Algebră, anul I Informatică

28 noiembrie 2024

1 Obligatorii

Exerciţiul 1 (E2.1.53) *Să se arate că grupurile* $(\mathbb{R},+)$ *şi* $(R_+^*,\cdot)$ *sunt izomorfe.*

Soluţie. Considerăm funcţia $f:\mathbb{R}\to(0,\infty)$, $f(x)=e^x$. Funcţia este bijectivă. Este şi homomorfism, deoarece $f(x+y)=e^{x+y}=e^xe^y=f(x)f(y)$, deci este izomorfism. $f^{-1}:(0,\infty)\to\mathbb{R}$, $f^{-1}(x)=\ln x$ este de asemenea izomorfism. ■

Exerciţiul 2 (E2.1.57) *Să se găsească toate subgrupurile lui* $(\mathbb{Z},+)$. *Indicaţie: Să se arate că*

$$Sub(\mathbb{Z},+)=\{nZ|n\in\mathbb{N}\},\ \textit{unde}\ n\mathbb{Z}=\{nx|x\in\mathbb{Z}\}.$$

Soluţie. Arătăm întâi că $n\mathbb{Z}$ este subgrup.

- $n\mathbb{Z}$ este parte stabilă a lui $(\mathbb{Z},+)$. Fie $u,v\in n\mathbb{Z}$; există $x,y\in\mathbb{Z}$ astfel încât $u=nx$ şi $v=ny$. Dar $u+v=nx+ny=n(x+y)\in n\mathbb{Z}$.
- $0=0x$, deci $0\in n\mathbb{Z}$
- $nx+n(-x)=n(x-x)=0$.

$n\mathbb{Z}$ este grup ciclic infinit. Arătăm că $\forall H\le G\ \exists n\in\mathbb{N}$ astfel încât $H=n\mathbb{Z}$, adică orice grup netrivial al lui $\mathbb{Z}$ este de forma $n\mathbb{Z}$. Fie $n\in H$, $n>0$ cel mai mic element pozitiv al lui h (el există datorită bunei ordonări şi faptului că dacă $x\in H$ şi $-x\in H$): $n=\underbrace{1+1+\cdots+1}_{n}$. H fiind subgrup n, $2n$, ..., kn, $\dots\in H$, deci $n\mathbb{Z}\subseteq H$. Incluziunea inversă prin reducere la absurd. Presupunem că $\exists m\in\mathbb{Z}:m\in H\setminus n\mathbb{Z}$. Atunci $m\neq0$ şi de asemenea $-m\in H\setminus n\mathbb{Z}$. Putem presupune că $m>0$; altfel considerăm $-m$. Din teorema împărţirii cu rest avem $m=qn+r$, unde $0\le r<n$. Aceasta înseamnă că $r=m-qn\in H$ şi $0\le r<n$. Aceasta înseamnă că n nu este cel mai mic element al lui $H\cap\mathbb{Z}$. Deci nu există nici un $m\in H\setminus n\mathbb{Z}$ şi atunci $H\setminus n\mathbb{Z}=\varnothing$. Rezultă $H\subseteq n\mathbb{Z}$ şi din dubla incluziune avem $H=n\mathbb{Z}$. ■

Exerciţiul 3 (E2.1.58) *Să se găsească un exemplu de două subgrupuri ale unui grup a căror reuniune nu este subgrup.*

Soluţie. Fie grupul $(\mathbb{C}, +)$ şi subgrupurile sale $(G_1, +) = (\{a + 0i | a \in \mathbb{R}\}, +) \cong \mathbb{R}$ şi $(G_2, +) = (\{bi | b \in \mathbb{R}\}, +)$. $1 \in G_1$, $i \in G_2$, $1 + i \notin G_1 \cup G_2$. ∎

Exerciţiul 4 (E2.1.66) *Fie $f : G \to H$ un homomorfism de grupuri. Dacă $x \in G$ este de ordin finit, atunci tot aşa este şi $f(x)$, si avem $ord(f(x))|ord(x)$.*

Soluţie. Fie $n = ord(x)$. $x^n = 1 \wedge f$ homomorfism$\Longrightarrow f(x^n) = [f(x)]^n = f(1) = 1$, deci $f(x)$ este de ordin finit şi ordinul lui $f(x)$ este divizor al lui n. ∎

2 Opţionale

2.1.56, 2.1.59, 2.1.60, 2.1.61, 2.1.62, 2.1.63, 2.1.64, 2.1.65, 2.1.67, 2.1.68, 2.1.69.

Exerciţiul 5 (E2.1.56) *Fie $n \in \mathbb{N}$, $n \geq 2$. Să se arate că*

$$U_n = \{x \in C | \exists n \in \mathbb{N}\ x^n = 1\}$$

este un subgrup a grupului $(\mathbb{C}^*, \cdot)$ şi că U_n este ciclic. Să se găsească un izomorfism între $(\mathbb{Z}_n, +)$ şi $(U_n, \cdot)$.

Soluţie. $x, y \in U_n \Longrightarrow (xy)^n = x^n y^n$ (comutativitate) $= 1 \Longrightarrow xy \in U_n$ parte stabilă

$1 \in U_n$, $x \in U_n \Longrightarrow \frac{1}{x^n} = \left(\frac{1}{x}\right)^n = 1 \Longrightarrow \frac{1}{x} = x^{-1} \in U_n \Longrightarrow U_n \leq C^*$.

Dar

$$U_n = \{z_k | k = 0, \ldots, n-1\} = \left\{\cos\frac{2k\pi}{n} + i\sin\frac{2k\pi}{n} | k = 0, \ldots, n-1\right\}.$$

Din formula lui Moivre rezultă că $U_n = \langle z_1 \rangle$, unde $z_1 = \cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n}$. Se observă că $z_k = z_1^k$ şi $z_1^n = z_0 = 1$.

Izomorfismul: $f : U_n \to \mathbb{Z}_n$, $f(z_k) = [k]$; se constată că este bijecţie şi $f(z_i z_j) = f(z_{i+j}) = [i+j] = [i] + [j] = f(z_i) + f(z_j)$, adică f este homomorfism. ∎

Exerciţiul 6 (E2.1.59) *Fie $(G, +)$ un grup abelian şi $H, K \leq G$ două subgrupuri. Să se arate că $\langle H \cup K \rangle = H + K$, unde $H + K = \{x + y | x \in H, y \in K\}$.*

Soluţie.

$$\langle H \cup K \rangle = \sup\{H, K\} = \left\{\sum_{j=1}^{n} x_j : x_j \in H \cup K, k \in \mathbb{N}^*\right\}. \tag{1}$$

$H + K$ este subgrup al lui G: $e \in G$, $e = e + e \in H + K$;

$$\left.\begin{array}{r} u \in H + K \Longrightarrow \exists h \in H \wedge \exists k \in K\ u = h + k; \\ h \in H \Longrightarrow -h \in H; \\ k \in K \Longrightarrow -k \in K; \end{array}\right\} \Longrightarrow -h-k = -(h+k) \in H+K$$

Deoarece $H \leq H+K$ şi $K \leq H+K$, rezultă $\langle H \cup K\rangle \leq H+K$.

Fie $u \in H+K \Longrightarrow \exists h \in H \wedge \exists k \in K\ u = h+k = k+h$. Elementele lui $H+K$ sunt sume de elemente din H sau K; datorita comutativităţii ele pot fi scrise în orice ordine, deci conform lui (1) $u \in \langle H \cup K\rangle$. ■

Exerciţiul 7 (E2.1.60) *Fie $(G,\cdot)$ un grup şi $H, K \leq G$. Să se arate că $H \cup K \leq G$ ddacă $H \subseteq K$ sau $K \subseteq H$.*

Soluţie. ($\Longleftarrow$) Dacă $H \subseteq K$ sau $K \subseteq H$, $H \cup K = K$ sau $H \cup K = H$, care sunt subgrupuri.

($\Longrightarrow$) $H, K \leq G$, $e \in H$, $e \in K \Longrightarrow e \in H \cup K$

$x \in H \cup K \Longrightarrow \left.\begin{array}{c}(x \in H) \vee (x \in K) \\ H, K \leq G\end{array}\right\} \Longrightarrow (x^{-1} \in H) \vee (x^{-1} \in K) \Longrightarrow x^{1} \in H \cup K$

În general $H \cup K$ nu este parte stabilă. Presupunem că este.

Pres. că $(H \nsubseteq K) \wedge (K \nsubseteq H) \Longleftrightarrow \{\exists h \in H \setminus K \wedge \exists k \in K \setminus H\}$. Fie $u = kh \in K \cup H$.

$$kh \in H \cup K \Longrightarrow \left\{\begin{array}{c} kh \in K \Longrightarrow k^{-1}kh \in K \Longrightarrow h \in K \text{ contradicţie} \\ \vee \\ kh \in H \Longrightarrow khh^{-1} \in H \Longrightarrow k \in H \text{ contradicţie}\end{array}\right.$$

Deci este adevărată negaţia lui $(H \nsubseteq K) \wedge (K \nsubseteq H)$, adică $(H \subseteq K) \vee (K \subseteq H)$. ■

Exerciţiul 8 (E2.1.61) *Fie $n, m \in \mathbb{Z}$. Să se arate că*

(a) $n\mathbb{Z} \subseteq m\mathbb{Z}, m|n$.

(b) $n\mathbb{Z} \cap m\mathbb{Z} = k\mathbb{Z}$, *unde* $k = \operatorname{lcm}(n,m)$.

(c) $n\mathbb{Z} + m\mathbb{Z} = d\mathbb{Z}$, *unde* $d = \gcd(n,m)$.

Soluţie. Grupurile de forma $p\mathbb{Z}$, $p \in \mathbb{Z}$ sunt abeliene.

(a) $m|n \Longrightarrow \exists a \in \mathbb{Z}\ n = am$. Se observă că

$$m\mathbb{Z} = \{0, m, \ldots, km, \ldots\}$$

şi

$$n\mathbb{Z} = \{0, n, \ldots, kn, \ldots\} = \{0, am, \ldots, akm, \ldots\}.$$

Fie $u = kn \in n\mathbb{Z}$. Avem $kn = akm \in m\mathbb{Z}$.

(b) Fie $x \in n\mathbb{Z} \cap m\mathbb{Z}$, rezultă că x este multiplu de m şi n, deci şi multiplu de $k = \operatorname{lcm}(n,m)$, adică $m \in k\mathbb{Z}$. Reciproc, dacă $y \in k\mathbb{Z}$, y trebuie să fie multiplu de m, adică $y \in m\mathbb{Z}$ şi multiplu de n, adică $y \in n\mathbb{Z}$, deci $y \in n\mathbb{Z} \cap m\mathbb{Z}$.

(c) ($\subseteq$) Conform punctului (a)

$$d|m \wedge d|n \Rightarrow m\mathbb{Z} \subseteq d\mathbb{Z} \wedge n\mathbb{Z} \subseteq d\mathbb{Z} \Rightarrow \langle n\mathbb{Z} \cup m\mathbb{Z} \rangle = n\mathbb{Z} + m\mathbb{Z} \subseteq d\mathbb{Z}$$

(conform exerciţiului 6).

($\supseteq$) $d = \gcd(n,m) \Rightarrow \exists s,t \in \mathbb{Z}\ d = sm + tn$. Fie $x \in d\mathbb{Z}$; $x = dk = (sm+tn)k = msk + ntk \in n\mathbb{Z} + m\mathbb{Z}$.

■

Exerciţiul 9 (E2.1.62) *Să se arate că pentru* $n, m \in \mathbb{N}$ *cu* $d = \gcd(n,m)$, *există două numere întregi* $s, t \in \mathbb{Z}$, *astfel încât* $d = sn + tm$. *Folosiţi acest rezultat ca să arătaţi că* $1 = gcd(n,m)$ *ddacă există* $s, t \in \mathbb{Z}$ *astfel încât* $1 = sn + tm$.

Soluţie. Fie şirul împărţirilor succesive din algoritmul lui Euclid

$$a = bq_1 + r_1, \qquad r_1 = 0 \ \vee r_1 < b \tag{2}$$
$$b = r_1 q_2 + r_2, \qquad r2 = 0 \vee r_2 < r_1 \tag{3}$$
$$r_1 = r_3 q_3 + r_3, \qquad r_3 = 0 \vee r_3 < r_2 \tag{4}$$
$$\vdots$$
$$r_{n-2} = r_{n-1} q_n + r_n, \qquad r_n = 0 \vee r_n < r_{n-1} \tag{5}$$
$$r_{n-1} = r_n q_{n+1}, \tag{6}$$

unde ultimul rest nenul este $c.m.m.d.c(a,b)$. Din (2) obţinem $r_1 = a - q_1 b = k_1 a + l_1 b$. Din (E2) obţinem $r_2 = b - r_1 q_2 = b - (k_1 a + l_1 b)\, q_2 = (-k_1 q_2)a + (1 - l_1 q_2)\, b = k_2 a + l_2 b$ unde $k_2 = -k_1 q_2$, $l_2 = 1 - l_1 q_2$. Presupunem că pentru m, $1 \leq m \leq n-1$ avem că pentru orice i, $1 \leq i \leq m$, există k_i, $l_i \in \mathbb{Z}$ astfel încât

$$r_i = k_i a + l_i b.$$

Din (6) rezultă că

$$\begin{aligned} r_{m+1} = r_{m-1} - r_m q_{m+1} &= k_{m-1} a + l_{m-1} b - (k_m a + l_m b)\, q_{m+1} \\ &= ()\, a + (l_{m-1} - l_m q_{m+1})\, b = k_{m+1} a + l_{m+1} b, \end{aligned}$$

unde

$$\begin{aligned} k_{m+1} &= k_{m-1} - k_m q_{m+1} \\ l_{m+1} &= l_{m-1} - l_m q_{m+1}. \end{aligned}$$

Rezultă prin inducţie că

$$r_n = k_n a + l_n b.$$

r_n este c.m.m.d.c. l lui a şi b. Luăm $s = k_n$, $t = l_n$. ■

Exerciţiul 10 (E2.1.63) *Să se folosească algoritmul lui Euclid pentru ca plecând de la $n, m \in \mathbb{N}$ să determinăm numerele întregi s, t cu proprietatea că* $\gcd(n, m) = sn + tm$.

Soluţie.

Teorema 11 (recursivitate c.m.m.d.c) *Pentru orice întreg nenegativ a şi orice întreg pozitiv b,*

$$\gcd(a, b) = \gcd(b, a \bmod b).$$

Demonstrație. Vom arăta că $\gcd(a, b)$ şi $\gcd(a, b)$ se divid unul pe altul, deci conform antisimetriei ele trebuie să fie egale (deoarece ambele sunt nenegative). Arătăm întâi că $\gcd(a, b) | \gcd(b, a \bmod b)$. Dacă $d = \gcd(a, b)$, atunci $d|a$ and $d|b$. Din teorema împărţirii cu rest, $a \bmod b = a - qb$, unde $q = \lfloor a/b \rfloor$. Deoarece $a \bmod b$ este o combinație liniară a lui a şi b, rezultă că $d| (a \bmod b)$. Deci, deoarece $d|b$ şi $d| \ (a \bmod b)$, din definiția lui gcd rezultă că $d| \gcd(b, a \bmod b)$ sau, echivalent, că

$$\gcd(a, b) | \gcd(b, a \bmod b). \tag{7}$$

Demonstrația lui $\gcd(b, a \bmod b) | \gcd(a, b)$ este aproape identică. Dacă luăm acum $d = \gcd(b, a \bmod b)$, atunci $d|b$ şi $d|(a \bmod b)$. Deoarece $a = qb + a \bmod b$, unde $q = \lfloor a/b \rfloor$, avem că a este o combinație liniară a lui b şi $a \bmod b$, de unde deducem că $d|a$. Deoarece $d|b$ şi $d|a$, avem $d| \gcd(a, b)$ sau, echivalent, că

$$\gcd(b, a \bmod b) | \gcd(a, b). \tag{8}$$

concluzia rezultă din (7) and (8) din antisimetria lui $|$. ∎

Elementele lui Euclid (circa 300 B.C.) descriu algoritmul gcd, deşi el ar putea avea o origine mult mai veche. Vom exprima algoritmul lui Euclid sub formă recursivă bazându-ne direct pe teorema 11. Intrările a şi b sunt întregi nenegativi arbitrari.

Euclid(a, b)
1: **if** $b == 0$ **then**
2:     **return** a
3: **else**
4:     **return** Euclid$(b, a \bmod b)$
5: **end if**

Ca exemplu de execuție a lui Euclid, să consideră calculul lui $\gcd(30, 21)$:

$$\begin{aligned} \text{Euclid}(30, 21) &= \text{EUCLID}(21, 9) \\ &= \text{EUCLID}(9, 3) \\ &= \text{EUCLID}(3, 0) \\ &= 3. \end{aligned}$$

Calculul acesta apelează recursiv Euclid de trei ori.

Corectitudinea lui Euclidrezultă din teorema 11 şi din proprietatea că dacă algoritmul returneză a în linia 2, atunci $b = 0$, deci $\gcd(a, b) = \gcd(a, 0) = a$.

Algoritmul nu se poate autoapela recursiv indefinit, deoarece al doilea argument descreşte strict şi este *ntotdeauna* nenegativ.

De aceea, EUCLID se termină întotdeauna cu răspunsul corect.

Forma extinsă a algoritmului lui Euclid

Vom rescrie algoritmul lui Euclid pentru a calcula coeficienţii întregi x şi y astfel încât

$$d = gcd(a, b) = ax + by. \tag{9}$$

De notat că x şi y pot fi negative sau zero. Aceşti coeficienţi sunt utili în Informatică la calculul inversului modular. Procedure EXTENDED-EUCLID acceptă la intrare o pereche de întregi nenegativi şi returnează un triplet de forma (d, x, y) care satisface ecuaţia (9).

EXTENDED-EUCLID (a, b)

1: **if** b==0 **then**
2:     **return** (a, 1, 0)
3: **else**
4:     (d', x', y') =EXTENDED-EUCLID$(b, a \bmod b)$
5:     $(d, x, y) = (d', y', x' - \lfloor a/b \rfloor y')$
6:     **return** (d, x, y)
7: **end if**

Tabela de mai jos ilustrează calculul lui gcd$(99, 78)$ cu EXTENDED-EUCLID.

a	b	$\lfloor a/b \rfloor$	d	x	y
99	78	1	3	11	14
78	21	3	3	3	11
21	15	1	3	2	3
15	6	2	3	1	2
6	3	2	3	0	1
3	0	–	3	1	0

Procedura EXTENDED-EUCLID este o variantă a procedurii EUCLID. Linia 1 este echivalentă cu testul "$b == 0$" din linia 1 a lui EUCLID. Dacă $b = 0$, atunci EXTENDED-EUCLID returnează nu numai $d = a$ în linia 2, dar de asemenea şi coeficienţii $x = 1$ şi $y = 0$, astfel că $a = ax+by$. Dacă $b \neq 0$, EXTENDED-EUCLID calculează întâi (d', x', y') astfel încât $d' = |\, \gcd(b, a \bmod b)$ şi

$$d' = bx' - (a \bmod b)y'. \tag{10}$$

La fel ca în EUCLID, avem în acest caz $d = \gcd(a, b) = d' = gcd(b, a \bmod b)$.

Pentru a obţine x şi y astfel încât $d = ax + by$, începem prin a rescrie ecuaţia (10) utilizând ecuaţia $d = d'$ ecuaţia (3.8):

$$\begin{aligned} d &= bx\prime + (a - b \lfloor a/b \rfloor)\, y' \\ &= ay' - b\, (x' - \lfloor a/b \rfloor y')\, . \end{aligned}$$

Astfel, alegând $x = y'$ şi $y = x' - \lfloor a/b \rfloor y'$ ecuaţia $d = ax+by$ este satisfăcută, dovedindu-se corectitudinea lui EXTENDED-EUCLID. ■

Deoarece numărul de apeluri recursive din Euclid este egal cu numărul de apeluri recursive din Extended-Euclid, timpii de execuție ai lui Euclid şi Extended-Euclid sunt identici, pqna la un factor constant. Adica, pentru $a > b > 0$, numărul de apeluri recursive este $O(\log b)$.

Exerciţiul 12 (E2.1.64) *Să se găsească toate grupurile (pâna la un izomorfism) care se pot defini pe o mulţime cu 4 elemente.*

Soluţie. Grupul ciclic $\mathbb{Z}_4$ şi grupul lui Klein. Grupul ciclic are tabela

$+$	$\widehat{0}$	$\widehat{1}$	$\widehat{2}$	$\widehat{3}$
$\widehat{0}$	$\widehat{0}$	1	2	3
1	1	2	3	0 .
2	2	3	0	1
3	3	0	1	2

Pentru orice grup G ordinul unui element diferit de e trebuie să dividă ordinul grupului, adică pe 4. Rezultă că elementele nenule trebuie să aibă ordinul 2.

$+$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

Grupul lui Klein este izomorf cu $(\mathbb{Z}_2 \times \mathbb{Z}_2, +)$ sau cu grupul diedral D_2 (izometriile dreptunghiului care nu este pătrat). ■

Exerciţiul 13 (E2.1.65) *Fie $(G, \cdot)$ un grup şi $x, y \in G$ astfel încât $xy = yx$. Avem:*

(a) $ord(x^{-1}) = ord(x)$

(b) $ord(xy) = ord(yx)$.

Soluţie. $ord(x) = n \Rightarrow x^n = 1 \Rightarrow (x^{-1})^n = (x^n)^{-1} = 1$, deci $ord(x^{-1}) = n$. Conform enunÈ>ului $ord(xy) = ord(yx)$. ■

Exerciţiul 14 (E2.1.67) *Două grupuri ciclice infinite sunt izomorfe. Două grupuri ciclice finite sunt izomorfe ddacă au acelaşi număr de elemente.*

Soluţie. Dacă $(G, \cdot)$ şi $(G', \cdot)$ sunt două grupuri ciclice infinite şi $G = \langle x \rangle_g$ şi $G' = \langle y \rangle_g$, atunci aplicaţia $f : G \to G'$, $f\left(x^k\right) = y^k$ este un izomorfism.

Fie G_1 şi G_2 două grupuri ciclice finite. Dacă ele au acelaşi număr de elemente, $n = |G_1| = |G_2|$, există $x \in G_1$ şi $y \in G_2$ astfel încât $ord(x) = n$ şi $ord(y) = n$.

Dar

$$G_1 = \langle x \rangle = \left\{x^0 = 1, x, x^2, \ldots, x^{n-1}\right\}$$

şi

$$G_2 = \langle y \rangle = \left\{ y^0 = 1, y, y^2, \ldots, y^{n-1} \right\};$$

aplicaţia $f : G_1 \to G_2$, $f\left(x^k\right) = y^k$ este un izomorfism.

Reciproc presupunem că G_1 şi G_2 sunt două grupuri ciclice finite izomorfe, şi fie $f : G_1 \to G_2$ un izomorfism. f fiind bijectivă, $|G_1| = |G_2|$. ■

Exerciţiul 15 (E2.1.68) *Dacă G este un grup ciclic, atunci există un homomorfism surjectiv $\mathbb{Z} \to G$.*

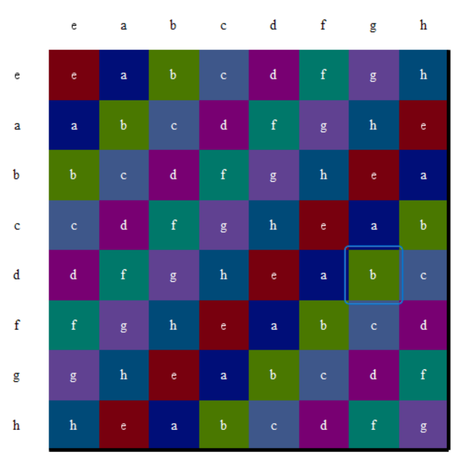
Soluţie. Dacă G este un grup ciclic infinit, $\mathbb{Z}$ şi G sunt izomorfe; orice izomorfism este homorfism surjectiv. Dacă G este finit şi are ordinul n el este izomorf cu $\mathbb{Z}_n$. Fie $f : \mathbb{Z}_n \to G$ un izomorfism. Funcţia $g : \mathbb{Z} \to \mathbb{Z}_n$ definită prin $g(z) = [z]$ este homomorfism surjectiv.Compusa $h = f \circ g : \mathbb{Z} \to \mathbb{G}$ este un homomorfism surjectiv. ■

Exerciţiul 16 (E2.1.69) *Să se arate că următoarele perechi de grupuri nu sunt izomorfe: $(\mathbb{Z}_n, +)$ şi $(\mathbb{Z}_m, +)$ şi $n \neq m$; $(\mathbb{Z}, +)$ şi $(\mathbb{Q}, +)$; $(\mathbb{Z}_8, +)$ şi $(Z_4 \times \mathbb{Z}_2, +)$ (pentru grupul produs vezi exerciţiul 2.1.47).*

Soluţie. $(\mathbb{Z}_n, +)$ şi $(\mathbb{Z}_m, +)$ sunt grupuri ciclice finite. Ele nu pot fi izomorfe, deoarece au număr diferit de elemente.

$(\mathbb{Z}_8, +)$ şi $(Z_4 \times \mathbb{Z}_2, +)$ - $(\mathbb{Z}_8, +)$ este ciclic, ar trebui ca şi $(Z_4 \times \mathbb{Z}_2, +)$ să fie ciclic; dacă ar fi ciclic toate subgrupurile sale ar trebui să fie ciclice, dar are un subgrup izomorf cu grupul Lui Klein şi anume $(\{(0,0), (0,1), (2,0), (2,1)\}, +)$.

Iată tabelele operaţiilor



	e	a	b	c	d	f	g	h
e	e	a	b	c	d	f	g	h
a	a	b	c	d	f	g	h	e
b	b	c	d	f	g	h	e	a
c	c	d	f	g	h	e	a	b
d	d	f	g	h	e	a	b	c
f	f	g	h	e	a	b	c	d
g	g	h	e	a	b	c	d	f
h	h	e	a	b	c	d	f	g

Figura 1: Tabela lui $(\mathbb{Z}_8, +)$

■

	e	a	b	c	d	f	g	h
e	e	a	b	c	d	f	g	h
a	a	b	c	e	f	g	h	d
b	b	c	e	a	g	h	d	f
c	c	e	a	b	h	d	f	g
d	d	f	g	h	e	a	b	c
f	f	g	h	d	a	b	c	e
g	g	h	d	f	b	c	e	a
h	h	d	f	g	c	e	a	b

Figura 2: Tabela grupului lui $\mathbb{Z}_4 \times \mathbb{Z}_2$