Inele şi corpuri

Rezolvări

1. Fie $n \geq 2$. Să se arate că inelul $(\mathbb{Z}_n, +, \cdot)$ nu are divizori ai lui zero ddacă n este prim.

<u>Soluţie</u> „$\Rightarrow$" Prin contrapoziţie vom arăta că dacă n nu este prim atunci $(\mathbb{Z}_n, +, \cdot)$ are divizori ai lui zero.

Într-adevăr dacă n nu este prim atunci ~~el~~ are o descompunere $n = mk$ cu $1 < m, k < n$. Vom avea în $\mathbb{Z}_n$:

$$\hat{m} \cdot \hat{k} = \widehat{mk} = \hat{n} = \hat{0} \quad \text{dar } \hat{m} \neq \hat{0} \text{ şi } \hat{k} \neq \hat{0}.$$

„$\Leftarrow$" Dacă n este prim atunci fie $\hat{m} \cdot \hat{k} = \hat{0}$ în $\mathbb{Z}_n$. Avem $\widehat{mk} = \hat{0}$ deci $n \mid m \cdot k$. Deoarece n este prim deducem $n \mid m$ sau $n \mid k$ deci $\hat{m} = \hat{0}$ sau $\hat{k} = \hat{0}$ în $\mathbb{Z}_n$.

2. Să se rezolve ecuaţiile

a) $x^2 - \hat{4}x + \hat{3} = \hat{0}$ în $\mathbb{Z}_{11}$ şi $\mathbb{Z}_{15}$

b) $\hat{3}x^2 - \hat{4}x + \hat{1} = \hat{0}$ în $\mathbb{Z}_5$ şi $\mathbb{Z}_9$.

<u>Soluţie</u>. a) Avem $x^2 - \hat{4}x + \hat{3} = (x - \hat{1})(x - \hat{3})$ atât în $\mathbb{Z}_{11}$ cât şi $\mathbb{Z}_{15}$.

Din $(x - \hat{1})(x - \hat{3}) = \hat{0}$ în $\mathbb{Z}_{11}$ deducem (deoarece 11 este prim deci $\mathbb{Z}_{11}$ nu are divizori ai lui zero)

$$x - \hat{1} = \hat{0} \text{ sau } x - \hat{3} = \hat{0} \quad \text{deci } x = \hat{1} \text{ sau } x = \hat{3}$$

Din $(x - \hat{1})(x - \hat{3}) = \hat{0}$ în $\mathbb{Z}_{15}$ deducem $x - \hat{1} = \hat{0}$ sau $x - \hat{3} = \hat{0}$ sau ($x - \hat{1} = \hat{3}$ şi $x - \hat{3} = \hat{5}$) sau ($x - \hat{1} = \hat{5}$ şi $x - \hat{3} = \hat{3}$) în $\mathbb{Z}_{15}$.

$x - \hat{1} = \hat{3}$ şi $x - \hat{3} = \hat{5}$ nu conduc la soluţii dar

$x - \hat{1} = \hat{5}$ şi $x - \hat{3} = \hat{3}$ implică $x = \hat{6}$.

Deci mulţimea soluţiilor este $\{\hat{1}, \hat{3}, \hat{6}\}$.

b). Se poate încerca să se aplice aceeaşi metodă ca şi în cazul a). Aici vom prezenta o metodă alternativă

În $\mathbb{Z}_5$

x	$\hat{0}$	$\hat{1}$	$\hat{2}$	$\hat{3}$	$\hat{4}$
$\hat{3}x^2 - \hat{4}x + \hat{1}$	$\hat{1}$	$\hat{0}$	$\hat{0}$	$\hat{2}$	$\hat{3}$

Mulţimea soluţiilor: $\{\hat{1}, \hat{2}\}$.

În $\mathbb{Z}_9$

x	$\hat{0}$	$\hat{1}$	$\hat{2}$	$\hat{3}$	$\hat{4}$	$\hat{5}$	$\hat{6}$	$\hat{7}$	$\hat{8}$
$\hat{3}x^2-\hat{4}x+\hat{1}$	$\hat{1}$	$\hat{0}$	$\hat{5}$	$\hat{7}$	$\hat{6}$	$\hat{2}$	$\hat{4}$	$\hat{3}$	$\hat{8}$

Deci mulțimea soluțiilor este $\{\hat{1}\}$

Observație. Verificați cu atenție calculele! Sper să nu se fi strecurat vreo greșeală dar nu este nici imposibil!

3. Să se rezolve în $(\mathbb{Z}_{12},+,\cdot)$ sistemul de ecuații

$$\begin{cases} \hat{2}x+\hat{3}y+\hat{3}z=\hat{2} \\ \hat{6}x+\hat{4}y+\hat{2}z=\hat{6} \\ \hat{3}x+\hat{2}y+\hat{4}z=\hat{3} \end{cases}$$

Soluție. Vom adapta metoda Gauss de rezolvare a sistemelor. Modificăm sistemul inițial notat cu (S_0) după cum urmează:

$$(S1)\begin{cases} x+\hat{11}y+z=\hat{1} \\ \hat{6}x+\hat{4}y+\hat{2}z=\hat{6} \\ \hat{3}x+\hat{2}y+\hat{4}z=\hat{3} \end{cases}$$

(am înlocuit prima linie cu rezultatul diferenței dintre a treia linie și prima de dinainte)

$$(S2)\begin{cases} x+\hat{11}y+z=\hat{1} \\ \hat{10}y+\hat{8}z=\hat{0} \\ \hat{5}y+z=\hat{0} \end{cases}$$

(din a doua linie am scăzut-o pe prima înmulțită cu 6 iar din a treia linie am scăzut-o pe prima înmulțită cu 3)

$$(S3)\begin{cases} x+\hat{11}y+z=\hat{1} \\ \hat{6}y=\hat{0} \\ \hat{5}y+z=\hat{0} \end{cases}$$

(din a doua linie am scăzut-o pe a treia înmulțită cu 8)

Deci $\hat{6}y=\hat{0}$ de unde $y\in\{\hat{0},\hat{2},\hat{4},\hat{6},\hat{8},\hat{10}\}$.

Pt un y fixat obținem din a treia ec. $z=-\hat{5}\cdot y=\hat{7}y$ iar din prima ecuație $x=\hat{1}-\hat{11}y-z=\hat{1}+y-7y=\hat{1}-\hat{6}y=\hat{1}$.

Deci mulțimea soluțiilor sistemului (S3) este

$$\{(\hat{1},\hat{0},\hat{0}),(\hat{1},\hat{2},\hat{2}),(\hat{1},\hat{4},\hat{4}),(\hat{1},\hat{6},\hat{6}),(\hat{1},\hat{8},\hat{8}),(\hat{1},\hat{10},\hat{10})\}.$$

Sistemul (S3) nu este neapărat echivalent cu (S_0). Înmulțind o ecuație cu $\hat{6}$ (sau cu $\hat{3}$ sau cu $\hat{8}$) este posibil să introducem soluții noi pt. că aceste elemente sunt divizori ai lui zero în $\mathbb{Z}_{12}$. Se observă însă cu ușurință prin verificare directă că toate soluțiile lui (S3) sunt și soluții pt. (S_0).

4. Pentru $a,b \in \mathbb{R}$ notăm $M(a,b) = \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \in M_{2\times 2}(\mathbb{R})$.

a) Să se arate că $K = \{ M(a,b) \mid a,b \in \mathbb{R} \}$ este un corp în raport cu adunarea și înmulțirea obișnuite ale matricilor.

b) Corpurile K și $(\mathbb{C},+,\cdot)$ sunt izomorfe.

c) Să se rezolve în K sistemul de ecuații

$$\begin{cases} X + Y = M(3,3) \\ X^3 + Y^3 = M(-9,9) \end{cases}$$

Soluție. Avem $O_2 = M(0,0) \in K$ și $I_2 = M(1,0) \in K$.

Mai mult dacă $M(a,b), M(c,d) \in K$ avem

$$M(a,b) + M(c,d) = M(a+c, b+d) \in K$$

$$M(a,b)\cdot M(c,d) = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}\begin{pmatrix} c & d \\ -d & c \end{pmatrix} = \begin{pmatrix} ac-bd & ad+bc \\ -bc-ad & -bd+ac \end{pmatrix} = M(ac-bd, ad+bc) \in K$$

deci adunarea și înmulțirea obișnuite ale matricilor induc operații pe K (altfel spus K este parte stabilă față de adunarea și înmulțirea matricilor).

În sfârșit dacă $M(a,b) \in K$ atunci $-M(a,b) = M(-a,-b) \in K$

și dacă $O_2 \neq M(a,b) \in K$ atunci $a \neq 0$ sau $b \neq 0$ deci $a^2+b^2 \neq 0$.

Observăm că $\det M(a,b) = \begin{vmatrix} a & b \\ -b & a \end{vmatrix} = a^2+b^2$ deci

$$M(a,b)^{-1} = \frac{1}{a^2+b^2}\begin{pmatrix} a & -b \\ b & a \end{pmatrix} = M\left(\frac{a}{a^2+b^2}, -\frac{b}{a^2+b^2}\right) \in K.$$

Restul axiomelor care definesc corpul sunt evidente pentru că ele sunt deja valabile pt. adunarea și înmulțirea oricăror matrici. Mai precis

1) „+" este asociativă și comutativă

2) „+" are elem. neutru $O_2 \in K$

3) dacă $M(a,b) \in K$ atunci $-M(a,b) \in K$ (am văzut mai sus)

4) „·" este asociativă

5) „·" are elem. neutru $I_2 \in K$

6) $O \neq M(a,b) \in K \Rightarrow M(a,b)^{-1} \in K$ (am văzut mai sus).

7). „·" este distributivă bilateral față de „+".

b). Considerăm funcția $f: K \to \mathbb{C}$, $f(M(a,b)) = a+ib$.

Atunci $f(M(a,b)+M(c,d)) = f(M(a+c,b+d)) = (a+c)+i(b+d)$

$f(M(a,b)) + f(M(c,d)) = a+ib+c+id = (a+c)+i(b+d)$

$f(M(a,b)\cdot M(c,d)) = f(M(ac-bd, ad+bc)) = (ac-bd)+i(ad+bc)$

$f(M(a,b))\cdot f(M(c,d)) = (a+ib)(c+id) = (ac-bd)+i(ad+bc)$

$f(I_2) = f(M(1,0)) = 1+i0 = 1$

Mai mult f este bijectivă pt. că este inversabilă cu inversa

$f^{-1}: \mathbb{C} \to K$ $\quad f^{-1}(a+ib) = \begin{pmatrix} a & b \\ -b & a \end{pmatrix} = M(a,b)$.

c) Vom "transfera" sistemul din K într-unul în $\mathbb{C}$ cu ajutorul izomorfismului f de la b.

Notăm $x \doteq f(X)$, $y \doteq f(Y)$ și obținem

$$\begin{cases} x+y = 3+3i \\ x^3+y^3 = -9+9i \end{cases}$$

Sistemul este omogen și îl rezolvăm considerând $s \doteq x+y$ și $p = x\cdot y$.

Avem $x^3+y^3 = (x+y)^3 - 3xy(x+y) = s^3 - 3ps$. Deci

$$\begin{cases} s = 3+3i \\ s^3 - 3ps = -9+9i \end{cases}$$

$s^3 = (3+3i)^3 = 3^3(1+i)^3 = 27(1+i)^2(1+i) = 27\cdot(2i)\cdot(1+i) = -54+54i$

$3ps = s^3+9-9i = -54+54i+9-9i = -45+45i$

$3p(3+3i) = -45+45i$

$9p(1+i) = -45+45i$

$p(1+i) = -5+5i \quad |\cdot(1-i)$

$2p = (-5+5i)(1-i) = -5(1-i)^2 = (-5)\cdot(-2i) = 10i$

$p = 5i$

Deci x și y vor fi soluțiile ecuației $z^2-(3+3i)z+5i = 0$

De aici $\Delta = (3+3i)^2 - 4\cdot 5i = 9\cdot 2i - 20i = -2i = (1-i)^2$ și

$$x = \frac{3+3i+(1-i)}{2} = 2+i \text{ și } y = \frac{3+3i-(1-i)}{2} = 1+2i$$

sau

$$x = 1+2i \text{ și } y = 2+i.$$

Pt a ne întoarce în K aplicăm funcția inversă f^{-1} și obținem soluțiile

$$X = \begin{pmatrix} 2 & 1 \\ -1 & 2 \end{pmatrix} \text{ și } Y = \begin{pmatrix} 1 & 2 \\ -2 & 1 \end{pmatrix}$$

sau

$$X = \begin{pmatrix} 1 & 2 \\ -2 & 1 \end{pmatrix} \text{ și } Y = \begin{pmatrix} 2 & 1 \\ -1 & 2 \end{pmatrix}$$

5. a) Să se descompună în factori ireductibili polinomul $X^3 + \hat{1} \in \mathbb{Z}_3[X]$

b) Să se descompună în factori ireductibili polinomul $X^p + \hat{1} \in \mathbb{Z}_p[X]$.

Soluție. a) Avem $(X+\hat{1})^3 = X^3 + \hat{3}X^2 + \hat{3}X + \hat{1} = X^3 + \hat{1}$ în $\mathbb{Z}_3$ pt. că $\hat{3} = \hat{0}$.

b). Aplicând formula binomului lui Newton avem

$$(X+1)^p = X^p + C_p^1 X^{p-1} + C_p^2 X^{p-2} + \dots + C_p^{p-1} X + \hat{1} \quad \text{în } \mathbb{Z}_p[X]$$

Dar pt. orice $1 \le k \le p-1$ avem

$$C_p^k = \frac{p!}{k!(p-k)!} = \frac{(k+1)(k+2)\dots(p-1)p}{1\cdot 2\cdot 3\cdot\dots\cdot k}$$

Cum p este prim, el nu se divide cu nici un număr $2, 3, \dots, k$ (de la numărător) deci $p \mid C_p^k$ $(1 \le k \le p-1)$

Așadar $C_p^k \equiv 0 \pmod p$ pt. $1 \le k \le p-1$ deci

$$(X+\hat{1})^p = X^p + \hat{1} \quad \text{în } \mathbb{Z}_p[X].$$

6. Fie $R = \{0, 1, a, b\}$ un inel cu 4 elemente (0 și 1 sunt elementele neutre pt. adunare respectiv înmulțire).

a) Să se arate că dacă R nu are divizori ai lui zero atunci $(R, +)$ este izomorf cu grupul lui Klein.

b) R este corp dacă ecuația $1 + x = x^2$ are soluții în R.

c) Arătați că există un corp cu 4 elemente și că el este cu necesitate comutativ.

Soluție. a) Vom arăta că $\forall x \in R$ avem $x+x=0$. (egalitate care este adevărată în grupul lui Klein).

Fie $f: R \to R$, $f(x)=x+1$. Funcția f este bijectivă cu inversa $f^{-1}: R \to R$, $f^{-1}(x)=x-1$ (se verifică imediat). Prin urmare $f(0), f(1), f(a), f(b)$ sunt tot elem. $0, 1, a, b$ eventual în altă ordine. Avem atunci

$f(0)+f(1)+f(a)+f(b) = 0+1+a+b$

$1+0+1+1+1+a+1+b = 0+1+a+b$

Deci $1+1+1+1=0$ și mai departe $(1+1)(1+1)=0$.

Pentru că R nu are divizori ai lui zero rezultă $1+1=0$ deci $x+x = x(1+1) = x \cdot 0 = 0$, $\forall x \in R$.

Construim acum tabla lui $(R,+)$:

+	0	1	a	b
0	0	1	a	b
1	1	0	?	
a	a		0	
b	b			0

Știm că în tabla unui grup finit pe fiecare linie și pe fiecare coloană un element apare exact o dată. Prin urmare în locul semnului ? nu poate să apară 1, 0 sau a. Judecând analog ajungem la

+	0	1	a	b
0	0	1	a	b
1	1	0	b	a
a	a	b	0	1
b	b	a	1	0

care este tabla grupului lui Klein.

b). Dacă R este corp atunci nu are divizori ai lui zero deci se aplică punctul a) și $(R,+)$ este izomorf cu grupul lui Klein. (are tabla de mai sus).

Observăm că 1 și 0 nu sunt soluții ale ecuației $1+x=x^2$.

Într-adevăr $1+1=0\neq 1=1^2$ și $1+0=1\neq 0=0^2$.

Dar $1+a=b$ și $1+b=a$. (*)

Pt. că R nu are divizori ai lui zero $ab\neq 0$.

Mai mult din $ab=a$ ar rezulta prin înmulțire cu a^{-1} (care există prin ipoteză) $b=1$ – contradicție. Analog din $ab=b$ ar rezulta $a=1$ – contradicție. Deci $a \cdot b = 1$

Revenind la egalitățile (*) avem

$$a(1+a) = ab = 1 \Rightarrow a + a^2 = 1 \ /+a \Rightarrow a^2 = 1 + a$$

Obs Analog $b(1+b) = ba = 1 \Rightarrow b^2 = 1 + b$ deci atât a cât și b sunt soluții ale ecuației $1 + x = x^2$.

c). După aceleași principii ca și în cazul adunării construim tabla operației multiplicative. Rezultă cu necesitate tabla

$\cdot$	0	1	a	b
0	0	0	0	0
1	0	1	a	b
a	0	a	b	1
b	0	b	1	a

$a^2 = 1 + a = b$
$ab = 1$
$b^2 = 1 + b = a$ le știm deja
$ba = 1$

Se observă că R este comutativ și orice element nenul este inversabil. De pe tablă se citește mai greu asociativitatea și distributivitatea. Pentru asociativitate să observăm că dacă "decupăm" din tabla de mai sus linia și coloana lui 0 obținem tablă izomorfă cu grupul $(\mathbb{Z}_3, +)$:

$\cdot$	1	a	b
1	1	a	b
a	a	b	1
b	b	1	a

și

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

deci trebuie să funcționeze și asociativitatea în $(R, \cdot)$.

Distributivitatea o verificăm pt. fiecare caz. Mai întâi observăm că nu mai este nevoie să o verificăm bilateral pt. că R e comut. Deci trebuie să verificăm: $x(y+z) = xy + xz$, $\forall x, y, z \in R$.

Dacă $x = 0$ sau $x = 1$ atunci egalit. este evidentă

Pt că a și b au rol simetric atât față de adunare cât și față de înmulțire este suficient să verificăm pt. $x = a$.

Dacă $y = 0$ sau $z = 0$ egalit. este evidentă.

Deci avem de verificat $a(1+a) = a+a^2 \Leftrightarrow a \cdot b = a+b \Leftrightarrow 1=1$ „A"

$a(1+b) = a+ab \Leftrightarrow a \cdot a = a+1 \Leftrightarrow b=b$ „A"

$a(a+b) = a^2+b^2 \Leftrightarrow a \cdot 1 = b+a \Leftrightarrow 1=1$ „A"

Obs O variantă mai „elegantă" pt. a demonstra distributivitatea ar fi fost să găsim un „model", adică să găsim două operații despre care știm că sunt distributive una față de cealaltă și care au table izomorfe cu cele pentru $(R,+)$ respectiv $(R,\cdot)$ (așa cum am făcut de altfel pt. asociativitatea înmulțirii). Puteți încerca singuri, eu nu știu un model pe care să-l pot prezenta la clasa a XII-a! În matematică însă există o metodă de a construi un corp cu 4 elemente (în general a construi un corp cu p^k elemente unde p este număr prim și $k \geq 1$). Această metodă este o parte a celebrei teorii a lui Galois, în care se arată că ecuația generală de grad ≥ 5 nu poate fi rezolvată prin radicali, dar această teorie depășește cunoștințele clasei a XII-a. Vă doresc succes la admiterea la Facultatea de Matematică, unde vă veți putea întâlni și cu teoria lui Galois! Merită!

7. Să se arate că structurile de corp $(\mathbb{R},+,\cdot)$ și $(\mathbb{C},+,\cdot)$ nu sunt izomorfe.

Soluție. Diferența dintre $\mathbb{R}$ și $\mathbb{C}$ este existența elementului $i \in \mathbb{C}$ cu proprietatea că $i^2=-1$ Deci dacă $f: \mathbb{C} \to \mathbb{R}$ ar fi un izomorfism de corpuri atunci $f(1)=1$ prin definiție deci $f(-1)=-f(1)$ pt. că f este un morfism de grupuri între $(\mathbb{C},+)$ și $(\mathbb{R},+)$ iar morfismele de grupuri aplică simetricul (aici opusul) unui element în simetricul (opusul) imaginii. Deci elementul $u=f(i) \in \mathbb{R}$ trebuie să aibă proprietatea $u^2 = u \cdot u = f(i) \cdot f(i) = f(i^2) = f(-1) = -1$ Cum nu există un

asemenea element în $\mathbb{R}$, nu există un izomorfism $f: \mathbb{C} \to \mathbb{R}$.
(de corpuri).

<u>Obs</u>. Deși nu este chiar simplu de demonstrat, se poate arăta că grupurile $(\mathbb{C},+)$ și $(\mathbb{R},+)$ sunt izomorfe; deci există un izomorfism de grupuri $f: \mathbb{C} \to \mathbb{R}$ dar care nu poate fi un izomorfism de inele.

8. Fie $(R,+,\cdot)$ un inel.

a) Dacă $(x^2-x)y = y(x^2-x)$, $\forall x,y \in R$ atunci R este comutativ.

b) Dacă $(x^3-x^2)y = y(x^3-x^2)$, $\forall x,y \in R$ atunci R este comutativ.

c) Dacă $f: R \to R$ este un morfism surjectiv de grupuri între $(R,+)$ și el însuși astfel încât $(x^2-f(x))y = y(x^2-f(x))$, $\forall x,y \in R$ atunci R este comutativ

d) Dacă $y(xzx - zxz) = (xzx - zxz)y$, $\forall x,y,z \in R$ atunci R este comutativ.

<u>Soluție</u>. Vom începe prin a arăta următoarea:

<u>Lemă</u> $Z(R) = \{x \in R \mid xy = yx \ \forall y \in R\}$ este un subgrup al grupului abelian $(R,+)$.

<u>Dem</u>. $0 \in Z(R)$ pentru că $0 \cdot y = 0 = y \cdot 0$, $\forall y \in R$.

Dacă $x_1, x_2 \in Z(R)$ atunci avem $(x_1+x_2)y = x_1y + x_2y = yx_1 + yx_2 = y(x_1+x_2)$ deci $x_1+x_2 \in Z(R)$

Dacă $x \in Z(R)$ atunci $(-x)y = -(xy) = -(yx) = y(-x)$ deci $-x \in Z(R)$.

<u>Obs</u>. Este evident că $1 \in Z(R)$ și se poate arăta chiar mai mult că $Z(R)$ este un subinel (puteți să vă închipuiți cam ce ar însemna aceasta!) al lui R numit centrul lui R. Însă pe noi **vom** folosi numai că suma a două elemente din $Z(R)$ și opusul unui element din $Z(R)$ rămân în $Z(R)$. (proprietăți demonstrate înainte).

Desigur R este comutativ ddacă $R = Z(R)$

Acum începem să demonstrăm afirmațiile din enunț

a) Ipoteza ne spune că $x^2-x\in Z(R)$, $\forall x\in R$.

Atunci pt. $x,y\in R$ avem $(x+y)^2-(x+y)\in Z(R)$. Dar

$(x+y)^2-(x+y)=x^2+xy+yx+y^2-x-y=(x^2-x)+(y^2-y)+xy+yx$

Deoarece (x^2-x), $(y^2-y)\in Z(R)$ și $Z(R)$ este subgrup în $(R,+,\cdot)$ deducem $xy+yx\in Z(R)$.

Așadar $x(xy+yx)=(xy+yx)x$ de unde $x^2y+xyx=xyx+yx^2$ deci $x^2y=yx^2$.

Cum y a fost ales arbitrar rezultă $x^2\in Z(R)$

Folosind încă o dată ipoteza $x^2-x\in Z(R)$ rezultă $-x\in Z(R)$ ~~...~~ deci $x\in Z(R)$.

Am arătat că pt. un $x\in R$ arbitrar $x\in Z(R)$ deci $R=Z(R)$ este comut.

b) Ipoteza se rescrie $x^3-x^2\in Z(R)$, $\forall x\in R$. Deci

$(-x)^3-(-x)^2\in Z(R) \Rightarrow -x^3-x^2\in Z(R)$ (*)

$(x^3-x^2)+(-x^3-x^2)\in Z(R)\Rightarrow -2x^2\in Z(R)\Rightarrow 2x^2\in Z(R)$

Înlocuind în $x^3-x^2\in Z(R)$ pe x cu $x+1$ obținem

$(x+1)^3-(x+1)^2\in Z(R)\Rightarrow x^3+3x^2+3x+1-x^2-2x-1\in Z(R) \Rightarrow$

$$\left.\begin{array}{l} x^3+2x^2+x\in Z(R) \\ \text{Dar știm că } 2x^2\in Z(R)\end{array}\right\}\Rightarrow x^3+x\in Z(R)$$

Folosim din nou relația (*) $\Rightarrow$

$x^3+x+(-x^3-x^2)\in Z(R)\Rightarrow -x^2+x\in Z(R)\Rightarrow x^2-x\in Z(R)$

Am obținut așadar ipoteza de la a), deci R este comutativ.

c) Ipoteza se rescrie $x^2-f(x)\in Z(R)$, $\forall x\in R$.

Atunci pt. orice $x,y\in R$ avem $(x+y)^2-f(x+y)\in Z(R)\Rightarrow$

$x^2+xy+yx+y^2-f(x)-f(y)\in Z(R)$

$$\left.\begin{array}{l}(x^2-f(x))+(y^2-f(y))+xy+yx\in Z(R)\\ \text{Dar } x^2-f(x)\in Z(R) \text{ și } (y^2-f(y))\in Z(R)\end{array}\right\}\Rightarrow xy+yx\in Z(R)$$

Ca și în dem. de la a) obținem $x^2\in Z(R)$, $\forall x\in R$ ceea ce împreună cu $x^2-f(x)\in Z(R)$ implică $f(x)\in Z(R)$. Cum f este surj. rezultă că $\forall y\in R$ $\exists x\in R$ a.î. $y=f(x)\in Z(R)$ deci R este comutativ.

d) Se ia $z=1$ și obținem ipoteza de la a).