Diszkrét matematika II.: 5. feladatlap 2 a, b, c, d és e feladatainak megoldása

Szoftverfejlesztő szakirány, 2019 ősz

(a) $(\mathbb{Z}, +, \cdot)$. [Megjegyzés: Ebben feladatban igazából nem bizonyítjuk be a $+$ és $\cdot$ műveletek olyan alaptulajdonságait $\mathbb{Z}$-n mint például az asszociativitás, hanem ezeket ismertnek tételezzük fel (mivel e tulajdonságok bizonyításához az egész számok és a $+$, $\cdot$ műveletek axiomatikus felépítésére lenne szükség). Ehelyett sorra vesszük a bizonyítandó tulajdonságokat, és eddigi tudásunk alapján megállapítjuk, hogy ezek teljesülnek-e.]

(i)
- $+$ binér művelet $\mathbb{Z}$-n, mert egész számok összege mindig egész szám.
- $+$ asszociatív $\mathbb{Z}$-n, mert $\forall a, b, c \in \mathbb{Z} : (a + b) + c = a + (b + c)$.
- $0 \in \mathbb{Z}$ semleges elem, mert $\forall a \in \mathbb{Z} : a + 0 = 0 + a = a$.
- Minden egésznek létezik additív inverze: $\forall a \in \mathbb{Z} : -a \in \mathbb{Z}$ és $a+(-a) = (-a)+a = 0$.

$\Rightarrow (\mathbb{Z}, +)$ Abel-csoport.

(ii)
- $\cdot$ binér művelet $\mathbb{Z}$-n, mert egész számok szorzata mindig egész szám.
- $\cdot$ asszociatív $\mathbb{Z}$-n, mert $\forall a, b, c \in \mathbb{Z} : (a \cdot b) \cdot c = a \cdot (b \cdot c)$.

$\Rightarrow (\mathbb{Z}, \cdot)$ félcsoport.

(iii) Teljesül $\cdot$ mindkét oldali disztributivitása $+$ felett, mert
$\forall a, b, c \in \mathbb{Z} : a \cdot (b + c) = a \cdot b + a \cdot c$ és $(a + b) \cdot c = a \cdot c + b \cdot c$
$\Rightarrow (\mathbb{Z}, +, \cdot)$ $\underline{\underline{\text{gyűrű}}}$.

(iv) Abel-csoport-e $(\mathbb{Z} \setminus \{0\}, \cdot)$?
- $\cdot$ művelet $(\mathbb{Z} \setminus \{0\})$-n, mert nemnulla egészek szorzata mindig nemnulla egész.
- $\cdot$ asszociativitását fent már „beláttuk" (azaz említettük).
- $1 \in \mathbb{Z} \setminus \{0\}$ egységelem, mert $\forall a \in \mathbb{Z} \setminus \{0\} : 1 \cdot a = a \cdot 1 = a$.
- Nincs minden elemnek multiplikatív inverze: pl. $2 \in \mathbb{Z} \setminus \{0\}$-höz nem létezik olyan $x \in \mathbb{Z} \setminus \{0\}$, melyre $2 \cdot x = 1$.

$\Rightarrow (\mathbb{Z} \setminus \{0\}, \cdot)$ nem csoport, így $(\mathbb{Z}, +, \cdot)$ $\underline{\underline{\text{nem test}}}$.

(b) $(2\mathbb{Z}, +, \cdot)$

[Megjegyzés: Ebben a bizonyításban felhasználhatjuk a $+$ és a $\cdot$ műveletek tulajdonságait $\mathbb{Z}$-n és hivatkozhatunk ezekre.]

(i)
- $+$ binér művelet $2\mathbb{Z}$-n, mert páros számok összege mindig páros szám, hiszen $\forall 2m, 2n \in \mathbb{Z}$: $2m + 2n = 2(m + n) \in 2\mathbb{Z}$.
- $+$ asszociatív $\mathbb{Z}$-n, így $2\mathbb{Z} \subseteq \mathbb{Z}$ miatt $+$ asszociatív $2\mathbb{Z}$-n is (más szóval az asszociativitás öröklődik $\mathbb{Z}$-ről $2\mathbb{Z}$-re).
- $0 \in 2\mathbb{Z}$ semleges elem, mert $\forall a \in 2\mathbb{Z} : a + 0 = 0 + a = a$.
- Tetszőleges $\forall 2m \in 2\mathbb{Z}$ inverze $-2m$, mert $-2m = 2(-m) \in 2\mathbb{Z}$ és $2m + (-2m) = (-2m) + 2m = 0$.
- $+$ kommutatív $\mathbb{Z}$-n, így $2\mathbb{Z} \subseteq \mathbb{Z}$ miatt $+$ kommutatív $2\mathbb{Z}$-n is (más szóval a kommutativitás öröklődik $\mathbb{Z}$-ről $2\mathbb{Z}$-re).

$\Rightarrow (2\mathbb{Z}, +)$ Abel-csoport.

(ii)
- $\cdot$ binér művelet $2\mathbb{Z}$-n, mert páros számok szorzata mindig páros szám, hiszen $\forall 2m, 2n \in 2\mathbb{Z} : (2m)(2n) = 2(m2n) = 2(2mn) \in 2\mathbb{Z}$.

- $\cdot$ asszociatív $\mathbb{Z}$-n, és $2\mathbb{Z} \subseteq \mathbb{Z}$ miatt $\cdot$ asszociatív $2\mathbb{Z}$-n is.

$\Rightarrow (\mathbb{Z}, \cdot)$ félcsoport.

(iii) $\mathbb{Z}$-ben teljesül $\cdot$ mindkét oldali disztributivitása $+$ felett, és $2\mathbb{Z} \subseteq \mathbb{Z}$ miatt ez öröklődik $2\mathbb{Z}$-re.

Tehát $(2\mathbb{Z}, +, \cdot)$ $\underline{\underline{\text{gyűrű}}}$.

(iv) Abel-csoport-e $(2\mathbb{Z} \setminus \{0\}, \cdot)$?

- $\cdot$ művelet $(2\mathbb{Z} \setminus \{0\})$-n: nemnulla páros számok szorzata mindig nemnulla páros szám.
- $\cdot$ asszociativitását fent már beláttuk.
- Nincs egységelem $2\mathbb{Z} \setminus \{0\}$-ben, mert $\nexists e \in 2\mathbb{Z}$, melyre teljesülne, hogy $\forall a \in 2\mathbb{Z}$: $ea = ae = 1$. (Ugyanis ha lenne ilyen $e \in 2\mathbb{Z}$ egységelem, akkor például $a = 2 \in 2\mathbb{Z}$ esetén $2e = 1$, azaz $e = \frac{1}{2} \notin 2\mathbb{Z}$ következne, ami ellentmondás.)

$\Rightarrow (2\mathbb{Z} \setminus \{0\}, \cdot)$ nem monoid, így nem is Abel-csoport. Tehát $(2\mathbb{Z}, +, \cdot)$ $\underline{\underline{\text{nem test}}}$.

(c) $(n\mathbb{Z}, +, \cdot)$, ahol $n \in \mathbb{Z}$ rögzített.

<u>1. eset:</u> $n \neq 0$

(i)
- $+$ binér művelet $n\mathbb{Z}$-n, mert $\forall nm, nk \in \mathbb{Z} : nk + nm = n(k+m) \in n\mathbb{Z}$.
- $+$ asszociatív $\mathbb{Z}$-n, így $n\mathbb{Z} \subseteq \mathbb{Z}$ miatt $+$ asszociatív $\mathbb{Z}$-n is.
- $0 = n0 \in n\mathbb{Z}$ semleges elem, mert $\forall a \in n\mathbb{Z} : a + 0 = 0 + a = a$.
- Tetszőleges $nk \in n\mathbb{Z}$ (additív) inverze $-nk$, mert $-nk = n(-k) \in n\mathbb{Z}$ és $nk + (-nk) = (-nk) + nk = 0$.
- Mivel $+$ kommutatív $\mathbb{Z}$-n így $n\mathbb{Z} \subseteq \mathbb{Z}$ miatt $+$ kommutatív $n\mathbb{Z}$-n is.

$\Rightarrow (n\mathbb{Z}, +)$ Abel-csoport.

(ii)
- $\cdot$ binér művelet $n\mathbb{Z}$-n, mert $\forall nk, nm \in n\mathbb{Z} : (nk)(nm) = n(knm) \in n\mathbb{Z}$.
- $\cdot$ asszociatív $\mathbb{Z}$-n, így $n\mathbb{Z} \subseteq \mathbb{Z}$ miatt $\cdot$ asszociatív $n\mathbb{Z}$-n is.

$\Rightarrow (n\mathbb{Z}, \cdot)$ félcsoport.

(iii) $\mathbb{Z}$-ben teljesül $\cdot$ mindkét oldali disztributivitása $+$ felett, és $n\mathbb{Z} \subseteq \mathbb{Z}$ miatt ezek teljesülnek $n\mathbb{Z}$-ben is.

Tehát $(n\mathbb{Z}, +, \cdot)$ $\underline{\underline{\text{gyűrű}}}$.

(iv) Ha $n = 1$, akkor $n\mathbb{Z} = \mathbb{Z}$, amiről az (a) részben már beláttuk, hogy nem test. Ha $n \neq 1$, akkor:

- $\cdot$ művelet $(n\mathbb{Z} \setminus \{0\})$-n: $\forall nk, nm \in n\mathbb{Z} \setminus \{0\} : (nk)(nm) = n(knm) \in \mathbb{Z} \setminus \{0\}$, mert $knm \in n\mathbb{Z}$ és nemnulla egészek szorzata is nemnulla.
- $\cdot$ asszociativitását fent már beláttuk.
- Mivel $n \neq 1$, így $1 \notin n\mathbb{Z} \setminus \{0\}$, így $n\mathbb{Z} \setminus \{0\}$-ben nincs egységelem.

Tehát $(n\mathbb{Z}, +, \cdot)$ $\underline{\underline{\text{nem test}}}$

.

<u>2. eset:</u> $n = 0$. Ekkor $n\mathbb{Z} = 0\mathbb{Z} = \{0\}$ egyelemű halmaz, amely csak a 0-t tartalmazza.

(i)
- $+$ művelet $0\mathbb{Z} = \{0\}$-n, mert $0 + 0 = 0 \in \{0\}$.
- $+$ asszociatív, mert: $(0 + 0) + 0 = 0 = 0 + (0 + 0)$.
- a 0 semleges elem, mert $0 + 0 = 0$.

- 0-nak önmaga az additív inverze, mert $0+0=0$.
- $+$ kommutatív, mert $0+0=0+0$.

$\Rightarrow (0\mathbb{Z},+)$ Abel-csoport.

(ii)
- $\cdot$ művelet, mert $0\cdot 0=0\in\{0\}$.
- $\cdot$ asszociatív, mert $(0\cdot 0)\cdot 0=0=0\cdot(0\cdot 0)$.

$\Rightarrow (0\mathbb{Z},\cdot)$ félcsoport.

(iii) $\mathbb{Z}$-ben teljesül $\cdot$ mindkét oldali disztributivitása $+$ felett, és $0\mathbb{Z}\subseteq\mathbb{Z}$ miatt ezek teljesülnek $0\mathbb{Z}$-ben is.

Tehát $(0\mathbb{Z},+,\cdot)$ gyűrű.

(iv) $0\mathbb{Z}\setminus\{0\}=\emptyset$, így $(0\mathbb{Z}\setminus\{0\},\cdot)$ nem lehet Abel-csoport, mert nincs eleme, így egységeleme sincs. Tehát $(0\mathbb{Z},+,\cdot)$ nem test.

(d) $(A,+,\cdot)$, ahol $A=\{a+b\sqrt{2}:\ a,b\in\mathbb{Z}\}$.

[Megjegyzés: A $+$ és $\cdot$ műveletek tulajdonságait $\mathbb{R}$-en ismertnek tekinthetjük, ezekre hivatkozhatunk.]

(i)
- $+$ művelet A-n, mert $\forall a,b,c,d\in\mathbb{Z}: (a+b\sqrt{2})+(c+d\sqrt{2})=a+c+(b+d)\sqrt{2}\in A$, mivel $(a+c)\in A$ és $(b+d)\in A$.
- $+$ asszociatív, mert: $\forall a,b,c,d,e,f\in\mathbb{Z}: [(a+b\sqrt{2})+(c+d\sqrt{2})]+(e+f\sqrt{2})=[a+c+(b+d)\sqrt{2}]+(e+f\sqrt{2})=(a+c)+e+((b+d)+f)\sqrt{2}=a+(c+e)+(b+(d+f))\sqrt{2}=a+b\sqrt{2}+[c+e+(d+f)\sqrt{2}]=a+b\sqrt{2}+[c+d\sqrt{2}+e+f\sqrt{2}]$. (Másik, rövidebb indoklás: Mivel $+$ asszociatív $\mathbb{R}$-en és $A\subseteq\mathbb{R}$, így $+$ asszociatív A-n is.)
- $0=0+0\sqrt{2}\in A$ semleges elem, mert $\forall a+b\sqrt{2}\in A: 0+0\sqrt{2}+a+b\sqrt{2}=a+b\sqrt{2}+0+0\sqrt{2}=a+b\sqrt{2}$.
- Tetszőleges $a+b\sqrt{2}\in A$ esetén $a+b\sqrt{2}\in A$ additív inverze $-a-b\sqrt{2}$, mert $-a-b\sqrt{2}\in A$ és $a+b\sqrt{2}+(-a-b\sqrt{2})=a-a+(b-b)\sqrt{2}=0$.
- $+$ kommutatív, mert $\forall a+b\sqrt{2},c+d\sqrt{2}\in A: a+b\sqrt{2}+c+d\sqrt{2}=a+c+(b+d)\sqrt{2}=c+a+(d+b)\sqrt{2}=c+d\sqrt{2}+a+b\sqrt{2}$. (Másik, rövidebb indoklás: Mivel $+$ kommutatív $\mathbb{R}$-en és $A\subseteq\mathbb{R}$, így $+$ kommutatív A-n is.)

$\Rightarrow (A,+)$ Abel-csoport.

(ii)
- $\cdot$ művelet A-n, mert $\forall a+b\sqrt{2},c+d\sqrt{2}\in A: (a+b\sqrt{2})\cdot(c+d\sqrt{2})=ac+2bd+(ad+bc)\sqrt{2}\in A$, mivel $ac+2bd\in\mathbb{Z}$ és $ad+bc\in\mathbb{Z}$.
- Mivel $\cdot$ asszociatív $\mathbb{R}$-en és $A\subseteq\mathbb{R}$, így $\cdot$ asszociatív A-n is.

$\Rightarrow (A,\cdot)$ félcsoport.

(iii) Mivel $\mathbb{R}$-ben $\cdot$ mindkét oldali disztributivitása teljesül $+$ felett és $A\subseteq\mathbb{R}$, így ezek teljesülnek A-n is.

$\Rightarrow (A,+,\cdot)$ gyűrű.

(iv)
- Legyenek $a+b\sqrt{2},c+d\sqrt{2}\in A$ tetszőlegesek. A fentiek alapján A zárt a szorzásra, így $a+b\sqrt{2},c+d\sqrt{2}\in A\setminus\{0\}$ esetén $(a+b\sqrt{2})\cdot(c+d\sqrt{2})\in A$. Másrészt nemnulla valós számok szorzata is nemnulla, így $(a+b\sqrt{2})\cdot(c+d\sqrt{2})\in A\setminus\{0\}$. Tehát $\cdot$ művelet $A\setminus\{0\}$-n.
- $\cdot$ asszociativitását korábban beláttuk.
- $1=1+0\sqrt{2}\in A\setminus\{0\}$, és mivel 1 egyégeleme $A\setminus$-nak, így $A\setminus\{0\}$-nak is az.

- Nincs minden $A \setminus \{0\}$-beli elemnek multiplikatív inverze. Például $1+2\sqrt{2} \in A \setminus \{0\}$-nek nincs, mert ha lenne $a+b\sqrt{2} \in A \setminus \{0\}$ inverze, akkor $(1+2\sqrt{2})(a+b\sqrt{2}) = a+4b+(2a+b)\sqrt{2} = 1$ miatt $a+4b=1$ és $2a+b=0$, ahonnan $a=-\frac{1}{7}$ és így $a+b\sqrt{2} \notin A \setminus \{0\}$ következik, ami ellentmondás.

$\Rightarrow$ $(A \setminus \{0\}, \cdot)$ nem csoport (így nem is Abel-csoport). Tehát $(A,+,\cdot)$ nem test.

(e) $(A,+,\cdot)$, ahol $A = \{a+bi \;:\; a,b \in \mathbb{Z}\}$.

[Megjegyzés: A $+$ és $\cdot$ műveletek tulajdonságait $\mathbb{C}$-n ismertnek tekinthetjük, ezekre hivatkozhatunk.]

(i)
- $\forall a+bi, c+di \in A : a+bi+c+di = a+c+(b+d)i \in A$, mert $a+c, b+d \in \mathbb{Z}$, így $+$ művelet A-n.
- Mivel komplex számok öszeadása asszociatív és $A \subseteq \mathbb{C}$, ezért $+$ asszociativitása öröklődik A-ra.
- $0 = 0+0i \in A$ semleges elem A-ban, mert 0 semleges elem $\mathbb{C}$-ben, és $A \subseteq \mathbb{C}$.
- Tetszőleges $a+bi \in A$ inverze $-a-bi \in A$, mert $a+bi+(-a-bi) = a-a+(b-b)i = 0$.
- Mivel komplex számok öszeadása kommutatív és $A \subseteq \mathbb{C}$, ezért $+$ kommutativitása öröklődik A-ra.

$\Rightarrow$ $(A,+)$ Abel-csoport.

(ii)
- $\cdot$ művelet A-n, mert $\forall a+bi, c+di \in A : (a+bi)\cdot(c+di) = ac-bd+(ad+bc)i \in A$, hiszen $ac-bd, ad+bc \in \mathbb{Z}$.
- $\cdot$ asszociatív, mert $\cdot$ asszociatív $\mathbb{C}$-n és $A \subseteq \mathbb{C}$ miatt az asszociativitás öröklődik A-ra.

$\Rightarrow$ $(A,\cdot)$ félcsoport.

(iii)
- Mivel $\cdot$ művelet A-n, így tetszőleges $a+bi, c+di \in A \setminus \{0\}$ esetén $(a+bi)(c+di) \in A$. Tudjuk, hogy nemnulla komplex számok szorzata nem nulla, ezért $(a+bi)(c+di) \in A \setminus \{0\}$ következik, így $\cdot$ művelet $A \setminus \{0\}$-n.
- $\cdot$ asszociativitását fentebb már igazoltuk.
- Mivel $1 = 1+0i \in A \setminus \{0\}$ és 1 egységelem $(A,\cdot)$-ban, így $(A \setminus \{0\}, \cdot)$-ban is az.
- Nincs minden $A \setminus \{0\}$-beli számnak multiplikatív inverze $A \setminus \{0\}$-ban. Például $2 \in A \setminus \{0\}$ multiplikatív inverze $\mathbb{C}$-ben $\frac{1}{2}$, de $\frac{1}{2} \notin A \setminus \{0\}$.

$\Rightarrow$ $(A \setminus \{0\}, \cdot)$ nem csoport (így nem is Abel-csoport) Tehát $(A,+,\cdot)$ nem test.