{Z}_3$ 3 necomutative : $D_6, DI_3,$ A_4	Problema 5.17., 5.25.
13	1	\mathbb{Z}_{13}	Problema 4.53.
14	2	\mathbb{Z}_{14}, D_7	Problema 4.75., 5.17.
15	1	\mathbb{Z}_{15}	Problema 5.23.

§6. Inel. Subinel. Exemple. Calcule în inele. Caracteristica unui inel. Elemente inversabile. Divizori ai lui zero. Elemente idempotente. Elemente nilpotente. Produse directe de inele.

6.1. Se observă că a defini o operație de înmulțire „ $*$ ” distributivă față de adunare revine la a defini $1*1$. Într-adevăr, avem de exemplu $n*m = \underbrace{(1+\dots+1)}_{\text{de } n \text{ ori}} * \underbrace{(1+\dots+1)}_{\text{de } m \text{ ori}} = \underbrace{1*1+\dots+1*1}_{\text{de } nm \text{ ori}} = (nm)(1*1)$, pentru $n, m \geq 0$. Pe de

altă parte, este clar pentru fiecare $k \in \mathbb{Z}$, că operația definită prin $n*m = (nm) \cdot k$ înzestreaază pe \mathbb{Z} împreună cu adunarea cu o structură de inel. Prin verificarea axiomelor se deduce imediat că doar pentru $k=1$ și $k=-1$ obținem structuri de inele unitare pe \mathbb{Z} .

6.2. Asociativitatea este imediată:

$(x*y)*z = x*(y*z) = x+y+z-xy-xz-yz+xyz$, oricare ar fi $x, y, z \in A$ (în baza asociativității operațiilor inelului A).

Elementul neutru al legii $*$ este 0 .

Dacă $y \in A$ este inversul lui $1-x$ în inelul A , atunci $1-y$ este inversul lui x față de legea $*$.

6.3. (i). Observăm că putem scrie $(f*g)(n) = \sum_{d_1 d_2 = n} f(d_1)g(d_2)$.

Folosind această scriere, dacă $f, g, h \in A$ vom avea $[(f*g)*h](n) = \sum_{d d_3 = n} (f*g)(d)h(d_3) = \sum_{d d_3 = n} \left(\sum_{d_1 d_2 = d} f(d_1)g(d_2) \right) h(d_3) = \sum_{d_1 d_2 d_3 = n} f(d_1)g(d_2)h(d_3)$.

Analog rezultă $[f*(g*h)](n) = \sum_{d_1 d_2 d_3 = n} f(d_1)g(d_2)h(d_3)$, deci

$(f*g)*h = f*(g*h)$ adică operația $*$ este asociativă. De asemenea, avem $(f*g)(n) = \sum_{d_1 d_2 = n} f(d_1)g(d_2) = (g*f)(n)$, adică $f*g = g*f$, ceea ce înseamnă că

operația $*$ este comutativă.

Notând cu e funcția aritmetică definită prin $e(n) = \begin{cases} 1, & \text{daca } n = 1 \\ 0, & \text{daca } n \geq 2 \end{cases}$ se

observă că pentru orice $f \in A$ avem $(f*e)(n) = \sum_{d_1 d_2 = n} f(d_1)e(d_2) = f(n) \cdot e(1) = f(n)$.

Prin urmare, $f * e = e * f = f$, oricare ar fi $f \in A$, ceea ce înseamnă că e este element neutru față de operația $*$. Așadar, $(A, *)$ este un monoid comutativ.

(ii). „ \Rightarrow ”. Dacă $f \in U(A)$ există $\tilde{f} \in U(A)$ astfel încât $f * \tilde{f} = \tilde{f} * f = e$. În particular, $(f * \tilde{f})(1) = e(1)$, adică $f(1) \cdot \tilde{f}(1) = 1$, deci $f(1) \neq 0$.

„ \Leftarrow ” Reciproc, să presupunem că $f(1) \neq 0$ și să arătăm că $f \in U(A)$. Definim funcția $\tilde{f} : \mathbb{N}^* \rightarrow \mathbb{C}$ recursiv în felul următor:

$$\tilde{f}(n) = \begin{cases} \frac{1}{f(1)}, & \text{daca } n = 1 \\ -\frac{1}{f(1)} \sum_{\substack{d|n \\ d > 1}} f(d) \tilde{f}\left(\frac{n}{d}\right), & \text{daca } n \geq 2 \end{cases}$$

Avem $(f * \tilde{f})(1) = f(1) \tilde{f}(1) = f(1) \cdot \frac{1}{f(1)} = 1 = e(1)$, iar pentru $n \geq 2$

$$(f * \tilde{f})(n) = \sum_{d|n} f(d) \tilde{f}\left(\frac{n}{d}\right) = f(1) \tilde{f}(n) + \sum_{\substack{d|n \\ d > 1}} f(d) \tilde{f}\left(\frac{n}{d}\right) = f(1) \tilde{f}(n) - f(1) \tilde{f}(n) =$$

$$= 0 = e(n)$$

Prin urmare, $f * \tilde{f} = \tilde{f} * f = e$, deci $f \in U(A)$ și inversul lui f este \tilde{f} .

(iii). Mai întâi observăm că pentru orice $f \in M$ avem $f(1) = 1$. Într-adevăr, există $k \in \mathbb{N}^*$ cu $f(k) \neq 0$ și cum $(1, k) = 1$ putem scrie $f(k) = f(1 \cdot k) = f(1) \cdot f(k)$ de unde prin simplificare cu $f(k)$ se obține $f(1) = 1$. Ținând seama de această observație și punctul (ii) deducem că $M \subseteq U(A)$. Pentru a dovedi că M este un subgrup al lui $U(A)$ vom arăta că :

1) oricare ar fi $f, g \in M \Rightarrow f * g \in M$;

2) oricare ar fi $f \in M \Rightarrow \tilde{f} \in M$.

Să probăm mai întâi 1). Dacă $f, g \in M$ avem $(f * g)(1) = f(1) \cdot g(1) = 1 \cdot 1 = 1$, deci $f * g$ este funcție aritmetică nenulă. Dacă $n, m \in \mathbb{N}^*$ și $(n, m) = 1$ atunci orice divizor al lui nm este de forma $d_1 d_2$, unde $d_1 | n$, $d_2 | m$ și în plus, rezultă $(d_1, d_2) = 1$,

$\left(\frac{n}{d_1}, \frac{m}{d_2}\right) = 1$, astfel că putem scrie:

$$(f * g)(nm) = \sum_{d|nm} f(d) g\left(\frac{nm}{d}\right) = \sum_{\substack{d_1|n \\ d_2|m}} f(d_1 d_2) g\left(\frac{nm}{d_1 d_2}\right)$$

$$\begin{aligned}
&= \sum_{\substack{d_1|n \\ d_2|m}} f(d_1)f(d_2)g\left(\frac{n}{d_1}\right)g\left(\frac{m}{d_2}\right) = \left(\sum_{d_1|n} f(d_1)g\left(\frac{n}{d_1}\right)\right)\left(\sum_{d_2|m} f(d_2)g\left(\frac{m}{d_2}\right)\right) \\
&= (f * g)(n) \cdot (f * g)(m).
\end{aligned}$$

Așadar, $f * g$ este funcție multiplicativă, deci $f * g \in M$.

Să probăm acum 2). Fie $f \in M$ și să dovedim că $\tilde{f} \in M$.

Pentru aceasta, considerăm funcția $g \in A$ definită astfel:

$$g(n) = \begin{cases} 1 & \text{daca } n = 1 \\ \tilde{f}(p_1^{\alpha_1}) \cdot \dots \cdot \tilde{f}(p_k^{\alpha_k}), & \text{daca } n = p_1^{\alpha_1} \cdot \dots \cdot p_k^{\alpha_k} \end{cases}$$

(unde p_1, \dots, p_k sunt numere prime distincte).

Se vede ușor că $g \in M$ căci g este nenulă iar dacă $n, m \in \mathbb{N}^*$, $(n, m) = 1$ scriind $n = p_1^{\alpha_1} \cdot \dots \cdot p_k^{\alpha_k}$, $m = p_{k+1}^{\alpha_{k+1}} \cdot \dots \cdot p_s^{\alpha_s}$, (unde $p_1, \dots, p_k, p_{k+1}, \dots, p_s$ sunt numere prime distincte), rezultă :

$$g(nm) = g\left(\prod_{i=1}^s p_i^{\alpha_i}\right) = \prod_{i=1}^s \tilde{f}(p_i^{\alpha_i}) = \prod_{i=1}^k \tilde{f}(p_i^{\alpha_i}) \cdot \prod_{i=k+1}^s \tilde{f}(p_i^{\alpha_i}) = g(n)g(m).$$

Deoarece $f, g \in M$, conform cu 1) rezultă $f * g \in M$. Arătăm că $f * g = e$ și pentru aceasta este suficient să probăm că $(f * g)(p^\alpha) = e(p^\alpha)$ pentru orice p prim și $\alpha \in \mathbb{N}$ (aceasta deoarece $f * g \in M$, $e \in M$ și două funcții multiplicative sunt egale dacă și numai dacă iau valori egale pe toate puterile de numere prime).

Într-adevăr, cum divizorii lui p^α sunt numerele p^i , $0 \leq i \leq \alpha$, avem $(f * g)(p^\alpha) = \sum_{i=0}^{\alpha} f(p^i)g(p^{\alpha-i}) = \sum_{i=0}^{\alpha} f(p^i)\tilde{f}(p^{\alpha-i}) = (f * \tilde{f})(p^\alpha) = e(p^\alpha)$. Așadar, $f * g = e$ și cum inversul lui f este unic rezultă $g = \tilde{f}$. Dar $g \in M$ și atunci $\tilde{f} \in M$, ceea ce încheie (iii).

(iv). Evident, $(A, +)$ este grup abelian în care elementul neutru este funcția nulă. Conform cu (i), $(A, *)$ este monoid comutativ. Dacă mai demonstrăm distributivitatea operației $*$ față de adunare, va rezulta că $(A, +, *)$ este inel comutativ unitar.

Într-adevăr, pentru $f, g, h \in A$ avem pentru orice $n \in \mathbb{N}^*$:

$$\begin{aligned}
[f * (g+h)](n) &= \sum_{d|n} f(d)(g+h)\left(\frac{n}{d}\right) = \sum_{d|n} f(d)g\left(\frac{n}{d}\right) + \sum_{d|n} f(d)h\left(\frac{n}{d}\right) \\
&= (f * g)(n) + (f * h)(n) = (f * g + f * h)(n).
\end{aligned}$$

Aceasta înseamnă că $f*(g+h)=f*g+f*h$, deci $*$ este distributivă la stânga față de $+$. Operația $*$ fiind comutativă, va fi distributivă și la dreapta, deci $(A, +, *)$ este inel comutativ unitar.

Mai rămâne să arătăm că inelul $(A, +, *)$ nu are divizori ai lui zero. Fie $f, g \in A$ două funcții nenule; vom proba că și $f*g$ este nenulă. Să notăm cu n și m cele mai mici numere naturale nenule cu proprietatea că $f(n) \neq 0$, respectiv $g(m) \neq 0$. Atunci, pentru $d < n$, avem $f(d) = 0$ iar pentru $d > n$ avem $\frac{nm}{d} < m$, deci $g\left(\frac{nm}{d}\right) = 0$, astfel că vom putea scrie:

$$\begin{aligned} (f*g)(nm) &= \sum_{d|nm} f(d)g\left(\frac{nm}{d}\right) = \sum_{\substack{d|nm \\ d < n}} 0 \cdot g\left(\frac{nm}{d}\right) + f(n)g(m) + \sum_{\substack{d|nm \\ d > n}} f(d) \cdot 0 \\ &= f(n)g(m) \neq 0. \end{aligned}$$

Așadar, funcția $f*g$ este nenulă și cu aceasta soluția se încheie.

6.4. Demonstrăm că $(A, +, \cdot)$ este un inel unitar și comutativ fără divizori ai lui zero. Elementul neutru la adunare este matricea $M(0) = O_3$ iar opusa matricei $M(a)$ este matricea $M(-a)$. Elementul neutru la înmulțire este matricea $M\left(\frac{1}{2}\right)$.

Pentru a demonstra că A este domeniu de integritate fie $M(a)$ și $M(b) \in A$ cu $M(a) \cdot M(b) \neq M(0)$ (adică $a, b \neq 0$).

Atunci $M(a) \cdot M(b) = M(2ab) \neq M(0)$.

6.5. Se verifică cu ușurință axiomele inelului: $(\mathbb{Z} \times \mathbb{Z}, +)$ este grup abelian; elementul neutru este $(0, 0)$ iar inversul lui (x, y) este $(-x, -y)$. $(\mathbb{Z} \times \mathbb{Z}, \cdot)$ este monoid comutativ; elementul unitate este $(1, 0)$. Distributivitatea înmulțirii față de adunare este imediată.

6.6. (i). Dacă $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\mathbb{C})$ și notăm cu $\text{Tr}(A) = a+d$, A verifică ecuația $x^2 - (a+d) \cdot x + (ad-bc) \cdot I_2 = O_2$. Dacă $\text{Tr}(A) = 0$, atunci $A^2 = (bc-ad) \cdot I_2$ și deci A^2 comută cu orice matrice din $M_2(\mathbb{C})$. Se verifică ușor că $\text{Tr}([A, B]) = \text{Tr}(AB-BA) = 0$, deci $[A, B]^2$ comută cu orice matrice din $M_2(\mathbb{C})$.

(ii). $([A, B] + [C, D])^2 = [A, B]^2 + [C, D]^2 + [A, B] \cdot [C, D] + [C, D] \cdot [A, B]$.

Cum $[A, B]^2, [C, D]^2$ comută cu orice matrice din $M_2(\mathbb{C})$ iar $([A, B] + [C, D])^2$ satisface și ea aceeași proprietate (pentru că $\text{Tr}([A, B] + [C, D]) = \text{Tr}([A, B]) + \text{Tr}([C, D]) = 0 + 0 = 0$) rezultă că $[A, B] \cdot [C, D] + [C, D] \cdot [A, B]$ comută cu orice matrice din $M_2(\mathbb{C})$.

6.7. (i). Fie $X = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ cu $a, b, c, d \in \mathbb{Z}_2$ a.î. $X^2 + I_2 = O_2$. Problema revine

la a rezolva sistemul
$$\begin{cases} a^2 + bc + \hat{1} = \hat{0} \\ b(a + d) = \hat{0} \\ c(a + d) = \hat{0} \\ d^2 + bc + \hat{1} = \hat{0} \end{cases}$$
. Dacă $a + d \neq \hat{0}$ atunci obligatoriu $b = c = \hat{0}$

iar $a^2 = d^2 = \hat{1}$, deci $a = d = \hat{1}$. În acest caz obținem $X_1 = \begin{pmatrix} \hat{1} & \hat{0} \\ \hat{0} & \hat{1} \end{pmatrix}$. Dacă $a + d = \hat{0}$

avem posibilitățile $a = d = \hat{0}$ sau $a = d = \hat{1}$. Pentru $a = d = \hat{0}$ obținem $bc = \hat{1}$, deci $b = c = \hat{1}$ rezultând matricea $\begin{pmatrix} \hat{0} & \hat{1} \\ \hat{1} & \hat{0} \end{pmatrix}$. Pentru $a = d = \hat{1}$ obținem $bc = \hat{0}$ rezultând

matricele $\begin{pmatrix} \hat{1} & \hat{0} \\ \hat{0} & \hat{1} \end{pmatrix}, \begin{pmatrix} \hat{1} & \hat{0} \\ \hat{1} & \hat{1} \end{pmatrix}, \begin{pmatrix} \hat{1} & \hat{1} \\ \hat{0} & \hat{1} \end{pmatrix}$.

Soluțiile sunt $\begin{pmatrix} \hat{1} & \hat{0} \\ \hat{0} & \hat{1} \end{pmatrix}, \begin{pmatrix} \hat{1} & \hat{0} \\ \hat{1} & \hat{1} \end{pmatrix}, \begin{pmatrix} \hat{1} & \hat{1} \\ \hat{0} & \hat{1} \end{pmatrix}, \begin{pmatrix} \hat{0} & \hat{1} \\ \hat{1} & \hat{0} \end{pmatrix}$.

(ii). Trebuie rezolvat în \mathbb{Z}_3 sistemul
$$\begin{cases} a^2 + bc = \hat{1} \\ b(a + d) = \hat{0} \\ c(a + d) = \hat{0} \\ d^2 + bc = \hat{1} \end{cases}$$
. Analog se obțin

matricele $\begin{pmatrix} \hat{1} & \hat{0} \\ \hat{0} & \hat{1} \end{pmatrix}, \begin{pmatrix} \hat{2} & \hat{0} \\ \hat{0} & \hat{2} \end{pmatrix}, \begin{pmatrix} \hat{1} & \hat{0} \\ \hat{0} & \hat{2} \end{pmatrix}, \begin{pmatrix} \hat{2} & \hat{0} \\ \hat{0} & \hat{1} \end{pmatrix}, \begin{pmatrix} \hat{0} & \hat{1} \\ \hat{1} & \hat{0} \end{pmatrix}, \begin{pmatrix} \hat{0} & \hat{2} \\ \hat{2} & \hat{0} \end{pmatrix}, \begin{pmatrix} \hat{2} & \hat{1} \\ \hat{0} & \hat{1} \end{pmatrix},$
 $\begin{pmatrix} \hat{2} & \hat{2} \\ \hat{0} & \hat{1} \end{pmatrix}, \begin{pmatrix} \hat{2} & \hat{0} \\ \hat{1} & \hat{1} \end{pmatrix}, \begin{pmatrix} \hat{2} & \hat{0} \\ \hat{2} & \hat{1} \end{pmatrix}, \begin{pmatrix} \hat{1} & \hat{1} \\ \hat{0} & \hat{2} \end{pmatrix}, \begin{pmatrix} \hat{1} & \hat{2} \\ \hat{0} & \hat{2} \end{pmatrix}, \begin{pmatrix} \hat{1} & \hat{0} \\ \hat{1} & \hat{2} \end{pmatrix}, \begin{pmatrix} \hat{1} & \hat{0} \\ \hat{2} & \hat{2} \end{pmatrix}$.

6.8. Fie $x \in A$ (respectiv $y \in A$) un nondivizor al lui zero la stânga (respectiv la dreapta). Aplicațiile $f_x: A \rightarrow A, g_y: A \rightarrow A$ definite prin $f_x(z) = x \cdot z$ și $g_y(z) = z \cdot y$ sunt injective. A fiind finit ele sunt chiar bijective. Deci există

elementele $u, v \in A$ a.î. $f_x(u) = x$ și $g_y(v) = y$. Fie $z \in A$ un element oarecare. Avem $f_x(uz) = xuz = xz = f_x(z)$, $g_y(zv) = g_y(z)$. Din injectivitate rezultă $uz = z = zv$. În particular, pentru $z = u$, v obținem $u = uv = v$ și evident u este elementul unitate al lui A .

6.9. Fie $A = \{0, 1, a, b, c\}$ și $(A, +, \cdot)$ inelul dat. Vom demonstra mai întâi că $1+1+1+1+1=0$ și apoi că $1+1, 1+1+1, 1+1+1+1 \neq 0$. Este evident că oricare ar fi $x, y \in A$ din $1+x \neq 1+y \Rightarrow x \neq y$. Putem deci spune că $\{1+0, 1+1, 1+a, 1+b, 1+c\} = A$ și atunci $(1+0)+(1+1)+(1+a)+(1+b)+(1+c) = 0+1+a+b+c \Leftrightarrow (1+1+1+1+1)+(0+1+a+b+c) = 0+1+a+b+c \Leftrightarrow 1+1+1+1+1=0$.

Să mai observăm că oricare ar fi $k \in \mathbb{N}^*$ și oricare ar fi $x \in A$ avem $\underbrace{(1+1+\dots+1)}_{\text{de } k \text{ ori}} + x \neq \underbrace{(1+1+\dots+1)}_{\text{de } k-1 \text{ ori}} + x$ deoarece dacă am presupune că există $y \in A$ a.î. $\underbrace{(1+1+\dots+1)}_{\text{de } k \text{ ori}} + y = \underbrace{(1+1+\dots+1)}_{\text{de } k-1 \text{ ori}} + y$ ar rezulta $1=0$.

$$1+1 \neq 0.$$

Presupunem deci că $1+1=0$; Atunci $\{1+0, 1+1, 1+a, 1+b, 1+c\} = \{0, 1, a, b, c\}$ de unde rezultă $a=1+b, b=1+c, c=1+a$ sau $a=1+c, b=1+a, c=1+b$, de unde ar rezulta că $a+b+c = (1+1+1)+a+b+c \Leftrightarrow 0 = 1+1+1$ și cum $1+1=0$, ar rezulta $1=0$, ceea ce este absurd, deci $1+1 \neq 0$.

$$1+1+1 \neq 0.$$

Presupunem deci că $1+1+1=0$. Atunci din $\{1+1, 1+1+1, 1+1+a, 1+1+b, 1+1+c\} = \{1, 1+1, 1+a, 1+b, 1+c\}$ și $1+1+1=0$ rezultă că

$$\{0, 1+1+a, 1+1+b, 1+1+c\} = \{1, 1+a, 1+b, 1+c\}.$$

Dacă $1+a=0$, atunci $1+1+a=1, 1+1+b=1+c, 1+1+c=1+b \Rightarrow (1+1+b)+(1+1+c) = (1+c)+(1+b) \Rightarrow 1+1+1+(1+b+c) = 1+(1+b+c) \Rightarrow 1+1+1=1 \Rightarrow 1+1=0$, ceea ce este absurd.

Analog dacă am presupune că $1+b=0$ sau $1+c=0$ ar rezulta $1=0$.

Prin urmare, $1+1+1 \neq 0$.

$$1+1+1+1 \neq 0.$$

Presupunem că $1+1+1+1=0$. Atunci $\{1+1+1, 1+1+1+1, 1+1+1+a, 1+1+1+b, 1+1+1+c\} = \{1+1, 1+1+1, 1+1+a, 1+1+b, 1+1+c\}$ și $1+1+1+1=0$ rezultă că $\{0, 1+1+1+a, 1+1+1+b, 1+1+1+c\} = \{1+1, 1+1+a, 1+1+b, 1+1+c\}$.

Deoarece $1+1 \neq 0$ rezultă că am putea avea $1+1+a=0$ și atunci din egalitatea de mulțimi precedentă rezultă că $\{1, 1+1+1+b, 1+1+1+c\} = \{1+1, 1+1+b, 1+1+c\} \Rightarrow 1+1+1+b+c=1+1+b+c \Rightarrow 1=0$, ceea ce este absurd. Analog dacă am presupune $1+1+b=0$ sau $1+1+c=0$ ar rezulta $1=0$.

Prin urmare, $1+1+1+1 \neq 0$. Cu aceasta am demonstrat că 5 este cel mai mic $n \in \mathbb{N}^*$ pentru care $\underbrace{(1+1+\dots+1)}_{\text{de } n \text{ ori}} = 0$.

Să demonstrăm acum că inelul $(A, +, \cdot)$ este comutativ. Avem în vedere că $A = \{0, 1, a, b, c\} = \{0, 1, 1+1, 1+1+1, 1+1+1+1\}$.

Dacă $x=0$ sau $y=0$ atunci $xy=yx=0$ iar dacă $x, y \in A^*$, atunci $x = \underbrace{(1+1+\dots+1)}_{\text{de } i \text{ ori}}$, $y = \underbrace{(1+1+\dots+1)}_{\text{de } j \text{ ori}}$ cu $i, j \in \{1, 2, 3, 4\}$.

$$\text{Avem } xy = \underbrace{(1+1+\dots+1)}_{\text{de } i \text{ ori}} \underbrace{(1+1+\dots+1)}_{\text{de } j \text{ ori}} = \underbrace{(1+1+\dots+1)}_{\text{de } ij \text{ ori}} \text{ și}$$

$$yx = \underbrace{(1+1+\dots+1)}_{\text{de } j \text{ ori}} \underbrace{(1+1+\dots+1)}_{\text{de } i \text{ ori}} = \underbrace{(1+1+\dots+1)}_{\text{de } ji \text{ ori}} \text{ și deoarece } ij=ji \text{ rezultă}$$

$xy=yx$. Prin urmare, oricare ar fi $x, y \in A$ avem $xy=yx$, adică inelul $(A, +, \cdot)$ este comutativ.

6.10. (i). $(x+1)^2 = x^2 + x + x + 1 = x^2 + x(1+1) + 1 = x^2 + 1$;
 $(x+1)^3 = (x+1)^2(x+1) = (x^2+1)(x+1) = x^3 + x^2 + x + 1$;
 $(x+1)^4 = (x^2+1)^2 = x^4 + x^2 + x^2 + 1 = x^4 + x^2(1+1) + 1 = x^4 + 1$;
 $(x+1)^5 = (x+1)^3(x+1)^2 = (x^3 + x^2 + x + 1)(x^2 + 1) = x^5 + x^4 + x^3 + x^2 + x^3 + x^2 + x + 1$
 $= x^5 + x^4 + x + 1$.

(ii). Avem $x^{n+1} = x^n$, oricare ar fi $x \in A \Rightarrow (-1)^{n+1} = (-1)^n \Rightarrow 1 = -1 \Rightarrow 1+1=0$. Vom demonstra prin inducție că oricare ar fi $k \in \mathbb{N}$ avem $x^{n+k} = x^n$, pentru orice $x \in A$. Într-adevăr, pentru $k=0$ rezultă $x^n = x^n$, oricare $x \in A$, ceea ce este evident. Pentru $k=1$ avem conform proprietății din enunț $x^{n+1} = x^n$, oricare ar fi $x \in A$. Presupunem deci că $x^{n+k} = x^n$, oricare ar fi $k \leq m$ și oricare ar fi $x \in A$ și să demonstrăm $x^{n+m+1} = x^n$ pentru orice $x \in A$. Într-adevăr, $x^{n+m+1} = x \cdot x^{n+m} = x \cdot x^n = x^{n+1} = x^n$, pentru orice $x \in A$ și deci afirmația este demonstrată.

Din $1+1=0$ deducem $x^n + x^n = 0$, oricare ar fi $x \in A$ și deoarece $x^{n+1} = x^n$ pentru orice $x \in A$ rezultă că $x^{n+1} + x^n = 0$, oricare ar fi $x \in A \Rightarrow x^n(x+1) = 0$, pentru

orice $x \in A$ iar de aici înlocuind pe x cu $x+1$ deducem $0 = (x+1)^n (x+1+1) = (x+1)^n \cdot x$, oricare ar fi $x \in A$.

În ultima egalitate dezvoltăm după formula binomului lui Newton și obținem $0 = (x^n + C_n^1 x^{n-1} + C_n^2 x^{n-2} + \dots + C_n^{n-1} x + 1)x$, oricare ar fi $x \in A$. De aici prin înmulțire cu x^{n-2} , după ce ținem cont că $x^{n+k} = x^n$, pentru orice $x \in A$ și orice $k \in \mathbb{N}$, deducem $0 = (2^n - 1) \cdot x^n + x^{n-1} = -x^n + x^{n-1} \Rightarrow x^{n-1} = x^n$, pentru orice $x \in A$.

Prin același procedeu ca mai sus deducem $x^{n-1} = x^{n-2}$, pentru orice $x \in A$, ș.a.m.d. obținem $x^2 = x$, pentru orice $x \in A$.

6.11. (i). Din $1+1=0$, înmulțind cu $x \in A$ obținem $x+x=0$ sau $x=-x$.

Relația $xy=yx$ este echivalentă deci cu $xy+yx=0$ sau $(x+y)^2 = x^2+y^2$. Dar $(x+y)^2$ și x^2+y^2 nu pot fi decât 0 sau 1. Presupunem prin reducere la absurd că $(x+y)^2 \neq x^2+y^2$ deci unul dintre termeni ar fi 1 iar celălalt ar fi 0.

Dacă $(x+y)^2 = 1$ și $x^2+y^2 = 0$ rezultă că $xy+yx=1$.

Dacă $(x+y)^2 = 0$ și $x^2+y^2 = 1$ rezultă că $xy+yx=1$.

În concluzie, dacă presupunem că $(x+y)^2 \neq x^2+y^2$ atunci este necesar ca:

(1) $xy+yx=1$. Înmulțind această relație cu x la stânga și cu y la dreapta obținem că: (2) $x^2y^2+(xy)^2=xy$.

Din (2) deducem că $xy=0$ sau $xy=1$.

Să presupunem că $xy=0$.

Din (1) rezultă $yx=1 \Rightarrow y(yx)x=yx \Rightarrow y^2x^2=yx=1 \Rightarrow y^2=1$ și $x^2=1$ (dacă $x^2=0$ sau $y^2=0 \Rightarrow y^2x^2=0$), de unde rezultă $x^2y^2=1$.

Dar din (2) rezultă $x^2y^2=0$, contradicție.

Să presupunem că $xy=1 \Rightarrow x(xy)y=xy=1 \Rightarrow x^2y^2=1$.

Dar din (2) rezultă că $x^2y^2=0$, contradicție.

În concluzie, deducem că $(x+y)^2 = x^2+y^2$, oricare ar fi $x, y \in A$, ceea ce este echivalent cu proprietatea că inelul A este comutativ.

(ii). Considerăm $A = \left\{ \begin{pmatrix} \hat{0} & \hat{0} \\ \hat{0} & \hat{0} \end{pmatrix}, \begin{pmatrix} \hat{1} & \hat{0} \\ \hat{0} & \hat{1} \end{pmatrix}, \begin{pmatrix} \hat{0} & \hat{1} \\ \hat{1} & \hat{0} \end{pmatrix}, \begin{pmatrix} \hat{1} & \hat{1} \\ \hat{1} & \hat{1} \end{pmatrix} \right\} \subset M_2(\mathbb{Z}_2)$. Se

demonstrează ușor că adunarea și înmulțirea matricelor din A determină pe mulțimea A o structură de inel comutativ în care au loc proprietățile din enunț.

6.12. (i). Fie $x=ba \Rightarrow x^2=(ba)(ba)=b(ab)a=0 \Rightarrow x=0$ deci $ba=0$. Pentru $x \in A$ arbitrar, notând $y=axb$ avem $y^2=(axb)(axb)=(ax)(ba)(xb)=0 \Rightarrow y=0$ deci $axb=0$.

(ii). Fie $x=a_2a_3a_1 \Rightarrow x^2=(a_2a_3a_1)(a_2a_3a_1)=(a_2a_3)(a_1a_2a_3)a_1=0 \Rightarrow x=0 \Rightarrow a_2a_3a_1=0$. Atunci din $a_2(a_3a_1)=0$ rezultă și $(a_3a_1)a_2=0$, adică $a_3a_1a_2=0$.

(iii). Fie $y=a_{i_1}a_{i_2}\dots a_{i_n}$. Avem $y^n = \underbrace{(a_{i_1}\dots a_{i_n}) \dots (a_{i_1}\dots a_{i_n})}_{\text{de } n \text{ ori}}$. În prima

paranteză la un moment dat apare a_1 . Să presupunem că $a_{i_k} = a_1$; în a doua paranteză apare a_2 . Să presupunem că $a_{i_l} = a_2$; în a treia paranteză apare a_3 ; să presupunem că $a_{i_m} = a_3$ ș.a.m.d. (unde $k \neq l \neq m, \dots$).

Deci

$$y^n = (a_{i_1}a_{i_2}\dots a_{i_{k-1}}a_1a_{i_{k+1}}\dots a_{i_n})(a_{i_1}a_{i_2}\dots a_{i_{l-1}}a_2a_{i_{l+1}}\dots a_{i_n})\dots (a_{i_1}a_{i_2}\dots a_{i_{m-1}}a_3a_{i_{m+1}}\dots a_{i_n}) \dots (1).$$

Avem $a_1a_2\dots a_n=0$. Luând $a=a_1$, $b=a_2\dots a_n$ și $x=a_{i_{k+1}}\dots a_{i_n}a_{i_1}a_{i_2}\dots a_{i_{l-1}}$ avem $ab=0$ deci $axb=0$ adică $a_1a_{i_{k+1}}\dots a_{i_n}a_{i_1}a_{i_2}\dots a_{i_{l-1}}a_2a_3\dots a_n = 0$ (2).

Luăm acum $a = a_1a_{i_{k+1}}\dots a_{i_n}a_{i_1}a_{i_2}\dots a_{i_{l-1}}a_2$, $b = a_3a_4\dots a_n$, $x = a_{i_{l+1}}\dots a_{i_n}a_{i_1}a_{i_2}\dots a_{i_{m-1}}$.

Din (2) avem $ab=0$, deci $axb=0$ adică

$$a_1a_{i_{k+1}}\dots a_{i_n}a_{i_1}a_{i_2}\dots a_{i_{l-1}}a_2a_{i_{l+1}}\dots a_{i_n}a_{i_1}a_{i_2}\dots a_{i_{m-1}}a_3a_4\dots a_n = 0.$$

Continuând raționamentul obținem din aproape în aproape întregul produs din membrul din dreapta al relației (1) egal cu 0. Deci $y^n=0$, de unde rezultă $y=0$, adică $a_{i_1}a_{i_2}\dots a_{i_n} = 0$.

6.13. (i). Fie $a \in M$ și $x \in A$. Atunci

$$(axa-ax)^2=(axa-ax)(axa-ax)=axaxa-axax-axaxa+axax=0 \text{ și}$$

$$(axa-xa)^2=(axa-xa)(axa-xa)=axaxa-axaxa-xaxa+xaxa=0, \text{ de unde rezultă}$$

că $axa=ax=xa$, deci a comută cu orice element al lui A . Dacă $a, b \in M$, cum $ab=ba$ obținem:

$$(a+b-2ab)^2=a^2+b^2+4a^2b^2+2ab-4a^2b-4ab^2=a+b+4ab+2ab-4ab-4ab=a+b-2ab,$$

deci $a+b-2ab \in M$.

(ii). Pe A introducem legea $*$ definită astfel: $x*y=x+y-2xy$. Din punctul (i) rezultă că M este parte stabilă a lui A în raport cu $*$. Se verifică ușor că $*$ este asociativă. Cum $0 \in M$, $a*0=0*a=a$ și $a*a=a+a-2a=0$ pentru orice $a \in M$, rezultă că $(M, *)$ este un grup în care orice element diferit de 0 are ordinul 2. Cum M este mulțime finită, din teorema lui Cauchy pentru grupuri finite rezultă că numărul elementelor sale este o putere naturală a lui 2.

6.14. Fie u inversul elementului $1-ab$. Vom demonstra că elementul $v=1+bu$ este inversul lui $1-ba$. Într-adevăr,

$$v(1-ba)=(1+bu)(1-ba)=1-ba+bu-buaba \quad (1)$$

Dar $u(1-ab)=1$, deci $uab=u-1$. Continuând în (1) rezultă:

$$v(1-ba)=1-ba+bu-b(u-1)a=1-ba+bu-bua+ba=1.$$

Arătăm că $(1-ba)v=1$.

$$(1-ba)v=(1-ba)(1+bu)=1+bu-ba-babu=1+bu-ba-b(u-1)a=1+bu-ba-bua+ba=1 \quad (\text{am folosit faptul că } (1-ab)u=1, \text{ adică } u-abu=1 \text{ sau } abu=u-1).$$

Deci $1-ba$ este inversabil, inversul acestui element fiind v .

6.15. Avem $1=(1-aba)^n=(1-aba)(1+aba+\dots+(aba)^{n-1})$, deci $1-aba$ este inversabil. Notăm cu $c=(1-aba)^{-1}$, deci $(1-aba)c=c(1-aba)=1$. Atunci:
 $(1-a^2b)(1+acab)=1-a^2b+acab-a^2bacab=1-a^2b+a[(1-aba)c]ab=1-a^2b+a^2b=1$ și
 $(1+acab)(1-a^2b)=1-a^2b+acab-acaba^2b=1-a^2b+a[c(1-aba)]ab=1-a^2b+a^2b=1$, deci $1-a^2b$ este inversabil. Analog se arată că: $(1-ba^2)(1+bac)=1$, de unde $1-ba^2$ este inversabil.

6.16. Dacă x are proprietatea (P) atunci există x^{-1} , pentru că $b=ax-x^2=x(a-x)$ și cum b este inversabil și b^{-1} comută cu x , avem:

$$1=x(ab^{-1}-xb^{-1})=(ab^{-1}-xb^{-1})x, \text{ deci } x^{-1}=ab^{-1}-xb^{-1}.$$

(i). Dacă $A = M_2(\mathbb{C})$ și matricea X are proprietatea (P), atunci X fiind inversabilă este nesingulară. Reciproc, dacă X este nesingulară și $X^2-(\text{Tr}(X)) \cdot X+(\det(X)) \cdot I_2=O_2$ rezultă că există matricele $(\text{Tr}(X)) \cdot I_2$ și $(\det(X)) \cdot I_2$ care comută cu X și $(\det(X)) \cdot I_2$ este inversabilă.

(ii). Fie $x \in A$ cu proprietatea (P), deci există $a, b \in A$ care comută cu x , b inversabil, a.f. $a=x-bx^{-1}$. Se demonstrează prin inducție după puterile lui x că dacă există $a_k, b_k \in A$ ce comută cu x^k , b_k inversabil și $a_k=x^k-b_k x^{-k}$, atunci x^{k+1} are aceeași proprietate.

6.17. Cum b și ab^{-1} sunt inversabile, rezultă că putem vorbi de elementul $b(ab^{-1})^{-1}$ care este element inversabil, fiind produsul a două elemente inversabile.

Observăm că $(a-b^{-1})[b(ab^{-1})^{-1}]=[a-b^{-1}]b(ab^{-1})^{-1}=(ab^{-1})(ab^{-1})^{-1}=1$ și cum $b(ab^{-1})^{-1}$ este element inversabil, rezultă că $a-b^{-1}$ este tocmai inversul acestui element. Atunci și $a-b^{-1}$ este inversabil și $(a-b^{-1})^{-1}=b(ab^{-1})^{-1}$.

Calculăm produsul:

$$[(a-b^{-1})^{-1}a^{-1}](aba-a)=[b(ab-1)^{-1}a^{-1}]\cdot(ab-1)a=b(ab-1)^{-1}(ab-1)a\cdot a^{-1}(ab-1)a=$$

$$=ba\cdot a^{-1}aba+a^{-1}a=1.$$

$$\text{Analog } (aba-a)[(a-b^{-1})^{-1}a^{-1}]= (aba-a)[b(ab-1)^{-1}a^{-1}]=(aba-a)b(ab-1)^{-1}\cdot(aba-a)a^{-1}=$$

$$=(abab-ab)(ab-1)^{-1}\cdot ab+1=ab(ab-1)(ab-1)^{-1}\cdot ab+1=ab\cdot ab+1=1.$$

Din aceste egalități rezultă că $(a-b^{-1})^{-1}a^{-1}$ este un element inversabil și inversul său este $aba-a$.

6.18. (i) \Rightarrow (ii). Presupunem prin reducere la absurd că a este inversabil și fie a^{-1} inversul său. Dacă $a\cdot x=1$, atunci $x=1\cdot x=(a^{-1}\cdot a)\cdot x=a^{-1}\cdot(a\cdot x)=a^{-1}$, de unde rezultă $\text{card}\{x\in A\mid a\cdot x=1\}=1$, contradicție.

(ii) \Rightarrow (iii). Cum a nu este inversabil avem $b\cdot a\neq 1$. Fie $c=b\cdot a-1\neq 0$.

$$\text{Calculăm } a\cdot c=a(ba-1)=(ab)a-a=1\cdot a-a=a-a=0.$$

(iii) \Rightarrow (i). Cum $c\neq 0 \Rightarrow c+b\neq b$. Dar $a(c+b)=ac+ab=0+1=1$. Deci mulțimea $\{x\in A\mid a\cdot x=1\}$ conține cel puțin elementele b și $c+b$, adică $\text{card}\{x\in A\mid a\cdot x=1\}>1$.

6.19. Presupunem că $X\neq\emptyset$ și fie $b\in X$. Dacă $x\in X$, atunci $a(1+b-xa)=a+ab-(ax)a=a+a\cdot b-1\cdot a=a+ab-a=ab=1$ (căci $b\in X$, adică $ab=1$), deci $1+b-xa\in X$.

Putem astfel defini funcția $f:X\rightarrow X$, $f(x)=1+b-xa$, oricare ar fi $x\in X$. Arătăm că f este funcție injectivă dar nu și surjectivă, de unde va rezulta că mulțimea X este infinită. Pentru injectivitate, dacă $f(x_1)=f(x_2)$ atunci $1+b-x_1a=1+b-x_2a \Rightarrow x_1a=x_2a$.

Avem $x_1=x_1\cdot 1=x_1\cdot(ab)=(x_1a)b=(x_2a)b=x_2\cdot(ab)=x_2\cdot 1=x_2$, deci f este funcție injectivă. Demonstrăm că f nu este surjectivă și anume că nu există $x\in X$ a.î. $f(x)=b$, căci din $1+b-xa=b$ se deduce $xa=1$ și atunci din $xa=1=ax$ ar rezulta că a este element inversabil, contradicție.

6.20. Dacă $x\in A\setminus(D\cup\{0\})$ și $d\in D$ atunci $xd\in D$ căci $xd\neq 0$ și întrucât există $y\in A\setminus\{0\}$ cu $dy=0$, avem și $(xd)y=x(dy)=x\cdot 0=0$.

Prin urmare funcția $d\in D\rightarrow xd$ este cu valori în D . Notând f_x această funcție ea va fi injectivă (căci $f_x(d_1)=f_x(d_2)$ înseamnă $x(d_1-d_2)=0$, deci $d_1=d_2$), deci bijectivă. Dacă $x,y\in A\setminus(D\cup\{0\})$ și $f_x=f_y$, atunci $x-y\in D\setminus\{0\}$, prin urmare există un număr finit de elemente în $A\setminus(D\cup\{0\})$ pentru care $f_x=f_y$.

Cum și numărul bijecțiilor de la D în D este finit rezultă că $A \setminus (D \cup \{0\})$ este o mulțime finită, așadar inelul A este finit.

Dacă $x \in A \setminus (D \cup \{0\})$ funcția $g_x: A \rightarrow A$, $g_x(y) = xy$ este injectivă, deci surjectivă, așadar orice element din $A \setminus (D \cup \{0\})$ este inversabil.

Să presupunem acum că $s = d_1 + d_2 + \dots + d_n \notin D \cup \{0\}$.

Atunci $1 = s^{-1}(d_1 + d_2 + \dots + d_n) = f_{s^{-1}}(d_1) + \dots + f_{s^{-1}}(d_n) = d_1 + d_2 + \dots + d_n = s$ și demonstrația este încheiată.

6.21. Dacă $D = \emptyset$ atunci $G = \{0\}$ este grup abelian. Presupunem $D \neq \emptyset$. Fie $a, b \in G \Rightarrow 2a = 0, 2b = 0 \Rightarrow 2(a+b) = 0 \Rightarrow a+b \in G$, deci G este parte stabilă a lui A față de operația de adunare, rezultă deci că „+” este asociativă și comutativă pe mulțimea G și deoarece $0 \in G$ rezultă că $(G, +)$ este monoid comutativ. Dacă $a \in G \Rightarrow 2a = 0 \Rightarrow 2(-a) = 0 \Rightarrow -a \in G$, deci orice element din G are opus în G , adică $(G, +)$ este grup abelian.

6.22. „ \Rightarrow ”. Numărul elementelor inversabile din inelul \mathbb{Z}_n este $\varphi(n)$, unde φ este indicatorul lui Euler. Prin urmare ipoteza este echivalentă cu $\varphi(n) = \frac{n}{2}$, adică (1): $n = 2\varphi(n)$. Fie $n = p_1^{u_1} \dots p_k^{u_k}$ descompunerea în factori primi a numărului natural n , unde $p_1 < p_2 < \dots < p_k$ sunt numere prime iar u_1, u_2, \dots, u_k sunt numere naturale nenule. Se știe atunci că $\varphi(n) = p_1^{u_1-1} \dots p_k^{u_k-1} (p_1 - 1) \dots (p_k - 1)$ și deci egalitatea (1) devine:

$$p_1 p_2 \dots p_k = 2(p_1 - 1)(p_2 - 1) \dots (p_k - 1). \quad (2)$$

Din (2) avem că 2 divide produsul $p_1 p_2 \dots p_k$ deci în mod necesar vom avea $p_1 = 2$. Dacă presupunem $k > 1$, egalitatea (2) devine:

$$p_2 p_3 \dots p_k = (p_2 - 1)(p_3 - 1) \dots (p_k - 1). \quad (3)$$

Dar (3) este imposibilă, deoarece membrul stâng este evident mai mare decât cel drept. Prin urmare $k = 1$ și $p_1 = 2$, ceea ce înseamnă că $n = 2^{u_1}$.

„ \Leftarrow ”. Dacă $n = 2^k$, atunci elementele inversabile din inelul \mathbb{Z}_{2^k} sunt clasele \hat{a} cu proprietatea $(a, 2^k) = 1$, adică clasele impare, iar clasele neinversabile sunt cele pare. Prin urmare, există 2^{k-1} elemente inversabile și tot 2^{k-1} elemente neinversabile.

6.23. (i). Fie $f, g \in A$. Se știe că suma lui f cu g este funcția $f+g: [0, 1] \rightarrow \mathbb{R}$, $(f+g)(x) = f(x) + g(x)$, oricare ar fi $x \in [0, 1]$ iar produsul lui f cu g este funcția $fg: [0, 1] \rightarrow \mathbb{R}$, $(f \cdot g)(x) = f(x) \cdot g(x)$, oricare ar fi $x \in [0, 1]$. Cum suma

și produsul a două funcții continue sunt funcții continue, rezultă că operațiile de adunare și înmulțire a funcțiilor sunt operații algebrice pe A.

Evident, ele verifică axiomele inelului comutativ. Elementul zero al acestui inel este funcția $0:[0, 1] \rightarrow \mathbb{R}$, $0(x)=0$, oricare ar fi $x \in [0, 1]$ iar elementul unitate este funcția $1:[0, 1] \rightarrow \mathbb{R}$, $1(x)=1$, oricare ar fi $x \in [0, 1]$.

(ii). „ \Leftarrow ”. Fie $f \in A$, $f \neq 0$ și $I=(a, b)$ cu $a < b$ un interval inclus în intervalul $[0, 1]$ a.î. $f(x) \neq 0$, oricare ar fi $x \in I$. Funcția $g:[0, 1] \rightarrow \mathbb{R}$,

$$g(x) = \begin{cases} (x-a)(x-b), & \text{pentru } x \in I \\ 0, & \text{pentru } x \in [0, 1] - I \end{cases}$$

este continuă, $g \neq 0$ și $fg=0$, deci f este divizor al lui zero.

„ \Rightarrow ”. Fie $f \in A$, $f \neq 0$, divizor al lui zero. Există atunci $g \in A$, $g \neq 0$ a.î. $f \cdot g=0$. Cum $g \neq 0$, există $x_0 \in [0, 1]$ a.î. $g(x_0) \neq 0$. Însă g este continuă, deci există un interval $I \subset [0, 1]$ a.î. $x_0 \in I$ și $g(x) \neq 0$, oricare ar fi $x \in I$. Cum $0=0(x)=(fg)(x)=f(x) \cdot g(x)$, oricare ar fi $x \in I$ rezultă că $f(x)=0$, oricare ar fi $x \in I$.

(iii). Demonstrăm că singurele funcții care verifică $f^2=f$ sunt 1 și 0. Evident dacă $f=0$ sau $f=1$ atunci $f^2=f$. Reciproc, dacă $f^2=f$, atunci $[f(x)]^2=f(x)$, oricare ar fi $x \in [0, 1]$, deci $f(x)[f(x)-1]=0 \Rightarrow f(x)=0$ sau $f(x)=1$ pentru $x \in [0, 1]$. Cum o funcție continuă are proprietatea lui Darboux, rezultă $f=0$ sau $f=1$.

(iv). Evident $f \in A$ este element inversabil al inelului A dacă și numai dacă $f(x) \neq 0$, oricare ar fi $x \in [0, 1]$.

6.24. (i). Fie $x_1, x_2 \in Z(A)$. Atunci pentru orice $y \in A$ putem scrie

$$(x_1-x_2)y = x_1y - x_2y = yx_1 - yx_2 = y(x_1-x_2), \text{ deci } x_1-x_2 \in Z(A).$$

De asemenea, $(x_1x_2)y = x_1(x_2y) = x_1(yx_2) = (x_1y)x_2 = (yx_1)x_2 = y(x_1x_2)$ deci $x_1x_2 \in Z(A)$. Rezultă că $Z(A)$ este subinel al lui A. El este evident și comutativ.

Să observăm că dacă A este inel unitar, atunci $Z(A)$ este un subinel unitar, căci 1 comută cu toate elementele inelului, deci $1 \in Z(A)$.

(ii). Vom arăta că orice element al inelului aparține centrului, deci $A=Z(A)$ și inelul va fi comutativ.

Fie $x \in A$ fixat. Pentru $y \in A$ oarecare avem :

$$(x+y)^2 - (x+y) = x^2 + y^2 + xy + yx - x - y = (x^2 - x) + (y^2 - y) + (xy + yx), \text{ de unde}$$

$xy+yx=[(x+y)^2-(x+y)]-(x^2-x)-(y^2-y)\in Z(A)$ (unde am ținut seama că fiecare din elementele $[(x+y)^2-(x+y)], (x^2-x), (y^2-y)\in Z(A)$).

Deoarece $xy+yx\in Z(A)$ avem că $x(xy+yx)=(xy+yx)x$, adică $x^2y+xyx=xyx+yx^2$ sau $x^2y=yx^2$. Cum $y\in A$ este arbitrar, ultima egalitate arată că $x^2\in Z(A)$. Deoarece $x^2-x\in Z(A)$, rezultă că $x=x^2-(x^2-x)\in Z(A)$. Deci $A=Z(A)$, adică A este comutativ.

6.25. (i). Avem $f(x,y)=(xy)^2-x^2y^2=xyxy-xxyy=x(yx-xy)y$.

Înlocuind pe x cu $1+x$ obținem:

$$f(1+x,y)=(1+x)[y(1+x)-(1+x)y]y=(1+x)(yx-xy)y.$$

Analog obținem $f(x, 1+y)=x(yx-xy)(1+y)$

$$f(1+x, 1+y)=(1+x)(yx-xy)(1+y).$$

Din cele de mai sus rezultă:

$f(1+x, 1+y)-f(1+x, y)=(1+x)(yx-xy)(1+y)-(1+x)(yx-xy)y=(1+x)(yx-xy)$ (1)
și analog

$$-f(x, 1+y)+f(x, y)=-x(yx-xy)(1+y)+x(yx-xy)y=-x(yx-xy). \quad (2)$$

Adunând (1) cu (2) rezultă:

$$E(x,y)=(1+x)(yx-xy)-x(yx-xy)=yx-xy.$$

(ii) Ipoteza $(xy)^2-(yx)^2=x^2y^2-y^2x^2$ este echivalentă cu $(xy)^2-x^2y^2=(yx)^2-y^2x^2$, adică $f(x,y)=f(y,x)$, oricare ar fi $x,y\in A$. Atunci folosind și definiția lui $E(x,y)$ avem: $E(x,y)-E(y,x)=f(1+x,1+y)-f(1+x,y)-f(x,1+y)+f(x,y)-f(1+y,1+x)+f(1+y,x)+f(y,1+x)-f(y,x)=0$.

Așadar, $E(x, y)=E(y, x)$ (3).

Pe de altă parte, folosind rezultatul de la (i) avem

$$E(x,y)=yx-xy=-(xy-yx)=-E(y, x), \text{ adică } E(y, x)=-E(x, y). \quad (4)$$

Din (3) și (4) rezultă $E(x, y)=-E(x, y)$ adică $E(x, y)+E(x, y)=0$ și folosind prima ipoteză de la (ii) rezultă $E(x, y)=0$. Așadar, $yx-xy=0 \Leftrightarrow yx=xy$ oricare ar fi $x, y\in A$, deci inelul A este comutativ.

6.26. Fie A un inel unitar cu pq elemente.

Considerăm mulțimea $Z(A)=\{x\in A \mid xy=yx, \text{ oricare ar fi } y\in A\}$. Se știe că $Z(A)$ este un subinel unitar și comutativ al lui A . În particular, $Z(A)$ este subgrup aditiv al lui A și conform teoremei lui Lagrange, $|Z(A)|$ divide pq . Cum $0, 1\in Z(A)$, avem $|Z(A)|\geq 2$, deci $|Z(A)|\in\{p, q, pq\}$.

Cazul 1. Dacă $|Z(A)|=pq$, rezultă $Z(A)=A$, deci A este inel comutativ.

Cazul 2. Dacă $|Z(A)|=p$

Alegem un element $\alpha \in A \setminus Z(A)$ și considerăm mulțimea

$$B = \{a_0 + a_1\alpha + \dots + a_n\alpha^n \mid n \in \mathbb{N}, a_i \in Z(A)\}.$$

Demonstrăm că B este un subinel unitar comutativ al lui A care include strict pe $Z(A)$. Într-adevăr, se observă că diferența a două elemente din B este de asemenea în B , iar pentru a arăta că produsul a două elemente din B este de asemenea în B este suficient să considerăm două monoame de forma $a_i\alpha^i$ și $a_j\alpha^j$, unde $i, j \in \mathbb{N}$ iar $a_i, a_j \in Z(A)$.

Ținând seama că a_i și a_j sunt în centrul lui A , putem scrie

$$(a_i\alpha^i)(a_j\alpha^j) = a_i\alpha^i a_j\alpha^j = a_i\alpha^i a_j\alpha^j = a_i\alpha^{i+j}a_j = (a_i a_j)\alpha^{i+j} \in B.$$

Deci B este un subinel al lui A .

Mai mult, putem arăta la fel că $(a_j\alpha^j)(a_i\alpha^i) = (a_i a_j)\alpha^{i+j}$, deci $(a_i\alpha^i)(a_j\alpha^j) = (a_j\alpha^j)(a_i\alpha^i)$, de unde ținând seama de distributivitatea înmulțirii față de adunare, deducem că B este și comutativ. Este clar că elementele lui $Z(A)$ aparțin și lui B , iar $\alpha \in A \setminus Z(A)$, deci inelul B include strict pe $Z(A)$. Conform teoremei lui Lagrange, $|B|$ va fi un divizor al lui pq și în același timp un multiplu de p , mai mare decât p , adică în mod necesar, $|B|=pq$. Aceasta înseamnă că $B=A$, deci A este comutativ, contradicție cu presupunerea că centrul lui A are doar p elemente. Așadar acest caz este imposibil.

Cazul 3. $|Z(A)|=q$. Se tratează analog cu cazul precedent, obținându-se că este un caz imposibil.

6.27. Luând $k = \max\{m, n\}$ rezultă că $x^k y = 0 = (x+1)^k y$.

Fie $l = \min\{s \in \mathbb{N} \setminus \{0\} \mid x^s y = 0 = (x+1)^s y\}$. Dacă $l \geq 2$ obținem:

$$\begin{cases} x^l y = 0 \\ (x+1)^l y = 0 \end{cases} \Rightarrow \begin{cases} (x+1)^{l-1} x^l y = 0 \\ x^{l-1} (x+1)^l y = 0 \end{cases} \Rightarrow \begin{cases} (x+1)^{l-1} ((x+1)-1)^l y = 0 \\ x^{l-1} (x+1)^l y = 0 \end{cases} \quad (*).$$

Dezvoltând după formula binomului lui Newton pe $[(x+1)-1]^l$, $(x+1)^l$ și folosind faptul că $x^l y = 0 = (x+1)^l y$, obținem din (*) relațiile $x^{l-1} y = 0 = (x+1)^{l-1} y$, cu $l-1 \geq 1$. Dar aceasta contrazice minimalitatea lui l . Deci $l=1$, adică $xy = 0 = (x+1)y$. Deducem de aici prin scădere că $y = (x+1)y - xy = 0 - 0 = 0$.

6.28. Conform ipotezei avem succesiv:

$x^{n+1} y^{n+1} = (xy)^{n+1} = (xy)^n (xy) = x^n y^n xy$, de unde (1) $x^n (xy^n - y^n x) y = 0$, pentru orice $x, y \in A$.

Luând în (1) $x+1$ în loc de x și observând că $(x+1)y^n - y^n(x+1) = xy^n - y^n x$, deducem de mai sus: (2) $(x+1)^n(xy^n - y^n x)y = 0$, pentru orice $x, y \in A$.

Din (1) și (2) rezultă conform problemei 6.27.: (3) $(xy^n - y^n x)y = 0$, pentru orice $x, y \in A$.

În particular, luând x^n în loc de x , rezultă din (3) că: (4) $(x^n y^n - y^n x^n)y = 0$, pentru orice $x, y \in A$. Folosind acum ipoteza găsim în (4) că:

$0 = (x^n y^n - y^n x^n)y = ((xy)^n - (yx)^n)y = (xy)^n y - y(xy)^n$, adică $y(xy)^n = (xy)^n y$. Egalitatea $(yx)^n y = y(xy)^n$ folosită mai sus se poate verifica ușor prin inducție după $n \geq 1$ (ea este practic evidentă conform asociativității înmulțirii).

6.29. Conform primei părți a problemei 6.28. obținem din relația (3) de acolo:

$$(5) (xy^n - y^n x)y = 0$$

$$(6) (xy^{n+1} - y^{n+1}x)y = 0.$$

Deducem de aici:

(7) $(xy - yx)y^{n+1} = (xy^{n+1} - y^{n+1}x)y - y(xy^n - y^n x)y = 0 - y \cdot 0 = 0 - 0 = 0$, pentru orice $x, y \in A$ (prima egalitate din șirul de egalități precedente se verifică prin calcul direct).

Luând în (7) $y+1$ în loc de y obținem și:

(8) $(xy - yx)(y+1)^{n+1} = 0$, pentru orice $x, y \in A$ (am folosit aici din nou egalitatea evidentă $x(y+1) - (y+1)x = xy - yx$).

Din (7) și (8) deducem conform problemei 6.27. că $xy - yx = 0$, adică A este comutativ (am folosit de fapt aici „simetrica” problemei 6.27. care afirmă că din $xy^n = 0 = x(y+1)^m$ rezultă $x = 0$. Aceasta se demonstrează analog cu soluția problemei 6.27.).

6.30. Fie $\alpha \in Z(A)$. Atunci conform condiției 1) din ipoteză $Z(A) \ni (\alpha x + y)^n - (\alpha x + y) = (\alpha x)^n - \alpha x + y^n - y + \sum_{j=1}^{n-1} \alpha^j P_j(x, y)$, unde $P_j(x, y)$ este suma tuturor celor C_n^j monoame de gradul n în x și y cu exact j apariții ale lui x , din dezvoltarea $(\alpha x + y)^n$ (de exemplu, $P_1(x, y) = \sum_{j=1}^n y^{j-1} x y^{n-j}$,

$$P_2(x, y) = \sum_{\substack{n_1, n_2, n_3 \geq 0 \\ n_1 + n_2 + n_3 = n-2}} y^{n_1} x y^{n_2} x y^{n_3}, \text{ ș.a.m.d.).}$$

Aplicând din nou ipoteza 1) găsim că $\sum_{j=1}^{n-1} \alpha^j P_j(x, y) \in Z(A)$ și prin

urmare: (*) $\sum_{j=1}^{n-1} \alpha^j [P_j(x, y), z] = 0$, pentru orice $\alpha \in Z(A)$ și $x, y, z \in A$.

Fixăm acum $x, y \in A$. Conform ipotezei 2) există elementele din $Z(A)$ distincte $\alpha_1, \dots, \alpha_{n-1} \neq 0$. Scriind relația (*) pentru $\alpha_1, \dots, \alpha_{n-1} \in Z(A) \setminus \{0\}$ cu $z=y$ și privind ecuațiile obținute ca un sistem în necunoscutele $[P_j(x, y), y]$ cu $1 \leq j \leq n-1$, obținem prin înmulțire la stânga cu matricea adjunctă a coeficienților (adjuncta unei matrice este transpusa reciprocei): $d[P_1(x, y), y] = d[P_2(x, y), y] = \dots = d[P_{n-1}(x, y), y] = 0$. Deci $d \neq 0$ este determinantul matricei Vandermonde a sistemului și este diferit de zero deoarece inelul A a fost presupus integru.

Cum într-un inel integru se poate simplifica cu elemente diferite de zero, rezultă că $[P_1(x, y), y] = [P_2(x, y), y] = \dots = [P_{n-1}(x, y), y] = 0$.

În particular din $P_1(x, y) \cdot y = y \cdot P_1(x, y)$, rezultă prin reducerea termenilor asemenea că $xy^n = y^n x$ (se folosește aici dezvoltarea lui $P_1(x, y)$ sub forma

$P_1(x, y) = \sum_{j=1}^n y^{j-1} xy^{n-j}$, când $j=1$, $y^0 xy^{n-1}$ este notație pentru xy^{n-1} , deci nu

presupunem că A este unitar. Dar $y^n - y \in Z(A)$ astfel că din $xy^n = y^n x$, obținem $xy = yx$.

6.31. Fie $y \in A$ un element arbitrar fixat. Vom arăta că $[x, y] = xy - yx = 0$.

Dacă $n=1$ sau $m=1$, atunci afirmația rezultă direct din enunț.

Fie deci $n > m > 1$ cu $(m, n) = 1$ și $[x, y^n] = 0 = [x, y^m]$.

Să observăm că pentru orice întregi $u, v \geq 1$ are loc egalitatea:

(1) $[x, y^{u+v}] = [x, y^u]y^v + y^u[x, y^v]$ (verificare directă).

Conform teoremei împărțirii cu rest avem o egalitate de tipul $n = q_1 m + r_1$ cu $0 < r_1 < m$.

De aici, din relația (1) pentru $u = q_1 m$, $v = r_1$ și din $[x, y^n] = 0 = [x, y^m]$ deducem că:

$$\begin{aligned} 0 &= [x, y^n] = [x, y^{q_1 m + r_1}] = [x, (y^m)^{q_1}] y^{r_1} + y^{q_1 m} [x, y^{r_1}] = \\ &= 0 \cdot y^{r_1} + y^{q_1 m} [x, y^{r_1}] = y^{q_1 m} [x, y^{r_1}] \end{aligned} \quad (2)$$

Fie acum $m = q_2 r_1 + r_2$ cu $0 < r_2 < r_1$, adică procedăm după algoritmul lui Euclid de calcul al c.m.m.d.c. Ca mai sus deducem: $0 = [x, y^m] = [x, y^{q_2 r_1}] y^{r_2} + y^{q_2 r_1} [x, y^{r_2}]$, de unde prin înmulțire la stânga cu $y^{q_1 m}$

rezultă conform lui (2): (3) $y^{q_1 m + q_2 n} [x, y^{1/2}] = 0$ (din $y^{q_1 m} [x, y^n] = 0$ rezultă ușor prin inducție după $q_2 \geq 1$ că $y^{q_1 m} [x, y^{q_2 n}] = 0$).

Se continuă până ce în algoritmul lui Euclid se obține un rest egal cu 1 (aceasta se întâmplă deoarece prin ipoteză m și n sunt relativ prime).

Găsim deci un întreg $k \geq 1$ pentru care $y^k [x, y] = 0$.

Până acum am arătat deci că pentru orice $y \in A$ există un întreg $k \geq 1$ cu $y^k [x, y] = 0$.

Cum și $y+1 \in A$, deducem existența unui întreg $l \geq 1$ cu $0 = (y+1)^l [x, y+1] = (y+1)^l [x, y]$.

Deci $y^k [x, y] = 0 = (y+1)^l [x, y]$ și conform problemei 6.27. deducem că $[x, y] = 0$. Deci $[x, y] = 0$, pentru orice $y \in A$, adică $x \in Z(A)$.

6.32. (i), (ii). Prin calcul direct.

(iii). Fie $z = m + n\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$ un element inversabil. Există deci $z' = x + y\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$ a.î. $zz' = 1$, ceea ce conduce la sistemul
$$\begin{cases} mx + 2ny = 1 \\ nx + my = 0 \end{cases}$$
.

Condiția necesară și suficientă ca pentru $m, n \in \mathbb{Z}$, dați, sistemul precedent să aibă soluție unică cu $x, y \in \mathbb{Z}$ este $m^2 - 2n^2 = \pm 1$ (condiția este evident suficientă; necesitatea rezultă deoarece conform primei ecuații $(m, n) = 1$ și se ține cont de forma termenului liber). Deci $\varphi(z) = 1 \Leftrightarrow z$ este inversabil.

Definim acum recurent următorul șir de numere întregi $x_0 = y_0 = 1$, $x_{n+1} + y_{n+1}\sqrt{2} = (x_n + y_n\sqrt{2})(1 + \sqrt{2})$. Numerele de forma $x_n + y_n\sqrt{2}$ sunt toate distincte, deoarece deducem de mai sus că $x_n + y_n\sqrt{2} = (1 + \sqrt{2})^n$ și evident $1 + \sqrt{2} \neq \pm 1$.

Conform punctului (ii) al problemei (sau prin inducție după n) rezultă $\varphi(x_n + y_n\sqrt{2}) = 1$, deci elementele distincte $x_n + y_n\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$ sunt inversabile.

6.33. (i). Notând $z = a + b\sqrt{d} \in \mathbb{Z}[\sqrt{d}]$ și cu $z^* = a - b\sqrt{d} \in \mathbb{Z}[\sqrt{d}]$, conjugatul pătratic al lui z , observăm că $z \cdot z^* = (a + b\sqrt{d})(a - b\sqrt{d}) = a^2 - db^2 = N(z)$.

Folosind faptul că conjugatul produsului este produsul conjugatilor avem pentru $z_1, z_2 \in \mathbb{Z}[\sqrt{d}]$:

$$N(z_1 \cdot z_2) = (z_1 z_2)(z_1 z_2)^* = (z_1 z_2)(z_1^* z_2^*) = (z_1 z_1^*)(z_2 z_2^*) = N(z_1) \cdot N(z_2).$$

(ii). „ \Rightarrow ”. Dacă $z \in \mathbb{Z}[\sqrt{d}]$ este un element inversabil, există $z^{-1} \in \mathbb{Z}[\sqrt{d}]$ a.î. $z \cdot z^{-1} = 1$. Trecând la normă, rezultă $N(z) \cdot N(z^{-1}) = 1$, deci $N(z)$ este un element inversabil în inelul \mathbb{Z} , adică $N(z) \in \{\pm 1\}$.

„ \Leftarrow ”. Reciproc, dacă $N(z) \in \{\pm 1\}$, luând $z^{-1} = N(z) \cdot z^*$ avem $z \cdot z^{-1} = N(z) \cdot z \cdot z^* = N(z) \cdot N(z) = [N(z)]^2 = (\pm 1)^2 = 1$ deci z este inversabil în inelul $\mathbb{Z}[\sqrt{d}]$.

(iii). Conform punctului (ii) un element $z = a + b\sqrt{d}$ aparține lui $U(\mathbb{Z}[\sqrt{d}])$ dacă și numai dacă $a^2 - db^2 = \pm 1$. (1)

Pentru $d < 0$ avem $a^2 - db^2 > 0$, deci ecuația (1) devine $a^2 - db^2 = 1$ (2).

Dacă $d = -1$ ecuația (2) devine $a^2 + b^2 = 1$ și admite în $\mathbb{Z} \times \mathbb{Z}$ soluțiile (1, 0), (-1, 0), (0, 1) și (0, -1). Rezultă $U(\mathbb{Z}[i]) = \{1, -1, i, -i\}$.

Dacă $d \leq -2$, ecuația (2) admite ca soluții (a, b) $\in \mathbb{Z} \times \mathbb{Z}$ doar cuplurile (1, 0) și (-1, 0) deci $U(\mathbb{Z}[\sqrt{d}]) = \{-1, 1\}$.

Observație. Pentru $d > 0$ se demonstrează că ecuația (2), numită *ecuația lui Pell*, are o infinitate de soluții în $\mathbb{Z} \times \mathbb{Z}$, deci în cazul $d > 0$ grupul $U(\mathbb{Z}[\sqrt{d}])$ este infinit.

6.34. (i). Fie $z = m + ni$, $m, n \in \mathbb{Z}$.

Avem $\varphi(z) = 0 \Leftrightarrow m^2 + n^2 = 0 \Leftrightarrow m = n = 0 \Leftrightarrow z = 0$.

(ii). Fie $z = m + ni$ și $z' = m' + n'i$ cu $m, m', n, n' \in \mathbb{Z}$.

Avem $\varphi(zz') = \varphi((m+ni)(m'+n'i)) = \varphi((mm' - nn') + i(mn' + m'n)) = (mm' - nn')^2 + (mn' + m'n)^2 = m^2m'^2 + n^2n'^2 - 2mm'nn' + m^2n'^2 + m'^2n^2 + 2mm'nn' = (m^2 + n^2)(m'^2 + n'^2) = \varphi(z) \cdot \varphi(z')$.

(iii). Fie $z, z' \in \mathbb{Z}[i]$, $z = m + ni$ și $z' = m' + n'i \neq 0$.

Atunci $\frac{z}{z'} = \frac{m + ni}{m' + n'i} = \frac{mm' + nn'}{m'^2 + n'^2} + i \frac{-mn' + m'n}{m'^2 + n'^2} = a + ib$, unde $a, b \in \mathbb{Q}$.

Alegem $u, v \in \mathbb{Z}$ a.î. $|a - u| \leq \frac{1}{2}$ și $|b - v| \leq \frac{1}{2}$ și punem $q = u + iv$. Se

verifică faptul că $r = z - qz'$ are proprietatea că $\varphi(r) < \varphi(z')$.

(iv). Dacă $z \in \{\pm 1, \pm i\} \Rightarrow z$ este inversabil \Rightarrow există un $z' \in \mathbb{Z}[i]$ a.î. $zz' = 1 \Rightarrow \varphi(zz') = \varphi(z) \cdot \varphi(z') = 1 \Rightarrow \varphi(z) = 1$.

Fie $z = m + ni$ și $\varphi(z) = 1$. Atunci $z' = m - ni$ este inversul lui z , deci z este inversabil. Avem $\varphi(z) = 1 \Leftrightarrow z$ este inversabil.

Dacă $\varphi(z)=1 \Rightarrow m^2+n^2=1 \Rightarrow m^2=0$ și $n^2=1$ sau $m^2=1$ și $n^2=0 \Rightarrow z \in \{\pm 1, \pm i\}$.

6.35. (i). Fie $z=m+ni\sqrt{2}$, $m, n \in \mathbb{Z}$.

Avem $\varphi(z)=0 \Leftrightarrow m^2+2n^2=0 \Leftrightarrow m=n=0 \Leftrightarrow z=0$.

(ii). Fie $z=m+ni\sqrt{2}$ și $z'=m'+n'i\sqrt{2}$ cu $m, m', n, n' \in \mathbb{Z}$.

Avem

$$\begin{aligned} \varphi(zz') &= \varphi((m+ni\sqrt{2})(m'+n'i\sqrt{2})) = \varphi((mm'-2nn')+i\sqrt{2}(mn'+m'n)) = \\ &= (mm'-2nn')^2 + 2(mn'+m'n)^2 = \\ &= m^2m'^2 + 4n^2n'^2 - 4mm'nn' + 2m^2n'^2 + 2m'^2n^2 + 4mm'nn' = \\ &= m^2(m'^2+2n'^2) + 2n^2(m'^2+2n'^2) = (m^2+2n^2)(m'^2+2n'^2) = \varphi(z) \cdot \varphi(z'). \end{aligned}$$

(iii). Fie $z, z' \in \mathbb{Z}[i\sqrt{2}]$, $z=m+ni\sqrt{2}$ și $z'=m'+n'i\sqrt{2} \neq 0$.

$$\text{Atunci } \frac{z}{z'} = \frac{m+ni\sqrt{2}}{m'+n'i\sqrt{2}} = \frac{mm'+2nn'}{m'^2+2n'^2} + i\sqrt{2} \frac{-mn'+m'n}{m'^2+2n'^2} = a+ib\sqrt{2}, \text{ unde } a,$$

$b \in \mathbb{Q}$.

Alegem $u, v \in \mathbb{Z}$ a.î. $|a-u| \leq \frac{1}{2}$ și $|b-v| \leq \frac{1}{2} < \frac{\sqrt{2}}{2}$ și punem $q=u+iv$. Se

verifică faptul că $r=z-qz'$ are proprietatea că $\varphi(r) < \varphi(z')$.

(iv). Dacă $z \in \{\pm 1\} \Rightarrow z$ este inversabil \Rightarrow există un $z' \in \mathbb{Z}[i\sqrt{2}]$ a.î.

$zz'=1 \Rightarrow \varphi(zz')=\varphi(z) \cdot \varphi(z')=1 \Rightarrow \varphi(z)=1$.

Fie $z=m+ni\sqrt{2}$ și $\varphi(z)=1$. Atunci $z'=m-ni\sqrt{2}$ este inversul lui z , deci z este inversabil. Avem $\varphi(z)=1 \Leftrightarrow z$ este inversabil.

Dacă $\varphi(z)=1 \Rightarrow m^2+2n^2=1 \Rightarrow m^2=1$ și $n^2=0 \Rightarrow n=0$ și $m=\pm 1 \Rightarrow z \in \{\pm 1\}$.

6.36. Notăm $N(A) = \{a \in A \mid \text{există } n \in \mathbb{N} \text{ a.î. } a^n = 0\}$.

Dacă $x \in U(A)$ și $y \in N(A)$, demonstrăm că $x+y \in U(A)$.

Scriind $x+y = x(1+x^{-1}y)$, cum $x^{-1}y = z \in N(A)$ pentru a demonstra că $x+y \in U(A)$ este suficient să arătăm că dacă $z \in N(A)$, atunci $1+z \in U(A)$.

Scriind din nou $1+z = 1-(-z)$, cum $t = -z \in N(A)$, totul s-a redus la a proba că dacă $t \in N(A)$ atunci $1-t \in U(A)$. Din $t \in N(A)$ rezultă că există $n \in \mathbb{N}$ a.î. $t^n = 0$ și astfel $1 = 1 - 0 = 1 - t^n = (1-t)(1+t+t^2+\dots+t^{n-1})$, de unde rezultă că $1-t \in U(A)$ iar $(1-t)^{-1} = 1+t+t^2+\dots+t^{n-1}$.

6.37. Faptul că adunarea și înmulțirea matricelor sunt operații algebrice pe A se verifică imediat; de asemenea structura de inel unitar se stabilește ușor. În acest inel matricea nulă O_3 este elementul zero, iar matricea unitate I_3 este elementul unitate.

Vom demonstra că inelul A este necomutativ.

Fie pentru aceasta matricele $X, Y \in A$, $X = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$, $Y = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix}$.

Avem $XY = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$, $YX = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$, deci $XY \neq YX$.

Să arătăm acum că orice element din A este inversabil sau nilpotent.

Pentru aceasta să considerăm un element $X \in A$, arbitrar, $X = \begin{pmatrix} a & b & c \\ 0 & a & d \\ 0 & 0 & a \end{pmatrix}$. Avem

$\det(X) = a^3$ și dacă $a \neq 0$, atunci X este o matrice inversabilă în inelul $M_3(\mathbb{R})$, dar se constată ușor că $X^{-1} \in A$ și aceasta înseamnă că X este element inversabil în

A . Dacă însă $a = 0$, atunci $X = \begin{pmatrix} 0 & b & c \\ 0 & 0 & d \\ 0 & 0 & 0 \end{pmatrix}$ și se observă că $X^3 = O_3$, ceea ce

înseamnă că X este element nilpotent în inelul A .

6.38. „ \Rightarrow ”. Dacă $\hat{m} \in \mathbb{Z}_n$ este element nilpotent, fie t a.î. $(\hat{m})^t = \hat{0}$. Atunci n divide m^t și deci fiecare p_i divide m^t . Numerele $\{p_i | 1 \leq i \leq k\}$ fiind prime, fiecare p_i divide m , adică $p_1 \dots p_k$ divide m .

„ \Leftarrow ”. Invers, dacă $p_1 \dots p_k | m \Rightarrow$ există $s \in \mathbb{Z}$ a.î. $m = s \cdot p_1 \dots p_k$. Pentru $n = p_1^{r_1} \dots p_k^{r_k}$ aleg $r = \max_{1 \leq i \leq k} r_i$. Evident $m^r = s^r p_1^{r_1} \dots p_k^{r_k} = n s^r p_1^{r-r_1} \dots p_k^{r-r_k}$, adică $(\hat{m})^r = \hat{0}$, deci $\hat{m} \in \mathbb{Z}_n$ este element nilpotent.

6.39. Fie $\varphi: \text{Idemp}(\mathbb{Z}_n) \rightarrow A$ definită prin $\varphi(x) =$ mulțimea numerelor prime distincte ce apar în descompunerea lui (x, n) .

Fie $\hat{x} \in \mathbb{Z}_n$ un element idempotent. Atunci $\hat{x}^2 = \hat{x}$, adică $n | x(x-1)$. Cum $\frac{x}{(x, n)}$

și $\frac{n}{(x, n)}$ sunt prime între ele, deducem că $\frac{n}{(x, n)} | x-1$. Deci (x, n) și $\frac{n}{(x, n)}$ sunt prime între ele pentru că sunt divizori ai unor numere prime între ele: x și $x-1$.

Rezultă că puterea unui prim, p_i , care se află în descompunerea lui (x, n) este α_i , altfel (x, n) și $\frac{n}{(x, n)}$ nu ar fi prime între ele.

Deci $\varphi(x)$ caracterizează perfect (x, n) .

Observăm că φ este o injecție.

Într-adevăr, dacă $\varphi(\hat{x}) = \varphi(\hat{y})$, atunci $(x, n) = (y, n)$ și rezultă că $\frac{n}{(x, n)} | x-1$ și $\frac{n}{(x, n)} | y-1$. Deci $\frac{n}{(x, n)} | x-y$. Cum $(x, n) | x-y$ și este prim cu $\frac{n}{(x, n)}$ deducem că n divide $x-y$, adică $\hat{x} = \hat{y}$.

φ este surjecție.

Dacă I este mulțimea indicilor numerelor prime care aparțin unui element din A , atunci considerăm numărul natural $a = \prod_{i \in I} p_i^{\alpha_i}$ ($a=1$ dacă $I=\emptyset$).

Evident există întregii s, t a.î. $sa + t\frac{n}{a} = 1$.

Fie $x=sa$. Evident, $n|x(x-1)$, adică x este idempotent. Rezultă $a=(x, n)$ și deci $\varphi(\hat{x}) = \{p_i\}_{i \in I}$.

Avem $12=2^2 \cdot 3$ și $A = \{\emptyset, \{2\}, \{3\}, \{2,3\}\}$. Elementelor lui A le corespund, în ordine, numerelor naturale $a_1=1, a_2=4, a_3=3, a_4=12$. Deci $\hat{x}_1 = \hat{1}, \hat{x}_2 = \hat{4}$ ($4-3=1$, adică $s_2=1$), $\hat{x}_3 = \hat{9}$ ($4-3=1$ adică $s_3=-1, x_2=-3$), $\hat{x}_4 = \hat{0}$.

6.40. Fie $n = p_1^{k_1} \dots p_r^{k_r}$ descompunerea în factori primi a lui n a.î. $k_i \geq 1, i \in \{1, \dots, r\}$ și $(p_i, p_j) = 1$ pentru $i \neq j$. Avem că $\hat{x} \in \mathbb{N} \Leftrightarrow p_i | x$ pentru orice $i \in \{1, \dots, r\}$. Fie acum $\hat{x} \in \mathbb{N} \cap I$. Există $k, m \in \mathbb{N}$ a.î. $\hat{x}^k = \hat{0}$ și $\hat{x}^m = \hat{x}$. Atunci $\hat{x}^{\wedge m} = \hat{x}$ oricare ar fi $i \geq 1$. Dacă luăm $m' \geq k$ atunci $\hat{x}^{\wedge m'} = \hat{0}$. Avem $\hat{x} = \hat{x}^{\wedge m'} = \hat{x}^{\wedge k+s} = \hat{x}^{\wedge k} \cdot \hat{x}^{\wedge s} = \hat{0} \Rightarrow \hat{x} = \hat{0}$ (unde $m' = k+s$).

6.41. Dacă $\hat{a} \in \mathbb{Z}_n$ este inversabil, există $\hat{b} \in \mathbb{Z}_n$ a.î. $\hat{a} \cdot \hat{b} = \hat{1}$. Deci $ab \equiv 1 \pmod{n}$, adică există $k \in \mathbb{Z}$ a.î. $ab-1=kn$, sau $ab+(-k)n=1$. De aici obținem că $(a, n)=1$. Reciproca este evidentă deoarece toate implicațiile de mai sus sunt echivalente.

6.42. (i). Presupunem prin reducere la absurd că ecuația are o soluție $\hat{x}_0 \in \mathbb{Z}_n$ și totuși $d \nmid b$. Atunci $\hat{a} \cdot \hat{x}_0 = \hat{b}$, deci $n \mid ax_0 - b$. Cum $d \mid n$ și $d \mid a$ rezultă $d \mid b$, contradicție cu presupunerea făcută.

(ii). Presupunem că $d \mid b$. Cum $d = (a, n)$ există $x_0' \in \mathbb{Z}$ și $y_0' \in \mathbb{Z}$ a.î. $d = ax_0' - ny_0'$. Dacă $c = \frac{b}{d}$, atunci $a(x_0'c) - n(y_0'c) = b$, adică $\hat{a} \left(\hat{x}_0'c \right) = \hat{b}$, deci $\hat{x}_0'c$ este soluție a ecuației $\hat{a}\hat{x} = \hat{b}$.

Să presupunem acum că \hat{x}_0 și \hat{x}_1 sunt două soluții ale ecuației $\hat{a}\hat{x} = \hat{b}$. Atunci $n \mid ax_0 - b$ și $n \mid ax_1 - b$ de unde $n \mid a(x_1 - x_0)$. Dacă notăm $n' = \frac{n}{d}$ și $a' = \frac{a}{d}$ atunci $(a', n') = 1$ și obținem $n' \mid x_1 - x_0$, adică $x_1 = x_0 + kn'$, cu $k \in \mathbb{Z}$.

Pe de altă parte, se verifică imediat că $\hat{x}_0 + kn'$ este o soluție a ecuației $\hat{a}\hat{x} = \hat{b}$ cu $k \in \{0, 1, \dots, d-1\}$. Cum nu este posibil să avem $\hat{x}_0 + kn' = \hat{x}_0 + k'n'$, pentru $k, k' \in \{0, 1, \dots, d-1\}$ și $k \neq k'$ (căci ar trebui ca $n \mid n'(k-k') \Leftrightarrow d \mid k-k'$, absurd) deducem că dacă $\hat{x}_0 \in \mathbb{Z}_n$ este soluție a ecuației $\hat{a}\hat{x} = \hat{b}$, atunci această

ecuație are d soluții și anume: $\hat{x}_0, \hat{x}_0 + n', \dots, \hat{x}_0 + (d-1)n'$.

(iii). Pentru $(a, n) = 1$ ecuația are soluție unică. Cum $(a, n) = 1$ există $u, v \in \mathbb{Z}$ a.î. $au + vn = 1$. Trecând la clase $\hat{a}\hat{u} = \hat{1}$. Deci soluția este $x = \hat{u}\hat{b}$.

6.43. Să notăm cu A mulțimea soluțiilor ecuației omogene $ax=0$, soluții considerate în inelul \mathbb{Z}_n ; de asemenea să notăm cu B mulțimea soluțiilor din \mathbb{Z}_n ale ecuației neomogene $ax=b$.

Fie x_0 o soluție fixată a ecuației neomogene (conform ipotezei această ecuație are soluții), deci $ax_0=b$. Vom demonstra că aplicația $\varphi: A \rightarrow B$, $\varphi(x) = x + x_0$ este o bijecție.

Mai întâi este clar că aplicația φ este bine definită, în sensul că pentru $x \in A$, avem $\varphi(x) \in B$. Într-adevăr, dacă $x \in A \Rightarrow ax=0$ și atunci $a(x+x_0) = ax + ax_0 = 0 + b = b$.

Funcția φ este injectivă, căci $\varphi(x) = \varphi(x') \Rightarrow x + x_0 = x' + x_0 \Rightarrow x = x'$.

De asemenea φ este surjectivă: luând $y \in B$ arbitrar și notând $x = y - x_0$, avem $x \in A$ căci $ax = a(y - x_0) = ay - ax_0 = b - b = 0$ și $\varphi(x) = y$.

Deoarece $\varphi: A \rightarrow B$ este bijecție, rezultă că A și B au același cardinal, deci ecuațiile au același număr de soluții în \mathbb{Z}_n .

Observație. Problema are loc în orice inel finit, sau mai general, în orice inel, dacă formulăm drept cerință existența unei bijecții între mulțimile de soluții A și B .

6.44. (i). Sistemul nu poate fi rezolvat prin metoda substituției deoarece nici unul dintre coeficienții săi nu este inversabil în \mathbb{Z}_{12} . Scăzând prima ecuație

$$\text{din a doua obținem: } \begin{cases} 3x + 2y = \hat{1} \\ x + y = \hat{1} \end{cases} \Leftrightarrow \begin{cases} 2x + y = \hat{0} \\ x + y = \hat{1} \end{cases} \Leftrightarrow \begin{cases} x = \hat{1} \\ y = \hat{2} \end{cases}.$$

(ii). Deoarece $\hat{7}$ este inversabil în \mathbb{Z}_{12} înmulțim prima ecuație cu

$$\text{inversul său, deci tot cu } \hat{7}. \text{ Obținem: } \begin{cases} x + \hat{9}y = \hat{2} \\ 4x + \hat{6}y = \hat{3} \end{cases} \Leftrightarrow \begin{cases} x = \hat{2} + \hat{3}y \\ \hat{8} + \hat{6}y = \hat{3} \end{cases} \Leftrightarrow$$

$$\begin{cases} x = \hat{2} + \hat{3}y \\ \hat{6}y = \hat{7} \end{cases}$$

Sistemul este incompatibil, ecuația $\hat{6}y = \hat{7}$ neavând soluții în \mathbb{Z}_{12} .

6.45. (i). Din $(1+1)^2 = 1+1$ deducem că $1+1+1+1 = 1+1$, adică $1+1 = 0$ și deci $\text{car}(A) = 2$.

(ii). Fie $x, y \in A$ arbitrare. Avem conform ipotezei $(x+y)^2 = x+y$. (1)

Pe de altă parte: $(x+y)^2 = (x+y)(x+y) = x^2 + xy + yx + y^2 = x + xy + yx + y$,

deci $(x+y)^2 = x + xy + yx + y$. (2)

Din (1) și (2) rezultă că $x + xy + yx + y = x + y$, deci $xy + yx = 0$, adică $xy = -yx$. (3)

Dar conform punctului (i), orice element coincide cu opusul său, astfel că egalitatea (3) devine $xy = yx$. Cum x, y au fost alese arbitrare în inelul A , rezultă că A este inel comutativ.

6.46. „ \Rightarrow ”. Dacă A este inel boolean avem $a = a^2 = \dots = a^n = \dots$ și evident zero este singurul element nilpotent. Avem $(a+b)ab = a^2b + ab^2 = ab + ba = 0$.

„ \Leftarrow ”. Reciproc, punând $b=a$ în relația dată obținem $(a+a) \cdot a \cdot a=0 \Leftrightarrow a^3+a^3=0$, de unde, prin înmulțiri succesive cu a obținem $a^n+a^n=0$, oricare ar fi $n \in \mathbb{N}, n \geq 3$.

Fie $b=a^2-a$. Obținem $a^4=a^5$ și prin înmulțiri succesive cu a avem $a^4=a^5=\dots=a^n=\dots$, pentru orice $n \in \mathbb{N}, n \geq 4$. În particular, $a^8=a^4$, deci este verificată $(a^2-a)^4=0$. Avem $(a^2-a)^2=a^4+a^2-a^3-a^3=a^4+a^2$ și prin urmare

$$(a^2-a)^4=(a^4+a^2)^2=a^8+a^6+a^6+a^4=a^4+a^4=0.$$

Cum A nu are elemente nilpotente nenule, $a^2-a=0$ și $a^2=a$.

6.47. Luând $a=-1$ obținem că în inelul dat are loc egalitatea $1+1=0$ și deci $1+1+1=1$. Luând un element oarecare $a \in A$ vom ține cont de faptul că $-a=a$ și de cele două relații:

$$a^3+a=0 \text{ și } (1+a)^3+(1+a)=0.$$

Efectuând calculele în a doua relație obținem $1+3a+3a^2+a^3+1+a=0$, de unde rezultă $a^2=a$, deci inelul A este boolean.

6.48. Demonstrăm mai întâi că $y \in A, y^2=0 \Rightarrow y=0$. Într-adevăr $y^2=0 \Rightarrow y^{2^{k(y)+1}}=0 \Rightarrow y=0$. Fie $x \in A$ fixat. Atunci

$$x^{2^k+1}=x \Rightarrow (x^{2^{k-1}+1}-x)^2=x^{2^k+2}-x^2=x(x^{2^k+1}-x)=0 \Rightarrow x^{2^{k-1}+1}-x=0 \Rightarrow x^{2^{k-1}+1}=x. \text{ Deci } k \text{ poate fi micșorat până la } k=0, \text{ deci } x^2=x.$$

6.49. Pentru $a=xab$ avem $a=a^2=(xab)^2=x(xa^2b^2)=x(xab)=xa$ respectiv pentru $x=a+b+ab$ rezultă:

$$\begin{aligned} xa &= (a+b+ab)a = a^2+ab+a^2b = a^2+ab+ab = a^2=a, \\ xb &= (a+b+ab)b = ab+b^2+ab^2 = ab+b^2+ab = b^2=b, \end{aligned}$$

(înmulțirea este comutativă și $\text{car}(A)=2$).

$$\text{În final, alegem } x = \sum_{i=1}^n a_i + \sum_{1 \leq i < j \leq n} a_i a_j + \dots + a_1 a_2 \dots a_n.$$

6.50. Din $x^6=x$ și $(-x)^6=-x$ rezultă $x=-x$ și atunci $\text{car}(A)=2$.

Din $(x+1)^6=x+1$ dezvoltând membrul drept obținem:

$$(x^6-x)+2(3x^5+7x^4+10x^3+7x^2+3x)+(x^4+x^2)=0 \Rightarrow x^4+x^2=0.$$

Atunci $x^4=-x^2=x^2$ și înmulțind cu x^2 obținem în final $x=x^6=x^4=x^2$.

6.51. Înlocuind pe x cu $-x$ în ipoteză, rezultă $(-x)^{12} = -x$ dar $(-x)^{12} = x^{12} = x$ și prin urmare $x = -x$, adică $2x = 0$, oricare ar fi $x \in A$ (1).

Din (1) rezultă că pentru orice $x \in A$ și $k \in \mathbb{Z}$ avem $kx = 0$, pentru k par, respectiv $kx = x$, pentru k impar.

Ținând cont de aceasta și de faptul că x și 1 comută la înmulțire putem scrie $(x+1)^{12} = x^{12} + C_{12}^1 x^{11} + C_{12}^2 x^{10} + \dots + C_{12}^{10} x^2 + C_{12}^{11} x + 1$
 $= x^{12} + 12x^{11} + 66x^{10} + 220x^9 + 495x^8 + 792x^7 + 924x^6 + 792x^5 + 495x^4 + 220x^3 + 66x^2 + 12x + 1 = x^{12} + x^8 + x^4 + 1.$

Dar din ipoteză $(x+1)^{12} = x+1$. Rezultă egalitatea $x^{12} + x^8 + x^4 + 1 = x+1$, de unde ținând cont că $x^{12} = x$, deducem $x^8 + x^4 = 0$. Adunând x^4 obținem $x^8 = x^4$. Înmulțind această egalitate cu x^4 obținem $x^{12} = x^8$ adică, $x = x^8$, deci $x = x^4$. (2)

Înmulțim cu x^8 și avem $x^9 = x^{12}$ sau $x^9 = x$ sau $(x^4)^2 x = x$, sau conform cu (2), $x^2 \cdot x = x$, adică $x^3 = x$. Înmulțind această egalitate cu x obținem $x^4 = x^2$ și folosind (2), rezultă $x = x^2$, ceea ce trebuia demonstrat.

6.52. (i). Din $x^3 = x$, deducem $x^4 = x^2$. Atunci

$$(x^2 y x^2 - x^2 y)^2 = (x^2 y x^2 - x^2 y)(x^2 y x^2 - x^2 y) = x^2 y x^4 y x^2 - x^2 y x^4 y - x^2 y x^2 y x^2 + x^2 y x^2 y = 0.$$

Analog $(x^2 y x^2 - y x^2)^2 = 0$.

(ii). Avem $(x^2 y x^2 - x^2 y)^3 = x^2 y x^2 - x^2 y = 0$. La fel $(x^2 y x^2 - y x^2)^3 = x^2 y x^2 - y x^2 = 0$, adică $x^2 y x^2 = x^2 y$, $x^2 y x^2 = y x^2$, deci $x^2 y = y x^2$, oricare ar fi $x, y \in A$.

Înlocuind x cu $x+1$ obținem $(x+1)^2 y = y(x+1)^2$, de unde $2xy = 2yx$. Dacă inelul A este de caracteristică diferită de 2 deducem că $xy = yx$. În cazul în care A este de caracteristică 2 deducem că $(a+1)^3 = a+1$, oricare ar fi $a \in A$, de unde $a^2 = a$, deci A este boolean, adică comutativ (vezi problema 6.45.).

6.53. Fie $A = \{a_1, a_2, \dots, a_n\}$ și $a \in A$. Cum $\{a, a^2, \dots, a^{n+1}\} \subset A$ există $i < j$ a.î. $a^i = a^{i+j}$. De aici, $a^k = a^{k+jl}$, oricare ar fi $k \geq i$ și $l \in \mathbb{N}$.

Aplicăm această observație pentru fiecare element al inelului A :

există i_1, j_1 a.î. $a_1^k = a_1^{k+j_1 l}$, oricare ar fi $k \geq i_1, l \in \mathbb{N}$;

.....

există i_n, j_n a.î. $a_n^k = a_n^{k+j_n l}$, oricare ar fi $k \geq i_n, l \in \mathbb{N}$;

Alegem acum $p \geq \max\{i_1, i_2, \dots, i_n\}$ și $q = \text{c.m.m.m.c.}\{j_1, j_2, \dots, j_n\}$ și rezultă $a^p = a^{p+q}$, oricare ar fi $a \in A$.

6.54. Notăm cu (E_k) egalitatea din enunț.

Ea se scrie echivalent: $\sum_{j=1}^{k-1} a^{k-j} b^j = b \sum_{j=1}^{k-1} a^{k-j} b^{j-1}$.

Dacă (E_m) și (E_{m+1}) sunt adevărate

$$\begin{aligned} \sum_{j=1}^m a^{m+1-j} b^j &= a^m b + \left(\sum_{i=1}^{m-1} a^{m-i} b^i \right) b \stackrel{(E_m)}{=} a^m b + b \left(\sum_{i=1}^{m-1} a^{m-i} b^{i-1} \right) b \stackrel{(E_{m+1})}{=} b \sum_{j=1}^m a^{m+1-j} b^{j-1} = \\ &= b a^m + b \sum_{i=1}^{m-1} a^{m-i} b^i \end{aligned}$$

de unde rezultă că $a^m b = b a^m$. Din (E_{m+1}) și (E_{m+2}) rezultă analog $a^{m+1} b = b a^{m+1}$, deci din (E_m) , (E_{m+1}) și (E_{m+2}) avem $a^{m+1} b = a \cdot a^m \cdot b = a b a^m = b a^{m+1} = b a \cdot a^m$.

Cum a este inversabil, din $a b a^m = b a a^m$ rezultă $a b = b a$.

6.55. (i). Punând $x = -1$ obținem $-1 = 1$ de unde $x + x = 0$, oricare ar fi $x \in A$. De aici $(1+x)^2 = 1 + x + x + x^2 = 1 + x^2$. De asemenea, oricare ar fi $x \in A$, $m \geq n$, $x^m = x^n$. Dacă $x^2 = 0$ atunci $(1+x)^2 = 1$, deci $(1+x)^{2n+1} = (1+x)^{2n} = 1$, adică $(1+x)(1+x)^{2n} = 1$, de unde $1+x = 1$, deci $x = 0$ și am demonstrat (i).

(ii). Avem $(x^2 + x)^{2^n} = x^{2^{n+1}} + x^{2^n} = x^{2^n} + x^{2^n} = 0$, de unde $x^2 + x = 0$, adică $x^2 = x$, oricare ar fi $x \in A$.

6.56. Se observă imediat că dacă A este un p -inel atunci acesta este redus (din $x^p = x$, rezultă prin inducție după $n \geq 1$ că $x^{p^n} = x$; deci dacă x este nilpotent există $n \geq 1$ cu $x^{p^n} = 0$, adică $x = 0$).

Tot din $x^p = x$ deducem că $(x^{p-1})^2 = x^{2p-2} = x^p \cdot x^{p-2} = x \cdot x^{p-2} = x^{p-1}$, adică x^{p-1} este idempotent. De aici rezultă prin calcul direct că pentru orice $x, y \in A$

$$(1) \quad (x^{p-1} y x^{p-1} - x^{p-1} y)^2 = 0 = (x^{p-1} y x^{p-1} - y x^{p-1})^2.$$

Din (1) rezultă conform faptului că A este redus (singurul element nilpotent al lui A este zero):

$$x^{p-1} y x^{p-1} - x^{p-1} y = 0 = x^{p-1} y x^{p-1} - y x^{p-1}$$

$$\text{adică } (2) \quad x^{p-1} y = x^{p-1} y x^{p-1} = y x^{p-1}.$$

Deci $x^{p-1} \in Z(A)$.

Deoarece $x^p = x$ și $x^{p-1} \in Z(A)$ deducem că:

(3) $(xy-yx)^{p-1} = xy-yx = x^{p-1}(xy-yx)$ (de exemplu:

$$(xy-yx)x^{p-1} = xyx^{p-1} - yxx^{p-1} = x^{p-1}xy - yx^p = xy-yx).$$

Dar (3) este adevărată pentru orice x, y deci este adevărată și dacă x se înlocuiește cu $x+i$, unde $1 \leq i \leq p-1$.

Deoarece însă $(x+i)y-y(x+i) = xy-yx+iy-yi = xy-yx$, deducem din (3):

$$(4) (x+i)^{p-1}(xy-yx) = xy-yx, \text{ pentru } 0 \leq i \leq p-1.$$

Să observăm că din $px=0$ rezultă conform micii teoreme a lui Fermat și din faptul că numărul soluțiilor unei congruențe nu poate depăși gradul acesteia (teorema lui Lagrange) că:

$$(5) (x+1)(x+2)\dots(x+(p-1)) = x^{p-1} + (p-1)! = x^{p-1} - 1.$$

Aplicând acum în ordine ipoteza ($x^p=x$) și relațiile (4), (2) și (5) obținem:

$$\begin{aligned} xy-yx &= (xy-yx)^p = [x^{p-1}(xy-yx)][(x+1)^{p-1}(xy-yx)]\dots[(x+(p-1))^{p-1}(xy-yx)] = \\ &= x^{p-1}(x+1)^{p-1}\dots(x+(p-1))^{p-1}(xy-yx)^p = [x(x+1)\dots(x+(p-1))]^{p-1}(xy-yx)^p = \\ &= [x(x^{p-1}-1)]^{p-1}(xy-yx) = (x^p-x)^{p-1}(xy-yx) = 0. \text{ Deci } xy-yx=0, \text{ adică } A \text{ este} \\ &\text{comutativ.} \end{aligned}$$

6.57. Conform ipotezei rezultă că aplicația $f_0: A \times A \rightarrow A$ definită prin $f_0(x,y) = (xy)^2 - x^2y^2$ este identic nulă.

Deci și $f_1: A \times A \rightarrow A$, $f_1(x,y) = f_0(x+1,y) - f_0(x,y)$ este identic nulă.

Efectuând calculele obținem $f_1(x,y) = -xy^2 + yxy = 0$.

Rezultă că și $f_2: A \times A \rightarrow A$, $f_2(x,y) = f_1(x,y+1) - f_1(x,y)$ va fi identic nulă.

Deci $0 = f_2(x,y) = f_1(x,y+1) - f_1(x,y) = -x(y+1)^2 + (y+1)x(y+1) + xy^2 - yxy = -2xy - x + xy + yx + x = yx - xy$, adică A este comutativ.

6.58. Fie $e \in A$ un element idempotent. Deci $e^2 = e$.

Pentru a arăta că $e \in Z(A)$, fie a un element arbitrar din inelul A și să notăm cu x diferența $ea - ae$. Vom demonstra că $x = 0$.

Într-adevăr, $ex + xe = ea - eae + eae - ae = x$, de unde $ex = x(1-e)$.

Întrucât $(1-e)e = e - e^2 = 0$ obținem: $(ex)e = x(1-e)e = x \cdot 0 = 0$, deci $(ex)^2 = ((ex)e)x = 0 \cdot x = 0$.

Așadar ex este nilpotent. Conform ipotezei, $ex = 0$ și în mod analog demonstrăm și că $xe = 0$. Deci $x = ex + xe = 0$.

6.59. Observăm că dacă x este idempotent atunci și $1-x$ este idempotent:

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

Rezultă că elementele lui M se pot grupa în perechi de forma $(x, 1-x)$. Elementele din oricare asemenea pereche sunt distincte.

Într-adevăr, dacă ar exista $x_0 \in M$ cu proprietatea că $x_0 = 1-x_0$, înmulțind cu x_0 și ținând cont că $x_0^2 = x_0$, obținem $x_0^2 = x_0 - x_0^2$ adică $x_0 = x_0 - x_0$, deci $x_0 = 0$.

În felul acesta egalitatea $x_0 = 1-x_0$ conduce la $1=0$, contradicție.

Notând cu n numărul perechilor din M de tipul descris mai sus, rezultă că M are $2n$ elemente.

6.60. Evident, 1 este element idempotent nenul. Avem două cazuri:

1) Singurul idempotent nenul este 1 . Atunci produsul elementelor idempotente nenule este egal cu 1 .

2) Există cel puțin un element idempotent nenul, diferit de 1 .

Fie x un astfel de element. Atunci și $1-x$ este element idempotent nenul conform soluției problemei **6.59**. Dar produsul elementelor idempotente nenule x și $1-x$ este $x(1-x) = x-x^2 = x-x = 0$.

Atunci produsul tuturor elementelor idempotente nenule este egal cu 0 .

6.61. (i). Pentru orice $x \in A$ avem $x+x = 1 \cdot x + 1 \cdot x = (1+1) \cdot x = 0 \cdot x = 0$, deci

$$(1+x)^2 = 1+x+x+x^2 = 1+x^2 = \begin{cases} 1, & \text{pentru } x \in O_A \\ 0, & \text{pentru } x \in E_A \\ 1+x, & \text{pentru } x \in I_A \end{cases}.$$

(ii). Conform punctului (i) putem defini aplicațiile $\varphi: O_A \rightarrow E_A$, $\varphi(x) = 1+x$, oricare ar fi $x \in O_A$, $\psi: E_A \rightarrow O_A$, $\psi(x) = 1+x$, oricare ar fi $x \in E_A$.

Pentru orice $x \in O_A$ avem:

$$(\psi \circ \varphi)(x) = \psi(\varphi(x)) = \psi(1+x) = 1+1+x = x$$

și analog pentru orice $x \in E_A$ avem:

$$(\varphi \circ \psi)(x) = \varphi(\psi(x)) = \varphi(1+x) = 1+1+x = x.$$

Deci $\psi \circ \varphi = 1_{O_A}$ și $\varphi \circ \psi = 1_{E_A}$. Atunci φ este bijectivă, adică $|O_A| = |E_A|$.

6.62. (i). Fie A un inel cu proprietatea $\mathbb{Z} \subseteq A \subseteq \mathbb{Z}[\sqrt{d}]$ și $A \neq \mathbb{Z}$. Atunci există $a+b\sqrt{d} \in A \setminus \mathbb{Z}$, deci $b \neq 0$. Cum $a \in \mathbb{Z} \subseteq A$ avem $(a+b\sqrt{d})-a \in A$, adică $b\sqrt{d} \in A$. Dar atunci $-b\sqrt{d} \in A$ și deci $|b|\sqrt{d} \in A$, unde $|b|$ este număr natural nenul.

Fie $k \in \mathbb{N}^*$ cel mai mic număr natural nenul pentru care $k\sqrt{d} \in A$.

Arătăm că avem egalitatea $A = \mathbb{Z}[k\sqrt{d}] = \{a + bk\sqrt{d} \mid a, b \in \mathbb{Z}\}$.

Deoarece $k\sqrt{d} \in A$ rezultă că $bk\sqrt{d} \in A$, pentru orice $b \in \mathbb{Z}$ și cum pentru orice $a \in \mathbb{Z}$ avem $a \in A$, obținem că $a + bk\sqrt{d} \in A$, oricare ar fi $a, b \in \mathbb{Z}$. Cu aceasta am demonstrat incluziunea $\{a + bk\sqrt{d} \mid a, b \in \mathbb{Z}\} \subseteq A$.

Pentru cealaltă incluziune, fie $x \in A$, arbitrar.

Deoarece $A \subseteq \mathbb{Z}[k\sqrt{d}]$ există $a, b \in \mathbb{Z}$ cu proprietatea $x = a + bk\sqrt{d}$. Conform teoremei împărțirii cu rest, există $q, r \in \mathbb{Z}$ a.î. $b = kq + r$ și $0 \leq r < k$. Atunci $x = a + b\sqrt{d} = a + kq\sqrt{d} + r\sqrt{d}$ și cum $a \in \mathbb{Z} \subseteq A$, $kq\sqrt{d} \in A$, vom avea $x - a - kq\sqrt{d} \in A$, adică $r\sqrt{d} \in A$. Datorită minimalității lui $k \in \mathbb{N}^*$, rezultă $r = 0$ și astfel $b = kq$, deci $x = a + kq\sqrt{d} \in \mathbb{Z}[k\sqrt{d}]$.

Cu aceasta am demonstrat și incluziunea $A \subseteq \mathbb{Z}[k\sqrt{d}]$, deci egalitatea $A = \mathbb{Z}[k\sqrt{d}]$.

Prin urmare inelele cerute sunt cele de tipul $\mathbb{Z}[k\sqrt{d}]$, cu $k \in \mathbb{N}$ (pentru $k = 0$ se obține $A = \mathbb{Z}$, iar pentru $k = 1$ se obține $A = \mathbb{Z}[\sqrt{d}]$).

Observație. În această soluție am folosit doar structura de grup aditiv din inelele \mathbb{Z} , A , $\mathbb{Z}[\sqrt{d}]$, $\mathbb{Z}[k\sqrt{d}]$. În acest fel, problema rămâne valabilă, cu aceeași soluție, dacă o reformulăm astfel: „Să se determine grupurile abeliene A cu proprietatea $\mathbb{Z} \subseteq A \subseteq \mathbb{Z}[\sqrt{d}]$ ”.

(ii). Vom arăta că singurele inele B cu proprietatea $\mathbb{Q} \subseteq B \subseteq \mathbb{Q}(\sqrt{d})$ sunt $B = \mathbb{Q}$ și $B = \mathbb{Q}(\sqrt{d})$. Într-adevăr, dacă $B \neq \mathbb{Q}$, există $x = a + b\sqrt{d} \in B \setminus \mathbb{Q}$, cu $a, b \in \mathbb{Q}$ și $b \neq 0$. Deoarece $a \in \mathbb{Q} \subseteq B$, avem $x - a \in B$, adică $b\sqrt{d} \in B$.

Dar $b^{-1} \in \mathbb{Q} \subseteq B$ și atunci $b^{-1}(b\sqrt{d}) \in B$, adică $\sqrt{d} \in B$. Pentru $u, v \in \mathbb{Q}$ oarecare, avem $u + v\sqrt{d} \in B$, deci $\mathbb{Q}(\sqrt{d}) \subseteq B$ și cum avem și cealaltă incluziune deducem $B = \mathbb{Q}(\sqrt{d})$.

6.63. Evident T este subgrup al lui $(M_n(A), +)$. Dacă $A = (a_{ij})$, $B = (b_{ij})$ și $A \cdot B = C = (c_{ij})$ atunci $c_{ij} = \sum_{k=1}^n a_{ik} b_{kj} = \sum_{1 \leq k \leq i} a_{ik} b_{kj} + \sum_{k=i}^n a_{ik} b_{kj} = 0 + \sum_{k=i}^n a_{ik} b_{kj}$.

Dacă $i > j$ atunci $k \geq i > j$ implică $b_{kj} = 0$ și atunci $c_{ij} = 0$.

6.64. $C(S)$ este format din matricele $\{(b_{ij}) \mid b_{ij}=0, i > j \text{ și } b_{ij}=b_{i+1,j+1}\}$

unde $1 \leq i, j < n$, adică din matricele de forma
$$\begin{pmatrix} u_1 & u_2 & \cdots & u_n \\ 0 & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & u_2 \\ 0 & \cdots & 0 & u_1 \end{pmatrix},$$
 unde $u_1, \dots,$

$u_n \in A$.

6.65. Se știe că dacă un număr prim p divide produsul xy , atunci p divide cel puțin unul dintre factori. Deci, adunând și înmulțind fracții cu numitorul nedivizibil prin p , obținem ca rezultate fracții cu numitorul nedivizibil prin p .

Aceasta înseamnă că $\mathbb{Z}_{(p)}$ este subinel al lui \mathbb{Q} .

6.66. (i). Orice subinel al lui \mathbb{Z} trebuie să fie subgrup al grupului aditiv $(\mathbb{Z}, +)$, adică să fie de forma $n\mathbb{Z}$ cu $n \in \mathbb{N}$.

Însă produsul a doi multipli de n este evident multiplu de n , deci mulțimile $n\mathbb{Z}$ sunt subinele ale inelului \mathbb{Z} al numerelor întregi. Dintre ele doar $\mathbb{Z} = 1\mathbb{Z}$ conține elementul unitate 1.

(ii). Adunând și înmulțind fracții al căror numitor este o putere a lui 2, obținem ca rezultat fracții având numitorul o putere a lui 2:

$$\frac{a}{2^n} \pm \frac{b}{2^m} = \frac{2^m a \pm 2^n b}{2^{n+m}}$$

$$\frac{a}{2^n} \cdot \frac{b}{2^m} = \frac{ab}{2^{n+m}}$$

Deci mulțimea $\mathbb{Z}[\frac{1}{2}]$ este subinel al lui \mathbb{Q} , de fapt este „cel mai mic” subinel al lui \mathbb{Q} care conține pe \mathbb{Z} și pe $\frac{1}{2}$.

Observație. În general, dacă p este un număr prim, notând cu $\mathbb{Z}[\frac{1}{p}]$ mulțimea numerelor raționale de forma $\frac{a}{p^n}$, cu $a \in \mathbb{Z}$, $n \in \mathbb{N}$ obținem un exemplu de subinel al lui \mathbb{Q} .

6.67. Dacă mulțimea dată ar fi subinel, pentru $u = \sqrt[3]{5}$ ar exista întregii a și b a.î. $u^2 = au + b$. Avem $5 = u^3 = u(au + b) = a(au + b) + bu = (a^2 + b)u + ab$.

Rezultă $a^2+b=0$ și $ab=5$ iar de aici $-a^3=5$, absurd. Deci mulțimea dată nu este subinel în \mathbb{C} .

6.68. Se verifică ușor axiomele inelului. Elementul neutru la adunare este $0=(0, 0)$ iar elementul unitate este $1=(1, 1)$. Inelul $A_1 \times A_2$ are divizori ai lui zero, de exemplu, $(1, 0) \cdot (0, 1) = (0, 0) = 0$. Elementele inversabile ale lui $A_1 \times A_2$ sunt perechi $(x_1, x_2) \in A_1 \times A_2$, cu x_1 inversabil în A_1 și x_2 inversabil în A_2 .

Aplicație.

a) Elementele inversabile în $\mathbb{Z} \times \mathbb{Z}$ sunt perechi de forma $(\pm 1, \pm 1)$.

b) Elementele inversabile în $\mathbb{Z} \times \mathbb{Q}$ sunt $(\pm 1, \frac{a}{b})$ cu $a, b \in \mathbb{Z}^*$

c) Elementele inversabile în $\mathbb{Z}_m \times \mathbb{Z}_n$ sunt perechi de forma (\hat{a}, \hat{b}) , cu $\hat{a} \in \mathbb{Z}_m$ și $(a, m)=1$, iar $\hat{b} \in \mathbb{Z}_n$ și $(b, n)=1$.

6.69. Cum $\text{car}(A)$ este ordinul lui 1 în grupul $(A, +)$, deducem imediat că $\text{car}(\mathbb{Z} \times \mathbb{Z}) = \text{car}(\mathbb{Z}_3 \times \mathbb{Z}) = \text{car}(\text{End}(\mathbb{Z})) = \infty$ iar $\text{car}(\text{End}(\mathbb{Z}_3)) = 3$.

6.70. Avem $\text{car}(\mathbb{Z}_m \times \mathbb{Z}_n) = \text{ord}([1]_m, [1]_n) = [m, n]$, (am notat $[1]_m$ clasa de echivalență a lui 1 modulo m , respectiv $[1]_n$ clasa de echivalență a lui 1 modulo n) (vezi problema 3.9).

Generalizare. Dacă $\text{car}(A)=m$ și $\text{car}(A')=n$ se poate demonstra analog $\text{car}(A \times A') = [m, n]$.

6.71. Avem $\text{car}(\mathbb{Z}_p \times \mathbb{Z}_p) = p$ și $\mathbb{Z}_p \times \mathbb{Z}_p$ nu este corp (având divizori ai lui zero).

6.72. Avem $A = \langle (\bar{1}, \bar{1}) \rangle = \{(\bar{0}, \bar{0}), (\bar{1}, \bar{1}), (\bar{2}, \bar{2}), (\bar{3}, \bar{3})\}$ (subinelul unitate generat de elementul unitate) și $\mathbb{Z}_4 \times \mathbb{Z}_4$ - subinel unitar. Fiecare subinel cu identitatea conține A și fie B un astfel de subinel și $(\bar{a}, \bar{a} + \bar{b}) \in B$ cu $\bar{b} \neq \bar{0}$.

Dacă $\bar{b} \in \{\bar{1}, \bar{3}\}$ atunci B este întreg inelul iar dacă $\bar{b} = \bar{2}$ atunci

$$B = A \cup \{(\bar{2}, \bar{0}), (\bar{0}, \bar{2}), (\bar{1}, \bar{3}), (\bar{3}, \bar{1})\}.$$

6.73. (i). Cum $1+1=0$ și $1 \neq 0$ rezultă $H = \{0, 1\}$ este un subgrup de ordin 2 al grupului $(A, +)$.

Fie $a \in A \setminus H$. Atunci $H \cap (H+a) = \emptyset$ și $A = H \cup (H+a) = \{0, 1, a, 1+a\}$.

Deci a^2 poate fi egal cu 0, 1, a sau $1+a$.

Dacă $a^2=1$ atunci $(1+a)^2=1+a+a+a^2=1+1+a+a=0+0=0$ și evident $1+a \notin H$. Așadar, înlocuind pe a cu $1+a$ suntem în cazul 1). Rezultă că se poate alege $a \in A \setminus H$ a.î. $a^2=0$ sau $a^2=a$ sau $a^2=1+a$.

(ii). Fie $A = \mathbb{Z}_2 \times \mathbb{Z}_2$ și $0 = (\hat{0}, \hat{0})$, $1 = (\hat{1}, \hat{1})$, $a = (\hat{1}, \hat{0})$.

Se observă că $\mathbb{Z}_2 \times \mathbb{Z}_2 = \{0, 1, a, 1+a\}$ și $a^2=a$. Atunci $(\mathbb{Z}_2 \times \mathbb{Z}_2, +, \cdot)$ este inel cu 4 elemente de tipul 2).

În inelul $M_2(\mathbb{Z}_2)$ considerăm matricele O, E, U și V astfel:

$$O = \begin{pmatrix} \hat{0} & \hat{0} \\ \hat{0} & \hat{0} \end{pmatrix}, E = \begin{pmatrix} \hat{1} & \hat{0} \\ \hat{0} & \hat{1} \end{pmatrix}, U = \begin{pmatrix} \hat{0} & \hat{0} \\ \hat{1} & \hat{0} \end{pmatrix}, V = \begin{pmatrix} \hat{0} & \hat{1} \\ \hat{1} & \hat{1} \end{pmatrix}.$$

Din calcul direct rezultă că $U^2=O$ și $V^2=E+V$. Cum $E+E=O$ se deduce că $X+X=O$, oricare ar fi $X \in M_2(\mathbb{Z}_2)$. Se deduce că:

$B = \{O, E, U, E+U\}$ și $C = \{O, E, V, E+V\}$ sunt părți stabile ale lui $M_2(\mathbb{Z}_2)$ în raport cu adunarea și înmulțirea matricelor și că sunt inele cu 4 elemente în raport cu operațiile induse. Evident, $(B, +, \cdot)$ este inel de tip 1) iar $(C, +, \cdot)$ este inel de tip 3).

6.74. (i). Dacă perechea (a, b) este un element nilpotent din inelul $A \times B$ atunci a și b sunt elemente nilpotente din A, respectiv din B.

Reciproc, dacă $a \in A$ și $a^n=0$ iar $b \in B$ și $b^m=0$, atunci

$$(a, b)^{n+m} = (a^n \cdot a^m, b^n \cdot b^m) = (0, 0), \text{ deci } (a, b) \text{ este nilpotent în } A \times B.$$

Putem identifica deci pe $N(A \times B)$ cu $N(A) \times N(B)$.

(ii). Descompunând pe n în produs de factori primi distincți, $n = p_1^{k_1} \dots p_r^{k_r}$ și notând $q_i = p_i^{k_i}$, știm că inelul \mathbb{Z}_n este izomorf cu produsul direct $\mathbb{Z}_{q_1} \times \dots \times \mathbb{Z}_{q_r}$.

Așadar este suficient să aflăm elementele nilpotente din fiecare inel \mathbb{Z}_{q_i} iar pentru aceasta a se vedea problema **10.47**.

§7. Morfisme de inele. Izomorfisme de inele.

7.1. Un exemplu de inel neunitar ne este oferit de $2\mathbb{Z}$ (evident, $1 \notin 2\mathbb{Z}$).

Pe mulțimea $B = \mathbb{Z} \times A$ considerăm operațiile algebrice:

$$(n, a) + (m, b) = (n+m, a+b)$$

$$(n, a) \cdot (m, b) = (nm, nb+ma+ab).$$

Prin calcul direct se verifică faptul că $(B, +, \cdot)$ este inel unitar (unitatea lui B fiind elementul $(1, 0)$).

De asemenea, $i: A \rightarrow B$, $i(a) = (0, a)$, pentru orice $a \in A$, este morfism injectiv de inele ($i(a)+i(b) = (0, a)+(0, b) = (0, a+b) = i(a+b)$);

$i(a) \cdot i(b) = (0, a) \cdot (0, b) = (0, ab) = i(ab)$; injectivitatea este imediată pentru că din $i(a) = i(b) \Rightarrow (0, a) = (0, b) \Rightarrow a = b$.

Astfel, A se identifică cu $\text{Im}(i)$ care este subinel al lui B .

Dacă A este comutativ, atunci și B este comutativ.

7.2. Definim $f(x)+f(y) = f(x+y)$ și $f(x)f(y) = f(xy)$, pentru orice $x, y \in A$.

Funcția f fiind injectivă, operațiile date mai sus sunt bine definite (de fapt, operațiile date sunt bine definite dacă și numai dacă relația de echivalență R dată pe A prin: „ $xRy \Leftrightarrow f(x) = f(y)$ ” este compatibilă cu adunarea și înmulțirea din A (f nu neapărat injectivă), adică xRy și $x'Ry' \Rightarrow (x+x')R(y+y')$ și $(xx')R(yy')$). Aceste operații sunt definite pe întreaga mulțime S , f fiind surjectivă. Cu operațiile date S devine inel în care $0_S = f(0)$ și $1_S = f(1)$ (în caz că A este unitar).

Evident, structura dată pe S este unica posibilă întrucât definiția ei constituie o consecință a faptului că f trebuie să devină morfism de inele.

7.3. Fie două operații $+, \cdot$ care dau o structură de inel pe o mulțime cu 4 elemente A .

Dacă $(A, +)$ este ciclic, atunci elementele lui A au forma $a, 2a, 3a, 0$ și a defini „ \cdot ” revine la a-l defini pe a^2 . Distingem patru cazuri posibile:

1) $a^2 = 0$. În acest caz produsul oricăror două elemente este nul (notăm cu N_4 această structură).

2) $a^2 = a$. În acest caz inelul este unitar izomorf cu \mathbb{Z}_4 .

3) $a^2 = 2a$. În acest caz se obține un inel comutativ fără unitate, neizomorf cu N_4 (notăm acest inel cu A_4).

4) $a^2=3a$. În acest caz avem $(3a)^2=3a$ și deci asocierea $a \rightsquigarrow 3a$ definește un automorfism al lui A în baza căruia ne reducem la cazul 2).

Dacă $(A, +)$ este de tip Klein atunci elementele lui A sunt de forma $\{0, a, b, a+b\}$, $2a=2b=0$ și a defini înmulțirea „ \cdot ” distributivă față de adunare revine la a defini pe a^2, b^2, ab, ba . Avem următoarele cazuri:

1') $a^2=b^2=0$. În acest caz, dacă $ab=a$ sau $a+b$ deducem că $0=ab^2=(ab)b=ab$, contradicție. Dacă $ab=b$, atunci avem $0=ab^2=a(ab)=ab$, contradicție. Rezultă $ab=0$. La fel obținem $ba=0$. Prin urmare, produsul oricăror două elemente din A este nul. Fie N_2 structura de inel dată pe grupul aditiv $(\mathbb{Z}_2, +)$ de înmulțirea $\hat{1} \cdot \hat{1} = \hat{0}$. Se observă că asocierea $a \rightsquigarrow (\hat{1}, \hat{0})$, $b \rightsquigarrow (\hat{0}, \hat{1})$ definește un izomorfism al lui A pe $N_2 \times N_2$.

2') $a^2=0, b^2=a$. Dacă $ab=b$ sau $a+b$, deducem că $0=ab^2=ab$, contradicție. Dacă $ab=a$, atunci avem $0=a^2=ab^2=ab$, contradicție. Rezultă $ab=0$. La fel obținem $ba=0$. Se verifică că într-adevăr înmulțirea astfel definită înzestrea grupul $(A, +)$ cu o structură de inel comutativ fără unitate pe care îl notăm cu B_4 .

3') $a^2=0, b^2=b$. Ca și la cazul 2') obținem $ab, ba \notin \{b, a+b\}$. Avem următoarele subcazuri:

i) $ab=ba=0$. În acest subcaz asocierea $a \rightsquigarrow (\hat{0}, \hat{1})$, $b \rightsquigarrow (1, 0)$ definește un izomorfism al lui A pe $\mathbb{Z}_2 \times N_2$.

ii) $ab=ba=a$. În acest subcaz b este unitate în A ; notăm inelul obținut prin I_4 .

iii) $ab=a, ba=0$. În acest subcaz obținem inelul Q_4 necomutativ și fără unitate.

iv) $ab=0, ba=a$. Se obține un inel P_4 necomutativ și fără unitate.

4') $a^2=0, b^2=a+b$. Ca și la 3') deducem că $ab, ba \notin \{b, a+b\}$.

Dacă A este comutativ atunci avem $(a+b)^2=a+b+ab+ba=a+b$ și schimbând pe $a+b$ cu b ne reducem la cazul 3'). Deci, dacă A este comutativ, atunci A este izomorf cu $\mathbb{Z}_2 \times N_2$ sau cu I_4 .

Dacă A nu este comutativ atunci avem două posibilități:

i) $ab=a, ba=0$. Avem $b=(a+b)b=b^2b=bb^2=b(a+b)=a+b$, contradicție.

ii) $ab=0, ba=a$. Obținem în același mod o contradicție.

5') $a^2, b^2, (a+b)^2$ sunt nenule și distincte. În acest caz obținem $(a+b)^2=a^2+b^2$ și rezultă $ab=ba$, adică A este comutativ.

Observăm că modulo o renotare a elementelor lui A putem presupune că $a^2=a$. Într-adevăr, în caz contrar am avea, eventual renotând elementele lui A , $a^2=b$, $b^2=a+b$, $(a+b)^2=a$. Rezultă (*): $a(ab)=a^2b=b^2=a+b$ și deci $ab \neq 0$.

Dacă $ab=a$ obținem din (*) $b=a+b$, contradicție.

Dacă $ab=b$ rezultă $ab=a+b$ și folosind (*) obținem o contradicție.

La fel $ab \neq a+b$, contradicție.

Distingem două subcazuri:

i') $a^2=a$, $b^2=b$. În acest subcaz obținem $a(ba)=ba^2=ba$ și rezultă $ba \neq a+b$.

Dacă $ba=0$ (respectiv $ba=a$ sau $ba=b$) asocierea $a \rightsquigarrow (\hat{0}, \hat{1})$, $b \rightsquigarrow (\hat{1}, \hat{0})$ (respectiv $a \rightsquigarrow (\hat{0}, \hat{1})$, $b \rightsquigarrow (\hat{1}, \hat{1})$ sau $a \rightsquigarrow (\hat{1}, \hat{1})$, $b \rightsquigarrow (\hat{0}, \hat{1})$) definește un izomorfism al lui A pe $\mathbb{Z}_2 \times \mathbb{Z}_2$.

ii') $a^2=a$, $b^2=a+b$. În acest subcaz obținem (**): $b(ab)=b^2a=a+ba$ și rezultă $ab \neq 0$, a , $a+b$.

Deci $ab=b$ iar elementul a constituie element unitate în A . Cum $b(a+b)=b+(a+b)=a$, deducem că A este corp (notăm acest corp cu GF_4).

6') a^2 , b^2 , $(a+b)^2$ nenule dar nu distincte. Renotând eventual elementele lui A putem presupune că $a^2=b^2=a$. Deci $(a+b)^2=ab+ba$. Prin urmare, A nu este comutativ, altfel rezultă $(a+b)^2=0$.

Evident avem (***) : $b(ba)=b^2a=a$ și deci $ba \neq 0$. Dacă $ba=a+b$ atunci din (***) obținem $a=b(a+b)=ba+a$, contradicție. La fel $ab \notin \{0, a+b\}$. Dacă $ab=a$, atunci $ba=b$ și deci $a=b^2=(ba)b=b(ab)=ba=b$, contradicție. La fel $ba \neq b$. Prin urmare, nu există structuri de inel în acest caz.

În consecință există 11 structuri de inel neizomorfe pe o mulțime finită cu 4 elemente: un corp: GF_4 , trei inele unitare comutative: \mathbb{Z}_4 , $\mathbb{Z}_2 \times \mathbb{Z}_2$, I_4 , cinci inele fără unitate comutative: N_4 , $\mathbb{Z}_2 \times N_2$, $N_2 \times N_2$, A_4 , B_4 , două inele necomutative P_4 , Q_4 .

7.4. Fie două operații $+$, \cdot care dau o structură de inel pe o mulțime cu p elemente A . Cum $(A, +)$ este ciclic, elementele lui A au forma $0, a, 2a, \dots, (p-1)a$, $pa=0$ și a defini „ \cdot ” revine la a-l defini pe a^2 .

Prin urmare, A este comutativ.

Avem următoarele două cazuri:

i) $a^2=0$. În acest caz produsul oricăror două elemente este nul (notăm cu N_p acest inel).

ii) $a^2=ia$, oricare i cu $1 \leq i \leq p-1$. Fie $u \in \{1, \dots, p-1\}$ un reprezentant al clasei i^{-1} din corpul \mathbb{Z}_p . Observăm că elementul $e=ua$ satisface relația $e(ja)=j(ui)a=ja$. Deci e este element unitate în A iar asocierea $\hat{i} \rightsquigarrow te$ definește un izomorfism al corpului \mathbb{Z}_p pe A .

7.5. Fie „ \circ ” o înmulțire pe G pentru care acesta devine inel unitar. Fie $e \in G$ unitatea sa și t ordinul lui e în grupul aditiv G . Avem $\hat{i} = t \cdot 1 = t(e \circ \hat{1}) = (te) \circ \hat{1} = \hat{0} \circ \hat{1} = \hat{0}$ (evident, $t(x \circ y) = (tx) \circ y$, întrucât tx este definit în baza adunării iar „ \circ ” este distributivă față de adunare).

Deci $n|t$, iar întrucât $\text{ord}(e)|n = \text{ord}G$, deducem că $n=t$.

Prin urmare, asocierea $\hat{k} \rightsquigarrow ke$ definește un izomorfism de grupuri $f: (\mathbb{Z}_n, +) \rightarrow (G, \circ)$.

Evident avem $f(\hat{k} \cdot \hat{i}) = f(\hat{kt}) = kte = (ke) \circ (te) = f(\hat{k}) \circ f(\hat{i})$, $f(\hat{1}) = e$.

Deci f este izomorfism de inele unitare.

În consecință, toate structurile posibile de inel unitar date pe G sunt izomorfe între ele. Întrucât pentru orice element e de ordin n al lui G izomorfismul f poate fi construit, deducem că există $\varphi(n)$ structuri de inel unitar pe G (pentru fiecare alegere posibilă a lui e).

Nu există operații de înmulțire pe H pentru care acesta devine (împreună cu adunarea) inel unitar. Într-adevăr, în caz contrar, fie dată o astfel

de operație \otimes și $e = \frac{m}{n}$ elementul unitate din inelul $(H, +, \otimes)$. Evident $e \neq \hat{0}$ (singurul inel în care elementul unitate coincide cu elementul nul este inelul nul). Putem alege reprezentantul $\frac{m}{n}$ al lui e a.î. $m, n > 0$.

Se observă că:

$$\frac{1}{m} = e \otimes \frac{1}{m} = (m \cdot \frac{1}{n}) \otimes \frac{1}{m} = m \cdot (\frac{1}{n} \otimes \frac{1}{m}) = \frac{1}{n} \otimes (m \cdot \frac{1}{m}) = \frac{1}{n} \otimes \hat{1} = \frac{1}{n} \otimes \hat{0} = \hat{0}.$$

Rezultă $\frac{1}{m} \in \mathbb{Z}$ și deci $m=1$.

Pe de altă parte avem,

$$\frac{\bigwedge_n}{n+1} = e \otimes \frac{\bigwedge_n}{n+1} = \frac{\bigwedge_1}{n} \otimes (n \cdot \frac{\hat{1}}{n+1}) = (n \cdot \frac{\bigwedge_1}{n}) \otimes \frac{\hat{1}}{n+1} = \hat{1} \otimes \frac{\bigwedge_1}{n+1} = \hat{0},$$

adică $n+1 | n$, contradicție.

7.6. Dacă $f: \mathbb{Z} \rightarrow \mathbb{Z}_n$ este un morfism de inele și notăm $f(1) = \hat{a}$, cu $\hat{a} \in \mathbb{Z}_n$, atunci se probează imediat că $f(x) = \hat{a} \cdot x$, oricare ar fi $x \in \mathbb{Z}$.

Dacă vom considera f morfism de inele unitare, atunci $f(1) = \hat{1} \Leftrightarrow \hat{a} = \hat{1}$ și astfel $f(x) = x \cdot \hat{1}$, oricare ar fi $x \in \mathbb{Z}$.

Dacă f nu este morfism de inele unitare (adică $f(1) \neq \hat{1}$), atunci din $f(1) = f(1 \cdot 1) = f(1) \cdot f(1)$ deducem că $\hat{a} = \hat{a}^2$, adică \hat{a} este idempotent în inelul \mathbb{Z}_n .

Cum pentru $x, y \in \mathbb{Z}$, $f(x)f(y) = (\hat{a}x)(\hat{a}y) = \hat{a}^2(xy) = \hat{a}xy = f(xy)$ deducem că:

i) Există un singur morfism de inele unitare $f: \mathbb{Z} \rightarrow \mathbb{Z}_n$ (și anume $f(x) = x \cdot \hat{1}$, oricare ar fi $x \in \mathbb{Z}$).

ii) În cazul în care $f: \mathbb{Z} \rightarrow \mathbb{Z}_n$ nu este morfism de inele unitare atunci $f(x) = x \cdot \hat{a}$, oricare ar fi $x \in \mathbb{Z}$ cu $\hat{a} \in \mathbb{Z}_n$ idempotent.

7.7. Pentru a nu se crea confuzie, să notăm $\mathbb{Z}_m = \left\{ \hat{0}, \hat{1}, \dots, \hat{m-1} \right\}$ și $\mathbb{Z}_n = \left\{ \bar{0}, \bar{1}, \dots, \overline{n-1} \right\}$. Dacă $f: \mathbb{Z}_m \rightarrow \mathbb{Z}_n$ este un morfism de inele și $f(\hat{1}) = \bar{a}$, în cazul în care f este morfism de inele unitare $\bar{a} = f(\hat{1}) = \bar{1}$ și atunci din aproape în aproape se arată că $f(\hat{2}) = 2\bar{a} = \bar{2}, \dots, f\left(\hat{m-1}\right) = \overline{m-1}$.

Cum $f(\hat{m}) = f(\hat{0}) = \bar{0}$ iar $f(\hat{m}) = m \cdot f(\hat{1}) = m \cdot \bar{a} = m \cdot \bar{1}$, cu necesitate $\overline{m} = \bar{0}$ (adică $n | m$). În concluzie, dacă $n \nmid m$ nu există morfisme unitare de inele de la \mathbb{Z}_m la \mathbb{Z}_n iar în cazul $n | m$ există un unic morfism unitar de inele (definit de condițiile $f(\hat{0}) = \bar{0}, f(\hat{1}) = \bar{1}, \dots, f\left(\hat{m-1}\right) = \overline{m-1}$).

Dacă $f: \mathbb{Z}_m \rightarrow \mathbb{Z}_n$ este un morfism de inele (nu neapărat unitare), atunci $f(\hat{1}) = \bar{a} \neq \bar{1}$. Din condiția de aditivitate a lui f deducem imediat că $f(\hat{k}) = k \cdot \bar{a}$, oricare ar fi $0 \leq k \leq m-1$ și $m \cdot \bar{a} = \bar{0}$ iar din condiția de multiplicitate a lui f

deducem că $\bar{a} = f(\hat{1}) = f(\hat{1} \cdot \hat{1}) = f(\hat{1})^2 = \bar{a}^2$ (adică \bar{a} este idempotent în inelul \mathbb{Z}_n).

În concluzie, morfismele de inele neunitare $f: \mathbb{Z}_m \rightarrow \mathbb{Z}_n$ sunt de forma $f(\hat{k}) = k \cdot \bar{a}$, cu $\bar{a} \in \mathbb{Z}_n$ idempotent ($0 \leq k \leq m-1$), $\bar{a} \neq \bar{1}$ și $m \cdot \bar{a} = \bar{0}$.

7.8. Fie $n \in \mathbb{Z}$, $n \neq 0$.

$$f(1) = f\left(n \cdot \frac{1}{n}\right) = f(n) \cdot f\left(\frac{1}{n}\right). \text{ La fel } g(1) = g\left(n \cdot \frac{1}{n}\right) = g(n) \cdot g\left(\frac{1}{n}\right).$$

Cum $f(1) = g(1) = 1_A$ și $f(n) = g(n)$, pentru orice $n \in \mathbb{Z}$, obținem $f\left(\frac{1}{n}\right) = g\left(\frac{1}{n}\right)$. De aici rezultă că $f\left(\frac{m}{n}\right) = f(m) \cdot f\left(\frac{1}{n}\right) = g(m) \cdot g\left(\frac{1}{n}\right) = g\left(\frac{m}{n}\right)$, oricare ar fi $\frac{m}{n} \in \mathbb{Q}$.

7.9. Dacă $a \in U(A)$ atunci există $a' \in A$ a.î. $aa' = a'a = 1$. Deducem imediat că $f(a) \cdot f(a') = f(a') \cdot f(a) = 1$, adică $f(a) \in U(A')$.

Dacă $a \in N(A)$ atunci există $n \in \mathbb{N}$ a.î. $a^n = 0$. Deducem imediat că $f^n(a) = 0$, adică $f(a) \in N(A')$.

Dacă $a \in A$ este divizor al lui zero atunci există $a' \in A^*$ a.î. $aa' = 0$. Deducem imediat că $f(a) \cdot f(a') = 0$, adică $f(a)$ este divizor al lui zero în A' (căci f fiind injecție, $f(a') \neq 0$).

7.10. Să presupunem, prin absurd, că există un izomorfism de inele $\varphi: I \rightarrow I'$. Atunci avem proprietatea:

$$\text{oricare ar fi } f \in I, f \geq 0 \Rightarrow \varphi(f) \geq 0. \quad (1)$$

Într-adevăr, dacă $f \in I$, $f \geq 0$, putem scrie:

$$\varphi(f) = \varphi(\sqrt{f} \cdot \sqrt{f}) = \varphi(\sqrt{f}) \cdot \varphi(\sqrt{f}) = \varphi(\sqrt{f})^2 \geq 0.$$

Vom arăta acum că $\varphi(a) = a$, oricare ar fi $a \in \mathbb{R}$, relație ce trebuie interpretată prin aceea că φ invariază toate funcțiile constante (pentru simplitate am notat cu a funcția constantă $f_a: [0, 1] \rightarrow \mathbb{R}$, $f_a(x) = a$, oricare ar fi $x \in [0, 1]$). Din aceea că φ este morfism unitar de inele rezultă că $\varphi(1) = 1$ și apoi rezultă ușor că $\varphi(a) = a$, oricare ar fi $a \in \mathbb{Q}$. Dacă $a \in \mathbb{R} \setminus \mathbb{Q}$, există (a_n') , (a_n'') șiruri de numere raționale, convergente la a , a.î. $a_n' < a < a_n''$, oricare ar fi $n \in \mathbb{N}$. Aplicând morfismul φ și ținând seama că φ este funcție crescătoare (datorită lui (1)) rezultă că $\varphi(a_n') \leq \varphi(a) \leq \varphi(a_n'')$, adică $a_n' \leq \varphi(a) \leq a_n''$, oricare ar fi $n \in \mathbb{N}$.

Trecând la limită după n , rezultă $\varphi(a)=a$. Vom dovedi acum reciproca lui (1) și anume:

$$\text{oricare ar fi } f \in I \text{ cu } \varphi(f) \geq 0 \Rightarrow f \geq 0. \quad (2)$$

Să presupunem prin reducere la absurd că există $f_0 \in I$, cu $\varphi(f_0) \geq 0$ dar $f_0 \not\geq 0$. Aceasta înseamnă că există $x_0 \in [0, 1]$ cu $f_0(x_0) < 0$. Fie $a = \frac{1}{2} f_0(x_0) < 0$ și să considerăm funcția $g: [0, 1] \rightarrow \mathbb{R}$, $g(x) = f_0(x) - a$.

$$\text{Evident, } g \in I \text{ și } g(x_0) = f_0(x_0) - a = \frac{1}{2} f_0(x_0) < 0.$$

Avem apoi $\varphi(g) = \varphi(f_0 - a) = \varphi(f_0) - \varphi(a) = \varphi(f_0) - a > 0$, unde pentru ultima inegalitate am ținut cont că $\varphi(f_0) \geq 0$ iar $a < 0$.

Să notăm $\varphi(g) = h$, deci $h \in I'$ și $h > 0$. Atunci $\sqrt{h} \in I'$ și cum φ este surjectiv există $u \in I$ a.î. $\varphi(u) = \sqrt{h}$.

Rezultă $\varphi(u^2) = \varphi(u)\varphi(u) = \sqrt{h} \cdot \sqrt{h} = h = \varphi(g)$ și folosind faptul că φ este injectiv obținem $g = u^2$, contradicție, căci $g(x_0) < 0$. Așadar implicația (2) este adevărată. Fie acum $f \in I'$, $f(x) = \left(x - \frac{1}{2}\right)^2$. Avem evident $f \geq 0$ și folosind

surjectivitatea lui φ , deducem că există $s \in I$ cu $\varphi(s) = f$. Din (2) avem $s \geq 0$. Evident, $\sqrt{s} \in I$ și avem $\varphi^2(\sqrt{s}) = \varphi(\sqrt{s})\varphi(\sqrt{s}) = \varphi(s) = f$. Atunci $\varphi(\sqrt{s}) = \sqrt{f}$, ceea ce arată că $\sqrt{f} \in I'$. Ar însemna că funcția $x \rightarrow \left|x - \frac{1}{2}\right|$ este derivabilă pe $[0, 1]$, ceea ce este o contradicție. Rezultă că cele două inele nu pot fi izomorfe.

7.11. Nu are loc nici o implicație.

Pentru $p_4: \mathbb{Z} \rightarrow \mathbb{Z}_4$, $p_4(x) = [x]_4$, avem $p_4(2) = [2]_4$, unde $[2]_4 \in \mathbb{Z}_4$ este divizor al lui zero ($[2]_4 \cdot [2]_4 = [0]_4$) dar $2 \in \mathbb{Z}$ nu este divizor al lui zero.

Invers, fie $f: \mathbb{Z}_6 \rightarrow \mathbb{Z}_3$, $f([x]_6) = [x]_3$.

Evident, $f([2]_6) = [2]_3$ și $[2]_6$ este divizor al lui zero în \mathbb{Z}_6 iar $[2]_3 \in \mathbb{Z}_3$ nu este divizor al lui zero (acesta este corp și $[2]_3 \neq [0]_3$).

Observație. Am notat $[x]_n$ clasa lui x în \mathbb{Z}_n .

7.12. (i) \Rightarrow (ii). Fie $e \in A$ un element idempotent diferit de 0 și 1.

Atunci $f: A \rightarrow A/(e) \times A/(1-e)$ definită prin $f(a) = (a+(e), a+(1-e))$ este izomorfism de inele. Într-adevăr, din $f(a) = (0, 0)$ rezultă $a \in (e)$ și $a \in (1-e)$, adică

$a=es=(1-e)t$. Deducem $ea=e^2s=es=a$ și $ea=e(1-e)t=0$. Deci $a=0$, ceea ce arată că f este injecție.

Dacă x și y sunt elemente arbitrare alese, atunci pentru $a=(1-e)x+ey$ avem $f(a)=(a+(e), a+(1-e))=((1-e)x+(e), ey+(1-e))=(x-ex+(e), -y(1-e)+y+(1-e))=(x+(e), y+(1-e))$, deci f este surjecție și avem (i) \Rightarrow (ii).

(ii) \Rightarrow (i). Reciproc, $e'=(1, 0)$ este element idempotent în $B \times C$ diferit de $(0, 0)$ și de $(1, 1)$. Elementul $e \in A$ corespunzător lui e' este idempotent diferit de 1 și 0. Deci (ii) \Rightarrow (i).

7.13. (i). Înmulțind între ele matricele $A = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ și $B = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ obținem $A \cdot B = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = B$ și $B \cdot A = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} = O_2$, ceea ce arată că inelul $T_2(\mathbb{Z})$ nu este comutativ.

Să presupunem că matricea $\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \in T_2(\mathbb{Z})$ comută cu toate elementele lui $T_2(\mathbb{Z})$. Din relația $\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \cdot A = A \cdot \begin{pmatrix} a & b \\ 0 & c \end{pmatrix}$ obținem $b=0$, apoi din relația $\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \cdot B = B \cdot \begin{pmatrix} a & b \\ 0 & c \end{pmatrix}$ obținem $a=c$. Constatăm imediat că centrul lui $T_2(\mathbb{Z})$ este format din matricele $\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$, cu $a \in \mathbb{Z}$. De altfel, centrul lui $T_2(\mathbb{Z})$ coincide cu centrul lui $M_2(\mathbb{Z})$.

(ii). Fie $X = \begin{pmatrix} a & b \\ 0 & c \end{pmatrix}$ și $Y = \begin{pmatrix} a' & b' \\ 0 & c' \end{pmatrix}$ două elemente din $T_2(\mathbb{Z})$.

Întrucât $X+Y = \begin{pmatrix} a+a' & b+b' \\ 0 & c+c' \end{pmatrix}$ și $X \cdot Y = \begin{pmatrix} aa' & ab'+bc' \\ 0 & cc' \end{pmatrix}$ observăm că :

$$\varphi(X+Y) = (a+a', c+c') = (a, c) + (a', c') = \varphi(X) + \varphi(Y) \text{ iar}$$

$$\varphi(X \cdot Y) = (aa', cc') = (a, c) \cdot (a', c') = \varphi(X) \cdot \varphi(Y).$$

Deci φ este morfism de inele. Nucleul său, $\text{Ker}(\varphi)$, este format din matricele $\begin{pmatrix} 0 & d \\ 0 & 0 \end{pmatrix}$, cu $d \in \mathbb{Z}$. Observăm că :

$$\begin{pmatrix} 0 & d \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} = \begin{pmatrix} 0 & dc \\ 0 & 0 \end{pmatrix} \in \text{Ker}(\varphi) \text{ și } \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \cdot \begin{pmatrix} 0 & d \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & ad \\ 0 & 0 \end{pmatrix} \in \text{Ker}(\varphi).$$

Nucleul $\text{Ker}(\varphi)$ este un exemplu de ideal bilateral al inelului $T_2(\mathbb{Z})$.

7.14. (i). Faptul că A_k este inel comutativ față de adunarea și înmulțirea matricelor se probează imediat.

(ii). Vom demonstra că A_k are divizori ai lui zero dacă și numai dacă k este pătrat perfect.

Să presupunem mai întâi că A_k are divizori ai lui zero și fie $X_1 = \begin{pmatrix} a_1 & b_1 \\ kb_1 & a_1 \end{pmatrix}$, $X_2 = \begin{pmatrix} a_2 & b_2 \\ kb_2 & a_2 \end{pmatrix}$ două matrice nenule din inelul A_k , cu proprietatea că $X_1 \cdot X_2 = O_2$, (1). Avem $b_1 \neq 0$, căci dacă am presupune $b_1 = 0$, cum $X_1 \neq O_2$ trebuie ca $a_1 \neq 0$ și atunci din (1) rezultă că $\begin{pmatrix} a_1 a_2 & a_1 b_2 \\ k a_1 b_2 & a_1 a_2 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$, de unde $a_2 = b_2 = 0$, adică $X_2 = O_2$, contradicție cu presupunerea făcută. Analog $b_2 \neq 0$.

Din (1) obținem $\det X_1 \cdot \det X_2 = 0$, deci $\det X_1 = 0$ sau $\det X_2 = 0$.

Rezultă $k = \left(\frac{a_1}{b_1}\right)^2$ sau $k = \left(\frac{a_2}{b_2}\right)^2$, deci k este pătratul unui număr rațional. Cum k este întreg, rezultă că este pătratul unui număr întreg, deci k este pătrat perfect.

Reciproc, dacă k este pătrat perfect, luând $X_1 = \begin{pmatrix} \sqrt{k} & 1 \\ k & \sqrt{k} \end{pmatrix}$, $X_2 = \begin{pmatrix} -\sqrt{k} & 1 \\ k & -\sqrt{k} \end{pmatrix}$, avem $X_1 \neq O_2$, $X_2 \neq O_2$ și $X_1 X_2 = O_2$, ceea ce înseamnă că inelul A_k are divizori ai lui zero.

(iii). Să presupunem că există un izomorfism de inele $\varphi: A_k \rightarrow A_p$. Considerăm matricea $X_0 = \begin{pmatrix} 0 & 1 \\ k & 0 \end{pmatrix} \in A_k$ și imagine sa $Y_0 = \varphi(X_0) = \begin{pmatrix} a & b \\ pb & a \end{pmatrix} \in A_p$.

Demonstrăm că în mod necesar avem $b \neq 0$. Într-adevăr dacă am admite că $b = 0$, atunci $Y_0 = \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} = a \cdot I_2$ și luând o matrice arbitrară $X = \begin{pmatrix} \alpha & \beta \\ k\beta & \alpha \end{pmatrix} \in A_k$ putem scrie $X = \alpha I_2 + \beta X_0$ și atunci

$\varphi(X) = \alpha \varphi(I_2) + \beta \varphi(X_0) = \alpha I_2 + \beta Y_0 = \alpha I_2 + \beta a I_2 = (\alpha + \beta a) I_2$, ceea ce arată că φ nu ar fi surjectiv, contradicție.

Observăm că matricea aleasă X_0 verifică egalitatea $X_0^2 = kI_2$ și de aici, aplicând izomorfismul φ obținem $Y_0^2 = kI_2$, ceea ce se scrie echivalent:

$$\begin{pmatrix} a & b \\ pb & a \end{pmatrix}^2 = \begin{pmatrix} k & 0 \\ 0 & k \end{pmatrix} \Leftrightarrow \begin{pmatrix} a^2 + pb^2 & 2ab \\ 2pab & a^2 + pb^2 \end{pmatrix} = \begin{pmatrix} k & 0 \\ 0 & k \end{pmatrix} \Leftrightarrow \begin{cases} a^2 + pb^2 = k \\ 2ab = 0 \end{cases}. \quad (2)$$

Deoarece $b \neq 0$ din a doua egalitate din (2) rezultă $a=0$, a.f. introducând în prima obținem $pb^2=k$. Aceasta arată că $p \mid k$ și mai mult, au și același semn. Analog, considerând izomorfismul invers $\varphi^{-1}: A_p \rightarrow A_k$, vom obține $k \mid p$. În concluzie $k=p$.

Reciproc, pentru $k=p$ avem egalitatea $A_k=A_p$ și atunci morfismul identic este un automorfism al inelului A_k .

$$7.15. \text{ (i). Aplicația } \varphi: \mathbb{Z}[\sqrt{d}] \rightarrow A_d \text{ definită prin } \varphi(m+n\sqrt{d}) = \begin{pmatrix} m & n \\ dn & m \end{pmatrix}$$

este un izomorfism de inele.

(ii). „ \Leftarrow ”. Dacă $d=d'$ atunci inelele $\mathbb{Z}[\sqrt{d}]$ și $\mathbb{Z}[\sqrt{d'}]$ coincid, deci sunt evident izomorfe.

„ \Rightarrow ”. Fie $f: \mathbb{Z}[\sqrt{d}] \rightarrow \mathbb{Z}[\sqrt{d'}]$ un izomorfism de inele și presupunem prin reducere la absurd că $d \neq d'$. Din $f(0)=0$ și $f(1)=1$ rezultă $f(a)=a$, oricare ar fi $a \in \mathbb{Z}$. Dacă $x=a+b\sqrt{d} \in \mathbb{Z}[\sqrt{d}]$ atunci $f(x)=a+bf(\sqrt{d})$.

$$\text{Fie } f(\sqrt{d})=m+n\sqrt{d'} \text{ cu } m, n \in \mathbb{Z}.$$

$$\text{Deci } d=f(d)=f(\sqrt{d} \cdot \sqrt{d})=(m+n\sqrt{d'})^2=m^2+n^2d'+2mn\sqrt{d'}.$$

De aici obținem $2mn=0$ și $d=m^2+n^2d'$, relații care conduc la o contradicție atât în cazul $m=0$ cât și în cazul $n=0$.

7.16. Fie $P, Q \in P(M)$. Diferența simetrică $P\Delta Q=(P \cup Q)-(P \cap Q)$ poate fi scrisă și ca $P\Delta Q=(P \cap C_M Q) \cup (Q \cap C_M P)$.

Pentru a arăta că Δ este operație asociativă probăm că $(P\Delta Q)\Delta R=(P \cap Q \cap R) \cup (P \cap C_M Q \cap C_M R) \cup (C_M P \cap Q \cap C_M R) \cup (C_M P \cap C_M Q \cap R) = P\Delta(Q\Delta R)$. (fie prin dublă incluziune, fie cu ajutorul proprietăților funcției caracteristice).

Comutativitatea este evidentă. Mulțimea vidă este elementul nul, căci $P\Delta \emptyset=P$. Deoarece $P\Delta P=\emptyset$, rezultă că inversul lui P este chiar P .

Pe de altă parte, intersecția este asociativă și are pe M ca element neutru. Se observă imediat că $P \cap (Q\Delta R)=(P \cap Q)\Delta(P \cap R)$, oricare ar fi $P, Q, R \in P(M)$, adică \cap este distributivă față de Δ .

Deci $(P(M), \Delta, \cap)$ este inel (comutativ). În acest inel $P \cap P = P$, oricare ar fi $P \in P(M)$, adică orice element este idempotent, deci $P(M)$ este inel boolean.

Pentru a doua parte, fie $M = \{1, 2, \dots, m\}$ cu $m \geq 1$.

Dacă $x \in \underbrace{Z_2 \times \dots \times Z_2}_{de\ m\ ori}$, $x = (\hat{i}_1, \dots, \hat{i}_m)$, definim $M_x = \{k \mid \hat{i}_k \neq \hat{0}\} \in P(M)$.

Se observă că $M_x \Delta M_y = M_{x+y}$ și $M_x \cap M_y = M_{xy}$ iar aplicația $\varphi: \underbrace{Z_2 \times \dots \times Z_2}_{de\ m\ ori} \rightarrow P(M)$, $\varphi(x) = M_x$ este bijectivă.

Elementul neutru pentru Δ este \emptyset , iar elementul neutru pentru \cap este M .

Dacă $X, Y, Z \in P(M)$, există $x, y, z \in \underbrace{Z_2 \times \dots \times Z_2}_{de\ m\ ori}$ a.î. $\varphi(x) = X$, $\varphi(y) = Y$,

$\varphi(z) = Z$. Avem:

$$\begin{aligned} (X \Delta Y) \Delta Z &= (M_x \Delta M_y) \Delta M_z = M_{x+y} \Delta M_z = M_{(x+y)+z} = M_{x+(y+z)} = M_x \Delta M_{y+z} = \\ &= M_x \Delta (M_y \Delta M_z) = X \Delta (Y \Delta Z) \text{ și} \end{aligned}$$

$$\begin{aligned} X \cap (Y \Delta Z) &= M_x \cap (M_y \Delta M_z) = M_x \cap M_{y+z} = M_{x(y+z)} = M_{xy+xz} = M_{xy} \Delta M_{xz} = \\ &= (X \cap Y) \Delta (X \cap Z). \end{aligned}$$

Analog se verifică și celelalte axiome ale inelului.

Cum φ este bijectivă și

$$\varphi(x+y) = M_{x+y} = M_x \Delta M_y = \varphi(x) \Delta \varphi(y)$$

$$\varphi(xy) = M_{xy} = M_x \cap M_y = \varphi(x) \cap \varphi(y),$$

avem că inelul $(P(M), \Delta, \cap)$ este izomorf cu inelul $(\underbrace{Z_2 \times \dots \times Z_2}_{de\ m\ ori}, +, \cdot)$.

7.17. Conform problemei **6.45**, avem $x+x=0$ și $xy=yx$, oricare ar fi $x, y \in A$.

Pe A introducem relația binară „ \leq ”: $a \leq b \Leftrightarrow a = ab$, care este o relație de ordine pe A . Elementele minimale ale mulțimii $A^* = A \setminus \{0\}$ le vom numi *atomi*. Așadar, un element $a \in A$, $a \neq 0$ este atom al lui A dacă din $x \leq a$, cu $x \neq 0$, rezultă $x = a$, ceea ce revine la: $x = xa$, $x \neq 0 \Rightarrow x = a$.

Dacă a_1 și a_2 sunt doi atomi distincți, atunci $a_1 a_2 = 0$.

Într-adevăr, fie $x = a_1 a_2$. Dacă $x \neq 0$, din $xa_1 = a_1 a_2 a_1 = a_1 a_2 = x$ și $xa_2 = x$ rezultă că $a_1 = x = a_2$, contradicție cu faptul că a_1, a_2 sunt distincți.

Cum A este o mulțime finită, rezultă imediat că pentru orice $b \in A$, $b \neq 0$, există un atom a a.î. $a \leq b$.

Fie a_1, a_2, \dots, a_m atomi distincți doi câte doi ai lui A . Avem $a_1 + \dots + a_m = 1$. Într-adevăr, în caz contrar avem $b \neq 0$, unde $b = a_1 + \dots + a_m + 1$. Să demonstrăm acest lucru.

Fie a un atom al lui A a.î. $a \leq b$. Există $k \in \{1, \dots, m\}$ a.î. $a = a_k$ și atunci $a = a_k = a_k b = a_k(a_1 + \dots + a_m + 1) = a_k^2 + a_k = a_k + a_k = 0$, contradicție. Deci obligatoriu $b = 0$, adică $a_1 + \dots + a_m = 1$.

Fie $x \in A$. Din $(xa_k)a_k = x a_k^2 = xa_k$ rezultă că $xa_k = 0$ sau $xa_k = a_k$ și cum $x = x \cdot 1 = x(a_1 + \dots + a_m) = xa_1 + \dots + xa_m$, se deduce că orice $x \in A$ se reprezintă în mod unic sub forma $x = i_1 a_1 + \dots + i_m a_m$, $0 \leq i_k < 2$.

$$\text{Definim } f: A \rightarrow \underbrace{Z_2 \times \dots \times Z_2}_{\text{de } m \text{ ori}}, f(x) = (\hat{i}_1, \dots, \hat{i}_m) \Leftrightarrow x = \sum_{k=1}^m i_k a_k, 0 \leq i_k < 2.$$

Dacă $x, y \in A$, $x = \sum_{k=1}^m i_k a_k$, $y = \sum_{k=1}^m j_k a_k$, $0 \leq i_k, j_k < 2$, atunci:

$$x + y = \sum_{k=1}^m (i_k + j_k) a_k = \sum_{k=1}^m (i_k \oplus j_k) a_k,$$

$$xy = \sum_{s,t} i_s j_t a_s a_t = \sum_{k=1}^m (i_k j_k) a_k^2 = \sum_{k=1}^m (i_k \otimes j_k) a_k,$$

unde „ \oplus ” și „ \otimes ” sunt simbolurile adunării, respectiv înmulțirii modulo doi.
Rezultă că:

$$f(x + y) = (\hat{i}_1 \oplus \hat{j}_1, \dots, \hat{i}_m \oplus \hat{j}_m) = (\hat{i}_1 + \hat{j}_1, \dots, \hat{i}_m + \hat{j}_m) = (\hat{i}_1, \dots, \hat{i}_m) + (\hat{j}_1, \dots, \hat{j}_m) = f(x) + f(y)$$

și analog $f(xy) = f(x) \cdot f(y)$. Deci f este morfism bijectiv de inele.

7.18. (i) „ \Rightarrow ”. Într-un inel boolean A avem $x+x=0$, oricare ar fi $x \in A$, deci în grupul $(A, +)$ ordinul fiecărui element este cel mult 2. Dacă p este prim a. î. $p \mid n$, din teorema lui Cauchy există în $(A, +)$ un element de ordin p . Deci p nu poate fi decât 2 și dacă singurul divizor prim al lui n este 2 rezultă că $n=2^k$. Se mai poate justifica acest fapt prin inducție după n sau considerând structura de spațiu vectorial a grupului $(A, +)$ peste corpul Z_2 .

„ \Leftarrow ”. $A = \mathbb{Z}_2 \times \dots \times \mathbb{Z}_2$ de k ori este un inel boolean (structură de produs direct de inele) iar această structură se transportă izomorf pe orice mulțime cu 2^k elemente (vezi problema 7.17.).

(ii). Fie $B = \{X \subset \mathbb{N} \mid X \text{ este mulțime finită}\}$ și $C = \{X \subset \mathbb{N} \mid C_{\mathbb{N}}X \text{ este mulțime finită}\}$. Avem $B \cap C = \emptyset$ și notăm $A = B \cup C$. Se arată ușor că (A, Δ, \cap) este inel boolean, unde Δ este diferența simetrică, adică $X \Delta Y = (X \cup Y) \setminus (X \cap Y)$.

Definim $f: A \rightarrow \mathbb{N}$ prin $f(\emptyset) = 0$, $f(\mathbb{N}) = 1$, $f(X) = \prod_{x \in X} p_x$, dacă $X \in B \setminus \{\emptyset\}$ și

$f(X) = \prod_{x \in C_{\mathbb{N}}X} p_x^2$, dacă $X \in C \setminus \{\mathbb{N}\}$, unde $p_0 < p_1 < \dots < p_n < \dots$ reprezintă șirul

numerelor prime pozitive. Se arată ușor că f este injectivă și fie $\text{Im}(f) = \{n_0, n_1, \dots, n_k, \dots\}$. Atunci funcția $g: A \rightarrow \mathbb{N}$, $g(X) = k$ dacă $f(X) = n_k$, este bijectivă și cu ajutorul funcției g transportăm structura de inel boolean de la A la \mathbb{N} .

7.19. Fie A inelul părților lui E cu operațiile date. Dacă F este o submulțime a lui E notăm prin $\varphi_F: E \rightarrow \mathbb{Z}_2$ funcția caracteristică a lui F definită prin:

$$\varphi_F(x) = \begin{cases} \hat{0}, & \text{pentru } x \notin F \\ \hat{1}, & \text{pentru } x \in F \end{cases}.$$

Această asociere $F \rightsquigarrow \varphi_F$ definește o aplicație de la A la \mathbb{Z}_2^E . În plus, φ este morfism de inele unitare. Într-adevăr avem identitățile: $\varphi_{\emptyset} = 0$, $\varphi_E = 1$, (adică funcția nulă, respectiv funcția constantă $\hat{1}$) $\varphi_{E_1 + E_2} = \varphi_{E_1} + \varphi_{E_2}$, $\varphi_{E_1 \cdot E_2} = \varphi_{E_1} \cdot \varphi_{E_2}$.

Observăm acum că întrucât elementele lui \mathbb{Z}_2 sunt idempotente, rezultă că și elementele lui \mathbb{Z}_2^E sunt idempotente. Evident,

$$P(M \cup N) \cong \prod_{i \in M \cup N} (\mathbb{Z}_2)_i = \prod_{i \in M} (\mathbb{Z}_2)_i \times \prod_{i \in N} (\mathbb{Z}_2)_i \cong P(M) \times P(N),$$

unde $(\mathbb{Z}_2)_i = \mathbb{Z}_2$.

7.20. Fie $f: \mathbb{Z} \rightarrow A$ un morfism de inele, atunci $x = f(1)$ este idempotent în A . Într-adevăr, $x^2 = f(1) \cdot f(1) = f(1 \cdot 1) = f(1) = x$. Această asociere $f \rightsquigarrow f(1)$ definește o aplicație φ de la morfismele de inele definite pe \mathbb{Z} cu valori în A , în mulțimea idempotenților lui A .

φ este injectivă pentru că $\varphi(f)=\varphi(g)$ înseamnă $f(1)=g(1)$, ceea ce implică $f(n) = \underbrace{f(1+\dots+1)}_{\text{de } n \text{ ori}} = \underbrace{f(1)+\dots+f(1)}_{\text{de } n \text{ ori}} = \underbrace{g(1)+\dots+g(1)}_{\text{de } n \text{ ori}} = \underbrace{g(1+\dots+1)}_{\text{de } n \text{ ori}} = g(n)$,

pentru orice $n \in \mathbb{N}$ (f și g sunt morfisme de inele $:\mathbb{Z} \rightarrow A$).

Cum $f(-n)=-f(n)=-g(n)=g(-n)$ deducem că f și g coincid și pe numerele întregi negative, deci $f=g$.

φ este și surjectivă. Într-adevăr, dacă $e^2=e \in A$ atunci considerăm aplicația $f:\mathbb{Z} \rightarrow A$ definită prin $f(n)=n \cdot e$. Se arată ușor că f este morfism de inele. În plus, $f(1)=e$.

Evident $e^2=e$, adică $e(e-1)=0$ are loc într-un domeniu de integritate numai pentru 0 și 1. Cum orice domeniu de integritate are doar două elemente idempotente, deducem că mulțimea morfismelor de la \mathbb{Z} într-un domeniu de integritate are două elemente (unul este morfismul nul).

7.21. (i). Suma a două morfisme de grupuri $f, g:G \rightarrow G$ este definită prin $(f+g)(x)=f(x)+g(x)$, oricare ar fi $x \in G$. Faptul că $f+g:G \rightarrow G$ este morfism de grupuri rezultă din comutativitatea grupului G . Această adunare este comutativă și asociativă. Elementul nul este morfismul nul $0:G \rightarrow G$, $0(x)=0$, oricare ar fi $x \in G$. Compunerea morfismelor este asociativă și distributivă față de adunare iar elementul unitate este funcția identică 1_G (evident un morfism de grupuri).

(ii). Dacă $\text{End}(A)$ este izomorf cu A , atunci evident $\text{End}(A)$ este inel comutativ.

Reciproc, să presupunem că $\text{End}(A)$ este inel comutativ, în raport cu adunarea și compunerea morfismelor. Fie $x \in A$. Notăm $\varphi_x:A \rightarrow A$ funcția definită prin $\varphi_x(y)=y \cdot x$, oricare ar fi $y \in A$. Datorită distributivității înmulțirii față de adunare în inelul A avem $\varphi_x(y+z)=(y+z) \cdot x=y \cdot x+z \cdot x=\varphi_x(y)+\varphi_x(z)$, deci φ_x este element din $\text{End}(A)$.

De asemenea $(\varphi_y \circ \varphi_x)(z)=\varphi_y(z \cdot x)=(z \cdot x) \cdot y=z \cdot (x \cdot y)=\varphi_{x \cdot y}(z)$.

Întrucât din ipoteză inelul $\text{End}(A)$ este comutativ avem $\varphi_x \circ \varphi_y=\varphi_y \circ \varphi_x=\varphi_{x \cdot y}$

Fie f un element oarecare din $\text{End}(A)$. Folosind ipoteza de comutativitate a compunerii deducem

$f(x)=f(1 \cdot x)=f(\varphi_x(1))=\varphi_x(f(1))=x \cdot f(1)=\varphi_{f(1)}(x)$, ceea ce înseamnă că f este perfect determinat de imaginea $f(1)$ a elementului unitate din A și coincide cu $\varphi_{f(1)}$.

Să considerăm funcția $\alpha:A \rightarrow \text{End}(A)$, descrisă prin $\alpha(x)=\varphi_x$.

Această funcție este, conform observației anterioare, surjectivă. Dacă $\alpha(x)=\alpha(y)$ atunci în particular $\varphi_x(1)=\varphi_y(1)$, de unde $x=y$; așadar α este injectivă. Am stabilit anterior că $\alpha(x \cdot y)=\varphi_{x \cdot y}=\varphi_x \circ \varphi_y=\alpha(x) \circ \alpha(y)$ iar $\alpha(x+y)=\alpha(x)+\alpha(y)$, după cum se constată imediat. Așadar α este izomorfism de inele.

Dacă $(A, +, \cdot)$ este un inel (unitar) oarecare, iar $(A, +)$ este grupul aditiv subiacent al său, putem considera funcția $\alpha: A \rightarrow \text{End}(A)$ definită prin $\alpha(x)=\varphi_x$, cu $\varphi_x(y)=y \cdot x$, oricare ar fi $y \in A$. Această funcție este injectivă dar poate să nu fie surjectivă. De asemenea, $\alpha(x \cdot y)=\alpha(y) \circ \alpha(x)$.

7.22. Conform problemei 7.21, inelul $\text{End}(\mathbb{Z})$ este izomorf cu \mathbb{Z} .

Pentru simplitate luăm $n=2$ (cazul general tratându-se asemănător).

Considerăm proiecțiile canonice $p_1: \mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z}$ și $p_2: \mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z}$ date prin $p_1((a, b))=a$, $p_2((a, b))=b$. Acestea sunt morfisme de inele, deci și de grupuri definite pe G cu valori în \mathbb{Z} .

De asemenea considerăm injecțiile canonice $i_1: \mathbb{Z} \rightarrow \mathbb{Z} \times \mathbb{Z}$ și $i_2: \mathbb{Z} \rightarrow \mathbb{Z} \times \mathbb{Z}$ date prin $i_1(a)=(a, 0)$ și $i_2(a)=(0, a)$. Și acestea sunt morfisme de grupuri definite pe \mathbb{Z} cu valori în G .

Au loc relațiile: $p_1 \circ i_1 = 1_{\mathbb{Z}}$, $p_1 \circ i_2 = 0$, $p_2 \circ i_1 = 0$, $p_2 \circ i_2 = 1_{\mathbb{Z}}$, $i_1 \circ p_1 + i_2 \circ p_2 = 1_G$.

Construim o funcție $\varphi: \text{End}(G) \rightarrow M_2(\text{End}(\mathbb{Z}))$ astfel:

Dacă $f: G \rightarrow G$ este morfism de grupuri atunci apar patru morfisme de grupuri $p_k \circ f \circ i_l : \mathbb{Z} \rightarrow \mathbb{Z}$ pe care le scriem într-o matrice pătratică de ordinul doi: $\begin{pmatrix} p_1 \circ f \circ i_1 & p_1 \circ f \circ i_2 \\ p_2 \circ f \circ i_1 & p_2 \circ f \circ i_2 \end{pmatrix}$. Definind $\varphi(f)=(f_{kl})$ unde $f_{kl}=p_k \circ f \circ i_l$, se verifică imediat că φ este izomorfism de inele.

7.23. Fie $(A, +, \cdot)$ un inel care este domeniu de integritate și (A^*, \cdot) grupul unităților sale (mulțimea elementelor inversabile ale lui A). Dacă $a \in A^*$ atunci $-a \in A^*$. Într-adevăr, $a \in A^* \Rightarrow$ există $a^{-1} \in A^*$ a.î. $a \cdot a^{-1} = a^{-1} \cdot a = 1$, unde 1 este unitatea inelului A , adică a grupului (A^*, \cdot) și deci $(-a)(-a^{-1}) = aa^{-1} = 1$, $(-a^{-1})(-a) = a^{-1}a = 1$. În particular, $-1 \in A^*$.

Presupunem că $(A, +) \cong (A^*, \cdot)$, adică există o bijecție $f: A \rightarrow A^*$ cu $f(x+y) = f(x) \cdot f(y)$, oricare ar fi $x, y \in A$. Deoarece $-1 \in A^*$ și f este izomorfism rezultă că există un $x \in A$ a.î. $f(x) = -1$. Se mai știe că $f(0) = 1$.

Avem $f(x+x) = f(x) \cdot f(x) = (-1) \cdot (-1) = 1 = f(0)$ și cum f este bijectivă rezultă că $x+x=0 \Leftrightarrow (1+1)x=0$ și cum A este integru rezultă $x=0$ sau $1+1=0 \Leftrightarrow 1=-1$.

Prin urmare, oricare ar fi $y \in A$ avem $y+y = (1+1)y = 0$ și deci $f^2(y) = f(y+y) = f(0) = 1$, oricare ar fi $y \in A \Leftrightarrow [f(y)-1][f(y)+1] = 0$, oricare ar fi $y \in A \Leftrightarrow f(y) = 1$ sau $f(y) = -1$ și deoarece $1 = -1$ rezultă că $f(y) = 1$, oricare ar fi $y \in A$.

Deci $f(A) = \{1\}$ și cum f este surjectivă rezultă că $A^* = \{1\}$ și deoarece f este bijecție rezultă $\text{card} A = \text{card} A^* = 1$. Acesta este un rezultat contradictoriu deoarece $0, 1 \in A$ și deci $\text{card} A \geq 2$. Prin urmare $(A, +) \not\cong (A^*, \cdot)$.

7.24. Se consideră mulțimile:

$$A_1 = \{y \in A \mid f(xy) = f(x)f(y), \text{ oricare ar fi } x \in A\}$$

$$A_2 = \{y \in A \mid f(xy) = f(y)f(x), \text{ oricare ar fi } x \in A\}.$$

Din ipoteza 1) rezultă că f este morfism de la grupul $(A, +)$ la grupul (B, \cdot) , deci $f(0_A) = 0_B$. Atunci se vede ușor că $0_A \in A_1, 0_A \in A_2$ deci A_1 și A_2 sunt nevide.

Arătăm că A_1 este subgrup al grupului aditiv $(A, +)$.

Într-adevăr, dacă $y_1, y_2 \in A_1$ avem pentru orice $x \in A$: $f(x(y_1 - y_2)) = f(xy_1 - xy_2) = f(xy_1) - f(xy_2) = f(x)f(y_1) - f(x)f(y_2) = f(x)[f(y_1) - f(y_2)] = f(x)f(y_1 - y_2)$, ceea ce arată că $y_1 - y_2 \in A_1$. Analog se arată că A_2 este subgrup al grupului $(A, +)$. Vom arăta acum egalitatea $A = A_1 \cup A_2$. (*) Deoarece incluziunea $A \supseteq A_1 \cup A_2$ este evidentă, rămâne să dovedim incluziunea $A \subseteq A_1 \cup A_2$. Fie $y_0 \in A$ fixat.

Considerăm mulțimile:

$$C_1(y_0) = \{x \in A \mid f(xy_0) = f(x)f(y_0)\}$$

$$C_2(y_0) = \{x \in A \mid f(xy_0) = f(y_0)f(x)\}.$$

Ca și mai înainte, se arată că $C_1(y_0)$ și $C_2(y_0)$ sunt subgrupuri ale grupului $(A, +)$. Evident avem incluziunea $C_1(y_0) \cup C_2(y_0) \subseteq A$. Dar, datorită ipotezei 2), pentru orice $x \in A$ avem $f(xy_0) = f(x)f(y_0)$ sau $f(xy_0) = f(y_0)f(x)$, adică $x \in C_1(y_0)$ sau $x \in C_2(y_0)$, deci $x \in C_1(y_0) \cup C_2(y_0)$. Aceasta înseamnă că $A \subseteq C_1(y_0) \cup C_2(y_0)$, deci de fapt, $C_1(y_0) \cup C_2(y_0) = A$. (**)

Dar grupul A nu poate fi scris ca reuniunea a două subgrupuri proprii, deci în egalitatea (***) avem $A=C_1(y_0)$ sau $A=C_2(y_0)$. Dacă $A=C_1(y_0)$, rezultă că pentru orice $x \in A$ avem $f(xy_0)=f(x)f(y_0)$, deci $y_0 \in A_1$. Dacă $C_2(y_0)=A$, rezultă că pentru orice $x \in A$ avem $f(xy_0)=f(y_0)f(x)$, deci $y_0 \in A_2$.

Am arătat aşadar că $y_0 \in A_1 \cup A_2$ şi cum y_0 a fost arbitrar fixat în A , deducem că $A \subseteq A_1 \cup A_2$ şi deci avem (*). Dar A nu se poate scrie ca reuniune de două subgrupuri proprii şi atunci din (*) trebuie să avem $A=A_1$ sau $A=A_2$. Dacă $A=A_1$ rezultă că f este morfism de inele, iar dacă $A=A_2$ rezultă că f este antimorfism de inele.

§8. Ideale. Latticea idealelor unui inel comutativ. Anulatorul și radicalul unui inel. Factorizarea unui inel printr-un ideal bilateral. Ideale prime. Ideale maximale.

8.1. În inelul $(\mathbb{Q}, +, \cdot)$, \mathbb{Z} este subinel fără a fi însă ideal (deoarece de exemplu $2 \in \mathbb{Z}$ iar pentru $\frac{2}{3} \in \mathbb{Q}$, $2 \cdot \frac{2}{3} = \frac{4}{3} \notin \mathbb{Z}$).

8.2. Alegem inelul \mathbb{Z} și idealele $2\mathbb{Z}$ și $3\mathbb{Z}$. Deoarece $3-2=1 \notin 2\mathbb{Z} \cup 3\mathbb{Z}$ deducem că $2\mathbb{Z} \cup 3\mathbb{Z}$ nu este ideal al lui \mathbb{Z} .

8.3. Dacă $(I_k)_{k \in K}$ este o familie de ideale ale lui A , atunci $\bigwedge_{k \in K} I_k = \bigcap_{k \in K} I_k$ iar $\bigvee_{k \in K} I_k = \left(\bigcup_{k \in K} I_k \right)$.

8.4. (i). P este subinel fără a fi ideal (deoarece dacă $f \in P$ și $g \in A$,

$$g(x) = \begin{cases} x \sin \frac{1}{x}, & x \neq 0 \\ 0, & x = 0 \end{cases}$$

atunci $f \cdot g$ are o infinitate de zerouri, deci $f \cdot g \notin P$).

(ii), (iii). Analog ca la (i), P_n și Q_n sunt doar subinele ale lui A fără a fi însă ideale (cu același argument ca la (i)).

(iv). B este ideal al lui A .

(v). C este doar subinel al lui A fără a fi însă ideal (căci dacă alegem $f \in C$, $f(x)=x+1$, $g \in A$, $g(x)=x$, atunci $(f \cdot g)(0)=0$, deci $f \cdot g \notin C$).

8.5. Considerăm de exemplu divizorii lui zero din inelul \mathbb{Z}_6 . Evident, $\hat{2}$ și $\hat{3}$ sunt divizori ai lui zero dar nu și $\hat{3} - \hat{2} = \hat{1}$.

8.6. Luăm $i: \mathbb{Z} \rightarrow \mathbb{Q}$, $i(n)=n$, pentru orice $n \in \mathbb{Z}$.

Evident, \mathbb{Z} este ideal (impropriu) al lui \mathbb{Z} și $i(\mathbb{Z})=\mathbb{Z}$ nu este ideal în \mathbb{Q} .

8.7. (i). Pentru a arăta că A_1 este subinel al lui A verificăm că oricare ar fi $ux, uy \in A_1$, $ux-uy \in A_1$ și $(ux)(uy) \in A_1$.

Observăm că $ux-uy=u(x-y) \in A_1$, $(ux) \cdot (uy)=u^2xy=u(xy) \in A_1$, oricare ar fi $x, y \in A$, deci A_1 este subinel al lui A .

(ii). Fie $A_2=(1-u)A=\{(1-u)x \mid x \in A\}$. Deoarece $1-u \notin \{0,1\}$ și $(1-u)^2=(1-u)(1-u)=1-2u+u^2=1-2u+u=1-u$, rezultă conform celor de mai sus că A_2 este subinel al lui A .

b) Evident orice element $x \in A$ se scrie $x=x_1+x_2$ cu $x_1=ux \in A_1$ și $x_2=(1-u)x \in A_2$.

c) Fie $x_1 \in A_1$ și $x_2 \in A_2$. Atunci există $x'_1 \in A$ a.î. $x_1=ux'_1$ și există $x'_2 \in A$ a.î. $x_2=(1-u)x'_2$, $x_1x_2=ux'_1(1-u)x'_2=u(1-u)x'_1x'_2=(u-u^2)x'_1x'_2=0 \cdot x'_1x'_2=0$.

d) Fie $y \in A_1 \cap A_2$; atunci $y=ux=(1-u)z$ cu $x, z \in A$. Atunci $y=ux=u^2x=u(ux)=uy=u(1-u)z=(u-u^2)z=0 \cdot z=0$.

(iii). Din d) rezultă că scrierea lui x sub forma x_1+x_2 cu $x_1 \in A_1$ și $x_2 \in A_2$ este unică, deci $f(x)=(x_1, x_2)$, pentru $x=x_1+x_2$ este bine definită. Faptul că $f:A \rightarrow A_1 \times A_2$, $f(x)=(x_1, x_2)$ pentru $x=x_1+x_2$ (operațiile din A se efectuează pe componente) este un izomorfism rezultă imediat din c), d) și din unicitatea scrierii $x=x_1+x_2$. Morfismul invers este $g:A_1 \times A_2 \rightarrow A$, $g(x_1, x_2)=x_1+x_2$.

8.8. Considerăm următoarele patru matrice:

$$E_{11} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, E_{12} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, E_{21} = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, E_{22} = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}.$$

$$\text{Între ele există relațiile } E_{ij} \cdot E_{kl} = \begin{cases} E_{il} & \text{pentru } j = k \\ O_2 & \text{pentru } j \neq k \end{cases}.$$

Orice matrice $A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$ poate fi scrisă sub forma

$$A = a_{11}E_{11} + a_{12}E_{12} + a_{21}E_{21} + a_{22}E_{22}.$$

Să presupunem acum că I este un ideal bilateral nenul al inelului $M_2(\mathbb{R})$.

În I există deci o matrice nenulă $X = \begin{pmatrix} x_{11} & x_{12} \\ x_{21} & x_{22} \end{pmatrix}$. Produsele $E_{ki} \cdot X \cdot E_{jl}$ aparțin

idealului I . Avem $E_{ki} \cdot X \cdot E_{jl} = x_{ij} \cdot E_{kl}$. Evident, nu toate cele patru componente $x_{11}, x_{12}, x_{21}, x_{22}$ ale matricei X sunt nule. Dacă de exemplu $x_{12} \neq 0$ atunci din $E_{k1} \cdot X \cdot E_{21} = x_{12} \cdot E_{k1} \in I$, deducem că $a_{kl}E_{kl} = (a_{kl}x_{12}^{-1}E_{kk})(x_{12}E_{k1}) \in I$ și deci $A \in I$.

Așadar I coincide cu $M_2(\mathbb{R})$.

8.9. Alegem A un inel unitar nenul iar $B=M_n(A)$ cu $n \geq 2$ care nu este inel comutativ. Dacă I este mulțimea matricelor din B cu prima coloană formată numai din elemente egale cu zero se verifică imediat că I este un ideal stâng în B ce nu este drept căci

$$\begin{pmatrix} 0 & \dots & 0 & 1 \\ 0 & \dots & 0 & 0 \\ \dots & \dots & \dots & \dots \\ 0 & \dots & \dots & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & 0 & \dots & 0 \\ 0 & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 1 & \dots & \dots & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & \dots & \dots & 0 \end{pmatrix} \notin I.$$

Evident, prin schimbarea coloanelor în linii obținem un ideal drept ce nu este stâng.

8.10. Asocierea $d \rightsquigarrow \hat{d} \mathbb{Z}_n$ constituie o aplicație u de la laticia divizorilor lui n în laticia idealelor lui \mathbb{Z}_n . Evident, dacă d și d' sunt divizori ai lui n și $d|d'$ atunci $\hat{d} \mathbb{Z}_n \supseteq \hat{d}' \mathbb{Z}_n$. Deci $u(d) \supseteq u(d')$.

Reciproc, dacă $u(d) \subseteq u(d')$ atunci $\hat{d}' \mathbb{Z}_n \subseteq \hat{d} \mathbb{Z}_n$ și deci există $\hat{x} \in \mathbb{Z}_n$ cu $\hat{d} \cdot \hat{x} = \hat{d}'$, adică $n|dx-d'$. Cum $d|n$, deducem că $d|d'$ adică $d < d'$.

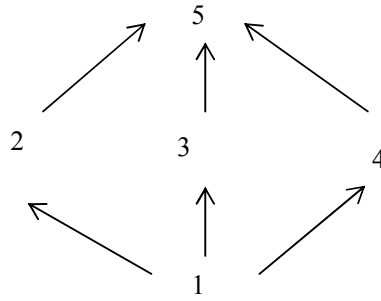
Deci dacă $u(d)=u(d')$, atunci avem $d < d'$ și $d' < d$, de unde rezultă că $d=d'$. În concluzie u este injectivă.

Fie acum I un ideal în \mathbb{Z}_n și $d = \inf\{t \in \mathbb{N} \mid t|n \text{ și } \hat{t} \in I\}$. Vom demonstra că $I = \hat{d} \mathbb{Z}_n = u(d)$. Evident, $I \supseteq \hat{d} \mathbb{Z}_n$. Pe de altă parte, dacă $\hat{x} \in I$ și $d' = (x, d)$, atunci există $p, q \in \mathbb{Z}$ cu $d' = px + qd$, de unde rezultă $\hat{d}' = \hat{p}x + \hat{q}d \in I$. Cum $d'|d$, deducem că $d=d'$. Deci $d|x$, adică $\hat{x} \in \hat{d} \mathbb{Z}_n$ și atunci $I \subseteq \hat{d} \mathbb{Z}_n$. În concluzie $I = u(d)$ și deci u este surjectivă.

8.11. Vom demonstra că laticia idealelor lui \mathbb{Z}_n este total ordonată dacă și numai dacă n este de forma p^s , p fiind un număr prim și s un număr natural. Evident, dacă $n = p^s$, atunci idealele lui \mathbb{Z}_n sunt de forma $(0) \subseteq (\hat{p}^{s-1}) \subseteq \dots \subseteq (\hat{p}) \subseteq (\hat{1}) = \mathbb{Z}_{p^s}$.

Reciproc, dacă n are în descompunerea sa doi factori primi distincți p și q , atunci laticia divizorilor lui n (deci și laticia idealelor lui \mathbb{Z}_n), (vezi problema **8.10.**) nu este total ordonată.

8.12. Nu. De exemplu, se observă că laticile idealelor lui \mathbb{Z}_n nu pot avea forma:



care este totuși o latice completă.

Dacă \mathbb{Z}_n are cinci ideale, ținând cont de descompunerea în factori primi a lui $n = p_1^{\alpha_1} \cdot \dots \cdot p_r^{\alpha_r}$ și de problema 8.10., deducem că $5 = \prod_{i=1}^r (\alpha_i + 1)$, de unde rezultă $r=1$ și $\alpha_1=4$. Deci n are forma generală p^4 , cu p prim. Pe de altă parte, $\mathbb{Z}/p^4\mathbb{Z}$ are laticea idealelor total ordonată, deci nu este de forma de mai sus.

8.13. Fie $f: \text{Id}_b(A) \rightarrow \text{Id}_b(M_n(A))$ definită prin

$$f(I) = \{(a_{ij}) \mid a_{ij} \in I \text{ pentru orice } i, j \in \{1, \dots, n\}\}.$$

Se verifică ușor că $f(I)$ este un ideal bilateral și că f este injectivă.

Fie U un ideal bilateral în $M_n(A)$. Definim pentru $t, s \in \{1, \dots, n\}$ mulțimile $U_{ts} = \{x \in A \mid \text{există o matrice } (a_{ij}) \text{ în } U \text{ a.î. } x = a_{ts}\}$. Se verifică ușor că U_{ts} sunt ideale bilaterale în A . Toate aceste ideale coincid, adică $U_{11} = U_{ts}$ pentru orice $t, s \in \{1, \dots, n\}$.

Într-adevăr, dacă $x \in U_{11}$ atunci există $(a_{ij}) \in U$ a.î. $x = a_{11}$.

Notăm prin P_{pq} ($p < q$) matricea care în pozițiile (t, t) cu $t \neq i, j$ și în pozițiile (i, j) și (j, i) are elementul $1 \in A$ și în rest 0.

Evident, prin înmulțirea matricei (a_{ij}) la stânga cu matricea P_{1t} și la dreapta cu matricea P_{1s} obținem o matrice care va aparține lui U și va conține elementul x în poziția (t, s) . Deci $x \in U_{ts}$. Analog demonstrăm că $U_{ts} \subseteq U_{11}$.

Notăm $I = U_{11}$. Vom arăta că $f(I) = U$. Evident, $U \subseteq f(I)$.

Fie acum $(a_{ij}) \in f(I)$. Deducem că $a_{ts} \in I = U_{11}$. Există deci o matrice $B_{ts} \in U$ care conține elementul a_{ts} pe poziția (t, s) . Notăm cu R_p matricea care are în

poziția (p, p) elementul 1 și în rest 0. Se observă ușor că avem $(a_{ij}) = \sum_{t,s=1}^n R_t B_{ts} R_s \in U$. Deci $U=f(I)$ și f este bijectivă.

8.14. Suma a două ideale $A+B=\{a+b|a \in A, b \in B\}$ este ideal. Deci $n\mathbb{Z}+m\mathbb{Z}$ este ideal. Cum \mathbb{Z} este principal există $D \in \mathbb{Z}$ a.î. $n\mathbb{Z}+m\mathbb{Z}=D\mathbb{Z}$.

Deci $n\mathbb{Z}, m\mathbb{Z} \subseteq D\mathbb{Z}$, adică $n, m \in D\mathbb{Z}$ și există $n', m' \in \mathbb{Z}$ a.î. $n=Dn'$ și $m=Dm'$. Rezultă $D|n$ și $D|m$.

Dacă avem $D' \in \mathbb{Z}$ a.î. $D'|n$ și $D'|m$ atunci există $n'', m'' \in \mathbb{Z}$ a.î. $n=D'n''$ și $m=D'm''$. Rezultă $n, m \in D'\mathbb{Z}$, adică $n\mathbb{Z}, m\mathbb{Z} \subseteq D'\mathbb{Z}$.

Din $n\mathbb{Z}+m\mathbb{Z} \subseteq D'\mathbb{Z} \Rightarrow D\mathbb{Z} \subseteq D'\mathbb{Z} \Rightarrow D \in D'\mathbb{Z} \Rightarrow D'|D \Rightarrow D=(n,m)$.

Intersecția a două ideale este un ideal. Rezultă că $n\mathbb{Z} \cap m\mathbb{Z}$ este ideal. Cum \mathbb{Z} este principal există $M \in \mathbb{Z}$ a.î. $n\mathbb{Z} \cap m\mathbb{Z}=M\mathbb{Z}$.

Cum $M \in M\mathbb{Z} \Rightarrow M \in n\mathbb{Z}, M \in m\mathbb{Z} \Rightarrow M$ este multiplu de m și n .

Dacă $M' \in \mathbb{Z}$ este un alt multiplu comun al numerelor n și m atunci $M' \in m\mathbb{Z}$ și $M' \in n\mathbb{Z}$, adică $M' \in n\mathbb{Z} \cap m\mathbb{Z}$, deci $M' \in M\mathbb{Z}$. Rezultă $M|M'$. Deci $M=[n,m]$.

8.15. Incluziunea $I+(J \cap K) \subseteq (I+J) \cap K$ este evidentă când $I \subseteq K$.

Reciproc, dacă $k \in (I+J) \cap K$, $k=i+j$ cu $i \in I, j \in J, k \in K$. Atunci $j=k-i \in K$ deoarece $I \subseteq K$ și atunci $k=i+j \in I+(J \cap K)$.

8.16. Înmulțind egalitatea $I+J=A$ cu L obținem $IL+JL=L$ și cum $IL \subseteq I, JL \subseteq I$ deducem că $L \subseteq I$.

8.17. Folosind inducția putem reduce problema la un ideal cu doi generatori, adică $A=Ax_1+Ax_2$. Fiecare element fiind idempotent sunt verificate egalitățile: $x_1=x_1(x_1+x_2-x_1x_2)$ și $x_2=x_2(x_1+x_2-x_1x_2)$.

Atunci $A=Ax_1+Ax_2=A(x_1+x_2-x_1x_2)$.

8.18. Idealul I fiind finit generat, fie $I=Ae_1+\dots+Ae_n$.

De asemenea, $I=Ia_1+\dots+Ia_n$ (sunt verificate $IA=I$ și $I^2=I$). Atunci pentru fiecare $k, 1 \leq k \leq n$ există un element $b_k \in I$ a.î. $(1-b_k)I \subseteq Ia_k+\dots+Ia_n$.

Se verifică prin inducție după k . Pentru $k=1$ avem $b_1=0$. Dacă $b_k \in I$, alegem un $b_{k+1} \in I$ a.î. $(1-b_{k+1})I \subseteq I a_{k+1} + \dots + I a_n$.

În final, $e=b_{n+1} \in I$ este elementul idempotent căutat.

8.19. Considerăm incluziunea $f: \mathbb{Z} \rightarrow \mathbb{C}[X, Y]$ și M idealul maximal al polinoamelor cu termenul liber nul. $f^{-1}(M) = \{0\} \neq \mathbb{Z}$, nu este ideal maximal al lui \mathbb{Z} .

Observație. Dacă $f: A \rightarrow A'$ este un morfism surjectiv de inele și M este ideal maximal în A' atunci $f^{-1}(M)$ este ideal maximal în A .

8.20. \mathbb{Z} fiind inel comutativ, idealul $n\mathbb{Z}$ este prim dacă și numai dacă $\mathbb{Z}/n\mathbb{Z}$ este domeniu de integritate, adică dacă și numai dacă \mathbb{Z}_n este domeniu de integritate, adică dacă n este număr prim.

Avem că $2\mathbb{Z}, 3\mathbb{Z}, 5\mathbb{Z}, \dots, p\mathbb{Z}, \dots$ (p prim) sunt ideale prime ale lui \mathbb{Z} .

8.21. Fie inelul \mathbb{Z} și idealul nul $I=(0)=\{0\}$. În mod evident I este prim dar nu este maximal.

8.22. Inelul $\mathbb{Z}/2^s\mathbb{Z}$ are idealele $(0) \subseteq (2^{s-1}) \subseteq (2^{s-2}) \dots \subseteq (2) \subseteq (1) = \mathbb{Z}/2^s\mathbb{Z}$.

Deci pentru orice $n \geq 1$, inelul $\mathbb{Z}/2^{n-1}\mathbb{Z}$ are n ideale. Evident, putem lua orice număr prim p în loc de 2.

8.23. Evident R este subinel: $A, B \in R \Rightarrow A-B \in R, A \cdot B \in R$.

$$\text{Avem } \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \neq \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}.$$

Deci R are proprietățile cerute.

$$\begin{pmatrix} 0 & a \\ 0 & b \end{pmatrix}^2 = \begin{pmatrix} 0 & ab \\ 0 & b^2 \end{pmatrix} = O_2 \Leftrightarrow b=0, \text{ deci } I = \left\{ \begin{pmatrix} 0 & a \\ 0 & 0 \end{pmatrix} \mid a \in Q \right\}.$$

Pentru $A, B \in I, C \in R$ avem $A-B, CA, AC \in I$.

$$\text{În final, } \begin{pmatrix} 0 & a_1 \\ 0 & b_1 \end{pmatrix} - \begin{pmatrix} 0 & a_2 \\ 0 & b_2 \end{pmatrix} \in I \Leftrightarrow b_1 = b_2.$$

Aplicația $f: \mathbb{R} \rightarrow \mathbb{Q}$, $f\left(\begin{pmatrix} 0 & a \\ 0 & b \end{pmatrix}\right) = b$, oricare ar fi $b \in \mathbb{Q}$ este un morfism

surjectiv de inele cu $\text{Ker}(f) = I$. Totul rezultă din teorema fundamentală de izomorfism pentru inele.

8.24. f fiind morfism de inele avem $f(I + \text{Ker}(f)) = f(I)$, deci $I + \text{Ker}(f) \subseteq f^{-1}(f(I))$. Invers, dacă $r \in f^{-1}(f(I))$ atunci $f(r) = f(a)$, pentru un anumit $a \in I$. Deci $f(r-a) = 0$, adică $r-a \in \text{Ker}(f)$. Rezultă $r \in a + \text{Ker}(f) \subseteq I + \text{Ker}(f)$.

8.25. Pentru funcția normă $N: \mathbb{Z}[i] \rightarrow \mathbb{Z}$, $N(a+bi) = a^2 + b^2$ în $\mathbb{Z}[i]$, avem $N(xy) = N(x) \cdot N(y)$, oricare ar fi $x, y \in \mathbb{Z}[i]$.

Unitățile lui $\mathbb{Z}[i]$ sunt $\{1, -1, i, -i\}$, adică acele elemente $x \in \mathbb{Z}[i]$ pentru care $N(x) = 1$.

Elementul x este prim în $\mathbb{Z}[i]$ dacă și numai dacă $N(x)$ este prim în \mathbb{Z} .

Deci $N(1+i) = 2$ implică faptul că idealul $(1+i)$ este prim.

În continuare vom demonstra că un număr prim $p \in \mathbb{N}^*$ este de asemenea prim în $\mathbb{Z}[i]$ dacă și numai dacă ecuația $a^2 + b^2 = p$ nu are soluții în \mathbb{Z} .

Astfel, dacă $a^2 + b^2 = p$ are soluții întregi atunci $p = (a+ib)(a-ib)$ este o descompunere netrivială pentru că $N(a+ib) = N(a-ib) = p \neq 1$. Invers, dacă $p = (a+ib)(c+id)$ este o descompunere netrivială, pentru $N(a+ib) \cdot N(c+id) = p^2$ trebuie să avem $N(a+ib) = N(c+id) = p$. Produsul $(a+ib)(c+id)$ fiind număr real și $a+ib, c+id$ având același modul, $a-ib = c+id$. Atunci $p = a^2 + b^2 = (a+ib)(a-ib)$.

În final, $a^2 + b^2 = 3$ nu are soluții întregi dar $a^2 + b^2 = 2$ are soluția $a = b = 1$. Deci (3) este ideal prim iar (2) nu este prim.

8.26. (i) \Rightarrow (ii). Presupunem că inelul cît A/P este integru și prin absurd, că există idealele I și J a.î. $I \not\subseteq P$ și $J \not\subseteq P$ dar $IJ \subseteq P$.

Alegem elementele $a \in I - P$ și $b \in J - P$. În inelul cît A/P avem $\bar{a}, \bar{b} \neq \bar{0}$. Însă $ab \in IJ \subseteq P$, deci $\bar{a}\bar{b} = \bar{0}$, se contrazice integritatea inelului A/P .

(ii) \Leftarrow (i). Reciproc, fie a, b elemente din A a.î. $\bar{a}\bar{b} = \bar{0}$ în A/P . Notăm $I = aA, J = bA$. Atunci $IJ \subseteq P$, deci $I \subseteq P$ sau $J \subseteq P$. Aceasta înseamnă că $\bar{a} = \bar{0}$ sau $\bar{b} = \bar{0}$, deci A/P este integru.

8.27. Fie J, K ideale ale lui A a.î. $J \not\subseteq I$ și $K \not\subseteq I$. Din maximalitatea lui I deducem că $(J+I) \cap S \neq \emptyset$ și $(K+I) \cap S \neq \emptyset$. Există atunci $s_1 \in (J+I) \cap S$ și $s_2 \in (K+I) \cap S$. S fiind sistem multiplicativ avem $s_1 s_2 \in S$, deci $s_1 s_2 \in (J+I)(K+I) \cap S$ și $s_1 s_2 \in JK+I$. Atunci $s_1 s_2 \notin I$ implică $JK \not\subseteq I$.

8.28. Notăm cu T intersecția idealelor maximale ale lui $A[X]$ și presupunem că $0 \neq f \in T$. Fie M un ideal maximal care include idealul principal $(1+Xf)$.

Un astfel de ideal maximal există deoarece $f \neq 0$ implică $1+Xf$ nu este inversabil în $A[X]$. Cum $f \in M$ rezultă $1 \in M$, contradicție.

8.29. Fie P un ideal prim în A . Atunci A/P este integru dar cum el este și finit rezultă că este corp. Deci, P este maximal.

8.30. Fie P un ideal prim și I un ideal în A a.î. $P \subsetneq I$. Deci există un $x \in I \setminus P$. Cum $x^n = x$, pentru un $n \in \mathbb{N}$ $0 = x(x^{n-1} - 1) \in P$. Astfel $(x^{n-1} - 1) \in P \subsetneq I$ și cum $x \in I$ obținem $1 \in I$, adică $I = A$. Rezultă că P este maximal.

8.31. Considerăm morfismul $\varphi: \mathbb{Z}[X, Y] \rightarrow \mathbb{Z}[Y]$ definit prin $\varphi(f) = g_0$ unde $f = g_n X^n + \dots + g_1 X + g_0 \in \mathbb{Z}[Y][X]$. Acesta este surjectiv și $\text{Ker}(\varphi) = (X)$, de unde obținem izomorfismul $\mathbb{Z}[X, Y]/(X) \simeq \mathbb{Z}[Y]$. Cum $\mathbb{Z}[Y]$ este integru dar nu este corp obținem rezultatul cerut.

8.32. (i). Considerăm morfismul compunere $A[X] \rightarrow A \rightarrow A/(a)$ pe care îl notăm cu φ și avem pentru $f = \sum_{i=0}^n a_i X^i$, $\varphi(f) = a_0 + (a)$.

φ este surjectiv și $\text{Ker}(\varphi) = \{ f = \sum_{i=0}^n a_i X^i \mid a_0 \in (a) \} = (X, a)$, de unde $A[X]/(X, a) \simeq A/(a)$

(ii). rezultă din (i) și pentru (iii) se alege $A = \mathbb{Z}$ și $a = 0$ după care se aplică (ii).

8.33. (i). Fie $x \in J(A)$. Deci $x \in M$ pentru orice ideal maximal M . Fie $y \in A$. Atunci $1 - xy \notin M$, altfel $1 \in M$ deci $M = A$, fals. Obținem astfel $M + (1 - xy) = A$, adică există un $z \in A$ pentru care $1 = 0 + (1 - xy)z$.

Deci $1-xy$ este inversabil pentru orice y , cum y a fost ales arbitrar. Presupunem acum că $x \notin M_0$, unde M_0 este ideal maximal. Atunci $M_0 + (x) = A$, adică există $y \in A$ pentru care $1-xy \in M_0$, deci este neinversabil, ceea ce contrazice ipoteza noastră.

(ii). Fie I un ideal în A care are proprietatea din enunț. Fie $x \in I$ și $y \in A$. Cum $xy \in I$ obținem $1-xy \in U(A)$ adică $x \in J(A)$.

8.34. Conform problemei **8.33.** căutăm matrice $\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}$ a.î. matricea

$$I_2 - \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \begin{pmatrix} x & y \\ 0 & z \end{pmatrix} = \begin{pmatrix} 1-ax & -ay-bz \\ 0 & 1-cz \end{pmatrix}$$

să fie inversabilă pentru orice $x, y, z \in \mathbb{Z}$, adică $(1-ax)(1-cz) = \pm 1$, pentru orice $x, y, z \in \mathbb{Z}$. De aici rezultă că $a=c=0$ și deci

$$J(A) = \left\{ \begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix} \mid b \in \mathbb{Z} \right\}.$$

8.35. Fie $A = (\mathbb{Q}, +, \odot)$, unde pentru $x, y \in \mathbb{Q}$, $x \odot y = 0$; evident A nu are element unitate diferit de 0. Idealele lui A sunt exact subgrupurile lui $(\mathbb{Q}, +)$. Cum $(\mathbb{Q}, +)$ este grup divizibil, \mathbb{Q} nu are subgrupuri maximale. Astfel, \mathbb{Z} este un ideal al lui A ce nu este conținut într-un ideal maximal.

8.36. Presupunem că există $f \in J(A[X])$ nenul. Atunci $g = fX + 1$ este element neinversabil în $A[X]$ deci există un ideal maximal M pentru care $g \in M$. Din alegerea lui f , $f \in M$ de unde rezultă $1 \in M$, adică $M = A$, ceea ce este fals.

8.37. (i). Dacă $x \in \text{Ann}(I)$ și $a \in A$, atunci pentru orice $i \in I$ avem $i(xa) = (ix)a = 0 \cdot a = 0$, adică $xa \in \text{Ann}(I)$.

Pentru a arăta că $r(I)$ este un ideal mai dificil este a demonstra că suma a două elemente din $r(I)$ se găsește în $r(I)$.

Fie $x, y \in r(I)$. Deci există numerele naturale m și n a.î. $x^m \in I$ și $y^n \in I$. În $(x+y)^k = \sum_{t=0}^k C_k^t x^{k-t} y^t$ luăm $k = m+n-1$. Dintre cei $m+n$ termeni ai sumei din membrul drept în primii n (deci cei pentru care $t \leq n-1$) apare ca factor x^m , iar în ceilalți apare ca factor y^n . Așadar, $(x+y)^{m+n-1} \in I$, ceea ce înseamnă că $x+y \in r(I)$.

(ii). 1) Incluziunea $I \subseteq r(I)$ este evidentă.

Deducem că $r(I) \subseteq r(r(I))$.

Fie $a \in r(I)$; rezultă că există $n \in \mathbb{N}$ a.î. $a^n \in r(I)$, deci există $m \in \mathbb{N}$ a.î. $(a^n)^m = a^{nm} \in I$, adică $a \in r(I)$. Deci $r(I) = r(r(I))$.

2) Din $a \in r(I) \cap r(J)$ rezultă că există m și $n \in \mathbb{N}$ a.î. $a^n \in I$ și $a^m \in J$, deci $a^{n+m} = a^n \cdot a^m \in I \cap J$, deci $a \in r(I \cap J)$.

3) Din $a \in r(r(I) + r(J))$ rezultă că există $k \in \mathbb{N}$ a.î. $a^k = s + t$, cu $s \in r(I)$, $t \in r(J)$. Dacă $s^n \in I$ și $t^m \in J$ aplicând din nou binomul lui Newton deducem că $a^{k(n+m)} = (s+t)^{n+m} \in I + J$ și obținem concluzia.

8.38. Notăm $s: A \rightarrow A/r(A)$ morfismul canonic.

Fie $x \in A$ a.î. $s(x)$ este nilpotent. Există deci $n \in \mathbb{N}$ a.î. $s(x)^n = s(0)$. Deci $x^n \in \text{Ker}(s) = r(A)$; există atunci $m \in \mathbb{N}$ a.î. $(x^n)^m = 0$. Aceasta înseamnă că $x^{nm} = 0$, deci x este nilpotent și astfel $s(x) = s(0)$. Putem spune deci că idealul $r(A/r(A))$ este nul.

8.39. Fie a, b elemente idempotente din A a.î. $f(a) = f(b)$.

Notăm $n = a - b \in \text{Ker}(f)$. Evident, avem $n^3 = a^3 - 3a^2b + 3ab^2 - b^3 = a - b = n$ și rezultă $n(1 - n^2) = 0$. Dar $1 - n^2$ este element inversabil (pentru că adunând un element nilpotent cu unul inversabil obținem un element inversabil) și deci $n = 0$.

Fie $a' = f(x)$ un element idempotent din A' . Căutăm un element a idempotent în A de forma $x + z$ cu $z \in \text{Ker}(f)$.

Analizăm întâi cazul cînd $(\text{Ker}(f))^2 = 0$. Astfel căutăm $z \in \text{Ker}(f)$ a.î. $(x+z)^2 = x+z$, adică a.î. $z(1-2x) = x^2 - x$.

Cum $x^2 - x \in \text{Ker}(f)$ rezultă $(1-2x)(1+2x-12x^2+8x^3) = 1 - 16(x^2-x)^2 = 1$. Deci $1-2x$ este inversabil în A și $z = (x^2-x)(1-2x)^{-1}$ este un element din $\text{Ker}(f)$ a.î. $a = x+z$ este idempotent.

În cazul general, alegem k a.î. $n = x^2 - x$ să satisfacă $n^k = 0$. Considerăm surjecțiile canonice $f_i: A/(n^{i+1}) \rightarrow A/(n^i)$, $1 \leq i < k$.

Evident, elementul $\text{cls } x \pmod{n}$ este idempotent în $A/(n)$. Cum $\text{Ker}(f_1) = (n)/(n^2)$ are pătratul nul, există $x_1 \in A$ a.î. $\text{cls } x_1 \pmod{n^2}$ să fie idempotent în $A/(n^2)$ iar $x_1 \equiv x \pmod{n}$. Raționând inductiv, obținem un element $x_{k-1} \in A$ a.î. $\text{cls } x_{k-1} \pmod{n^k}$ să fie idempotent în $A/(n^k)$ iar $x_{k-1} \equiv x \pmod{n}$. Luăm $a = x_{k-1}$.

8.40. Fie p un număr prim și s un număr natural. Evident $r(\mathbb{Z}/p^s\mathbb{Z})$ este idealul principal generat de p . Deci $r(\mathbb{Z}/p^s\mathbb{Z})$ are p^{s-1} elemente. Folosind faptul că $r(A \times B) = r(A) \times r(B)$ deducem că dacă $n = p_1^{\alpha_1} \dots p_r^{\alpha_r}$ este descompunerea în factori primi a lui n ($p_i \neq p_j$ pentru $i \neq j$) atunci avem $r\left(\prod_{i=1}^r \mathbb{Z}/p_i^{\alpha_i}\mathbb{Z}\right) = \prod_{i=1}^r r(\mathbb{Z}/p_i^{\alpha_i}\mathbb{Z})$. Deci $r\left(\prod_{i=1}^r \mathbb{Z}/p_i^{\alpha_i}\mathbb{Z}\right)$ are $\prod_{i=1}^r p_i^{\alpha_i-1}$ elemente și cum $\mathbb{Z}/n\mathbb{Z} \cong \prod_{i=1}^r \mathbb{Z}/p_i^{\alpha_i}\mathbb{Z}$ deducem că $r(\mathbb{Z}/n\mathbb{Z})$ are același număr de elemente. În particular, $\mathbb{Z}/n\mathbb{Z}$ este redus dacă și numai dacă, $r(\mathbb{Z}/n\mathbb{Z})$ are un singur element ($\hat{0}$), adică dacă și numai dacă, $\prod_{i=1}^r p_i^{\alpha_i-1} = 1$, ceea ce este echivalent cu $\alpha_i = 1$, pentru orice $i \in \{1, \dots, r\}$.

8.41. Faptul că I este ideal se verifică fie prin calcul direct, fie observând că este nucleul morfismului de inele $F: C([0, 1], \mathbb{R}) \rightarrow \mathbb{R}$, $F(f) = f(0)$, ce evaluează în punctul $t=0$ funcțiile continue pe $[0, 1]$.

Să presupunem prin reducere la absurd că I ar fi principal, generat de funcția continuă $\varphi: [0, 1] \rightarrow \mathbb{R}$. Atunci $\varphi(0) = 0$ și orice funcție $f \in I$ ar fi multiplu al lui φ . În particular, luând funcția f descrisă de $f(t) = \sqrt[3]{\varphi(t)}$, $t \in [0, 1]$, avem $f \in I$, deci putem scrie $\varphi(t) \cdot g(t) = \sqrt[3]{\varphi(t)}$, $t \in [0, 1]$, cu g funcție continuă pe $[0, 1]$. Funcția φ nu este identic nulă căci $I \neq \{0\}$, în mod evident. Dacă notăm $\bar{t} = \sup\{t \mid \varphi(t) = 0\}$ atunci $\bar{t} < 1$, $\varphi(\bar{t}) \neq 0$, pentru $\bar{t} < t \leq 1$, iar $\varphi(\bar{t}) = 0$ datorită continuității lui φ . Pentru fiecare argument t cu $\bar{t} < t \leq 1$ obținem deci $1 = [\sqrt[3]{\varphi(t)}]^2 \cdot g(t)$, de unde trecând la limită când $t \rightarrow \bar{t}$ obținem $1 = 0 \cdot g(\bar{t}) = 0$, contradicție. Deci inelul $C([0, 1], \mathbb{R})$ nu este principal.

8.42. Determinăm numerele întregi de forma $u = (a+b\sqrt{d})(m+n\sqrt{d})$, $a, b, m, n \in \mathbb{Z}$. Aceasta are loc dacă și numai dacă $an+bm=0$, care are soluțiile întregi de forma $n = \frac{-b}{(a,b)} \cdot s$, $m = \frac{a}{(a,b)} \cdot s$, unde $s \in \mathbb{Z}$. Deci numerele întregi u

de mai sus trebuie să fie de forma $am + bnd = \frac{a^2 - b^2d}{(a,b)} \cdot s$, $s \in \mathbb{Z}$. Notând

$$t = \frac{a^2 - b^2d}{(a,b)} \text{ dacă } b \neq 0 \text{ și } t = a \text{ când } b = 0, \text{ obținem } (x) \cap \mathbb{Z} = t\mathbb{Z}.$$

Evident $(x) = (0)$ implică $(x) \cap \mathbb{Z} = (0)$. Reciproc, dacă $(x) \cap \mathbb{Z} = (0)$ atunci $(t) = (0)$, deci $t = 0$. Obținem $a^2 - b^2d = 0$. Dar d este liber de pătrate și deci b trebuie să fie nul (altfel am avea $d = \left(\frac{a}{b}\right)^2$, contradicție). În concluzie, $a = b = 0$, adică $(x) = (0)$.

8.43. Inelul $A = T_2(\mathbb{Z}_2)$ are ca elemente matricele $\begin{pmatrix} a & b \\ \hat{0} & c \end{pmatrix}$ cu $a, b, c \in \mathbb{Z}_2$.

Întrucât \mathbb{Z}_2 are doar două elemente și anume clasele $\hat{0}$ și $\hat{1}$ deducem că inelul $T_2(\mathbb{Z}_2)$ are $2^3 = 8$ elemente. Grupul aditiv subiacent inelului este izomorf cu $(\mathbb{Z}/2\mathbb{Z})^3$; notând $X = \begin{pmatrix} \hat{1} & \hat{0} \\ \hat{0} & \hat{0} \end{pmatrix}$, $Y = \begin{pmatrix} \hat{0} & \hat{1} \\ \hat{0} & \hat{0} \end{pmatrix}$, $Z = \begin{pmatrix} \hat{0} & \hat{0} \\ \hat{0} & \hat{1} \end{pmatrix}$ cele opt elemente ale

inelului $T_2(\mathbb{Z}_2)$ pot fi descrise astfel: $O, X, Y, Z, X+Y, X+Z, Y+Z, X+Y+Z$. Înmulțirea inelului este descrisă (ținând cont de distributivitatea ei față de adunare) de tabelul:

·	X	Y	Z
X	X	Y	O
Y	O	O	Y
Z	O	O	Z

Observăm că elementele inversabile sunt $X+Z$ (elementul unitate) și $X+Y+Z = \begin{pmatrix} \hat{1} & \hat{1} \\ \hat{0} & \hat{1} \end{pmatrix}$.

Vom determina mai întâi idealele stângi principale.

Elementul X determină un ideal stâng format doar din matricele O și X . La fel elementele Y și $X+Y$ determină idealele stângi formate doar din câte două elemente. Elementele Z și $Y+Z$ sunt asociate și determină un ideal stâng format din patru elemente: $O, Y, Z, Y+Z$.

Idealele stângi ale inelului pot fi ordonate (prin incluziune) ca în Figura 1:

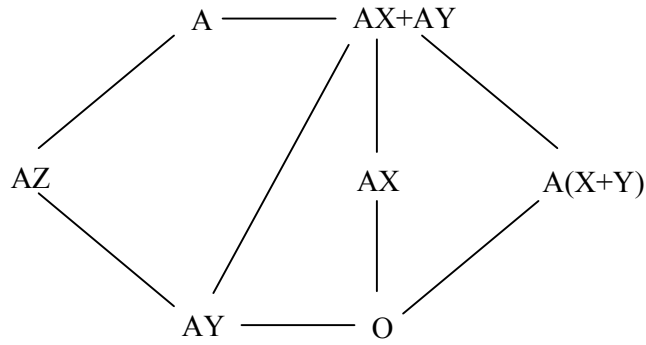


Figura 1

Unul singur este neprincipal și anume $AX+AY$, format din matricele

$$\begin{pmatrix} a & b \\ \hat{0} & \hat{0} \end{pmatrix}.$$

Idealele drepte se obțin observând dualitatea „stânga-dreapta” între X și Z . Ele sunt prezentate în Figura 2:

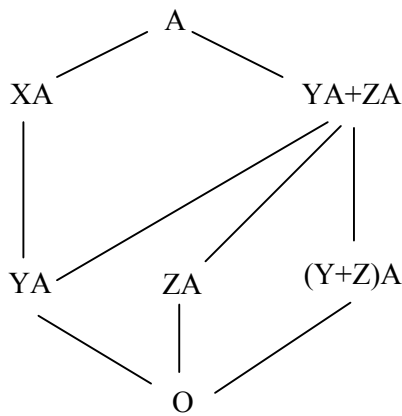


Figura 2

În final observăm că inelul $A=T_2(\mathbb{Z}_2)$ are trei ideale bilaterale netriviiale: primul $AY=YA$, format din matricele $\begin{pmatrix} \hat{0} & b \\ \hat{0} & \hat{0} \end{pmatrix}$; al doilea,

$AX+AY=XA$, format din matricele $\begin{pmatrix} a & b \\ \hat{0} & \hat{0} \end{pmatrix}$; al treilea, $AZ=YA+ZA$, format din matricele $\begin{pmatrix} \hat{0} & b \\ \hat{0} & c \end{pmatrix}$.

8.44. Faptul că A este subinel al lui B și că B este subinel al lui $T_2(\mathbb{Q})$ se verifică imediat. Putem scrie, simbolic, $A = \begin{pmatrix} Z & Q \\ 0 & Z \end{pmatrix}$ și $B = \begin{pmatrix} Z & Q \\ 0 & Q \end{pmatrix}$.

Determinăm mai întâi idealele bilaterale ale inelului B .

Fie I un asemenea ideal. Considerând funcțiile $f: B \rightarrow \mathbb{Z}$ și $g: B \rightarrow \mathbb{Q}$ ce asociază matricei $\begin{pmatrix} a & p \\ 0 & q \end{pmatrix}$ pe a respectiv pe q , obținem (ca în problema 7.13.) că f și g sunt morfisme de inele. Deci $f(I)$ este ideal al lui \mathbb{Z} , adică este de forma $m\mathbb{Z}$ (cu $m \in \mathbb{N}$) iar $g(I)$ este ideal al lui \mathbb{Q} , deci este nul sau coincide cu \mathbb{Q} . Așadar I este de forma $\begin{pmatrix} mZ & T \\ 0 & 0 \end{pmatrix}$ sau de forma $\begin{pmatrix} mZ & T \\ 0 & Q \end{pmatrix}$.

Identificăm proprietățile submulțimii T a lui \mathbb{Q} .

Din $I+ICI$ rezultă că $T+T \subset T$ iar din $IBCI$ rezultă că $m\mathbb{Q}+T\mathbb{Q} \subset T$, adică T este ideal al lui \mathbb{Q} ce conține pe $m\mathbb{Q}$. În cazul când $m \neq 0$, obținem $T = \mathbb{Q}$, iar dacă $m = 0$, putem avea $T = \{0\}$ sau $T = \mathbb{Q}$.

Idealele bilaterale ale inelului B sunt deci următoarele:

$$\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & Q \end{pmatrix}, \begin{pmatrix} mZ & Q \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} mZ & Q \\ 0 & Q \end{pmatrix} \text{ cu } m \in \mathbb{N}.$$

Pentru a determina idealele bilaterale ale inelului A procedăm asemănător. Considerăm morfismele surjective de inele $f: A \rightarrow \mathbb{Z}$ și $g: A \rightarrow \mathbb{Z}$ ce asociază matricei $\begin{pmatrix} a & p \\ 0 & b \end{pmatrix}$ pe a respectiv pe b . Dacă I este un ideal bilateral al lui A , atunci atât $f(I)$ cât și $g(I)$ sunt ideale ale lui \mathbb{Z} , deci de forma $m\mathbb{Z}$, respectiv $n\mathbb{Z}$ (cu $m, n \in \mathbb{N}$) iar $I = \begin{pmatrix} mZ & T \\ 0 & nZ \end{pmatrix}$.

Determinăm forma lui T . Din $I+ICI$ rezultă că $T+T \subset T$, din $IACI$ rezultă $m\mathbb{Q}+T\mathbb{Z} \subset T$ iar din $AICI$ rezultă $n\mathbb{Q}+T\mathbb{Z} \subset T$. Din aceste condiții deducem că T trebuie să fie subgroup aditiv al lui \mathbb{Q} iar în caz că $m \neq 0$ sau $n \neq 0$, T trebuie să-l conțină pe \mathbb{Q} , deci să coincidă cu \mathbb{Q} .

Dacă însă $m=n=0$, T poate fi orice subgrup al grupului aditiv al numerelor raționale \mathbb{Q} . Idealele bilaterale ale inelului B sunt deci de forma $\begin{pmatrix} m\mathbb{Z} & \mathcal{Q} \\ 0 & \mathbb{Z} \end{pmatrix}$ cu $m, n \in \mathbb{N}$ sau de forma $\begin{pmatrix} 0 & T \\ 0 & 0 \end{pmatrix}$, unde T este subgrup aditiv al lui \mathbb{Q} .

Inelul $T_2(\mathbb{Q})$ are doar trei ideale bilaterale netriviale: $\begin{pmatrix} 0 & \mathcal{Q} \\ 0 & 0 \end{pmatrix}$, $\begin{pmatrix} \mathcal{Q} & \mathcal{Q} \\ 0 & 0 \end{pmatrix}$, $\begin{pmatrix} 0 & \mathcal{Q} \\ 0 & \mathcal{Q} \end{pmatrix}$.

Prin același procedeu se obțin și idealele bilaterale ale lui $T_2(\mathbb{Z})$. Ele sunt de forma $\begin{pmatrix} m\mathbb{Z} & d\mathbb{Z} \\ 0 & n\mathbb{Z} \end{pmatrix}$ cu $m, n \in \mathbb{N}$ iar d divizor comun al lui m și n .

8.45. Dacă I și J sunt ideale nilpotente atunci fiecare element din $I+J$ este nilpotent. Într-adevăr, fie $x+y=z \in I+J$ ($x \in I, y \in J$) și $k \in \mathbb{N}^*$ a.î. $x^k=0$. Avem $z^k=(x+y)^k=x^k+a$ cu $a \in J$. În fiecare produs $xyxy\dots xy$ orice $xy \in J$ pentru că J este ideal stâng, $xyx \in J$ pentru că J este ideal drept.

În final, există $l \in \mathbb{N}^*$ a.î. $a^l=0$, deci $z^{kl}=a^l=0$, adică z este nilpotent și deci $I+J$ este nilpotent. Dacă I și J sunt ideale nilpotente și $I^n=J^m=0$ atunci $(I+J)^{n+m} \subset I^{n+m}+J^{n+m}$, deci $I+J$ este nilpotent.

Verificarea incluziunii inverse se probează astfel:

Orice element din $(I+J)^{n+m}$ este o sumă de produse care conțin $n+m$ factori din I sau J , adică (cel puțin n) factori din I sau (cel puțin m) factori din J , (adică un produs finit de forma $a_1 b_1 a_2 b_2 \dots$ cu $a_i \in I$ și $b_j \in J$ poate fi scris ca $a_1' a_2' a_3' \dots$ cu $a_i' \in I$, folosind faptul că I este ideal stâng sau $b_1' b_2' b_3' \dots$ cu $b_j' \in J$, folosind faptul că J este ideal stâng) și folosim incluziunile evidente $I^t \subseteq I^{n+m}, J^t \subseteq J^{n+m}$ pentru orice $t \leq n+m$.

8.46. Presupunem prin reducere la absurd că pe \mathbb{Q}/\mathbb{Z} avem definită o înmulțire \cdot care împreună cu adunarea să determine o structură de inel unitar. Fie u elementul unitate al acestui inel. Îl putem scrie pe u sub formă de fracție ireductibilă, $u = \frac{m}{n}$, cu $1 \leq m < n$, m, n numere întregi prime între ele.

Deoarece, $x=u \cdot x$ pentru orice $x \in \mathbb{Q}/\mathbb{Z}$ avem în particular pentru $x = \frac{1}{m}$:

$$\frac{1}{m} = \frac{m}{n} \bullet \frac{1}{m} = \left(\underbrace{\frac{1}{n} + \dots + \frac{1}{n}}_{\text{de } m \text{ ori}} \right) \bullet \frac{1}{m} = \underbrace{\frac{1}{n} \bullet \frac{1}{m} + \dots + \frac{1}{n} \bullet \frac{1}{m}}_{\text{de } m \text{ ori}} = \frac{1}{n} \bullet \left(\underbrace{\frac{1}{m} + \dots + \frac{1}{m}}_{\text{de } m \text{ ori}} \right) = \frac{1}{n} \bullet 1 = \frac{1}{n} \bullet 0 = 0$$

(am folosit faptul că $1=0$ în \mathbb{Q}/\mathbb{Z}). Din $\frac{1}{m}=0$ deducem că $m=1$. Deci elementul unitate al inelului trebuie să fie de forma $u = \frac{1}{n}$ cu $n > 1$.

Luând $x = \frac{n}{n+1}$ în relația $x=u \cdot x$, obținem:

$$\frac{n}{n+1} = \frac{1}{n} \bullet \frac{n}{n+1} = \frac{1}{n} \bullet \left(\underbrace{\frac{1}{n+1} + \dots + \frac{1}{n+1}}_{\text{de } n \text{ ori}} \right) = \left(\underbrace{\frac{1}{n} + \dots + \frac{1}{n}}_{\text{de } n \text{ ori}} \right) \bullet \frac{1}{n+1} = 1 \bullet \frac{1}{n+1} = 0 \bullet \frac{1}{n+1} = 0$$

Deci $\frac{n}{n+1} = 0$ în \mathbb{Q}/\mathbb{Z} , adică $\frac{n}{n+1}$ este un număr întreg, absurd.

8.47. Considerăm morfismele canonice $p_I: A \rightarrow A/I$, $p_J: A \rightarrow A/J$. Proprietatea de universalitate a produsului direct induce morfismul de inele $\alpha: A \rightarrow A/I \times A/J$ care are nucleul $I \cap J$. Folosind teorema lui Noether de izomorfism avem $A/I \cap J \simeq A/I \times A/J \Leftrightarrow \alpha$ este surjectiv.

Dacă I și J sunt comaximale demonstrăm că α este surjectiv.

Pentru un element arbitrar $(a+I, b+J)$ din $A/I \times A/J$ considerăm $a-b \in A=I+J$. Dacă $i \in I$ și $j \in J$ a.î. $a-b = -i+j$ notăm prin $r = a+i = b+j$. Rezultă că $\alpha(r+(I \cap J)) = (a+I, b+J)$, adică α este surjectiv.

Reciproc, din faptul că α este surjectiv deducem că oricare ar fi $a, b \in A$ există $r \in A$ a.î. $a-r \in I$ și $b-r \in J$. Luând $b=0$ obținem $a = (a-r) + r \in I+J$, adică $A=I+J$.

8.48. Dacă $I \subseteq \prod_{i=1}^n A_i$ este un ideal stâng, atunci evident $I \subseteq \prod_{i=1}^n p_i(I)$.

Fie $x=(x_1, \dots, x_n) \in \prod_{i=1}^n p_i(I)$. Cum p_i sunt surjecțiile canonice $A \rightarrow A_i$, deducem că pentru orice $i \in \{1, \dots, n\}$ există un element $y^{(i)} \in I$, $y^{(i)} = (y_1^{(i)}, \dots, y_n^{(i)})$ cu $y_i^{(i)} = x_i$. Fie $z^{(i)} = (z_1^{(i)}, \dots, z_n^{(i)})$ elementul din A definit prin $z_j^{(i)} = \delta_{ij}$ ($i, j \in \{1, \dots, n\}$), unde δ_{ij} este simbolul lui Kronecker. Avem $x = \sum_{i=1}^n z^{(i)} y^{(i)}$. Deci $x \in I$ pentru că $\{y^{(i)}\}_i \in I$. În concluzie $I = \prod_{i=1}^n p_i(I)$.

Analog demonstrăm pentru cazul când I este ideal drept folosind egalitatea $x = \sum_{i=1}^n y^{(i)} z^{(i)}$. Se observă că subgrupul T al lui $\mathbb{Z} \times \mathbb{Z}$ format din elementele $\{(k, k) \mid k \in \mathbb{Z}\}$, nu poate fi ideal deoarece, de exemplu $T \neq \mathbb{Z} \times \mathbb{Z} = p_1(T) \times p_2(T)$.

8.49. Se aplică teorema fundamentală de izomorfism surjecției canonice $A \rightarrow \prod_{i=1}^n A_i / I_i$, definită prin $(x_1, \dots, x_n) \sim (\hat{x}_1, \dots, \hat{x}_n)$.

8.50. Dacă I și J sunt ideale în inelele comutative unitare A și B atunci $I \times J$ este ideal în $A \times B$.

Invers, dacă I este ideal în $A \times B$ notând cu p_A respectiv p_B proiecțiile canonice ale produsului direct, se demonstrează că $I = p_A(I) \times p_B(I)$, unde $p_A(I)$ este ideal în A iar $p_B(I)$ este ideal în B .

Orice corp necomutativ K are numai idealele $\{0\}$ și K . Atunci $\{0\} \times K$ și $K \times \{0\}$ sunt singurele ideale netriviale în $K \times K$. Idealele lui $\mathbb{Z} \times \mathbb{Z}$ sunt de forma $m\mathbb{Z} \times n\mathbb{Z}$, cu $m, n \in \mathbb{N}$.

8.51. Fie morfismul de inele $\varphi: A[X] \rightarrow S^{-1}A$ dat prin $\varphi(X) = a^{-1}$. Se demonstrează ușor că $\text{Ker}(\varphi) = (aX - 1)$ și apoi se aplică teorema fundamentală de izomorfism pentru inele.

8.52. Necesitatea este evidentă.

Folosind problema **8.42**, observăm că este suficient să arătăm că $x \neq 0$ implică $\mathbb{Z}[\sqrt{d}]/(t)$ finit (unde t este generatorul idealului $(x) \cap \mathbb{Z}$), deoarece $(t) \subseteq (x)$. Dar $x \neq 0$ implică $t \neq 0$ și evident $\mathbb{Z}[\sqrt{d}]/(t)$ are cel mult t^2 elemente.

8.53. Grupul $(\mathbb{Z}/4\mathbb{Z})^*$ are elementele $\{\bar{1}, \bar{3}\}$ și este izomorf cu subgrupul ciclic al lui \mathbb{Z} format de 1 și -1 (în raport cu înmulțirea).

Fie $f^*: (\mathbb{Z}/2^n\mathbb{Z})^* \rightarrow (\mathbb{Z}/4\mathbb{Z})^* \simeq \{\pm 1\}$, $n \geq 3$ componerea izomorfismului de mai sus cu morfismul surjectiv indus de surjecția canonică $\mathbb{Z}/2^n\mathbb{Z} \rightarrow \mathbb{Z}/4\mathbb{Z}$.

Avem $(\mathbb{Z}/2^n\mathbb{Z})^*/\text{Ker } f^* \simeq \{\pm 1\}$, f^* fiind surjectiv.

Deci $\text{Ker } f^*$ are ordinul 2^{n-2} întrucât $(\mathbb{Z}/2\mathbb{Z})^*$ are ordinul $\varphi(2^n) = 2^{n-1}$.

Observăm că $\hat{5}$, clasa lui 5 modulo 2^n , generează pe $\text{Ker } f^*$.

Într-adevăr, dacă k este ordinul lui $\hat{5}$, atunci $(1+4)^k \equiv 1 \pmod{2^n}$, adică $k + C_k^2 \cdot 4 + C_k^3 \cdot 4^2 + \dots + C_k^k \cdot 4^{k-1} \equiv 0 \pmod{2}$.

Folosim inducția pentru a arăta că $2^{n-2} | k$.

Evident $4 | k$ iar dacă $2^i | k$, $i < n-2$, atunci $2^{i-1} | C_k^2$, $2^{i-2} | C_k^3$, $2^{i-3} | C_k^4$, ... și

în concluzie $2^{i+1} | k$ în baza congruenței de mai sus.

Deci $\text{Ker } f^*$ are ordinul 2^{n-2} și $2^{n-2} | \text{ord } \hat{5}$.

Deducem că $\hat{5}$ generează pe $\text{Ker } f^*$ și astfel $\mathbb{Z}/2^{n-2}\mathbb{Z} \simeq \text{Ker } f^*$ (primul grup fiind aditiv).

Fie acum $u: (\mathbb{Z}/2^n\mathbb{Z})^* \rightarrow \{\pm 1\} \times \text{Ker } f^*$ morfismul de grupuri definit prin $u(\hat{x}) = (f^*(\hat{x}), f^*(\hat{x}) \cdot \hat{x})$. u este bine definit pentru că

$$f^*(f^*(\hat{x}) \cdot \hat{x}) = f^*(\hat{x}) \cdot f^*(\hat{x}) = 1 \text{ și deci } f^*(\hat{x}) \cdot \hat{x} \in \text{Ker } f^*.$$

În plus, dacă $u(\hat{x}) = (1, \hat{1})$ atunci $f^*(\hat{x}) \cdot \hat{x} = \hat{1}$ și $f^*(\hat{x}) = 1$. Deci $\hat{x} = \hat{1}$.

Rezultă că u este injectivă și grupurile având același ordin deducem că u este și bijectivă.

Deci $(\mathbb{Z}/2^n\mathbb{Z})^* \simeq \{\pm 1\} \times (\mathbb{Z}/2^{n-2}\mathbb{Z}) \simeq (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2^{n-1}\mathbb{Z})$, pentru $n \geq 3$.

8.54. Fie $f: \mathbb{Z}/p^n\mathbb{Z} \rightarrow \mathbb{Z}/p\mathbb{Z}$ morfismul surjectiv canonic și fie $f^*: (\mathbb{Z}/p^n\mathbb{Z})^* \rightarrow (\mathbb{Z}/p\mathbb{Z})^*$ morfismul de grupuri indus de f . Observăm că f^* este surjectiv. Într-adevăr, dacă $x \in \mathbb{Z}$ are clasa modulo p inversabilă în $\mathbb{Z}/p\mathbb{Z}$ atunci $p \nmid x$, de unde rezultă că $(x, p^n) \simeq 1$. Deci clasa modulo p^n a lui x este inversabilă în $\mathbb{Z}/p^n\mathbb{Z}$ și imaginea ei prin f^* este clasa modulo p a lui x .

Pe de altă parte, ordinul grupului $(\mathbb{Z}/p^n\mathbb{Z})^*$ este $\varphi(p^n) = p^{n-1}(p-1)$ și $\text{Ker } f^*$ are indicele $p-1$ în $(\mathbb{Z}/p^n\mathbb{Z})^*$. Deducem că $\text{Ker } f^*$ are ordinul p^{n-1} . Am folosit aici faptul că $(\mathbb{Z}/p\mathbb{Z})^*/\text{Ker } f^* \simeq (\mathbb{Z}/p\mathbb{Z})^*$, f^* fiind surjectivă.

Avem $(\mathbb{Z}/p^n\mathbb{Z})^* \simeq \text{Ker } f^* \times (\mathbb{Z}/p\mathbb{Z})^*$, deoarece ordinele grupurilor $\text{Ker } f^*$ și $(\mathbb{Z}/p\mathbb{Z})^*$ sunt prime între ele.

Grupul $\text{Ker } f^*$ este ciclic generat de clasa lui $1+p$ modulo p^n .

Într-adevăr, dacă $(p+1)^k \equiv 1$ modulo p^n , deducem

$$k \cdot p + C_k^2 \cdot p^2 + C_k^3 \cdot p^3 + \dots + C_k^k \cdot p^k \equiv 0, \text{ modulo } p^n.$$

Deci $p|k$ și cum $p \neq 2$ rezultă că $p|C_k^2$, de unde obținem că $p^2|k$.

Aplicăm inducția. Dacă avem $p^i|k$, pentru un $i < n-1$, atunci $p^i|C_k^2$, $p^{i-1}|C_k^3$ (dacă $p \neq 3$ am fi dedus chiar $p^i|C_k^3$), ..., $p^{i-j}|C_k^{j+2}$ pentru $j < i$. Din

aceeași congruență de mai sus rezultă $p^{i+1}|k$. Am arătat că $p^{n-1}|k$. Cum \bigwedge

în $\text{Ker } f^*$, care are ordinul p^{n-1} , deducem că \bigwedge $1+p$ este un generator al lui $\text{Ker } f^*$.

Deci $(\mathbb{Z}/p^n\mathbb{Z})^* \simeq \mathbb{Z}/p^{n-1}\mathbb{Z} \times \mathbb{Z}/(p-1)\mathbb{Z} \simeq \mathbb{Z}/p^{n-1}(p-1)\mathbb{Z}$, $(\mathbb{Z}/p\mathbb{Z})^*$ fiind ciclic.

§9. Corp. Subcorp. Caracteristica unui corp. Morfisme de corpuri. Izomorfisme de corpuri.

9.1. În inelul \mathbb{Z}_n , \hat{a} este inversabil dacă și numai dacă $(a, n)=1$.

„ \Rightarrow ”. Dacă n este prim, atunci $1, \dots, n-1$ sunt relativ prime cu n și atunci toate elementele nenule ale inelului \mathbb{Z}_n sunt inversabile, deci \mathbb{Z}_n este corp.

„ \Leftarrow ”. Dacă \mathbb{Z}_n este corp atunci toate elementele nenule sunt inversabile, deci $(i, n)=1$, pentru orice $i \in \{1, \dots, n-1\}$, adică în particular avem că numărul natural n nu este divizibil prin nici un număr prim $p \leq \sqrt{n}$, deci n este prim.

9.2. Din prima ecuație avem $y=-x$ și înlocuind în a doua ecuație obținem $-x^2 = \hat{5}$, adică $x^2 = \hat{2}$. Ecuația $x^2 = \hat{2}$ are în corpul \mathbb{Z}_7 două soluții: $x_1 = \hat{3}$ și $x_2 = \hat{4}$. Corespunzător obținem: $y_1 = -x_1 = \hat{4}$ respectiv $y_2 = -x_2 = \hat{3}$.

Soluțiile sistemului sunt: $\begin{cases} x_1 = \hat{3} \\ y_1 = \hat{4} \end{cases}$ și $\begin{cases} x_2 = \hat{4} \\ y_2 = \hat{3} \end{cases}$.

9.3. Fie A un inel integru finit și $a \in A$, $a \neq 0$. Definim $\varphi_a: A \rightarrow A$ prin $\varphi_a(x) = ax$, oricare ar fi $x \in A$. Deoarece A este integru rezultă că φ_a este injectivă și cum A este finit este și surjectivă. Există deci $a' \in A$ a.î. $\varphi_a(a') = 1$, adică $aa' = 1$. Avem $a' \neq 0$ și există $a'' \in A$ a.î. $\varphi_{a'}(a'') = 1$, adică $a'a'' = 1$.

Atunci $a = a \cdot 1 = a(a'a'') = (aa')a'' = 1 \cdot a'' = a''$. Deci și $a'a = 1$. În consecință a este inversabil și a' este inversul său.

9.4. Fie I un ideal la stânga în corpul K .

Dacă $I \neq (0)$, atunci există în I un element nenul a , deci $1 = a \cdot a^{-1} \in I$. Dacă b este un element arbitrar din K , atunci din egalitatea $b = b \cdot 1$ obținem că $b \in I$, deci I conține toate elementele lui K , adică $I = K$.

În mod analog se arată că orice ideal drept coincide cu (0) sau K . Deci singurele ideale bilaterale în K sunt (0) și K .

9.5. Pentru a demonstra că K este corp trebuie să arătăm că orice element nenul din K este inversabil. Fie $x \in K, x \neq 0$. Deoarece idealele xK și Kx sunt nenule, deducem că $xK = Kx = K$. Deci există x' și $x'' \in K$ a.î. $xx' = 1$ și $x''x = 1$. Atunci obținem $x' = 1 \cdot x' = (x''x)x' = x''(xx') = x'' \cdot 1 = x''$, deci $x' = x''$ și deci x este inversabil.

9.6. (i). Se verifică axiomele grupului comutativ (K, \oplus) . Elementul neutru la \oplus este 1 iar inversul lui x este $\frac{1}{x}$. (K, \odot) este monoid comutativ, elementul unitate fiind e . Pentru a arăta comutativitatea operației \odot observăm că:

$$x \odot y = x^{\ln y} = e^{\ln x^{\ln y}} = e^{\ln x \cdot \ln y} = e^{\ln y \cdot \ln x} = y^{\ln x} = y \odot x.$$

Orice element x diferit de 1 este inversabil, iar $x^{-1} = e^{1/\ln x}$.

(ii). Definim $f: (K, \oplus, \odot) \rightarrow (\mathbb{R}, +, \cdot)$, $f(x) = \ln x$ și demonstrăm că f este un izomorfism de corpuri:

$$f(x \oplus y) = \ln(x \oplus y) = \ln(xy) = \ln(x) + \ln(y) = f(x) + f(y),$$

$$f(x \odot y) = \ln(x \odot y) = \ln(x^{\ln y}) = \ln(y) \cdot \ln(x) = f(x) \cdot f(y),$$

oricare ar fi $x, y \in K$, $f(e) = \ln(e) = 1$. Evident, f este funcție bijectivă.

9.7. Definim $x \otimes 0 = 0 \otimes x = 0$, oricare ar fi $x \in \mathbb{Q}$ și în felul acesta operația \otimes se prelungește de la \mathbb{Q}^* la \mathbb{Q} . Să notăm cu e elementul neutru față de operația \otimes , adică elementul unitate al inelului $(\mathbb{Q}, +, \otimes)$. Mai notăm $e\mathbb{Z} = \{ke \mid k \in \mathbb{Z}\}$, adică subgrupul ciclic generat de elementul e în grupul aditiv $(\mathbb{Q}, +)$. Datorită distributivității operației \otimes față de adunarea $+$, rezultă ușor că $ne \otimes me = nm(e \otimes e) = nme$, oricare ar fi $n, m \in \mathbb{N}$ și datorită regulilor de calcul

$(-x) \otimes y = x \otimes (-y) = -x \otimes y$, $(-x) \otimes (-y) = x \otimes y$, valabile pentru orice $x, y \in (\mathbb{Q}, +, \otimes)$ rezultă:

$$n \otimes m = nm, \text{ oricare ar fi } n, m \in \mathbb{Z} \quad (1).$$

Din această ultimă egalitate, deducem că $(e\mathbb{Z}, +, \otimes)$ este un inel, de fapt un subinel al inelului $(\mathbb{Q}, +, \otimes)$. Aplicația $f: (\mathbb{Z}, +, \cdot) \rightarrow (e\mathbb{Z}, +, \otimes)$, $f(n) = ne$ este un izomorfism de inele, ceea ce se probează ușor pe baza lui (1). Cum $(\mathbb{Z}, +, \cdot)$ este domeniu de integritate, rezultă că și $(\mathbb{Z}, +, \otimes)$ este domeniu de integritate și atunci are un corp de fracții, care este tocmai $(\mathbb{Q}, +, \otimes)$. Așadar, $(\mathbb{Q}, +, \otimes)$ este un corp.

9.8. (i). Fie K corpul căutat. Fiind de caracteristică zero, el va conține un subcorp izomorf cu \mathbb{Q} . Putem considera că $\mathbb{Q} \subset K$, deci $a \in K$ pentru orice $a \in \mathbb{Q}$. De asemenea, deoarece $\sqrt{2} \in K$ rezultă că $b\sqrt{2} \in K$, pentru orice $b \in \mathbb{Q}$. Așadar orice număr de forma $a + b\sqrt{2}$ cu a, b numere raționale este în K .

Acum este suficient să arătăm că numerele de forma $a + b\sqrt{2}$ formează un subcorp al lui \mathbb{R} . Evident, ele formează un subinel al lui \mathbb{R} ; rămâne de demonstrat că orice element de această formă, nenul, are inversul (în \mathbb{R}) tot de această formă. Se arată imediat că $a + b\sqrt{2} = 0$ dacă și numai dacă $a^2 - 2b^2 = 0$ adică, dacă și numai dacă $a = b = 0$ iar dacă $a + b\sqrt{2} \neq 0$ atunci $(a + b\sqrt{2})^{-1} = c + d\sqrt{2}$ cu $c = \frac{a}{a^2 - 2b^2}$, $d = \frac{-b}{a^2 - 2b^2}$ raționale.

(ii). Se verifică imediat că F este subinel al lui \mathbb{R} .

Într-adevăr dacă $x, y \in F$, $x = a + b\sqrt[3]{2} + c\sqrt[3]{4}$ și $y = a' + b'\sqrt[3]{2} + c'\sqrt[3]{4}$ cu $a, b, c, a', b', c' \in \mathbb{Q}$ atunci:

$$x - y = (a + b\sqrt[3]{2} + c\sqrt[3]{4}) - (a' + b'\sqrt[3]{2} + c'\sqrt[3]{4}) = (a - a') + (b - b')\sqrt[3]{2} + (c - c')\sqrt[3]{4} \in \mathbb{Q}(\sqrt[3]{2}),$$

$$xy = (a + b\sqrt[3]{2} + c\sqrt[3]{4})(a' + b'\sqrt[3]{2} + c'\sqrt[3]{4}) = (aa' + 2bc' + 2cb') + (ab' + a'b + 2cc')\sqrt[3]{2} + (ac' + a'c + bb')\sqrt[3]{4} \in \mathbb{Q}(\sqrt[3]{2}).$$

Evident, $1 \in \mathbb{Q}(\sqrt[3]{2})$.

Arătăm că $a + b\sqrt[3]{2} + c\sqrt[3]{4} = 0$ (*) dacă și numai dacă $a = b = c = 0$.

Scriem egalitatea $a + b\sqrt[3]{2} + c\sqrt[3]{4} = 0$ sub forma $b\sqrt[3]{2} + c\sqrt[3]{4} = -a$.

Înmulțind ambii membri ai lui (*) cu $\sqrt[3]{2}$ obținem: $a\sqrt[3]{2} + b\sqrt[3]{4} = -2c$, de unde sistemul:

$$(S) \begin{cases} b\sqrt[3]{2} + c\sqrt[3]{4} = -a \\ a\sqrt[3]{2} + b\sqrt[3]{4} = -2c \end{cases} . \text{Înmulțind prima ecuație a sistemului (S) cu } -b \text{ și}$$

pe a doua cu c obținem:
$$\begin{cases} -b^2\sqrt[3]{2} - bc\sqrt[3]{4} = ba \\ ac\sqrt[3]{2} + bc\sqrt[3]{4} = -2c^2 \end{cases}$$
 și prin adunare

$(ac-b^2)\sqrt[3]{2} = ab-2c^2$, de unde $ac=b^2$ și $ab=2c^2$. Atunci $abc=2c^3$, adică $b^3=2c^3$, de unde $b=c=0$ (căci în caz contrar am deduce că $\sqrt[3]{2} = \frac{b}{c} \in \mathbb{Q}$, absurd). Rezultă

imediat că și $a=0$. Demonstrăm că orice element nenul din $\mathbb{Q}(\sqrt[3]{2})$ este inversabil în $\mathbb{Q}(\sqrt[3]{2})$, adică dacă $\alpha \in \mathbb{Q}(\sqrt[3]{2})$, $\alpha \neq 0$, atunci și $\alpha^{-1} \in \mathbb{Q}(\sqrt[3]{2})$.

Dacă $\alpha = a + b\sqrt[3]{2} + c\sqrt[3]{4}$, cu $a, b, c \in \mathbb{Q}$, $\alpha \neq 0$, (echivalent deci cu $a^2 + b^2 + c^2 \neq 0$) trebuie să găsim $\beta = a' + b'\sqrt[3]{2} + c'\sqrt[3]{4}$ cu $a', b', c' \in \mathbb{Q}$, $a'^2 + b'^2 + c'^2 \neq 0$ a.f. $\alpha \cdot \beta = 1$.

Folosind calculul anterior

$$\alpha \cdot \beta = (aa' + 2bc' + 2cb') + (ab' + a'b + 2cc')\sqrt[3]{2} + (ac' + a'c + bb')\sqrt[3]{4} .$$

Cum $\alpha \cdot \beta = 1$, trebuie să arătăm că următorul sistem liniar

$$(S') \begin{cases} aa' + 2bc' + 2cb' = 1 \\ ab' + a'b + 2cc' = 0 \\ ac' + bb' + a'c = 0 \end{cases} \text{ în necunoscutele } a', b', c' \text{ are o soluție}$$

rațională. Înmulțind ecuațiile sistemului (S') cu un multiplu comun diferit de zero al numitorilor numerelor raționale a, b, c putem presupune că $a, b, c \in \mathbb{Z}$, nu toate nule. Determinantul sistemului (S') este

$$\Delta = \begin{vmatrix} a & 2c & 2b \\ b & a & 2c \\ c & b & a \end{vmatrix} = a^3 + 2b^3 + 4c^3 - 6abc .$$

Presupunem prin reducere la absurd că $\Delta = 0$.

Atunci $a^3 + 2b^3 + 4c^3 - 6abc = 0$. Putem presupune că nu toate numerele a, b, c sunt pare căci altfel $0 = \Delta = 8(a_1^3 + 2b_1^3 + 4c_1^3 - 6a_1b_1c_1)$ unde $a = 2a_1$, $b = 2b_1$, $c = 2c_1$ deci $a_1^3 + 2b_1^3 + 4c_1^3 - 6a_1b_1c_1 = 0$ și nu toate a_1, b_1, c_1 sunt nule. Din $\Delta = 0$ rezultă că $2|a$ deci $a = 2a_0$, $a_0 \in \mathbb{Z}$. Înlocuindu-l pe a obținem $4a_0^3 + b^3 + 2c^3 - 6a_0bc = 0$, ceea ce implică $2|b$, contradicție căci ar trebui și $2|c$.

Deci $\Delta \neq 0$. Atunci (S') este sistem Cramer și are soluție unică.

9.9. Fie φ , e respectiv elementul nul și elementul unitate din inelul A . Pentru fiecare $x \in (0, 1)$ vom avea $x + \varphi = x$ respectiv $x e = x$, de unde rezultă $\varphi = 0$ respectiv $e = 1$. Deoarece $1 \in A$ rezultă $\mathbb{Z} \subseteq A$.

Arătăm că $\mathbb{R} \subseteq A$. Fie, într-adevăr, $x \in \mathbb{R}$ arbitrar. Avem $x = [x] + \{x\}$ și cum $[x] \in \mathbb{Z} \subseteq A$, iar $\{x\} \in [0, 1) \subseteq A$, rezultă $x \in A$, deci $\mathbb{R} \subseteq A$.

Avem de analizat două cazuri, după cum $A \subseteq \mathbb{R}$, respectiv $A \not\subseteq \mathbb{R}$.

i) $A \subseteq \mathbb{R}$. Deoarece am arătat că $\mathbb{R} \subseteq A$, rezultă $A = \mathbb{R}$.

ii) $A \not\subseteq \mathbb{R}$. Fie $z_0 = a_0 + ib_0 \in A \setminus \mathbb{R}$, unde $a_0, b_0 \in \mathbb{R}$, $b_0 \neq 0$. Deoarece $z_0, a_0 \in A$ rezultă $z_0 - a_0 \in A$, adică $ib_0 \in A$. Cum $\frac{1}{b_0} \in \mathbb{R} \subseteq A$ rezultă $\frac{1}{b_0} \cdot (ib_0) \in A$, adică $i \in A$. Atunci luând $z = a + ib \in \mathbb{C}$ avem $a, b \in \mathbb{R} \subseteq A$ și $i \in A$, deci $z \in A$. Așadar $\mathbb{C} \subseteq A$ și cum $A \subseteq \mathbb{C}$, rezultă $A = \mathbb{C}$.

9.10. (i). $\mathbb{Q}(\sqrt{d_1}) \cap \mathbb{Q}(\sqrt{d_2})$ este intersecția a două corpuri deci va fi tot un corp ce include în mod evident corpul \mathbb{Q} . Avem extinderile de corpuri:

$$\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{d_1}) \cap \mathbb{Q}(\sqrt{d_2}) \subseteq \mathbb{Q}(\sqrt{d_1}).$$

Relația asupra gradelor se scrie:

$$\begin{aligned} 2 &= [\mathbb{Q}(\sqrt{d_1}) : \mathbb{Q}] \\ &= [(\mathbb{Q}(\sqrt{d_1}) \cap \mathbb{Q}(\sqrt{d_2})) : \mathbb{Q}] \cdot [\mathbb{Q}(\sqrt{d_1}) : (\mathbb{Q}(\sqrt{d_1}) \cap \mathbb{Q}(\sqrt{d_2}))]. \end{aligned}$$

Rezultă $[(\mathbb{Q}(\sqrt{d_1}) \cap \mathbb{Q}(\sqrt{d_2})) : \mathbb{Q}] \in \{1, 2\}$.

Dacă am avea $[(\mathbb{Q}(\sqrt{d_1}) \cap \mathbb{Q}(\sqrt{d_2})) : \mathbb{Q}] = 2$, atunci ar rezulta egalitatea $\mathbb{Q}(\sqrt{d_1}) \cap \mathbb{Q}(\sqrt{d_2}) = \mathbb{Q}(\sqrt{d_1})$. În particular, am avea $\sqrt{d_2} \in \mathbb{Q}(\sqrt{d_1})$, adică $\sqrt{d_2} = \alpha + \beta\sqrt{d_1}$, $\alpha, \beta \in \mathbb{Q}$. Dacă $\beta = 0$, atunci $\sqrt{d_2} = \alpha \in \mathbb{Q}$, contradicție. Dacă $\alpha = 0$, atunci $\sqrt{\frac{d_2}{d_1}} = \beta \in \mathbb{Q}$, contradicție. Deci $\alpha \neq 0$, $\beta \neq 0$ și ridicând la pătrat obținem $d_2 = \alpha^2 + \beta^2 d_1 + 2\alpha\beta\sqrt{d_1}$, de unde $\sqrt{d_1} = \frac{d_2 - \alpha^2 - \beta^2 d_1}{2\alpha\beta} \in \mathbb{Q}$, contradicție.

Rămâne drept unică posibilitate $[(\mathbb{Q}(\sqrt{d_1}) \cap \mathbb{Q}(\sqrt{d_2})) : \mathbb{Q}] = 1$, adică egalitatea: $\mathbb{Q}(\sqrt{d_1}) \cap \mathbb{Q}(\sqrt{d_2}) = \mathbb{Q}$.

(ii). Evident, $\mathbb{Z} \subseteq \mathbb{Z}[\sqrt{d_1}] \cap \mathbb{Z}[\sqrt{d_2}]$, căci \mathbb{Z} este inclus în fiecare dintre cele două inele.

Deoarece $\mathbb{Z}[\sqrt{d_1}] \subseteq \mathbb{Q}(\sqrt{d_1})$ și $\mathbb{Z}[\sqrt{d_2}] \subseteq \mathbb{Q}(\sqrt{d_2})$ vom avea:

$$\mathbb{Z}[\sqrt{d_1}] \cap \mathbb{Z}[\sqrt{d_2}] \subseteq \mathbb{Q}(\sqrt{d_1}) \cap \mathbb{Q}(\sqrt{d_2}) = \mathbb{Q}.$$

Pe de altă parte, $\mathbb{Z}[\sqrt{d_1}] \cap \mathbb{Z}[\sqrt{d_2}] \subseteq \mathbb{Z}[\sqrt{d_1}]$ deci

$$\mathbb{Z}[\sqrt{d_1}] \cap \mathbb{Z}[\sqrt{d_2}] \subseteq \mathbb{Q} \cap \mathbb{Z}[\sqrt{d_1}] = \mathbb{Z}, \text{ adică } \mathbb{Z}[\sqrt{d_1}] \cap \mathbb{Z}[\sqrt{d_2}] \subseteq \mathbb{Z}.$$

Așadar $\mathbb{Z}[\sqrt{d_1}] \cap \mathbb{Z}[\sqrt{d_2}] = \mathbb{Z}$.

9.11. Deoarece K este corp rezultă că $\mathbb{Q} \subset K$.

În ipoteza (ii) cu $a=1$ rezultă $\sqrt{3} \in K$.

În ipoteza (i) cu $a=1$ rezultă $\sqrt{2} \in K$ și apoi cu $a=\sqrt{2}$ rezultă $\sqrt{3} \in K$.

În orice corp K , $a \in K$ implică în condițiile ipotezei (ii) că

$$a^2 + a + 1 = \left(a + \frac{1}{2}\right)^2 + \frac{3}{4} = \left(\frac{\sqrt{3}}{2}\right)^2 \left\{ \left[\frac{2}{\sqrt{3}} \left(a + \frac{1}{2}\right) \right]^2 + 1 \right\}.$$

Evident funcția $f: K \rightarrow K$, $f(a) = \frac{2}{\sqrt{3}} \left(a + \frac{1}{2}\right)$ este bijectivă. De asemenea,

$$\text{putem scrie: } a^2 + 1 = \left(\frac{2}{\sqrt{3}}\right)^2 \left[\left(\frac{\sqrt{3}}{2}a - \frac{1}{2}\right)^2 + \left(\frac{\sqrt{3}}{2}a - \frac{1}{2}\right) + 1 \right], \text{ oricare ar fi } a \in K.$$

Deci (i) \Leftrightarrow (ii).

Ca exemplu de corp pentru care una din afirmațiile (i) sau (ii) este adevărată putem lua $K = \mathbb{R}$.

9.12. Notăm cu \mathbb{P} mulțimea numerelor prime. Pentru $P \subseteq \mathbb{P}$ considerăm

$$A(P) = \left\{ \frac{m}{n} \in \mathbb{Q} \mid p|n \Rightarrow p \in P \right\}, \text{ adică toate fracțiile (ireductibile) } \frac{m}{n} \text{ a.î.}$$

divizorii primi ai lui n sunt doar din P .

Pentru un subinel A unitar al lui \mathbb{Q} considerăm $P(A)$ mulțimea tuturor divizorilor primi ai numitorilor tuturor fracțiilor (ireductibile) din A .

Vom arăta că aceste două corespondențe sunt una inversa celeilalte (adică, $A(P(A)) = A$ și $P(A(P)) = P$), adică există o bijecție între mulțimea tuturor subinelor unitare ale lui \mathbb{Q} și $P(\mathbb{P})$ mulțimea tuturor submulțimilor finite sau infinite de numere prime.

Toate fracțiile sunt presupuse ireductibile.

Dacă un subinel unitar conține $\frac{m}{n}$ trebuie de asemenea să conțină $\frac{1}{n}$.

Într-adevăr, dacă $(m, n)=1$ atunci $um+vn=1$ are loc pentru $u, v \in \mathbb{Z}$.
 Rezultă $\frac{1}{n} = \frac{um+vn}{n} = u \cdot \frac{m}{n} + v \cdot 1$. Deci $\mathbb{Z} = \langle 1 \rangle$, evident cel mai mic subinel unitar al lui \mathbb{Q} .

În final $P(A(P))=P$ și $A \subseteq A(P(A))$ sunt evidente, conform definiției anterioare. Pentru a demonstra că $A(P(A)) \subseteq A$, fie $\alpha = \frac{m}{p_1^{r_1} \cdots p_k^{r_k}} \in A(P(A))$.

Pentru $p_1 \in P(A)$, există o fracție $\frac{s}{p_1^{e_1} \cdot t} \in A$ și cu remarca de mai sus $\frac{1}{p_1} \in A$.

Analog $\frac{1}{p_2} \in A, \dots, \frac{1}{p_k} \in A$, adică $\alpha \in A$.

Observație. Dacă $P = \{p_1, \dots, p_k\}$ este mulțime finită atunci $P(A)$ este subinelul generat de $\frac{1}{p_1 \cdots p_k}$.

9.13. Dacă în egalitatea $a^n b^n - b^{n+1} a^{n+1} = 1$ înmulțim la dreapta cu a^n obținem:

$$a^n b^n a^n - b^{n+1} a^{2n+1} = a^n \quad (1)$$

Din ipoteză avem $a^{2n+1} = -b^{2n+1}$ și înmulțind cu b^{n+1} mai întâi la stânga și apoi la dreapta obținem respectiv:

$$b^{n+1} a^{2n+1} = -b^{3n+2} \quad (2)$$

$$a^{2n+1} b^{n+1} = -b^{3n+2} \quad (3)$$

Din (2) și (3) rezultă că $b^{n+1} a^{2n+1} = a^{2n+1} b^{n+1}$ (4).

Din (1) și (4) rezultă $a^n b^n a^n - a^{2n+1} b^{n+1} = a^n$ și înmulțind la stânga cu a^n rezultă $b^n a^n - a^{n+1} b^{n+1} = 1$, adică egalitatea cerută.

9.14. Deoarece $K \subset K(x)$ și $ax+b \in K(x)$ rezultă $K(ax+b) \subset K(x)$. Pentru a stabili și incluziunea inversă observăm că $x = a^{-1}(ax+b) - a^{-1}b \in K(ax+b)$.

9.15. (i). Cum ordinul lui 1 în grupul $(A, +)$ este n , elementele $0, 1, 2 \cdot 1, \dots, (n-1) \cdot 1$ sunt distincte și $n \cdot 1 = 0$. Avem $A = \{0, 1, 2 \cdot 1, \dots, (n-1) \cdot 1\}$. Așadar, dacă $x \in A$, atunci x se reprezintă în mod unic sub forma $x = i \cdot 1, 0 \leq i < n$. Definim $f: A \rightarrow \mathbb{Z}_n, f(i \cdot 1) = \hat{i} \Leftrightarrow x = i \cdot 1, 0 \leq i < n$. Evident f este aplicație bijectivă. Fie $x, y \in A, x = i \cdot 1, y = j \cdot 1, 0 \leq i, j < n$. Atunci:

$$x+y = i \cdot 1 + j \cdot 1 = (i+j) \cdot 1 = (i \oplus j) \cdot 1,$$

$$xy = (i \cdot 1)(j \cdot 1) = (ij) \cdot 1 = (i \otimes j) \cdot 1,$$

unde \oplus și \otimes sunt simbolurile adunării respectiv înmulțirii modulo n .

Rezultă că:

$$f(x+y) = i \hat{\oplus} j = \hat{i} + \hat{j} = f(x) + f(y), \quad f(xy) = i \hat{\otimes} j = \hat{ij} = f(x)f(y),$$

deci f este izomorfism de inele.

(ii). Cum $|A| = p > 1$, rezultă că $0 \neq 1$. Deci ordinul elementului 1 în grupul $(A, +)$ este egal cu p și $A = \{0, 1, 1+1, \dots, (p-1) \cdot 1\}$. Conform punctului (i), rezultă că $(A, +, \cdot) \simeq (\mathbb{Z}_p, +, \cdot)$. Cum \mathbb{Z}_p este corp comutativ și $(A, +, \cdot) \simeq (\mathbb{Z}_p, +, \cdot)$, rezultă că și A este corp comutativ.

9.16. (i). Pentru orice $x \in A$ avem $x+x=0$.

Într-adevăr, $x+x = 1 \cdot x + 1 \cdot x = (1+1) \cdot x = 0 \cdot x = 0$. Deducem că $x = -x$, oricare ar fi $x \in A$.

$$\begin{aligned} \text{Avem:} \quad x^7 + 1 &= x^7 - 1 = (x-1)(x^6 + x^5 + x^4 + x^3 + x^2 + x + 1) \\ &= (x+1)[(x^6 + x^4 + x^3) + (x^5 + x^3 + x^2) + (x^3 + x + 1)] \\ &= (x+1)[x^3(x^3 + x + 1) + x^2(x^3 + x + 1) + (x^3 + x + 1)] \\ &= (x+1)(x^3 + x^2 + 1)(x^3 + x + 1). \end{aligned}$$

(ii). Presupunem că A este corp și fie $A^* = A \setminus \{0\}$. Atunci (A^*, \cdot) este un grup cu 7 elemente. Fie $a \in A^*$, $a \neq 1$. Avem $a^7 = 1$, deci $(a+1)(a^3 + a^2 + 1)(a^3 + a + 1) = 0$.

Cum A este corp și $a \neq 1$, deducem că $a^3 + a + 1 = 0$ sau că $a^3 + a^2 + 1 = 0$. Dacă $a^3 + a^2 + 1 = 0$, atunci $(1+a)^3 + (1+a) + 1 = 1 + 3a + 3a^2 + a^3 + 1 + a + 1 = a^3 + a^2 + 1 = 0$ și din nou avem proprietatea cerută cu $1+a$ în loc de a .

Reciproc, fie $a \in A$ a.î. $a^3 + a + 1 = 0$. Cum $1 \neq 0$, se deduce că $a \neq 0$ și $a \neq 1$. Din (i) rezultă că $a^7 = 1$, deci a este element inversabil al inelului A . Cum $a \neq 1$ și $a^7 = 1$, rezultă că a este un element de ordin 7 al grupului unităților inelului A . Așadar A are cel puțin 7 elemente inversabile, anume $1, a, a^2, a^3, a^4, a^5, a^6$. Cum $|A| = 8$, rezultă că orice element diferit de 0 al lui A este inversabil, deci A este corp.

9.17. (i) \Rightarrow (ii). Fie $a \in A \setminus \{0, 1\}$ neinversabil și $B = \{a^k \mid k \in \mathbb{N}^*\}$. Evident $1 \notin B$ și B este finită. Distingem cazurile:

1) $0 \in B$. Atunci există $s \in \mathbb{N}^*$ cu $a^s \neq 0$ și $a^{s+1} = 0$. Fie $x_0 = a^s$, $y_0 = 1 - a^s \neq 0$. Cum $x_0 + y_0 = 1$ rezultă că ecuația $x + y = z$ are soluții în A^* .

Dacă $n \geq 2$ atunci $x_0^n = 0$ și cum $x_0^n + x_0^n = x_0^n$ rezultă că ecuația $x^n + y^n = z^n$ are soluția $(x_0, x_0, x_0) \in (A^*)^3$.

2) $0 \notin B$. Cum B este finită există $i > j \geq 1$ cu $a^i = a^j$. Dacă $i = j + p$ cu $p \in \mathbb{N}^*$ atunci $a^j(a^p - 1) = 0 = (a^p - 1)a^j$. Fie $x_0 = a^j$ și $y_0 = a^p - 1$.

Cum $0, 1 \notin B$ rezultă că $x_0, y_0 \neq 0$. Dacă $z_0 = x_0 + y_0 = a^j + a^p - 1$ rezultă $z_0 \neq 0$ (în caz contrar, rezultă că $a^j + a^p = 1 \Leftrightarrow a(a^{j-1} + a^{p-1}) = 1$, deci a este inversabil, fals).

Cum $x_0 y_0 = y_0 x_0 = 0$, rezultă că pentru orice $n \in \mathbb{N}^*$ avem:

$$z_0^n = (x_0 + y_0)^n = x_0^n + \sum_{k=1}^{n-1} C_n^k x_0^{n-k} y_0^k + y_0^n = x_0^n + y_0^n,$$

deci ecuația $x^n + y^n = z^n$ are soluția $(x_0, y_0, z_0) \in (A^*)^3$.

(ii) \Rightarrow (i). Presupunem că A este corp. Fie $q = |A|$ (numărul elementelor lui A) Cum $q \geq 2$ atunci există $x_0, y_0, z_0 \in A^*$ cu $x_0^{q-1} + y_0^{q-1} = z_0^{q-1}$. Deci $1 + 1 = 1$, de unde $1 = 0$, absurd.

9.18. Grupul (K^*, \cdot) are 7 elemente, deci pentru orice $x \in K^*$ avem $x^7 = 1$. Rezultă că polinomul $f(X) = X^8 - X$ are ca rădăcini toate elementele lui K . Deoarece K este corp comutativ, f are 8 factori de gradul întâi. Considerăm $g(X) = X^3 - X - 1$; Se verifică ușor că $f(X) = g(X) \cdot (X^5 + X^3 + X^2 + X)$, deoarece $-1 = 1$ în K . Atunci g conține 3 factori liniari ai lui f , deci are rădăcini în K . Dacă $a \in K$ este o rădăcină a lui g , atunci $a^3 = a + 1$.

9.19. (i) \Rightarrow (ii). Considerăm K corp. Cum $|K| = 4$ rezultă că ordinul lui 1 în grupul $(K, +)$ poate fi 2 sau 4, deci $\text{car}(K) = 2$ sau $\text{car}(K) = 4$.

Dacă $\text{car}(K) = 4$ atunci $1 + 1 \neq 0$ și $1 + 1 + 1 + 1 = 0$, de unde $(1 + 1)(1 + 1) = 1 + 1 + 1 + 1 = 0$, contradicție, căci un corp nu are divizori ai lui zero. Așadar $1 + 1 = 0$ și avem $x + x = 1 \cdot x + 1 \cdot x = (1 + 1)x = 0 \cdot x = 0$, oricare ar fi $x \in K$.

Fie $K^* = K \setminus \{0\}$. (K^*, \cdot) este grup și $|K^*| = 3$.

Fie $a \in K^*$, $a \neq 1$. Atunci $a^3 = 1$.

Avem $0 = a^3 + 1 = (a + 1)(a^2 - a + 1) = (a + 1)(a^2 + a + 1)$ și cum $a + 1 \neq 0$ iar K este corp, rezultă $a^2 + a + 1 = 0$, deci $a^2 = a + 1$.

(ii)⇒(i). Presupunem că există $a \in K$ a.î. $a^2 = a + 1$. Atunci $a \neq 0$ și $a \neq 1$ căci în caz contrar $1 = 0$, contradicție.

Presupunem că $\text{car}(K) = 4$. Atunci $K = \{0, 1, 1+1, 1+1+1\}$. Cum $a \neq 0$ și $a \neq 1$, rezultă că $a = 1+1$ sau $a = 1+1+1$.

Dacă $a = 1+1$ atunci din $a^2 = a + 1$ deducem că $(1+1)^2 = 1 + (1+1) \Leftrightarrow 1+1+1+1 = 1+1+1$ rezultă $1 = 0$, contradicție.

De asemenea, dacă $a = 1+1+1$, din $a^2 = a + 1$ rezultă $1 = 0$, contradicție.

Ambele cazuri sunt imposibile, deci $\text{car}(K) = 2$. Așadar K este inel de tipul 2) (vezi problema 6.73.).

Cum $(1+a)a = a + a^2 = a + 1 + a = (a+a) + 1 = 0 + 1 = 1$ și $a(1+a) = a + a^2 = 1$, în mod analog, rezultă că toate elementele diferite de zero ale lui K sunt inversabile, deci K este corp.

9.20. (i). Cum $E \neq O$ și $E + E = O$, rezultă că E este element de ordin 2 al grupului $(M_3(\mathbb{Z}_2), +)$. Rezultă că elementul unitate al inelului $M_3(\mathbb{Z}_2)$ are ordinul aditiv egal cu 2, deci $M_3(\mathbb{Z}_2)$ este inel de caracteristică 2.

(ii). O verificare directă arată că $U^3 + U + E = O$. Cum $E + E = O$, se deduce că: $X + X = O$, $X^7 + E = (X + E)(X^3 + X^2 + E)(X^3 + X + E)$, oricare ar fi $X \in M_3(\mathbb{Z}_2)$.

Acum din $U^3 + U + E = O$ rezultă $U^7 = E$ și cum $U \neq E$, deducem că U este element de ordin 7 al grupului unităților inelului $M_3(\mathbb{Z}_2)$, deci $F_8^* = \{E, U, U^2, U^3, U^4, U^5, U^6\}$ formează grup cu 7 elemente în raport cu înmulțirea matricelor.

Așadar $|F_8| = 8$ și cum: $U^4 = U^3 U = (E + U)U = U + U^2$,

$U^5 = U^4 U = U^2 + U^3 = E + U + U^2$, $U^6 = U^5 U = U + U^2 + U^3 = E + U^2$, avem:

$$F_8 = \{O, E, U, E + U, U^2, E + U^2, U + U^2, E + U + U^2\}.$$

Se deduce că orice element $X \in F_8$ se reprezintă în mod unic sub forma $X = iE + jU + kU^2$, $0 \leq i, j, k < 2$.

Dacă de asemenea, $Y \in F_8$, $Y = sE + tU + uU^2$, $0 \leq s, t, u < 2$, atunci $X + Y = (i+s)E + (j+t)U + (k+u)U^2 = (i \oplus s)E + (j \oplus t)U + (k \oplus u)U^2$, unde \oplus este simbolul adunării modulo 2. Rezultă că F_8 este o parte stabilă a lui $M_3(\mathbb{Z}_2)$ în raport cu adunarea matricelor și evident $(F_8, +)$ este grup abelian. Deci $(F_8, +, \cdot)$ este inel cu toate elementele diferite de O inversabile, deci este corp cu 8 elemente.

(iii). Cum $|K| = 8$, ordinul lui 1 în grupul $(K, +)$ poate fi 2, 4 sau 8. Dacă ordinul lui 1 este 8, atunci $(K, +, \cdot) \simeq (\mathbb{Z}_8, +, \cdot)$ și cum \mathbb{Z}_8 nu este corp se obține

o contradicție. Dacă ordinul aditiv al lui 1 este 4, atunci $1+1 \neq 0$ și $(1+1)(1+1)=1+1+1+1=0$, deci corpul K are divizori ai lui zero, contradicție.

Așadar $1+1=0$, deci există $a \in K$ a.î. $a^3+a+1=0$ (vezi problema 9.16.). Ca și la punctul (ii) se deduce că $K = \{0, 1, a, 1+a, a^2, 1+a^2, a+a^2, 1+a+a^2\}$, deci orice $x \in K$ se reprezintă în mod unic sub forma $x = i \cdot 1 + j \cdot a + k \cdot a^2$, $0 \leq i, j, k < 2$.

Rezultă că aplicația $f: K \rightarrow F_8$, $f(x) = iE + jU + kU^2 \Leftrightarrow x = i \cdot 1 + j \cdot a + k \cdot a^2$, $0 \leq i, j, k < 2$, este bijectivă. Cum $x+x=0$, oricare ar fi $x \in K$, $X+X=O$, oricare ar fi $X \in F_8$, $a^3+a+1=0$ și $U^3+U+E=O$ se arată că $f(x+y)=f(x)+f(y)$, $f(xy)=f(x)f(y)$, oricare ar fi $x, y \in K$, de unde $(K, +, \cdot) \simeq (F_8, +, \cdot)$.

9.21. Demonstrăm că orice element nenul este inversabil.

Fie $a \in A$, $a \neq 0$ și $b \in A$ a.î. $ba=1$. Evident $b \neq 0$ și fie $b' \in A$ cu $b'b=1$. Atunci $a=1 \cdot a = (b'b)a = b'(ba) = b' \cdot 1 = b'$, adică $b'=a$. Deci $ab=ba=1$ și rezultă că a este inversabil.

9.22. Elementul unitate este $(1, 0)$. Dacă $(a, b) \neq (0, 0)$ atunci $(a, b)^{-1} = \left(\frac{a}{a^2 + b^2}, \frac{-b}{a^2 + b^2} \right)$. $K_1 = \{(x, 0) | x \in K\} \subset K \times K$ este un subcorp al lui $K \times K$ și aplicația $f: K \rightarrow K_1$ definită prin $f(x) = (x, 0)$ este un izomorfism de corpuri.

Ecuția $x^2+1=0$ are în corpul $K \times K$ soluția $x=(0, 1)$.

Fie $K = \mathbb{Z}_p$ cu p număr prim de forma $4k+3$, $k \in \mathbb{N}$ inelul claselor de resturi modulo p . Să presupunem că $x \in K$ are proprietatea că $x^2+1=0$. Atunci conform teoremei lui Fermat rezultă că $1 = x^{p-1} = (x^2)^{\frac{p-1}{2}} = (-1)^{2k+1} = -1$, contradicție.

9.23. Fie $M = \begin{pmatrix} \alpha & \beta \\ -\bar{\beta} & \bar{\alpha} \end{pmatrix}$ și $N = \begin{pmatrix} \gamma & \delta \\ -\bar{\delta} & \bar{\gamma} \end{pmatrix}$ două elemente din H .

Atunci $M \cdot N = \begin{pmatrix} \alpha - \gamma & \beta - \delta \\ -(\bar{\beta} - \bar{\delta}) & \bar{\alpha} - \bar{\gamma} \end{pmatrix} \in H$, $MN = \begin{pmatrix} \alpha\gamma - \beta\bar{\delta} & \alpha\delta + \beta\bar{\gamma} \\ -\alpha\bar{\delta} + \beta\bar{\gamma} & \alpha\gamma - \beta\bar{\delta} \end{pmatrix} \in H$ și

$I_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ -\bar{0} & \bar{1} \end{pmatrix} \in H$, de unde concluzia că H este subinel (unitar) al lui

$M_2(\mathbb{C})$. Mai avem de demonstrat faptul că dacă $M \in H$, $M = \begin{pmatrix} \alpha & \beta \\ -\bar{\beta} & \bar{\alpha} \end{pmatrix} \neq O_2$, atunci

există $N \in H$ a.î. $MN = NM = I_2$. Din $M \neq O_2$ deducem că $\Delta = \alpha\bar{\alpha} + \beta\bar{\beta} = |\alpha|^2 + |\beta|^2 \neq 0$. Considerând $N = \begin{pmatrix} \alpha' & \beta' \\ -\bar{\beta}' & \bar{\alpha}' \end{pmatrix} \in H$, unde $\alpha' = \overline{(\alpha/\Delta)}$ și

$\beta' = -\frac{\beta}{\Delta}$ avem:

$$MN = \begin{pmatrix} \alpha & \beta \\ -\bar{\beta} & \bar{\alpha} \end{pmatrix} \begin{pmatrix} \alpha' & \beta' \\ -\bar{\beta}' & \bar{\alpha}' \end{pmatrix} = \begin{pmatrix} \alpha\alpha' - \beta\bar{\beta}' & \alpha\beta' + \beta\bar{\alpha}' \\ -(\alpha\beta' + \beta\bar{\alpha}') & \alpha\alpha' - \beta\bar{\beta}' \end{pmatrix} \text{ iar}$$

$$\alpha\alpha' - \beta\bar{\beta}' = \alpha \left(\frac{\alpha}{\Delta} \right) + \beta \left(\frac{\beta}{\Delta} \right) = \frac{\alpha\bar{\alpha} + \beta\bar{\beta}}{\Delta} = \frac{|\alpha|^2 + |\beta|^2}{\Delta} = \frac{\Delta}{\Delta} = 1$$

$$\alpha\beta' + \beta\bar{\alpha}' = -\alpha \left(\frac{\beta}{\Delta} \right) + \beta \left(\frac{\alpha}{\Delta} \right) = -\frac{\alpha\beta}{\Delta} + \frac{\alpha\beta}{\Delta} = 0,$$

de unde $MN = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I_2$ și analog $NM = I_2$, adică $M^{-1} = N$.

9.24. (i). Fie $M = \begin{pmatrix} \alpha & \beta \\ -\bar{\beta} & \bar{\alpha} \end{pmatrix}$ cu $\alpha = a+bi$ și $\beta = c+di$; Se observă că asocierea

$M \rightarrow \begin{pmatrix} a & b & c & d \\ -b & a & -d & c \\ -c & d & a & -b \\ -d & -c & b & a \end{pmatrix}$ definește un morfism de inele de la corpul

quaternionilor în $M_4(\mathbb{R})$.

Observăm că $A \cdot A^t = (a^2 + b^2 + c^2 + d^2) \cdot I_4$, de unde $\det A = (a^2 + b^2 + c^2 + d^2)^2$.

Dacă $A \neq O_4$, atunci $\det A \neq 0$ și matricea A este inversabilă.

Observație. Considerăm K mulțimea expresiilor formale de forma $a+bi+cj+dk$ cu $a, b, c, d \in \mathbb{R}$. Definind pentru două elemente din K suma pe componente și produsul polinomial (ținând cont că $i^2=j^2=k^2=-1$, $ij=-ji=k$, $jk=-kj=i$, $ki=-ik=j$) se observă că $(K, +, \cdot)$ devine corp izomorf cu corpul H al quaternionilor.

(ii). Fie $x = a+bi+cj+dk$ un quaternion din centrul lui H . Din condiția de comutare $x \cdot i = i \cdot x$ rezultă că $ai-b-ck+dj = ai-b+ck-dj$, de unde $c=d=0$. Din

condiția de comutare $x \cdot j = j \cdot x$ rezultă și $b=0$. Așadar centrul lui H este mulțimea \mathbb{R} a numerelor reale.

9.25. Presupunem prin reducere la absurd că avem $\bigcup_{i=1}^3 K_i = K$.

Atunci în mod necesar $K_1 \not\subseteq K_2 \cup K_3$, $K_2 \not\subseteq K_1 \cup K_3$, $K_3 \not\subseteq K_1 \cup K_2$, (căci dacă am avea de exemplu $K_1 \subseteq K_2 \cup K_3$, atunci $K = K_2 \cup K_3$ și gândind această egalitate pentru grupurile aditive corespunzătoare, rezultă $K = K_2$ sau $K = K_3$, imposibil).

Prin urmare putem alege elementele $x_1 \in K_1 \setminus (K_2 \cup K_3)$ și $x_2 \in K_2 \setminus (K_1 \cup K_3)$. Evident $x_1 \neq 0$ și $x_2 \neq 0$ și $x_1 + x_2 \notin K_1 \cup K_2$ (căci dacă, de exemplu, $x_1 + x_2 \in K_1$, atunci $x_2 = -x_1 + (x_1 + x_2) \in K_1$, contrar alegerii lui x_2). Prin urmare, $x_1 + x_2 \in K_3$. Considerăm elementul $z = x_1^{-1}(x_1 + x_2) = 1 + x_1^{-1}x_2$. Cum $x_1^{-1} \in K_1$ și $x_1 + x_2 \in K_3 \setminus \{0\}$, rezultă ca mai sus, că $z \notin K_1 \cup K_2$, deci neapărat $z \in K_3$. Atunci $z - 1 \in K_3$, adică $x_1^{-1}x_2 \in K_3$. Din faptul că $x_2 \in K_2 \setminus \{0\}$, rezultă $(x_1^{-1}x_2)x_2^{-1} \in K_2$, adică $x_1^{-1} \in K_2$ și de aici $x_1 \in K_2$, ceea ce este o contradicție cu alegerea lui x_1 .

9.26. Cazul 1. Studiem mai întâi cazul când corpul dat $(K, +, \cdot)$ este finit. Să presupunem că avem o scriere a sa $K = \bigcup_{i=1}^n K_i$, unde $K_i \subset K$,

$i \in \{1, \dots, n\}$ sunt subcorpuri proprii ale lui K . Se știe că grupul multiplicativ (K^*, \cdot) al lui K este ciclic și fie $a \in K^*$ un generator al său. Există atunci $i \in \{1, 2, \dots, n\}$ a.î. $a \in K_i$, de exemplu, $a \in K_1$. Atunci $a^m \in K_1$, oricare ar fi $m \in \mathbb{Z}$ și deci $K^* \subset K_1$. Așadar găsim $K = K_1$, care contrazice faptul că subcorpul K_1 este propriu. Problema este deci rezolvată în cazul unui corp finit K .

Cazul 2. Fie acum un corp infinit K . Să presupunem prin reducere la absurd că există K_1, K_2, \dots, K_n ($n \geq 2$), subcorpuri proprii ale lui K a.î.

$$K = \bigcup_{i=1}^n K_i \text{ și } K_i \neq \bigcup_{\substack{j=1 \\ j \neq i}}^n K_j, \text{ oricare ar fi } i \in \{1, \dots, n\}. (*)$$

Vom arăta că intersecția celor n subcorpuri K_1, K_2, \dots, K_n este infinită. Demonstrăm prin inducție matematică după $k \leq n$, arătând că pentru orice $k \leq n$, intersecția primelor k subcorpuri K_i conține un șir infinit de elemente distincte.

Într-adevăr, cazul $k=1$ este evident, căci K_1 , de exemplu trebuie să fie infinit. Presupunem afirmația adevărată pentru k , deci există un șir de elemente distincte $(x_n)_n \subset \bigcap_{i=1}^k K_i$. Cum $K \neq \bigcup_{j=1}^k K_j$, fie $b \in K - \bigcup_{j=1}^k K_j$.

Considerăm $A = \{x_1b, x_2b, \dots, x_nb, \dots\} = (x_nb)_{n \geq 1}$.

Evident $A \not\subset \bigcup_{j=1}^k K_j$ și cum $K = \bigcup_{j=1}^n K_j$ rezultă $A \subset \bigcup_{j=k+1}^n K_j$. Există deci

un subșir al lui $(x_nb)_{n \geq 1}$ inclus într-un K_j ($j \geq k+1$), de exemplu putem presupune că subșirul este $(x_{n_p}b)_{p \geq 1} \subset K_{k+1}$. Deoarece $(x_{n_1}b)(x_{n_p}b)^{-1} = x_{n_1}x_{n_p}^{-1} \in K_{k+1}$,

oricare ar fi $p \geq 1$ și cum în mod evident, șirul $(x_{n_1}x_{n_p}^{-1})_{p \geq 1} \subset \bigcap_{i=1}^k K_i$ rezultă că

$(x_{n_1}x_{n_p}^{-1})_{p \geq 1} \subset \bigcap_{i=1}^{k+1} K_i$, ceea ce încheie demonstrația prin inducție.

În particular, când $k=n$ obținem că $P = \bigcap_{i=1}^n K_i$ este infinită.

Observăm că P este subcorp în fiecare K_i și în K . Vom arăta că din (*) obținem că P are cel mult $n-1$ elemente; aceasta va contrazice faptul că P este infinită și încheie demonstrația.

Într-adevăr, să presupunem că există $a_1, a_2, \dots, a_n \in P$ distincte. Fie $a_1 \in K_1 \setminus \bigcup_{j=2}^n K_j$ și fie $b \in K_2 \setminus K_1$. Valorile $a_i \cdot a + b$ formează o mulțime de n

elemente distincte (altfel avem $a_i \cdot a + b = a_j \cdot a + b$, cu $i \neq j$ implică $a_i = a_j$, fals). În plus, $a_i \cdot a + b \notin K_1$, oricare ar fi $i \in \{1, \dots, n\}$ (într-adevăr, dacă pentru un i am avea $a_i \cdot a + b = y \in K_1$, cum $a_i \cdot a \in K_1$ ar rezulta $b \in K_1$, fals). Atunci conform principiului lui Dirichlet va exista un K_j , $j \geq 2$ care include cel puțin două elemente de forma $a_i \cdot a + b$.

Dacă $a_{i_1}a + b, a_{i_2}a + b \in K_j$ rezultă că $(a_{i_1} - a_{i_2})a \in K_j$ deci, $a \in K_j$ (deoarece $a_{i_1} - a_{i_2} \neq 0$), imposibil. Contradicția rezultă din faptul că ar exista elementele $a_1, a_2, \dots, a_n \in P$ distincte. Deci $\text{card } P \leq n-1$. Dar în condițiile ipotezei (*) am demonstrat că avem $\text{card } P = \infty$. Din contradicția obținută rezultă că (*) nu este adevărată și deci problema este rezolvată.

9.27. „ \Leftarrow ”. Fie E_1, E_2, \dots, E_n liniile matricei E . Dacă E nu este inversabilă, atunci $\det(E)=0$, deci există $r_1, r_2, \dots, r_n \in K$ nu toți nuli a.î. $\sum_{i=1}^n r_i E_i = 0$ în mulțimea $M_{1 \times n}(K)$. Fie $F_1 = (r_1, r_2, \dots, r_n)$ și $F_i = (0, 0, \dots, 0)$

pentru $1 < i \leq n$. Matricea F formată cu liniile F_1, F_2, \dots, F_n constituie un divizor al lui zero la stânga pentru E .

„ \Rightarrow ”. Dacă E este divizor al lui zero atunci există $F \neq O_n$ a.î. $EF = O_n$. Presupunem prin reducere la absurd că E este inversabilă. Există deci E^{-1} inversa sa. Atunci $E^{-1}E = I_n$ și înmulțind la dreapta cu $F \neq O_n$ deducem că $E^{-1}(EF) = F$, adică, $E^{-1} \cdot O_n = F$ deci $O_n = F$, contradicție.

Dacă K nu este corp, afirmația nu este valabilă după cum se observă în cazul matricei $2I_n \in M_n(\mathbb{Z})$.

9.28. Considerând ecuația $x^3 - 1 = 0$, se observă că are o singură rădăcină în \mathbb{R} și anume $x = 1$ iar în \mathbb{C} are trei rădăcini $x_1 = 1, x_2 = \frac{-1 + i\sqrt{3}}{2}, x_3 = \frac{-1 - i\sqrt{3}}{2}$.

9.29. Fie $f: K \rightarrow A$ un morfism unitar de inele. Știm că f este injectiv dacă și numai dacă $\text{Ker}(f)$ este idealul nul în K . Deoarece $\text{Ker}(f)$ este ideal bilateral în K și K este corp deducem, conform problemei **9.4.**, că $\text{Ker}(f) = K$ sau $\text{Ker}(f) = (0)$.

Egalitatea $\text{Ker}(f) = K$ nu poate avea loc deoarece ar rezulta $f(1) = 0$, ceea ce contrazice faptul că $f(1)$ este elementul unitate la înmulțire în A și acesta este diferit de zero, deoarece A este inel nenul.

Observație. Deducem că morfismele de corpuri sunt în particular funcții injective.

9.30. Fie $f: \mathbb{Q} \rightarrow \mathbb{Q}$ morfism de corpuri, deci morfism de inele și $f(1) = 1$. În particular, f este endomorfism al grupului aditiv $(\mathbb{Q}, +)$.

$$f(0) = f(0+0) = f(0) + f(0) = f(0) \Rightarrow f(0) = 0.$$

Din $f(1) = 1$ rezultă că $f(n) = \underbrace{f(1 + \dots + 1)}_{\text{de } n \text{ ori}} = n \cdot f(1) = n$, oricare ar fi $n \in \mathbb{N}$.

De asemenea, pentru $n \in \mathbb{N}^*$ avem $1 = f(1) = f(\underbrace{\frac{1}{n} + \dots + \frac{1}{n}}_{\text{de } n \text{ ori}}) = nf\left(\frac{1}{n}\right)$ de

unde $f\left(\frac{1}{n}\right) = \frac{1}{n}$. Dacă $m, n \in \mathbb{N}^*$ avem $f\left(\frac{m}{n}\right) = f(\underbrace{\frac{1}{n} + \dots + \frac{1}{n}}_{\text{de } m \text{ ori}}) = mf\left(\frac{1}{n}\right) = \frac{m}{n}$. Deci

$f(q) = q$, oricare ar fi $q \in \mathbb{Q}_+$. Pentru $q \in \mathbb{Q}_-$ avem $-q \in \mathbb{Q}_+$

$0 = f(q + (-q)) = f(q) + f(-q)$ deci $f(q) = -f(-q)$ și cum $-q > 0$ rezultă că $f(-q) = -q$, deci $f(q) = q$. Am arătat că singurul endomorfism al corpului \mathbb{Q} este cel identic.

9.31. (i). $f(0) = f(0+0) = f(0) + f(0)$ deci $f(0) = 0$.

$f(1) = 1$, pentru că f este morfism unitar de inele.

$f((-1)^2) = [f(-1)]^2$, deci $1 = [f(-1)]^2$ de unde $f(-1) \in \{\pm 1\}$.

Nu putem avea $f(-1) = 1$, căci ar rezulta $f(-1) = f(1)$, deci f nu ar fi injectivă.

Așadar $f(-1) = -1$.

(ii). Din $f(1) = 1$ rezultă $f(n) = f(\underbrace{1 + \dots + 1}_{\text{de } n \text{ ori}}) = n \cdot f(1) = n$, oricare ar fi $n \in \mathbb{N}$.

De asemenea, pentru $n \in \mathbb{N}^*$ avem $1 = f(1) = f(\underbrace{\frac{1}{n} + \dots + \frac{1}{n}}_{\text{de } n \text{ ori}}) = nf\left(\frac{1}{n}\right)$, de

unde $f\left(\frac{1}{n}\right) = \frac{1}{n}$.

Dacă $m, n \in \mathbb{N}^*$ avem $f\left(\frac{m}{n}\right) = f(\underbrace{\frac{1}{n} + \dots + \frac{1}{n}}_{\text{de } m \text{ ori}}) = mf\left(\frac{1}{n}\right) = \frac{m}{n}$. Deci $f(q) = q$,

oricare ar fi $q \in \mathbb{Q}_+$. Pentru $q \in \mathbb{Q}_-$ avem $-q \in \mathbb{Q}_+$, $0 = f(q + (-q)) = f(q) + f(-q)$ deci $f(q) = -f(-q)$ și cum $-q > 0$ rezultă că $f(-q) = -q$, deci $f(q) = -(-q) = q$.

(iii). Dacă $\alpha > 0$, atunci există $\beta \in \mathbb{R}^*$ a.î. $\alpha = \beta^2$, deci $f(\alpha) = f(\beta^2) = [f(\beta)]^2 > 0$. Fie $x_1, x_2 \in \mathbb{R}$ cu $x_1 < x_2$. Atunci $\alpha = x_2 - x_1 > 0$ deci $f(\alpha) = f(x_2 - x_1) > 0 \Leftrightarrow f(x_2) - f(x_1) > 0 \Leftrightarrow f(x_2) > f(x_1)$, deci f este strict crescătoare. (Am ținut cont că $f(-x_1) = -f(x_1)$, ceea ce se arată ca și la (ii) când am demonstrat că $f(-q) = -f(q)$).

(iv). Fie f un endomorfism al lui \mathbb{R} . Ținând cont de (ii) este suficient să arătăm că $f(x)=x$, oricare ar fi $x \in \mathbb{R} \setminus \mathbb{Q}$.

Fie $x \in \mathbb{R} \setminus \mathbb{Q}$ fixat și $(q_n)_n, (r_n)_n$ șirurile aproximărilor raționale ale lui x prin lipsă respectiv prin adaos. Avem $q_n < x < r_n$ deci $f(q_n) < f(x) < f(r_n)$, adică, $q_n < f(x) < r_n$, oricare ar fi $n \in \mathbb{N}$. Trecând la limită după n , obținem $x \leq f(x) \leq x$, deci $f(x)=x$.

9. 32. Egalitatea $f \circ \lambda_a = \lambda_a \circ f$, pentru orice $a \in K$, se scrie $\lambda_a(f(x)) = f(\lambda_a(x))$, oricare ar fi $a, x \in K$ sau $af(x) - f(x)a = f(ax - xa)$, oricare ar fi $a, x \in K$, sau încă:

$$af(x) - f(x)a = f(a)f(x) - f(x)f(a), \text{ oricare ar fi } a, x \in K. (1)$$

Egalitatea (1) poate fi scrisă și sub forma:

$$[a - f(a)]f(x) = f(x)[a - f(a)], \text{ oricare ar fi } a, x \in K. (2)$$

Punând $b = a - f(a) \in \text{Im}(1_K - f)$, egalitatea (2) devine:

$$bf(x) = f(x)b, \text{ oricare ar fi } x \in K, b \in \text{Im}(1_K - f). (3)$$

Atunci, pentru orice $x \in K$ și $b \in \text{Im}(1_K - f)$, avem:

$$f(bx - xb) = f(b)f(x) - f(x)f(b) \stackrel{(1)}{=} bf(x) - f(x)b \stackrel{(3)}{=} 0,$$

de unde, ținând seama că f este injectiv, rezultă $bx - xb = 0$, adică $bx = xb$.

Înseamnă că $\text{Im}(1_K - f) \subset Z(K)$, centrul corpului K . Atunci, întrucât $\lambda_a(x) = 0$, oricare ar fi $a \in K$ și $x \in Z(K)$, rezultă $\lambda_a \circ (1_K - f) = 0$. (4)

Observăm ușor că $\lambda_a \in \text{End}(K)$, oricare ar fi $a \in K$, unde $(\text{End}(K), +, \circ)$ este inelul endomorfismelor grupului abelian $(K, +)$. În acest inel de endomorfisme, egalitatea (4) devine $\lambda_a = \lambda_a \circ f$, sau folosind ipoteza, $f \circ \lambda_a = \lambda_a$. (5)

Mai observăm că: $\lambda_a(ax) = a\lambda_a(x)$, oricare ar fi $a, x \in K$. (6)

Pentru a arăta că corpul $(K, +, \cdot)$ este comutativ, este suficient să demonstrăm că grupul (K^*, \cdot) este comutativ. Cum $Z(K^*)$ este centrul grupului K^* este suficient să stabilim egalitatea $Z(K^*) = K^*$. Observăm ușor că $F = \text{Ker}(1_K - f)^* = \{x \in K^* \mid f(x) = x\}$ este un subgrup al lui K^* . Fie $a \in K^* \setminus F$, deci $f(a) \neq a$. Atunci, oricare ar fi $x \in K$ avem $\lambda_a(x) = 0$, căci dacă ar exista un $x_0 \in K$ cu $\lambda_a(x_0) \neq 0$, din (6) am avea $\lambda_a(ax_0) = a\lambda_a(x_0)$, deci $f(\lambda_a(ax_0)) = f(a)f(\lambda_a(x_0))$ și din (5) ar însemna că $\lambda_a(ax_0) = f(a)\lambda_a(x_0)$, adică $a\lambda_a(x_0) = f(a)\lambda_a(x_0)$ și după o simplificare la dreapta cu $\lambda_a(x_0) \neq 0$, am obține $a = f(a)$, contrar presupunerii făcute asupra lui a . Cum $\lambda_a(x) = 0$, oricare ar fi $x \in K$ înseamnă că $a \in Z(K^*)$. Am demonstrat așadar incluziunea $K^* \setminus F \subset Z(K^*)$ și de aici rezultă egalitatea de grupuri multiplicative $K^* = F \cup Z(K^*)$. Dar un grup nu poate fi scris ca reuniune a două subgrupuri

proprii ale sale, deci neapărat $F=K^*$ sau $Z(K^*)=K^*$. Nu putem avea $F=K^*$, căci ar rezulta $f=1_K$, contrar ipotezei. Rezultă $Z(K^*)=K^*$, deci grupul (K^*, \cdot) este comutativ.

9.33. Ambele corpuri sunt conținute în \mathbb{R} . Deoarece elementele lui $\mathbb{Q}(\sqrt{2})$ se scriu în mod unic sub forma $a+b\sqrt{2}$ cu $a, b \in \mathbb{Q}$, orice automorfism φ al lui $\mathbb{Q}(\sqrt{2})$ este determinat de $\varphi(\sqrt{2})$, care trebuie să fie o rădăcină a polinomului X^2-2 . Avem două posibilități: $\varphi(\sqrt{2})=\sqrt{2}$ (și obținem automorfismul identic $\varphi(a+b\sqrt{2})=a+b\sqrt{2}$) sau $\varphi(\sqrt{2})=-\sqrt{2}$ (și obținem automorfismul de „conjugare” $\varphi(a+b\sqrt{2})=a-b\sqrt{2}$); acesta are proprietatea că $\varphi \circ \varphi = 1$). Automorfismele lui $\mathbb{Q}(\sqrt{2})$ formează un grup izomorf cu $\mathbb{Z}/2\mathbb{Z}$.

La fel, un automorfism ψ al lui $\mathbb{Q}(\sqrt[3]{2})$ este determinat de imaginea $\psi(\sqrt[3]{2})$, care trebuie să fie o rădăcină (reală) a polinomului X^3-2 . Cum acest polinom are o singură rădăcină reală, corpul $\mathbb{Q}(\sqrt[3]{2})$ are un singur automorfism, cel identic.

9.34. Fie $f: \mathbb{C} \rightarrow \mathbb{C}$ un morfism de corpuri cu $f(x)=x$, pentru orice $x \in \mathbb{R}$. Dacă $f(i)=\alpha$ atunci $-1=f(-1)=f(i^2)=f(i)^2=\alpha^2$, deci $\alpha \in \{\pm i\}$.

Pentru $f(i)=i$ obținem $f(z)=f(x+iy)=x+f(i)y=x+iy=z$, iar pentru $f(i)=-i$ obținem $f(z)=f(x+iy)=x+f(i)y=x-iy=\bar{z}$.

Deci singurele morfisme de corpuri $f: \mathbb{C} \rightarrow \mathbb{C}$ care invariază \mathbb{R} sunt identitatea și conjugarea, care sunt evident automorfisme.

9.35. Este suficient să demonstrăm că dacă K nu este corp există un morfism de la K la un inel nenul care nu este injectiv.

Dacă K nu este corp, conform problemei 7.4., există în K un ideal I diferit de (0) și K . Deoarece K este un inel comutativ, idealul I este bilateral, deci există inelul factor $A=K/I$. Atunci morfismul canonic $p: K \rightarrow K/I$ nu este injectiv, căci $\text{Ker}(p)=I \neq (0)$.

9.36. Să presupunem mai întâi că f este morfism sau antimorfism de corpuri și să demonstrăm că satisface 1), 2), 3). Să presupunem că f este morfism de corpuri (analog se procedează dacă f este antimorfism). Condiția 1) rezultă din definiția morfismului (ea apare și în definiția antimorfismului).

Arătăm acum 3): Deoarece f este neconstantă, există $x \in K$ cu $f(x) \neq 0$. Cum $f(x)=f(1 \cdot x)=f(1) \cdot f(x)$, rezultă $f(1) \neq 0$. Pe de altă parte,

$f(1)=f(1 \cdot 1)=f(1) \cdot f(1)$, adică $f(1) \cdot [1-f(1)]=0$ și cum $f(1) \neq 0$ rezultă că $1-f(1)=0$, adică $f(1)=1$.

Arătăm 2): Pentru $x \in K \setminus \{0\}$, putem scrie $1=f(1)=f(x \cdot x^{-1})=f(x) \cdot f(x)^{-1}$ și analog $1=f(x^{-1}) \cdot f(x)$. Deducem că $f(x)$ este inversabil (deci nenul) și $f(x^{-1})=f(x)^{-1}$.

Reciproc, să presupunem că f verifică condițiile 1), 2), 3) și să arătăm că este morfism sau antimorfism de corpuri.

Fie $x, y \in K$. Dacă $x \neq 0, y \neq 0$ și $xy \neq 1$, din problema 6.17. rezultă

$$xyx = x + ((x \cdot y^{-1})^{-1} - x^{-1})^{-1}.$$

Cum f verifică condițiile 1), 2), 3) rezultă:

$$f(xyx) = f(x) + ((f(x) - f(y)^{-1})^{-1} - f(x)^{-1})^{-1} \quad (1)$$

Pe de altă parte, f este injectivă. Într-adevar, dacă avem $u, v \in K$ cu $f(u)=f(v)$, din 1) rezultă $f(u-v)=0$ sau $f(t)=0$, unde $t=u-v$. Dacă am avea $t \neq 0$, din 2) ar rezulta, $f(t^{-1})=f(t)^{-1}=0^{-1}$, adică 0 ar fi inversabil, contradicție. Deci $t=0$, adică $u=v$, ceea ce înseamnă că f este injectivă. Atunci cum $x \neq 0, y \neq 0, xy \neq 1$, rezultă $f(x) \neq f(0)=0, f(y) \neq 0$, precum și $f(x)f(y) \neq 1$ (căci $f(x)f(y)=1$ ar conduce la $f(x)=f(y)^{-1}$ sau $f(x)=f(y^{-1})$, deci $x=y^{-1}$, adică $xy=1$, contradicție). În aceste condiții aplicând problema 6.17. rezultă:

$$f(x)f(y)f(x) = f(x) + ((f(x) - f(y)^{-1})^{-1} - f(x)^{-1})^{-1}. \quad (2)$$

Comparând (1) cu (2) rezultă $f(xyx)=f(x)f(y)f(x)$ pentru acele elemente $x, y \in K$ cu $x, y \neq 0, xy \neq 1$. Dar egalitatea precedentă se verifică în mod evident și dacă $x=0$ sau $y=0$ sau $xy=1$ (de exemplu, dacă $xy=1$, atunci $x=y^{-1}$, deci $f(x)=f(y^{-1})=f(y)^{-1}$ și atunci $f(x)f(y)=1$, încât egalitatea se reduce la $f(x)=f(x)$).

Așadar putem scrie:

$$f(xyx)=f(x)f(y)f(x), \text{ oricare ar fi } x, y \in K. \quad (3)$$

Pentru $y=1$ rezultă $f(x^2)=f(x)^2$, oricare ar fi $x \in K$. (4)

Dacă în (4) înlocuim x cu $x+y$ obținem

$$f(x^2+xy+yx+y^2)=f(x)^2+f(x)f(y)+f(y)f(x)+f(y)^2, \text{ adică}$$

$$f(x^2)+f(xy)+f(yx)+f(y^2)=f(x)^2+f(x)f(y)+f(y)f(x)+f(y)^2.$$

Reducând termenii egali conform cu (4) rezultă:

$$f(xy)+f(yx)=f(x)f(y)+f(y)f(x). \quad (5)$$

Calculăm următorul produs, pentru $x, y \in K, x \neq 0, y \neq 0$:

$$\begin{aligned} [f(xy)-f(x)f(y)]f(xy)^{-1}[f(xy)-f(y)f(x)] &= [1-f(x)f(y)f(xy)^{-1}] \cdot [f(xy)-f(y)f(x)] = \\ &= f(xy)-f(x)f(y)-f(y)f(x)+f(x)f(y)f(xy)^{-1}f(y)f(x) = -f(yx)+f(x)f(y)f(xy)^{-1}f(y)f(x) \\ &\stackrel{(3)}{=} -f(yx)+f(x)f(y(xy)^{-1}y)f(x) = -f(yx)+f(x)f(x^{-1}y)f(x) = -f(yx)+f(x(x^{-1}y)x) = \\ &= -f(yx)+f(yx)=0. \end{aligned}$$

Deoarece $f(xy)^{-1} \neq 0$, iar într-un corp nu avem divizori ai lui zero, rezultă $f(xy) - f(x)f(y) = 0$ sau $f(xy) - f(y)f(x) = 0$, pentru orice $x, y \in K \setminus \{0\}$. Dacă $x=0$ sau $y=0$, aceste egalități au loc, în mod evident. Prin urmare am obținut că $f(xy) = f(x)f(y)$ sau $f(xy) = f(y)f(x)$, oricare ar fi $x, y \in K$. Conform problemei 7.24. rezultă că f este morfism sau antimorfism de inele, deci de corpuri.

9.37. „ \Rightarrow ”. Dacă f este morfism de corpuri afirmațiile 1), 2), 3) sunt satisfăcute.

„ \Leftarrow ”. Reciproc, să presupunem că 1), 2), 3) sunt satisfăcute și să demonstrăm că f este morfism de corpuri.

Vom arăta mai întâi egalitatea $f(x^2) = f(x)^2$, oricare ar fi $x \in K$. (1)

Într-adevăr, din 2) avem $f((1+x)^3) = [f(1+x)]^3$ și ținând cont de 1) și de 3) obținem: $f(1+3x+3x^2+x^3) = [1+f(x)]^3 \Leftrightarrow$

$f(1)+3f(x)+3f(x^2)+f(x^3) = 1+3f(x)+3[f(x)]^2+[f(x)]^3 \Leftrightarrow 3[f(x)]^2 = 3f(x^2)$
(la reducerile de termeni asemenea am folosit 1) și 3)).

Ultima egalitate se scrie $3[f(x^2) - f(x)^2] = 0$ și cum corpul L este de caracteristică zero, rezultă $f(x^2) - f(x)^2 = 0$, adică (1).

Arătăm acum că $f(xy) = f(x) \cdot f(y)$, oricare ar fi $x, y \in K$. (2)

Avem evident $2xy = (x+y)^2 - x^2 - y^2$. Aplicând funcția f și ținând cont că f este morfism de grupuri aditive, rezultă: $2f(xy) = f((x+y)^2) - f(x^2) - f(y^2)$. Folosind (1) ultima egalitate se transcrie succesiv:

$$2f(xy) = [f(x+y)]^2 - f(x)^2 - f(y)^2 \Leftrightarrow 2f(xy) = [f(x)+f(y)]^2 - f(x)^2 - f(y)^2 \Leftrightarrow$$

$$2f(xy) = 2f(x)f(y) \Leftrightarrow 2[f(xy) - f(x)f(y)] = 0.$$

Cum L are caracteristica zero rezultă că $f(xy) - f(x)f(y) = 0$, adică (2). Aceasta înseamnă că f este morfism de corpuri.

Observație. Ipoteza conform căreia corpurile K și L sunt de caracteristică 0, poate fi înlocuită cu una mai generală: caracteristica acestor corpuri să nu fie egală cu 2 sau 3.

9.38. (i). Fie $A = \{1, 2 \cdot 1, 3 \cdot 1, \dots, n \cdot 1\}$ care este o submulțime a corpului K . Deoarece K este de caracteristică zero sau de caracteristică $p > n$, deducem că elementele lui A sunt distincte două câte două. Dacă $a \in A$ și $x \in K$, avem evident $ax = xa$ și deci funcționează formula binomului lui Newton:

$$(x+a)^n = x^n + C_n^1 x^{n-1} a + C_n^2 x^{n-2} a^2 + \dots + C_n^{n-2} x^2 a^{n-2} + C_n^{n-1} x a^{n-1} + a^n.$$

Luând în această identitate pe rând $a=1, a=2 \cdot 1, \dots, a=n \cdot 1$ obținem sistemul:

$$\begin{aligned}
(x+1)^n - 1^n &= x^n + C_n^1 x^{n-1} + C_n^2 x^{n-2} + \dots + C_n^{n-2} x^2 + C_n^{n-1} x \\
(x+2 \cdot 1)^n - 2^n \cdot 1 &= x^n + C_n^1 (2 \cdot 1) x^{n-1} + C_n^2 (2 \cdot 1)^2 x^{n-2} + \dots + C_n^{n-2} (2 \cdot 1)^{n-2} x^2 + C_n^{n-1} (2 \cdot 1)^{n-1} x \\
&\dots\dots\dots \\
(x+n \cdot 1)^n - n^n \cdot 1 &= x^n + C_n^1 (n \cdot 1) x^{n-1} + C_n^2 (n \cdot 1)^2 x^{n-2} + \dots + C_n^{n-2} (n \cdot 1)^{n-2} x^2 + C_n^{n-1} (n \cdot 1)^{n-1} x
\end{aligned}$$

în care avem n ecuații și n necunoscute x, x^2, \dots, x^n .

Determinantul sistemului este:

$$\begin{aligned}
\delta &= \begin{vmatrix} 1 & C_n^1 \cdot 1 & C_n^2 \cdot 1^2 & \dots & C_n^{n-1} \cdot 1^{n-1} \\ 1 & C_n^1 \cdot (2 \cdot 1) & C_n^2 \cdot (2 \cdot 1)^2 & \dots & C_n^{n-1} \cdot (2 \cdot 1)^{n-1} \\ \dots & \dots & \dots & \dots & \dots \\ 1 & C_n^1 \cdot (n \cdot 1) & C_n^2 \cdot (n \cdot 1)^2 & \dots & C_n^{n-1} \cdot (n \cdot 1)^{n-1} \end{vmatrix} \\
&= C_n^1 \cdot C_n^2 \cdot \dots \cdot C_n^{n-1} \cdot \begin{vmatrix} 1 & 1 & 1^2 & \dots & 1^{n-1} \\ 1 & (2 \cdot 1) & (2 \cdot 1)^2 & \dots & (2 \cdot 1)^{n-1} \\ \dots & \dots & \dots & \dots & \dots \\ 1 & (n \cdot 1) & (n \cdot 1)^2 & \dots & (n \cdot 1)^{n-1} \end{vmatrix} \\
&= C_n^1 \cdot C_n^2 \cdot \dots \cdot C_n^{n-1} \cdot \prod_{1 \leq i < j \leq n} (j \cdot 1 - i \cdot 1),
\end{aligned}$$

unde am ținut seama că ultimul determinant este Vandermonde. Așadar, observăm că $\delta = c \cdot 1$, cu $c \in \mathbb{Z}$, iar datorită faptului că suntem în caracteristică zero sau $p > n$, avem $C_n^1 \cdot 1 \neq 0, C_n^2 \cdot 1 \neq 0, \dots, C_n^{n-1} \cdot 1 \neq 0, \prod_{1 \leq i < j \leq n} (j \cdot 1 - i \cdot 1) \neq 0$, deci

$\delta \neq 0$. Aplicând regula lui Cramer, obținem că necunoscutele x, x^2, \dots, x^n se exprimă ca niște combinații liniare de elementele $(x+1)^n, (x+2 \cdot 1)^n, \dots, (x+n \cdot 1)^n$ cu coeficienți „numere raționale” (aici prin „număr rațional” înțelegem un element din K de forma $\frac{\alpha \cdot 1}{\beta \cdot 1} = (\alpha \cdot 1) \cdot (\beta \cdot 1)^{-1}$, cu $\alpha, \beta \in \mathbb{Z}$). Facem observația că

deși suntem într-un corp necomutativ, am operat numai cu elemente ce comută, deci toate considerațiile din cazul comutativ (de exemplu, regula lui Cramer) rămân valabile. Din 1) și 3) rezultă ușor $f(r \cdot 1) = r \cdot f(1) = r \cdot 1$, pentru orice $r \in \mathbb{Z}$.

Dacă r este rațional, adică $r = \frac{\alpha}{\beta}$, cu $\alpha, \beta \in \mathbb{Z}$, atunci $\beta r = \alpha$, deci

$f(\beta \cdot r \cdot 1) = f(\alpha \cdot 1) = \alpha \cdot 1$, adică $\beta f(r \cdot 1) = \alpha \cdot 1$, de unde $f(r \cdot 1) = (\alpha \cdot 1)(\beta \cdot 1)^{-1}$. Deci funcția f invariază numerele raționale, în accepțiunea de mai sus.

Exprimăm necunoscuta x^2 sub forma unei combinații liniare de tipul:

$$x^2 = r_1(x+1)^n + r_2(x+2 \cdot 1)^n + \dots + r_n(x+n \cdot 1)^n. \quad (1)$$

Să observăm că în (1), coeficienții r_1, r_2, \dots, r_n depind numai de elementele din A și de niște combinări, deci rămân aceiași pentru orice $x \in K$. În

mod similar, o relație analogă cu (1) funcționează pentru orice $y \in L$ și în particular pentru elementele $y=f(x) \in L$, cu $x \in K$. Altfel spus, egalitatea (1) se menține când se înlocuiește x cu $f(x)$. Aplicând atunci f în (1) și ținând seama de proprietățile 1) și 2) precum și de cele spuse anterior, va rezulta $f(x^2)=f(x)^2$, oricare ar fi $x \in K$;

(ii). Dacă L și K sunt corpuri comutative, în egalitatea $f(x^2)=f(x)^2$ să înlocuim pe x cu $x+y$, unde $x, y \in K$. Deoarece $(x+y)^2=x^2+y^2+2xy$, rezultă $f(x^2+2xy+y^2)=f(x)^2+2f(x)f(y)+f(y)^2$, adică $f(x^2)+2f(xy)+f(y^2)=f(x)^2+2f(x)f(y)+f(y)^2$ sau încă $2[f(xy)-f(x)f(y)]=0$. Deoarece caracteristica este zero sau $p>2$, rezultă $f(xy)=f(x)f(y)$, oricare ar fi $x, y \in K$, deci f este morfism de corpuri.

9.39. (i). Se arată ușor că $f(x)=x$, oricare ar fi $x \in \mathbb{Q}$. Deoarece $f(\sqrt{d_1}) \in \mathbb{Q}(\sqrt{d_2})$ există $a, b \in \mathbb{Q}$ a.î. $f(\sqrt{d_1})=a+b\sqrt{d_2}$ (1).

Atunci $d_1=f(d_1)=[f(\sqrt{d_1})]^2=(a+b\sqrt{d_2})^2$, deci $d_1=a^2+d_2b^2+2ab\sqrt{d_2}$. (2)

Dacă $a \neq 0$ și $b \neq 0$, din (2) rezultă $\sqrt{d_2} \in \mathbb{Q}$, contradicție. Deci $a=0$ sau $b=0$.

Dacă $b=0$, atunci din (2) rezultă $\sqrt{d_1}=\pm a \in \mathbb{Q}$, contradicție. Așadar $b \neq 0$ și atunci obligatoriu $a=0$. Egalitatea (2) devine $d_1=d_2b^2$ și arată că $\frac{d_1}{d_2}=b^2$, deci $\frac{d_1}{d_2}$ este pătratul unui număr rațional. Dacă d_1 și d_2 sunt întregi liberi de pătrate, diferiți, această egalitate nu poate avea loc, deci neapărat $d_1=d_2$.

În particular, rezultă $\mathbb{Q}(\sqrt{d_1})=\mathbb{Q}(\sqrt{d_2})$, adică două corpuri pătratice sunt izomorfe dacă și numai dacă sunt egale.

(ii). Reluând cele de la punctul (i) în care $d_1=d_2=d$, vom avea, conform cu (1) și (2): $f(\sqrt{d})=a+b\sqrt{d}$, unde $a=0$ și $d=db^2$, adică $b^2=1$ deci $b \in \{\pm 1\}$.

Pentru $b=1$ obținem $f(\sqrt{d})=\sqrt{d}$, adică $f(x)=x$, oricare ar fi $x \in \mathbb{Q}(\sqrt{d})$, deci f este automorfismul identic al corpului $\mathbb{Q}(\sqrt{d})$.

Pentru $b=-1$ obținem $f(\sqrt{d})=-\sqrt{d}$, adică $f(x)=x^*$ (conjugatul pătratic al lui x) pentru orice $x \in \mathbb{Q}(\sqrt{d})$, deci f este automorfismul conjugare al lui $\mathbb{Q}(\sqrt{d})$.

9.40. Fie $\varphi: (\mathbb{Z}_p, +) \rightarrow (\mathbb{Z}_p^*, \cdot)$ un morfism de grupuri. Nucleul morfismului φ , $\text{Ker}(\varphi)$, este un subgrup al lui $(\mathbb{Z}_p, +)$. Dar conform teoremei lui Lagrange rezultă că singurele subgrupuri ale lui \mathbb{Z}_p sunt $\{\hat{0}\}$ și \mathbb{Z}_p .

Dacă $\text{Ker}(\varphi) = \{\hat{0}\}$, atunci φ ar fi injectiv, ceea ce nu se poate deoarece \mathbb{Z}_p are p elemente iar \mathbb{Z}_p^* are $p-1$ elemente.

Dacă $\text{Ker}(\varphi) = \mathbb{Z}_p$, atunci $\varphi(x) = \hat{1}$, oricare ar fi $x \in \mathbb{Z}_p$.

Deci unicul morfism căutat este cel nul, care duce toate elementele grupului $(\mathbb{Z}_p, +)$ în elementul neutru al grupului (\mathbb{Z}_p^*, \cdot) .

9.41. Fie $f: (\mathbb{Q}, +) \rightarrow (\mathbb{Q}^*, \cdot)$ un morfism de grupuri.

Pentru orice $x \in \mathbb{Q}$ putem scrie $f(x) = f\left(\frac{x}{2} + \frac{x}{2}\right) = \left[f\left(\frac{x}{2}\right)\right]^2 > 0$, deci f ia

valori strict pozitive. Arătăm că $f(x) = [f(1)]^x$, pentru orice $x \in \mathbb{Q}$. Avem $f(x) = f(\underbrace{1 + \dots + 1}_{\text{de } x \text{ ori}}) = \underbrace{f(1) \cdot \dots \cdot f(1)}_{\text{de } x \text{ ori}} = [f(1)]^x$. Demonstrăm că $f(1) = 1$.

Presupunem prin reducere la absurd că $f(1) = \frac{a}{b}$, unde $a, b \in \mathbb{N}^*$, $a \neq b$, a, b relativ prime.

Fie p natural, $p > \max(a, b)$. Atunci cel puțin unul dintre numerele a sau b nu este putere de ordin p a unui număr natural și deci fracția $\frac{a}{b}$ nu este putere de ordinul p a unui număr rațional. Luând $x = \frac{1}{p} \in \mathbb{Q}$ avem

$f(x) = [f(1)]^x = \left(\frac{a}{b}\right)^{\frac{1}{p}} = \sqrt[p]{\frac{a}{b}} \notin \mathbb{Q}$, contradicție. Deci $f(1) = 1$ și în concluzie

$f(x) = [f(1)]^x = 1^x = 1$, oricare ar fi $x \in \mathbb{Q}$. Deci unicul morfism de grupuri de la $(\mathbb{Q}, +)$ la (\mathbb{Q}^*, \cdot) este cel constant, care duce toate elementele lui $(\mathbb{Q}, +)$ în elementul neutru 1 din grupul (\mathbb{Q}^*, \cdot) .

9.42. (i). Presupunem prin reducere la absurd că p nu este prim, deci există k, t numere naturale mai mici decât p a.î. $p = kt$. Egalitatea $p \cdot 1_K = 0_K$ devine $(kt) \cdot 1_K = 0_K \Leftrightarrow (k \cdot 1_K)(t \cdot 1_K) = 0_K$ și cum un corp nu are divizori ai lui zero, rezultă $k \cdot 1_K = 0_K$ sau $t \cdot 1_K = 0_K$. Oricare dintre aceste egalități contrazice minimalitatea lui p . Rezultă că p este prim.

(ii). Folosind binomul lui Newton (K corp comutativ) avem pentru orice $x, y \in K$: $(x+y)^p = x^p + y^p + \sum_{i=1}^{p-1} C_p^i x^{p-i} y^i$ (*). Dar pentru p prim avem $C_p^i = pa_i$, pentru $i \in \{1, \dots, p-1\}$ (unde a_i este un număr natural) a.î. pentru orice $\alpha \in K$ avem: $C_p^i \alpha = (pa_i)\alpha = (p \cdot 1_K)(a_i \alpha) = 0_K(a_i \alpha) = 0_K$.

Rezultă că suma din membrul drept al egalității (*) este nulă și obținem $(x+y)^p = x^p + y^p$, oricare ar fi $x, y \in K$. Dacă în această egalitate înlocuim pe y cu $-y$ obținem $(x-y)^p = x^p + (-1)^p y^p$.

Pentru p prim impar egalitatea devine $(x-y)^p = x^p - y^p$ iar pentru $p=2$, ținând cont că într-un corp de caracteristică 2 fiecare element este egal cu opusul său, obținem $(x-y)^2 = x^2 + y^2 = x^2 - y^2$. Deci am demonstrat că $(x \pm y)^p = x^p \pm y^p$, pentru orice p prim și $x, y \in K$.

(iii). Fie $f: (K, +) \rightarrow (K^*, \cdot)$ un morfism de grupuri.

Pentru orice $x \in K$ avem $px = (p \cdot 1_K)x = 0_K \cdot x = 0_K$, deci aplicând morfismul f rezultă că $f(px) = f(0_K)$, adică $[f(x)]^p = 1_K$.

Ultima egalitate poate fi scrisă sub forma $[f(x)]^p - (1_K)^p = 0_K$ sau, ținând cont de (ii): $[f(x) - 1_K]^p = 0_K \Rightarrow f(x) - 1_K = 0_K \Rightarrow f(x) = 1_K$.

Deci unicul morfism de grupuri căutat este cel nul care duce toate elementele grupului $(K, +)$ în elementul neutru al grupului (K^*, \cdot) .

9.43. Elementele acestui corp pot fi reprezentate sub forma: $0, 1, 2, y, 2y, 1+y, 1+2y, 2+y, 2+2y$ unde $3y=0$. Pentru un element oarecare a se verifică $a+a+a=0$. Deci caracteristica căutată este 3.

9.44. Va trebui să arătăm că $Z(K)=K$. Pentru aceasta procedăm prin reducere la absurd, presupunând că $Z(K) \subsetneq K$. Fie deci $x \in K \setminus Z(K)$ și să considerăm $n \geq 1$ un întreg minimal cu proprietatea $x^{p^n} \in Z(K)$.

Din minimalitatea lui n rezultă că elementul $a = x^{p^{n-1}}$ verifică condițiile: $a \in K \setminus Z(K)$ și $a^p \in Z(K)$. Definem aplicația $\delta: K \rightarrow K$ prin $\delta(y) = ya - ay$ și inductiv iteratele sale prin $\delta^1 = \delta$; $\delta^{k+1} = \delta \cdot \delta^k$, pentru $k \geq 1$. Se verifică imediat

prin inducție după $k \geq 1$ că: (1)

$$\delta^k(y) = ya^k - k a y a^{k-1} + \frac{k(k-1)}{1 \cdot 2} a^2 y a^{k-2} - \frac{k(k-1)(k-2)}{1 \cdot 2 \cdot 3} a^3 y a^{k-3} + \dots + (-1)^k a^k y =$$

$$= \sum_{j=0}^k (-1)^j C_k^j a^j y a^{k-j}$$

(în pasul inductiv se folosește formula de descompunere a combinărilor).

Deoarece p este prim rezultă că $p \mid C_p^j$ pentru orice $2 \leq j \leq p-1$. De aici

și din (1) aplicată pentru $k=p$ rezultă conform ipotezei 1) că:

$$(2) \delta^p(y) = ya^p - a^p y = 0, \text{ oricare ar fi } y \in K \text{ (deoarece } a^p \in Z(K)).$$

Din $a \notin Z(K)$ rezultă că $\delta \neq 0$. Deci dacă $y \in K \setminus \{0\}$ verifică $\delta(y) \neq 0$, deducem din (2) existența unui întreg k cu $1 < k \leq p$ având proprietatea că $\delta^k(y) = 0$ și $\delta^{k-1}(y) \neq 0$.

Fie $z = \delta^{k-1}(y) \neq 0$. Deoarece $k > 1$, rezultă $k-1 \geq 1$ și prin urmare $z = \delta(w) = wa - aw$ pentru $w = \delta^{k-2}(y) \neq 0$ (pentru $k=2$, $\delta^{2-2}(y) = \delta^0(y)$ este notație pentru y).

Luând $u = za^{-1}$ putem scrie $z = ua$ și deoarece z comută cu a (căci $z = \delta^{k-1}(y)$ și prin urmare $0 = \delta^k(y) = \delta(\delta^{k-1}(y)) = \delta(z) = za - az$) rezultă că și u comută cu a . Rezultă din cele de mai sus că $au = z = wa - aw$ și prin urmare

$$a = (wa - aw)u^{-1} = (wu^{-1})a - a(wu^{-1}) = ca - ac,$$

unde am notat $c = wu^{-1}$. Ultima relație conduce la $c = 1 + aca^{-1}$.

De aici și din ipoteza 1) deducem prin inducție după $t \geq 1$ că:

$$(3) c^{p^t} = (1 + aca^{-1})^{p^t} = 1^{p^t} + (aca^{-1})^{p^t} = 1 + ac^{p^t} a^{-1}.$$

Datorită ipotezei 2) există un $t \geq 1$ cu $c^{p^t} \in Z(K)$ și conform lui (3): $c^{p^t} = 1 + ac^{p^t} a^{-1} = 1 + aa^{-1} c^{p^t} = 1 + c^{p^t}$, adică $0 = 1$. Contradicția obținută arată că K este corp comutativ.

9.45. Deoarece corpul K este finit, caracteristica sa este un număr natural nenul (nu putem avea caracteristica 0, căci atunci elementele $1_K, 2 \cdot 1_K, 3 \cdot 1_K, \dots, n \cdot 1_K, \dots$ ar fi distincte și în consecință corpul K ar fi infinit).

Conform problemei 9.42., caracteristica sa este un număr prim, să-l notăm cu p .

Tot în problema 9.42. am demonstrat că singurul morfism de grupuri de la $(K, +)$ la (K^*, \cdot) este morfismul nul $\varphi: (K, +) \rightarrow (K^*, \cdot)$, $\varphi(x) = 1_K$.

Determinăm în continuare morfismele de grup de la (K^*, \cdot) la $(K, +)$.

Observăm mai întâi că numărul de elemente al corpului K este o putere a lui p . Într-adevăr, operația externă $\alpha: \mathbb{Z}_p \times K \rightarrow K$, $\alpha(\hat{i}, x) = ix = \underbrace{x + \dots + x}_{\text{de } i \text{ ori}}$

determină pe K o structură de \mathbb{Z}_p -spațiu vectorial. Notând cu q dimensiunea acestui spațiu, avem izomorfismul de \mathbb{Z}_p -spații vectoriale $\mathbb{Z}_p^q \cong K$, încât dacă trecem la cardinale vom avea $|K| = p^q$.

Rezultă că pentru orice $x \in K$ avem $x^{p^q} = x$.

Fie atunci $\psi: (K^*, \cdot) \rightarrow (K, +)$ un morfism de grupuri.

Avem pentru orice $x \in K$, $\psi(x) = \psi(x^{p^q}) = p^q \cdot \psi(x) = 0_K$.

Deci singurul morfism $\psi: (K^*, \cdot) \rightarrow (K, +)$ este cel constant, $\psi(x) = 0_K$.

Pentru $K = \mathbb{Z}_p$ regăsim rezultatul din problema 9.40.

9.46. Observăm că $a \neq -1$: Existența lui f implică $\text{car}(K) = 2$. Pentru $a = -1$, $f(x) + f(-x) = 2x$ și înlocuind x cu $-x$, $f(-x) + f(x) = -2x$, deci $2[f(x) + f(-x)] = 0$ sau (înmulțind cu 2^{-1}), $f(x) + f(-x) = 2x = 0$, oricare ar fi $x \in K$.

Pentru $a^{2n+1} + 1 = (a+1)(a^{2n} - a^{2n-1} + \dots - a + 1)$ rezultă

$a^{2n} - a^{2n-1} + \dots - a + 1 = 2(a+1)^{-1}$ (pentru că $a+1 \neq 0$). În final alegem $f: K \rightarrow K$, $f(x) = 2(a+1)^{-1}x$, oricare ar fi $x \in K$.

Observație. Se poate arăta că f este unica aplicație cu proprietățile cerute.

9.47. (i). Faptul că $(K, +, \cdot)$ este corp se verifică imediat. Funcția $f: K \rightarrow \mathbb{C}$, $f(M(a, b)) = a + ib$ este un izomorfism de corpuri, fapt care se probează imediat.

(ii). Rezolvăm în corpul \mathbb{C} sistemul „izomorf”: $\begin{cases} u + v = 3 + 3i \\ u^3 + v^3 = -9 + 9i \end{cases}$, unde

$u = f(X)$ iar $v = f(Y)$. Sistemul este simetric și vom nota $u + v = s$, $uv = p$ obținând

sistemul în s și p : $\begin{cases} s = 3 + 3i \\ s^3 - 3ps = -9 + 9i \end{cases}$.

Acest sistem are soluție unică $\begin{cases} s = 3 + 3i \\ p = 5i \end{cases}$.

Deci obținem sistemul în u și v : $\begin{cases} u+v=3+3i \\ uv=5i \end{cases}$ care are soluțiile

$$\begin{cases} u_1 = 2+i \\ v_1 = 1+2i \end{cases} \text{ respectiv } \begin{cases} u_2 = 1+2i \\ v_2 = 2+i \end{cases}.$$

Soluțiile sistemului matriceal în X și Y vor fi:

$$\begin{cases} X_1 = f^{-1}(u_1) = \begin{pmatrix} 2 & 1 \\ -1 & 2 \end{pmatrix} \\ Y_1 = f^{-1}(v_1) = \begin{pmatrix} 1 & 2 \\ -2 & 1 \end{pmatrix} \end{cases} \text{ și } \begin{cases} X_2 = f^{-1}(u_2) = \begin{pmatrix} 1 & 2 \\ -2 & 1 \end{pmatrix} \\ Y_2 = f^{-1}(v_2) = \begin{pmatrix} 2 & 1 \\ -1 & 2 \end{pmatrix} \end{cases}.$$

9.48. (i). Se verifică axiomele corpului comutativ. Elementul neutru la adunare este $0=0+0 \cdot \sqrt{d}$ iar opusul lui $x=a+b\sqrt{d}$ este $-x=-a+(-b)\sqrt{d}$. Elementul unitate este $1=1+0 \cdot \sqrt{d}$. Orice element nenul $x=a+b\sqrt{d}$ este inversabil, inversul său fiind $x^{-1} = \frac{1}{a^2 - db^2} (a - b\sqrt{d})$.

(ii). Se verifică axiomele corpului comutativ. Elementul neutru la adunare este O_2 , elementul unitate este matricea I_2 iar inversa unei matrice nenule $\begin{pmatrix} a & b \\ db & a \end{pmatrix}$ (adică cel puțin unul dintre a și b este diferit de 0) este $\frac{1}{a^2 - db^2} \cdot \begin{pmatrix} a & -b \\ -db & a \end{pmatrix}$.

(iii). Aplicația $f: \mathbb{Q}(\sqrt{d}) \rightarrow K$, $f(a+b\sqrt{d}) = \begin{pmatrix} a & b \\ db & a \end{pmatrix}$ este un izomorfism de corpuri.

9.49. Evident $\mathbb{Q} \subseteq K$ și $\mathbb{Q} \neq K$, căci corpul \mathbb{Q} are un singur endomorfism. Unul din endomorfismele lui K fiind cel identic, putem presupune că $g=1_K$. Avem $f \circ f = f$ sau $f \circ f = g = 1_K$. Nu se poate însă ca $f \circ f = f$, căci f fiind injectiv ar rezulta $f = g = 1_K$, absurd, deci $f \circ f = 1_K$. (1) Cum $g=1_K$, ipoteza ii) se mai scrie $f(x)=x \Rightarrow x \in \mathbb{Q}$ (2).

Să considerăm un element oarecare $x \in K \setminus \mathbb{Q}$ și apoi elementele $a=x+f(x) \in K$, $b=xf(x) \in K$. (3) Din (1), (2), (3) avem :

$$f(a)=f(x)+f(f(x))=f(x)+x=a \Rightarrow a \in \mathbb{Q}$$

$$f(b)=f(x)f(f(x))=xf(x)=b \Rightarrow b \in \mathbb{Q}.$$

Rezultă că x și $f(x)$ sunt rădăcinile ecuației cu coeficienți raționali:

$$x^2 - ax + b = 0. (4)$$

Din (4) rezultă că $x = \frac{1}{2}(a \pm \sqrt{a^2 - 4b})$. Scriind $a^2 - 4b = q^2 d$ cu $q \in \mathbb{Q}$ și $d \in \mathbb{Z} \setminus \{1\}$ liber de pătrate, avem $x = \frac{1}{2}(a \pm q\sqrt{d}) \in \mathbb{Q}(\sqrt{d})$. Luând acum un alt $x' \in K \setminus \mathbb{Q}$, există în mod analog un întreg $d' \in \mathbb{Z} \setminus \{1\}$ liber de pătrate a.î. $x' \in \mathbb{Q}(\sqrt{d'})$. Arătăm că $d = d'$. Mai întâi observăm că: $(f(\sqrt{d}))^2 = f((\sqrt{d})^2) = f(d) = d$, de unde $f(\sqrt{d}) = \pm\sqrt{d}$. Dacă am avea $f(\sqrt{d}) = \sqrt{d}$ din (2) ar rezulta $\sqrt{d} \in \mathbb{Q}$, imposibil. Așadar $f(\sqrt{d}) = -\sqrt{d}$ și analog $f(\sqrt{d'}) = -\sqrt{d'}$.

Atunci: $f(\sqrt{dd'}) = f(\sqrt{d})f(\sqrt{d'}) = (-\sqrt{d})(-\sqrt{d'}) = \sqrt{dd'}$ și din (2) rezultă $\sqrt{dd'} \in \mathbb{Q}$. Cum d și d' sunt libere de pătrate, rezultă că $d = d'$. Din cele spuse rezultă că există și este unic un întreg liber de pătrate $d \neq 1$, a.î. $K \subseteq \mathbb{Q}(\sqrt{d})$. Incluziunea reciprocă este imediată căci din $x = \frac{1}{2}(a \pm q\sqrt{d}) \in K$ rezultă că și $\sqrt{d} \in K$ și de aici $\mathbb{Q}(\sqrt{d}) \subseteq K$. Deducem egalitatea $K = \mathbb{Q}(\sqrt{d})$.

9.50. Dacă $a^2 + b^2 \neq 0$ atunci determinantul $\begin{vmatrix} a & b \\ qb & a \end{vmatrix} = a^2 - qb^2 \neq 0$, dacă q

nu este pătratul unui număr rațional (matricele cu $b=0$ dar $a \neq 0$ sunt evident inversabile).

9.51. Observăm că putem scrie

$$M(a, b) = a \cdot \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + b \cdot \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} = a \cdot I_2 + b \cdot X, \text{ unde matricea } X \text{ are proprietatea că}$$

$$X^2 = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} = \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix} = 2 \cdot I_2.$$

Pentru a demonstra că K este corp arătăm mai întâi faptul că aceste matrice formează parte stabilă în raport cu adunarea și înmulțirea matricelor, adică suma și produsul a două matrice $M(a, b)$, $M(c, d)$ sunt matrice de aceeași formă:

$$M(a, b) + M(c, d) = (a \cdot I_2 + b \cdot X) + (c \cdot I_2 + d \cdot X) = (a+c) \cdot I_2 + (b+d) \cdot X = M(a+c, b+d),$$

$$M(a, b) \cdot M(c, d) = (a \cdot I_2 + b \cdot X) \cdot (c \cdot I_2 + d \cdot X) = ac \cdot I_2 + ad \cdot X + bc \cdot X + bd \cdot 2I_2 =$$

$$= (ac + 2bd) \cdot I_2 + (ad + bc) \cdot X = M(ac + 2bd, ad + bc).$$

Axiomele corpului se verifică ușor. Elementul nul este matricea $M(0, 0)$ iar elementul unitate este matricea $M(1, 0)$. Matricea $M(a, b)$ are determinantul

a^2-2b^2 , deci este nenulă dacă și numai dacă este inversabilă. Inversa matricii $M(a, b)$ este matricea $M\left(\frac{a}{a^2-2b^2}, \frac{-b}{a^2-2b^2}\right)$.

Funcția $f: \mathbb{Q}(\sqrt{2}) \rightarrow K$, $f(a+b\sqrt{2}) = \begin{pmatrix} a+b & b \\ b & a-b \end{pmatrix}$ este bijectivă și morfism de corpuri. Deci K este izomorf cu corpul $\mathbb{Q}(\sqrt{2})$.

9.52. Dacă $A = \begin{pmatrix} 2 & 3 \\ 2 & -2 \end{pmatrix} \in K$ și $M(x, y) = \begin{pmatrix} x+2y & 3y \\ 2y & x-2y \end{pmatrix} \in K$ (cu $x, y \in \mathbb{Q}$), atunci $M(x, y) = x \cdot I_2 + y \cdot A$. Să notăm că $A^2 = 10 \cdot I_2$ și atunci $M(x, y) + M(z, t) = M(x+z, y+t)$, $M(x, y) \cdot M(z, t) = M(xz+10yt, xt+yz) \in K$. Mai mult, dacă $M(x, y) \neq M(0, 0)$ avem $x^2-10y^2 \neq 0$ (căci $\sqrt{10} \notin \mathbb{Q}$) și atunci $M(x, y)^{-1} = M\left(\frac{x}{x^2-10y^2}, -\frac{y}{x^2-10y^2}\right) \in K$, de unde concluzia că $(K, +, \cdot)$ este corp comutativ. Se verifică prin calcul că $f: K \rightarrow \mathbb{Q}(\sqrt{10})$, $f(M(x, y)) = x+y\sqrt{10}$ este un izomorfism de corpuri.

9.53. Demonstrăm mai întâi următoarea Lemă:

Fie $p \geq 3$ un număr prim. Următoarele afirmații sunt echivalente:

- (i) Există $a, b \in \mathbb{Z}_p$, $a \neq \hat{0}$ sau $b \neq \hat{0}$ a.î. $a^2+b^2 = \hat{0}$;
- (ii) Există $x \in \mathbb{Z}_p$ a.î. $x^2 = -\hat{1}$;
- (iii) $p = 4k+1$, $k \in \mathbb{N}^*$.

Demonstrația lemei: Arătăm echivalența afirmațiilor (i) și (ii):

(i) \Rightarrow (ii). Să presupunem că $a^2+b^2 = \hat{0}$, unde $a, b \in \mathbb{Z}_p$ și de exemplu $b \neq \hat{0}$.

Înmulțind cu $(b^{-1})^2$ rezultă $(ab^{-1})^2 + \hat{1} = \hat{0}$ și notând $x = ab^{-1} \in \mathbb{Z}_p$ am obținut deci $x^2 = -\hat{1}$ (spunem că $-\hat{1}$ este rest pătratic modulo p).

(ii) \Rightarrow (i). Dacă există $x \in \mathbb{Z}_p$ a.î. $x^2 = -\hat{1}$, atunci $x^2 + \hat{1} = \hat{0}$, deci luăm $a = x$, $b = \hat{1}$ și (i) se verifică.

Arătăm echivalența afirmațiilor (ii) și (iii):

(ii) \Rightarrow (iii). Să presupunem că există $x \in \mathbb{Z}_p$ a.î. $x^2 = -\hat{1}$. Ridicând la puterea $\frac{p-1}{2}$ obținem $x^{p-1} = (-\hat{1})^{p-1/2}$, dar în grupul (\mathbb{Z}_p^*, \cdot) avem, conform teoremei lui Fermat, $x^{p-1} = \hat{1}$, încât egalitatea precedentă devine $\hat{1} = (-\hat{1})^{p-1/2}$.

Dacă numărul întreg $\frac{p-1}{2}$ ar fi impar am obține $\hat{1} = -\hat{1}$, adică $\hat{2} = \hat{0}$, contradicție cu faptul că $p \geq 3$. Deci $\frac{p-1}{2}$ este par, adică $\frac{p-1}{2} = 2k$ și atunci $p = 4k + 1$.

(iii) \Rightarrow (ii). Să presupunem că $p = 4k + 1$. Conform teoremei lui Fermat polinomul $f = X^{p-1} - \hat{1} \in \mathbb{Z}_p[X]$ are toate cele $p-1$ rădăcini în corpul \mathbb{Z}_p (chiar în \mathbb{Z}_p^*).

Dar $f = f_1 f_2$, unde $f_1 = X^{p-1/2} + \hat{1}$ și $f_2 = X^{p-1/2} - \hat{1}$ și atunci înseamnă că fiecare dintre polinoamele f_1 și f_2 au toate cele $\frac{p-1}{2}$ rădăcini în \mathbb{Z}_p (căci rădăcinile lui f_1 și f_2 sunt și rădăcini ale lui f).

Fie $\alpha \in \mathbb{Z}_p$ o rădăcină a lui f_1 adică $\alpha^{p-1/2} + \hat{1} = \hat{0}$.

Această egalitate se mai scrie $\alpha^{2k} + \hat{1} = \hat{0}$ și dacă notăm $x = \alpha^k \in \mathbb{Z}_p$ am obținut $x^2 + \hat{1} = \hat{0}$ adică $x^2 = -\hat{1}$. Cu aceasta **lema** este demonstrată.

Trecem la soluția problemei:

Se demonstrează ușor că mulțimea K înzestrată cu operațiile de adunare și înmulțire a matricelor este inel unitar (chiar comutativ). Atunci K este corp dacă și numai dacă orice matrice nenulă din K are determinantul un element inversabil (adică un element nenul) în corpul \mathbb{Z}_p .

Cazul $p=2$ iese din discuție pentru că matricea $A = \begin{pmatrix} \hat{1} & \hat{1} \\ -\hat{1} & \hat{1} \end{pmatrix}$ este nenulă,

dar $\det(A) = \hat{2} = \hat{0}$, deci în acest caz K nu este corp.

Considerăm cazul $p \geq 3$.

Să presupunem mai întâi că inelul K este corp și să demonstrăm că $p \equiv 3 \pmod{4}$.

Dacă prin absurd, $p \not\equiv 3 \pmod{4}$, deoarece p este prim rezultă $p \equiv 1 \pmod{4}$, adică (iii) din lema se verifică. Atunci are loc și (i) din lema, deci există $a, b \in \mathbb{Z}_p$, $a \neq \hat{0}$ sau $b \neq \hat{0}$ a.î. $a^2 + b^2 = \hat{0}$.

Luând $A = \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \in K$, rezultă că A este o matrice nenulă din K , dar

neinversabilă, căci $\det(A) = a^2 + b^2 = \hat{0}$.

Aceasta contrazice faptul că în corpul K toate elementele nenule sunt inversabile. Contradicția obținută arată că trebuie să avem $p \equiv 3 \pmod{4}$.

Reciproc, să presupunem că $p \equiv 3 \pmod{4}$ și să arătăm că inelul K este corp.

Dacă prin reducere la absurd K nu este corp, există $A = \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \in K$

matrice nenulă, neinvertibilă, adică având $\det(A) = \hat{0}$. Așadar $a \neq \hat{0}$ sau $b \neq \hat{0}$ dar $a^2 + b^2 = \hat{0}$, ceea ce înseamnă că se verifică (i) din lemă. Atunci are loc și (iii) din lemă, deci $p \equiv 1 \pmod{4}$, ceea ce contrazice presupunerea că $p \equiv 3 \pmod{4}$. Contradicția obținută arată că în mod necesar K este corp.

9.54. (i). Faptul că $(K, +, \cdot)$ este corp comutativ de probează imediat. Elementul nul este matricea $\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$, elementul unitate este matricea $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, iar inversa unei matrice nenule $\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix}$ este matricea $\begin{pmatrix} a^{-1} & 0 \\ 0 & 0 \end{pmatrix}$.

Aplicația $\varphi: K \rightarrow \mathbb{R}$, $\varphi\left(\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix}\right) = a$, este un izomorfism de corpuri.

(ii). Inelul K , deși are element unitate, nu este subinel unitar al inelului $M_2(\mathbb{R})$, căci elementele lor unitate diferă. Invertibilitatea în inelul K nu este legată de invertibilitatea în inelul $M_2(\mathbb{R})$, deci grupul $U(K)$ al unităților lui K nu este subgrup al grupului $U(M_2(\mathbb{R}))$ al unităților lui $M_2(\mathbb{R})$. Acest fapt explică de ce toate elementele nenule din K sunt inversabile în K , în timp ce, dacă le privim în $M_2(\mathbb{R})$ nici unul dintre ele nu este inversabil.

9.55. Considerăm funcția $f: A \rightarrow A$, $f(x) = \begin{cases} 0, & \text{pentru } x = 0 \\ 1, & \text{pentru } x \neq 0 \end{cases}$.

Deoarece f este funcție polinomială, există $a_0, a_1, \dots, a_n \in A$ a.î. $f(x) = a_0 + a_1x + \dots + a_nx^n$, oricare ar fi $x \in A$. Cum $f(0) = 0$ rezultă $a_0 = 0$.

Atunci $f(x) = (a_1 + a_2x + \dots + a_nx^{n-1})x = g(x) \cdot x$, unde am notat $g(x) = a_1 + a_2x + \dots + a_nx^{n-1}$. Vom arăta că orice element nenul din A este inversabil.

Fie într-adevăr, $a \in A \setminus \{0\}$.

Punând $g(a) = b$, avem $b \neq 0$ (căci dacă am avea $g(a) = 0$, atunci $f(a) = g(a) \cdot a = 0$, ceea ce contrazice definiția funcției f).

Din faptul că $b \neq 0$, deducem $f(b) = 1$, adică $g(b) \cdot b = 1$. (1)

Dar și $f(a) = 1$, ceea ce se mai scrie $g(a) \cdot a = 1$ sau $ba = 1$. (2)

Din (1) și (2) deducem că $g(b)=g(b) \cdot 1=g(b) \cdot ba=1 \cdot a=a$ și atunci (1) devine $ab=1$. (3)

Egalitățile (2) și (3) arată că elementul a este inversabil în inelul A , inversul său fiind elementul b . Deci $(A, +, \cdot)$ este corp.

9.56. (i). Se verifică imediat prin calcul direct.

(ii). Faptul că f, Δ, N sunt morfisme de grupuri se probează ușor.

Pentru Δ avem $\Delta(AB)=\det(AB)=\det(A) \cdot \det(B)=\Delta(A) \cdot \Delta(B)$, oricare ar fi $A, B \in K_d^*$.

Pentru N avem: $N(z)=z \cdot \bar{z}$, oricare ar fi $z \in \mathbb{Q}(\sqrt{d})^*$, unde \bar{z} este conjugatul pătratic al lui z , adică putem scrie $N(z_1 z_2) = (z_1 z_2)(\overline{z_1 z_2}) = z_1 z_2 \overline{z_1 z_2} = (z_1 \overline{z_1})(z_2 \overline{z_2}) = N(z_1)N(z_2)$, oricare ar fi $z_1, z_2 \in \mathbb{Q}(\sqrt{d})^*$.

Demonstrăm că $\Delta \circ f = N$. Fie $z = a + b\sqrt{d} \in \mathbb{Q}(\sqrt{d})^*$, oarecare.

Avem:

$$\begin{aligned} (\Delta \circ f)(z) &= \Delta(f(z)) = \Delta(f(a + b\sqrt{d})) = \Delta\left(\begin{pmatrix} a & bd \\ b & a \end{pmatrix}\right) = \det\begin{pmatrix} a & bd \\ b & a \end{pmatrix} = a^2 - db^2 = \\ &= N(a + b\sqrt{d}) = N(z). \end{aligned}$$

9.57. Avem de exemplu $(1, 0) \cdot (0, 1) = (0, 0)$, deci $K_1 \times K_2$ nu este corp (având divizori ai lui zero).

9.58. Notăm $A = K_1 \times K_2 \times K_3$ și $B = K_4 \times K_5$. Considerăm în A elementele $e_1 = (1, 0, 0)$, $e_2 = (0, 1, 0)$, $e_3 = (0, 0, 1)$ și în B elementele $f_1 = (1, 0)$, $f_2 = (0, 1)$. Aceste elemente satisfac relațiile: (1) $e_1^2 = e_1$, $e_2^2 = e_2$, $e_3^2 = e_3$, $f_1^2 = f_1$, $f_2^2 = f_2$ (sunt elemente idempotente);

(2) $e_i e_j = e_j e_i = 0$, $f_i f_j = f_j f_i = 0$, pentru $i \neq j$ (elementele e_1, e_2, e_3 respectiv f_1, f_2 sunt ortogonale);

(3) $e_1 + e_2 + e_3 = (1, 1, 1)$, $f_1 + f_2 = (1, 1)$.

Presupunem prin absurd că există un izomorfism de inele $\varphi: A \rightarrow B$.

Deoarece relațiile (1), (2), (3) sunt algebrice rezultă că $\varphi(e_i) \in B$ ($i \in \{1, 2, 3\}$) sunt elemente idempotente ortogonale nenule. Fie $(x, y) \in B$ un element idempotent. Atunci $x^2 = x$ în K_4 și $y^2 = y$ în K_5 . Dar ecuația $z^2 = z$ echivalentă cu $z(z-1) = 0$ are în orice corp K soluțiile $z_1 = 0$ și $z_2 = 1$. Rezultă că singurele elemente idempotente ale lui B sunt $0, f_1, f_2, 1 = (1, 1)$. Rezultă că în B nu există trei elemente idempotente ortogonale, nenule, ceea ce contrazice existența lui φ .

§10. Inele de polinoame

10.1. Arătăm simultan (i) și (ii).

Vom analiza întâi cazul când I are un singur element.

Fie P_s mulțimea polinoamelor cu coeficienți în A într-o nedeterminată de grad cel mult $s \geq 0$.

P_s este echipotentă cu mulțimea funcțiilor $\{0, 1, \dots, s\} \rightarrow A$, adică cu A^{s+1} .

Obținem că P_s sunt mulțimi finite dacă A este finit și au cardinalul lui A în caz contrar (A^q are cardinalul lui A când A este infinită iar $q \geq 1$ este număr natural).

Pe de altă parte, $A[X] = A[X; I] = \bigcup_{s \geq 0} P_s$.

Deci $A[X]$ este cel mult numărabilă dacă A este mulțime finită și are cardinalul lui A în caz contrar (o reuniune numărabilă de mulțimi finite este cel mult numărabilă, iar o reuniune numărabilă de mulțimi infinite de același cardinal u are cardinalul u).

Observăm că $A[X]$ nu poate fi finită conținând $\{X^n\}_{n \geq 0}$, de unde rezultă că $A[X]$ este numărabilă când A este mulțime finită.

Am arătat deci (i) și (ii) pentru $\text{card } I = 1$.

În continuare aplicăm inducția ținând cont de faptul că $A[X, Y] = A[X][Y]$.

(iii). Observăm că $A[X; I] = \bigcup_{\substack{J \subset I \\ J \text{ finita}}} A[X; J]$.

Prin (i) $A[X; J]$ sunt toate numărabile. Deci $A[X; I]$ este reuniunea unei familii de mulțimi numărabile indexate de mulțimea părților finite ale lui I care are cardinalul lui I (mulțimea părților finite ale unei mulțimi M infinite are cardinalul lui M).

Deci $A[X; I]$ are cardinalul lui I (reuniunea unei familii de mulțimi numărabile indexate de o mulțime infinită de cardinal u are cardinalul u).

10.2. Fie A o mulțime finită cu n elemente iar $u: \mathbb{Z}_n \rightarrow A$ o bijecție oarecare. Considerăm pe A structura de inel dată de problema 7.2.

Dacă A este o mulțime infinită atunci considerăm inelul $\mathbb{Z}[X; A]$ al polinoamelor în nedeterminatele $\{X_a\}_{a \in A}$ cu coeficienți întregi. Conform problemei 10.1., inelul $\mathbb{Z}[X; A]$ are cardinalul lui A , adică există o bijecție

$u: \mathbb{Z}[X;A] \rightarrow A$. Structura de inel a lui $\mathbb{Z}[X;A]$ induce prin u o structură de inel pe A .

10.3. Fie G un subgrup de ordin n al lui $U(A)$ și $d = \text{cel mai mic multiplu comun al ordinelor elementelor din } G$. Evident $d|n$.

Fie $d = p_1^{\alpha_1} \dots p_r^{\alpha_r}$ descompunerea în factori primi a lui d . Atunci există elementele $x_1, \dots, x_r \in G$ a.î. $p_i^{\alpha_i} | \text{ord } x_i$, adică $\text{ord } x_i = p_i^{\alpha_i} \cdot t_i$, $t_i \in \mathbb{N}$. Se verifică ușor că $x = x_1^{t_1} \dots x_r^{t_r}$ are ordinul d .

Ecuția $X^d - 1 = 0$ are cel mult d rădăcini în corpul de fracții al lui A .

Cum toate elementele lui G constituie rădăcini ale ecuației date, deducem că $n = d$. Deci G este ciclic.

10.4. (i). Fie K un corp finit. Conform teoremei lui Wedderburn corpul K este comutativ. Considerăm grupul abelian finit (K^*, \cdot) și calculăm produsul elementelor sale.

În orice grup abelian finit produsul elementelor grupului este egal cu produsul elementelor de ordin 2 (căci elementele de ordin mai mare ca 2 se pot grupa în perechi, fiecare cu inversul său și astfel produsul lor este egal cu elementul unitate; de asemenea, mai observăm că singurul element de ordin 1 este elementul unitate și în felul acesta produsul elementelor de ordin diferit de 2 este egal cu elementul unitate).

Căutăm elementele de ordin 2 din grupul (K^*, \cdot) . Fie x un astfel de element. Atunci $x^2 = 1$ și $x \neq 1$. Dar polinomul $X^2 - 1 \in K[X]$ are în corpul K doar rădăcinile ± 1 și vom avea $x = -1$. Deci unicul element de ordin 2 din grupul (K^*, \cdot) este -1 și astfel produsul elementelor acestui grup este egal cu -1 .

(ii). Considerăm corpul \mathbb{Z}_p al claselor de resturi modulo p .

Conform punctului (i) avem $1 \cdot 2 \cdot \dots \cdot \overset{\wedge}{p-1} = -1$, adică $(p-1)! \equiv -1 \pmod{p}$, deci $p | (p-1)! + 1$.

Observație. Este valabilă și *reciproca teoremei lui Wilson*: Dacă $p \geq 2$ este un număr natural a.î. $p | (p-1)! + 1$, atunci p este număr prim.

Într-adevăr, fie q un divizor al lui p , $0 < q < p$. Cum $p | (p-1)! + 1$ rezultă că și $q | (p-1)! + 1$. Dar $q | (p-1)!$. Scăzând cele două relații obținem $q | 1$, adică $q = 1$.

Deci singurul divizor al lui p , mai mic decât p este 1, și în consecință p este prim.

10.5. (i). Să presupunem că polinomul f este inversabil în $A[X]$ și fie $g=b_0+b_1X+\dots+b_mX^m \in A[X]$ inversul său. Din $fg=1$ deducem relațiile următoare, ce leagă coeficienții celor două polinoame:

$$\begin{cases} a_0b_0 = 1 \\ a_0b_1 + a_1b_0 = 0 \\ a_0b_2 + a_1b_1 + a_2b_0 = 0 \\ \dots\dots\dots \\ a_{n-1}b_m + a_nb_{m-1} = 0 \\ a_nb_m = 0 \end{cases}$$

Din ultimele două relații (înmulțind ambii membri ai penultimei relații cu a_n și folosind ultima) obținem $a_n^2b_{m-1}=0$. Înmulțind ambii membri ai antepenultimei relații cu a_n obținem $a_n^3b_{m-2}=0$. Din aproape în aproape, obținem relațiile $a_n^kb_{m-k+1}=0$ ($k \geq 1$) și, în final, pentru $k=m+1$, $a_n^{m+1}b_0=0$. Acum, înmulțind ambii membri ai acestei relații cu a_0 obținem că $a_n^{m+1}=0$, adică a_n este nilpotent. Polinomul a_nX^n fiind nilpotent, rezultă acum că $f-a_nX^n = a_0+a_1X+\dots+a_{n-1}X^{n-1}$ este inversabil (și are gradul mai mic decât gradul lui f). Așadar un raționament inductiv ne conduce la concluzia că $a_n, a_{n-1}, \dots, a_2, a_1$ sunt nilpotente în A ; a_0 este evident inversabil în A .

Reciproc, dacă a_0 este inversabil în A , el rămîne inversabil și ca element al lui $A[X]$. Dacă a_1 este nilpotent în A , atunci a_1X este nilpotent în $A[X]$; așadar, polinomul a_0+a_1X este inversabil. Dacă a_2 este nilpotent în A , atunci a_2X^2 este nilpotent în $A[X]$; așadar, polinomul $a_0+a_1X+a_2X^2$ este inversabil. Din aproape în aproape, obținem că dacă a_1, a_2, \dots, a_n sunt nilpotente (în A), atunci polinomul f este inversabil în $A[X]$.

(ii). Conform celor stabilite în problema **6.36.**, dacă f este nilpotent în $A[X]$ atunci polinomul $1+fX=1+a_0X+a_1X^2+\dots+a_nX^{n+1}$ este inversabil în $A[X]$. Deci a_0, a_1, \dots, a_n sunt elemente nilpotente în A . Reciproc, este evident, căci elementele nilpotente formează un ideal.

(iii). Polinomul f , având gradul ≥ 0 , este nenul. Dacă există $a \in A, a \neq 0$, a.î. $a \cdot f=0$, interpretând pe a ca polinom de gradul zero, rezultă că f este divizor al lui zero.

Să presupunem că f este divizor al lui zero și fie $g=b_0+b_1X+\dots+b_mX^m$ un polinom nenul, de grad minim, pentru care $f \cdot g=0$. Atunci $a_n \cdot b_m=0$; de aici rezultă că $a_n \cdot g$ este un polinom de grad mai mic decât gradul lui g , iar $(a_n \cdot g) \cdot f=0$; deci $a_n \cdot g=0$. Printr-un raționament inductiv putem stabili că $a_{n-1} \cdot g=0, a_{n-2} \cdot g=0, \dots, a_1 \cdot g=0, a_0 \cdot g=0$. De aici, $a_i b_j=0$ pentru orice indici i, j . Întrucât am presupus că $g \neq 0$, există un coeficient $b_k \neq 0$.

Însă $a_0 \cdot b_k = a_1 \cdot b_k = \dots = a_n \cdot b_k=0$, astfel că avem $b_k \cdot f=0$.

10.6. Fie (x, y) o soluție a ecuației date. Dacă $x = \hat{0}$ rezultă și $y = \hat{0}$ și reciproc. Așadar o soluție este $(\hat{0}, \hat{0})$, iar celelalte soluții (dacă există) vor avea ambele componente nenule.

Vom încerca să caracterizăm aceste soluții.

Conform teoremei lui Fermat, avem $\alpha^{p-1} = \hat{1}$, pentru orice $\alpha \in \mathbb{Z}_p \setminus \{\hat{0}\}$. Aceasta înseamnă că polinomul $f = X^{p-1} - \hat{1} \in \mathbb{Z}_p[X]$ are toate cele $p-1$ rădăcini în corpul \mathbb{Z}_p . Dar putem scrie

$$f = X^{p-1} - \hat{1} = \left(X^{p-1/2} \right)^2 - \hat{1} = \left(X^{p-1/2} - \hat{1} \right) \left(X^{p-1/2} + \hat{1} \right) = f_1 \cdot f_2,$$

unde $f_1 = \left(X^{p-1/2} - \hat{1} \right)$ și $f_2 = \left(X^{p-1/2} + \hat{1} \right)$. Fiecare dintre polinoamele f_1 și f_2 au gradul $\frac{p-1}{2}$, deci au câte $\frac{p-1}{2}$ rădăcini în corpul \mathbb{Z}_p .

$$\text{Notând } A = \{ \alpha \in \mathbb{Z}_p^* \mid f_1(\alpha) = \hat{0} \} = \{ \alpha \in \mathbb{Z}_p^* \mid \alpha^{p-1/2} = \hat{1} \} \text{ și}$$

$$B = \{ \alpha \in \mathbb{Z}_p^* \mid f_2(\alpha) = \hat{0} \} = \{ \alpha \in \mathbb{Z}_p^* \mid \alpha^{p-1/2} = -\hat{1} \}$$

avem $\mathbb{Z}_p^* = A \cup B$, unde mulțimile A și B sunt disjuncte, fiecare având câte $\frac{p-1}{2}$ elemente.

Arătăm acum că dacă $x, y \in \mathbb{Z}_p^*$, cuplul (x, y) este soluție a ecuației considerate dacă și numai dacă $(x, y) \in (A \times B) \cup (B \times A)$.

Într-adevăr, dacă (x, y) este soluție cu $x, y \in \mathbb{Z}_p^* = A \cup B$, dacă de exemplu $x \in A$ avem $x^{p-1/2} = \hat{1}$ și atunci din ecuație rezultă $y^{p-1/2} = -\hat{1}$, deci $y \in B$, adică $(x, y) \in A \times B$. Dacă am fi presupus $x \in B$, rezultă $y \in A$, adică $(x, y) \in B \times A$.

Prin urmare, orice soluție (x, y) cu componente nenule aparține mulțimii $(A \times B) \cup (B \times A)$.

Reciproc, dacă $(x, y) \in (A \times B) \cup (B \times A)$, avem $x^{p-1/2} = \hat{1}$, $y^{p-1/2} = -\hat{1}$ sau $x^{p-1/2} = -\hat{1}$, $y^{p-1/2} = \hat{1}$, deci oricum $x^{p-1/2} + y^{p-1/2} = \hat{0}$, adică (x, y) este soluție pentru ecuația considerată.

În urma acestor considerații rezultă că mulțimea soluțiilor ecuației date este $\{(\hat{0}, \hat{0})\} \cup (A \times B) \cup (B \times A)$.

Cardinalul acestei mulțimi este $2 \cdot \left(\frac{p-1}{2}\right)^2 + 1 = \frac{(p-1)^2}{2} + 1$, deoarece cele trei mulțimi ce apar în reuniunea de mai sus sunt disjuncte două câte două.

10.7. Pentru fiecare $k \in \mathbb{N}^*$, scriind matricea $A_k + \alpha B_k$ și dezvoltând conform definiției, constatăm că $\det(A_k + \alpha B_k)$ este un polinom în α , în care termenul ce conține pe α^n are coeficientul $\det(B_k) \neq 0$. Deci acest polinom este nenul (are gradul n) și în consecință mulțimea rădăcinilor sale reale este finită (eventual poate fi mulțimea vidă).

Să notăm $X_k = \{\alpha \in \mathbb{R} \mid \det(A_k + \alpha B_k) = 0\}$, $k = 1, 2, 3, \dots$

Mulțimea $X = \bigcup_{k \in \mathbb{N}^*} X_k$ este o reuniune numărabilă de mulțimi finite, deci este numărabilă.

Deoarece \mathbb{R} nu este numărabilă, rezultă că mulțimea $\mathbb{R} \setminus X$ este infinită. Dar pentru $\alpha \in \mathbb{R} \setminus X$, avem $\alpha \notin X_k$, oricare ar fi $k \in \mathbb{N}^*$, deci $\det(A_k + \alpha B_k) \neq 0$, adică $A_k + \alpha B_k$ este inversabilă, oricare ar fi $k \in \mathbb{N}^*$.

10.8. (i) \Rightarrow (ii). Fie $A = \{a_1, \dots, a_k\}$ un corp finit, deci comutativ. Un polinom $P \in A[X]$ de grad $n > 1$ admite în corpul comutativ A cel mult n rădăcini distincte.

Fie acum $f: A \rightarrow A$ o funcție arbitrară. Considerăm polinomul de interpolare al lui Lagrange:

$$Q = \sum_{i=1}^k \frac{(X - a_1)(X - a_2) \dots (X - a_{i-1})(X - a_{i+1}) \dots (X - a_n)}{(a_i - a_1)(a_i - a_2) \dots (a_i - a_{i-1})(a_i - a_{i+1}) \dots (a_i - a_n)} \cdot f(a_i).$$

Avem $Q \in A[X]$ și notând \tilde{Q} funcția polinomială asociată lui Q , se observă ușor că $\tilde{Q}(a_i) = f(a_i)$, $i = 1, \dots, k$.

Aceasta înseamnă că $f = \tilde{Q}$, deci funcția f este polinomială.

(ii) \Rightarrow (i). Presupunem îndeplinite ipotezele de la (ii).

Demonstrăm mai întâi că A este inel finit.

Să presupunem prin reducere la absurd că A este infinit și să considerăm funcția $f: A \rightarrow A$, $f(x) = \begin{cases} 0, & \text{pentru } x \neq 0 \\ 1, & \text{pentru } x = 0 \end{cases}$.

Conform lui (ii) există un polinom $P = a_0 + a_1 X + \dots + a_n X^n \in A[X]$ cu $f = \tilde{P}$.

Avem $n \geq 1$, căci dacă $n \leq 0$, ar însemna că P este un polinom constant, deci $\tilde{P} = f$ ar fi o funcție constantă, ceea ce nu este posibil, deoarece inelul A având cel puțin două elemente, avem $0 \neq 1$.

Așadar polinomul P de grad $n \geq 1$ are în A o infinitate de rădăcini (toate elementele nenule din A), contradicție cu (ii). Deci A este finit.

Demonstrăm că A este un domeniu de integritate.

Să presupunem, prin reducere la absurd, că există $a, b \in A$, $a \neq 0$, $b \neq 0$ cu $ab = 0$. Atunci polinomul $P \in A[X]$, $P = aX$, care are gradul 1, admite în A două rădăcini distincte și anume 0 și b , contradicție cu (ii).

Deci A este domeniu de integritate.

Dar un domeniu de integritate finit este corp, deci A este corp finit.

10.9. (i). Să presupunem mai întâi că $f = \hat{a} + \hat{b}X$ este inversabil. Atunci există polinomul $\hat{c}_0 + \hat{c}_1 X + \dots + \hat{c}_m X^m$ a.î. $(\hat{a} + \hat{b}X)(\hat{c}_0 + \hat{c}_1 X + \dots + \hat{c}_m X^m) = \hat{1}$.

$$\text{Rezultă } \hat{a}\hat{c}_0 = \hat{1} \quad (0)$$

$$\hat{a}\hat{c}_1 + \hat{b}\hat{c}_0 = \hat{0} \quad (1)$$

$$\hat{a}\hat{c}_2 + \hat{b}\hat{c}_1 = \hat{0} \quad (2)$$

.....

$$\hat{a}\hat{c}_m + \hat{b}\hat{c}_{m-1} = \hat{0} \quad (m)$$

$$\hat{b}\hat{c}_m = \hat{0} \quad (m+1)$$

Din (0) deducem că \hat{a} și \hat{c}_0 sunt inversabile, ceea ce este echivalent cu $p \nmid a$ și $p \nmid c_0$.

Dacă am presupune că $p \mid b$, atunci din (1), (2), ..., (m) rezultă succesiv că $\hat{c}_1, \hat{c}_2, \dots, \hat{c}_m$ sunt inversabile și atunci din (m+1) rezultă $\hat{b} = \hat{0}$, de unde deducem că $p^r \mid b$, adică $p \mid b$, contradicție.

Prin urmare, în mod necesar $p \nmid b$.

Reciproc, să presupunem că $p \nmid a$ și $p \nmid b$ și să arătăm că polinomul $\hat{a} + \hat{b}X$ este inversabil în inelul $\mathbb{Z}_p^r[X]$.

Fie $b = pc$; atunci $\hat{b}^r = p^r \cdot \hat{c}^r = \hat{0}$ și rezultă

$$\hat{a}^r = \hat{a}^r + \hat{0} = \hat{a}^r + (\hat{b}X)^r = (\hat{a} + \hat{b}X - \hat{b}X)^r + (\hat{b}X)^r = M_{(\hat{a} + \hat{b}X)}.$$

Deci există $g \in \mathbb{Z}_{p^r}[X]$ a.î. $\hat{a}^r = (\hat{a} + \hat{b}X)g(X)$ sau

$\bigwedge (\hat{a} + \hat{b}X)[(a^{-1})^r g(X)] = \hat{1}$, ceea ce arată că polinomul $f = \hat{a} + \hat{b}X$ este inversabil.

(ii). Fie $A = \{a \mid 0 \leq a \leq p^r - 1, p \nmid a\}$ și $B = \{b \mid 0 \leq b \leq p^r - 1, p \mid b\}$.

Evident B are p^{r-1} elemente iar A are $p^r - p^{r-1}$ elemente.

Notând F mulțimea polinoamelor de gradul cel mult 1, inversabile din inelul $\mathbb{Z}_{p^r}[X]$, deducem pe baza punctului (i) că aplicația $\varphi: F \rightarrow A \times B$,

$\varphi(\hat{a} + \hat{b}X) = (a, b)$ este o bijecție.

Rezultă atunci egalitatea:

$$\text{card}(F) = \text{card}(A) \cdot \text{card}(B) = (p^r - p^{r-1})p^{r-1} = p^{2(r-1)}(p-1).$$

10.10. Evident $\varphi_n(fg) = \varphi_n(f)\varphi_n(g)$, oricare ar fi $f, g \in A[X]$. Aceasta arată că φ_n este endomorfism al inelului de polinoame $A[X]$ dacă și numai dacă $\varphi_n(f+g) = \varphi_n(f) + \varphi_n(g)$, adică echivalent $(f+g)^n = f^n + g^n$, oricare ar fi $f, g \in A[X]$. Cum $M \neq \emptyset$ există $n_0 \in M$, deci avem $(f+g)^{n_0} = f^{n_0} + g^{n_0}$, oricare ar fi $f, g \in A[X]$. Luând $f=g=1$ obținem $(1+1)^{n_0} = 1+1$, adică $(2^{n_0} - 2) \cdot 1 = 0$.

Există așadar numerele întregi $k \geq 2$ pentru care $k \cdot 1 = 0$ (de exemplu $k = 2^{n_0} - 2$) și fie atunci $p \geq 2$ minim cu $p \cdot 1 = 0$. Arătăm că p este număr prim.

Într-adevăr, dacă p nu ar fi prim am avea $p = p_1 p_2$ cu $1 < p_1 < p$ și $1 < p_2 < p$ și din $p \cdot 1 = 0$ ar rezulta $(p_1 \cdot 1)(p_2 \cdot 1) = 0$ deci $p_1 \cdot 1 = 0$ sau $p_2 \cdot 1 = 0$, (căci A este inel integru) contrar minimalității lui p .

Mai remarcăm că pentru $k \in \mathbb{Z}$ avem echivalența $k \cdot 1 = 0 \Leftrightarrow k \equiv 0 \pmod{p}$ căci implicația \Leftarrow este evidentă, iar pentru implicația \Rightarrow folosim împărțirea cu rest a lui k prin p și minimalitatea lui p a.î. $p \cdot 1 = 0$.

Demonstrăm egalitatea de mulțimi cerută prin dublă incluziune, p având semnificația de mai înainte (caracteristica inelului A).

„ \subseteq ” Fie $n \in M$, deci $(f+g)^n = f^n + g^n$, oricare ar fi $f, g \in A[X]$. Luând $f=X$, $g=1$ avem $(X+1)^n = X^n + 1$, adică $C_n^1 X^{n-2} + C_n^2 X^{n-3} + \dots + C_n^{n-2} X + C_n^{n-1} = 0$ (am ținut seama că din A integru rezultă că și $A[X]$ este integru și am simplificat prin X).

Ultima egalitate arată că în inelul A avem $C_n^1 \cdot 1 = 0$, $C_n^2 \cdot 1 = 0, \dots, C_n^{n-2} \cdot 1 = 0$, $C_n^{n-1} \cdot 1 = 0$ și de aici rezultă că în \mathbb{Z} avem: $C_n^1 \equiv 0 \pmod{p}$, $C_n^2 \equiv 0 \pmod{p}, \dots, C_n^{n-1} \equiv 0 \pmod{p}$.

Se știe atunci (vezi observația din final) că există $k \in \mathbb{Z}$, $k \geq 1$ a.î. $n = p^k$.

„ \supseteq ” Fie $n=p^k$ cu $k \geq 1$. Tot datorită observației din final avem $C_n^1 \equiv 0(\text{mod } p)$, $C_n^2 \equiv 0(\text{mod } p)$, ..., $C_n^{n-1} \equiv 0(\text{mod } p)$, deci:

$$(f+g)^n = f^n + C_n^1 f^{n-1} g + \dots + C_n^{n-1} f g^{n-1} + g^n = f^n + g^n,$$

ceea ce arată că φ_n este endomorfism al inelului $A[X]$ și prin urmare $n \in M$.

Unicitatea lui p este clară: Dacă am mai avea $q > 0$ număr prim, cu $M = \{q, q^2, q^3, \dots, q^k, \dots\}$ din egalitatea $\{p, p^2, p^3, \dots, p^k, \dots\} = \{q, q^2, q^3, \dots, q^k, \dots\}$ rezultă evident $p=q$.

Observație. Am utilizat rezultatul cunoscut (vezi, de exemplu, [15]) următor:

$$(C_n^1, C_n^2, \dots, C_n^{n-1}) = \begin{cases} p, & \text{daca } n = p^k, \text{ } p \text{ prim, } k \geq 1 \\ 1, & \text{daca } n \text{ are cel puțin 2 factori primi distincti} \end{cases}$$

10.11. Fie A un astfel de inel. A fiind subinel unitar al lui $A[X]$ el trebuie să fie izomorf cu un subinel unitar al lui $(\mathbb{Z}, +, \cdot)$. În particular, $(A, +)$ trebuie să fie izomorf cu un subgrup nenul al lui $(\mathbb{Z}, +)$, deci să existe un $n \in \mathbb{N}^*$ a.î. $A \simeq n\mathbb{Z}$.

Din $1 \in A$ rezultă $n=1$ și atunci $\mathbb{Z} \simeq \mathbb{Z}[X]$ (\mathbb{Z} este ciclic și evident $\mathbb{Z}[X]$ nu este ciclic), contradicție.

10.12. „ \Leftarrow ”. Presupunem că inelele A și \mathbb{Z} sunt izomorfe și demonstrăm că inelele $A[X]$ și $\mathbb{Z}[X]$ sunt izomorfe.

Într-adevăr, dacă $\varphi: \mathbb{Z} \rightarrow A$ este un izomorfism de inele, definim aplicația $\bar{\varphi}: \mathbb{Z}[X] \rightarrow A[X]$ prin $\bar{\varphi}(a_0 + a_1 X + \dots + a_n X^n) = \varphi(a_0) + \varphi(a_1) X + \dots + \varphi(a_n) X^n$, pentru orice polinom $a_0 + a_1 X + \dots + a_n X^n \in \mathbb{Z}[X]$.

Se demonstrează că $\bar{\varphi}$ este izomorfism de inele.

„ \Rightarrow ”. Reciproc, să presupunem că inelele $A[X]$ și $\mathbb{Z}[X]$ sunt izomorfe și demonstrăm că inelele \mathbb{Z} și A sunt izomorfe.

Fie $\psi: \mathbb{Z}[X] \rightarrow A[X]$ un izomorfism de inele. Atunci ψ este un morfism unitar de inele, deci $\psi(1) = 1_A$. Rezultă imediat că pentru orice $k \in \mathbb{Z}$, $\psi(k) = k \cdot 1_A$, ceea ce arată că $\psi(\mathbb{Z}) \subseteq A$.

Deoarece \mathbb{Z} este domeniu de integritate, rezultă că inelul său de polinoame $\mathbb{Z}[X]$ este domeniu de integritate și cum $A[X] \simeq \mathbb{Z}[X]$, vom avea că și $A[X]$ este domeniu de integritate și de aici rezultă că A este domeniu de integritate.

Demonstrăm acum că $\psi^{-1}(A) \subseteq \mathbb{Z}$, unde ψ^{-1} este izomorfismul invers al lui ψ . Să presupunem prin absurd că nu există această incluziune, adică există $\alpha \in A$ cu $\psi^{-1}(\alpha) \notin \mathbb{Z}$.

Atunci $\psi^{-1}(\alpha) = a_0 + a_1X + \dots + a_nX^n \in \mathbb{Z}[X]$, unde $n \in \mathbb{N}^*$ și $a_n \neq 0$.

Observăm că $\psi(X) \notin A$, căci în caz contrar, cum avem $\psi(\mathbb{Z}) \subseteq A$, rezultă $\psi(\mathbb{Z}[X]) \subseteq A$, ceea ce face ca morfismul $\psi: \mathbb{Z}[X] \rightarrow A[X]$ să nu fie surjectiv.

Fie deci $\psi(X) = b_0 + b_1X + \dots + b_pX^p \in A[X]$, unde $p > 0$ și $b_p \neq 0_A$.

Avem atunci

$$\begin{aligned} \alpha &= \psi(\psi^{-1}(\alpha)) = \psi(a_0 + a_1X + \dots + a_nX^n) = \psi(a_0) + \psi(a_1)\psi(X) + \dots + \psi(a_n)\psi(X)^n = \\ &= \psi(a_0) + \psi(a_1)(b_0 + b_1X + \dots + b_pX^p) + \dots + \psi(a_n)(b_0 + b_1X + \dots + b_pX^p)^n. \end{aligned}$$

Această egalitate este însă o contradicție, căci α este un polinom de gradul 0, în timp ce polinomul scris ultima dată are gradul $np > 0$, căci coeficientul său dominant este $\psi(a_n)b_p^n \neq 0_A$ (ținem seama că A este domeniu de integritate).

Deci am demonstrat că $\psi^{-1}(A) \subseteq \mathbb{Z}$.

Notăm cu ψ_1 respectiv ψ_1^{-1} restricțiile lui ψ și ψ^{-1} respectiv la \mathbb{Z} și la A . Din cele demonstrate anterior, rezultă că avem $\psi_1: \mathbb{Z} \rightarrow A$, $\psi_1^{-1}: A \rightarrow \mathbb{Z}$. Evident ψ_1 și ψ_1^{-1} sunt morfisme de inele și $\psi_1 \circ \psi_1^{-1} = 1_A$, $\psi_1^{-1} \circ \psi_1 = 1_{\mathbb{Z}}$, ceea ce înseamnă că $\psi_1: \mathbb{Z} \rightarrow A$ este morfism inversabil de inele, adică izomorfism de inele.

10.13. „ \Leftarrow ”. Să presupunem că inelele K și A sunt izomorfe și să demonstrăm că și inelele $K[X]$ și $A[X]$ sunt izomorfe.

Într-adevăr, dacă $\varphi: K \rightarrow A$ este un izomorfism de inele atunci $\psi: K[X] \rightarrow A[X]$, $\psi(a_0 + a_1X + \dots + a_nX^n) = \varphi(a_0) + \varphi(a_1)X + \dots + \varphi(a_n)X^n$ este un izomorfism de inele.

„ \Rightarrow ”. Reciproc, să presupunem că inelele $K[X]$ și $A[X]$ sunt izomorfe și să demonstrăm că și inelele K și A sunt izomorfe.

Fie $\psi: K[X] \rightarrow A[X]$ un izomorfism de inele.

Inelul $K[X]$ fiind domeniu de integritate, rezultă că și $A[X]$ este domeniu de integritate și de aici rezultă că A este domeniu de integritate.

Polinoamele inversabile din inelul $K[X]$ sunt elementele nenule din corpul K , iar polinoamele inversabile din $A[X]$ sunt elementele inversabile din inelul A .

Ținând seama că izomorfismul ψ duce elementele inversabile din $K[X]$ în elementele inversabile din $A[X]$ și că $\psi(0_K) = 0_A$, rezultă că $\psi(K) \subseteq A$.

Analog cu demonstrația problemei **10.12.** se arată și incluziunea $\psi^{-1}(A) \subseteq K$ (reducere la absurd).

Atunci, avem restricțiile ψ_1 și ψ_1^{-1} ale lui ψ și ψ^{-1} respectiv la K și A : $\psi_1: K \rightarrow A$, $\psi_1^{-1}: A \rightarrow K$. Evident, ψ_1 și ψ_1^{-1} sunt morfisme de inele și cum $\psi_1 \circ \psi_1^{-1} = 1_A$, $\psi_1^{-1} \circ \psi_1 = 1_K$, ele vor fi inversabile.

Aceasta înseamnă că inelele A și K sunt izomorfe.

10.14. Dacă inelele $k[X]$ și $K[X]$ ar fi izomorfe, atunci grupurile elementelor inversabile din cele două inele ar fi izomorfe.

Se arată ușor (prin trecere la grade) că un polinom din inelul $K[X]$ este inversabil dacă și numai dacă este un polinom de gradul zero, adică dacă și numai dacă aparține lui K^* . Deci grupul elementelor inversabile din $K[X]$ este $U(K[X]) = K^*$. Analog $U(k[X]) = k^*$.

Prin urmare, dacă inelele $k[X]$ și $K[X]$ ar fi izomorfe, ar rezulta că grupurile (k^*, \cdot) și (K^*, \cdot) ar fi izomorfe, contradicție cu ipoteza.

Deci, în ipoteza dată, cele două inele nu sunt izomorfe.

Luând $k = \mathbb{Q}$ și $K = \mathbb{R}$ avem $(\mathbb{Q}^*, \cdot) \neq (\mathbb{R}^*, \cdot)$, căci \mathbb{Q}^* este mulțime numărabilă, iar \mathbb{R}^* nu este numărabilă.

Luând $k = \mathbb{R}$ și $K = \mathbb{C}$ avem că $(\mathbb{R}^*, \cdot) \neq (\mathbb{C}^*, \cdot)$, deoarece în (\mathbb{R}^*, \cdot) singurele elemente de ordin finit sunt ± 1 în timp ce în (\mathbb{C}^*, \cdot) orice rădăcină a unității, complexă, nereală, de ordin mai mare ca 2, este element de ordin finit.

Atunci, conform celor stabilite anterior, deducem că inelele $\mathbb{Q}[X]$ și $\mathbb{R}[X]$, respectiv $\mathbb{R}[X]$ și $\mathbb{C}[X]$ nu sunt izomorfe.

10.15. Inelele \mathbb{R} și $\mathbb{R}[X]$ nu pot fi izomorfe pentru că \mathbb{R} este corp în timp ce $\mathbb{R}[X]$ nu este corp (polinoamele inversabile din inelul $\mathbb{R}[X]$ sunt polinoamele constante nenule).

Dacă considerăm însă \mathbb{Q} -spațiile vectoriale \mathbb{R} și $\mathbb{R}[X]$, ambele au dimensiunea c , deci sunt spații vectoriale izomorfe.

În particular, rezultă că grupurile abeliene $(\mathbb{R}, +)$ și $(\mathbb{R}[X], +)$ sunt izomorfe.

10.16. Fie φ un automorfism al lui $A[X]$. Avem $\varphi(0) = 0$ și să presupunem că $\varphi(X) = b_0 + b_1X + \dots + b_mX^m$ are gradul m . Dacă $f = a_0 + a_1X + \dots + a_nX^n$ este un polinom de grad $n \geq 0$, atunci $\varphi(f) = \varphi(a_0) + \varphi(a_1)\varphi(X) + \dots + \varphi(a_n)\varphi(X)^n$, deci $\varphi(f)$ este un polinom de gradul mn .

În particular, dacă f este un element nenul al inelului A (element asimilat cu un polinom de gradul 0), atunci $\varphi(f)$ va fi un polinom de gradul 0, deci va fi și el un element al inelului A .

Deci putem defini o funcție $\psi:A \rightarrow A$, prin $\psi(a)=\varphi(a)$.

Această funcție este un automorfism al inelului A .

Din ipoteză φ este surjectiv, deci există un polinom f a.î. $\varphi(f)=X$.

În consecință, $m \cdot \text{grad}(f)=1$, ceea ce înseamnă că $m=1$ și deci $\varphi(X)=b_0+b_1X$ cu $b_1 \neq 0$.

Observăm că automorfismul φ al lui $A[X]$ este perfect determinat de imaginea $\varphi(X)$ și de automorfismul ψ al lui A , deoarece $\varphi(a_0+a_1X+\dots+a_nX^n)=\psi(a_0)+\psi(a_1)\varphi(X)+\dots+\psi(a_n)\varphi(X)^n$.

Rămâne să precizăm imaginea $\varphi(X)$.

Fie $f=a_0+a_1X$ acel polinom pentru care $\varphi(f)=X$.

Așadar, $\psi(a_0)+\psi(a_1) \cdot (b_0+b_1X)=X$, de unde deducem că $\psi(a_1)b_1=1$, ceea ce înseamnă că b_1 este inversabil în A .

Aceasta este singura condiție pe care trebuie să o îndeplinească imaginea $\varphi(X)=b_0+b_1X$.

10.17. Dacă a este inversabil vom considera morfismul $\psi:A[X] \rightarrow A[X]$ dat prin $\psi(f(X))=f(a^{-1}X-a^{-1}b)$. Morfismul ψ este inversul lui φ .

Reciproc, fie $u:A[X] \rightarrow A[X]$ un automorfism cu $u(a)=a$, oricare ar fi $a \in A$ și fie inversul acestuia $v=u^{-1}$.

Dacă $u=a_0+a_1X+\dots+a_nX^n$ și $v=b_0+b_1X+\dots+b_mX^m$ din $(uv)(X)=X$ se obține $mn=1$, de unde rezultă că $m=n=1$, ș.a.m.d.

10.18. (i). $(x+\alpha)^5=x^5$, $x \neq 0 \Leftrightarrow \left(\frac{x+\alpha}{x}\right)^5=1$. Rezultă că $\frac{x+\alpha}{x} \in \mathbb{C} \setminus \mathbb{R}$ și

apoi $x \in \mathbb{C} \setminus \mathbb{R}$.

(ii). Fie $x_1 < \dots < x_n$ rădăcinile lui P și $y_k \in (x_k, x_{k+1})$ rădăcinile derivatei.

Fie $\beta = \min\{y_k - x_k, x_{k+1} - y_k \mid 0 \leq k \leq n-1\}$. Pe fiecare interval $[x_k, x_{k+1}]$ și pentru orice $0 < \alpha < \beta$ definim $g(X) = P(X+\alpha) - P(X)$. Cum y_k este unicul punct de extrem al lui P pe intervalul $[x_k, x_{k+1}]$, presupunând de exemplu că este punct de maxim, avem $g(x_k) = P(x_k+\alpha) - P(x_k) > 0$, $g(y_k) = P(y_k+\alpha) - P(y_k) < 0$, deci există $z_k \in (x_k, x_{k+1})$ cu $g(z_k) = 0$.

Se poate alege orice $\alpha \in (0, \beta) \cap \mathbb{Q}$.

10.19. Dacă $f(1)=\alpha \in \mathbb{R}$, se arată imediat că $f(k)=k\alpha$, pentru orice $k \in \mathbb{N}$, astfel că polinomul $g=f-\alpha X$ are o infinitate de rădăcini în \mathbb{R} , de unde concluzia că $g=0$, adică $f=\alpha X$.

10.20. (i). Avem că $f(a)=[f(a)+a]-a$ divide $f(f(a)+a)-f(a)$.

(ii). Alegem $b \in \mathbb{Z}$ a.î. $f(b) \neq 0, \pm 1$. Conform cu (i), $f(b) | f(b+f(b))$, astfel că putem alege $a=b+f(b)$.

(iii). Totul rezultă din (ii).

10.21. Pentru $x=0$ egalitatea devine $-3P(1)=0$, deci $P(X)$ este divizibil cu $X-1$. Pentru $x=3$ vom avea $3P(3)=0$, deci $P(X)$ este divizibil cu $X-3$.

Rezultă că $P(X)=(X-1)(X-3)Q(X)$, cu $Q(X) \in \mathbb{R}[X]$ și înlocuind în relația dată pe $P(X)$ și $P(X+1)$ obținem $(X-1)Q(X)=(X-2)Q(X+1)$.

Pentru $x=2$, $Q(2)=0$, deci $Q(X)$ este divizibil cu $X-2$ și atunci

$$P(X)=(X-1)(X-2)(X-3)R(X) \text{ cu } R(X) \in \mathbb{R}[X].$$

Înlocuind în egalitatea din enunț obținem:

$$X(X-1)(X-2)(X-3)R(X)=(X-3)X(X-1)(X-2)R(X+1),$$

deci $R(X)=R(X+1)$, adică $R(0)=R(1)=R(2)=\dots=R(n)=k$, $k \in \mathbb{R}$.

Rezultă că polinomul de grad n , R este egal cu k .

Deci $P=k(X-1)(X-2)(X-3)$.

10.22. (i). Fie $f(X)=(X-1)^m-X^m+1$. Dacă α este o rădăcină a lui X^2-X+1 trebuie ca $f(\alpha)=0$. Cum $\alpha^2-\alpha+1=0$, atunci $f(\alpha)=\alpha^{2m}-\alpha^m+1$.

$$\text{Dacă } m=6k \Rightarrow f(\alpha)=\alpha^{12k}-\alpha^{6k}+1=1 \neq 0$$

$$\text{Dacă } m=6k+1 \Rightarrow f(\alpha)=\alpha^2-\alpha+1=0$$

$$\text{Dacă } m=6k+2 \Rightarrow f(\alpha)=-\alpha^2-\alpha+1 \neq 0$$

$$\text{Dacă } m=6k+3 \Rightarrow f(\alpha)=3 \neq 0$$

$$\text{Dacă } m=6k+4 \Rightarrow f(\alpha)=\alpha^2+\alpha+1 \neq 0$$

$$\text{Dacă } m=6k+5 \Rightarrow f(\alpha)=\alpha^2-\alpha+1=0.$$

Valorile căutate ale lui m sunt $m=6k+1$ și $m=6k+5$, $k \in \mathbb{N}$.

(ii). Se procedează analog cu punctul (i) și se obține $m=6k+2$ și $m=6k+4$, $k \in \mathbb{N}$.

10.23. Conform teoremei împărțirii cu rest avem $f(X)=(X-a)(X-b)q(X)+r(X)$ cu $r(X)=\alpha X+\beta$, $\alpha, \beta \in \mathbb{R}$.

Avem $f(a)=r(a)=\alpha a+\beta$ și $f(b)=r(b)=\alpha b+\beta$.

Rezolvând sistemul de ecuații: $\begin{cases} \alpha a + \beta = f(a) \\ \alpha b + \beta = f(b) \end{cases}$ obținem

$$\begin{cases} \alpha = \frac{f(a) - f(b)}{a - b} \\ \beta = \frac{af(b) - bf(a)}{a - b} \end{cases} \text{ . Atunci:}$$

$$r = \frac{f(a) - f(b)}{a - b} X + \frac{af(b) - bf(a)}{a - b} = \frac{-f(a)X + f(b)X + bf(a) - af(b)}{b - a} =$$

$$= \frac{(X - a)f(b) - (X - b)f(a)}{b - a} = \frac{f(b) - f(a)}{b - a} X + \frac{bf(a) - af(b)}{b - a}$$

10.24. „ \Leftarrow ”. Dacă $f = \frac{1}{2}[cX^2 + (2b - c)X + 2a]$ cu $a, b, c \in \mathbb{Z}$, atunci

$$f(n) = \frac{1}{2}[cn^2 + (2b - c)n + 2a] = \frac{1}{2}[cn(n - 1) + 2(bn + a)] = c \frac{n(n - 1)}{2} + (bn + a).$$

Cum $2|n(n-1)$, pentru orice $n \in \mathbb{Z}$ avem $f(n) \in \mathbb{Z}$, oricare ar fi $n \in \mathbb{Z}$.

„ \Rightarrow ”. Reciproc, fie $f = aX^2 + bX + c$ cu $a, b, c \in \mathbb{Q}$. Dacă $f(n) \in \mathbb{Z}$, oricare ar fi $n \in \mathbb{Z}$, atunci și $f(0), f(1), f(-1) \in \mathbb{Z}$. Dar $f(0) = c$, $f(1) = a + b + c$, $f(-1) = a - b + c$.

Deci $c \in \mathbb{Z}$, $a + b + c = k_1 \in \mathbb{Z}$, $a - b + c = k_2 \in \mathbb{Z}$. Atunci $a = \frac{k_1 + k_2 - 2c}{2}$ și $b = \frac{k_1 - k_2}{2}$.

Notăm $k_1 + k_2 - 2c = m$, $k_1 - k_2 = 2n - m$. Atunci $f = \frac{1}{2}[mX^2 + (2n - m)X + 2c]$, unde $m, n, c \in \mathbb{Z}$.

10.25. Dacă f este un c.m.m.d.c. al polinoamelor $X^n - 1$ și $X^m - 1$ atunci orice rădăcină a lui f este rădăcină a lui $X^d - 1$, unde $d = (m, n)$ este c.m.m.d.c. al numerelor n și m .

Invers, fie f, g două polinoame; dacă d este un c.m.m.d.c. al lui f și g , atunci există două polinoame u și v a.î. $d = uf + vg$. Atunci orice rădăcină a lui $X^d - 1$ este rădăcină a lui f , deci $f = X^d - 1$.

10.26. Fie $d = (m, n)$. Procedând ca la problema **10.25.** se obține că dacă numerele $\frac{m}{d}$ și $\frac{n}{d}$ sunt ambele impare atunci un c.m.m.d.c. al polinoamelor

date este $X^d + a^d$, iar dacă cel puțin unul dintre numerele $\frac{m}{d}$ sau $\frac{n}{d}$ este par, un c.m.m.d.c. al polinoamelor date este 1.

10.27. Presupunem prin reducere la absurd că polinomul admite rădăcini multiple. Fie α o astfel de rădăcină. Atunci cel puțin $f(\alpha) = f'(\alpha) = 0$.

Cum $f(\alpha) - f'(\alpha) = \frac{\alpha^n}{n!}$ obținem $\alpha = 0$. Dar $f(0) = 1$, contradicție.

10.28. Se știe că orice polinom $f = a_0 + a_1X + \dots + a_nX^n$ de gradul $n \geq 1$ cu coeficienți reali este un produs de polinoame de gradul 1 sau 2 cu coeficienți reali, adică poate fi pus sub forma:

$$f = a_n(X - \alpha_1)^{k_1} \dots (X - \alpha_p)^{k_p} (X^2 + b_1X + c_1)^{l_1} \dots (X^2 + b_sX + c_s)^{l_s},$$

unde $\alpha_1, \dots, \alpha_p \in \mathbb{R}$ și $b_1^2 - 4c_1 < 0, \dots, b_s^2 - 4c_s < 0$.

Aplicând această teoremă și ținând cont de ipoteză, f se poate scrie sub forma $f = g^2h$, unde h nu are nici o rădăcină reală. Vom împărți rădăcinile complexe ale lui h în două grupe: rădăcinile complexe conjugate fac parte din grupe distincte. Făcând produsul factorilor de gradul întâi care corespund rădăcinilor fiecărei grupe obținem polinoamele $h_1 + ih_2$ și $h_1 - ih_2$, iar $h = (h_1 + ih_2)(h_1 - ih_2) = h_1^2 + h_2^2$. Deci $f = (gh_1)^2 + (gh_2)^2$.

10.29. Fie $f = \sum_{i \geq 0} a_i X^i$ și $g = \sum_{i \geq 0} b_i X^i$.

Presupunem prin reducere la absurd că $p | a_0, p | a_1, \dots, p | a_{k-1}$ și $p \nmid a_k$, și $p | b_0, p | b_1, \dots, p | b_{s-1}$ și $p \nmid b_s$. Scriem $fg = \sum_{i \geq 0} c_i X^i$, $c_n = \sum_{i+j=n} a_i b_j$.

Avem $c_{k+s} = a_0 b_{k+s} + a_1 b_{k+s-1} + \dots + a_k b_s + a_{k+1} b_{s-1} + \dots + a_{k+s} b_0$. Cum p divide toți termenii în afara lui $a_k b_s$ (căci $p \nmid a_k$ și $p \nmid b_s$) obținem $p \nmid c_{k+s}$, contradicție.

10.30. Putem scrie $f = c(f) \cdot f'$, $g = c(g) \cdot g'$ cu $f', g' \in \mathbb{Z}[X]$ și $c(f') = c(g') = 1$. Conform problemei **10.29.** avem $c(f'g') = 1$. Atunci $fg = c(f) \cdot f' \cdot c(g) \cdot g' = c(f) \cdot c(g) \cdot f'g'$. Deci $c(fg) = c(f) \cdot c(g)$.

10.31. Rădăcinile polinomului $X^{2n} + X^n + 1$ se obțin din $x^n = \frac{-1 \pm i\sqrt{3}}{2}$
 deci $x = \cos \frac{2(3k+1)\pi}{3n} \pm i \sin \frac{2(3k+1)\pi}{3n}$, $k = 0, 1, \dots, n-1$.

Este suficient să avem $\left[\cos \frac{2(3k+1)\pi}{3n} + i \sin \frac{2(3k+1)\pi}{3n} \right]^m - 1 = 0$, $k=0, 1, \dots, n-1$ și deci $\cos \frac{2m(3k+1)\pi}{3n} = 1$, $\sin \frac{2m(3k+1)\pi}{3n} = 0$, $k=0, 1, \dots, n-1$, adică $\frac{2m(3k+1)\pi}{3n} = 2h_k\pi$, de unde $m = \frac{3h_k n}{3k+1}$.

Pentru $k=0$ avem $m=3h_0n$.

Această condiție este necesară și suficientă deoarece:

$$X^m - 1 = X^{3h_0n} - 1 = (X^{3n})^{h_0} - 1 = (X^{3n} - 1)[X^{3n(h_0-1)} + X^{3n(h_0-2)} + \dots + 1]$$

și $X^{3n} - 1 = (X^n - 1)(X^{2n} + X^n + 1)$. Deci m este multiplu de $3n$.

10.32. Deoarece coeficientul dominant al polinomului este 1, el nu admite rădăcini fracționare. Polinomul nu admite nici rădăcini întregi deoarece $P(k) = k^5 - k + m = M_5 + m$; cum m nu este divizibil prin 5 rezultă că $P(k) \neq M_5$, oricare ar fi $k \in \mathbb{Z}$ și deci $P(k) \neq 0$.

Deci P nu are factori de gradul întâi.

Presupunem că $P = (X^3 + aX^2 + bX + c)(X^2 + pX + q)$.

Identificând coeficienții găsim: $p = -a$, $q = a^2 - b$, $c = 2ab - a^3$, $a^4 + 1 = b(a^2 + b)$, $a(2b - a^2)(a^2 - b) = m$. Cum $m \not\equiv 0 \pmod{5} \Rightarrow a \not\equiv 0 \pmod{5}$, $a^2 - 2b \not\equiv 0 \pmod{5}$, $a^2 - b \not\equiv 0 \pmod{5}$. Cum $a^5 \equiv a \pmod{5}$ și $a \not\equiv 0 \pmod{5}$ rezultă că $a^4 \equiv 1 \pmod{5}$ și deci din $a^4 + 1 = b(a^2 + b)$ rezultă $b(a^2 + b) \equiv 2 \pmod{5}$. (1)

Din $a^2 - 2b \not\equiv 0 \pmod{5}$, $a^2 - b \not\equiv 0 \pmod{5}$ rezultă că $(a^2 - 2b)(a^2 - b) \not\equiv 0 \pmod{5}$ sau $a^4 - 3ba^2 + 2b^2 \equiv a^4 + 2a^2b + 2b^2 \not\equiv 0 \pmod{5}$. Cum $a^4 \equiv 1 \equiv -4 \pmod{5}$ rezultă $-4 + 2a^2b + 2b^2 \not\equiv 0 \pmod{5}$, adică $b(a^2 + b) \not\equiv 2 \pmod{5}$, ceea ce contrazice relația (1). Așadar P este ireductibil în $\mathbb{Z}[X]$.

10.33. $X^2 + \hat{1}$ este ireductibil în $\mathbb{Z}_3[X]$, dar $X^2 + \hat{1} = (X + \hat{2})(X + \hat{3})$ în $\mathbb{Z}_5[X]$.

Al doilea polinom este reductibil și în $\mathbb{Z}_3[X]$ și în $\mathbb{Z}_5[X]$:

$$\text{Avem } X^3 + X + \hat{2} = (X + \hat{1})(X^2 - X + \hat{2}).$$

10.34. \mathbb{Z}_5 fiind corp, (\mathbb{Z}_5^*, \cdot) este grup cu patru elemente, deci conform teoremei lui Lagrange obținem $t^4 = 1$, oricare ar fi $\hat{0} \neq t \in \mathbb{Z}_5$.

Avem $f(t) = t^4 + at + \hat{1} = at + \hat{2}$ și evident pentru fiecare $a \neq \hat{0}$ polinomul are rădăcini în \mathbb{Z}_5 ($a = \hat{1}$, $t = \hat{3}$; $a = \hat{2}$, $t = \hat{4}$ și invers).

În cazul $a = \hat{0}$, avem $f(X) = X^4 + \hat{1} = (X^2 + \hat{2})(X^2 + \hat{3})$.

Deci f este tot timpul reducibil.

10.35. Se verifică ușor că $\tilde{f}(\hat{0}) = \tilde{g}(\hat{0}) = \hat{0}$, $\tilde{f}(\hat{1}) = \tilde{g}(\hat{1}) = \hat{0}$ și $\tilde{f}(\hat{2}) = \tilde{g}(\hat{2}) = \hat{0}$.

10.36. (i). Cum $p^2 + p + 1 \equiv 1 \pmod{p}$, va fi suficient să determinăm restul împărțirii numărului $a = \prod_{k=1}^{p-1} (k^2 + k + 1)$ la p . Fie $\alpha = \cos\left(\frac{2\pi}{3}\right) + i \sin\left(\frac{2\pi}{3}\right)$.

Atunci $k^2 + k + 1 = (\alpha - k)(\bar{\alpha} - k)$ și deci

$$a = \prod_{k=1}^{p-1} (\alpha - k) \cdot \prod_{k=1}^{p-1} (\bar{\alpha} - k) = f(\alpha) \cdot f(\bar{\alpha}), \text{ unde } f = (X-1)(X-2)\dots(X-p+1) \in \mathbb{Z}[X].$$

Fie $g = X^{p-1} - 1 \in \mathbb{Z}[X]$, $\bar{f} = (X - \hat{1})(X - \hat{2})\dots(X - \hat{p-1})$ și

$\bar{g} = X^{p-1} - \hat{1} \in \mathbb{Z}_p[X]$. Cum \bar{f} și \bar{g} au aceleași rădăcini $\hat{1}, \hat{2}, \dots, \hat{p-1}$ în \mathbb{Z}_p rezultă $\bar{f} = \bar{g}$ și deci există $h \in \mathbb{Z}[X]$ a.î. $f = g + p \cdot h$. Obținem:

$$\begin{aligned} a = f(\alpha)f(\bar{\alpha}) &= [g(\alpha) + ph(\alpha)][g(\bar{\alpha}) + ph(\bar{\alpha})] = g(\alpha)g(\bar{\alpha}) + p[g(\alpha)h(\bar{\alpha}) + g(\bar{\alpha})h(\alpha)] + \\ &+ p^2h(\alpha)h(\bar{\alpha}) = g(\alpha)g(\bar{\alpha}) + pb + p^2b_1 \text{ unde } b = g(\alpha)h(\bar{\alpha}) + g(\bar{\alpha})h(\alpha) \text{ și } b_1 = h(\alpha)h(\bar{\alpha}). \end{aligned}$$

Cum g și $h \in \mathbb{Z}[X]$, rezultă $b = u + v\alpha$ cu $u, v \in \mathbb{Z}$. Dar $b = \bar{b} \Rightarrow u + v\alpha = u + v\bar{\alpha} \Rightarrow v(\alpha - \bar{\alpha}) = 0 \Rightarrow v = 0 \Rightarrow b = u \in \mathbb{Z}$. Analog $b_1 \in \mathbb{Z}$. Cum $g(\alpha)g(\bar{\alpha}) = (\alpha^{p-1} - 1)(\bar{\alpha}^{p-1} - 1) =$
 $= 2 - (\alpha^{p-1} + \bar{\alpha}^{p-1}) = 2 - 2\text{Re}(\alpha^{p-1}) = 2 - 2 \cos\left(\frac{2\pi(p-1)}{3}\right)$ rezultă

$$a \equiv 2 - 2 \cos\left(\frac{2\pi(p-1)}{3}\right) \pmod{p}.$$

Dacă $p \equiv 1 \pmod{3} \Rightarrow a \equiv 0 \pmod{p}$.

Dacă $p \equiv 2 \pmod{3} \Rightarrow a \equiv 3 \pmod{p}$.

(ii). $X^2 + X + \hat{1}$ este ireducibil în $\mathbb{Z}_p[X] \Leftrightarrow X^2 + X + \hat{1}$ nu are rădăcini în \mathbb{Z}_p
 $\Leftrightarrow \prod_{k=1}^{p-1} (k^2 + k + 1)$ nu este congruent cu $0 \pmod{p} \Leftrightarrow p \equiv 2 \pmod{3}$.

10.37. În condițiile enunțului funcția $f: K \rightarrow K$, $f(x) = x^{p^n}$, oricare ar fi $x \in K$ este morfism de corpuri (deci funcție injectivă), astfel că dacă pentru $x \in K$ există $y \in K$ a.î. $y^{p^n} = x$, atunci y este unic cu această proprietate.

10.38. Se știe că orice corp finit este comutativ. Fie A mulțimea din enunț și m numărul elementelor lui K . Vom arăta că $A = \{2, 3\}$. Pentru început să arătăm că 2 și 3 aparțin lui A .

Fie $M = \{f = X^2 + aX + b \mid a, b \in K\}$. Avem echivalența $f = g \Leftrightarrow f$ și g au aceleași rădăcini. Numărul polinoamelor din M care au rădăcini egale (de forma $(X-a)^2$) este m , iar cel al polinoamelor din M care au rădăcini distincte (de forma $(X-a)(X-b)$ cu $a \neq b$) este $C_m^2 = \frac{m(m-1)}{2}$. Deci numărul polinoamelor din M care au rădăcini în K este $m + \frac{m(m-1)}{2} = \frac{m(m+1)}{2} < m^3 =$ numărul elementelor lui M . Rezultă că există polinoame din M care nu au rădăcini în K , iar numărul lor este $\frac{m(m-1)}{2}$. Evident $2 \in A$.

Fie $N = \{f = X^3 + aX^2 + bX + c \mid a, b, c \in K\}$. Numărul polinoamelor din N care au o rădăcină simplă în K (de forma $(X-a)h$, unde $h \in M$ și nu are rădăcini în K) este $m \cdot \frac{m(m-1)}{2}$ (conform etapei anterioare). Numărul polinoamelor din N care au trei rădăcini în K , nu toate distincte se obține astfel:

i) polinoame cu o rădăcină triplă (de forma $(X-a)^3$) în număr de m ;
 ii) polinoame cu o rădăcină dublă și una simplă (de forma $(X-a)^2(X-b)$ cu $a \neq b$) în număr de $2 \cdot C_m^2 = m(m-1)$. În total avem $m + m(m-1) = m^2$ polinoame cu trei rădăcini nedistincte în K . Numărul polinoamelor din N care au trei rădăcini distincte în K este $C_m^3 = \frac{m(m-1)(m-2)}{6}$. Deci numărul polinoamelor

din N care au rădăcini în K este $\frac{m^2(m-1)}{2} + m^2 + \frac{m(m-1)(m-2)}{6} = \frac{2m^3 + m}{3} < m^3 =$ numărul elementelor din N .

Deci există polinoame din N care nu au rădăcini în K , de unde în final vom arăta că pentru orice $n \geq 4$, rezultă $n \notin A$. Fie $n \geq 4$. Atunci există $p, q \in \mathbb{N}$ a.î. $n = 2p + 3q$ (dacă n este par $\Rightarrow n = 2p$, iar dacă n este impar $\Rightarrow n = 2k + 1, k \geq 2 \Rightarrow n = 2(k-1) + 3$). Fie $f \in M$ și $g \in N$, polinoame care nu au rădăcini în K . Atunci vom lua polinomul $h = f^p \cdot g^q \in K[X]$ de grad $2p + 3q = n$ (dacă $q = 0$ luăm $h = f^p$ și $p \geq 2$). Polinomul h nu are rădăcini în K și este reducibil în $K[X]$, deci $n \notin A$.

10.39. (i). În orice corp comutativ de caracteristică diferită de 2 funcționează formula obișnuită de rezolvare a ecuației de gradul al doilea. Mai precis, dacă considerăm ecuația $ax^2 + bx + c = 0$, cu $a, b, c \in K, a \neq 0$ (K corp

comutativ cu $\text{car}(K) \neq 2$), această ecuație are soluții în K dacă și numai dacă există $u \in K$ a.î. $b^2 - 4ac = u^2$ și soluțiile sale sunt: $x_{1,2} = (-b \pm u)(2a)^{-1}$.

Folosind aceste considerații se obține că ecuația $3x^2 - 4x + 1 = 0$ se comportă astfel în corpurile considerate:

- 1) în \mathbb{Z}_5 are rădăcinile $x_1 = \hat{1}$, $x_2 = \hat{2}$;
- 2) în \mathbb{Z}_7 are rădăcinile $x_1 = \hat{1}$, $x_2 = \hat{5}$;
- 3) în \mathbb{Z}_{11} are rădăcinile $x_1 = \hat{1}$, $x_2 = \hat{4}$;
- 4) în \mathbb{Z}_{13} are rădăcinile $x_1 = \hat{1}$, $x_2 = \hat{9}$;
- 5) în \mathbb{Z}_{17} are rădăcinile $x_1 = \hat{1}$, $x_2 = \hat{6}$;
- 6) în \mathbb{Z}_{19} are rădăcinile $x_1 = \hat{1}$, $x_2 = \hat{13}$;

(ii). Analog, ecuația $x^2 - x + 5 = 0$ are următoarea comportare în corpurile considerate:

- 1) în \mathbb{Z}_7 are rădăcinile $x_1 = \hat{2}$, $x_2 = \hat{6}$;
- 2) în \mathbb{Z}_{11} are rădăcinile $x_1 = \hat{3}$, $x_2 = \hat{9}$;
- 3) în \mathbb{Z}_{17} are rădăcinile $x_1 = \hat{4}$, $x_2 = \hat{14}$;
- 4) în \mathbb{Z}_{19} are rădăcinile $x_1 = x_2 = \hat{10}$.

10.40. Dacă $a=0$ atunci $Q(X) = 2P(X)$ și afirmația este evidentă.

Fie acum $a \neq 0$ și y o rădăcină a polinomului Q . Atunci $Q(y) = P(y+ia) + P(y-ia) = 0$, deci (1) $P(y+ia) = -P(y-ia)$.

Dacă x_1, \dots, x_n sunt cele n rădăcini reale ale polinomului P , atunci

$$P(X) = (X-x_1)(X-x_2)\dots(X-x_n)$$

și (1) se scrie $(y+ia-x_1)(y+ia-x_2)\dots(y+ia-x_n) = -(y-ia-x_1)(y-ia-x_2)\dots(y-ia-x_n)$, de unde obținem relația: (2)

$$|y-(x_1-ia)| \cdot |y-(x_2-ia)| \cdot \dots \cdot |y-(x_n-ia)| = |y-(x_1+ia)| \cdot |y-(x_2+ia)| \cdot \dots \cdot |y-(x_n+ia)|$$

Din (2) se deduce că numărul y este real.

Într-adevăr, este evident că polinomul Q are coeficienți reali. Dacă $\text{Im}(y) \neq 0$, obținem $\text{Im}(y) > 0$ sau $\text{Im}(y) < 0$.

Să presupunem de exemplu că $\text{Im}(y) > 0$.

Atunci dacă $a > 0$, notând $z_j = x_j + ia$, pentru $j=1, \dots, n$, obținem că $|y-z_j| < |y-\bar{z}_j|$, ceea ce contrazice (2). La fel dacă $a < 0$, $|y-z_j| > |y-\bar{z}_j|$, ceea ce contrazice de asemenea (2).

Deci y nu poate fi o rădăcină complexă cu $\text{Im}(y) > 0$. La fel, y nu poate fi o rădăcină complexă cu $\text{Im}(y) < 0$ deoarece în acest caz \bar{y} ar fi o rădăcină complexă cu $\text{Im}(\bar{y}) > 0$, ceea ce este imposibil.

10.41. Fie $k_1 = 0_K$, $k_2 = 1_K$. În grupul finit multiplicativ $K^* = \{k_2, k_3, \dots, k_n\}$ avem $k_i^{n-1} = 1_K$, adică $k_i^n = k_i$ sau încă $k_i^n - k_i = 0$, pentru orice $i \in \{2, \dots, n\}$.

Dar ultima egalitate este evident satisfăcută și pentru $k_1 = 0_K$, a.î. putem afirma că polinomul $f = X^n - X \in K[X]$ are ca rădăcini pe k_1, k_2, \dots, k_n .

Corpul K fiind finit, este comutativ (teorema lui Wedderburn). Dar se știe că un polinom de grad n cu coeficienți într-un corp comutativ, care are exact n rădăcini în acel corp, se descompune într-un produs de n factori de gradul întâi peste acel corp. În acest caz, cum f are n rădăcini în corpul de coeficienți K , se descompune în factori de gradul întâi în inelul $K[X]$ sub forma

$$X^n - X = \prod_{i=1}^n (X - k_i).$$

10.42. Fie $\alpha \in \mathbb{Z}$ rădăcina comună. Avem relațiile: $\alpha^3 + 2\alpha^2 + a\alpha + b = 0$ și $\alpha^3 - \alpha^2 + b\alpha + a = 0$. Prin scădere obținem $3\alpha^2 + (a-b)(\alpha-1) = 0$.

Cum $\alpha = 1$ nu verifică simultan ecuațiile date avem $\alpha \neq 1$ și deci

$$b - a = \frac{3\alpha^2}{\alpha - 1} = 3(\alpha + 1) + \frac{3}{\alpha - 1} \in \mathbb{Z}, \text{ deci } \alpha - 1 \in \{-1, 1, -3, 3\}.$$

$$\text{Dacă } \alpha - 1 = 1 \Rightarrow \alpha = 2 \Rightarrow \begin{cases} 2a + b = -16 \\ 2b + a = -4 \end{cases} \Rightarrow a, b \notin \mathbb{Z};$$

$$\text{Dacă } \alpha - 1 = -1 \Rightarrow \alpha = 0 \Rightarrow a = b = 0;$$

$$\text{Dacă } \alpha - 1 = -3 \Rightarrow \alpha = -2 \Rightarrow \begin{cases} -2a + b = 0 \\ -2b + a = 12 \end{cases} \Rightarrow \begin{cases} a = -4 \\ b = -8 \end{cases}$$

$$\text{Dacă } \alpha - 1 = 3 \Rightarrow \alpha = 4 \Rightarrow \begin{cases} 4a + b = -96 \\ 4b + a = -48 \end{cases} \Rightarrow a, b \notin \mathbb{Z}.$$

10.43. $P(1) = a_0 + a_1 + \dots + a_n = \text{impar}$. Cum a_0, a_n sunt impare rezultă că $a_1 + a_2 + \dots + a_{n-1} = 2k + 1$ (impar), $k \in \mathbb{N}$.

Presupunem prin reducere la absurd că există $\frac{p}{q}$ o rădăcină rațională a lui $P(X)$, $p, q \in \mathbb{Z}^*$. Cum $p | a_n$ și $q | a_0$ rezultă că p și q sunt impare.

$$P\left(\frac{p}{q}\right) = 0 \Leftrightarrow a_0 p^n + a_1 p^{n-1} q + \dots + a_{n-1} p q^{n-1} + a_n q^n = 0 \text{ și deci}$$

$$a_0 p^n + a_n q^n + a_1 (p^{n-1} q - 1) + \dots + a_{n-1} (p q^{n-1} - 1) = -2k - 1.$$

Însă $a_0 p^n + a_n q^n$ este un număr par.

La fel, $p^{n-k} q^k - 1$, oricare ar fi $k \in \{1, \dots, n-1\}$ sunt numere pare, contradicție.

10.44. Fie $P \in \mathbb{Q}[X]$. Avem, în baza teoremei împărțirii cu rest,

$$P(X) = C(X)(X^3 - 2) + aX^2 + bX + c, \quad a, b, c \in \mathbb{Q}.$$

$$\text{Cum } P(\sqrt[3]{2}) = 0 \text{ avem } a\sqrt[3]{4} + b\sqrt[3]{2} + c = 0. \quad (1)$$

$$\text{Înmulțind (1) cu } \sqrt[3]{2} \text{ obținem } b\sqrt[3]{4} + c\sqrt[3]{2} + 2a = 0. \quad (2)$$

$$\text{Eliminând pe } \sqrt[3]{4} \text{ din (1) și (2) avem } (b^2 - ac)\sqrt[3]{2} = 2a^2 - bc. \quad (3)$$

$$\text{Dacă } b^2 - ac \neq 0 \text{ atunci obținem contradicția } \sqrt[3]{2} = \frac{2a^2 - bc}{b^2 - ac} \in \mathbb{Q}.$$

$$\text{Dacă } b^2 - ac = 0 \text{ atunci } 2a^2 - bc = 0.$$

$$\text{Pentru } a = 0, (1) \text{ devine } b\sqrt[3]{2} + c = 0 \text{ și deci } b = c = 0.$$

$$\text{Pentru } a \neq 0, \text{ avem } c = \frac{b^2}{a} \text{ și } 2a^2 - \frac{b^3}{a} = 0. \text{ Rezultă că, } \sqrt[3]{2} = \frac{b}{a},$$

contradicție cu faptul că $\sqrt[3]{2} \notin \mathbb{Q}$ și $\frac{b}{a} \in \mathbb{Q}$. Deci $a = b = c = 0$ și deci

$$P(X) = C(X)(X^3 - 2).$$

10.45. Pentru $X \neq 1$ avem:

$$\begin{aligned} P(X) &= \left(\frac{X^{n+1} - 1}{X - 1} \right)^2 - X^n = \frac{X^{2n+2} - 2X^{n+1} + 1}{(X - 1)^2} - X^n = \frac{X^{2n+2} + 1 - X^{n+2} - X^n}{(X - 1)^2} = \\ &= \frac{(X^n - 1)(X^{n+2} - 1)}{(X - 1)^2} = (X^{n-1} + X^{n-2} + \dots + X + 1)(X^{n+1} + X^n + \dots + X + 1) \end{aligned}$$

Identitatea este evident adevărată și pentru $X = 1$.

Deci P este reductibil în $\mathbb{Z}[X]$.

10.46. Polinomul P se mai scrie:

$$\begin{aligned} P &= \left[(X^n - X - 2) + X \right]^n - X - 2 = (X^n - X - 2)^n + C_n^1 (X^n - X - 2)^{n-1} X + \dots + \\ &+ C_n^{n-1} (X^n - X - 2) X^{n-1} + X^n - X - 2 = (X^n - X - 2) Q \end{aligned}$$

unde Q este un polinom cu coeficienți întregi.

10.47. Conform problemei **10.5.**, un polinom $f = \hat{a}_0 + \hat{a}_1 X + \hat{a}_2 X^2 + \dots + \hat{a}_n X^n$ este inversabil în $\mathbb{Z}_{p^k}[X]$ dacă și numai dacă are coeficientul \hat{a}_0 inversabil în \mathbb{Z}_{p^k} , iar coeficienții $\hat{a}_1, \hat{a}_2, \dots, \hat{a}_n$ nilpotenți în \mathbb{Z}_{p^k} .

Însă în \mathbb{Z}_{p^k} avem $\varphi(p^k) = (p-1)p^{k-1}$ elemente inversabile.

Orice element care nu este inversabil este de forma \hat{b} cu b număr întreg divizibil prin p ; El poate fi scris $\hat{b} = m \cdot p^r$, cu $0 \leq m < p$ și $0 \leq r < k$.

Se observă că un asemenea element este nilpotent (căci $\hat{p}^k = \hat{0}$). Așadar, în inelul \mathbb{Z}_{p^k} orice element care nu este inversabil este nilpotent, iar numărul elementelor nilpotente din \mathbb{Z}_{p^k} este deci $p^k - \varphi(p^k) = p^{k-1}$.

Pentru a obține un polinom f inversabil, de grad $\leq n$, putem alege pe \hat{a}_0 printre cele $(p-1)p^{k-1}$ elemente inversabile din \mathbb{Z}_{p^k} iar pe $\hat{a}_1, \hat{a}_2, \dots, \hat{a}_n$ printre cele p^{k-1} elemente nilpotente din \mathbb{Z}_{p^k} .

În total avem $(p-1)p^{(k-1)(n+1)}$ posibilități de alegere.

De exemplu, în inelul \mathbb{Z}_4 avem ca elemente inversabile pe $\hat{1}$ și pe $\hat{3}$, iar ca elemente nilpotente pe $\hat{0}$ și pe $\hat{2}$.

Așadar numărul polinoamelor inversabile de grad mai mic sau egal cu n din inelul $\mathbb{Z}_4[X]$ este 2^{n+1} .

10.48. Egalitatea $(\hat{1} + \hat{2}X)(\hat{1} + \hat{2}X) = \hat{1} + \hat{4}X + \hat{4}X^2 = \hat{1}$, ne arată că polinomul $\hat{1} + \hat{2}X$ este inversabil în inelul $\mathbb{Z}_4[X]$.

10.49. Cum grad $P=3$, dacă el nu ar fi ireductibil ar avea obligatoriu o rădăcină.

$a \in \mathbb{Z}_3$ deci $a \in \{\hat{0}, \hat{1}, \hat{2}\}$.

Pentru $a = \hat{0}$, $P = \hat{2}X^3 + \hat{2}X + \hat{1}$ și $P(\hat{2}) = \hat{0}$ deci P este reductibil.

Pentru $a = \hat{1}$, $P = \hat{2}X^3 + \hat{1}$ și $P(\hat{1}) = \hat{0}$ deci și în acest caz P este reductibil.

Pentru $a = \hat{2}$, rezultă $P = \hat{2}X^3 + X + \hat{1}$ este ireductibil în $\mathbb{Z}_3[X]$ pentru că avem $P(\hat{0}) = \hat{1}$, $P(\hat{1}) = \hat{1}$, $P(\hat{2}) = \hat{1}$.

10.50. Conform teoremei lui Fermat, $\hat{x}^6 = \hat{1}$, pentru orice $\hat{x} \in \mathbb{Z}_7^*$.

Dacă $\hat{a} \neq \hat{0}$ atunci există \hat{a}^{-1} inversul său (\mathbb{Z}_7 fiind corp).

$P(\hat{a}^{-1}) = (\hat{a}^{-1})^6 + \hat{a} \cdot \hat{a}^{-1} + \hat{5} = \hat{1} + \hat{1} + \hat{5} = \hat{0}$. Deci \hat{a}^{-1} este rădăcină a lui P, pentru $\hat{a} \neq \hat{0}$, deci P este în acest caz reductibil.

Dacă $\hat{a} = \hat{0}$ atunci $P = X^6 + \hat{5} = (X^3 + \hat{4})(X^3 + \hat{3})$ este reductibil.

10.51. 1) P_1 este ireductibil în $\mathbb{Z}_2[X]$, pentru că fiind de gradul 3 ar trebui să aibă cel puțin o rădăcină pentru a fi reductibil, dar $P_1(\hat{0}) = \hat{1}$, $P_1(\hat{1}) = \hat{1}$.

2) $P_2(\hat{0}) = \hat{1}$, $P_2(\hat{1}) = \hat{1}$, deci P_2 nu are rădăcini. Dacă P_2 ar fi reductibil în $\mathbb{Z}_2[X]$ el s-ar descompune în produs de două polinoame de gradul doi $P_2 = (X^2 + \hat{a}X + \hat{b})(X^2 + \hat{c}X + \hat{d})$, cu $\hat{a}, \hat{b}, \hat{c}, \hat{d} \in \mathbb{Z}_2$.

Identificând coeficienții obținem:

$$\begin{cases} a + c = \hat{1} \\ d + b + ac = \hat{0} \\ ad + bc = \hat{0} \\ bd = \hat{1} \end{cases}$$

Din ultima relație rezultă $b = d = \hat{1}$ și înlocuind avem $\begin{cases} a + c = \hat{1} \\ ac = \hat{0} \\ a + c = \hat{0} \end{cases}$,

imposibil deci P_2 este ireductibil în $\mathbb{Z}_2[X]$.

3) $P_3 = X^5 + \hat{1} = (X + \hat{1})(X^4 + \hat{2}X^3 + X^2 + \hat{2}X + \hat{1})$. Analog cu 2) se probează că $X^4 + \hat{2}X^3 + X^2 + \hat{2}X + \hat{1}$ este ireductibil în $\mathbb{Z}_3[X]$.

4) $P_4 = X^4 - \hat{1} = (X + \hat{1})(X - \hat{1})(X^2 + \hat{1})$.

10.52. Să presupunem prin reducere la absurd că f este reductibil în $\mathbb{Z}[X]$, adică putem scrie $f = (b_0 + b_1X + \dots + b_mX^m)(c_0 + c_1X + \dots + c_kX^k)$ cu $m, k \geq 1$ și $m+k=n$. Identificând coeficienții lui f deducem că:

$$(*) \quad \begin{cases} a_0 = b_0 c_0 \\ a_1 = b_0 c_1 + b_1 c_0 \\ a_2 = b_0 c_2 + b_1 c_1 + b_2 c_0 \\ \dots \\ a_{n-1} = b_{m-1} c_k + b_m c_{k-1} \\ a_n = b_m c_k \end{cases}$$

Cum $p \nmid a_0$ iar $p^2 \nmid a_0$ deducem că $p \mid b_0$ și $p \nmid c_0$ sau $p \mid c_0$ și $p \nmid b_0$.

Să presupunem de exemplu că $p \mid b_0$ și $p \nmid c_0$.

Dacă ținem cont de relațiile (*) deducem din aproape în aproape că $p \mid b_1, p \mid b_2, \dots, p \mid b_m$ și din ultima relație din (*) am deducem că $p \mid a_n$, absurd.

Analog dacă $p \mid c_0$ și $p \nmid b_0$ am deduce că $p \mid c_1, p \mid c_2, \dots, p \mid c_k$ și din ultima relație din (*) am deducem că $p \mid a_n$, absurd.

10.53. Sub această formă nu putem aplica criteriul lui Eisenstein dar se vede imediat că f este ireductibil dacă polinomul $g(X)=f(X+1)$ este ireductibil.

Cum $f(X) = \frac{X^p - 1}{X - 1}$ obținem că:

$$\begin{aligned} g(X) &= \frac{(X+1)^p - 1}{X} = X^{p-1} + C_p^1 X^{p-2} + C_p^2 X^{p-3} + \dots + C_p^{p-1} = \\ &= X^{p-1} + C_p^1 X^{p-2} + C_p^2 X^{p-3} + \dots + C_p^{p-2} X + p. \end{aligned}$$

Deoarece p este prim avem că $p \mid C_p^k$, oricare ar fi $1 \leq k \leq p-1$ și deci conform criteriului lui Eisenstein, g este un polinom ireductibil în $\mathbb{Z}[X]$.

10.54. Se aplică problema **10.53.** pentru numărul prim $p=53$.

10.55. Se aplică criteriul lui Eisenstein pentru numărul prim $p=3$ sau $p=5$.

10.56. Se aplică criteriul lui Eisenstein pentru numărul prim p .

10.57. Sub această formă nu putem aplica criteriul lui Eisenstein.

Vom arăta în schimb că polinomul $g=f(X+1)=(X+1)^{2^n} + 1$ este ireductibil.

$$\text{Într-adevăr, avem } g = X^{2^n} + \sum_{1 \leq k \leq 2^n - 1} C_{2^n}^k X^k + 2.$$

Vom dovedi că $2 \mid C_{2^n}^k$, oricare ar fi $1 \leq k \leq 2^n - 1$.

$$\text{Avem că } C_{2^n}^k = \frac{2^n(2^n-1)(2^n-2)\dots(2^n-k+1)}{k!}.$$

Fie $1 \leq k' < k$; putem scrie atunci $k' = 2^p r$, unde $p < n$ și r este un număr impar. Deoarece $\frac{2^n - k'}{k'} = \frac{2^p(2^{n-p} - r)}{2^p r} = \frac{2^{n-p} - r}{r}$, atunci $\frac{2^n - k'}{k'}$ este egal cu câțul a două numere impare. Deci expresia $\frac{(2^n-1)(2^n-2)\dots(2^n-(k-1))}{1 \cdot 2 \cdot \dots \cdot (k-1)}$ este câțul a două numere impare. Cum $k < 2^n$, atunci în câțul $\frac{2^n}{k}$ apare cel puțin un factor egal cu 2. Deci $2 \mid C_{2^n}^k$.

Luând numărul prim $p=2$ și aplicând criteriului lui Eisenstein obținem că polinomul $g(X)$ este ireductibil. Aceasta arată că $f = X^{2^n} + 1$ este un polinom ireductibil în $\mathbb{Z}[X]$.

10.58. Vom proceda ca la problema **10.57**. Pentru a arăta că f este ireductibil este suficient să dovedim că $g = f(X+1)$ este ireductibil.

Într-adevăr, avem

$$\begin{aligned} g(X) &= (X+1)^{p^n} + p - 1 = X^{p^n} + \sum_{1 \leq k \leq p^n-1} C_{p^n}^k X^k + 1 + p - 1 = \\ &= X^{p^n} + \sum_{1 \leq k \leq p^n-1} C_{p^n}^k X^k + p. \end{aligned}$$

Vom dovedi că $p \mid C_{p^n}^k$, oricare ar fi $1 \leq k \leq p^n - 1$.

$$\text{Avem că } C_{p^n}^k = \frac{p^n(p^n-1)(p^n-2)\dots(p^n-k+1)}{k!}.$$

Fie $1 \leq k' < k$; putem scrie atunci $k' = p^t r$, unde $t < n$ și $(p, r) = 1$.

Deoarece $\frac{p^n - k'}{k'} = \frac{p^t(p^{n-t} - r)}{p^t r} = \frac{p^{n-t} - r}{r}$ se observă că din condiția că

$(p, r) = 1$ rezultă că în fracția $\frac{p^n - k'}{k'}$ după simplificare, numărătorul și numitorul nu se mai divid cu p . Deci fracția $\frac{(p^n-1)(p^n-2)\dots(p^n-(k-1))}{1 \cdot 2 \cdot \dots \cdot (k-1)}$, după simplificare este câțul a două numere naturale în care atât numitorul cât și numărătorul nu se mai divid cu p . Cum $k < p^n$, atunci putem scrie $k = p^s k_1$, unde

$s < n$ și $(p, k_1) = 1$. Deci $\frac{p^n}{k} = \frac{p^{n-s}}{k_1}$. Deci numărul întreg $C_{p^n}^k$ este câtu a două numere naturale în care numărătorul se divide cu p (de fapt cu p^{n-s}) și numitorul nu se divide cu p . Deci $p \mid C_{p^n}^k$.

Aplicând criteriului lui Eisenstein pentru numărul prim p obținem că polinomul g este ireductibil. Aceasta arată că $f = X^{p^n} + p - 1$ este un polinom ireductibil în $\mathbb{Z}[X]$.

10.59. Fie $u_i = q_i m + r_i$, $0 \leq r_i < m$. Observăm că $X^m - 1 = (X-1)P(X)$.

Apoi, $X^{u_i} = X^{q_i m + r_i} = X^{r_i} (X^{q_i m} - 1) + X^{r_i}$. Cum $X^m = (X-1)P(X) + 1$,

obținem că $X^{q_i m} = A_i(X)P(X) + 1$, unde $A_i(X)$ este un polinom în nedeterminata X .

Deci $Q(X) = G(X) \cdot P(X) + (X^{r_1} + X^{r_2} + \dots + X^{r_n})$.

Așadar $P \mid Q \Leftrightarrow P \mid X^{r_1} + X^{r_2} + \dots + X^{r_n} = H$.

Dar cum $H = n_0 + n_1 X + \dots + n_{m-1} X^{m-1}$ are gradul mai mic sau egal cu gradul lui P , rezultă că $P \mid H$ dacă și numai dacă există $\alpha \in \mathbb{R}$ a.î. $H = \alpha P$. De aici rezultă că $n_0 = n_1 = \dots = n_{m-1}$.

10.60. Demonstrăm prin inducție după n următoarea **Propoziție**:

Oricare ar fi $x_1, x_2, \dots, x_n \in [0, 1]$, oricare ar fi k , $1 \leq k \leq n$, are loc inegalitatea:

$$(-1)^k [P_n(1) - 1 + S_1 - S_2 + \dots + (-1)^k S_{k-1}] \geq 0; \quad (1)$$

unde $P_n(x) = (x-x_1) \dots (x-x_n)$ și $S_l(x_1, \dots, x_n) = \sum x_1 x_2 \dots x_l = a_l$.

Pentru $n=1$ inegalitatea este evidentă (aici $k=1$). Presupunem că

$$(-1)^k [P_n(1) - 1 + S_1 - S_2 + \dots + (-1)^k S_{k-1}] \geq 0 \quad (*)$$

și să demonstrăm că:

$$(-1)^k [P_{n+1}(1) - 1 + S_1(x_1, \dots, x_{n+1}) - S_2(x_1, \dots, x_{n+1}) + \dots + (-1)^k S_{k-1}(x_1, \dots, x_{n+1})] \geq 0,$$

oricare ar fi $k \leq n+1$. Înmulțind (*) cu $1-x_{n+1} \geq 0$ rezultă:

$$(-1)^k [P_n(1)(1-x_{n+1}) - (1-x_{n+1}) + a_1(1-x_{n+1}) - a_2(1-x_{n+1}) + \dots + (-1)^k a_{n-1}(1-x_{n+1})] \geq 0$$

$(-1)^k [P_{n+1}(1) - 1 + (a_1 + x_{n+1}) - (a_2 + a_1 x_{n+1}) + \dots + (-1)^k (a_{k-1} + a_{k-2} x_{n+1}) - (-1)^k a_{k-1} x_{n+1}] \geq 0$, de unde rezultă că:

$$(-1)^k [P_{n+1}(1) - 1 + S_1(x_1, \dots, x_{n+1}) - S_2(x_1, \dots, x_{n+1}) + \dots + (-1)^{k+1} S_{k-1}(x_1, \dots, x_{n+1})] \geq a_{k-1} x_{n+1},$$

oricare ar fi $k \leq n$. Pentru $k=n+1$ relația este imediată din enunț (s-a folosit relația $S_k(x_1, \dots, x_n) = S_k(x_1, \dots, x_{n-1}) + x_n S_{n-1}(x_1, \dots, x_{n-1})$).

10.61. În rezolvare vom folosi faptul că:

$$(1) D_n(z) = \begin{vmatrix} a_1 & a_2 & a_3 & \dots & a_n \\ za_n & a_1 & a_2 & \dots & a_{n-1} \\ za_{n-1} & za_n & a_1 & \dots & a_{n-2} \\ \dots & \dots & \dots & \dots & \dots \\ za_2 & za_3 & za_4 & \dots & a_1 \end{vmatrix} = \prod_{k=0}^{n-1} (a_1 + a_2 z_k + a_3 z_k^2 + \dots + a_n z_k^{n-1})$$

unde $a_1, a_2, \dots, a_n, z \in \mathbb{C}$, iar z_k ($k \in \{0, \dots, n-1\}$) sunt rădăcinile de ordinul n ale numărului z . Într-adevăr, să notăm cu V_n determinantul Vandermonde de ordinul n asociat numerelor z_k ($k \in \{0, \dots, n-1\}$). Avem:

$$V_n = \begin{vmatrix} 1 & 1 & 1 & \dots & 1 \\ z_0 & z_1 & z_2 & \dots & z_{n-1} \\ z_0^2 & z_1^2 & z_2^2 & \dots & z_{n-1}^2 \\ \dots & \dots & \dots & \dots & \dots \\ z_0^{n-1} & z_1^{n-1} & z_2^{n-1} & \dots & z_{n-1}^{n-1} \end{vmatrix} \stackrel{not}{=} |v_{ij}|_{i,j=1,n}.$$

Calculând în continuare $D_n(z) \cdot V_n$ vom deduce formula (1).

Fie $P_n = D_n(z) \cdot V_n \stackrel{not}{=} |p_{ij}|_{i,j=1,n}$ Avem:

$$\begin{aligned} p_{ij} &= \sum_{k=1}^n d_{ik} v_{kj} \\ &= za_{n-i+2} + za_{n-i+3} z_{j-1} + za_{n-i+4} z_{j-1}^2 + \dots + za_n z_{j-1}^{i-2} + a_1 z_{j-1}^{i-1} + a_2 z_{j-1}^i + \dots + a_{n-i+1} z_{j-1}^{n-1} \\ &= a_{n-i+2} z_{j-1}^n + a_{n-i+3} z_{j-1}^{n+1} + a_{n-i+4} z_{j-1}^{n+2} + \dots + a_n z_{j-1}^{n+i-2} + a_1 z_{j-1}^{i-1} + a_2 z_{j-1}^i + \dots + a_{n-i+1} z_{j-1}^{n-1} \\ &= z_{j-1}^{i-1} (a_{n-i+2} z_{j-1}^{n-i+1} + a_{n-i+3} z_{j-1}^{n-i+2} + a_{n-i+4} z_{j-1}^{n-i+3} + \dots + \\ &\quad + a_n z_{j-1}^{n-1} + a_1 + a_2 z_{j-1} + \dots + a_{n-i+1} z_{j-1}^{n-1}) \\ &= z_{j-1}^{i-1} (a_1 + a_2 z_{j-1} + a_3 z_{j-1}^2 + \dots + a_{n-i+1} z_{j-1}^{n-1} + \dots + a_n z_{j-1}^{n-1}) \\ &= v_{ij} (a_1 + a_2 z_{j-1} + a_3 z_{j-1}^2 + \dots + a_n z_{j-1}^{n-1}) \end{aligned}$$

Deci elementele coloanei j din P_n se obțin prin înmulțirea elementelor coloanei j din V_n cu factorul $a_1 + a_2 z_{j-1} + a_3 z_{j-1}^2 + \dots + a_n z_{j-1}^{n-1}$. Deducem astfel că:

$$D_n(z) \cdot V_n = \prod_{k=0}^{n-1} (a_1 + a_2 z_k + a_3 z_k^2 + \dots + a_n z_k^{n-1}) \cdot V_n$$

Cum $V_n \neq 0$, rezultă că: $D_n(z) = \prod_{k=0}^{n-1} (a_1 + a_2 z_k + a_3 z_k^2 + \dots + a_n z_k^{n-1})$.

Caz particular $z=1$. Avem:

$$D_n(1) = \begin{vmatrix} a_1 & a_2 & a_3 & \dots & a_n \\ a_n & a_1 & a_2 & \dots & a_{n-1} \\ a_{n-1} & a_n & a_1 & \dots & a_{n-2} \\ \dots & \dots & \dots & \dots & \dots \\ a_2 & a_3 & a_4 & \dots & a_1 \end{vmatrix} = \prod_{k=0}^{n-1} (a_1 + a_2 \varepsilon_k + a_3 \varepsilon_k^2 + \dots + a_n \varepsilon_k^{n-1}),$$

$\varepsilon_k = \cos \frac{2k\pi}{n} + i \sin \frac{2k\pi}{n}$, $k = \overline{0, n-1}$. Conform celor stabilite anterior, cu notația

$P(x) = a_1 + a_2x + a_3x^2 + \dots + a_nx^{n-1}$ vom obține că ecuațiile $x^n - 1 = 0$ și $P(x) = 0$ au cel puțin o rădăcină comună dacă și numai dacă $P(\varepsilon_1) \cdot \dots \cdot P(\varepsilon_n) = 0 \Leftrightarrow D_n(1) = 0$.

10.62. Fie $s_i = \sum x_1 x_2 \dots x_i$, $i = 1, 2, \dots, n$. Atunci, elementele x_i , $i = 1, 2, \dots, n$ sunt soluții ale ecuației:

$$P(X) = X^n - s_1 X^{n-1} + s_2 X^{n-2} - \dots + (-1)^n s_n = 0.$$

Cum implicația de la stânga la dreapta este banală, să presupunem că numerele s_1, s_2, \dots, s_n sunt pozitive și să demonstrăm că $x_1, x_2, \dots, x_n \geq 0$. Dacă, prin absurd există $i \in \{1, 2, \dots, n\}$ a.î. $x_i < 0$, atunci (dacă de exemplu, n este impar) deducem că $P(x_i) < 0 \Leftrightarrow 0 < 0$, absurd. Dacă n este par, obținem contradicția $P(x_i) > 0 \Leftrightarrow 0 > 0$.

10.63. Să considerăm $q(x) = (x-x_1)(x-x_2)\dots(x-x_{n+1})$.

Observăm că $q'(x_k) = (x_k - x_1)\dots(x_k - x_{k-1})(x_k - x_{k+1})\dots(x_k - x_{n+1})$, $k = 1, 2, \dots, n+1$. Atunci relația din enunț devine:

$$\sum_{k=1}^{n+1} \frac{P(x_k)}{q'(x_k)} = \begin{cases} 0, & \text{dacă } \text{grad}(P) \leq n-1 \\ a_0, & \text{dacă } \text{grad}(P) = n \end{cases}.$$

Pentru aceasta, scriem polinomul de interpolare Lagrange pentru polinomul x^s , cu $0 \leq s \leq n$ și avem:

$$x^s = \sum_{i=1}^{n+1} \frac{(x-x_1)\dots(x-x_{i-1})(x-x_{i+1})\dots(x-x_{n+1})}{q'(x_i)} \cdot x_i^s. \quad (1)$$

Dacă $s \leq n-1$, identificând coeficientul lui x^n în (1), obținem:

$$\sum_{i=1}^{n+1} \frac{x_i^n}{q'(x_i)} = 0 \quad (0 \leq s \leq n-1).$$

Dacă $s = n$, procedând la fel deducem că: $\sum_{i=1}^{n+1} \frac{x_i^n}{q'(x_i)} = 1$.

Fie $P(x) = a_0 x^m + a_1 x^{m-1} + \dots + a_m$, cu $m \leq n$. Având în vedere cele de mai sus putem scrie:

$$\sum_{i=1}^{n+1} \frac{P(x_i)}{q'(x_i)} = \sum_{i=1}^{n+1} \frac{1}{q'(x_i)} \cdot \sum_{k=0}^m a_k x_i^{m-k} = \sum_{k=0}^m a_k \left(\sum_{i=1}^{n+1} \frac{x_i^{m-k}}{q'(x_i)} \right) = \begin{cases} 0, & \text{daca } m \leq n-1 \\ a_0, & \text{daca } m = n \end{cases}$$

10.64. Să presupunem că există $n+1$ numere distincte $x_1, \dots, x_{n+1} \in \{0, 1, \dots, p-1\}$ a. î. $P(x_i)$ se divide la p pentru orice $i=1, 2, \dots, n+1$. Folosind formula din enunțul problemei **10.63.** și aducând la același numitor obținem o relație de forma: $A_1 P_1(x_1) + \dots + A_{n+1} P(x_{n+1}) = a_0 \cdot \prod_{\substack{i,j=1 \\ i \neq j}}^{n+1} (x_i - x_j)$, cu A_1, \dots, A_{n+1} numere

întregi.

Cum $P(x_1), \dots, P(x_{n+1})$ sunt divizibile prin p , rezultă că membrul drept al egalității anterioare este divizibil prin p . Dar $0 < |x_i - x_j| < p$, pentru orice $i, j \in \{1, 2, \dots, n+1\}$ și, cum p este prim, avem că $p \nmid |x_i - x_j|$ și atunci, a_0 se divide la p , absurd.

10.65. Rezultă imediat din problema **10.64.**, considerând $P(x) = f^{(r)}(x)$, iar $q(x) = f(x)$.

10.66. Deoarece $s_1 = s_2 = \dots = s_6 = 0$ și $s_7 = 1$, conform formulelor lui Newton vom avea $S_1 = S_2 = \dots = S_6 = 0$ și cum din ecuația dată avem:

$$x_k^{7+\alpha} - x_k^\alpha = 0, \quad k=1, \dots, 7, \quad \alpha \in \mathbb{N}, \quad \text{deducem că } S_7 = 7.$$

$$\text{De asemenea, rezultă că } S_i = \begin{cases} 0, & \text{pentru } i \neq 7m \\ 7, & \text{pentru } i = 7m \end{cases}, \quad m \in \mathbb{N}.$$

În acest caz, $S_7 = S_{14} = 7$ și $S_i = 0$ pentru $i \in \{1, \dots, 20\} \setminus \{7, 14\}$.

Atunci pentru suma cerută avem:

$$\begin{aligned} S &= \sum (x_1 + x_2)^{20} = \sum \left(\sum_{i=0}^{20} C_{20}^i x_1^{20-i} x_2^i \right) = \sum_{i=0}^{20} C_{20}^i \left(\sum x_1^{20-i} x_2^i \right) = \sum_{i=0}^{20} C_{20}^i (S_{20-i} S_i - S_{20}) = \\ &= \sum_{i=0}^{20} C_{20}^i S_{20-i} S_i = C_{20}^7 S_{13} S_7 + C_{20}^{14} S_6 S_{14} = 0. \end{aligned}$$

Observație. Am notat $s_1 = x_1 + \dots + x_n, \dots, s_n = x_1 \cdot \dots \cdot x_n$ și

$$S_k = x_1^k + \dots + x_n^k, \quad k \in \mathbb{N}.$$

10.67.

$$(i). \quad S_p \cdot S_q = (x_1^p + \dots + x_n^p)(x_1^q + \dots + x_n^q) = \sum_{i=1}^n x_i^{p+q} + \sum_{i \neq j} x_i^p x_j^q = S_{p+q} + \sum_{i \neq j} x_i^p x_j^q$$

$$\Rightarrow \sum_{i \neq j} x_i^p x_j^q = S_p \cdot S_q - S_{p+q}.$$

Suma din membrul stâng reprezintă un polinom în nedeterminatele x_1, \dots, x_n simetric și omogen de gradul $p+q$.

(ii). În particular, dacă în (i) punem $p=q$ obținem

$$\sum_{i \neq j} x_i^p x_j^p = \frac{1}{2} \cdot [(S_p)^2 - S_{2p}], \quad i, j \in \{1, \dots, n\}.$$

(iii).

$$\begin{aligned} S_p \cdot S_q \cdot S_r &= (x_1^p + \dots + x_n^p)(x_1^q + \dots + x_n^q)(x_1^r + \dots + x_n^r) = \sum_{i=1}^n x_i^{p+q+r} + \sum_{i \neq j} x_i^{p+q} x_j^r + \\ &+ \sum_{i \neq j} x_i^{p+r} x_j^q + \sum_{i \neq j} x_i^{q+r} x_j^p + \sum_{i \neq j \neq k} x_i^p x_j^q x_k^r = S_{p+q+r} + S_{p+q} S_r - S_{p+q+r} + S_{p+r} S_q - \\ &- S_{p+q+r} + S_{q+r} S_p - S_{p+q+r} + \sum_{i \neq j \neq k} x_i^p x_j^q x_k^r \\ \Rightarrow \sum_{i \neq j \neq k} x_i^p x_j^q x_k^r &= S_p \cdot S_q \cdot S_r - S_{p+q} \cdot S_r - S_{p+r} \cdot S_q - S_{r+q} \cdot S_p + 2S_{p+q+r}, \end{aligned}$$

$i, j, k \in \{1, \dots, n\}$.

În particular, pentru $p=q=r$ avem:

$$\sum_{i \neq j \neq k} x_i^p x_j^p x_k^p = \frac{1}{6} [(S_p)^3 - 3S_{2p} \cdot S_p + 2S_{3p}], \quad i, j, k \in \{1, \dots, n\}.$$

10.68. Conform formulelor demonstrate la problema **10.67.** avem

$$\sum_{i \neq j} x_i^3 x_j^2 = S_3 \cdot S_2 - S_5 \quad \text{și cum în acest caz } s_1 = x_1 + x_2 + x_3 = 0,$$

$$s_2 = x_1 x_2 + x_1 x_3 + x_2 x_3 = 3, \quad s_3 = x_1 x_2 x_3 = 5, \quad \text{obținem } S_2 = -6, \quad S_3 = 15, \quad S_5 = -75,$$

$$(S_2 = s_1^2 - 2s_2 = -6, \quad S_3 = -3s_1 + 15 = -3s_1 + 15 = 15, \quad S_5 = -3s_3 + 5S_2 = -75).$$

$$\text{Atunci } \sum_{i \neq j} x_i^3 x_j^2 = -90 + 75 = -15.$$

10.69. Notez $s_1 = x_1 + x_2 + x_3$, $s_2 = x_1 x_2 + x_1 x_3 + x_2 x_3$, $s_3 = x_1 x_2 x_3$ și considerând

$$S_n = x_1^n + x_2^n + x_3^n \text{ avem:}$$

$$S_2 = x_1^2 + x_2^2 + x_3^2 = s_1^2 - 2s_2 = 4 - 2s_2,$$

$$S_3 = x_1^3 + x_2^3 + x_3^3 = s_1 S_2 - s_2 S_1 + 3s_3 = 8 - 6s_2 + 3s_3,$$

$S_4 = x_1^4 + x_2^4 + x_3^4 = s_1 S_3 - s_2 S_2 + s_3 S_1 = 16 - 12s_2 + 6s_3 - 4s_2 + 2s_2^2 + 2s_3 = 2s_2^2 - 16s_2 + 8s_3 + 16$, și cum $S_4 = x_1^4 + x_2^4 + x_3^4 = 8$, rezultă că $2s_2^2 - 16s_2 + 8s_3 + 16 = 8$ deci $s_2^2 - 8s_2 + 4s_3 + 4 = 0$.

De asemenea, $S_5 = s_1 S_4 - s_2 S_3 + s_3 S_2 = 16 - 8s_2 - 3s_2 s_3 + 4s_3 + 6s_2^2 - 2s_2 s_3 = 6s_2^2 - 5s_2 s_3 - 8s_2 + 4s_3 + 16$ și cum $S_5 = x_1^5 + x_2^5 + x_3^5 = 32$ rezultă că $6s_2^2 - 5s_2 s_3 - 8s_2 + 4s_3 + 16 = 32$, deci $6s_2^2 - 5s_2 s_3 - 8s_2 + 4s_3 - 16 = 0$.

Trebuie rezolvat sistemul de ecuații:

$$\begin{cases} 6s_2^2 - 5s_2 s_3 - 8s_2 + 4s_3 - 16 = 0 \\ s_2^2 - 8s_2 + 4s_3 + 4 = 0 \end{cases}$$

echivalent, după eliminarea lui s_2^2 , cu sistemul:

$$\begin{cases} s_2^2 - 8s_2 + 4s_3 + 4 = 0 \\ 8s_2 - 4s_3 - s_2 s_3 - 8 = 0 \end{cases}$$

din care, eliminând pe s_3 , avem: $s_2^3 - 4s_2^2 + 4s_2 - 16 = 0$, care se mai scrie $(s_2 - 4)(s_2^2 + 4) = 0$ și vom avea două cazuri:

1) $s_2 - 4 = 0$. Atunci $s_2 = 4$, $s_3 = 3$ și prin urmare:

$$\begin{cases} x_1 + x_2 + x_3 = 2 \\ x_1 x_2 + x_1 x_3 + x_2 x_3 = 4 \\ x_1 x_2 x_3 = 3 \end{cases}$$

sistem a cărui rezolvare revine la rezolvarea ecuației de gradul trei $t^3 - 2t^2 + 4t - 3 = 0$ ale cărei rădăcini sunt $t_1 = 1$, $t_{2,3} = \frac{1 \pm i\sqrt{11}}{2}$.

Deci o soluție a sistemului va fi $x_1 = 1$, $x_2 = \frac{1 + i\sqrt{11}}{2}$, $x_3 = \frac{1 - i\sqrt{11}}{2}$ și cum el este simetric în x_1, x_2, x_3 obținem alte cinci soluții ale sale prin permutările acestei soluții.

2) Dacă $s_2^2 + 4 = 0 \Rightarrow s_2 = \pm 2i$.

$$\text{Dacă } s_2 = 2i \text{ atunci } s_3 = 4i \text{ și deci } \begin{cases} x_1 + x_2 + x_3 = 2 \\ x_1 x_2 + x_1 x_3 + x_2 x_3 = 2i \\ x_1 x_2 x_3 = 4i \end{cases}$$

Obținem ecuația $t^3 - 2t^2 + 2it - 4i = 0$, adică $(t-2)(t^2 + 2i) = 0$.

Avem soluțiile $x_1 = 2$, $x_2 = \sqrt{-2i}$, $x_3 = -\sqrt{-2i}$ și permutările acestora.

Dacă $s_2 = -2i$ atunci $s_3 = -4i$ adică $(t-2)(t^2 - 2i) = 0$ și vom avea soluțiile $x_1 = 2$, $x_2 = \sqrt{2i}$, $x_3 = -\sqrt{2i}$ și permutările acestora.

10.70. Demonstrăm că P este ireductibil în $\mathbb{Z}[X]$.

Presupunem prin absurd că $P = P_1 \cdot P_2$, cu $P_1, P_2 \in \mathbb{Z}[X]$, neconstante. Deoarece $P(x) > 0$, oricare ar fi $x \in \mathbb{R}$, rezultă că P_1 și P_2 nu au rădăcini reale și deci păstrează semn constant pe \mathbb{R} ; Să zicem $P_1, P_2 > 0$ (analog, se va raționa dacă $P_1, P_2 < 0$).

Vom demonstra că $\text{grad } P_1 = \text{grad } P_2 = n$.

Să presupunem de exemplu că $\text{grad } P_1 < \text{grad } P_2$ și deci $\text{grad } P_1 < n$ iar $\text{grad } P_2 > n$.

Făcând $x = a_1, \dots, a_n$ avem:

$$P_1(a_1) \cdot P_2(a_1) = 1$$

.....

$$P_1(a_n) \cdot P_2(a_n) = 1.$$

Deoarece $P_1(x) > 0$ și $P_2(x) > 0$ rezultă

$$P_1(a_1) = P_2(a_1) = 1$$

.....

$$P_1(a_n) \cdot P_2(a_n) = 1. \quad (1)$$

Polinomul $P_1(X) - 1$ de grad mai mic decât n are n rădăcini a_1, \dots, a_n deci este polinomul identic nul. Deci $P_1(x) = 1$, oricare ar fi $x \in \mathbb{R}$, absurd!

Deci $\text{grad } P_1 = \text{grad } P_2 = n$ și din relațiile (1) deducem că $P_1(X) - 1 = \alpha(X - a_1) \dots (X - a_n)$ și $P_2(X) - 1 = \beta(X - a_1) \dots (X - a_n)$, cu $\alpha, \beta \in \mathbb{Z}$. Din $P = P_1 P_2$ deducem că

$$P = \alpha\beta(X - a_1)^2 \dots (X - a_n)^2 + (\alpha + \beta)(X - a_1) \dots (X - a_n) + 1,$$

de unde $\alpha\beta = 1$ și $\alpha + \beta = 0$, adică $-\alpha^2 = 1$, absurd!

Demonstrăm că Q este ireductibil în $\mathbb{Z}[X]$.

Se observă că $Q(a_i) = -1$, oricare ar fi i cu $1 \leq i \leq n$.

Presupunem prin reducere la absurd că $Q = Q_1 \cdot Q_2$, cu $Q_1, Q_2 \in \mathbb{Z}[X]$ neconstante și $\text{grad}(Q_1), \text{grad}(Q_2) < n = \text{grad}(Q)$.

Cum $Q(a_i) = -1$ rezultă că $Q_1(a_i)Q_2(a_i) = -1$ deci $Q_1(a_i) = 1$ și $Q_2(a_i) = -1$ sau $Q_1(a_i) = -1$ și $Q_2(a_i) = 1$ pentru un $i \in \{1, \dots, n\}$.

În ambele cazuri $Q_1(a_i) + Q_2(a_i) = 0$, oricare ar fi i cu $1 \leq i \leq n$ și $\text{grad}(Q_1 + Q_2) < n$. Cum polinomul $Q_1 + Q_2$ are gradul mai mic decât n și n rădăcini obținem că $Q_1 + Q_2 = 0$. Deci $Q_1 = -Q_2$.

Putem scrie $-Q_1^2(X) = (X - a_1)(X - a_2) \dots (X - a_n) - 1$.

Identificând coeficienții lui X^n din cei doi membrii obținem $1 = -1$, contradicție, deci Q este ireductibil.

10.71. Este clar că (0) și (X^n) , $n \in \mathbb{N}$, sunt ideale ale lui $K[[X]]$. Se arată acestea sunt singurele ideale ale sale. Dacă $I \neq (0)$ este un ideal, atunci fie $\text{ord}(I) = \min \{\text{ord}(f) \mid f \in I\}$. Se demonstrează că $I = (X^{\text{ord}(I)})$.

10.72. Termenul principal al polinomului f este $X_1^4 X_2^2$.

Atunci exponenții termenilor principali ai polinoamelor care vor rămâne după eliminarea succesivă a termenilor principali vor fi $(4,2,0)$, $(4,1,1)$, $(3,3,0)$, $(3,2,1)$ și $(2,2,2)$.

Deci $f = S_1^2 S_2^2 + a S_1^3 S_3 + b S_2^3 + c S_1 S_2 S_3 + d S_3^2$, unde a, b, c, d sunt numere reale. Determinăm acești coeficienți dând valori numerice nedeterminatele X_1, X_2, X_3 .

X_1	X_2	X_3	S_1	S_2	S_3	f
1	1	0	2	1	0	0
2	-1	-1	0	-3	2	0
1	-2	-2	-3	0	4	0
1	-1	-1	-1	-1	1	0

Obținem astfel sistemul de ecuații:
$$\begin{cases} 4 + b = 0 \\ -27b + 4d = 0 \\ -108a + 16d = 0 \\ 1 - a - b + c + d = 0 \end{cases} \quad \text{de unde}$$

$$\begin{cases} a = -4 \\ b = -4 \\ c = 18 \\ d = -27 \end{cases}$$

Prin urmare,

$$f = (X_1 - X_2)^2 (X_1 - X_3)^2 (X_2 - X_3)^2 = S_1^2 S_2^2 - 4S_1^3 S_3 - 4S_2^3 + 18S_1 S_2 S_3 - 27S_3^2.$$

10.73. Notând $X_1 + X_2 + \dots + X_n = S_1$, $X_1 X_2 + \dots + X_{n-1} X_n = S_2$, ..., $X_1 X_2 \dots X_n = S_n$, avem

$$\begin{aligned} f &= (S_1 - 2X_1) \dots (S_1 - 2X_n) = S_1^n - 2(X_1 + \dots + X_n) S_1^{n-1} - \dots + (-2)^n S_n = \\ &= -S_1^n + 4S_1^{n-2} S_2 - 8S_1^{n-3} S_3 + \dots + (-2)^n S_n. \end{aligned}$$

La același rezultat se ajunge și folosind procedeul descris în teorema fundamentală a polinoamelor simetrice.

10.74. Avem $Z^2 = Y^2X^2 - (XY-Z)(YX+Z) \in (X^2, XY-Z)$ și deci $Z^2K[X,Y] \subseteq (X^2, XY-Z) \cap K[X,Y]$.

Reciproc, dacă P este un polinom din $K[Y,Z]$ de forma $X^2g + (XY-Z)(t_0 + t_1X + t_2X^2)$ cu $g, t_2 \in K[X,Y,Z]$ și $t_0, t_1 \in K[Y,Z]$ atunci avem $P = X^2(g + (XY-Z)t_2 + t_1Y) + X(t_0Y - t_1Z) - t_0Z$, de unde rezultă $g + (XY-Z)t_2 + t_1Y = 0$ și $t_0Y - t_1Z = 0$.

Deci $Z|t_0$ și deducem că $P = -t_0Z \in Z^2K[Y,Z]$.

În concluzie, dacă g este compunerea morfismelor de inele $K[Y,Z] \rightarrow K[X,Y,Z]$ (incluziunea canonică) și $K[X,Y,Z] \rightarrow K[X,Y,Z]/(X^2, XY-Z)$ (surjecția canonică) atunci avem $\text{Ker}(g) = Z^2K[Y,Z]$.

Deci g induce o injecție $K[Y,Z]/(Z^2) \rightarrow K[X,Y,Z]/(X^2, XY-Z)$ care aplică $K[Y,Z]/(Z^2)$ izomorf pe $\text{Im}(g)$.

10.75. Morfismul de inele $f: K[X] \rightarrow K$, $f(a_0 + a_1X + \dots + a_nX^n) = a_0$ este surjectiv și $\text{Ker}(f) = (X)$. Atunci $K \simeq K[X]/(X)$ și $K[X]/(X)$ fiind inel, (X) este ideal maximal.

10.76. Aplicăm teorema fundamentală de izomorfism pentru inele morfismului de inele $\varphi: A[X_1, \dots, X_n] \rightarrow A$, dat prin $\varphi(P) = P(a_1, \dots, a_n)$.

10.77. Fie $f: \mathbb{Z}[X] \rightarrow \mathbb{Z}[\sqrt{d}]$ morfismul de \mathbb{Z} -algebre dat prin $f(X) = \sqrt{d}$. Evident, $\text{Ker}(f) \supseteq (X^2 - d)$. Fie $P \in \mathbb{Z}[X]$ a.î. $f(P) = P(\sqrt{d}) = 0$ și $R(X) = aX + b \in \mathbb{Z}[X]$ restul împărțirii lui $P(X)$ la $X^2 - d$. Obținem $R(\sqrt{d}) = 0$ și rezultă $R \equiv 0$, adică $\text{Ker}(f) = (X^2 - d)$. Aplicăm în continuare prima teoremă de izomorfism.

10.78. Aplicăm problema **8.39.**, pentru cazul $x = \text{cls}X \text{ mod } (X^2 + X + \hat{2})$.

Fie surjecția canonică $f_2: \mathbb{Z}_8[X]/(X^2 + X + \hat{2}) \rightarrow \mathbb{Z}_4[X]/(X^2 + X + \bar{2})$, unde „-” notează clasele modulo 4.

Conform problemei **8.39.**, clasa modulo $(X^2 + X + \bar{2})$ a elementului

$X + (X^2 - X)(\bar{1} + \bar{2}X - \bar{12}X^2 + \bar{8}X^3) = -X - \bar{2}$ (egalitatea se obține înlocuind X^2 cu $-X - \bar{2}$) constituie un element idempotent al inelului $\mathbb{Z}_4[X]/(X^2 + X + \bar{2})$.

La fel, clasa modulo $(X^2 + X + \bar{2})$ a elementului

$$\begin{aligned} & (-X - \hat{2}) + [(-X - \hat{2})^2 - (-X - \hat{2})][\hat{1} + \hat{2}(-X - \hat{2}) - \hat{12}(-X - \hat{2})^2] = \\ & = (-X - \hat{2}) + (\hat{4}X + \hat{4})(\hat{2}X - \hat{3}) = \hat{3}X + \hat{2} \end{aligned}$$

este un element idempotent diferit de 0 și 1 în inelul $\mathbb{Z}_8[X]/(X^2+X+\hat{2})$.

10.79. (i). Într-adevăr, dacă $f(a)$ este inversabil atunci există $a' \in A$ a.î. $aa' = 1+n$, unde $n \in A$ este un nilpotent. Dar $1+n$ este inversabil (suma dintre un element inversabil și unul nilpotent este element inversabil) deci și a este inversabil.

Reciproc este evident, pentru că morfismele de inele unitare transportă elementele inversabile în elemente inversabile.

(ii). Suficiența nu este adevărată.

De exemplu, pentru $A = \mathbb{Q}[X, Y]/(X^2, XY)$, $A' = \mathbb{Q}[Y]$ și f definit prin $f(\hat{P}(X, Y)) = P(0, Y)$, observăm că \hat{Y} este divizor al lui zero în A dar $f(\hat{Y})$ nu este divizor al lui zero.

În plus, $\text{Ker}(f) = (X)$ este format din elemente nilpotente.

Nici necesitatea nu este adevărată.

De exemplu, pentru $B = \mathbb{Q}[X, Y, Z]/(X^2, XY-Z)$ și $g: B \rightarrow A$, definit prin $g(\text{cls } P(X, Y, Z)) = P(X, Y, 0)$ observăm că $g(\text{cls } Y) = \hat{Y}$ este divizor al lui zero dar nu și $\text{cls } Y$.

Într-adevăr, dacă $(\text{cls } Y) \cdot (\text{cls}(a_1 X + G(Y)Z + H(Y))) = 0$, $a_1 \in \mathbb{Q}$ și $G(Y), H(Y) \in \mathbb{Q}[Y]$ atunci rezultă $\text{cls}(-a_1 Z + G(Y)YZ + YH(Y)) = 0$, adică $-a_1 Z + G(Y)YZ + YH(Y) \in (X^2, XY-Z) \cap \mathbb{Q}[Y, Z] = (Z^2)$ (vezi problema **10.74.**), ceea ce implică $a_1 = G(Y) = H(Y) = 0$.

Deci $\text{cls } Y$ nu este divizor al lui zero (am utilizat faptul că elementele lui B pot fi scrise sub forma $\text{cls}(a_1 X + G(Y)Z + H(Y))$, deoarece $XZ \in (X^2, XY-Z)$ iar XY aparține lui $\text{cls } Z$).

În plus, $\text{Ker}(g) = (\text{cls } Z)$, iar $\text{cls } Z$ este nilpotent pentru că $Z^2 \in (X^2, XY-Z)$.

(iii). Suficiența este evidentă.

Necesitatea nu este în general valabilă.

De exemplu, considerăm cazul $A = \mathbb{Z}_4[X]/(X^2+X-\hat{2})$, $A' = \mathbb{Z}_2[X]/(X^2-X)$, $f: A \rightarrow A'$ fiind morfismul surjectiv indus de morfismul $\mathbb{Z}_4 \rightarrow \mathbb{Z}_2$.

Atunci $f(\hat{X})$ este idempotent deși \hat{X} nu este idempotent.

BIBLIOGRAFIE

1. Gh. Andrei, C. Caragea, V. Ene : *Algebră : Culegere de probleme pentru examenele de admitere și olimpiade școlare*, Ed. Scorpion 7, București, 1995.
2. M. Becheanu, C. Vraciu : *Probleme de teoria grupurilor*, Reprografia Universității din București, 1982.
3. D. Bușneag : *Teoria grupurilor*, Ed. Universitaria, Craiova, 1994.
4. D. Bușneag, D. Piciu : *Lecții de algebră*, Ed. Universitaria, Craiova, 2002.
5. G. Călugăreanu, P. Hamburg: *Exercices in Basic Rings Theory*, Kluwer Academic Press, 1998.
6. C. Dan: *Probleme de algebra: Inele. Module. Teorie Galois*, Reprografia Universității din Craiova, 2000.
7. A. Dincă: *Lecții de algebră*, Ed. Universitaria, Craiova, 1999.
8. J. D. Dixon : *Problems in group theory*, Blaisdell Publishing Company, 1967.
9. A. Fadeev, I. Sominsky: *Problems in Higher algebra*, Mir Publishers Moscow, 1968.
10. I. D. Ion, C. Manoil, S. Răianu : *Structuri algebrice (probleme rezolvate)*, Reprografia Univ. din București, 1981.
11. I. D. Ion, C. Niță, N. Radu, D. Popescu: *Probleme de algebra*, Ed Didactică și Pedagogică, București, 1981.
12. I. D. Ion, N. Radu: *Algebra*, Ed Didactică și Pedagogică, București, 1991.
13. C. Năstăsescu, C. Niță, C Vraciu: *Bazele algebrei*, (vol.1), Ed Academiei, București, 1986.
14. C. Năstăsescu, M. Țena, G. Andrei, I. Odărașeanu : *Probleme de structuri algebrice*, Ed. tehnică, București, 1988.

15. C. Năstăsescu, C. Niță, M. Brandiburu, D. Joița : *Exerciții de algebră*, Ed. Didactică și Pedagogică, București, 1992.
16. C. Niță, T. Spiru : *Probleme de structuri algebrice*, Ed. tehnică, București, 1974.
17. L. Panaitopol, I. C. Drăghicescu: *Polinoame și ecuații algebrice*, Ed Albatros, București, 1980.
18. D. Popescu, C. Vraciu : *Elemente de teoria grupurilor finite*, Ed. Științifică și Enciclopedică, București, 1986.
19. J. S. Rose : *A course în Group Theory*, Cambridge University Press, 1978.
20. J. J. Rotman : *The Theory of Groups (An introduction)*, Allyn and Bacon Inc., 1966.
21. M. Suzuki : *Group Theory*, Springer – Verlag, 1982.
22. T. Spiru : *Structuri algebrice prin probleme*, Ed. Științifică, București, 1991.
23. I. Tomescu (coordonator) : *Probleme date la olimpiadele de matematică pentru liceu, (1950 – 1990)*, Ed. Științifică, București, 1992.
24. Gazeta Matematică (1980 – 2002).

Ne face plăcere să amintim aici numele autorilor mai multor probleme cuprinse în această lucrare (împreună cu soluțiile corespunzătoare) : T. Albu, Gh. Andrei, M. Andronache, B. Berceanu, Ș. Buzeteanu, M. Chiriță, I. Cuculescu, S. Dăscălescu, M. Deaconescu, I. Dinulescu, M. Ghergu, I. D. Ion, D. Miheț, C. Năstăsescu, C. Niță, L. Panaitopol, M. Piticari, D. Popovici, M. Rădulescu, S. Rădulescu, I. Savu și M. Țena.