Művelettartó leképezések. A számfogalom fölépítése. Kvaterniók, egész számok

1. a) *Keressük meg az egységeket és a nullosztókat a $\mathbb{Z}_{12}$ gyűrűben.*
b) *Hány egység, illetve nullosztó van a $\mathbb{Z}_{100}$ gyűrűben?*

Megoldás. a) Egységnek a gyűrű azon elemeit nevezzük, amelyek mindennek osztói. Ez ekvivalens azzal, hogy az elem osztója az 1-nek, azaz invertálható. Így tehát az $ax \equiv 1 \pmod{12}$ kongruenciát kell megoldanunk. Ez pontosan akkor oldható meg, ha a relatív prím a modulushoz, azaz 12-höz. Ez azt jelenti, hogy egységek $\mathbb{Z}_{12}$-ben az $\{1, 5, 7, 11\}$ halmaz elemei. – Egy maradék akkor lesz nullosztó, ha önmaga nem nulla (tehát a szám nem osztható 12-vel), de van hozzá olyan szintén nem nulla maradék, amivel összeszorozva már osztható lesz 12-vel. Ez pontosan aztjelenti, hogy a szám nem relatív prím a modulushoz, mert akkor nem kell a modulus minden prímtényezőjével és teljes hatványon megszorozni az oszthatóság eléréséhez. Így $\mathbb{Z}_{12}$-ben nulllosztók lesznek a $\{2, 3, 4, 6, 8, 9, 10\}$ elemei.
b) A fönti gondolatmenet tetszőleges modulusra alkalmazható: egységek a redukált maradékok (azaz amik relatív prímek a modulushoz), nullosztók pedig a nem redukált maradékok (kivéve a 0-t). Így $\mathbb{Z}_{100}$-ban az egységek száma $\varphi(100) = \varphi(2^2d^2) = \varphi(2^2)\varphi(5^2) = 2 \cdot 20 = 40$ (itt $\varphi(n)$ az n-hez relatív prím maradékok száma), a nullosztók száma pedig $100 - 40 - 1 = 59$ (itt a nullosztók számnál az összesmaradék számból le kellett vonni a redukált maradékok számát, és ki kellett még zárni a 0-t is).

2. a) *Ellenőrizzük, hogy minden r valós számra és q kvaternióra $rq = qr$ teljesül.*
b) *Igazoljuk, hogy minden $q \in \mathbb{H} \setminus \mathbb{R}$ esetén van olyan $q' \in \mathbb{H}$, melyre $qq' \neq q'q$.*

Megoldás. a) Valós szám alatt most az $r = r + 0i + 0j + 0k$ alakú kvaterniókat értjük, kvaterniók szorzása alatt pedig az alábbit:

$$(a+bi+cj+dk)(x+yi+zj+tk) = (ax-by-cz-dt)+(ay+bx+ct-dz)i+(az-bt+cx+dy)j+(at+bz-cy+dx)k$$

Ha a fönti r valós számot szorozzuk a $q = a+bi+cj+dk)$ kvaternióval, akkor a definíció szerint az alábbiakat kapjuk:

$$rq = (ra) + (rb)i + (rc)j + (rd)k$$
$$qr = (ar) + (br)i + (cr)j + (dr)k$$

Ezek pedig egyenlők, hiszen a valós számok szorzása kommutatív.
b) Ha $q = a + bi + cj + dk \in \mathbb{H} \setminus \mathbb{R}$, akkor b, c, d közül legalább az egyik nem nulla. Legyen ez pl. az i együtthatója, azaz b. Ekkor qj-ben az $ij = k$ együtthatója b, míg jq-ban a k együtthatója $-b$, a két szorzat tehát nem egyenlő.

3. *A $z = a + bi, w = c + di$ jelölés mellett legyen $\varphi\left(\begin{bmatrix} z & w \\ -\overline{w} & \overline{z} \end{bmatrix}\right) = a + bi + cj + dk$. Ellenőrizzük, hogy ez a $\varphi : \mathbb{K} \to \mathbb{H}$ leképezés művelettartó. (Itt $\mathbb{K}$ az 1. feladatsor 7. feladatában szereplő ferdetest, melynek elemei az olyan mátrixok, mint amilyenek a φ argumentumában szerepelnek.)*

Megoldás. Az összegtartás egyszerű, ezért csak a szorzattaratást mutatjuk meg. Azt kell megmutatnunk, hogy $z' = a' + b'i$ és $w' = c' + d'i$, illetve $z'' = a'' + b''i$ és $w'' = c'' + d''i$ esetén:

$$\varphi\left(\begin{bmatrix} z' & w' \\ -\overline{w'} & \overline{z'} \end{bmatrix} \cdot \begin{bmatrix} z'' & w'' \\ -\overline{w''} & \overline{z''} \end{bmatrix}\right) = \varphi\left(\begin{bmatrix} z' & w' \\ -\overline{w'} & \overline{z'} \end{bmatrix}\right) \cdot \varphi\left(\begin{bmatrix} z'' & w'' \\ -\overline{w''} & \overline{z''} \end{bmatrix}\right)$$

Ehhez a két mátrix szorzatát kell először kiszámolnunk:

$$\begin{bmatrix} z' & w' \\ -\overline{w'} & \overline{z'} \end{bmatrix} \cdot \begin{bmatrix} z'' & w'' \\ -\overline{w''} & \overline{z''} \end{bmatrix} = \begin{bmatrix} z'z'' - w'\overline{w''} & z'w'' + w'\overline{z''} \\ -\overline{w'}z'' - \overline{z'}\overline{w''} & -\overline{w'}w'' + \overline{z'}\overline{z''} \end{bmatrix}.$$

(Vegyük észre, hogy a szorzatmátrix benne van $\mathbb{K}$-ban, amint az el is várható.) A szorzatmátrix első sorának elemei:

$$z'z' - w'\overline{w''} = \big((a'a'' - b'b'') - (c'c'' + d'd'')\big) + \big((a'b'' + b'a'') - (-c'd'' + d'c'')\big)i$$
$$z'w'' + w'\overline{z''} = \big((a'c'' - b'd'') + (c'a'' + d'b'')\big) + \big((a'd'' + b'c'') + (-c'b'' + d'a'')\big)i$$

Ekkor viszont φ a szorzatmátrixhoz pont azt a kvaterniót rendeli, ami a fönti szorzatokból adódik (az első sorban szereplő számot plusz a második szám j-szeresét). Ez mutatja a szorzattartást.

4. a) *Mutassunk példát olyan $\mathbb{R} \to \mathbb{R}$ leképezésre, amely az összeadásra nézve művelettartó, és a pozitív számokhoz negatív számokat rendel.*
b) *Legyen φ olyan $\mathbb{R} \to \mathbb{R}$ leképezés, amely a szorzásra nézve művelettartó. Igazoljuk, hogy ha $x \geq 0$, akkor $\varphi(x) \geq 0$.*

Megoldás. a) A $\varphi(a) = -a$ ilyen hozzárendelés lesz.
b) Ha $x \geq 0$, akkor van olyan y, melyre $x = y^2$. De ekkor $\varphi(x) = \varphi(y^2) = \varphi(y)\varphi(y) \geq 0$, hiszen valós számok negyzete mindig nemnegatív.

5. a) *Igazoljuk, hogy a kvaterniók vektorteret alkotnak a valós, illetve a komplex számtest fölött a megszokott műveletekre nézve. Melyik vektortérnek mennyi a dimenziója?*
b) *Érvényes-e ezekben a vektorterekben az $\lambda(uv) = (\lambda u)v = u(\lambda v)$ azonosság ($\lambda \in T$, $u, v \in V$)?*

Megoldás. a) Egyszerű számolás. A dimenziók: valós fölött 4, hiszen $1, i, j, k$ bázist alkotnak, míg $\mathbb{C}$ fölött a dimenzió 2 (bázis: $1, j$).
b) A valós számtest fölött érvényes, hiszen a 2.a) feladat alapján minden valós szám minden kvaternióval „fölcserelhető” (azaz szorzásnál a sorrendje megcserélhető vele). Ugyanakkor $\mathbb{C}$ fölött már nem igaz az összefüggés, hiszen pl. $\lambda = i$, $u = j$ és $v = 1$ esetén $\lambda(uv) = ij = k$, míg $u(\lambda v) = ji = -k$.

6. *Az összeadás rekurzív definíciójából kiindulva igazoljuk, hogy ha $a, b, c \in \mathbb{N}$ és $a + c = b + c$, akkor $a = b$.*

Megoldás. Írjuk föl a Peano-axiómákat:
(PA1) $1 \in \mathbb{N}$;
(PA2) $(\forall n \in \mathbb{N})\ (\exists n^+ \in \mathbb{N})$;
(PA3) $(\forall n, m \in \mathbb{N})\ (n^+ = m^+) \Rightarrow (n = m)$;
(PA4) $\nexists n \in \mathbb{N}\ (n^+ = 1)$;
(PA5) $(H \subseteq \mathbb{N})$, $(1 \in H)$, $(n \in H \Rightarrow n^+ \in H) \implies (H = \mathbb{N})$ (teljes indukciós séma).
Az összeadás rekurzív definíciója:
(OA1) $a + 1 = a^+$;
(OA1) $a + b^+ = (a + b)^+$.
A szorzás rekurzív definíciója:
(SZ1) $a1 = a$;
(SZ2) $a(b^+) = ab + a$.
Továbbá bizonyítottnak tekintjük az összeadás asszociativitását (ÖAA) és az összeadás kommutativitását (ÖAK). A fentiek fölhasználásával bizonyítsuk az állítást.
Állítás: $(a + c = b + c) \Rightarrow (a = b)$.
Bizonyítás: c-re conatkozó indukcióval. H azoknak a c számoknak a halmaza, melyekre minden a, b mellett igaz az állítás. Ekkor:

$$\begin{aligned}
1 \in H: &\quad a + 1 = b + 1 \overset{(OA1)}{\Longrightarrow} a^+ = a + 1 = b + 1 = b^+ \overset{(PA3)}{\Longrightarrow} a = b \\
(c \in H \Rightarrow c^+ \in H): &\quad a + c^+ = b + c^+ \overset{(OA2)}{\Longrightarrow} (a + c)^+ = a + c^+ = b + c^+ = (b + c)^+ \overset{(PA3)}{\Longrightarrow} \\
&\quad \overset{(PA3)}{\Longrightarrow} a + c = b + c \overset{(IND)}{\Longrightarrow} a = b \\
\Longrightarrow &\quad H = \mathbb{N}
\end{aligned}$$

A fönti okfejtésben (IND) az indukciós hipotézist, azaz a $c \in H$ feltételt jelöli.

7. *A szorzás rekurzív definíciójából kiindulva igazoljuk, hogy a természetes számok halmazán a szorzás kommutatív és asszociatív. (Az összeadásról tanultakat itt már felhasználhatjuk.)*

Megoldás. Csak a kommutativitást bizonyítjuk. Először egy speciális esetet igazolunk. Tudjuk, hogy $a1 = a$ (SZ1). Igazoljuk, hogy $1a = a$ is teljesül minden a-ra (SP1). a-ra vonatkozó indukcióval bizonyítunk. A jó $a \in \mathbb{N}$-ek halmazát jelölje H.

$$\begin{aligned}
1 \in H: &\quad 1 \cdot 1 \overset{(SZ1)}{=} 1 \\
(a \in H \Rightarrow a^+ \in H): &\quad 1a^+ \overset{(SZ2)}{=} 1a + 1 \overset{(IND)}{=} a + 1 \overset{(OA1)}{=} a^+ \\
\Longrightarrow &\quad H = \mathbb{N}
\end{aligned}$$

Második lépésként igazoljuk, hogy $a^+b = ab + b$ minden a-ra és b-re (SP2). Itt b-re vonatkozó indukcióval bizonyítunk.

$$\begin{aligned}
1 \in H: &\quad a^+ \cdot 1 \overset{(SZ1)}{=} a^+ \overset{(OA1)}{=} a + 1 \overset{(SZ1)}{=} a \cdot 1 + 1 \\
(b \in H \Rightarrow b^+ \in H): &\quad a^+b^+ \overset{(SZ2)}{=} a^+b + a^+ \overset{(IND)}{=} (ab + b) + a^+ \overset{(OA1)}{=} (ab + b) + (a + 1) \overset{(OAA)}{=} \\
&\quad \overset{(OAA)}{=} ab + (b + a) + 1 \overset{(OAK)}{=} ab + (a + b) + 1 \overset{(OAA)}{=} (ab + a) + (b + 1) \overset{(SZ2)}{=} \\
&\quad \overset{(SZ2)}{=} ab^+ + (b + 1) \overset{(OA1)}{=} ab^+ + b^+ \\
\Longrightarrow &\quad H = \mathbb{N}
\end{aligned}$$

Végezetül igazoljuk általánosan, hogy $ab = ba$, ismét b-re vonatkozó indukcióval.

$$\begin{aligned} 1 \in H: &\quad a1 \overset{(SZ1)}{=} a \overset{(SP1)}{=} 1a \\ (b \in H \Rightarrow b^+ \in H): &\quad ab^+ \overset{(SZ2)}{=} ab + a \overset{(IND)}{=} ba + a \overset{(SP2)}{=} b^+a \\ \Longrightarrow &\quad H = \mathbb{N} \end{aligned}$$

Ezzel a szorzás kommutativitását beláttuk.
Megjegyzés: Hasonlóan, c-re vonatkozó indukcióval bizonyítható az $(ab)c = a(bc)$ asszociativitás, de célszerű előtte megcsinálni a következő feladatot, mert hasnáånunk kell a disztributivitást.

8. *Igazoljuk, hogy a természetes számok halmazán a szorzás disztributív az összeadás fölött.*

Megoldás. Az $(a + b)c = ac + bc$ összefüggést, az előzőekhez hasonlóan, c-re vonatkozó indukcióval bizonyíthatjuk. Az $a(b + c) = ab + ac$ disztributivitásnál már használhatjuk az előző állítást és a szorzás kommutativitását.

9. *Az $\{(a, b) \mid a, b \in \mathbb{N}\}$ halmazon vezessük be következő relációt: legyen $(a, b) \sim (c, d)$ akkor és csakis akkor, ha $a + d = b + c$. Ellenőrizzük, hogy ez egy ekvivalenciareláció.*

Megoldás. *Reflexivitás:* $(a, b) \sim (a, b)$, hiszen $a + b = b + a$ (az összeadás a természetes számok halmazán kommutatív.
Szimmetria: $(a, b) \sim (c, d)$ esetén $a + d = b + c$, s ekkor $c + b = d + a$ is igaz, hiszen az összeadás komutatív, és az egyenlőség szimmetrikus reláció, így $(c, d) \sim (b, a)$.
Tranzitivitás: $(a, b) \sim (c, d)$ és $(c, d) \sim (e, f)$ esetén $a + d = b + c$, és $c + f = d + e$. Adjunk az első egyenlőség mindkét oldalához e-t: azt kapjuk, hogy $a + d + e = b + c + e$, és a második egyenlőséget használva $d + e$ helyére írhatunk $c + f$-et: $a + c + f = b + c + e$. Használjuk a kommutativitást: $a + f + c = b + e + c$, és ebből az egyszerűsítési szabályt alkalmazva (lásd 6. feladat) $a + f = b + e$ adódik, ami azt jelenti, hogy $(a, b) \sim (e, f)$.

10. *Legyen az (a, b) és a (c, d) pár szorzata $(ac + bd, ad + bc)$.*
a) *Ellenőrizzük, hogy ha $(c, d) \sim (c', d')$, akkor $(a, b)(c, d) \sim (a, b)(c', d')$.*
b) *Vezessük be két ekvivalenciaosztály szorzatát, ellenőrizve azt is, hogy ez jól definiált.*
c) *Ellenőrizzük, hogy az összeadás nullelemét bármelyik osztállyal szorozva a nullelemet kapjuk.*
d) *Keressük meg az egységelemet a szorzásra nézve.*

Megoldás. a) Tegyük föl, hogy $(c, d) \sim (c', d')$. Ez azt jelenti, hogy $c + d' = d + c'$. Számoljuk ki a két megadott szorzatot is:

$$(a, b)(c, d) = (ac + bd, ad + bc) \quad \text{és} \quad (a, b)(c', d') = (ac' + bd', ad' + bc').$$

Azt kell megmutatnunk, hogy $ac+bd+ad'+bc' = ad+bc+ac'+bd'$. De fölhasználva a természetes számokra már bizonyított műveleti tulajdonságokat – összeadás kommutativitása, asszociativitása, disztributivitás – az alábbiakat kapjuk:

$$ac + bd + ad' + bc' = a(c + d') + b(d + c') \quad \text{és} \quad ad + bc + ac' + bd' = a(d + c') + b((c + d').$$

De az a két kifejezés az első ekvivalencia miatt megegyezik, mivel az a-t és a b-t szorzó tényezők a föltevés szerint megegyeznek.
b) Szorozzuk úgy az ekvivalenciaosztályokat, hogy kivesszük egy-egy eleműket, azokat a párokat a fönti definíció alapján összeszorozzuk, majd vesszük az eredmény ekvivalenciaosztályát. Az eredmény független a reprezentáns elemek kiválasztásától: ezt az a) rész biztosítja, illetve annak szimmetrikus párja, amikor a szorzásnál az első párt cseréljük vele ekvivalensre. (Ez utóbbi ugyanúgy bizonyítható, vagy pedig bizonyíthatjuk a párok szorzásának a kommutativitását, fölhasználva a természetes számok műveleteinek tulajdonságait.)
c) Az öszeadás nulleleme az (a, a) párok ekvivalenciaosztálya lesz. Azt, hogy ezek a párok ekvivalensek, könnyű számolás mutatja: $(a, a) \sim (b, b)$, hiszen $a + b = a + b$. Másrészt az is világos, hogy más típusú eleme nincs az ekvivaenciaosztálynak: $(a, b) \sim (c, c)$, akkor $a + c = b + c$, és akkor a 6. feladat egyszerűsítűi szabálya miatt $a = b$. H amost alkalmazzuk a szorzás definícióját, akkor az alábbit kapjuk: $(a, a)(b, c) = (ab + ac, ac + ab)$, és ez utóbbi pár benne van a 0-elemet adó ekvivalenciaosztályban, hiszen a természetes számok összeadása kommutatív.
d) Az $(a^+, a) = (a+1, a)$ párok ekvivalenciaosztályt alkotnak (ez hasonlóan bizonyítható, mint a c) részben a nullelemet adó osztåynál), és $(a+1, a)(b, c) = ((a+1)b+ac, (a+1)c+ab) = (ab+b+ac, ac+c+ab) \sim (b, c)$, hiszen $ab + b + ac + c = ac + c + ab + b$). Itt használjuk a természetes számok műveleteinek szokásos tulajdonságait.
Megjegyzés: Könnyen látható, hogy az (a, b) párt, illetve annak ekvivalenciaosztályát az $a - b$ egész számnak szeretnénk megfeleltetni: ennek a szellemében adtuk meg az ekvivalenciájukat, illetve a műveleteket. A tulajdonságok bizonyításánál lehet használni az intuíciót pl. arra, hogy kitalåajuk, mi is lesz a nullelem $((a, a) \leftrightarrow a - a = 0)$ vagy az egységelem $((a + 1, a) \leftrightarrow a + 1 - a = 1)$, de nem használhatjuk a bizonyítás során, hogy az $(a + 1, a)$ ezért egységelem, mert $a + 1 - a = 1$, és az 1 az egész számok körében egységelem. Ne feledjük: az egész számokat most konstruáljuk, a műveletek tulajdonságait most bizonyítjuk.