Hányadostest. Karakterisztika.

1. **a)** *Ellenőrizzük, hogy az egész számok számpárokkal történő konstrukciójában* $(1,m^+)(1,n^+)=((mn)^+,1)$.
b) *Mivel egyenlő* $(1,m^+)(n^+,1)$*?*
c) *Igazoljuk, hogy* $\mathbb{Z}$ *nullosztómentes.*

Megoldás. a) A bizonyítás során használhatjuk a természetes számokra vonatkozó axiómákat, a műveletek definícióitt, illetve a már bizonyított műveleti összefüggéseket, pl. azt, hogy az összeadás kommutatív, asszociatív, $n^+=n+1$, a szorzás kommutatív és asszociatív, az 1 egységelem a szorzásra nézve, és érvényes a disztributivitás. Ekkor a párok szorzásának definíciója szerint az kell, hogy:

$$(1,m^+)(1,n^+)=(1\cdot 1+m^+n^+,1\cdot n^+ + m^+\cdot 1)\sim((mn)^+,1).$$

A bal oldali részt kifejtve:

$$(1\cdot 1+m^+n^+,1\cdot n^+ + m^+\cdot 1)=(1+(m+1)(n+1),n+1+m+1)=(mn+m+n+2,m+n+2).$$

A párok ekvivalenciájának definíciója szerint ez utóbbi pár valóban ekvivalens az $((mn)^+,1)=(mn+1,1)$ párral, ugyanis a párok ekvivalenciájának definíciója szerint azt kell látni, hogy:

$$mn+m+n+2+1=m+n+2+mn+1.$$

De a természetes számok számolási szabályai szerint mindkét oldal egyenlő $mn+m+n+3$-mal. *Megjegyzés:* A bizonyítás során nem használhatjuk azt az *intuitív információt*, hogy az (a,b) pár az $a-b$ egész számnak fog majd megfelelni. Ehhez ugyanis még nem rendelkezünk pl. a kivonás definíciójával (vagy a negatív számok és műveleteik definíciójával). A „hitünket" ugyan erősíthetjük, hogy a fönti összefüggés valóban igaz (hiszen ez tkp. a $(-m)(-n)=mn$ számolási szabályt akarja jelenteni, amiről tudjuk, hogy „teljesülni fog" az egész számok körében), de ehhez egyelőre nem értelmeztük a szükséges megfeleltetéseket.
b) A szorzás definíciója és a természetes számok már ismert műveleti tulajdonságai szerint:

$$(1,m^+)(n^+,1)=(1\cdot n^+ + m^+\cdot 1,1\cdot 1+m^+\cdot n^+)=(n+m+2,1+(m+1)(n+1))=(n+m+2,mn+m+n+2),$$

ez pedig az ekvivalencia definíciója szerint ekvivalens $(1,(mn)^+)$-szal. Vegyük észre, hogy itt a $(-m)n=-(mn)$ szabály elkódolásáról van szó, de ismét nem hivatkozhattunk arra, hogy mi már „tudjuk" ezt a szabályt egész számokra, hiszen még csak most vezetjük be az egész számok fogalmát és műveleteit.
c) (Vázlat) Indukcióval beláthatjuk: tetszőleges (a,b) számpárra teljesül, hogy ha $a\neq b$, akkor (a,b) ekvivalens egy $(c^+,1)$ vagy egy $(1,c^+)$ számpár valamelyikével valamilyen c természetes számra. Az (a,b) pár ekvivalenciaosztályát nevezzük az első esetben pozitív egész számnak, a másik esetben negatívnak, és az (a,a) párok osztályát nevezzük 0-nak. Megmutatjuk, hogy a pozitív számok halmaza kölcsönösen egyértelműen megfeleltethető a természetes számok halmazának, méghozzá művelettartó módon:

$$a\mapsto (a^+,1) \text{ osztálya, és:}$$
$$((a+b)^+,1)\sim(a^+,1)+(b^+,1),\ \text{valamint}\ ((ab)^+,1)\sim(a^+,1)\cdot(b^+,1).$$

Vegyük azt is észre, hogy $(a^+,1)$ és $(1,a^+)$ osztályának az összege $(a^++1,a^++1)\sim 0$, tehát egy pozitív egész számnak van ellentettje, és az negatív (és fordítva). Ha nem nulla egész számokat (vagyis párok ekvivalenciaosztályait) szorozzuk, akkor két pozitívat összeszorozva nem nullát kapunk, mert a természetes számok szorzásáról már beláttuk, hogy nullosztómentes. Két negatív szám szorzata az a) rész alapján pozitív (tehát nem nulla), végezetül ha pl. a negatív, b pedig pozitív, akkor a szoratuk a b) rész alapján negatív, tehát ismét nem nulla.

2. *Ellenőrizzük, hogy a hányadostest konstrukciójánál bevezetett összeadás jól definiált, vagyis hogy az eredmény független a reprezentánsok megválasztásától.*

Megoldás. Emlékeztető: ha az R kommutatív és nullosztómentes gyűrű hányadostestét akarjuk megkonstruálni, akkor az alábbi halmazon vezetünk be egy ekvivalenciát:

$$\{(a,b)\,|\,a,b,\in R,\ b\neq 0\}\,, \qquad \text{és} \qquad (a,b)\sim(c,d) \iff ad=bc.$$

A hányadostest elemei a fönti halmaz ekvivalenciaosztályai lesznek: ezek halmazát jelölje Q, az (a,b) pár osztályát pedig jelölje $[(a,b)]$. Az alábbi összeadást vezetjük be a párokon, illetve azok ekvivalenciaosztályain:

$$(a,b)+(c,d)=(ad+bc,bd) \qquad \text{és} \qquad [(a,b)]+[(c,d)]=[(ad+bc,bd)].$$

A fönti definícióban az lehet probléma, hogy az ekvivalenciaosztályok más elemeit választva esetleg azoknak az összege nem lesz ekvivalens az eredetileg választott párok összegével. Azaz: be kell látnunk, hogy az ekvivalenciaosztályok összeadásánál a fölírt eredmény független a reprezentánsok kiválasztásától.
Legyen tehát $(a,b)\sim(a',b')$ és $(c,d)\sim(c',d')$. Ekkor (1) $ab'=ba'$ és (2) $cd'=dc'$. Azt szeretnénk megmutatni, hogy $(a,b)(c,d)\sim(a',b')(c',d')$. Itt:

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

A két szorzat ekvivalenciájához azt kell megmutatnunk, hogy $(ad+bc)b'd'=bd(a'd'+b'c')$. Ezt az alábbi számolás mutatja (menet közben használjuk a fönti (1) és (2) föltevéseket:

$$\begin{aligned}(ad+bc)b'd' &= adb'd'+bcb'd' = ab'dd'+bb'cd' \overset{(1)}{=} ba'dd'+bb'cd' \overset{(2)}{=} ba'dd'+bb'dc' = \\ &= bda'd'+bdb'c' = bd(a'd'+b'c').\end{aligned}$$

3. *Ellenőrizzük, hogy a hányadostest konstrukciójában az összeadás asszociatív.*

Megoldás. Használjuk az összeadás előző feladatban megadott definícióját:

$$\big((a_1,b_1)+(a_2,b_2)\big)+(a_3,b_3)=(a_1b_2+b_1a_2,b_1b_2)+(a_3,b_3)=(a_1b_2b_3+b_1a_2b_3+b_1b_2a_3,b_1b_2b_3)$$
$$(a_1,b_1)+\big((a_2,b_2)+(a_3,b_3)\big)=(a_1,b_1)+(a_2b_3+b_2a_3,b_2b_3)=(a_1b_2b_3+b_1a_2b_3+b_1b_2a_3,b_1b_2b_3)$$

Vagyis az összeadás asszociatív. (Menetközben szabadon használtuk az egész számokra vonatkozó műveleti tulajdonságokat: az összeadás és szorzás asszociativitását, valamint a disztributivitást.) – Megjegyzés: a párok „indexelt" jelölésének annyi előnye van, hogy könnyebben különböztetjük meg a számlálókat és a nevezőket, mint akkor, ha $(a,b),(c,d)$ stb. párokkal számolnánk.

4. *Ellenőrizzük, hogy a hányadostest konstrukciójánál azon (r,r) számpárok, ahol $r\in R\setminus\{0\}$, egy osztályt alkotnak, ami rendelkezik az egységelemtől elvárt tulajdonsággal.*

Megoldás. $(r,r)\sim(s,s)$, hiszen $rs=rs$. Tehát minden ilyen típusú pár ekvivalens. Másrészt, ha $(r,r)\sim(s,t)$, akkor $rt=rs$, azaz $r(t-s)=0$. Mivel az egész számok szorzása nullosztómentes, és $r\neq 0$ ezért $t=s$. Ezzel megmutattuk, hogy az ekvivalenciaosztálynak minden eleme (r,r) alakú. Megmutatjuk, hogy $[(r,r)][(a,b)]=[(a,b)]$, és $[(a,b)][(r,r)]=[(a,b)]$:

$$(r,r)(a,b)=(ra,rb)\sim(a,b), \quad \text{hiszen} \quad rab=rba.$$

A másik irányból vett vett szorzatra hasonló a számolás. Itt használtuk a párokra értelmezett $(a,b)(c,d)=(ac,bd)$ szorzást, illetve hogy ekvivalenciaosztályokra is értelmezhetjük a szorzást a reprezentánsaik szorzatával.

5. *Keressük meg az alábbi gyűrűk hányadostestét:*
a) *a 3-mal osztható számok gyűrűje;*
b) *az $a+b\sqrt{2}$ alakú számok gyűrűje, ahol $a,b\in\mathbb{Z}$.*

Megoldás. a) Kiindulhatunk a konstrukcióból: a számpárokat a megfelelő racionális számokkal azonosíthatjuk: $[(3a,3b)]=3a/3b$. Az iiteni ekvivalens párok ugyanis az egész számok hányadostestñek konstrukciójánál is ekvivalensek. De azt is észrevehetjük, hogy minden racionális számot megkapunk: $a/b=[(3a,3b)]$ tetszőleges (a,b) párra, ha $b\neq 0$. Így a hányadostest $\mathbb{Q}$. – A R gyűrű hányadostestét egyébként megkaphatjuk másképp is: ha R-et részgyűrűként megtaláljuk egy testben (mint jelen esetben $\mathbb{Q}$-ban), akkor a hányadostest lesz a legszűkebb résztest, ami tartalmazza az adott R részgyűrűt. Itt most láthatjuk, hogy $\mathbb{Q}$-nak nincs valódi részteste, tehát maga $\mathbb{Q}$ a hányadostest.
b) A előző megjegyzés alapján a hányadostest az $(a+b\sqrt{2})/(c+d\sqrt{2})$ alakú valós számokból áll, ahol $a,b,c,d\in\mathbb{Z}$ és $c+d\sqrt{2}\neq 0$. De minden ilyen szám a gyöktelenítési eljárással $p+q\sqrt{2}$ alakra hozható, ahol $p.q\in\mathbb{Q}$, és világos, hogy minden ilyen számot elő is tudunk állítani hányadosként, ezért a hányadostest jelen esetben $Q=\big\{p+q\sqrt{2}\,|\,p,q\in\mathbb{Q}\big\}$.

6. *Tekintsük a $\mathbb{Z}_2$ test fölötti racionális törtfüggvények testét. Hány eleme van ennek a testnek, és mennyi a karakterisztikája?*

Megoldás. A mondott test $\mathbb{Z}_2[x]$ hányadosteste. $\mathbb{Z}[x]$-nek megszámlálhatóan végtelen sok eleme van, és akkor ugyanennyi párt is képezhetünk belőlük. Ez azt jelenti, hogy az ekvivalenciaosztályok száma is legföljebb megszámlálhatóan végtelen. Ugyanakkor, persze, $\mathbb{Z}_2[x]$ részgyűrűként benne is van a hányadostestben, tehát pontosan megszámlálható végtelen eleme van. A karakterisztika bámely nem nulla elem additív rendjeként megkapható, és így, mivel $\mathbb{Z}$-ben az egységelem rendje 2, ezért a karakterisztika 2.

7. *Mennyi lehet a karakterisztikája egy olyan testnek, amelynek* **a)** *27;* **b)** *64;* **c)** *végtelen sok eleme van?*

Megoldás. a) A karakterisztika véges (mert az additív csoport véges), és osztója 27-nek (a Lagrange-tétel miatt), továbbá karakterisztika prímszám. Ezért a karakterisztika csak 3 lehet.
b) Hasonló okoskodás miatt a karakterisztika 2.
c) Végtelen testnek mármilyen karakterisztikája lehet. Véges karakterisztikájú végtelen testtel még ne találkoztunk, de a félév vége felé talán már tudunk ilyent konstruálni. Természetesen 0 karakterisztikájú végtelen testtel már találkoztunk: $\mathbb{Q}$ ilyen.

8. *Oldjuk meg az $(x+1)^3 = x^3+1$ egyenletet a $\mathbb{Z}_3$, illetve a $\mathbb{Z}_{23}$ test fölött.*

Megoldás. $\mathbb{Z}_3$ fölött: $(x+1)^3 = x^3+3x^3+3x+1 = x^3+1$, ugyanis $\mathbb{Z}$-ban $3=0$ (ez mindig igaz, ha a karakterisztika 3). Ez azt jelenti, hogy a fölírt egyenlet $\mathbb{Z}_3[x]$-ben azonosság, vagyis $\mathbb{Z}_3$ minden eleme megoldása az egyenletnek.
$\mathbb{Z}_{23}$ fölött: $(x+1)^3 = x^3+3x^2+3x+1 = x^3+1$ azzal ekvivalens, hogy $3x^2+3x=0$. Mivel $\mathbb{Z}_{23}$-ban oszthatunk 3-mal, ezért tkp. az $x^2+x=0$ egyenletet kell megoldanunk: ennek $x^2+x = x(x+1)$ miatt $x=0$ és $x=-1$, azaz $x=22$ a megoldása.

9. *Oldjuk meg az $(x+1)^4 = x^4+1$ egyenletet a $\mathbb{Z}_3$, illetve a $\mathbb{Z}_{23}$ test fölött.*

Megoldás. $\mathbb{Z}_3$ fölött: $(x+1)^4 = x^4+4x^3+6x^2+4x+1 = x^4+x^3+x+1$, hiszen $6x^2=0$. A megadott egyenlet tehát azzal ekvivalens, hogy $x^4+x^3+x+1 = x^4+1$, vagyis $x^3+x=0$. De $x^3+x = x(x^2+1) = 0$-nak $x=0$ az egyetlen megoldása, hiszen x^2+1-nek nincs gyöke $\mathbb{Z}_3$-ban.
$\mathbb{Z}_{23}$ fölött: Az előző számolás miatt az $(x+1)^4 = x^4+4x^3+6x^2+4x+1 = x^4+x^3+x+1 = x+1$ egyenletet kell megoldanunk, ami ekvivalens azzal, hogy $4x^3+6x^2+4x=0$, vagy 2-vel egyszerűsítve $2x^3+3x^2+2x = x(2x^2+3x+2)=0$. Itt az első tényező miatt $x=0$ megoldás; a másodfokú $2x^2+3x+2=0$ egyenletnek pedig a másodfokú egyenlet megldóképlete miatt a megoldásai:

$$x_{1,2} = \frac{-3\pm\sqrt{9-16}}{4} = \frac{-3\pm\sqrt{-7}}{4} = \frac{-3\pm\sqrt{16}}{4} = \frac{-3\pm 4}{4} = \begin{cases} 1/4 = 6 \\ -7/4 = 16/4 = 4 \end{cases}$$

A fönti számolásnál természetesen modulo 23 kellett a gyökvonást és az osztást elvégezni.

10. *Legyen* $\mathrm{char}(T) = p$. *Igazoljuk, hogy*
a) *minden $a,b \in T$ esetén $(a+b)^p = a^p+b^p$;*
b) *minden $n \in \mathbb{N}$ és $a_1, \dots a_n \in T$ esetén*

$$\Big(\sum_{i=1}^{n} a_i\Big)^p = \sum_{i=1}^{n} a_i^p.$$

Megoldás. a) A binomiális tétel alapján:

$$(a+b)^p = \binom{p}{0}a^p + \binom{p}{1}a^{p-1} + \binom{p}{2}a^{p-2} + \dots + \binom{p}{p-1}a + \binom{p}{p}.$$

Itt azonban $\binom{p}{k}$ mindig osztható p-vel, ha $1 \le k \le p-1$, hiszen a binomiális együttható fölírásánál a számlálóban levő p-t mint tényezőt nem egyszerűsítheti ki semmi a nevezőből. Ekkor viszont p karakterisztika esetén ezek a tagok eltűnnek, és így $(a+b)^p = a^p+b^p$. – *Megjegyzés:* Vegyük észre, hogy a fönti igen egyszerű módja a hatványra emelésnek (azaz, hogy tagonként hatványozunk – lásd: „középiskolások álma") csak a p-edik hatványra emelésnél működik, más kitevőkre már nem feltétlenül igaz. Az azonban még könnyen meggondolható, hogy p^k-adik hatványra is így kell emelni.
b) Az összeadandók számára vonatkozó teljes indukcióval igazoljuk, hogy a p-edik hatványra emelést szabad tagonként elvégezni.