

Előszó

A matematika tanárképzés oktatási programjában fontos szerepet játszik a számfogalom precíz matematikai felépítése, és a különböző számstruktúrák fontosabb tulajdonságainak levezetése az axiómákból. A matematika tanárok ezen ismeretek nélkül csak hiányosan tudják ellátni feladatukat. Ezt a hallgatók általában az alaptárgyakon belül (algebra, analízis, stb.) sajátíthatták el korlátozott terjedelemben és részletességgel. A téma fontosságára való tekintettel a számfogalom felépítését és a kapcsolódó legfontosabb ismereteket a József Attila Tudományegyetemen 1992 óta minden megfelelő előismeretekkel rendelkező hallgató által felvehető egy féléves tárgyként oktatjuk. Sajnos a téma a magyar nyelvű szakirodalomban hiányosan és csak több könyvben található meg. Ezt a hiányt igyekszik pótolni ez a jegyzet, mely lényegében az említett előadás anyagát tartalmazza néhány kiegészítéssel.

A jegyzetben a számfogalom felépítése a természetes számok halmazának Peano-axiómákkal történő megadásával indul, és az algebra tanulmányokból ismert differencia gyűrű, illetve hányadostest konstrukcióval jut az egész számok, illetve a racionális számok struktúrájához. A valós számokat nemcsak racionális számsorozatok segítségével, hanem ún. Dedekind-féle szeletekkel is megadjuk. A komplex számok szokásos elempáros bevezetése mellett két algebrai konstrukciót is ismertetünk. Külön fejezetben tárgyaljuk a racionális, az irracionális, az algebrai és a transzcendens számokat. Részletesen foglalkozunk a számkör további bővítésének lehetőségeivel. Tárgyaljuk az algebraikra és a hiperkomplex számokra vonatkozó legfontosabb ismereteket. Így megismerhetjük a komplex számkör két legfontosabb bővítését, a kvaterniók és a Cayley-számok algebraját. A számfogalom felépítése Frobenius tételével zárul. Az utolsó fejezetben röviden vázoljuk Conway konstrukcióját, mely ötvözi a természetes számok halmazelmélet axiómáira épülő megadását a valós számok Dedekind-féle szeletekre épülő konstrukciójával.

Mivel a konstrukciókban építünk absztrakt algebrai ismeretekre, az első fejezetben felsoroljuk a szükséges fogalmakat és összefüggéseket. A második fejezetben a részbenrendezett csoportokat, gyűrűket és testeket tárgyaljuk azzal a céllal, hogy az olvasó megismerje min múlnak az egész, a racionális és a valós számkör rendezésének közös tulajdonságai.

1. Absztrakt algebrai bevezető

Legyen A nemüres halmaz, n pedig nemnegatív egész szám. Az $f: A^n \rightarrow A$ leképezéseket A -n értelmezett n -változós műveleteknek nevezzük. Az $(a_1, \dots, a_n) \in A^n$ elem f szerinti képét $f(a_1, \dots, a_n)$ jelöli. Mivel $A^0 = \{\emptyset\}$, a 0-változós műveleteket egyértelműen meghatározza az $f(\emptyset) \in A$ elem, s ezért azonosítani is szoktuk vele.

Legyen \mathcal{F} egy halmaz, és nevezzük elemeit *műveletjeleknek*. Tegyük fel, hogy \mathcal{F} minden f eleméhez egy n nemnegatív egész szám van rendelve. Ekkor \mathcal{F} -et *algebratípusnak*, f -et pedig *n -változós műveletjelnek* nevezzük. Azt mondjuk, hogy az $(A; F)$ rendezett elempár \mathcal{F} -típusú *algebrai struktúra* (vagy röviden *algebra*), ha A nemüres halmaz (az *algebra alaphalmaza*) $F = \{f^A: f \in \mathcal{F}\}$ pedig A -n értelmezett műveleteknek egy rendszere, ahol minden $f \in \mathcal{F}$ esetén f^A egy A -n értelmezett n -változós művelet (n az f műveletjel változószáma). A gyakorlatban f^A helyett egyszerűen f -et írunk. Az ebből eredő kétértelműség csak ritkán okoz problémát. Ha \mathcal{F} véges, pl. $\mathcal{F} = \{f_1, \dots, f_k\}$, akkor $(A; F)$ helyett az $(A; f_1, \dots, f_k)$ jelölést is használjuk, többnyire úgy, hogy f_1, \dots, f_k változószámuk szerint csökkenő sorrendben követik egymást. Ha nem okoz félreértést, akkor az algebrát egyszerűen az alaphalmazával jelöljük. A kétváltozós műveleteket általában a $+$ vagy a \cdot szimbólumokkal jelöljük, és az (a, b) elempár képét e műveletek során $a + b$, $a \cdot b$ (vagy egyszerűen ab) jelöli, és az adott elemek összegének, illetve szorzatának nevezzük.

Egy algebrai struktúrát *grupoidnak* nevezünk, ha egyetlen kétváltozós művelettel rendelkezik. Ha a műveletnek van egységelem, illetve a művelet kommutatív, akkor *egységelemes*, illetve *kommutatív* grupoidról beszélünk. Az asszociatív műveletű grupoidokat *félcsoportoknak*, az olyan egységelemes félcsoportokat pedig, melyekben minden elemnek van inverze, *csoportoknak* nevezzük.

Azt mondjuk, hogy egy $(R; +, \cdot)$ algebrai struktúra *félgűrű*, ha $(R; +)$ kommutatív és egységelemes félcsoport, $(R; \cdot)$ félcsoport, és a szorzás disztributív az összeadásra nézve. Az $(R; +, \cdot)$ félgűrűt *gyűrűnek* nevezzük, ha $(R; +)$ csoport. Ha egy félgűrű vagy gyűrű szorzása egységelemes, illetve kommutatív akkor egységelemes, illetve kommutatív félgűrűnek vagy gyűrűnek hívjuk. Azt mondjuk, hogy az $(R; +, \cdot)$ gyűrű *integritástartomány*, ha kommutatív, egységelemes és zérusosztómentes, azaz bármely $a, b \in R$ esetén, ha

$ab = 0$, akkor $a = 0$ vagy $b = 0$. Az olyan $(R; +, \cdot)$ kommutatív gyűrűket, melyekre $(R \setminus \{0\}; \cdot)$ csoport (0 az additív egységelem), *testeknek* nevezzük. Ha R a szorzás kommutativitását esetleg leszámítva a testek minden tulajdonságával rendelkezik, akkor *ferdetestnek* nevezzük. Ha $(R; +, \cdot)$ a szorzás asszociativitását leszámítva minden gyűrű axiómát teljesít, akkor *nem-asszociatív gyűrűnek* hívjuk. A nem-asszociatív jelző csak annyit jelent, hogy a szorzás asszociativitása nem axióma, de nem zárja ki érvényességét.

Legyen $(A; F)$ és $(B; F)$ két azonos típusú algebra. Egy $\varphi: A \rightarrow B$ leképezést *homomorfizmusnak* nevezünk, ha felcserélhető a műveletekkel, azaz tetszőleges $f \in F$ n -változós ($n \geq 0$) művelet és $a_1, \dots, a_n \in A$ esetén

$$f(a_1, \dots, a_n)\varphi = f(a_1\varphi, \dots, a_n\varphi).$$

Ha φ szürjektív, akkor a második struktúrát az első *homomorfképének* nevezzük. A bijektív homomorfizmust *izomorfizmusnak*, az injektívét pedig *beágyazásnak* hívjuk. Homomorfizmusok szorzata homomorfizmus, és izomorfizmusok inverze is izomorfizmus.

Számos művelettulajdonság öröklődik szürjektív homomorfizmus esetén. Ilyen tulajdonságok például a kommutativitás, az asszociativitás, a disztributivitás, valamint az egységelem és inverz elem létezése. Így csoport, félgűrű, illetve gyűrű homomorf képe is csoport, félgűrű, illetve gyűrű.

Legyen $(A; F)$ algebrai struktúra és ρ ekvivalenciareláció az A halmazon. Azt monjuk, hogy ρ *kongruenciareláció*, és a hozzá tartozó ekvivalenciareláció *kompatibilis osztályozás*, ha a műveletek megőrzik, azaz tetszőleges $f \in F$ n -változós ($n \geq 0$) művelet és $a_1, b_1, \dots, a_n, b_n \in A$ esetén

$$(a_1, b_1), \dots, (a_n, b_n) \in \rho \Rightarrow (f(a_1, \dots, a_n), f(b_1, \dots, b_n)) \in \rho.$$

Csoportok kompatibilis osztályozásai a normálosztó szerinti, gyűrűk kompatibilis osztályozásai pedig az ideál szerinti osztályozások. Ha f kétváltozós, és az egyszerűség kedvéért \cdot jelöli, akkor elegendő megkövetelni a következő látszólag gyengébb feltételt: Tetszőleges $a, b, c \in S$ esetén,

$$(a, b) \in \rho \Rightarrow (ac, bc) \in \rho, (ca, cb) \in \rho.$$

Ugyanis, ha $(a, b) \in \rho$ és $(c, d) \in \rho$, akkor $(ac, bc) \in \rho$ és $(bc, bd) \in \rho$, amiből ρ tranzitivitása miatt $(ac, bd) \in \rho$ következik.

Legyen ρ az $(A; F)$ algebra kongruenciarelációja. Jelölje A/ρ az A halmaz ρ szerinti faktorhalmazát, azaz ρ osztályainak halmazát, s ha $a \in A$, akkor az a -t tartalmazó osztályt jelölje a/ρ . Ha nem okoz félreértést, akkor a/ρ helyett az \bar{a} jelölést is használjuk. Minden $f \in F$ n -változós ($n \geq 0$) művelet segítségével természetesen módon értelmezhetünk egy ugyancsak f -fel jelölt n -változós műveletet az A/ρ halmazon: Tetszőleges $a_1/\rho, \dots, a_n/\rho \in A/\rho$ esetén legyen

$$f(a_1/\rho, \dots, a_n/\rho) \stackrel{\text{def}}{=} f(a_1, \dots, a_n)/\rho.$$

Így az $(A; F)$ algebraival azonos típusú $(A/\rho; F)$ algebraát definiáltunk, melyet $(A; F)$ ρ szerinti *faktorstruktúrájának* vagy *faktoralgebrájának* nevezzük. Könnyen ellenőrizhető, hogy az $A \rightarrow A/\rho$, $a \mapsto a/\rho$ leképezés szürjektív homomorfizmus.

Egy nemüres A halmazon értelmezett kétváltozós ρ relációt *részbenrendezésnek* nevezünk, ha reflexív, antiszimmetrikus és tranzitív. Ha ρ dichotom, azaz bármely $a, b \in A$ esetén $a \rho b$ vagy $b \rho a$, akkor ρ -t *rendezésnek* vagy *lineáris rendezésnek* hívjuk.

2. Részbenrendezett csoportok és gyűrűk

2.1. Definíció. Legyen $(G; \cdot)$ csoport és \leq részbenrendezés G -n. G *részbenrendezett csoport* \leq -re nézve, ha tetszőleges $a, b, c \in G$ esetén $a \leq b$ -ből $ac \leq bc$ és $ca \leq cb$ következik. Ha ráadásul \leq rendezés, akkor azt mondjuk, hogy G *rendezett*, *lineárisan rendezett* vagy *elrendezett csoport* \leq -re nézve. Ha G részbenrendezett csoport a \leq részbenrendezésre nézve, akkor az $\{a \in G: 1 \leq a\}$ halmazt a részbenrendezett csoport *pozitivitási tartományának* nevezzük, ahol 1 a csoport egységeleme.

2.2. Állítás. Legyen $(G; \cdot)$ egy csoport és \leq egy részbenrendezés G -n. A következő állítások ekvivalensek:

- (1) Tetszőleges $a, b, c \in G$, ha $a \leq b$, akkor $ac \leq bc$ és $ca \leq cb$.
- (2) Tetszőleges $a, b, c, d \in G$ esetén, ha $a \leq b$ és $c \leq d$, akkor $ac \leq bd$ és $ca \leq db$.
- (3) Tetszőleges $a, b, c \in G$ esetén, ha $a < b$, akkor $ac < bc$ és $ca < cb$.

Bizonyítás. (1) \Rightarrow (2). Ha $a \leq b$ és $c \leq d$, akkor (1) miatt $ac \leq bc$ és $bc \leq bd$, amiből a tranzitivitás miatt $ac \leq bd$ következik. (2) \Rightarrow (1). Ha $a \leq b$ és $c \in G$, akkor $c \leq c$, és így (2) miatt $ac \leq bc$ és $ca \leq cb$.

(1) \Rightarrow (3). Ha $a < b$ és $c \in G$, akkor $a \leq b$ és $a \neq b$. Ezért (1) szerint $ac \leq bc$ és $ca \leq cb$. Ha valamelyik reláció egyenlőséggel teljesülne, akkor abból az $a = b$ ellentmondás következne, mert csoportban lehet egyszerűsíteni. Tehát $ac < bc$ és $ca < cb$.

(3) \Rightarrow (1). Legyen $a \leq b$ és $c \in G$. Ha $a = b$, akkor $ac = bc$ és $ca = cb$. Ha $a \neq b$, azaz $a < b$, akkor (3) szerint $ac < bc$ és $ca < cb$. Tehát mindkét esetben $ac \leq bc$ és $ca \leq cb$. ■

2.3. Tétel. Legyen $(G; \cdot)$ részbenrendezett csoport a \leq részbenrendezésre nézve, és jelölje P a pozitivitási tartományát. Ekkor $a \leq b$ akkor és csak akkor, ha $a^{-1}b \in P$ ($ba^{-1} \in P$). G akkor és csak akkor lineárisan rendezett \leq -re nézve, ha bármely $x \in G$ esetén $x \in P$ vagy $x^{-1} \in P$. Továbbá, P rendelkezik a következő négy tulajdonsággal:

- (a) $1 \in P$.
- (b) Ha $a \in P$ és $a^{-1} \in P$, akkor $a = 1$.
- (c) Ha $a, b \in P$, akkor $ab \in P$.
- (d) Ha $a \in P$ és $x \in G$, akkor $x^{-1}ax \in P$.

Bizonyítás. Ha $a \leq b$, akkor $1 = a^{-1}a \leq a^{-1}b$ ($1 = aa^{-1} \leq ba^{-1}$), és így $a^{-1}b \in P$ ($ba^{-1} \in P$). Ha $a^{-1}b \in P$ ($ba^{-1} \in P$), akkor $1 \leq a^{-1}b$ ($1 \leq ba^{-1}$), amiből $a = a1 \leq a(a^{-1}b = b)$ ($a = 1a \leq (ba^{-1})a = b$) következik. Ezzel az első állítást igazoltuk.

Ha G lineárisan rendezett, akkor bármely $a \in G$ esetén $1 \leq a$ vagy $a \leq 1$. Az első esetben $a \in P$, a második esetben pedig $1 = aa^{-1} \leq 1a^{-1} = a^{-1}$, és így $a^{-1} \in P$. Tegyük fel, hogy bármely $x \in G$ esetén $x \in P$ vagy $x^{-1} \in P$. Ha $a, b \in G$, akkor $a^{-1}b \in P$ vagy $b^{-1}a = (a^{-1}b)^{-1} \in P$, azaz $1 \leq a^{-1}b$ vagy $1 \leq b^{-1}a$. Az első esetben $a = a1 \leq a(a^{-1}b) = b$, a második esetben pedig $b = b1 \leq b(b^{-1}a) = a$. Tehát G lineárisan rendezett.

Most rátérünk P tulajdonságainak igazolására. Mivel $1 \leq 1$, ezért $1 \in P$. Ha $a \in P$ és $a^{-1} \in P$, azaz $1 \leq a$ és $1 \leq a^{-1}$, akkor a második relációból $a = a1 \leq aa^{-1} = 1$ következik, és így az antiszimetria miatt $a = 1$. Ha $a, b \in P$, azaz $1 \leq a$ és $1 \leq b$, akkor $1 = 11 \leq ab$, vagyis $ab \in P$. Ha $a \in P$, azaz $1 \leq a$, és $x \in G$, akkor $1 = x^{-1}1x \leq x^{-1}ax$. Tehát $x^{-1}ax \in P$. ■

2.4. Tétel. Legyen $(G; \cdot)$ csoport és $P \subseteq G$ olyan részhalmaz, mely rendelkezik a 2.3. Tételben megfogalmazot (a), (b), (c) és (d) tulajdonságokkal. Definiáljunk egy \leq relációt G -n a következőképpen:

$$a \leq b \stackrel{\text{def}}{\Leftrightarrow} a^{-1}b \in P, \quad a, b \in G.$$

Ekkor \leq részbenrendezés, melyre nézve G részbenrendezett csoport a P pozitivitási tartománnyal.

Bizonyítás. Tegyük fel, hogy $(G; \cdot)$, P és \leq teljesítik a tétel feltételeit. Az (a) feltétel miatt $1 \in P$. Ezért bármely $a \in G$ esetén $a^{-1}a \in P$, és így $a \leq a$. Ha $a \leq b$ és $b \leq a$, azaz $a^{-1}b \in P$ és $(a^{-1}b)^{-1} = b^{-1}a \in P$, akkor (b) miatt $a^{-1}b = 1$ és $a = b$. Ha $a \leq b$ és $b \leq c$, vagyis $a^{-1}b \in P$ és $b^{-1}c \in P$, akkor (c) szerint $a^{-1}c = (a^{-1}b)(b^{-1}c) \in P$ és $a \leq c$. Tehát \leq reflexív, antiszimmetrikus és tranzitív, és így részbenrendezés.

Ha $a \leq b$, azaz $a^{-1}b \in P$, és $c \in G$, akkor egyrészt $((ca)^{-1})(cb) = (a^{-1}c^{-1})(cb) = a^{-1}b \in P$ és $ac \leq bc$, másrészt (d) miatt $(ac)^{-1}(bc) = (c^{-1}a^{-1})(bc) = c^{-1}(a^{-1}b)c \in P$ és $ac \leq bc$. Tehát G részbenrendezett csoport a \leq relációra nézve. Mivel $1 \leq a$ ekvivalens azzal, hogy $a = 1a = 1^{-1}a \in P$, a pozitivitási tartományra vonatkozó állítás is igaz. ■

2.5. Definíció. Legyen $(R; +, \cdot)$ gyűrű és \leq részbenrendezés R -en. Azt mondjuk, hogy R *részbenrendezett gyűrű* a \leq relációra nézve, ha tetszőleges $a, b, c \in R$ esetén $a \leq b$ -ből $a + c \leq b + c$ következik, azaz $(R; +)$ részbenrendezett csoport \leq -re nézve, és bármely $a, b, c \in R$ esetén, ha $a \leq b$ és $0 < c$, akkor $ac \leq bc$ és $ca \leq cb$. Ha ráadásul \leq rendezés, akkor azt mondjuk, hogy R *rendezett, lineárisan rendezett vagy elrendezett gyűrű* a \leq részbenrendezésre nézve. Ha R részbenrendezett gyűrű \leq -re nézve, akkor az $\{a \in R: 0 \leq a\}$ halmazt a részbenrendezett gyűrű *pozitivitási tartományának* nevezzük.

2.6. Állítás. Legyen $(R; +, \cdot)$ zérusosztómentes gyűrű és \leq részbenrendezés R -en. A következő két állítás ekvivalens:

- (1) Tetszőleges $a, b, c \in R$ esetén, ha $a \leq b$ és $0 < c$, akkor $ac \leq bc$ és $ca \leq cb$.
- (2) Tetszőleges $a, b, c \in R$ esetén, ha $a < b$ és $0 < c$, akkor $ac < bc$ és $ca < cb$.

Bizonyítás. Mivel zérusosztómentes gyűrűben 0-tól különböző tényezővel lehet egyszerűsíteni, a 2.2. Tétel bizonyításának (1) \Rightarrow (3) és (3) \Rightarrow (1) részét szinte szó szerint átvehetjük. ■

2.7. Tétel. Legyen $(R; +, \cdot)$ részbenrendezett gyűrű a \leq részbenrendezésre nézve, és jelölje P a pozitivitási tartományát. Ekkor $a \leq b$ akkor és csak akkor, ha $b - a \in P$. R akkor és csak akkor lineárisan rendezett \leq -re nézve, ha bármely $x \in R$ esetén $x \in P$ vagy $-x \in P$. Továbbá, P rendelkezik a következő négy tulajdonsággal:

- (i) $0 \in P$.
- (ii) Ha $a \in P$ és $-a \in P$, akkor $a = 0$.
- (iii) Ha $a, b \in P$, akkor $a + b \in P$.
- (iv) Ha $a, b \in P$, akkor $ab \in P$.

Bizonyítás. Tegyük fel, hogy $(R; +, \cdot)$, P és \leq teljesítik a tétel feltételeit. Mivel az $(R; +)$ kommutatív csoport részbenrendezett \leq -re nézve, a tétel állításai (iv)-et kivéve a 2.3. Tételből következnek. Legyen $a, b \in P$, azaz $0 \leq a, b$. Ha $b=0$, akkor $ab = a0 = 0 \in P$. Ha pedig $0 < b$, akkor $0 = 0b \leq ab$, vagyis $ab \in P$. ■

2.8. Tétel. Legyen $(R; +, \cdot)$ gyűrű és $P \subseteq R$ egy olyan részhalmaz, mely rendelkezik a 2.7. Tételben megfogalmazot (i), (ii), (iii) és (iv) tulajdonságokkal. Defináljunk egy \leq relációt R -en a következőképpen:

$$a \leq b \stackrel{\text{def}}{\iff} b - a \in P, \quad ab \in R.$$

Ekkor \leq részbenrendezés, melyre nézve R részbenrendezett gyűrű a P pozitivitási tartománnyal.

Bizonyítás. Tegyük fel, hogy $(R; +, \cdot)$, P és \leq teljesítik a tétel feltételeit. Ekkor az (i), (ii) és (iii) feltételek és $+$ kommutativitása biztosítják, hogy $(R; +)$, P és \leq teljesítik 2.4. Tétel feltételeit. Ezért $(R; +)$ részbenrendezett csoport \leq -re nézve a P pozitivitási tartománnyal. Ha $a \leq b$ és $0 < c$, akkor $b - a, c = c - 0 \in P$, és így (iv) szereint $bc - ac = (b - a)c \in P$ és $cb - ca = c(b - a) \in P$, amiből \leq definíciója miatt $ac \leq bc$ és $ca \leq cb$ következik. ■

2.9. Tétel. Legyen $(R; +, \cdot)$ részbenrendezett gyűrű a P pozitivitási tartománnyal. Legyen továbbá R' az R gyűrű egy részbenrendezett részgyűrűje a P' pozitivitási tartománnyal. Ekkor R' részbenrendezése akkor és csak akkor megszorítása R részbenrendezésének, ha $P' \subseteq P$. Az állítás érvényes csoportokra is.

Bizonyítás. Jelölje \leq az R gyűrű, \preceq pedig az R' részgyűrű részbenrendezését. Ha $P' \subseteq P$ és $a \preceq b$, akkor $b - a \in P' \subseteq P$, amiből $a \leq b$ következik. Tegyük fel, hogy \preceq megszorítása \leq -nek. Ha $a \in P'$, akkor $0 \preceq a$, amiből a feltevés szerint $0 \leq a$ és $a \in P$ következik. ■

2.10. Tétel. Ha $(R; +, \cdot)$ gyűrű, s jelölje \mathcal{R} R részbenrendezéseinek halmazát, \mathcal{P} pedig R azon részhalmazainak halmazát, melyek rendelkeznek a pozitivitási tartományok tulajdonságaival. Ekkor

$$\mathcal{R} \rightarrow \mathcal{P}, \quad \leq \mapsto \{x \in G: 1 \leq x\}$$

tartalmazástartó bijektív leképezés. Hasonló állítás érvényes csoportok részbenrendezéseire és pozitivitási tartományaira.

Bizonyítás. Állításaink a 2.3, 2.4, 2.7, 2.8 és 2.9 tételek következménye. ■

2.11. Tétel. Legyen R egy lineárisan rendezett gyűrű a \leq relációra nézve, és definiáljuk R elemeinek abszolút értékét a következőképpen:

$$|x| = \begin{cases} x, & \text{ha } x \geq 0; \\ -x, & \text{különben.} \end{cases}$$

Ekkor tetszőleges $a, b \in R$ esetén $-|a| \leq a \leq |a|$, $|a| = |-a|$, $|ab| = |a| \cdot |b|$ és $|a + b| \leq |a| + |b|$.

Bizonyítás. Az első két állítás azonnal adódik a definícióból. A harmadik állítás igazolását az olvasóra bizzuk, mert attól függően, hogy a és b eleme a pozitivitási tartománynak vagy nem, az $ab = (-a)(-b)$ és $a - ab = (-a)b = a(-b)$ egyenlőségek felhasználásával egyszerű számolással megkapható. Most nézzük a negyedik állítást. Ha $a + b \geq 0$, akkor $|a + b| = a + b \leq |a| + |b|$. Ha $a + b < 0$, akkor $|a + b| = -(a + b) = (-a) + (-b) \leq |a| + |b|$. ■

2.12. Tétel. Ha $(R; +, \cdot)$ egy lineárisan rendezett gyűrű a P pozitivitási tartománnyal, akkor bármely $a_1, \dots, a_n \in R$ esetén $a_1^2 + \dots + a_n^2 \in P$. Ha ráadásul R zérusosztómentes, akkor $a_1^2 + \dots + a_n^2 = 0$ -ből $a_1 = \dots = a_n = 0$ következik.

Bizonyítás. Legyen R egy lineárisan rendezett gyűrű a P pozitivitási tartománnyal, és legyen $a_1, \dots, a_n \in R$. A 2.7. Tétel szerint $a_i \in P$ vagy $-a_i \in P$, $i = 1, \dots, n$. Ezért ugyancsak a 2.7. Tétel szerint $a_i^2 = a_i a_i = (-a_i)(-a_i) \in P$ és $a_1^2 + \dots + a_n^2 \in P$. Ha R zérusosztómentes és $a_1^2 + \dots + a_n^2 = 0$, akkor $a_i^2 \in P$ és $-a_i^2 = (a_1^2 + \dots + a_{i-1}^2 + a_{i+1}^2 + \dots + a_n^2) \in P$, amiből $a_i^2 = 0$ és $a_i = 0$ következik, $i = 1, \dots, n$. ■

2.13. Tétel. Egy $(R; +, \cdot)$ integritástartománynak akkor és csak akkor van lineáris rendezése, ha bármely $a_1, \dots, a_n \in R$ esetén $a_1^2 + \dots + a_n^2 = 0$ -ből $a_1 = \dots = a_n = 0$ következik.

Bizonyítás. A szükségesség a 2.12. Tétel második állítása. Tegyük fel, hogy az R integritástartomány teljesíti a tétel feltételét. Könnyű ellenőrizni, hogy az

$$X = \{a_1^2 + \dots + a_n^2 : n \in \mathbf{N}, a_1, \dots, a_n \in R\}$$

halmaz rendelkezik a pozitivitási tartományok tulajdonságaival. Ha X_i , $i \in I$ olyan X -et tartalmazó pozitivitási tartományok, melyek közül bármelyik kettő összehasonlítható a tartalmazási reláció szerint, akkor $\bigcup_{i \in I} X_i$ is pozitivitási tartomány. Valóban, ha $a, b \in \bigcup_{i \in I} X_i$, akkor van olyan $i, j \in I$, hogy $a \in X_i$ és $b \in X_j$. A feltevés miatt a két halmaz közül az egyik tartalmazza a másikat, ezért abban benne van a és b is, és így tartalmazza az $a + b$ és az ab elemeket is, amiből $a + b, ab \in \bigcup_{i \in I} X_i$ következik. Ha $a, -a \in \bigcup_{i \in I} X_i$, akkor van olyan $i, j \in I$, hogy $a \in X_i$ és $-a \in X_j$. A két halmaz közül a bővebb tartalmazza az a és $-a$ elemet is, ezért $a = 0$.

Mindezek miatt a Zorn-lemma szerint van R -ben maximális X -et tartalmazó pozitivitási tartomány, s legyen P egy ilyen. Megmutatjuk, hogy R a P pozitivitási tartománnyal lineárisan rendezett gyűrű. Előbb megmutatjuk, hogy P teljesíti a következőt:

(*) Ha $a \in P$, $a \neq 0$, és $ax \in P$, akkor $x \in P$.

Tekintsük a

$$P' = \{x \in R : \text{van olyan } a \in P, \text{ hogy } a \neq 0 \text{ és } ax \in P\}$$

halmazt. P szorzásra való zártsága miatt $P \subseteq P'$. Ha $x, y \in P'$, akkor van olyan $a, b \in P$, $a, b \neq 0$, hogy $ax, by \in P$. Ekkor a zérusosztómentesség miatt $ab \neq 0$, és $(ab)(x + y) = (ax)b + a(by)$, $(ab)(xy) \in P$. Ezért $x + y, xy \in P'$. Ha $x, -x \in P'$, akkor van olyan $a, b \in P$, $a, b \neq 0$, hogy $ax, -bx = b(-x) \in P$. Ezért $abx = (ax)b \in P$ és $-abx = a(b(-x)) \in P$, amiből $abx = 0$ és $x = 0$ következik. Tehát P' is pozitivitási tartomány. P maximalitásából $P = P'$ és (*) következik.

Már csak azt kell megmutatni, hogy tetszőleges $x \in R$ esetén $x \in P$ vagy $-x \in P$. Tegyük fel, hogy $x \neq 0$ és $x \notin P$. Tekintsük a

$$Q = \{a + bx : a, b \in P\}$$

halmazt. Ha $a+bx, c+dx \in Q, a, b, c, d \in P$, akkor $(a+bx)+(c+dx) = (a+c)+(b+d)x \in Q$, és $x^2 \in X \subseteq P$ miatt $(a+bx)(c+dx) = (ab+bdx^2) + (ad+bc)x \in Q$, vagyis Q zárt az összeadásra és a szorzásra. P valódi részhalmaza Q -nak, mert ha $a \in P$, akkor $a = a+0x \in Q$, és $x = 0+1x \in Q$, hiszen $1 = 1^2 \in X \subseteq P$. Ezért P maximalitása miatt Q nem lehet pozitivitási tartomány.

Mivel Q tartalmazza a 0 -t, és zárt az összeadásra és a szorzásra, ez csak úgy lehet, hogy valamely $y \in R, y \neq 0$, elemre $y, -y \in Q$. Ekkor van olyan $a, b, c, d \in P$, hogy $y = a+bx$ és $c+dx = -y$. Ebből $(a+c)+(b+d)x = 0$ és $(b+d)(-x) = a+c \in P$ következik. Ha $b+d \neq 0$, akkor (*) szerint $-x \in P$, amit igazolni akartunk. Végül $b+d = 0$ nem teljesülhet, mert ellenkező esetben $a+c = 0$, amiből $a, -a = c, b, -b = d \in P, a = b = c = d = 0$ és $y = a+bx = 0$ következik, ami ellentmond feltevésünknek. ■

Példák és feladatok

1. A $(\mathbf{Z}; +, \cdot)$ gyűrű részenrendezett a következő pozitivitási tartományokkal:

$$P_{a_1, \dots, a_n} = \left\{ \sum_{i=1}^n a_i x_i : x_1, \dots, x_n \in \mathbf{N}_0 \right\}, \quad n, a_1, \dots, a_n \in \mathbf{N},$$

és

$$\hat{P}_{a_1, \dots, a_n} = \left\{ \sum_{i=1}^n a_i x_i : x_1, \dots, x_n \in \mathbf{N} \right\} \cup \{0\}, \quad n, a_1, \dots, a_n \in \mathbf{N}.$$

- Ekkor például $P_1 = \mathbf{N}_0, P_0 = \{0\}, P_3 = \hat{P}_3 = \{3x : x \in \mathbf{N}_0\}, P_{2,3} = \mathbf{N}_0 \setminus \{1\}$ és $\hat{P}_{2,3} = \mathbf{N}_0 \setminus \{1, 2, 3, 4, 6\}$.
2. Az $(\mathbf{R}; +, \cdot)$ test részenrendezett a következő pozitivitási tartományokkal: $\mathbf{Q}^+ \cup \{0\}, \{x \in \mathbf{R} : a \leq x\} \cup \{0\} (a \geq 1)$,

$$P_{a_1, \dots, a_n} = \left\{ \sum_{i=1}^n a_i x_i : x_1, \dots, x_n \in \mathbf{R}^+ \cup \{0\} \right\}, \quad a_1, \dots, a_n \in \mathbf{R}^+, n \in \mathbf{N},$$

és

$$\hat{P}_{a_1, \dots, a_n} = \left\{ \sum_{i=1}^n a_i x_i : x_1, \dots, x_n \in \mathbf{R}^+ \right\} \cup \{0\}, \quad a_1, \dots, a_n \in \mathbf{R}^+, n \in \mathbf{N}.$$

3. Az $(\mathbf{R}^2; +)$ csoport részenrendezett a $P_1 = \{(x, y) \in \mathbf{R}^2 : x, y \geq 0\}$, és rendezett a $P_2 = \{(x, y) \in \mathbf{R}^2 : x > 0 \text{ vagy } x, y \geq 0\}$ pozitivitási tartományokkal. (x, y) pontosan akkor kisebb (u, v) -nél P_1 szerint, ha $x \leq u$ és $y \leq v$, P_2 szerint pedig pontosan akkor, ha $x < u$ vagy $x = u$ és $y \leq v$. A második reláció \mathbf{R}^2 lexikografikus rendezése.
4. Bizonyítsuk be, hogy az egész számok gyűrűjének, a racionális és a valós számok testének egyetlen rendezése van, a komplex számok testének pedig nincs rendezése.
5. A valós számsorozatok $(\mathbf{R}^{\mathbf{N}}; +)$ csoportja rendezett a

$$P = \{f \in \mathbf{R}^{\mathbf{N}} : f \text{ minden tagja } 0, \text{ vagy } f(1) = \dots = f(n-1) = 0, f(n) > 0 \text{ valamely } n \in \mathbf{N}\text{-re}\}$$

pozitivitási tartománnyal. A P -hez tartozó reláció a lexikografikus rendezés.

6. A valós számsorozatok $(\mathbf{R}^{\mathbf{N}}; +, \cdot)$ gyűrűje részenrendezett az

$$\{f \in \mathbf{R}^{\mathbf{N}} : f(n) \geq 0 \text{ minden } n \in \mathbf{N}\text{-re, és } f \in S\}$$

pozitivitási tartománnyal, ahol S a korlátos sorozatok halmaza, vagy a konvergens sorozatok halmaza, vagy azoknak a sorozatoknak a halmaza, melyeknek véges sok nullától különböző tagja van, vagy sorozatoknak bármely olyan halmaza, mely tartalmazza a 0 -t, és zárt az összeadásra és a szorzásra. Adjunk további példákat S -re.

7. A valós függvények $(\mathbf{R}^{\mathbf{R}}; +, \cdot)$ gyűrűje részenrendezett az

$$\{f \in \mathbf{R}^{\mathbf{R}} : f(x) \geq 0 \text{ minden } x \in \mathbf{R}\text{-re, és } f \in F\}$$

pozitivitási tartománnyal, ahol F a polinomok halmaza, vagy a differenciálható függvények halmaza, vagy az integrálható függvények halmaza, vagy a lépcsős függvények halmaza, vagy bármely olyan függvényhalmaz, mely tartalmazza a 0-t, és zárt az összeadásra és a szorzásra. Adjunk további példákat F -re.

8. Igazoljuk, hogy az $(\{a+b\sqrt{2}: a, b \in \mathbf{Q}\}; +, \cdot)$ test rendezett az $\{a+b\sqrt{2}: a, b \in \mathbf{Q}, a-b\sqrt{2} \geq 0\}$ pozitivitási tartománnyal.

3. Természetes számok

Azt mondjuk, hogy az N halmaz a *természetes számok* halmaza, ha teljesíti az ún. *Peano-féle axiómarendszert*:

- (P1) N nemüres halmaz és van egy $0 \in N$ kitüntetett eleme.
- (P2) Adott egy $': N \rightarrow N$ leképezés.
- (P3) Nincs olyan $n \in N$, melyre $n' = 0$.
- (P4) Minden $m, n \in N$ esetén valahányszor $m' = n'$, mindannyiszor $m = n$ (azaz $'$ injektív).
- (P5) Ha $U \subseteq N$ olyan, hogy $0 \in U$, és valahányszor $u \in U$, mindannyiszor $u' \in U$, akkor $U = N$.

Az algebrai struktúrák nyelvén a következőképpen fogalmazhatunk: A természetes számok halmaza egy olyan $(N; ', 0)$ algebrai struktúra, melyre (P1) és (P2) szerint 0 nullaváltozós, $'$ pedig egyváltozós művelet, mely teljesíti a (P3) és (P4) axiómát. A (P5) axióma pontosan azt jelenti, hogy $(N; ', 0)$ -nak nincs valódi részstruktúrája. Ugyanis egy $U \subseteq N$ halmaz pontosan akkor részstruktúra, ha zárt a 0 nullaváltozós műveletre, azaz $0 \in U$, és zárt a $'$ egyváltozós műveletre, vagyis $n \in U$ esetén $n' \in U$ is teljesül.

A halmazelmélet Zermelo-Frankel-féle axiómarendszerére építve megmutatható, hogy létezik az

$$N = \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}, \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}, \dots\}$$

halmaz. Ekkor $(N; *, \emptyset)$ modellje a Peano-féle axiómarendszernek, ahol minden $n \in N$ -re $n^* = n \cup \{n\}$.

A Peano-féle axiómarendszer nem biztosítja a természetes számok halmazának létezését, de – mint azt hamarosan látni fogjuk – izomorfiától eltekintve egyértelműen meghatározza. Ennek igazolásához szükségünk van a rekurzív definícióra, amit a következő tétel biztosít:

3.1. Tétel. *Legyen A nemüres halmaz, $a_0 \in A$, és $*$: $A \rightarrow A$ egy leképezés. Tegyük fel továbbá, hogy $(N; ', 0)$ teljesíti a Peano-féle axiómákat. Ekkor létezik pontosan egy olyan $\varphi: N \rightarrow A$ leképezés, melyre $0\varphi = a_0$ és minden $n \in N$ esetén $n'\varphi = (n\varphi)^*$.*

Bizonyítás. Definiáljunk egy φ parciális leképezést N -ből A -ba a következőképpen: legyen $0\varphi = a_0$, és ha valamely n -re $n\varphi$ értelmezve van, akkor legyen $n'\varphi = (n\varphi)^*$. A (P4) axióma biztosítja φ egyértékűségét, (P5) pedig azt, hogy N minden elemére definiálva van. Tehát létezik a tétel feltételeinek eleget tevő leképezés. Az egyértelműség igazolásához tegyük fel, hogy egy $\psi: N \rightarrow A$ leképezésre is $0\psi = a_0$, és $n'\psi = (n\psi)^*$ minden $n \in N$ esetén. Legyen $U = \{n \in N: n\varphi = n\psi\}$. Ekkor $0 \in U$, és ha $n \in U$, azaz $n\varphi = n\psi$, akkor $n'\varphi = (n\varphi)^* = (n\psi)^* = n'\psi$, vagyis $n' \in U$. Így (P5) szerint $U = N$ és $\varphi = \psi$. ■

3.2. Tétel. *A természetes számok halmaza a Peano-féle axiómarendszerrel izomorfiától eltekintve egyértelműen meghatározott.*

Bizonyítás. Tegyük fel, hogy az $(N; ', 0)$ és az $(M; *, o)$ algebrai struktúrák kielégítik a (P1)–(P5) axiómákat. A rekurzív definíció értelmében léteznek olyan $\varphi: N \rightarrow M$ és $\psi: M \rightarrow N$ leképezések, melyekre $0\varphi = o$, $o\psi = 0$ és $n'\varphi = (n\varphi)^*$, $m*\psi = (m\psi)'$ minden $n \in N$ és $m \in M$ esetén. Elegendő azt megmutatni, hogy φ izomorfizmus. Mivel φ felcserélhető mind a nullaváltozós mind pedig az egyváltozós művelettel, ezért homomorfizmus. Legyen $U = \{n \in N: n(\varphi\psi) = n\}$. Most $0(\varphi\psi) = (0\varphi)\psi = o\psi = 0$, ezért $0 \in U$. Ha $n \in U$, azaz $n(\varphi\psi) = n$, akkor $n'(\varphi\psi) = (n'\varphi)\psi = ((n\varphi)^*)\psi = ((n\varphi)\psi)' = (n(\varphi\psi))' = n'$, amiből $n' \in U$ következik. Így (P5) miatt $U = N$, azaz $\varphi\psi = \text{id}_N$. Hasonlóan látható be $\psi\varphi = \text{id}_M$ is. Ezért φ bijektív, és így izomorfizmus. ■

Legyen $(\mathbf{N}_0; ', 0)$ a Peano-féle axiómarendszer egy rögzített modellje. Mostantól a természetes számok halmazának mindig ezt a modellt tekintjük. Vezessük be a megszokott $\mathbf{N} = \mathbf{N}_0 \setminus \{0\}$ jelölést.

Az ötödik axiómát a *teljes indukció axiómájának* is nevezik, mivel a teljes indukciós bizonyításnak ez az alapja.

3.3. Teljes indukció tétele. *A P_n kijelentés, amelynek megfogalmazásában az n természetes szám mint paraméter előfordul, igaz minden természetes számra, ha P_0 igaz, és valahányszor P_k igaz, mindannyiszor $P_{k'}$ is igaz.*

Bizonyítás. Jelölje U azoknak az n természetes számoknak a halmazát, amelyekre P_n igaz. A tétel feltételei és (P5) miatt $U = \mathbf{N}_0$. ■

3.4. Állítás. $\mathbf{N} = \{n' : n \in \mathbf{N}_0\}$.

Bizonyítás. Világos, hogy az $U = \{0\} \cup \{n' : n \in \mathbf{N}_0\}$ halmaz teljesíti (P5) feltételeit. Ezért $U = \mathbf{N}_0$, amiből következik az állítás. ■

3.5. Állítás. *Minden n természetes számra $n' \neq n$.*

Bizonyítás. Legyen $U = \{n \in \mathbf{N}_0 : n' \neq n\}$. (P3) miatt $0 \in U$. Ha $n \in U$, akkor $n' \in U$, mert ellenkező esetben $(n')' = n'$, amiből (P4) miatt $n' = n$ és $n \notin U$ következik. ■

A természetes számok halmazán az összeadást, illetve a szorzást rekurzív definícióval adjuk meg oly módon, hogy tetszőleges m első tagra, illetve első tényezőre megmondjuk, hogy hogyan kell m -hez hozzáadni a második tagot, illetve hogyan kell megszorozni m -et a második tényezővel:

3.6. Definíció. Tetszőleges $m \in \mathbf{N}_0$ esetén legyen

$$m + 0 \stackrel{\text{def}}{=} m \quad \text{és} \quad m + n' \stackrel{\text{def}}{=} (m + n)',$$

$$m \cdot 0 \stackrel{\text{def}}{=} 0 \quad \text{és} \quad m \cdot n' \stackrel{\text{def}}{=} m \cdot n + m.$$

Vezessük be a következő jelölést: $1 = 0'$. Vegyük észre, hogy minden $n \in \mathbf{N}_0$ -re $n' = (n+0)' = n+0' = n+1$.

A következőkben az összeadás és a szorzás tulajdonságait vizsgáljuk.

3.7. Az összeadás asszociatív: $(k + m) + n = k + (m + n)$ tetszőleges $k, m, n \in \mathbf{N}_0$ esetén.

Bizonyítás. A bizonyítás n szerinti teljes indukcióval történik. Azt mutatjuk meg, hogy minden n természetes számra igaz a következő állítás: $(k+m)+n=k+(m+n)$ minden $k, m \in \mathbf{N}_0$ -ra. Az összeadás definícióját felhasználva $n = 0$ -ra az állítás azonnal adódik: $(k + m) + 0 = k + m = k + (m + 0)$. Tegyük fel, hogy n -re teljesül az állítás. Ekkor $(k + m) + n' = ((k + m) + n)' = (k + (m + n))' = k + (m + n)' = k + (m + n')$. Tehát n' -re is teljesül az állítás. ■

3.8. A 0 additív egységelem: $n + 0 = 0 + n = n$ minden $n \in \mathbf{N}_0$ esetén.

Bizonyítás. Az összeadás definíciója szerint $n + 0 = n$ minden n -re. Ezért csak a következő állítást kell igazolni: $0 + n = n$ minden n -re. $0 + 0 = 0$ az összeadás definíciója miatt. Ha $0 + n = n$, akkor $0 + n' = (0 + n)' = n'$. Tehát az állítást teljes indukcióval igazoltuk. ■

3.9. Az összeadás kommutatív: $m + n = n + m$ tetszőleges $m, n \in \mathbf{N}_0$ esetén.

Bizonyítás. A bizonyítás n szerinti teljes indukcióval történik. $n = 0$ -ra 3.8 miatt igaz. $n = 1$ -re is igazoljuk m szerinti teljes indukcióval az állítást: $m + 1 = 1 + m$ minden $m \in \mathbf{N}_0$ -re. Ez $m = 0$ -ra 3.8 miatt igaz. Ha $m + 1 = 1 + m$, akkor 3.7-et felhasználva azt kapjuk, hogy $m' + 1 = (m + 1) + 1 = (1 + m) + 1 = 1 + (m + 1) = 1 + m'$.

Végül tegyük fel, hogy $m + n = n + m$. Ekkor $m + n' = m + (n + 1) = (m + n) + 1 = (n + m) + 1 = n + (m + 1) = n + (1 + m) = (n + 1) + m = n' + m$. ■

3.10. Az összeadás egyszerűsítési művelet: $k + n = m + n$ -ből $m = k$ következik bármely $k, m, n \in \mathbf{N}_0$ esetén.

Bizonyítás. A bizonyítást n szerinti teljes indukcióval végezzük. $n = 0$ -ra az összeadás definíciója miatt igaz. Tegyük fel, hogy n -re teljesül az állítás. Ha $k + n' = m + n'$, akkor a definíció miatt $(k + n)' = (m + n)'$. Ebből a (P4) axióma és az indukciós feltevés szerint $k + n = m + n$ és $m = k$ következik. ■

3.11. A 0 multiplikatív zéruselem: $n \cdot 0 = 0 \cdot n = 0$ minden $n \in \mathbf{N}_0$ esetén.

Bizonyítás. A szorzás definíciója szerint $n \cdot 0 = 0$ minden n -re. Ezért csak a következő állítást kell igazolni: $0 \cdot n = 0$ minden n -re. $0 \cdot 0 = 0$ a szorzás definíciója miatt. Ha $0 \cdot n = 0$, akkor a definíciót és 3.8-at felhasználva azt kapjuk, hogy $0 \cdot n' = 0 \cdot n + 0 = 0 + 0 = 0$. ■

3.12. A szorzás jobbról disztributív az összeadásra nézve: $(k + m)n = kn + mn$ tetszőleges $k, m, n \in \mathbf{N}_0$ esetén.

Bizonyítás. n szerinti teljes indukcióval bizonyítunk. Az $n = 0$ esetre a műveletek definíciójából következik: $(k + m)0 = 0 = 0 + 0 = k0 + m0$. Ha az állítás n -re teljesül, akkor az összeadás asszociativitását és kommutativitását többször kihasználva kapjuk, hogy $(k + m)n' = (k + m)n + (k + m) = (kn + mn) + (k + m) = \dots = (kn + k) + (mn + m) = kn' + mn'$. ■

3.13. Az 1 multiplikatív egységelem: $1 \cdot n = n \cdot 1 = n$ tetszőleges $n \in \mathbf{N}_0$ esetén.

Bizonyítás. $n = 0$ -ra 3.11 miatt igaz az állítás. Ha $1 \cdot n = n \cdot 1 = n$, akkor $1 \cdot n' = 1 \cdot n + 1 = n + 1 = n'$ és $n' \cdot 1 = (n + 1) \cdot 1 = n \cdot 1 + 1 \cdot 1 = n + 1 \cdot 0' = n + (1 \cdot 0 + 1) = n + (0 + 1) = n + 1 = n'$ adódik a szorzás definíciója és 3.12 alapján. ■

3.14. A szorzás kommutatív művelet: $mn = nm$ minden $m, n \in \mathbf{N}_0$ esetén.

Bizonyítás. n szerinti teljes indukciót alkalmazunk. $n = 0$ -ra 3.11 miatt igaz az állítás. Tegyük fel, hogy n -re is igaz. Ekkor 3.12-t felhasználva adódik, hogy $mn' = mn + m = nm + 1 \cdot m = (n + 1)m = n'm$. ■

3.12 és 3.14 következményeként adódik

3.15. A szorzás disztributív az összeadásra nézve.

3.16. A szorzás asszociatív: $(km)n = k(mn)$ tetszőleges $k, m, n \in \mathbf{N}_0$ esetén.

Bizonyítás. n szerinti teljes indukciót alkalmazunk. $n = 0$ -ra a szorzás definíciója biztosítja az állítás helyességét: $(km)0 = 0 = k0 = k(m0)$. Ha n -re igaz, akkor $(km)n' = (km)n + km = k(mn) + km = k(mn + m) = k(mn')$. ■

3.17. Ha két természetes szám összege 0, akkor mindkettő egyenlő 0-val.

Bizonyítás. Kontrapozícióval bizonyítunk. Legyen $m, n \in \mathbf{N}_0$, és tegyük fel, hogy valamelyik nem 0. Az összeadás kommutativitása miatt feltehető, hogy $n \neq 0$. Ekkor 3.4 miatt van olyan k természetes szám, melyre $n = k'$, és így $m + n = m + k' = (m + k)'$. A (P3) axióma szerint $(m + k)' \neq 0$. ■

3.18. Ha két természetes szám szorzata 0, akkor legalább az egyik egyenlő 0-val.

Bizonyítás. Kontrapozícióval bizonyítunk. Legyen $m, n \in \mathbf{N}_0$, és tegyük fel, hogy egyik sem 0. Ekkor 3.4 miatt vannak olyan k és l természetes számok, melyekre $m = k'$, és $n = l'$. Így $mn = k'l' = (k+1)(l+1) = (kl+k+l) + 1 = (kl+k+l)'$, ami a (P3) axióma szerint nem lehet 0. ■

Eddigi eredményeinket a következőképpen foglalhatjuk össze:

3.19. Tétel. Az $(\mathbf{N}_0; +, \cdot, 0, 1)$ algebrai struktúra olyan kommutatív és egységelemes félgűrű, melyre 0 az összeadás, 1 pedig a szorzás egységeleme. Az összeadás egyszerűsítéses, 0 összegként csak úgy állhat elő, ha az összeg minden tagja 0, és az $\mathbf{N}_0 \setminus \{0\}$ halmaz zárt a szorzásra.

Most definiáljuk a természetes számok halmazának rendezését, és megadadjuk legfontosabb tulajdonságait is.

3.20. Definíció. Az m, n természetes számokra legyen

$$m \leq n \stackrel{\text{def}}{\iff} \exists k \in \mathbf{N}_0: m + k = n.$$

Ha $m \leq n$ és $m \neq n$, akkor erre a szokásos $m < n$ jelölést használjuk. Továbbá $m \leq n$, illetve $m < n$ helyett az $n \geq m$, illetve $n > m$ jelölést is használjuk.

3.21. Tétel. Az \mathbf{N}_0 halmazon a \leq reláció egy olyan rendezés, melyre nézve 0 a legkisebb elem.

Bizonyítás. Tetszőleges $m \in \mathbf{N}_0$ esetén $m + 0 = m$, ami éppen azt jelenti, hogy $m \leq m$. Tehát \leq reflexív reláció. Ha $m \leq n$ és $n \leq m$, akkor a definíció szerint vannak olyan k, l természetes számok, hogy $m + k = n$ és $n + l = m$. Behelyettesítve n -et a második egyenlőségbe azt kapjuk, hogy $m + (k + l) = m + 0$, amiből $k + l = 0$ következik, hiszen az összeadás egyszerűsítéses. Ebből pedig 3.17 miatt $k = l = 0$ és $m = n$ adódik. Tehát \leq antiszimmetrikus. Ha valamely m, n, s természetes számokra $m \leq n$ és $n \leq s$, akkor vannak olyan k, l természetes számok, melyekre $m + k = n$ és $n + l = s$, amiből $s = n + l = (m + k) + l = m + (k + l)$ és $m \leq s$ adódik. Tehát \leq tranzitív is, és így részbenrendezés. 0 a legkisebb elem, hiszen tetszőleges $m \in \mathbf{N}_0$ esetén $m = 0 + m$ és $0 \leq m$.

Most már csak azt kell igazolni, hogy bármely két természetes szám összehasonlítható. Legyen m tetszőleges természetes szám, és legyen

$$U = \{n \in \mathbf{N}_0: m \leq n \text{ vagy } n \leq m\}.$$

Azt kell belátni, hogy $U = \mathbf{N}_0$. $0 \in U$ hiszen 0 a legkisebb elem. Tegyük fel, hogy $n \in U$, azaz $m \leq n$ vagy $n < m$. Az első esetben van olyan k , hogy $n = m + k$. Ekkor $n' = n + 1 = (m + k) + 1 = m + (k + 1)$, azaz $m \leq n'$, és ezért $n' \in U$. A második esetben van olyan $l \neq 0$, melyre $m = n + l$. Mivel $l \neq 0$, ezért 3.4 szerint van olyan t , melyre $l = t' = t + 1$. Így $m = n + l = n + (t + 1) = (n + 1) + t = n' + t$, amiből $n' \leq m$ és $n' \in U$ adódik. Így a (P5) axióma szerint $U = \mathbf{N}_0$. ■

A következő tétel a \leq reláció és a műveletek kapcsolatára vonatkozó legfontosabb tudnivalókat foglalja össze.

3.22. Tétel. Tetszőleges $m, n, k, l \in \mathbf{N}_0$ esetén teljesülnek a következők:

- Az összeadás monoton művelet: ha az $m \leq n$ és $k \leq l$, akkor $m + k \leq n + l$. Ha továbbá $m < n$ vagy $k < l$ akkor $m + k < n + l$.
- A szorzás monoton művelet: ha $m \leq n$ és $k \leq l$, akkor $mk \leq nl$. Ha továbbá $m < n$ és $l \neq 0$, vagy $k < l$ és $n \neq 0$, akkor $mk < nl$.
- Ha $m + k \leq n + k$, akkor $m \leq n$. Ha $m + k < n + k$, akkor $m < n$.
- Ha $mk \leq nk$ és $k \neq 0$, akkor $m \leq n$, Ha $mk < nk$ és $k \neq 0$, akkor $m < n$.

Bizonyítás. Legyen $m, n, k, l \in \mathbf{N}_0$. Először tegyük fel, hogy $m \leq n$ és $k \leq l$. Ekkor van olyan s, t , hogy $n = m + s$ és $l = k + t$, és ezért

$$n + k = (m + k) + s, \quad n + l = (n + k) + t \quad \text{és} \quad nk = mk + sk, \quad nl = nk + nt.$$

Tehát

$$m + k \leq n + k, \quad n + k \leq n + l \quad \text{és} \quad mk \leq nk, \quad nk \leq nl,$$

amiből \leq tranzitivitása miatt $m + k \leq n + l$ és $mk \leq nl$ következik.

Ha $m < n$ vagy $k < l$, akkor $s \neq 0$ vagy $t \neq 0$. Ezért 3.17 miatt $s+t \neq 0$ és $n+l = (m+k)+(s+t) \neq m+k$. Tehát $m + k < n + l$, amivel (a) igazolását befejeztük.

A szorzás kommutativitása miatt (b) második állítását elég az $m < n$ és $l \neq 0$ esetben igazolni. Ekkor $n \neq 0$ és $s \neq 0$. Ezért $sk + nt \neq 0$, mert ellenkező esetben 3.17 és 3.18 miatt $sk = nt = 0$, $k = t = 0$ és $l = k+t = 0$, ami ellentmond feltevésünknek. Így $nl = n(k+t) = nk + nt = (m+s)k + nt = mk + (sk + nt) \neq mk$ és $mk < nl$.

Most (c) igazolása céljából tegyük fel, hogy $m + k \leq n + k$. Ekkor valamely s -re $n + k = (m + k) + s = (m + s) + k$, amiből 3.10 szerint $n = m + s$ és $m \leq n$ következik. Ha $m + k < n + k$, akkor $s \neq 0$ és $m < n$.

Végül (d) igazoláshoz tegyük fel, hogy $mk \leq nk$ és $k \neq 0$. Ha az állítás nem teljesül, azaz $n < m$, akkor (b) szerint $nk < mk$, ami ellentmond a feltevésnek. Ha $mk < nk$, akkor $mk \leq nk$. Így az előzőek szerint $m \leq n$. Mivel $mk \neq nk$, ezért $m \neq n$ és $m < n$. ■

3.23. Következmény. A szorzásnál 0-tól különböző tényezővel lehet egyszerűsíteni: ha $mk = nk$ és $k \neq 0$, akkor $m = n$.

Bizonyítás. Ha $mk = nk$ és $k \neq 0$, akkor $mk \leq nk$, $nk \leq mk$, és ezért 3.22(d) szerint $m \leq n$ és $n \leq m$, amiből $m = n$ következik. ■

3.24. Definíció. Legyen $(R; +, \cdot)$ félgűrű és ρ részbenrendezés R -en. Azt mondjuk, hogy $(R; +, \cdot)$ részbenrendezett félgűrű ρ -ra nézve, ha bármely $a, b, c \in R$ esetén, ha $a \rho b$, akkor $a + c \rho b + c$, $ac \rho bc$ és $ca \rho cb$. Ha ráadásul ρ rendezés, akkor R -et rendezett vagy lineárisan rendezett félgűrűnek nevezzük.

3.25. Tétel. A természetes számok félgűrűje rendezett a \leq relációra nézve. A természetes számok félgűrűjének két rendezése van: a \leq és a \geq rendezés.

Bizonyítás. Az első állítás lényegében összeloglalja néhány korábbi állításunkat. Legyen \preceq a természetes számok félgűrűjének egy rendezése. Vegyük észre, hogy ekkor a természetes számok félgűrűjének \succeq rendezése.

Legyen először $0 \preceq 1$. Megmutatjuk, hogy $\leq \subseteq \preceq$, amiből $\leq = \preceq$ következik, mert mindkét reláció rendezés. Valóban, ha $\leq \subseteq \preceq$, és van olyan $a, b \in \mathbf{N}_0$, hogy $a \preceq b$ és $a \not\leq b$, akkor $b \leq a$, $b \preceq a$ és $a = b$, ami $a \not\leq b$ miatt nem teljesülhet.

Az $\leq \subseteq \preceq$ tartalmazás igazolásához elegendő azt megmutatni, hogy tetszőleges $m \in \mathbf{N}_0$ -ra az $U_m = \{x \in \mathbf{N}_0 : m \preceq m + x\}$ halmaz megegyezik \mathbf{N}_0 -lal. Világos, hogy $0 \in U_m$. Ha $n \in U_m$, akkor $m \preceq n$ és $m = m + 0 \preceq n + 1 = n'$ és $n' \in U_m$. Ezért (P5) szerint $U_m = \mathbf{N}_0$. Végül ha $1 \preceq 0$, akkor a fentiek szerint $\succeq = \leq$. ■

4. Egész számok

Az egész számok gyűrűjének konstrukciója arra a tényre épül, hogy minden egész szám két természetes szám különbsége.

4.1. Definíció. Az \mathbf{N}_0^2 halmazon értelmezzük az összeadás és a szorzás műveleteket, valamint egy kétváltozós ρ relációt a következőképpen: Tetszőleges $(a, b), (c, d) \in \mathbf{N}_0^2$ esetén legyen

$$(a, b) + (c, d) \stackrel{\text{def}}{=} (a + c, b + d),$$

$$(a, b) \cdot (c, d) \stackrel{\text{def}}{=} (ac + bd, ad + bc)$$

és

$$(a, b) \rho (c, d) \stackrel{\text{def}}{\Leftrightarrow} a + d = b + c.$$

4.2. Tétel.

- (1) Az $(\mathbf{N}_0^2; +, \cdot)$ algebrai struktúra kommutatív és egységelemes félgűrű, melynek ρ kongruenciarelációja.
- (2) Az $(\mathbf{N}_0^2/\rho; +, \cdot)$ faktorstruktúra olyan integritástartomány, melyre az $\mathbf{N}_0 \rightarrow \mathbf{N}_0^2/\rho; n \mapsto \overline{(n, 0)}$ leképezés az $(\mathbf{N}_0; +, \cdot)$ félgűrűnek $(\mathbf{N}_0^2/\rho; +, \cdot)$ -ba való beágyazása.
- (3) $\mathbf{N}_0^2/\rho = \{-\overline{(n, 0)} : n \in \mathbf{N}\} \cup \{\overline{(0, 0)}\} \cup \{\overline{(n, 0)} : n \in \mathbf{N}\}$, és az egyesítésben szereplő három halmaz páronként diszjunkt.

Bizonyítás. Egyszerű számolással ellenőrizhető, hogy \mathbf{N}_0^2 -en az összeadás és a szorzás kommutatív és asszociatív, a szorzás disztributív az összeadásra nézve, a $(0, 0)$ additív, az $(1, 0)$ pedig multiplikatív egységelem. Például a szorzás asszociativitását és az összeadásra vonatkozó disztributivitását a következőképpen igazolhatjuk: Tetszőleges $(a, b), (c, d), (e, f) \in \mathbf{N}_0^2$ esetén

$$\begin{aligned} ((a, b) \cdot (c, d)) \cdot (e, f) &= (ac + bd, ad + bc) \cdot (e, f) = \\ &= ((ac + bd)e + (ad + bc)f, (ac + bd)f + (ad + bc)e) = \\ &= (a(ce + df) + b(cf + de), a(cf + de) + b(ce + df)) = \\ &= (a, b) \cdot (ce + df, cf + de) = (a, b) \cdot ((c, d) \cdot (e, f)) \end{aligned}$$

és

$$\begin{aligned} ((a, b) + (c, d)) \cdot (e, f) &= (a + c, b + d) \cdot (e, f) = \\ &= ((a + c)e + (b + d)f, (a + c)f + (b + d)e) = (ae + ce + bf + df, af + cf + be + de) = \\ &= (ae + bf, af + be) + (ce + df, cf + de) = (a, b) \cdot (e, f) + (c, d) \cdot (e, f). \end{aligned}$$

Tehát $(\mathbf{N}_0^2; +, \cdot)$ kommutatív és egységelemes félgűrű.

Most megvizsgáljuk a ρ reláció tulajdonságait. A definícióból közvetlenül adódik, hogy ρ reflexív és szimmetrikus. Ha $(a, b) \rho (c, d)$ és $(c, d) \rho (e, f)$, akkor $a + d = b + c$ és $c + f = d + e$, amiből $a + d + c + f = b + c + d + e$, $a + f = b + e$ és $(a, b) \rho (e, f)$ következik. Tehát ρ tranzitív is, és ezért ekvivalenciareláció.

Ahhoz, hogy ρ kongruenciareláció legyen, már csak azt kell igazolni, hogy ha $(a, b) \rho (c, d)$ és $(e, f) \in \mathbf{N}_0^2$, akkor

$$(a, b) + (e, f) = (a + e, b + f) \rho (c + e, d + f) = (c, d) + (e, f)$$

és

$$(a, b) \cdot (e, f) = (ae + bf, af + be) \rho (ce + df, cf + de) = (c, d) \cdot (e, f).$$

$(a + e, b + f) \rho (c + e, d + f)$ ekvivalens azzal, hogy $a + e + d + f = b + f + c + e$, ami igaz, ha $(a, b) \rho (c, d)$, azaz $a + d = b + c$. $(ae + bf, af + be) \rho (ce + df, cf + de)$ ekvivalens azzal, hogy $ae + bf + cf + de = af + be + ce + df$. Ez igaz, ha $a + d = b + c$, hiszen

$$ae + bf + cf + de = (a + d)e + (b + c)f = (b + c)e + (a + d)f = be + ce + af + df.$$

Tehát ρ kongruenciareláció.

Mivel az $\mathbf{N}_0^2 \rightarrow \mathbf{N}_0^2/\rho$, $(a, b) \mapsto \overline{(a, b)}$ leképezés homomorfizmus, az $(\mathbf{N}_0^2/\rho; +, \cdot)$ faktorstruktúra is kommutatív és egységelemes félgűrű, melynek $(0, 0)$ az additív, $(1, 0)$ pedig a multiplikatív egységeleme. Vegyük észre, hogy $\overline{(x, y)} = \overline{(0, 0)}$ ekvivalens azzal, hogy $x = y$. Ezért $\overline{(b, a)}$ az $\overline{(a, b)}$ elem additív inverze, hiszen

$$\overline{(a, b)} + \overline{(b, a)} = \overline{(a + b, b + a)} = \overline{(0, 0)}.$$

Tehát $(\mathbf{N}_0^2/\rho; +, \cdot)$ gyűrű.

Tegyük fel, hogy $\overline{(a, b)} \cdot \overline{(c, d)} = \overline{(ac + bd, ad + bc)} = \overline{(0, 0)}$, azaz $ac + bd = ad + bc$. Ha valamelyik tényező, mondjuk $\overline{(a, b)} \neq \overline{(0, 0)}$, akkor $a \neq b$, és mivel $a < b$ vagy $b < a$, van olyan $k \neq 0$ természetes szám, melyre $b = a + k$ vagy $a = b + k$. Az első esetben

$$ac + ad + kd = ac + (a + k)d = ac + bd = ad + bc = ad + (a + k)c = ad + ac + kc,$$

a második esetben pedig

$$bc + kc + bd = (b + k)c + bd = ac + bd = ad + bc = (b + k)d + bc = bd + kd + bc.$$

Ebből mindkét esetben $kd = kc$, $c = d$ és $\overline{(c, d)} = \overline{(0, 0)}$ következik. Tehát $(\mathbf{N}_0^2/\rho; +, \cdot)$ zérusosztómentes is, és így integritástartomány.

Most tekintsük a

$$\varphi: \mathbf{N}_0 \rightarrow \mathbf{N}_0^2/\rho, \quad a \mapsto \overline{(a, 0)}$$

leképezést. Ha $a\varphi = b\varphi$, akkor $\overline{(a, 0)} = \overline{(b, 0)}$, azaz $(a, 0) \rho (b, 0)$, amiből $a = b$ következik. Tehát φ injektív. φ felcserélhető a műveletekkel, ugyanis tetszőleges $a, b \in \mathbf{N}_0$ esetén

$$(a + b)\varphi = \overline{(a + b, 0)} = \overline{(a, 0)} + \overline{(b, 0)} = a\varphi + b\varphi$$

és

$$(ab)\varphi = \overline{(ab, 0)} = \overline{(a, 0)} \cdot \overline{(b, 0)} = \overline{(a, 0)} \cdot \overline{(b, 0)} = a\varphi \cdot b\varphi.$$

Tehát φ beágyazás.

Az utolsó állítás igazolása céljából tekintsünk egy $\overline{(a, b)} \in \mathbf{N}_0^2/\rho$ elemet. Mivel $a, b \in \mathbf{N}_0$, ezért $a < b$, $a = b$ és $b < a$ közül valamelyik teljesül. Ha $a = b$, akkor $\overline{(a, b)} = \overline{(0, 0)}$. Ha $a < b$, akkor van olyan $n \in \mathbf{N}_0$, $n \neq 0$, melyre $b = a + n$. Ezért

$$\overline{(a, b)} = \overline{(a, a + n)} = \overline{(0, n)} = -\overline{(n, 0)}.$$

Ha pedig $b < a$, akkor van olyan $n \in \mathbf{N}_0$, $n \neq 0$, melyre $a = b + n$. Így

$$\overline{(a, b)} = \overline{(b + n, b)} = \overline{(n, 0)}.$$

A $\overline{(0, 0)}$ elem a rá vonatkozó észrevételünk miatt nem eleme az egyesítésben szereplő első és harmadik halmaznak. Ha az első és harmadik halmaz nem volna diszjunkt, akkor valamely $m, n \in \mathbf{N}$ elemekre

$$\overline{(m, 0)} = -\overline{(n, 0)} = \overline{(0, n)}$$

teljesülne, amiből $m + n = 0 + 0 = 0$ következne. Ez pedig lehetetlen. ■

4.3. Definíció. Jelöljük az \mathbf{N}_0^2/ρ halmazt \mathbf{Z} -vel, és az $\overline{(n, 0)}$, $n \in \mathbf{N}_0$, alakú elemeket pedig egyszerűen n -nel. \mathbf{Z} elemeit egész számoknak nevezzük. Értelmezzünk a \leq relációt \mathbf{Z} -n a következőképpen:

$$a \leq b \stackrel{\text{def}}{\iff} b - a \in \mathbf{N}_0$$

4.4. Tétel. A $(\mathbf{Z}; +, \cdot)$ olyan integritástartomány, melynek $(\mathbf{N}_0; +, \cdot)$ részfélgűrűje, és minden eleme $a - b$, $a, b \in \mathbf{N}_0$, alakú. Továbbá $(\mathbf{Z}; +, \cdot)$ lineárisan rendezett gyűrű a \leq relációra nézve az \mathbf{N}_0 pozitívítási tartománnyal, és a \leq reláció \mathbf{N}_0 -ra való megszorítása megegyezik \mathbf{N}_0 előző fejezetben bevezetett rendezésével.

Bizonyítás. Ha $\overline{(a, b)} \in \mathbf{Z}$, $a, b \in \mathbf{N}_0$, akkor

$$\overline{(a, b)} = \overline{(a, 0)} + \overline{(0, b)} = \overline{(a, 0)} - \overline{(b, 0)} = a - b.$$

Ebből és 4.2(2)-ből már következik az első állítás. $\mathbf{N}_0 \subseteq \mathbf{Z}$ tartalmazza a 0-t, zárt az összeadásra és a szorzásra. Továbbá a 4.2(3) állítás szerint, ha $a, -a \in \mathbf{N}_0$, akkor $a = 0$, és bármely $a \in \mathbf{Z}$ esetén $a \in \mathbf{N}_0$ vagy $-a \in \mathbf{N}_0$. Ezért a 2.7 és 2.8. Tétel szerint $(\mathbf{Z}; +, \cdot)$ lineárisan rendezett gyűrű \leq -re nézve. A \leq reláció megszorítására vonatkozó állítás közvetlenül adódik a definíciókból. ■

Most már definiálhatjuk egész számok abszolút értékét:

$$|x| = \begin{cases} x, & \text{ha } x \geq 0; \\ -x, & \text{különben.} \end{cases}$$

A 2.11. Tétel speciális eseteként kapjuk a következőt:

4.5. Tetszőleges $a, b \in \mathbf{Z}$ esetén $-|a| \leq a \leq |a|$, $|a| = |-a|$ és $|ab| = |a| \cdot |b|$ és $|a + b| \leq |a| + |b|$.

4.6. Tétel. Az egész számok gyűrűjének a most bevezetett \leq részbenrendezés az egyetlen lineáris rendezése.

Bizonyítás. Legyen P a pozitív tartománya az egész számok gyűrűje valamely lineáris rendezésének. A 2.10. Tétel szerint elegendő azt megmutatni, hogy $P = \mathbf{N}_0$. $0 \in P$ nyilvánvaló. $1 \in P$ is teljesül, mert a feltevés szerint $1 \in P$ vagy $-1 \in P$, és a második eset nem teljesülhet, mert P szorzásra való zártsága miatt $1 = (-1)(-1) \in P$. Abból, hogy $1 \in P$, és P zárt az összeadásra, azonnal adódik, hogy $\mathbf{N}_0 \subseteq P$. P negatív számokat nem tartalmazhat, mert akkor lenne olyan 0-tól különböző szám, mely az additív inverzával együtt P -ben van, ami P egyik tulajdonsága szerint lehetetlen. Tehát $P = \mathbf{N}_0$. ■

5. Racionális számok

A racionális számok testének alábbi konstrukciója arra a tényre épül, hogy minden racionális szám két egész szám hányadosa.

5.1. Definíció. Legyen $S = \{(a, b) : a, b \in \mathbf{Z}, b \neq 0\}$, és értelmezzük az összeadást, a szorzást, valamint egy kétváltozós ρ relációt az S halmazon a következőképpen: Tetszőleges $(a, b), (c, d) \in S$ esetén legyen

$$(a, b) + (c, d) \stackrel{\text{def}}{=} (ad + bc, bd),$$

$$(a, b) \cdot (c, d) \stackrel{\text{def}}{=} (ac, bd)$$

és

$$(a, b) \rho (c, d) \stackrel{\text{def}}{\Leftrightarrow} ad = bc.$$

5.2. Tétel. A fent definiált $(S; +, \cdot)$ algebrai struktúrára és ρ relációra érvényesek a következők:

- (1) A $+$, illetve a \cdot művelet kommutatív, asszociatív és egységelemes a $(0, 1)$, illetve az $(1, 1)$ egységelemekkel.
- (2) ρ kongruenciareláció.
- (3) Az $(S/\rho; +, \cdot)$ faktorstruktúra olyan test, melyre a $\mathbf{Z} \rightarrow S/\rho, n \mapsto \overline{(n, 1)}$ leképezés az egész számok gyűrűjének beágyazása $(S/\rho, +, \cdot)$ -ba.
- (4) $S/\rho = \{\overline{-(m, n)} : m, n \in \mathbf{N}\} \cup \{\overline{(0, 1)}\} \cup \{\overline{(m, n)} : m, n \in \mathbf{N}\}$ és az egyesítésben szereplő három halmaz páronként diszjunkt.

Bizonyítás. Az (1) állítás a műveletek definícióját felhasználva egyszerű számolással adódik. Ezért csak az összeadás asszociativitását részletezzük. Tetszőleges $(a, b), (c, d), (e, f) \in S$ esetén

$$\begin{aligned} ((a, b) + (c, d)) + (e, f) &= (ad + bc, bd) + (e, f) = ((ad + bc)f + (bd)e, (bd)f) = \\ &= (a(df) + b(cf + de), b(df)) = (a, b) + (cf + de, df) = (a, b) + ((c, d) + (e, f)). \end{aligned}$$

Most megvizsgáljuk a ρ reláció tulajdonságait. Az nyilvánvaló, hogy ρ reflexív és szimmetrikus. Ha $(a, b) \rho (c, d)$ és $(c, d) \rho (e, f)$, akkor $ad = bc$ és $cf = de$, amiből szorzással $adc f = bcde$, és egyszerűsítéssel $acf = bce$ következik. Ha $c \neq 0$, akkor további egyszerűsítéssel $af = be$ adódik, azaz $(a, b) \rho (e, f)$. Ha

$c = 0$, akkor $ad = bc = 0$ és $de = cf = 0$, amiből $d, f \neq 0$ miatt $a = e = 0$ következik. Ezért $af = 0 = be$, és így $(a, b) \rho (e, f)$. Tehát ρ tranzitív is, és ezért ekvivalenciareláció.

Ahhoz, hogy ρ kongruenciareláció legyen, már csak azt kell igazolni, hogy ha $(a, b) \rho (c, d)$ és $(e, f) \in S$, akkor

$$(a, b) + (e, f) = (af + be, bf) \rho (cf + de, df) = (c, d) + (e, f)$$

és

$$(a, b) \cdot (e, f) = (ae, bf) \rho (ce, df) = (c, d) \cdot (e, f).$$

Tegyük fel, hogy $(a, b) \rho (c, d)$, azaz $ad = bc$. Ekkor egyrészt $(af + be)df = adf^2 + bdef = bcf^2 + bdef = bf(cf + de)$, vagyis $(af + be, bf) \rho (cf + de, df)$, másrészt $(ae)(df) = adef = bcef = (bf)(ce)$, vagyis $(a, b) \cdot (e, f) = (ae, bf) \rho (ce, df) = (c, d) \cdot (e, f)$. Tehát ρ valóban kongruenciareláció.

Mivel az $S \rightarrow S/\rho$, $(a, b) \mapsto \overline{(a, b)}$ leképezés homomorfizmus, (1) miatt az $(S/\rho; +, \cdot)$ faktorstruktúra mindkét művelete kommutatív és asszociatív. Továbbá $\overline{(0, 1)}$ az additív, $\overline{(1, 1)}$ pedig a multiplikatív egységelem. Vegyük észre, hogy tetszőleges $(x, y) \in S$ esetén $\overline{(x, y)} = \overline{(0, 1)}$, illetve $\overline{(x, y)} = \overline{(1, 1)}$ ekvivalens azzal, hogy $(x, y) \rho (0, 1)$, azaz $x = 0$, illetve $(x, y) \rho (1, 1)$, azaz $x = y$. Ezért $\overline{(-a, b)}$ az $\overline{(a, b)}$ elem additív inverze, hiszen

$$\overline{(a, b)} + \overline{(-a, b)} = \overline{(ab + b(-a), b^2)} = \overline{(0, b^2)} = \overline{(0, 1)}.$$

Továbbá, ha $\overline{(a, b)} \neq \overline{(0, 1)}$, azaz $a \neq 0$, akkor $\overline{(b, a)}$ az $\overline{(a, b)}$ elem multiplikatív inverze, mert

$$\overline{(a, b)} \cdot \overline{(b, a)} = \overline{(ab, ba)} = \overline{(1, 1)}.$$

Legyen $\overline{(a, b)}, \overline{(c, d)}, \overline{(e, f)} \in S/\rho$. Ekkor

$$\begin{aligned} \overline{((a, b) + (c, d))} \cdot \overline{(e, f)} &= \overline{(ad + bc, bd)} \cdot \overline{(e, f)} = \overline{((ade + bce, bdf))} = \\ &= \overline{(adef + bcef, bdf^2)} = \overline{(ae, bf)} + \overline{(ce, df)} = \overline{(a, b)} \cdot \overline{(e, f)} + \overline{(c, d)} \cdot \overline{(e, f)}, \end{aligned}$$

mert a harmadik egyenlőség ekvivalens az igaz

$$(ade + bce)bdf^2 = bdf(adef + bcef)$$

egyenlőséggel, a többi egyenlőség pedig a műveletek definíciója miatt teljesül. Tehát a szorzás disztributív az összeadásra nézve, és ezért $(S/\rho; +, \cdot)$ test.

Most tekintsük a

$$\varphi: \mathbf{Z} \rightarrow S/\rho, a \mapsto \overline{(a, 1)}$$

leképezést. Ha $a\varphi = b\varphi$, akkor $\overline{(a, 1)} = \overline{(b, 1)}$, vagyis $(a, 1) \rho (b, 1)$, amiből $a = b$ következik. Tehát φ injektív. φ felcserélhető a műveletekkel, ugyanis tetszőleges $a, b \in S$ esetén

$$(a + b)\varphi = \overline{(a + b, 1)} = \overline{(a \cdot 1 + 1 \cdot b, 1 \cdot 1)} = \overline{(a, 1)} + \overline{(b, 1)} = a\varphi + b\varphi$$

és

$$(ab)\varphi = \overline{(ab, 1)} = \overline{(a, 1)} \cdot \overline{(b, 1)} = a\varphi \cdot b\varphi.$$

Tehát φ beágyazás.

A (4) állítás igazolása céljából tekintsünk egy $\overline{(a, b)} \in S/\rho$ elemet. Feltehető, hogy $b > 0$, mert $\overline{(a, b)} = \overline{(-a, -b)}$, és ezért $b < 0$ esetén $\overline{(a, b)}$ -t helyettesíthetjük $\overline{(-a, -b)}$ -vel. Már említettük, hogy $\overline{(a, b)} = \overline{(0, 1)}$ pontosan akkor, ha $a = 0$. Tegyük fel, hogy $a \neq 0$. Ekkor az a egész számra az $-a \in \mathbf{N}$ és $a \in \mathbf{N}$ állítások közül pontosan az egyik teljesül. Ha $-a \in \mathbf{N}$, akkor $\overline{(a, b)} = -\overline{(-a, b)} \in \{-\overline{(m, n)}: m, n \in \mathbf{N}\}$. Ha $a \in \mathbf{N}$, akkor $\overline{(a, b)} \in \{\overline{(m, n)}: m, n \in \mathbf{N}\}$. Ahhoz, hogy a (4) állításban szereplő halmazok páromként diszjunktak már csak azt kell észrevenni, hogy $\overline{(x, y)} = \overline{(u, v)}$ nem teljesülhet $x, y, -u, v \in \mathbf{N}$ esetén, hiszen az egyenlőségből $xv = yu$ következik. ■

5.3. Definíció. Jelöljük az S/ρ halmazt \mathbf{Q} -val, és az $\overline{(n,1)}$, $n \in \mathbf{Z}$, alakú elemeket pedig egyszerűen n -nel. \mathbf{Q} elemeit *racionális számoknak* nevezzük. Ha $a, b \in \mathbf{Q}$ és $b \neq 0$, akkor ab^{-1} helyett $\frac{a}{b}$ -t vagy a/b -t is írunk. Legyen továbbá $\mathbf{Q}^+ = \{\overline{(m,n)}: m, n \in \mathbf{N}\}$ és $\mathbf{Q}^- = \{-\overline{(m,n)}: m, n \in \mathbf{N}\}$. \mathbf{Q}^+ elemeit *pozitív racionális számoknak*, \mathbf{Q}^- elemeit pedig *negatív racionális számoknak* hívjuk. Értelmezzünk a \leq relációt \mathbf{Q} -n a következőképpen:

$$a \leq b \stackrel{\text{def}}{\Leftrightarrow} b - a \in \mathbf{Q}^+ \cup \{0\}.$$

5.4. Tétel. A $(\mathbf{Q}; +, \cdot)$ algebrai struktúra olyan test, melynek $(\mathbf{Z}; +, \cdot)$ részgyűrűje, és minden eleme $\frac{a}{b}$ ($a, b \in \mathbf{Z}$, $b \neq 0$) alakú. Továbbá $(\mathbf{Q}; +, \cdot)$ rendezett test a \leq relációra nézve, és a \leq reláció \mathbf{Z} -re való megszorítása megegyezik \mathbf{Z} előző fejezetben bevezetett rendezésével.

Bizonyítás. Az első állítás az 5.2(3) állításból és az alábbi észrevételből következik:

$$\overline{(a,b)} = \overline{(a,1)} \cdot \overline{(1,b)} = \overline{(a,1)} \cdot \left(\overline{(b,1)}\right)^{-1} = \frac{a}{b}.$$

$\mathbf{Q}^+ \cup \{0\}$ tartalmazza a 0-t, zárt az összeadásra és a szorzásra. Továbbá az 5.2(4) állítás szerint ha $r, -r \in \mathbf{Q}^+ \cup \{0\}$, akkor $r = 0$, és bármely $r \in \mathbf{Q}$ esetén $r \in \mathbf{Q}^+ \cup \{0\}$ vagy $-r \in \mathbf{Q}^+ \cup \{0\}$. Ezért második állításunk a 2.7, 2.8 és 2.9 tételekből következik.

Az egész számokéhoz hasonlóan definiáljuk a racionális számok abszolút értékét:

$$|x| = \begin{cases} x, & \text{ha } x \geq 0; \\ -x, & \text{különben.} \end{cases}$$

A 2.11. Tétel speciális eseteként adódik a következő:

5.5. Állítás. Tetszőleges $a, b \in \mathbf{Q}$ esetén $-|a| \leq a \leq |a|$, $|a| = |-a|$, $|ab| = |a| \cdot |b|$ és $|a+b| \leq |a| + |b|$.

5.6. Állítás. A racionális számhalmaz rendezése sűrű: tetszőleges $a, b \in \mathbf{Q}$ esetén, ha $a < b$, akkor van olyan $x \in \mathbf{Q}$, hogy $a < x < b$. Bármely $a \in \mathbf{Q}$ számhoz van egyetlen olyan n egész szám, hogy $n \leq a < n+1$.

Bizonyítás. Legyen $a, b \in \mathbf{Q}$, $a < b$. Mivel $b - a > 0$, ezért van olyan $m, n \in \mathbf{N}$, hogy $b - a = \frac{m}{n}$. Ekkor $0 < \frac{m}{2n} < \frac{m}{n} = b - a$, amiből $a < \frac{m}{2n} + a < b$ következik.

A második állítás igazolásához legyen $a = \frac{p}{q} \in \mathbf{Q}$, ahol $q \in \mathbf{N}$ és $p \in \mathbf{Z}$. Mivel $-|p|q \leq p \leq |p|q$, ezért $-|p| \leq a = \frac{p}{q} \leq |p|$. Tehát az $a \in \mathbf{Q}$ elem két egész szám között van, és így létezik egy legnagyobb a -nál nem nagyobb n egész szám, amire nyilván teljesül $n \leq a < n+1$.

Az egyértelműség igazolásához tegyük fel, hogy m és n olyan egész számok, hogy $m \leq a < m+1$ és $n \leq a < n+1$. Ekkor $m \leq a < n+1$ és $n \leq a < m+1$, amiből $m \leq n$, $n \leq m$ és $m = n$ következik. ■

5.7. Definíció. Legyen a egy racionális szám. Az a szám $[a]$ egész része az 5.6 Állításban szereplő n szám, törtrésze pedig $\{a\} = a - [a]$.

5.8. Következmény. Tetszőleges $a \in \mathbf{Q}$ számra $[a] \leq a < [a] + 1$ és $0 \leq \{a\} < 1$.

5.9. Tétel. A racionális számok testének a most bevezetett \leq rendezés az egyetlen rendezése.

Bizonyítás. Legyen P a pozitivitási tartománya a racionális számok teste valamely lineáris rendezésének. A 2.10. Tétel szerint elegendő azt megmutatni, hogy $P = \mathbf{Q}^+ \cup \{0\}$. $0 \in P$ nyilvánvaló. $1 \in P$ is teljesül, mert a feltevés szerint $1 \in P$ vagy $-1 \in P$, és a második eset nem teljesülhet, mert P szorzásra való zártsága

miatt abból $1 = (-1)(-1) \in P$ következik. Abból, hogy $0, 1 \in P$, és P zárt az összeadásra, azonnal adódik, hogy $\mathbf{N}_0 \subseteq P$. Ha a pozitív racionális szám, akkor van olyan $m, n \in \mathbf{N}$, hogy $a = \frac{m}{n}$. Ekkor $a \in P$, mert ellenkező esetben $-a = \frac{-m}{n} \in P$, amiből P szorzásra való zártsága miatt $-m = n \frac{-m}{n} \in P$ következik. Ez pedig lehetetlen, mert $m \in P$. P negatív számokat nem tartalmazhat, mert akkor lenne olyan 0-tól különböző szám, mely az additív inverzével együtt P -ben van, ami P már felhasznált egyik tulajdonsága szerint lehetetlen. Tehát $P = \mathbf{Q}^+ \cup \{0\}$. ■

6. Valós számok Cantor-féle konstrukciója

A valós számok testének Cantor-féle konstrukciója arra a szemléletes tényre épül, hogy a számegyenes bármely pontjának akármilyen kis környezetében van racionális koordinátájú pont. Következésképpen minden valós szám racionális számsorozat határértéke.

6.1. Definíció. Tekintsük a végtelen racionális számsorozatok $\mathbf{Q}^{\mathbf{N}}$ halmazát, melynek elemeit (r_i) -vel jelöljük, ahol r_i a sorozat i -edik tagját jelöli, $i \in \mathbf{N}$. Ha $r \in \mathbf{Q}$, akkor (r) azt a sorozatot jelöli, melynek minden tagja r . Egy $(r_i) \in \mathbf{Q}^{\mathbf{N}}$ sorozatot *alapsorozatnak* vagy *Cauchy-sorozatnak* nevezünk, ha teljesíti a Cauchy-féle belső konvergencia-kritériumot: Bármely $\varepsilon \in \mathbf{Q}^+$ számhoz van olyan $n_0 \in \mathbf{N}$ küszöbszám, melyre $|r_m - r_n| < \varepsilon$ valahányszor $m, n \geq n_0$. Egy $(r_i) \in \mathbf{Q}^{\mathbf{N}}$ sorozatot *nullsorozatnak* nevezzük, ha bármely $\varepsilon \in \mathbf{Q}^+$ számhoz van olyan $n_0 \in \mathbf{N}$ küszöbszám, melyre $|r_n| < \varepsilon$ valahányszor $n \geq n_0$. Jelölje R az alapsorozatok, I pedig a nullsorozatok halmazát. Értelmezzük az összeadás és a szorzás műveleteket az R halmazon a következőképpen: Teszőleges $(q_i), (r_i) \in R$ esetén legyen

$$(q_i) + (r_i) \stackrel{\text{def}}{=} (q_i + r_i),$$

és

$$(q_i) \cdot (r_i) \stackrel{\text{def}}{=} (q_i r_i)$$

Vegyük észre, hogy az összeadás és a szorzás a számsorozatok szokásos tagonkénti összeadása és szorzása.

6.2. Állítás. Minden nullsorozat alapsorozat, azaz $I \subseteq R$. Az alapsorozatok korlátosak: ha $(r_i) \in R$, akkor van olyan $K \in \mathbf{Q}^+$, hogy $|r_i| < K$ minden $i \in \mathbf{N}$ esetén.

Bizonyítás. Legyen először $(r_i) \in I$, és legyen $\varepsilon \in \mathbf{Q}^+$ tetszőleges. A definíció szerint van olyan $n_0 \in \mathbf{N}$, hogy $|r_n| < \frac{\varepsilon}{2}$ valahányszor $n \geq n_0$. Ezért, ha $m, n \geq n_0$, akkor

$$|r_n - r_m| \leq |r_m| + |r_n| < \frac{\varepsilon}{2} + \frac{\varepsilon}{2} = \varepsilon.$$

Tehát (r_i) alapsorozat.

Legyen másodszer $(r_i) \in R$. A definíció szerint van olyan $n_0 \in \mathbf{N}$, melyre $|r_m - r_{n_0}| < 1$, azaz $r_{n_0} - 1 < r_m < r_{n_0} + 1$ valahányszor $m \geq n_0$. Ha $K_1 = \min(r_0, \dots, r_{n_0-1}, r_{n_0} - 1)$, $K_2 = \max(r_0, \dots, r_{n_0-1}, r_{n_0} + 1)$ és $K = \max(|K_1|, |K_2|)$, akkor $|r_i| < K$ minden $i \in \mathbf{N}$ esetén. ■

6.3. Segédteétel. Tetszőleges $(r_i) \in R \setminus I$ esetén a következő két állítás közül pontosan az egyik teljesül:

(*) Van olyan $t \in \mathbf{Q}^+$ és $n_0 \in \mathbf{N}$, hogy $t \leq r_n$ minden $n \geq n_0$ esetén.

(**) Van olyan $t \in \mathbf{Q}^+$ és $n_0 \in \mathbf{N}$, hogy $r_n \leq -t$ minden $n \geq n_0$ esetén.

A nullsorozatok egyik tulajdonsággal sem rendelkeznek.

Bizonyítás. Legyen $(r_i) \in R \setminus I$. Mivel (r_i) nem nullsorozat, van olyan $\varepsilon \in \mathbf{Q}^+$, hogy bármely $n \in \mathbf{N}$ esetén $|r_m| \geq \varepsilon$ valamely $m \geq n$ -re. Mivel (r_i) alapsorozat, ezért van olyan $n_1 \in \mathbf{N}$, hogy $|r_n - r_m| < \frac{\varepsilon}{2}$

valahányszor $m, n \geq n_1$. Az előbbieket szerint van olyan $n_0 \geq n_1$, hogy $|r_{n_0}| \geq \varepsilon$. Legyen $t = \frac{\varepsilon}{2}$. Ha $r_{n_0} > 0$, akkor bármely $n \geq n_0$ esetén

$$r_n = r_{n_0} - (r_{n_0} - r_n) = |r_{n_0}| - (r_{n_0} - r_n) \geq \varepsilon - \frac{\varepsilon}{2} = \frac{\varepsilon}{2} = t.$$

Tehát (*) teljesül. Ha pedig $r_{n_0} < 0$, akkor bármely $n \geq n_0$ esetén

$$-r_n = -r_{n_0} - (r_n - r_{n_0}) = |r_{n_0}| - (r_n - r_{n_0}) \geq \varepsilon - \frac{\varepsilon}{2} = \frac{\varepsilon}{2} = t,$$

amiből $r_n \leq -t$ következik. Tehát (**) teljesül. Mindkét esetben úgy csökkentettünk, hogy a kisebbítendőket csökkentettük a kivonandókat pedig növeltük. Az világos, hogy a két állítás egyszerre nem teljesülhet, és a nullsorozatok egyik állítást sem teljesítik. ■

6.4. Definíció. Azokat az alapsorozatotkat, melyekre (*), illetve (**) teljesül, *pozitív sorozatoknak*, illetve *negatív sorozatoknak* nevezzük. Jelölje R^+ a pozitív, R^- pedig a negatív alapsorozatok halmazát. Mivel a nullsorozatok sem a (*) sem a (**) tulajdonsággal nem rendelkezhetnek, a 6.3 Segédtevéből kapjuk a következőt:

6.5. Következmény. $R = R^+ \cup R^- \cup I$ és az egyesítésben szereplő három halmaz páronként diszjunkt.

6.6. Állítás.

- (a) Ha $(q_i), (r_i) \in R$ és $(s_i), (t_i) \in I$, akkor $(q_i + r_i), (q_i r_i) \in R$ és $(q_i s_i), (s_i + t_i), (-s_i) \in I$.
- (b) Ha $(q_i), (r_i) \in R^+$ és $(s_i) \in I$, akkor $(q_i + r_i), (q_i r_i), (q_i + s_i) \in R^+$ és $(-q_i) \in R^-$.
- (c) Ha $(q_i), (r_i) \in R^-$ és $(s_i) \in I$, akkor $(q_i + r_i), (q_i + s_i) \in R^-$ és $(-q_i), (q_i r_i) \in R^+$.

Bizonyítás. Az (a) állítás igazolásához legyen $(q_i), (r_i) \in R, (s_i), (t_i) \in I$ és $\varepsilon \in \mathbf{Q}^+$. Ekkor vannak olyan $n_1, n_2 \in \mathbf{N}$ számok, hogy $|q_m - q_n| < \frac{\varepsilon}{2}$, illetve $|r_m - r_n| < \frac{\varepsilon}{2}$ valahányszor $m, n \geq n_1$, illetve $m, n \geq n_2$. Ha $n_0 = \max(n_1, n_2)$ és $m, n \geq n_0$, akkor

$$\begin{aligned} |(q_m + r_m) - (q_n + r_n)| &= |(q_m - q_n) + (r_m - r_n)| \leq \\ &\leq |q_m - q_n| + |r_m - r_n| < \frac{\varepsilon}{2} + \frac{\varepsilon}{2} = \varepsilon. \end{aligned}$$

Tehát $(q_i + r_i) \in R$.

A 6.2. Állítás szerint van olyan $K_1, K_2 \in \mathbf{Q}^+$, hogy $|q_i| < K_1$ és $|r_i| < K_2$ minden $i \in \mathbf{N}$ esetén. Olyan $n_3, n_4 \in \mathbf{N}$ is van, hogy $|q_m - q_n| < \frac{\varepsilon}{2K_2}$, illetve $|r_m - r_n| < \frac{\varepsilon}{2K_1}$ valahányszor $m, n \geq n_3$, illetve $m, n \geq n_4$. Ha $n_5 = \max(n_3, n_4)$ és $m, n \geq n_5$, akkor

$$\begin{aligned} |(q_m r_m) - (q_n r_n)| &= |(q_m r_m - q_m r_n) + (q_m r_n - q_n r_n)| \leq \\ &\leq |q_m r_m - q_m r_n| + |q_m r_n - q_n r_n| = \\ &= |q_m| |r_m - r_n| + |r_n| |q_m - q_n| < K_1 \frac{\varepsilon}{2K_1} + K_2 \frac{\varepsilon}{2K_2} = \varepsilon. \end{aligned}$$

Tehát $(q_i r_i) \in R$. Mivel (s_i) nullsorozat, van olyan $n_6 \in \mathbf{N}$, hogy $|s_n| < \frac{\varepsilon}{2K_1}$ minden $n \geq n_6$ esetén. Ezért ha $n \geq n_6$, akkor

$$|q_n s_n| = |q_n| |s_n| < K_1 \frac{\varepsilon}{2K_1} = \varepsilon,$$

és ezért $(q_i s_i) \in I$.

Végül vannak olyan $n_7, n_8 \in \mathbf{N}$ számok is, hogy $|s_n| < \frac{\varepsilon}{2}$, illetve $|t_n| < \frac{\varepsilon}{2}$ valahányszor $m, n \geq n_7$, illetve $m, n \geq n_8$. Ha $n_9 = \max(n_7, n_8)$ és $m, n \geq n_9$, akkor

$$|s_n + t_n| \leq |s_n| + |t_n| < \frac{\varepsilon}{2} + \frac{\varepsilon}{2} = \varepsilon.$$

Tehát $(s_i + t_i) \in I$. A $(-s_i) \in I$ állítás nyilvánvaló.

A (b) állítás igazolásához legyen $(q_i), (r_i) \in R^+$ és $(s_i) \in I$. A definíciók szerint van olyan $t_1, t_2 \in \mathbf{Q}^+$ és $n_1, n_2, n_3 \in \mathbf{N}$, hogy $q_k \geq t_1$, $r_m \geq t_2$ és $|s_n| < \frac{t_1}{2}$, ha $k \geq n_1$, $m \geq n_2$ és $n \geq n_3$. Legyen $n_0 = \max(n_1, n_2, n_3)$, Ekkor

$$q_n + r_n \geq t_1 + t_2, \quad q_n r_n \geq t_1 t_2, \quad -q_n \leq -t_1$$

és

$$q_n + s_n \geq q_n - |s_n| \geq t_1 - \frac{t_1}{2} = \frac{t_1}{2},$$

ha $n \geq n_0$. Ezért $(q_i + r_i), (q_i r_i), (q_i + s_i) \in R^+$ és $(-q_i) \in R^-$. A (c) állítás igazolása hasonlóan történhet, ezért az olvasóra bízunk. ■

6.7. Tétel. Az $(R; +, \cdot)$ algebrai struktúrára érvényesek a következők:

- (1) A $(R; +, \cdot)$ kommutatív és egységelemes gyűrű, melynek (0) az additív (1) pedig a multiplikatív egységeleme.
- (2) I ideál az R gyűrűben, és az $(R/I; +, \cdot)$ faktorstruktúra olyan test, melyre a $\mathbf{Q} \rightarrow R/I$, $r \mapsto \overline{(r)} = I + (r)$ leképezés a $(\mathbf{Q}, +, \cdot)$ test beágyazása $(R/I, +, \cdot)$ -be.
- (3) $R/I = \{\overline{(r_i)} : (r_i) \in R^+\} \cup \{\overline{(0)}\} \cup \{\overline{(r_i)} : (r_i) \in R^-\}$, és az egyesítésben szereplő három halmaz páronként diszjunkt.

Bizonyítás. 6.6(a) szerint R zárt az összeadásra és a szorzásra. Tehát $(R; +, \cdot)$ algebrai struktúra. Az első állítás azon része, mely az összeadás és a szorzás tulajdonságaira vonatkozik, egyszerű számolással igazolható, s ezért itt nem részletezzük.

Ismét 6.6(a) szerint I olyan részgyűrű, melyre $(q_i)(s_i) \in I$ bármely $(q_i) \in R$ és $(s_i) \in I$ esetén. Tehát I ideál. Az $(R/I; +, \cdot)$ faktorstruktúra kommutatív és egységelemes gyűrű, melynek $\overline{(0)}$ az additív, $\overline{(1)}$ pedig a multiplikatív egységeleme, mert az $(R; +, \cdot)$ gyűrű $R \rightarrow R/I$, $(r_i) \mapsto \overline{(r_i)} = I + (r_i)$ homomorfizmus melletti képe.

Legyen $\overline{(r_i)} \in R/I$, és tegyük fel, hogy $\overline{(r_i)} \neq \overline{(0)} = I$. Ekkor $(r_i) \notin I$, és így a 6.3. Segédtelem szerint van olyan $t \in \mathbf{Q}^+$ és $n_0 \in \mathbf{N}$, hogy $t \leq |a_n|$ minden $n_0 \leq n$ esetén. Ezért az (r_i) sorozatnak csak az n_0 -nál kisebb indexű tagjai lehetnek 0-val egyenlők. Defináljuk az (s_i) sorozatot a következőképpen:

$$s_i = \begin{cases} r_i, & \text{ha } i \geq n_0; \\ t, & \text{különben.} \end{cases}$$

Ekkor $(s_i - r_i) \in I$, hiszen csak véges sok tagja különbözik 0-tól. Ezért $(s_i) = (s_i - r_i) + (r_i)$ alapsorozat, és $\overline{(s_i)} = \overline{(r_i)}$. Az $\left(\frac{1}{s_i}\right)$ sorozat is alapsorozat. Ennek igazolásához legyen $\varepsilon \in \mathbf{Q}^+$, és $n_1 \in \mathbf{N}$ olyan, hogy $|s_m - s_n| < \varepsilon t^2$ minden $m, n \geq n_1$ esetén. Ha $m, n \geq n_1$, akkor

$$\left| \frac{1}{s_m} - \frac{1}{s_n} \right| = \frac{|s_n - s_m|}{|s_m||s_n|} < \frac{\varepsilon t^2}{t^2} = \varepsilon.$$

Tehát $\overline{\left(\frac{1}{s_i}\right)} \in R/I$, és az $\overline{(r_i)} = \overline{(s_i)} \in R/I$ elemnek multiplikatív inverze, mert

$$\overline{(s_i)} \cdot \overline{\left(\frac{1}{s_i}\right)} = \overline{\left(s_i \frac{1}{s_i}\right)} = \overline{(1)}.$$

Tehát $(R/I; +, \cdot)$ test.

Most tekintsük a

$$\varphi: \mathbf{Q} \rightarrow R/I, r \mapsto \overline{r}$$

leképezést. Ha $q\varphi = r\varphi$, akkor $\overline{r} = \overline{q}$, vagyis a konstans $(q-r)$ sorozat I -ben van, amiből $q = r$ következik. Tehát φ injektív. φ felcserélhető a műveletekkel, ugyanis tetszőleges $q, r \in S$ esetén

$$(q+r)\varphi = \overline{(q+r)} = \overline{q} + \overline{r} = q\varphi + r\varphi$$

és

$$(qr)\varphi = \overline{(qr)} = \overline{q} \cdot \overline{r} = q\varphi \cdot r\varphi.$$

Tehát φ beágyazás.

A (3) állítás igazolása céljából tekintsünk egy tetszőleges $\overline{(r_i)} \in R/I$ elemet. $\overline{(r_i)} = \overline{(0)} = I$ pontosan akkor, ha $\overline{(r_i)} \in I$. Tegyük fel, hogy $\overline{(r_i)} \neq \overline{(0)}$, vagyis $(r_i) \notin I$. Ekkor a 6.3. Segédteétel és a 6.4. Definíció szerint $\overline{(r_i)} \in \{\overline{(r_i)}: (r_i) \in R^+\}$ vagy $\overline{(r_i)} \in \{\overline{(r_i)}: (r_i) \in R^-\}$. Ahhoz, hogy a (3) állításban szereplő halmazok páronként diszjunktak, már csak azt kell észrevenni, hogy $\overline{(q_i)} = \overline{(r_i)}$, azaz $(q_i - r_i) \in I$, nem teljesülhet $(q_i) \in R^+$ és $(r_i) \in R^-$ esetén, hiszen ellenkező esetben 6.6(b) szerint $(q_i - r_i) = (q_i) + (-r_i) \in R^+$, ami 6.3. Segédteétel szerint lehetetlen. ■

6.8. Definíció. Jelöljük az R/I halmazt \mathbf{R} -rel, és az $\overline{(r)}$, $r \in \mathbf{Q}$, alakú elemeket pedig egyszerűen r -rel. \mathbf{R} elemeit *valós számoknak* nevezzük. Legyen továbbá $\mathbf{R}^+ = \{\overline{(r_i)}: (r_i) \in R^+\}$ és $\mathbf{R}^- = \{\overline{(r_i)}: (r_i) \in R^-\}$. \mathbf{R}^+ elemeit *pozitív valós számoknak* \mathbf{R}^- elemeit pedig *negatív valós számoknak* hívjuk. Értelmezzünk a \leq relációt \mathbf{R} -n a következőképpen:

$$a \leq b \stackrel{\text{def}}{\Leftrightarrow} b - a \in \mathbf{R}^+ \cup \{0\}.$$

6.9. Tétel. Az $(\mathbf{R}; +, \cdot)$ algebrai struktúra olyan test, melynek $(\mathbf{Q}; +, \cdot)$ részgyűrűje. Továbbá $(\mathbf{R}; +, \cdot)$ lineárisan rendezett test a \leq relációra nézve, és a \leq reláció \mathbf{Q} -ra való megszorítása megegyezik \mathbf{Q} előző fejezetben bevezetett rendezésével.

Bizonyítás. Az első állítás az 6.7(2) állításból következik. Mivel $\mathbf{R}^+ \cup \{0\}$ tartalmazza a 0-t, zárt az összeadásra és a szorzásra, valamint a 6.7(3) állítás szerint ha $a, -a \in \mathbf{R}^+ \cup \{0\}$, akkor $a = 0$, és bármely $a \in \mathbf{R}$ esetén $a \in \mathbf{R}^+ \cup \{0\}$ vagy $-a \in \mathbf{R}^+ \cup \{0\}$. Ezért második állításunk a 2.7, 2.8 és 2.9 tételekből következik.

Terjesszük ki az abszolút érték függvényt a valós számok halmazára is:

$$|x| = \begin{cases} x, & \text{ha } x \geq 0; \\ -x, & \text{különben.} \end{cases}$$

A 2.11. Tétel speciális eseteként adódik most is a következő:

6.10. Állítás. Tetszőleges $a, b \in \mathbf{R}$ esetén $-|a| \leq a \leq |a|$, $|a| = |-a|$, $|ab| = |a| \cdot |b|$ és $|a+b| \leq |a| + |b|$.

6.11. Állítás. Tetszőleges a valós számhoz van egyetlen olyan $n \in \mathbf{Z}$, hogy $n \leq a < n+1$.

Bizonyítás. Legyen az a valós szám az (r_i) alapsorozattal megadva: $a = \overline{(r_i)}$. 6.2 szerint (r_i) korlátos. Ezért vannak olyan k és K racionális számok, hogy $k+1 \leq r_n \leq K-1$ minden $n \in \mathbf{N}$ esetén. Most $r_n - k \geq 1$ és $K - r_n \geq 1$ minden n -re, amiből a definíció szerint $a - k = \overline{(r_i - k)} \in \mathbf{R}^+$ és $K - a = \overline{(K - r_i)} \in \mathbf{R}^+$ következik. Tehát $[k] \leq k < a < K < [K] + 1$, azaz a két egész szám között van, és így létezik egy legnagyobb a -nál nem nagyobb n egész szám, amire nyilván teljesül $n \leq a < n+1$. Az egyértelműség igazolására az 5.6. Állítás bizonyításának megfelelő részét ismételhetjük meg. ■

6.12. Definíció. Legyen a valós szám. Az a szám $[a]$ egész része az 6.11. Állításban szereplő n szám, törtrésze pedig $\{a\} = a - [a]$.

6.13. Következmény. Tetszőleges $a \in \mathbf{R}$ számra $[a] \leq a < [a] + 1$ és $0 \leq \{a\} < 1$.

6.14. Állítás. A valós számhalmaz rendezése sűrű: tetszőleges $a, b \in \mathbf{R}$ esetén, ha $a < b$, akkor van olyan $x \in \mathbf{R}$, hogy $a < x < b$. Sőt x racionális számnak is választható.

Bizonyítás. Legyen $a, b \in \mathbf{R}$, $a < b$. Mivel $b - a > 0$, ezért van olyan $(r_i) \in R^+$, hogy $b - a = \overline{(r_i)}$. A definíció szerint van olyan $t \in \mathbf{Q}^+$ és $n_0 \in \mathbf{N}_0$, hogy $r_n \geq 2t$ valahányszor $n \geq n_0$. Ha $n \geq n_0$, akkor $r_n - t \geq 2t - t = t$. Ezért $(r_i) - t = \overline{(r_i - t)} \in \mathbf{R}^+$, amiből $0 < t < \overline{(r_i)} = b - a$ következik. Világos, hogy a

$$\dots < -3t < -2t < -t < 0 < t < 2t < 3t < \dots$$

racionális számok között van $[a]$ -nél, és így a -nál is kisebb, valamint $([a] + 1)$ -nél, és így a -nál is nagyobb szám. Ha m olyan egész szám, melyre $(m - 1)t \leq a < mt$, akkor $mt = (m - 1)t + t < a + (b - a) = b$. Tehát $a < mt < b$. ■

6.15. Definíció. Azt mondjuk, hogy az a_n , $n \in \mathbf{N}$, valós számsorozatnak az a valós szám a határértéke, ha bármely $\varepsilon \in \mathbf{R}^+$ számhoz van olyan $n_0 \in \mathbf{N}$, hogy $|a - a_n| < \varepsilon$ valahányszor $n \geq n_0$. (Mivel minden pozitív valós számmal van kisebb pozitív racionális szám, ha $\varepsilon \in \mathbf{R}^+$ helyett $\varepsilon \in \mathbf{Q}^+$ -t írunk, akkor az eredetivel ekvivalens definíciót kapunk. A későbbiekben ezt rendszeresen kihasználjuk.) Ha egy sorozatnak van határértéke, akkor *konvergens sorozatnak* nevezzük. A racionális számsorozatokhoz hasonlóan egy a_n , $n \in \mathbf{N}$, valós számsorozatot *Cauchy-sorozatnak* nevezünk, ha teljesíti a Cauchy-féle belső konvergencia-kritériumot: bármely $\varepsilon \in \mathbf{R}^+$ számhoz van olyan $n_0 \in \mathbf{N}$, hogy $|a_n - a_m| < \varepsilon$ valahányszor $m, n \geq n_0$.

6.16. Tétel. Ha valamely a valós számra és (r_i) alapsorozatra $a = \overline{(r_i)}$, akkor a az r_n , $n \in \mathbf{N}$, sorozat határértéke. Tehát minden valós szám racionális számsorozat határértéke.

Bizonyítás. Szükségünk lesz a következő észrevételre: Tetszőleges $\overline{(q_i)}$ valós számra $\overline{(|q_i|)} = \overline{(|q_i|)}$. Ugyanis, ha $\overline{(q_i)} = 0$, akkor (q_i) és így $(|q_i|)$ is nullsorozat, és ezért $\overline{(|q_i|)} = |0| = 0 = \overline{(|q_i|)}$. Ha $\overline{(q_i)} > 0$, akkor $(q_i) \in R^+$. A definícióból következően (q_i) tagjai valamely küszöbszámtól kezdve pozitívak, és így megegyeznek $(|q_i|)$ tagjaival. A $(q_i - |q_i|)$ sorozat nullsorozat, mert az előbb említett küszöbszámtól kezdve minden tagja nulla. Tehát $\overline{(|q_i|)} = \overline{(q_i)} = \overline{(|q_i|)}$. Ha $\overline{(q_i)} < 0$, akkor $\overline{(-q_i)} > 0$, és az előző esetet felhasználva kapjuk, hogy $\overline{(|q_i|)} = |-\overline{(q_i)}| = \overline{(-q_i)} = \overline{(|-q_i|)} = \overline{(|q_i|)}$.

Legyen $a = \overline{(r_i)}$, és $\varepsilon \in \mathbf{Q}^+$ tetszőleges. Mivel r_n , $n \in \mathbf{N}$, Cauchy-sorozat, van olyan $n_0 \in \mathbf{N}$, hogy $|r_m - r_n| < \frac{\varepsilon}{2}$ valahányszor $m, n \geq n_0$. Ha $n \geq n_0$, akkor $(\varepsilon - |r_i - r_n|) \in R^+$, mert

$$\varepsilon - |r_i - r_n| > \varepsilon - \frac{\varepsilon}{2} = \frac{\varepsilon}{2}$$

minden $i \geq n_0$ esetén. Tehát

$$\varepsilon - \overline{(|r_i - r_n|)} = \overline{(\varepsilon - |r_i - r_n|)} > 0,$$

vagyis

$$|a - r_n| = |\overline{(r_i)} - r_n| = \overline{(|r_i - r_n|)} = \overline{(|r_i - r_n|)} < \varepsilon$$

valahányszor $n \geq n_0$. ■

6.17. Tétel. Minden valós Cauchy-sorozatnak van határértéke.

Bizonyítás. Legyen $a_n = \overline{(r_i^n)}$, $n \in \mathbf{N}$, egy valós Cauchy-sorozat. A 6.16. Tétel szerint minden n -re $a_n = \overline{(r_i^n)}$ az r_i^n , $i \in \mathbf{N}$, sorozat határértéke. Ezért minden $n \in \mathbf{N}$ -re van olyan $n' \in \mathbf{N}$, hogy

$$|r_{n'}^{n'} - a_n| < \frac{1}{2^n}.$$

Legyen $q_i = r_{i'}$, $i \in \mathbf{N}$. Megmutatjuk, hogy (q_i) alapsorozat, és az $a = \overline{(q_i)}$ valós szám az a_n , $n \in \mathbf{N}$, sorozat határértéke.

Az $r_{n'} - a_n$, $n \in \mathbf{N}$ sorozat konvergens, mert abszolút értékét a nullához tartó $\frac{1}{2^n}$ sorozat majorálja. Ismert, hogy a konvergens sorozatok Cauchy-sorozatok. A racionális számsorozatokra vonatkozó megfelelő bizonyítást szó szerint megismételve megmutatható, hogy valós Cauchy-sorozatok összege is Cauchy-sorozat. Mindezek miatt

$$q_n = r_{n'} = (r_{n'} - a_n) + a_n, \quad n \in \mathbf{N},$$

Cauchy-sorozat. Legyen $\varepsilon \in \mathbf{R}^+$. A 6.16. Tétel szerint az $a = \overline{(q_i)}$ valós szám az q_n , $n \in \mathbf{N}$, sorozat határértéke. Ezért van olyan $n_1 \in \mathbf{N}$, hogy $|a - q_n| < \frac{\varepsilon}{2}$, ha $n \geq n_1$. Olyan $n_2 \in \mathbf{N}$ is van, melyre $\frac{1}{2^n} < \frac{\varepsilon}{2}$ valányszor $n \geq n_2$. Legyen $n_0 = \max(n_1, n_2)$. Ha $n \geq n_0$, akkor

$$|a - a_n| \leq |(a - q_n)| + |(q_n - a_n)| = |a - q_n| + |r_{n'} - a_n| < \frac{\varepsilon}{2} + \frac{1}{2^n} < \frac{\varepsilon}{2} + \frac{\varepsilon}{2} = \varepsilon.$$

Tehát a az a_n , $n \in \mathbf{N}$, sorozat határértéke. ■

6.18. Segédteétel. Minden monoton növekvő vagy monoton csökkenő korlátos valós számsorozat Cauchy-sorozat.

Bizonyítás. Legyen a_n , $n \in \mathbf{N}$, egy monoton növekvő korlátos sorozat. Ha a_n nem Cauchy-sorozat, akkor van olyan $\varepsilon \in \mathbf{R}^+$, hogy minden $n \in \mathbf{N}$ -ra $a_l - a_k \geq \varepsilon$ valamely $n \leq k < l$ esetén. Ebből a monoton növekvést is figyelembe véve azt kapjuk, hogy van olyan $\varepsilon \in \mathbf{R}^+$, hogy minden $n \in \mathbf{N}$ -ra $a_l - a_n \geq \varepsilon$, azaz $a_n + \varepsilon \leq a_l$, valamely $n < l$ esetén. Ez pedig lehetetlen, mert a_n felülről korlátos. Tehát a_n Cauchy-sorozat. Ha a_n , $n \in \mathbf{N}$, egy monoton csökkenő korlátos sorozat, akkor $-a_n$ egy monoton növekvő korlátos sorozat, és az előzőek szerint Cauchy-sorozat. Ezért a_n is Cauchy-sorozat. ■

6.19. Tétel. Bármely a pozitív valós számhoz van egyetlen olyan b pozitív valós szám, hogy $a = b^2$.

Bizonyítás. Legyen a egy pozitív valós szám. Tegyük fel először, hogy $a \geq 1$, és definiáljuk az a_n , $n \in \mathbf{N}$, sorozatot a következőképpen:

$$a_1 = a \quad \text{és} \quad a_{n+1} = \frac{a_n}{2} + \frac{a}{2a_n}, \quad n \in \mathbf{N}.$$

n szerinti teljes indukcióval megmutatjuk, hogy $1 \leq a_n \leq a$ minden n -re. $n = 1$ -re nyilván igaz. Tegyük fel, hogy n -re is igaz. Ekkor

$$1 = \frac{1}{2} + \frac{a}{2a} \leq \frac{a_n}{2} + \frac{a}{2a_n} = a_{n+1} \leq \frac{a}{2} + \frac{a}{2 \cdot 1} = a.$$

Az is igaz minden n -re, hogy $a_n^2 \geq a$. Valóban $a \geq 1$ -ből $a_1^2 = a^2 \geq a$ következik, és

$$a_{n+1}^2 - a = \left(\frac{a_n}{2} + \frac{a}{2a_n}\right)^2 - a = \left(\frac{a_n}{2} - \frac{a}{2a_n}\right)^2 \geq 0$$

miatt $a_{n+1}^2 \geq a$. Az a_n sorozat monoton csökkenő, hiszen minden n -re

$$a_n - a_{n+1} = a_n - \left(\frac{a_n}{2} + \frac{a}{2a_n}\right) = \frac{a_n}{2} - \frac{a}{2a_n} = \frac{a_n^2 - a}{2a_n} \geq \frac{a - a}{2a_n} = 0.$$

A 6.18. Segédteétel szerint a_n Cauchy-sorozat, ezért a 6.17. Tétel szerint konvergens. Jelölje b a határértékét. A $2a_n a_{n+1} = a_n^2 + a$ egyenlőséget és a konvergens sorozatok összegének, valamint szorzatának határértékére vonatkozó — jelen tárgyalásban nem bizonyított — alapvető tényeket felhasználva kapjuk, hogy $2bb = b^2 + a$, vagyis $b^2 = a$.

Ha $0 \leq a \leq 1$, akkor $1 \leq \frac{1}{a}$, és így az előzőek szerint $\frac{1}{a} = c^2$ valamely $c \in \mathbf{R}$ -re. Ebből pedig $a = \left(\frac{1}{c}\right)^2$ következik.

Végül az egyértelműség igazolásához legyen $x, y \in \mathbf{R}^+$ és $x^2 = a = y^2$. Mivel $x+y \neq 0$ és $(x+y)(x-y) = x^2 - y^2 = 0$, ezért $x - y = 0$, azaz $x = y$. ■

6.20. Tétel. A valós számok testének a 6.8. Definícióban bevezetett \leq rendezés az egyetlen lineáris rendezése.

Bizonyítás. Legyen P a pozitívítási tartománya a valós számok teste valamely lineáris rendezésének. A 2.10. Tétel szerint elegendő azt megmutatni, hogy $P = \mathbf{R}^+ \cup \{0\}$. $0 \in P$ nyilvánvaló. Ha $a \in \mathbf{R}^+$, akkor a 6.19. Tétel szerint van olyan b valós szám, hogy $a = b^2$. Mivel $b \in P$ vagy $-b \in P$, és ebből $a = b^2 = bb \in P$ vagy $a = b^2 = (-b)(-b) \in P$ következik. P negatív számokat nem tartalmazhat, mert akkor lenne olyan 0 -tól különböző szám mely az additív inverzével együtt P -ben van, ami P egyik tulajdonsága szerint lehetetlen. Tehát $P = \mathbf{R}^+ \cup \{0\}$. ■

7. A valós számok Dedekind-féle konstrukciója

A valós számok Dedekind-féle konstrukciója abból a szemléletes tényből indul ki, hogy bármely a száme-
gyenesen bármely pontját egyértelműen meghatáéizza a tőle jobbra eső racionális pontok halmaza. Ugyanis
két különböző pont esetén ez a két halmaz különböző, mivel a két pont között biztosan van racionális szám.

7.1. Definíció. A racionális számok \mathbf{Q} halmazának minden olyan X valódi részhalmazát *Dedekind-féle szeletnek* (röviden *szeletnek*) nevezzük, melyre teljesülnek a következők:

- (a) Ha $q \in X$ és $q < r$, akkor $r \in X$.
- (b) X -nek nincs legkisebb eleme.

Egy X szeletet *pozitív szeletnek*, illetve *negatív szeletnek* nevezzük, ha van olyan $r \in \mathbf{Q}^+$, hogy $r \notin X$, illetve van olyan $r \in \mathbf{Q}^-$, hogy $r \in X$. Jelölje \mathcal{R} , \mathcal{R}^+ és \mathcal{R}^- a szeletek, a pozitív szeletek és a negatív szeletek halmazát. Ha $r \in \mathbf{Q}$, akkor legyen

$$\bar{r} = \{x \in \mathbf{Q} : x > r\}.$$

Világos, hogy \bar{r} szelet. (Vegyük észre, hogy $\bar{0} = \mathbf{Q}^+$.) Az \bar{r} , $r \in \mathbf{Q}$, alakú halmazokat *racionális szeleteknek* nevezzük. Értelmezzük az összeadást az \mathcal{R} halmazon, a szorzást pedig az $\mathcal{R}^+ \cup \{\bar{0}\}$ halmazon a következőképpen:

$$X + Y \stackrel{\text{def}}{=} \{x + y : x \in X, y \in Y\}, \quad X, Y \in \mathcal{R},$$

és

$$X \cdot Y \stackrel{\text{def}}{=} \{xy : x \in X, y \in Y\}, \quad X, Y \in \mathcal{R}^+ \cup \{\bar{0}\}.$$

Végül, ha $X \in \mathcal{R}$, illetve $X \in \mathcal{R}^+$, akkor legyen

$$-X \stackrel{\text{def}}{=} \{u - v : u \in \mathbf{Q}^+, v \notin X\},$$

illetve

$$X^{-1} \stackrel{\text{def}}{=} \left\{ \frac{u}{v} : u > 1, v \in \mathbf{Q}^+ \setminus X \right\}.$$

7.2. Segédteétel. Ha $X \in \mathcal{R}$ és $t \in \mathbf{Q}^+$, akkor van olyan u racionális szám, melyre $u \notin X$ és $u + t \in X$.

Bizonyítás. Mivel X szelet, van olyan $v \in \mathbf{Q}$, hogy $v \notin X$. A

$$v + t, v + 2t, \dots, v + nt, \dots$$

sorozat tagjai elég nagy n esetén már X -ben vannak. Ezért, ha k a legkisebb olyan pozitív egész szám, melyre $v + kt \in X$, akkor $u = v + (k - 1)t \notin X$ és $u + t = v + kt \in X$. ■

7.3. Tétel. $(\mathcal{R}; +)$ kommutatív csoport a $\bar{0}$ additív egységelemmel, $(\mathcal{R}^+ \cup \{\bar{0}\}; +, \cdot)$ pedig egy olyan kommutatív és egységelemes félgűrű, melynek $\bar{0}$ multiplikatív zéruseleme, $\bar{1}$ pedig multiplikatív egységeleme, és a $\bar{0}$ -tól különböző elemeknek van multiplikatív inverze.

Bizonyítás. Először megmutatjuk, hogy az összeadás nem vezet ki a szeletek halmazából. Legyen $X, Y \in \mathcal{R}$. Ha $x \notin X$ és $y \notin Y$, akkor $x + y \notin X + Y$. Ellenkező esetben van olyan $u \in X$ és $v \in Y$, hogy $x + y = u + v$. Az egyenlőség miatt $x > u$ és $y > v$ egyszerre nem teljesülhet. Ezért $x \leq u$ vagy $y \leq v$. Az első esetben $y = (u - x) + v \geq v$ miatt $y \in Y$, a második esetben pedig $x = u + (v - y) \geq u$ miatt $x \in X$, ami a feltevés szerint lehetetlen. Legyen $z \in X + Y$, azaz $z = x + y$ valamely $x \in X$ és $y \in Y$ elemekre. Ha $z < t$, akkor $t = x + (y + (t - z)) \in X + Y$, mert $y < y + (t - z)$ miatt $y + (t - z) \in Y$. Mivel Y -nak nincs legkisebb eleme, valamely $v \in Y$ -ra $v < y$, és ezért $x + y > x + v \in X + Y$. Tehát $X + Y$ szelet.

Az \mathcal{R} halmazon definiált összeadás kommutativitása és asszociativitása a definíció közvetlen következménye. A $\bar{0}$ szelet additív egységelem. Valóban legyen X szelet és $z \in X + \bar{0}$. Ekkor valamely $x \in X$ és $y \in \bar{0} = \mathbf{Q}^+$ elemekre $z = x + y > x$, amiből $z \in X$ következik. Ha $x \in X$, akkor van olyan $u \in X$, hogy $u < x$. Mivel $x - u \in \bar{0}$, ezért $x = u + (x - u) \in X + \bar{0}$. Tehát $X + \bar{0} = X$.

Legyen X egy szelet. Megmutatjuk, hogy X -nek $-X$ az additív inverze. Először is azt kell belátni, hogy $-X$ szelet. Mivel X minden eleme a $\mathbf{Q} \setminus X$ halmaz felső korlátja, van a $\mathbf{Q} \setminus X$ halmaznak pozitív felső korlátja is. Legyen k egy pozitív felső korlát. Ha $x \in -X$, azaz $x = u - v$ valamely $u \in \bar{0} = \mathbf{Q}^+$ és $v \notin X$ esetén, akkor $x = u - v > -v \geq -k$, hiszen az utolsó egyenlőtlenség $v \leq 0$ esetén nyilvánvaló, pozitív v esetén pedig $v \leq k$ -ből következik. Tehát $-X$ nem tartalmaz $-k$ -nál kisebb racionális számokat. Legyen ismét $x \in -X$, vagyis $x = u - v$ valamely $u \in \bar{0}$ és $v \notin X$ esetén. Ha $y > x$, akkor $(y - x) + u > u > 0$ miatt $y = y + v - v = y + (u - x) - v = ((y - x) + u) - v \in -X$. Ha $0 < t < u$, akkor $t - v \in -X$ és $t - v < u - v = x$. Tehát $-X$ rendelkezik a szeletek tulajdonságaival.

Megmutatjuk, hogy $X + (-X) = \bar{0}$. Ha $y \in X + (-X)$, akkor van olyan $x \in X$, $u \in \bar{0}$ és $v \notin X$, hogy $y = x + (u - v)$, amiből $x > v$ miatt $y = u + (x - v) > u > 0$ és $y \in \bar{0}$ következik. Tehát $X + (-X) \subseteq \bar{0}$. Legyen $y \in \bar{0}$. A 7.2. Segédtelem szerint van olyan $u \notin X$, hogy $u + \frac{y}{2} \in X$. Ebből $y = (u + \frac{y}{2}) + (\frac{y}{2} - u) \in X + (-X)$, hiszen $(\frac{y}{2} - u) \in -X$. Tehát $\bar{0} \subseteq X + (-X)$, és így $X + (-X) = \bar{0}$. Ezzel befejeztük annak igazolását, hogy $(\mathcal{R}; +)$ kommutatív csoport a $\bar{0}$ additív egységelemmel.

Most megvizsgáljuk az $\mathcal{R}^+ \cup \{\bar{0}\}$ halmazon értelmezett szorzás tulajdonságait. Az nyilvánvaló, hogy a szorzat nem függ a tényezők sorrendjétől, és három tényező esetén a zárójelvezéstől. A $\bar{0}$ elem zéruselem, azaz $X \cdot \bar{0} = \bar{0}$ minden $X \in \mathcal{R}^+ \cup \{\bar{0}\}$ esetén. $X \cdot \bar{0} \subseteq \bar{0}$ nyilvánvaló. Ha $z \in \bar{0}$, akkor valamely $x \in X$ -re $\frac{z}{x} \in \bar{0}$, és $z = x \cdot \frac{z}{x} \in X \cdot \bar{0}$. Tehát $\bar{0} \subseteq X \cdot \bar{0}$ is teljesül.

Legyen $X, Y \in \mathcal{R}^+$. Ha $x \in \mathbf{Q}^+ \setminus X$ és $y \in \mathbf{Q}^+ \setminus Y$, akkor $xy \in \mathbf{Q}^+ \setminus (X \cdot Y)$. Ellenkező esetben van olyan $u \in X$ és $v \in Y$, hogy $xy = uv$. Mivel mind a négy szám pozitív, az egyenlőség miatt $x > u$ és $y > v$ egyszerre nem teljesülhet. Ezért $x \leq u$ vagy $y \leq v$. Az első esetben $y = \frac{u}{x} \cdot v \geq 1 \cdot v = v$ miatt $y \in Y$, a második esetben pedig $x = \frac{v}{y} \cdot u \geq 1 \cdot u = u$ miatt $x \in X$, ami a feltevés szerint lehetetlen. Legyen $z \in X \cdot Y$, azaz $z = xy$ valamely $x \in X$ és $y \in Y$ elemekre. Ha $z < t$, akkor $t = x(y \frac{t}{z}) \in X \cdot Y$, mert $y < y \frac{t}{z}$ miatt $y \frac{t}{z} \in Y$. Mivel Y -nak nincs legkisebb eleme, valamely $v \in Y$ -ra $v < y$, és ezért $xy > xv \in X \cdot Y$. Tehát $X \cdot Y$ pozitív szelet. Abból, hogy $\bar{0}$ a zéruselem, és \mathcal{R}^+ zárt a szorzásra, következik az $\mathcal{R}^+ \cup \{\bar{0}\}$ halmaz szorzásra való zártsága.

Legyen X egy pozitív szelet. Megmutatjuk, hogy X -nek X^{-1} a multiplikatív inverze. Először is azt kell belátni, hogy X^{-1} pozitív szelet. Legyen $k \in X$. Világos, hogy k a $\mathbf{Q}^+ \setminus X$ halmaz felső korlátja. Ha $x \in X^{-1}$, azaz $x = \frac{u}{v}$ valamely $u > 1$ és $v \in \mathbf{Q}^+ \setminus X$ esetén, akkor $x = \frac{u}{v} > \frac{1}{v} \geq \frac{1}{k}$ (az utolsó egyenlőtlenség a $v \leq k$ -ből következik). Tehát X^{-1} nem tartalmaz $\frac{1}{k}$ -nél kisebb pozitív racionális számokat. Legyen ismét

$x \in X^{-1}$, vagyis $x = \frac{u}{v}$ valamely $u > 1$ és $v \in \mathbf{Q}^+ \setminus X$ esetén. Ha $y > x$, akkor $\frac{y}{x}u > u > 1$ miatt $\frac{y}{x}u \in \bar{1}$, és

$$y = \frac{yv}{v} = \frac{y \frac{u}{x}}{v} = \frac{\frac{y}{x}u}{v} \in X^{-1}.$$

Ha $1 < t < u$, akkor $\frac{t}{v} \in X^{-1}$ és $\frac{t}{v} < \frac{u}{v} = x$. Tehát X^{-1} rendelkezik a pozitív szeletek tulajdonságaival.

Megmutatjuk, hogy $X \cdot X^{-1} = \bar{1}$. Ha $y \in X \cdot X^{-1}$, akkor van olyan $x \in X$, $u > 1$ és $v \in \mathbf{Q}^+ \setminus X$, hogy $y = x \frac{u}{v}$, amiből $x > v$ miatt $y = \frac{x}{v}u > u > 1$ és $y \in \bar{1}$ következik. Tehát $X \cdot X^{-1} \subseteq \bar{1}$.

Legyen $z \in \bar{1}$. és válasszuk t -t úgy, hogy $1 < t < z$. Ekkor

$$\frac{z}{t} = 1 + \varepsilon \text{ és } z = t(1 + \varepsilon)$$

valamely $\varepsilon \in \mathbf{Q}^+$ -ra. Legyen $x \in \mathbf{Q}^+ \setminus X$. A 7.2. Segédteél szerint van olyan $u \notin X$, hogy $u + \varepsilon x \in X$. Legyen $v = \max(x, u)$. Mivel $v + \varepsilon v \geq u + \varepsilon x \in X$, ezért $v + \varepsilon v \in X$. Továbbá $v \geq x > 0$, és $x, u \notin X$ miatt $v \notin X$, amiből $\frac{t}{v} \in X^{-1}$ következik. Ezeket felhasználva azt kapjuk, hogy

$$z = t(1 + \varepsilon) = (v(1 + \varepsilon)) \frac{t}{v} \in X \cdot X^{-1},$$

és ezért $\bar{1} \subseteq X \cdot X^{-1}$. Ezzel befejeztük az $X \cdot X^{-1} = \bar{1}$ egyenlőség igazolását. Tehát X multiplikatív inverze X^{-1} .

A tétel $(\mathcal{R}^+ \cup \{\bar{0}\}; +, \cdot)$ -ra vonatkozó állításának igazolásához már csak a szorzás összeadásra vonatkozó disztributivitását kell belátni. Ez a két művelet definíciójának közvetlen következménye. Ezért itt nem részletezzük. ■

7.4. Definíció. Értelmezzünk egy kétváltozós \leq relációt a \mathcal{R} halmazon a következőképpen:

$$X \leq Y \stackrel{\text{def}}{\iff} Y - X \in \mathcal{R}^+ \cup \{\bar{0}\}.$$

7.5. Tétel. A most definiált \leq reláció az $(\mathcal{R}; +)$ csoport lineáris rendezése, mely megegyezik a \supseteq relációval. Bármely $X \leq Y$ szelethez van olyan $r \in \mathbf{Q}$, melyre $X < \bar{r} < Y$.

Bizonyítás. A definíciókat, valamint a 7.3. Tétel bizonyítása során nyert információkat figyelembe véve könnyen belátható, hogy $\mathcal{R}^+ \cup \{\bar{0}\}$ rendelkezik a pozitivitási tartományok tulajdonságaival. Sőt minden $x \in \mathcal{R}$ esetén X vagy $-X$ az $\mathcal{R}^+ \cup \{\bar{0}\}$ halmazban van. Ezért a 2.4 és 2.3 Tételek szerint \leq az $(\mathcal{R}; +)$ csoport lineáris rendezése.

Legyen $X, Y \in \mathcal{R}$. Mivel \leq lineáris rendezés, $X \leq Y$ vagy $Y \leq X$. Ha $X \leq Y$, akkor van olyan $Z \in \mathcal{R}^+ \cup \{\bar{0}\}$, hogy $Y = X + Z$. Ezért, ha $y \in Y$, akkor $y = x + z$ valamely $x \in X$ és $z \in Z$ esetén. Mivel $z > 0$, ebből $y > x$ és $y \in X$ következik. Tehát $X \supseteq Y$. Hasonlóan látható be, hogy $Y \leq X$ esetén $Y \supseteq X$. Végül, ha $X \supseteq Y$ és $X \neq Y$, akkor mivel \leq lineáris rendezés, $X \leq Y$ vagy $Y \leq X$. A második eset nem teljesülhet, mert abból az előzőek szerint $Y \supseteq X$ és $X = Y$ következne.

A második állítás igazolásához legyen X és Y két olyan szelet, melyre $X < Y$. Az előzőek szerint $X \supset Y$. Ezért van olyan $r \in \mathbf{Q}$, hogy $r \in X$ és $r \notin Y$. Ekkor $X \supset \bar{r} \supset Y$, azaz $X \leq \bar{r} \leq Y$. ■

7.6. Állítás. $\mathcal{R} = \mathcal{R}^+ \cup \{\bar{0}\} \cup \mathcal{R}^-$, és az egyesítésben szereplő három halmaz páronként diszjunkt. Továbbá \mathcal{R}^+ és \mathcal{R}^- zárt az összeadásra, és $X \in \mathcal{R}^+$, illetve $X \in \mathcal{R}^-$, akkor $-X \in \mathcal{R}^-$, illetve $-X \in \mathcal{R}^+$.

Bizonyítás. A definíciókat, valamint a 7.3. Tétel bizonyítása során nyert információkat figyelembe véve könnyen belátható. ■

7.7. Definíció. Terjesszük ki a szorzást az összes szeletek halmazára a következőképpen:

$$X \cdot Y \stackrel{\text{def}}{=} \begin{cases} \bar{0} & \text{ha } X = \bar{0} \text{ vagy } Y = \bar{0}; \\ X \cdot Y, & \text{ha } X, Y \in \mathcal{R}^+; \\ (-X) \cdot (-Y), & \text{ha } X, Y \in \mathcal{R}^-; \\ -((-X) \cdot Y), & \text{ha } X \in \mathcal{R}^- \text{ és } Y \in \mathcal{R}^+; \\ -(X \cdot (-Y)), & \text{ha } X \in \mathcal{R}^+ \text{ és } Y \in \mathcal{R}^-. \end{cases}$$

7.8. Tétel. Az $(\mathcal{R}; +, \cdot)$ algebrai struktúra olyan test, melynek a \leq reláció lineáris rendezése. Továbbá a $\mathbf{Q} \rightarrow \mathcal{R}$, $r \mapsto \bar{r}$ leképezés az $(\mathbf{Q}; +, \cdot)$ test rendezéstartó beágyazása $(\mathcal{R}; +, \cdot)$ -ba.

Bizonyítás. A szorzás definíciójának helyességét a 7.6. Állítás biztosítja. A 7.2. Tétel szerint a $(\mathcal{R}^+; \cdot)$ kommutatív csoport az $\bar{1}$ egységelemmel. Ezt és a szorzás definícióját figyelembe véve több esetre bontott egyszerű számolással megmutatható, hogy $(\mathcal{R}^+ \cup \mathcal{R}^-; \cdot)$ is kommutatív csoport az $\bar{1}$ egységelemmel. A 7.3. Tétel szerint $(\mathcal{R}; +)$ kommutatív csoport. Ezért annak igazolásához, hogy $(\mathcal{R}; +, \cdot)$ test már csak a szorzás összeadásra való disztributivitását kell belátni. Mivel ez az eddigi tények és a szorzás definíciójának felhasználásával ugyancsak több esetre bontott egyszerű számolást igényel, nem részletezzük.

A 7.8. Tétel szerint \leq az $(\mathcal{R}; +)$ csoport lineáris rendezése, és pozitivitási tartománya $\mathcal{R}^+ \cup \{\bar{0}\}$ zárt a szorzásra. Ezért a 2.8. Tétel szerint \leq az $(\mathcal{R}; +, \cdot)$ testnek is lineáris rendezése.

Tekintsük most a $\varphi: \mathbf{Q} \rightarrow \mathcal{R}$, $r \mapsto \bar{r}$ leképezést. φ injektív, mert Ha $q, r \in \mathbf{Q}$ és $q < r$, akkor van olyan $s \in \mathbf{Q}$, hogy $q < s < r$, amiből $s \in \bar{q}$, $s \notin \bar{r}$ és $s\varphi = \bar{s} \neq \bar{r} = r\varphi$ következik. Ha $q, r \in \mathbf{Q}$ és $q \leq r$, akkor $\bar{q} \supseteq \bar{r}$, amiből a 7.5. Tétel szerint $\bar{q} \leq \bar{r}$ következik. Tehát φ rendezéstartó.

Be kell látni, hogy φ felcserélhető az összeadással: $q\varphi + r\varphi = \bar{q} + \bar{r} = \overline{q+r} = (q+r)\varphi$ minden $q, r \in \mathbf{Q}$ esetén, ami ekvivalens azzal, hogy $\bar{q} + \bar{r} = \overline{q+r}$. Ha $z \in \bar{q} + \bar{r}$, vagyis $z = x + y$ valamely $x > q$ és $y > r$ racionális számra, amiből $z = x + y > q + r$ és $z \in \overline{q+r}$ következik. Ha pedig $z \in \overline{q+r}$, akkor $z > q + r$. Ha $t = \frac{z - (q+r)}{2}$, akkor $q + t \in \bar{q}$ és $r + t \in \bar{r}$ és $z = (q+t) + (r+t) \in \bar{q} + \bar{r}$. Tehát $\bar{q} + \bar{r} = \overline{q+r}$.

A következő tényt később fogjuk használni: tetszőleges $r \in \mathbf{Q}$ esetén $-\bar{r} = \overline{-r}$. Ehhez csak azt kell belátni, hogy $\bar{r} + \overline{-r} = \bar{0}$. Ez pedig igaz, hiszen, $\bar{r} + \overline{-r} = r + (-r) = \bar{0}$.

Hátra van még annak megmutatása, hogy tetszőleges $q, r \in \mathbf{Q}$ esetén $q\varphi \cdot r\varphi = (qr)\varphi$, ami ekvivalens a $\bar{q} \cdot \bar{r} = \overline{qr}$ egyenlőséggel. Ha $q = 0$ vagy $r = 0$, akkor $\bar{q} \cdot \bar{r} = \bar{0} = \overline{qr}$. Legyen $q, r > 0$. Ha $z \in \bar{q} \cdot \bar{r}$, vagyis $z = xy$ valamely $x > q$ és $y > r$ racionális számra, amiből $z = xy > qr$ és $z \in \overline{qr}$ következik. Ha pedig $z \in \overline{qr}$, akkor $z > qr$, és $t = \frac{z}{qr} > 1$. Ezért van olyan $m, n \in \mathbf{N}$, $1 < m < n$, hogy $t = \frac{n}{m}$. Legyen $u = \frac{2n}{2n-1}$ és $u = \frac{2n-1}{2m}$. Ekkor $t = uv$ és $u, v > 1$. Az utóbbi miatt $q < qu$ és $r < rv$, amiből $qu \in \bar{q}$ és $rv \in \bar{r}$ következik. Ezért

$$z = qr \frac{z}{qr} = qrt = (qu)(rv) \in \bar{q} \cdot \bar{r},$$

és így $\overline{qr} \subseteq \bar{q} \cdot \bar{r}$ is teljesül. Tehát ebben az esetben is $\bar{q} \cdot \bar{r} = \overline{qr}$. Ha $q, r < 0$, akkor

$$\bar{q} \cdot \bar{r} = (-\overline{-q}) \cdot (-\overline{-r}) = \overline{-q} \cdot \overline{-r} = \overline{qr}.$$

Ha $q < 0$ és $r > 0$, akkor

$$\bar{q} \cdot \bar{r} = (-\overline{-q}) \cdot \bar{r} = -(\overline{-q} \cdot \bar{r}) = -\overline{-qr} = \overline{qr}.$$

Végül ha $q > 0$ és $r < 0$, akkor

$$\bar{q} \cdot \bar{r} = \bar{q} \cdot (-\overline{-r}) = -(\bar{q} \cdot \overline{-r}) = -\overline{-qr} = \overline{qr}.$$

■

7.9. Megjegyzés. Mivel a $\mathbf{Q} \rightarrow \mathcal{R}$, $r \mapsto \bar{r}$ leképezés beágyazás, a racionális szeleteket a megfelelő racionális számmal is fogjuk jelölni.

7.10. Tétel. Tetszőleges $a \in \mathbf{R}$ valós számra legyen $\bar{a} = \{r \in \mathbf{Q} : r > a\}$. Ekkor a $\varphi: \mathbf{R} \rightarrow \mathcal{R}$, $a \mapsto \bar{a}$ leképezés a valós számok testének az $(\mathcal{R}; +, \cdot)$ testbe való rendezéstartó izomorfizmusa. Tehát a valós számok Cantor-féle és Dedekind-féle konstrukciója egymással izomorf testeket eredményezett.

Bizonyítás. Ha $a, b \in \mathbf{R}$ és $a \neq b$, mondjuk $a < b$, akkor 6.14. Tétel szerint van olyan $r \in \mathbf{Q}$, hogy $a < r < b$. Ekkor $r \in \bar{a}$ és $r \notin \bar{b}$. Ezért $a\varphi = \bar{a} \neq \bar{b} = b\varphi$. Tehát φ injektív. A szürjektivitás igazolásához szükségünk lesz a következő észrevételeire.

(*) Tetszőleges $X \in \mathcal{R}$, $q \in X$ és $t \in \mathbf{Q}^+$ esetén van egyetlen olyan $k \in \mathbf{N}_0$, hogy $q - (k+1)t \notin X$ és $q - kt \in X$.

Ez abból következik, hogy míg az

$$q, q - t, q - 2t, \dots, q - kt, \dots$$

sorozat első tagja X -ben van, valamelyik későbbi tagja szükségképpen X -en kívül esik. Az egyértelműség a szelet definíciójából következik.

Legyen $X \in \mathcal{R}$, és válasszunk ki egy $r \in X$ racionális számot. Defináljuk az r_n , $n \in \mathbf{N}$, sorozatot a következőképpen: $r_1 = r$. Ha r_n már értelmezve van, akkor legyen $r_{n+1} = r_n - k_n \frac{1}{2^{n+1}} \in X$ arra a (*)

szerint egyértelműen létező k_n -re, melyre $r_{n+1} - \frac{1}{2^{n+1}} = r_n - (k_n + 1) \frac{1}{2^{n+1}} \notin X$. A definícióból adódóan r_n monoton csökkenő, és korlátos is, hiszen bármely X -en kívüli racionális szám alsó korlátja. A 6.18. Segédtelet szerint a_n alapsorozat. Legyen $a = \overline{(r_i)} \in \mathbf{R}$. Vegyük észre, hogy minden n -re $a \leq r_n$. Ugyanis $r_n - a = r_n - \overline{(r_i)} = \overline{(r_n - r_i)}$, és az $r_n - r_i$, $i \in \mathbf{N}$, sorozat tagjai nemnegatívak az n -edik tagtól kezdődően, amiért nullsorozat vagy pozitív sorozat, és így a 6.8. Definíció szerint $r_n - a \geq 0$.

Megmutatjuk, hogy $a\varphi = \bar{a} = X$. Ha $x \in \bar{a}$, azaz $a < x$, akkor $0 < x - a = x - \overline{(r_i)} = \overline{(x - r_i)}$. A 6.8. Definícióból következik, hogy van olyan $t \in \mathbf{Q}^+$ és $n \in \mathbf{N}$, hogy $x - r_n \geq t$. Mivel $r_n \in X$, ezért $x \in X$. Tehát $\bar{a} \subseteq X$. Legyen $x \in X$. Megmutatjuk, hogy van olyan n , hogy $r_n < x$. Ugyanis, ha minden n -re $x \leq r_n$, akkor mivel az r_n sorozat definíciójából következően minden n -re $r_n - \frac{1}{2^n} \notin X$, ezért ugyancsak minden n -re $x - \frac{1}{2^n} \notin X$. Ebből pedig az következik, hogy x az X szelet legkisebb eleme, ami lehetetlen. Legyen $r_n < x$. Ekkor $a \leq r_n$ miatt $a \leq r_n < x$ és $x \in \bar{a}$. Tehát $X \subseteq \bar{a}$, és így $X = \bar{a}$. Ezzel beláttuk φ szürjektivitását is.

Ha $a \leq b$, akkor nyilván $\bar{a} \supseteq \bar{b}$. Ezért a 7.5. Tétel szerint $\bar{a} \leq \bar{b}$. Tehát φ rendezéstartó. Hátra van még annak igazolása, hogy φ felcserélhető a műveletekkel. Ezt most nem részletezzük, mert szinte szó szerint megegyezik a 7.8. Tétel bizonyításában szereplő racionális számokra vonatkozó gondolatmenettel. ■

A 7.10. Tétel szerint a valós számok racionális számsorozatokra, illetve a Dedekind-szeletekre épülő konstrukciója ugyanarra az eredményre vezetett. Ezért mostantól kezdve \mathcal{R} elemeit is valós számoknak nevezzük. Most kizárólag Dedekind-szeletek segítségével megmutatjuk, hogy minden pozitív valós számnak van n -edik gyöke ($n \geq 1$).

7.11. Segédtelet. Bármely $n \in \mathbf{N}$ -hez és bármely $a < b$ pozitív szelethez található olyan x pozitív racionális szelet, melyre $a < x^n < b$.

Bizonyítás. Legyen $n \in \mathbf{N}$ és $a < b$ pozitív szeletek. A 7.5. Tétel második állítása szerint található olyan u, v pozitív racionális szeletek, melyekre, $u < \min(a, 1)$ és $\max(b, 1) < v$. Ekkor $u < 1$ és $1 < v$ miatt $u^n \leq u$ és $v \leq v^n$. Tehát a, b, u, v olyan pozitív szeletek, melyekre

$$u^n < a < b < v^n.$$

Legyen m egy később meghatározandó pozitív egész szám és $\varepsilon = \frac{v-u}{m}$. Tekintsük most az

$$u^2 < (u + \varepsilon)^n < (u + 2\varepsilon)^n < \dots < (u + (m-1)\varepsilon)^n < (u + m\varepsilon)^n = v^2$$

sorozatot. Megmutatjuk, hogy megadható m úgy, hogy e sorozat szomszédos tagjainak különbsége kisebb legyen $b - a$ -nál. A rövideg kedvért legyen $t = u + (k - 1)\varepsilon$, $k = 1, \dots, m$. Ekkor felhasználva, hogy

$$\sum_{i=0}^n \binom{n}{i} = 2^n, \quad \text{és} \quad t, \varepsilon < v$$

kapjuk, hogy

$$\begin{aligned} (u + k\varepsilon)^n - (u + (k - 1)\varepsilon)^n &= (t + \varepsilon)^n - t^n = \\ &= \sum_{i=0}^n \binom{n}{i} t^{n-i} \varepsilon^i - t^n = \varepsilon \left(\sum_{i=1}^n \binom{n}{i} t^{n-i} \varepsilon^{i-1} \right) < \varepsilon \left(\sum_{i=1}^n \binom{n}{i} v^{n-1} \right) < \varepsilon v^{n-1} 2^n. \end{aligned}$$

Legyen m olyan, hogy

$$\varepsilon v^{n-1} 2^n = \frac{v - a}{m} v^{n-1} 2^n < b - a,$$

vagyis

$$m > \frac{2^n v^{n-1} (v - a)}{b - a}.$$

Ekkor a fenti sorozat első tagja a -nál kisebb, az utolsó tagja b -nél nagyobb, és a szomszédos tagjainak különbsége kisebb, mint $b - a$. Ezért szükségképpen van olyan tagja, mely a és b közé esik. ■

7.12. Tétel. *Bármely $n \in \mathbf{N}$ -hez és A pozitív szelethez létezik egyetlen olyan X pozitív szelet, melyre $A = X^n$.*

Bizonyítás. Legyen A egy pozitív szelet, és

$$X = \{r \in \mathbf{Q}^+ : r^n \in A\}.$$

Megmutatjuk, hogy X olyan pozitív szelet, melyre $X^n = A$. Ha $q \in X$ és $q < r$, akkor $q^n \in A$ és $q^n < r^n$ miatt $r^n \in A$, vagyis $r \in X$. Válasszuk az $a \in A$ elemet úgy, hogy $a < q^n$. A 7.11. Segédtelet szerint van olyan $s \in \mathbf{Q}^+$, hogy $\bar{a} < \bar{s}^n = \overline{s^n} < \overline{q^n}$. Ekkor egyrészt $a < s^n$ miatt $s^n \in A$ és $s \in X$, másrészt $s^n < q^n$ miatt $s < q$. Tehát X rendelkezik a szeletek mindkét tulajdonságával. Mivel A pozitív szelet, van olyan $u \in \mathbf{Q}^+$, hogy $u \notin A$. A 7.11. Segédtelet szerint van olyan $v \in \mathbf{Q}^+$, hogy $\bar{v}^n = \overline{v^n} < \bar{u}$. Ekkor $v^n < u \notin A$ miatt $v^n \notin A$ és $v \notin X$. Tehát X pozitív szelet.

Most rátérünk az $A = X^n$ egyenlőség igazolására. Legyen $r_1, \dots, r_n \in X$ és $r = \min(r_1, \dots, r_n)$. Ekkor $r \leq r_1, \dots, r_n$ miatt $r^n \leq r_1 \cdots r_n$, amiből $r^n \in A$ miatt $r_1 \cdots r_n \in A$ következik. Tehát $X^n \subseteq A$. Legyen most $b \in A$. Vegyünk egy $a \in A$ elemet úgy, hogy $a < b$. A 7.11. Segédtelet szerint van olyan $r \in \mathbf{Q}^+$, hogy $\bar{a} < \bar{r}^n = \overline{r^n} < \bar{b}$. Ekkor $a < r^n < b$ miatt $r^n \in A$, $r \in X$, $r^n \in X^n$ és $b \in X^n$. Tehát $A \subseteq X^n$ is teljesül.

Az egyértelműség igazolásához legyenek X és Y olyan pozitív szeletek, hogy $X^n = Y^n$. Ekkor

$$0 = X^n - Y^n = (X - Y)(X^{n-1} + X^{n-2}Y + \dots + XY^{n-2} + Y^{n-1}).$$

Mivel a második tényező nem nulla, $X - Y = 0$ és $X = Y$. ■

8. Komplex számok

8.1. Definíció. Az \mathbf{R}^2 halmazon értelmezzük az összeadás és a szorzás műveleteket a következőképpen: Tetszőleges $(a, b), (c, d) \in \mathbf{R}^2$ esetén legyen

$$(a, b) + (c, d) \stackrel{\text{def}}{=} (a + c, b + d)$$

és

$$(a, b) \cdot (c, d) \stackrel{\text{def}}{=} (ac - bd, ad + bc).$$

8.2. Tétel. Az $(\mathbf{R}^2; +, \cdot)$ algebrai struktúra olyan test, melynek $(0, 0)$ az additív $(1, 0)$ pedig a multiplikatív egységeleme, és az $\mathbf{R} \rightarrow \mathbf{R}^2, a \mapsto (a, 0)$ leképezés a valós számok testének beágyazása az $(\mathbf{R}^2, +, \cdot)$ -ba.

Bizonyítás. Egyszerű számolással ellenőrizhető, hogy az összeadás és a szorzás kommutatív és asszociatív, a szorzás disztributív az összeadásra nézve, a $(0, 0)$ additív, az $(1, 0)$ pedig multiplikatív egységelem, és az $(a, b) \in \mathbf{R}$ elemnek $(-a, -b)$ az additív inverze. Például a szorzás asszociativitását és az összeadásra vonatkozó disztributivitását a következőképpen igazolhatjuk: Tetszőleges $(a, b), (c, d), (e, f) \in \mathbf{R}^2$ esetén

$$\begin{aligned} ((a, b) \cdot (c, d)) \cdot (e, f) &= (ac - bd, ad + bc) \cdot (e, f) = \\ &= ((ac - bd)e - (ad + bc)f, (ac + bd)f + (ad + bc)e) = \\ &= ((a(ce - df) - b(cf + de), a(cf + de) + b(ce + df)) = \\ &= (a, b) \cdot (ce - df, cf + de) = (a, b) \cdot ((c, d) \cdot (e, f)) \end{aligned}$$

és

$$\begin{aligned} ((a, b) + (c, d)) \cdot (e, f) &= (a + c, b + d) \cdot (e, f) = \\ &= ((a + c)e - (b + d)f, (a + c)f + (b + d)e) = \\ &= (ae + ce - bf - df, af + cf + be + de) = (ae - bf, af + be) + (ce - df, cf + de) = \\ &= ((a, b) \cdot (e, f)) + ((c, d) \cdot (e, f)). \end{aligned}$$

Ha $(a, b) \neq (0, 0)$, akkor $a^2 + b^2 \neq 0$ és

$$(a, b) \cdot \left(\frac{a}{a^2 + b^2}, \frac{-b}{a^2 + b^2} \right) = \left(\frac{a^2}{a^2 + b^2} - \frac{-b^2}{a^2 + b^2}, \frac{ab}{a^2 + b^2} + \frac{-ab}{a^2 + b^2} \right) = (1, 0).$$

Tehát (a, b) -nek $\left(\frac{a}{a^2 + b^2}, \frac{-b}{a^2 + b^2} \right)$ a multiplikatív inverze. Mindezeket figyelembe véve azt kapjuk, hogy $(\mathbf{R}^2; +, \cdot)$ test.

Most tekintsük a

$$\varphi: \mathbf{R} \rightarrow \mathbf{R}^2, a \mapsto (a, 0)$$

leképezést. Világos, hogy φ injektív. Ha $a, b \in \mathbf{R}$, akkor

$$(a + b)\varphi = (a + b, 0) = (a, 0) + (b, 0) = a\varphi + b\varphi$$

és

$$(ab)\varphi = (ab, 0) = (ab - 0 \cdot 0, a \cdot 0 + b \cdot 0) = (a, 0) \cdot (b, 0) = a\varphi \cdot b\varphi.$$

Tehát φ beágyazás. ■

8.3. Definíció. Jelöljük az \mathbf{R}^2 halmazt \mathbf{C} -vel, az $(a, 0), a \in \mathbf{R}$, alakú elemeket egyszerűen a -val, a $(0, 1)$ elemet pedig i -vel. \mathbf{C} elemeit *komplex számoknak* nevezzük. (Vegyük észre, hogy $i^2 = -1$.)

8.4. Tétel. A $(\mathbf{C}; +, \cdot)$ algebrai struktúra olyan test, melynek $(\mathbf{R}; +, \cdot)$ részteste, minden eleme $a + bi$ ($a, b \in \mathbf{R}$) alakban írható, és nincs lineáris rendezése.

Bizonyítás. Mivel $1^2 + i^2 = 1 - 1 = 0$, a 2.13. Tétel szerint nincs \mathbf{C} -nek lineáris rendezése. Ha $(a, b) \in \mathbf{C}$, akkor

$$(a, b) = (a, 0) + (0, b) = (a, 0) + (b, 0) \cdot (0, 1) = a + bi.$$

Ebből és a 8.2 Tételből már következik állításunk. ■

8.5. Definíció. Egy $z = a + bi \in \mathbf{C}$ komplex szám \bar{z} konjugáltját és $|z|$ abszolút értékét a következőképpen értelmezzük:

$$\bar{z} = a - bi, \quad |z| = \sqrt{a^2 + b^2}.$$

A komplex számokra vonatkozó számolási szabályokkal szinte mindegyik bevezető jellegű felsőbb algebra tankönyv részletesen foglalkozik. Ezért most csak a legfontosabbakat ismertetjük bizonyítás nélkül.

8.6. Tétel. Bármely $z, z_1, z_2 \in \mathbf{C}$ esetén

$$\begin{aligned} \overline{\bar{z}} &= z, \quad |z| = |\bar{z}|, \quad z\bar{z} = |z|^2, \quad \frac{1}{z} = \frac{\bar{z}}{|z|^2} \quad (z \neq 0), \\ |z_1 z_2| &= |z_1| |z_2|, \quad \overline{z_1 + z_2} = \bar{z}_1 + \bar{z}_2, \quad \overline{z_1 z_2} = \bar{z}_1 \cdot \bar{z}_2, \\ \frac{\overline{z_1}}{z_2} &= \frac{\bar{z}_1}{\bar{z}_2} \quad (z_2 \neq 0) \quad \text{és} \quad |z_1 + z_2| \leq |z_1| + |z_2|. \end{aligned}$$

Az alábbiakban két olyan konstrukciót ismertetünk, melynek eredménye a komplex számok teste.

8.7. Tétel. Legyen C az $\begin{pmatrix} a & b \\ -b & a \end{pmatrix}$ ($a, b \in \mathbf{R}$) alakú 2×2 -es mátrixok halmaza. Ekkor C a mátrixok összeadására és szorzására nézve a komplex számok testével izomorf testet alkot.

Bizonyítás. Tekintsük a

$$\varphi: \mathbf{C} \rightarrow C, \quad a + bi \mapsto \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$$

leképezést. Az nyilvánvaló, hogy φ bijektív. Ha $a + bi, c + di \in \mathbf{C}$, akkor

$$\begin{aligned} ((a + bi) + (c + di))\varphi &= ((a + c) + (b + d)i)\varphi = \\ &= \begin{pmatrix} a + c & b + d \\ -(b + d) & a + c \end{pmatrix} = \begin{pmatrix} a & b \\ -b & a \end{pmatrix} + \begin{pmatrix} c & d \\ -d & c \end{pmatrix} = \\ &= (a + bi)\varphi + (c + di)\varphi \end{aligned}$$

és

$$\begin{aligned} ((a + bi)(c + di))\varphi &= ((ac - bd) + (ad + bc)i)\varphi = \\ &= \begin{pmatrix} ac - bd & ad + bc \\ -(ad + bc) & ac - bd \end{pmatrix} = \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \cdot \begin{pmatrix} c & d \\ -d & c \end{pmatrix} = \\ &= (a + bi)\varphi \cdot (c + di)\varphi \end{aligned}$$

Tehát φ felcserélhető az összeadással és a szorzással, és ezért izomorfizmus. ■

8.8. Tétel. Tekintsük a valós számok teste feletti egyhatározatlanú polinomok $(\mathbf{R}[x]; +, \cdot)$ gyűrűjét. Ekkor $\mathbf{R}[x]$ -ben az

$$I = \{(x^2 + 1)q(x) : q(x) \in \mathbf{R}[x]\}$$

halmaz ideált alkot, és az $\mathbf{R}[x]/I$ faktorgyűrű izomorf a komplex számok testével.

Bizonyítás. Ha $f, g \in I$ és $h \in \mathbf{R}[x]$, akkor valamely $f_1, g_1 \in \mathbf{R}[x]$ polinomokra $f = (x^2 + 1)f_1$ és $g = (x^2 + 1)g_1$. Ezért

$$f + g = (x^2 + 1)(f_1 + g_1), \quad f - g = (x^2 + 1)(f_1 - g_1) \in I$$

és

$$fh = (x^2 + 1)(f_1 h) \in I.$$

Tehát I ideál. Az $\mathbf{R}[x]/I$ faktorgyűrű elemei az $I + f$ ($f \in \mathbf{R}[x]$) alakú mellékosztályok. Az egyszerűség kedvéért $I + f$ helyett \overline{f} -et, ha pedig a egy konstans polinom, akkor \overline{a} helyett egyszerűen a -t fogunk írni. Vegyük észre, hogy

$$\overline{x^2} = \overline{x^2} = \overline{x^2 + 1} - 1 = \overline{0} - 1 = -1.$$

Telintsük a

$$\varphi: \mathbf{C} \rightarrow \mathbf{R}[x]/I, \quad a + bi \mapsto a + b\overline{x}$$

leképezést. Ha $a + bi, c + di \in \mathbf{C}$ és $(a + bi)\varphi = (c + di)\varphi$, akkor $a + b\overline{x} = c + d\overline{x}$. Ezért

$$\overline{(a - c) + (b - d)x} = (a + b\overline{x}) - (c + d\overline{x}) = \overline{0} = I,$$

amiből $(a - c) + (b - d)x \in I$ következik. Tehát az $(a - c) + (b - d)x$ elsőfokú polinom az $x^2 + 1$ polinom többszöröse, ami csak úgy teljesülhet, ha a zérus polinom, azaz $a = c$ és $b = d$. Tehát φ injektív. Ha $\overline{f} \in \mathbf{R}[x]/I$, akkor van olyan $q, r \in \mathbf{R}[x]$, hogy $f = (x^2 + 1)q + r$, ahol r legfeljebb elsőfokú polinom, azaz $r = a + bx$ valamely $a, b \in \mathbf{R}$ esetén. Ekkor

$$\overline{f} = \overline{(x^2 + 1)q + r} = \overline{x^2 + 1} \cdot \overline{q} + \overline{r} = \overline{0} \cdot \overline{q} + \overline{r} = \overline{r} = a + b\overline{x} = (a + bi)\varphi.$$

Tehát φ szürjektív is. Legyen ismét $a + bi, c + di \in \mathbf{C}$. Ekkor

$$\begin{aligned} ((a + bi) + (c + di))\varphi &= ((a + c) + (b + d)i)\varphi = \\ &= (a + c) + (b + d)\overline{x} = (a + b\overline{x}) + (c + d\overline{x}) = (a + bi)\varphi + (c + di)\varphi. \end{aligned}$$

és

$$\begin{aligned} ((a + bi)(c + di))\varphi &= ((ac - bd) + (ad + bc)i)\varphi = (ac - bd) + (ad + bc)\overline{x} = \\ &= (ac + bd\overline{x}^2) + (ad + bc)\overline{x} = (a + b\overline{x}) \cdot (c + d\overline{x}) = (a + bi)\varphi \cdot (c + di)\varphi. \end{aligned}$$

Tehát φ felcserélhető a műveletekkel, és ezért izomorfizmus. ■

9. Irracionális, algebrai és transzcendens számok

A $\mathbf{R} \setminus \mathbf{Q}$ elemeit *irracionális számoknak* nevezzük. A halmazelmélet számosságokra vonatkozó alapismeretei szerint \mathbf{R} kontinuum számosságú, \mathbf{Q} pedig megszámlálhatóan végtelen halmaz, s ebből következően $\mathbf{R} \setminus \mathbf{Q}$ is kontinuum számosságú. Egyszerűen fogalmazva azt is mondhatjuk, hogy több irracionális szám van, mint racionális. A legegyszerűbben gyökvonással juthatunk irracionális számokhoz.

9.1. Állítás. Tetszőleges $n, k \in \mathbf{N}$ esetén $\sqrt[k]{n} \in \mathbf{Q}$ akkor és csak akkor, ha van olyan $p \in \mathbf{N}$, hogy $n = p^k$.

Bizonyítás. Ha $\sqrt[k]{n}$ racionális szám, akkor vannak olyan relatív prím $p, q \in \mathbf{N}$ számok, hogy

$$\sqrt[k]{n} = \frac{p}{q}, \quad \text{vagyis} \quad q^k n = p^k.$$

Mivel p és q relatív prímekek, ezért p^k és q^k is relatív prímekek. Ismert, hogy ha egy egész szám osztója egy szorzatnak, és a szorzat egyik tényezőjéhez relatív prím, akkor osztója a másik tényezőnek. Ezért a második egyenlőségéből $n|p^k$, $p^k|n$ és $n = p^k$ következik. ■

A valós számok tizedestört alakjáról is leolvasható, hogy racionális szám-e vagy sem.

9.2. Tétel. *Egy valós szám akkor és csak akkor racionális, ha tizedestört alakja valamelyik jegytől kezdődően periodikus.*

Bizonyítás. Egy racionális szám, azaz két egész szám hányadosának tizedestört alakjához úgy jutunk, hogy a számlálót osztjuk a nevezővel, és ha számláló jegyeiből kifogytunk, a hányadosban kiteszük a tizedes vesszőt, és a maradékhoz egy-egy 0-t írva folytatjuk az osztást. A maradék mindig az osztónál kisebb nemnegatív szám. Így az osztás során szükségképpen fel kell lépni egy olyan maradéknak, mely korábban már szerepelt. Ezért a két egyforma maradéktól kezdve a hányados jegyei rendre megegyeznek. Tehát innen kezdve, a tizedesjegyek sorozata periodikus.

Megfordítva, legyen egy u pozitív valós szám tizedestört alakja valamelyik jegytől kezdve periodikus, azaz

$$u = \overline{a_1 a_2 \dots a_k, b_1 b_2 \dots b_m c_1 c_2 \dots c_n c_1 c_2 \dots c_n \dots}$$

alakú. Legyen

$$a = \overline{a_1 a_2 \dots a_k}, \quad b = \overline{b_1 b_2 \dots b_m} \quad \text{és} \quad c = \overline{c_1 c_2 \dots c_n}.$$

Ekkor

$$10^m u = 10^m a + b + \frac{c}{10^n} + \frac{c}{10^{2n}} + \dots$$

és

$$10^{m+n} u = 10^{m+n} a + 10^n b + c + \frac{c}{10^n} + \frac{c}{10^{2n}} + \dots,$$

amiből

$$(10^{m+n} - 10^m)u = (10^{m+n} - 10^m)a + (10^n - 1)b + c$$

és

$$u = \frac{(10^{m+n} - 10^m)a + (10^n - 1)b + c}{10^{m+n} - 10^m}$$

következik. Tehát u racionális szám. ■

A következő tétel segítségével többek között az e és a π számok irracionálisát igazolhatjuk.

9.3. Tétel. *Legyen c egy pozitív valós szám és $f(x)$ egy olyan valós függvény, mely a $[0, c]$ zárt intervallumon folytonos, és a $(0, c)$ nyitott intervallumon pozitív. Legyen továbbá $f_1(x), f_2(x), \dots$ egy olyan függvény-sorozat, melyre $f_1'(x) = f(x)$ és $f_k'(x) = f_{k-1}(x)$ minden $k \geq 2$ esetén. Ha $f_k(0)$ és $f_k(c)$ egész számok, $k = 1, 2, \dots$, akkor c irracionális szám.*

Bizonyítás. Tegyük fel, hogy $c, f(x)$ és $f_1(x), f_2(x), \dots$ teljesítik a tétel feltételeit. Legyen

$$P = \{g(x) \in \mathbf{R}[x]: g^{(k)}(0), g^{(k)}(c) \in \mathbf{Z}, k = 0, 1, 2, \dots\},$$

ahol $g^{(k)}$ a g polinom k -adik deriváltja.

9.3.1. $\int_0^c f(x)g(x)dx$ egész szám minden $g(x) \in P$ esetén.

A parciális integrálás többszöri alkalmazásával kapjuk, hogy

$$\int_0^c f(x)g(x)dx = \left[f_1 g - f_2 g' + f_3 g'' - \dots + (-1)^d f_{d+1} g^{(d)} \right]_0^c,$$

ahol d g fokszáma. Ebből pedig következik 9.3.1.

Parciális deriválással azonnal adódik a következő:

9.3.2. Ha $g(x), h(x) \in P$, akkor $g(x)h(x) \in P$.

Most a tétel állításával ellentétben tegyük fel, hogy c racionális szám, azaz $c = \frac{m}{n}$, ahol m és n pozitív egész számok. Könnyen ellenőrizhető, hogy

$$m - 2nx \in P. \quad (*)$$

Legyen

$$g_k(x) = \frac{x^k(m - nx)^k}{k!}, \quad k = 0, 1, 2, \dots$$

9.3.3. $g_k(x) \in P$ minden k -ra.

Állításunk igazolása k szerinti teljes indukcióval történik. $g_0(x) = 1 \in P$ nyilvánvaló. Tegyük fel, hogy $k \geq 1$ és $g_{k-1}(x) \in P$. Mivel

$$g'_k = g_{k-1}(x)(m - 2nx),$$

ezért 9.3.2 állítást és $(*)$ -ot figyelembe véve azt kapjuk, hogy $g'_k(x) \in P$. Ebből és $g_k(0) = g_k(c) = 0$ -ból $g_k(x) \in P$ következik.

Mivel $g_k(x)$ és $f(x)$ is pozitív $(0, c)$ -n, ezért

$$\int_0^c f(x)g_k(x)dx > 0, \quad k = 0, 1, \dots$$

Ez az integrál 9.3.1 miatt egész szám, és így

$$\int_0^c f(x)g_k(x)dx \geq 1, \quad k = 0, 1, \dots \quad (**)$$

Legyen M az $x(m - nx)$ függvény maximuma $[0, c]$ -n, L pedig $f(x)$ maximuma $[0, c]$ -n. Ekkor

$$\int_0^c f(x)g_k(x)dx \leq \int_0^c L \cdot \frac{M^k}{k!} dx = c \cdot L \cdot \frac{M^k}{k!},$$

ami

$$\lim_{k \rightarrow \infty} \frac{M^k}{k!} = 0$$

miatt ellentmond $(**)$ -nak. Tehát c nem lehet racionális szám. ■

9.4. Következmény. Ha $0 < |r| \leq \pi$ és $\sin r, \cos r$ racionális számok, akkor r irracionális szám. Speciálisan π irracionális.

Bizonyítás. Ha $\sin r, \cos r$ racionális számok, akkor $\sin |r|, \cos |r|$ is racionális számok. Ezért van olyan n pozitív egész szám, hogy $n \sin |r|, n \cos |r|$ egész számok. Alkalmazva a 9.2. Tételt $c = |r|$ -re és $f(x) = n \sin x$ -re azt kapjuk, hogy $|r|$ és r irracionális számok.

9.5. Következmény. Ha $r \neq 1$ pozitív racionális szám, akkor $\ln r$ irracionális szám. e irracionális szám.

Bizonyítás. Feltehető, hogy $r > 1$, és így $\ln r > 0$. (Ellenkező esetben helyettesítsük r -et $\frac{1}{r}$ -rel.) Legyen $r = \frac{m}{n}$, ahol m és n pozitív egész számok. Alkalmazva a 9.2. Tételt $c = \ln r$ -re és $f(x) = ne^x$ -re, az első állítást kapjuk.

Ha e racionális szám volna, akkor első állításunk szerint $1 = \ln e$ irracionális lenne. Tehát e irracionális.

Az érdekeség kedvéért egy közvetlen bizonyítást is adunk arra, hogy e irracionális. Ha e racionális volna, akkor elég nagy n -ekre $n!e$ egész szám, $n!e - n! \sum_{i=0}^n \frac{1}{i!}$ pedig egy pozitív egész szám lenne. Ezért

$$1 \leq n!e - n! \sum_{i=0}^n \frac{1}{i!} = n! \left(\sum_{i=0}^{\infty} \frac{1}{i!} - \sum_{i=0}^n \frac{1}{i!} \right) =$$

$$n! \sum_{i=1}^{\infty} \frac{1}{(n+i)!} = \sum_{i=1}^{\infty} \frac{1}{(n+1) \cdots (n+i)} <$$

$$< \sum_{i=1}^{\infty} \frac{1}{(n+1)^i} = \frac{1}{n}.$$

Ez pedig $n \geq 1$ estén lehetetlen. ■

9.6. Definíció. Egy a komplex számot *algebrai számnak* nevezünk, ha van olyan $f \in \mathbf{Q}[x]$, $f \neq 0$, polinom, melyre $f(a) = 0$. Ha $a \in \mathbf{C}$ nem algebrai, akkor *transzcendens számnak* hívjuk. Jelölje \mathbf{A} az algebrai számok halmazát. (Vegyük észre, hogy $\mathbf{Q} \subseteq \mathbf{A}$.)

9.7. Tétel. Az algebrai számok \mathbf{A} halmaza megszámlálhatóan végtelen.

Bizonyítás. A bizonyításban felhasználjuk a halmazelmélet megszámlálható (véges vagy megszámlálhatóan végtelen) halmazokra vonatkozó következő eredményeit: Ha A megszámlálható halmaz és $n \in \mathbf{N}$, akkor A^n is megszámlálható halmaz. Speciálisan \mathbf{Q}^n megszámlálhatóan végtelen halmaz. Ha I és A_i , $i \in I$ megszámlálható halmazok, akkor $\bigcup_{i \in I} A_i$ is megszámlálható halmaz.

Tetszőleges $n \in \mathbf{N}$ -re jelölje P_n a legfeljebb n -edfokú racionális-együtthatós polinomok halmazát. Mivel

$$\mathbf{Q}^{n+1} \rightarrow P_n, (a_0, a_1, \dots, a_n) \mapsto a_0 + a_1x + \dots + a_nx^n$$

bijektív leképezés, P_n megszámlálható halmaz. Ezért

$$\mathbf{Q}[x] = \bigcup_{n \in \mathbf{N}} P_n$$

is megszámlálható halmaz. Tetszőleges $f \in \mathbf{Q}[x]$ -re jelölje G_f az f polinom gyökeinek halmazát. Ekkor

$$\mathbf{A} = \bigcup_{f \in \mathbf{Q}[x] \setminus \{0\}} G_f$$

miatt \mathbf{A} is megszámlálható halmaz. ■

9.8. Definíció. Egy polinomot *főpolinomnak* hívunk, ha főegyütthatója 1. Azt mondjuk, hogy az $f \in \mathbf{Q}[x]$ főpolinom az a algebrai szám *minimálpolinomja*, ha $f(a) = 0$, és a egyetlen f -nél kisebb fokú 0-tól különböző $\mathbf{Q}[x]$ -beli polinomnak sem gyöke. Az f polinom f^* fokszámát az a algebrai szám *fokának* is mondjuk. Egy algebrai szám *konjugáltjainak* minimálpolinomjának gyökeit nevezzük.

9.9. Tétel. Minden algebrai számnak egyetlen minimálpolinomja van, és az irreducibilis. Legyen a egy algebrai szám és f a minimálpolinomja. Ha valamely $g \in \mathbf{Q}[x]$ polinomra $g(a) = 0$, akkor $f|g$.

Bizonyítás. Legyen a egy algebrai szám. Azon nem nulla $\mathbf{Q}[x]$ -beli polinomok fokszámai, melyeknek a gyöke \mathbf{N} -nek egy nemüres U részhalmazát alkotják, ezért van U -nak legkisebb eleme: $n \in U$. Ha választunk egy olyan n -edfokú polinomot $\mathbf{Q}[x]$ -ből melynek a gyöke, és elosztjuk főegyütthatójával, akkor a egy

minimálpolinomját kapjuk. Legyen f az a szám egy minimálpolinomja. Legyen továbbá $g \in \mathbf{Q}[x]$ olyan polinom, hogy $g(a) = 0$. Végezzünk euklideszi osztást g -n és f -en: $g = fq + r$, $r^* < f^*$. Ekkor $r^* < f^*$ és

$$r(a) = g(a) - f(a)q(a) = 0$$

miatt $r = 0$ és $f|g$. Ha a -nak g is minimálpolinomja, akkor $f|g$ és $g|f$. Ezért valamely t racionális számra $g = tf$. Mivel mindkét polinom főpolinom, szükségképpen $t = 1$, és így $g = f$. Ezzel az egyértelműséget is igazoltuk.

Ha $f = gh$, $g, h \in \mathbf{Q}[x]$, akkor $g^*, h^* \leq f^*$. Továbbá $g(a)h(a) = f(a) = 0$ miatt $g(a) = 0$ vagy $h(a) = 0$. Az első esetben $f|g$, amiből $f^* \leq g^*$, $f^* = g^*$ és $h^* = 0$ következik. A második esetben hasonlóan kapjuk, hogy $f^* = h^*$ és $g^* = 0$. Tehát f irreducibilis. ■

9.10. Tétel. *Az algebrai számok testet alkotnak az összeadásra és szorzásra, azaz ha a és b algebrai számok, akkor $a + b$, $a - b$, ab is algebrai számok, és amennyiben $a \neq 0$, akkor $\frac{1}{a}$ is algebrai szám. Sőt az algebrai számok teste algebrailag zárt, azaz bármely $f \in \mathbf{A}[x]$ polinomnak van gyöke \mathbf{A} -ban.*

Bizonyítás. Legyen a egy m -edfokú, b pedig egy n -edfokú algebrai szám, s legyenek f és g a megfelelő minimálpolinomok. Legyenek továbbá a konjugáltjai $a_1 = a, \dots, a_m$, b konjugáltjai pedig $b_1 = b, \dots, b_n$. Tekintsük a következő három polinomot:

$$f_{a+b}(x) = \prod_{i=1}^m \prod_{j=1}^n (x - (a_i + b_j)), \quad f_{a-b}(x) = \prod_{i=1}^m \prod_{j=1}^n (x - (a_i - b_j))$$

és

$$f_{ab}(x) = \prod_{i=1}^m \prod_{j=1}^n (x - a_i b_j).$$

Világos, hogy $f_{a+b}(a+b) = f_{a-b}(a-b) = f_{ab}(ab) = 0$. Ha belátjuk, hogy mindhárom polinom $\mathbf{Q}[x]$ -ben van, akkor azzal igazoljuk, hogy $a+b$, $a-b$ és ab algebrai számok. Jelölje h a három polinom valamelyikét. Írjuk fel h -t x hatványai szerint, s jelölje c valamelyik együtthatóját. Világos, hogy valamely $r \in \mathbf{Q}[x_1, \dots, x_m, y_1, \dots, y_n]$ polinomra

$$c = q(a_1, \dots, a_m, b_1, \dots, b_n).$$

Másrészt az is nyilvánvaló, hogy h invariáns az a_1, \dots, a_m , illetve b_1, \dots, b_n elemek bármely permutációjára, s ezért ugyanez teljesül az q polinomra is. Ezért a több határozatlanrendszerre szimmetrikus polinomok alaptétele szerint van olyan $r \in \mathbf{Q}[x_1, \dots, x_m, y_1, \dots, y_n]$, hogy

$$q = r(\sigma_1, \dots, \sigma_m, \tau_1, \dots, \tau_n),$$

ahol $\sigma_1, \dots, \sigma_m$, illetve τ_1, \dots, τ_n az x_1, \dots, x_m , illetve y_1, \dots, y_n határozatlanok elemi szimmetrikus polinomjai. A polinomok gyökei és együtthatói közötti ismert összefüggéseket figyelembe véve azt kapjuk, hogy minden i -re és j -re

$$\sigma_i(a_1, \dots, a_m), \quad \text{illetve} \quad \tau_j(b_1, \dots, b_n)$$

előjeltől eltekintve az f , illetve a g polinom két együtthatójának hányadosa, s ezért racionális számok. Emiatt

$$c = r(\sigma_1(a_1, \dots, a_m), \dots, \sigma_m(a_1, \dots, a_m), \tau_1(b_1, \dots, b_n), \dots, \tau_n(b_1, \dots, b_n))$$

is racionális szám. Ezzel beláttuk, hogy $h (= f_{a+b}, f_{a-b}, f_{ab})$ együtthatói racionális számok.

Ha $a \neq 0$ és $f(x) = c_0 + c_1x + \dots + c_mx^m$, akkor

$$c_0 \left(\frac{1}{a}\right)^m + c_1 \left(\frac{1}{a}\right)^{m-1} + \dots + c_n = \frac{1}{a^m} (c_0 + c_1a + \dots + c_ma^m) = \frac{1}{a^m} f(a) = 0,$$

amiből $\frac{1}{a} \in \mathbf{A}$ következik.

Végül legyen $f(x) = a_0 + a_1x + \dots + a_nx^n \in \mathbf{A}[x]$, s legyenek $a_{i1} = a_i, a_{i2}, \dots, a_{ik_i}$ az a_i algebrai szám konjugáltjai ($i = 0, \dots, n$). Tekintsük az

$$F(x) = \prod_{i_0=1}^{k_0} \prod_{i_1=1}^{k_1} \dots \prod_{i_n=1}^{k_n} (a_{0i_0} + a_{1i_1}x + \dots + a_{ni_n}x^n)$$

polinomot. Mivel f szerepel F tényezői között, ezért f minden gyöke F -nek is gyöke. A h polinomra vonatkozó gondolatmenet kis módosításával belátható, hogy $F \in \mathbf{Q}[x]$. Ezért gyökeivel együtt f gyökei is algebrai számok. Tehát \mathbf{A} algebrailag zárt test. ■

Mivel \mathbf{C} kontinuum számosságú, \mathbf{A} pedig megszámlálhatóan végtelen halmaz, a transzcendens számok $\mathbf{C} \setminus \mathbf{A}$ halmaza is kontinuum számosságú. Egyszerűen fogalmazva azt is mondhatjuk, hogy több transzcendens szám van, mint algebrai. Ezek után azt várná az olvasó, hogy könnyen lehet konkrét példákat adni transzcendens számokra. Ez azonban nem így van. Az egyszerűnek látszó esetekben is komoly munkát igényel a transzcendencia igazolása.

9.11. Definíció. Azt mondjuk, hogy a ξ valós szám n -ed rendben approximálható racionális számokkal, ha létezik olyan csak ξ -től függő K_ξ valós szám, hogy a

$$\left| \frac{p}{q} - \xi \right| < \frac{K_\xi}{q^n}$$

egyenlőtlenségnek végtelen sok $\frac{p}{q}$ megoldása van ($p, q \in \mathbf{Z}$).

9.12. Tétel. A racionális számok 1 rendben approximálhatók, de nagyobb rendben nem.

Bizonyítás. Legyen $\xi = \frac{a}{b}$, ahol $a, b \in \mathbf{Z}$, $b > 0$, $(a, b) = 1$ és $K_\xi = \frac{2}{b}$. A kétismeretlenes diofantoszi egyenletekre vonatkozó ismereteket és $(a, b) = 1$ -et figyelembe véve, a $bp - aq = 1$ egyenletnek végtelen sok olyan megoldása van \mathbf{Z} -ben, melyre $q > 0$. Ezért végtelen sok $\frac{p}{q}$ racionális számra

$$\left| \frac{p}{q} - \xi \right| = \left| \frac{p}{q} - \frac{a}{b} \right| = \frac{1}{bq} < \frac{K_\xi}{q}.$$

Tegyük fel, hogy valamely K_ξ és $p, q \in \mathbf{Z}$, $q > 0$, esetén

$$\left| \frac{p}{q} - \xi \right| < \frac{K_\xi}{q^n}, \quad n > 1. \quad (*)$$

Ekkor $\frac{p}{q} \neq \xi$ esetén

$$\frac{1}{bq} \leq \frac{|bp - aq|}{bq} = \left| \frac{p}{q} - \xi \right| < \frac{K_\xi}{q^n},$$

mi csak véges sok q -ra teljesül. Ezért (*) is csak véges sok $\frac{p}{q}$ racionális számra igaz. ■

9.13. Liouville-tétel. Bármely ξ n -edfokú valós algebrai számhoz van olyan $C_\xi \in \mathbf{R}^+$, melyre

$$\left| \frac{p}{q} - \xi \right| > \frac{C_\xi}{|q|^n}$$

minden $p, q \in \mathbf{Z}$, $q \neq 0$, esetén a $\xi = \frac{p}{q}$ triviális esetet leszámítva (ami nyilván csak $n = 1$ esetén lehetséges).

Bizonyítás. Legyen ξ egy n -edrendű valós algebrai szám, Ha $n = 1$, akkor ξ racionális szám. Ebben az esetben az állítást a 9.12. Tétel bizonyítása során már megkaptuk. Ha $n > 1$, akkor ξ nem racionális, s minimálpolinomját alkalmas egész számmal megszorozva egész együtthatós polinomot kapunk. Legyen egy ilyen polinom $f(x) = a_0 + a_1x + \dots + a_nx^n$. Mivel $f(x)$ irreducibilis, nincs racionális gyöke. Az $I = [\xi - 1, \xi + 1]$ zárt intervallumban $f'(x)$ korlátos, vagyis létezik olyan M , melyre $|f'(x)| < M$ minden $x \in I$ -re. Legyen $C_\xi = \min(\frac{1}{M}, 1)$. Ekkor a $\frac{p}{q} \notin I$ racionális számokra

$$\left| \frac{p}{q} - \xi \right| > 1 \geq \frac{C_\xi}{|q|^n}.$$

Ha pedig $\frac{p}{q} \in I$, akkor

$$\left| f\left(\frac{p}{q}\right) \right| = \frac{|a_0q^n + a_1pq^{n-1} + \dots + a_np^n|}{|q|^n} \geq \frac{1}{|q|^n}.$$

Alkalmazzuk a Lagrange-féle középértéktételt:

$$f\left(\frac{p}{q}\right) = f\left(\frac{p}{q}\right) - f(\xi) = \left(\frac{p}{q} - \xi\right)f'(a)$$

valamely $a \in I$ számra. Ezt felhasználva

$$\left| \frac{p}{q} - \xi \right| = \frac{f\left(\frac{p}{q}\right)}{|f'(a)|} > \frac{1}{M|q|^n} \geq \frac{C_\xi}{|q|^n}.$$

■

9.14. Következmény. Az n -edrendű valós algebrai számok nem approximálhatók n -nél nagyobb rendben.

Liouville tétele alapján példát adhatunk transzcendens számra:

9.15. Tétel. Az $\alpha = \sum_{n=1}^{\infty} \frac{1}{10^{n!}}$ szám transzcendens.

Bizonyítás. Tekintsük a $p_k = 10^{k!} \sum_{l=1}^k \frac{1}{10^{l!}}$ és $q_k = 10^{k!}$, $k = 1, 2, \dots$, egész számokat. Tegyük fel, hogy α algebrai szám, és legyen n a foka. Ekkor $\frac{p_k}{q_k} \neq \alpha$, és Liouville tétele szerint valamely $C_\alpha \in \mathbf{R}^+$ számra

$$\begin{aligned} \frac{C_\alpha}{10^{n \cdot k!}} &= \frac{C_\alpha}{|q_k|^n} < \left| \frac{p_k}{q_k} - \alpha \right| = \sum_{l=k+1}^{\infty} \frac{1}{10^{l!}} < \\ &< \frac{1}{10^{(k+1)!}} \left(1 + \frac{1}{10} + \frac{1}{10^2} + \dots \right) = \frac{10}{9 \cdot 10^{(k+1)!}}, \quad k = 1, 2, \dots \end{aligned}$$

Ebből minden $k > n$ számra

$$C_\alpha < \frac{10 \cdot 10^{n \cdot k!}}{9 \cdot 10^{(k+1)!}} < \frac{2}{10^{(k+1)! - n \cdot k!}} = \frac{2}{10^{k!((k+1)-n)}} < \frac{2}{10^{k!}}$$

következik. Mivel ez elég nagy k -ra nem igaz, α nem lehet algebrai. ■

10. Algebrák

10.1. Definíció. Legyen K egy test és $(R; +, \cdot)$ egy nem-asszociatív gyűrű. Azt mondjuk, hogy R algebra a K test felett, ha értelmezve van R elemeinek a K test elemeivel való szorzása úgy, hogy azzal $(R; +)$ vektorteret alkot K felett, valamint bármely $a, b \in R$ és $\lambda \in K$ esetén $\lambda(ab) = (\lambda a)b = a(\lambda b)$. Röviden azt is szoktuk mondani, hogy R K -algebra. Ha az algebrának egyetlen eleme van, akkor *triviális algebrának* nevezzük. Ha R — mint vektortér — véges dimenziós (n -dimenziós), akkor *véges rangú* (n *rangú*) algebrának nevezzük. (Vegyük észre, hogy egy algebra pontosan akkor 0 rangú, ha triviális.) Ha a szorzás asszociatív, akkor R -et *asszociatív algebrának* nevezzük.

Valamely R K -algebra egy nemüres S részhalmazát *részalgebrájának* nevezzük, ha S zárt az összeadásra, a szorzásra és K elemeivel való szorzásra. Könnyű belátni, hogy részalgebrák metszete is részalgebra. Ha $X \subseteq R$, akkor az X -nél bővebb részalgebrák metszetét az X által *generált részalgebrának* nevezzük. Az R algebra (illetve gyűrű) *centrumának* az

$$\mathcal{C}(R) = \{x \in R: \forall a \in R \text{ esetén } xa = ax\}$$

részhalmazát nevezzük. Könnyen ellenőrizhető, hogy $\mathcal{C}(R)$ részalgebra (illetve részgyűrű). Ha R — mint gyűrű — kommutatív, egységelemes, illetve zérus-osztómentes, akkor R -et *kommutatív, egységelemes, illetve zérusosztómentes algebrának* hívjuk.

10.2. Példa. Legyen R egy egységelemes nem-asszociatív gyűrű és K olyan részteste R -nek, mely R centrumában van. Ekkor R tekinthető K -algebrának, hiszen a feltételek miatt R elemeit lehet szorozni K elemeivel, és az algebra definíciójában szereplő tulajdonságok nyilvánvalóan teljesülnek. Speciális esetként adódnak a következő példák:

- (1) \mathbf{R} végtelen rangú \mathbf{Q} -algebra, melyben az $\{a + b\sqrt{2}: a, b \in \mathbf{Q}\}$ halmaz 2 rangú részalgebra. \mathbf{C} 2 rangú \mathbf{R} -algebra.
- (2) Ha K egy test, és $K(a)$ a K test a elemmel való testbővítése, akkor $K(a)$ végesrangú vagy végtelen rangú K -algebra aszerint, hogy a algebrai vagy transzcendens elem K felett.
- (3) Egy K test feletti n határozatlanú polinomok $K[x_1, \dots, x_n]$ gyűrűje végtelen rangú K -algebra ($n \geq 1$). Ha $f \in K[x_1, \dots, x_n]$, akkor az $\{fg: g \in K[x_1, \dots, x_n]\}$ részhalmaz részalgebra, mely csak akkor egységelemes, ha f konstans polinom.
- (4) Legyen K egy test, $K_{n \times n}$ pedig a K feletti $n \times n$ -es mátrixok gyűrűje. A $K \rightarrow K_{n \times n}$, $\lambda \mapsto \lambda E$, leképezés — ahol E az egységmátrixot jelöli — K beágyazása $K_{n \times n}$ -be. Ezért tekinthetjük K -t $K_{n \times n}$ résztestének, és ekkor $K_{n \times n}$ n^2 -dimenziós K -algebra.

10.3. Tétel. Legyen K egy test és R egy egységelemes nem-triviális K -algebra az e multiplikatív egységelemmel. Ekkor a $\varphi: K \rightarrow R$, $\lambda \mapsto \lambda e$ leképezés K beágyazása R -be, és bármely $\lambda \in K$ és $a \in R$ esetén $\lambda a = (\lambda e)a$ és $\lambda e \in \mathcal{C}(R)$.

Bizonyítás. Mivel R nem-triviális algebra, $e \neq 0$. Ha $\lambda, \mu \in K$ és $\lambda\varphi = \mu\varphi$, azaz $\lambda e = \mu e$, akkor $(\lambda - \mu)e = 0$, amiből $\lambda - \mu = 0$ és $\lambda = \mu$ következik. Tehát φ injektív. Legyen ismét $\lambda, \mu \in K$. Ekkor

$$(\lambda + \mu)\varphi = (\lambda + \mu)e = \lambda e + \mu e = \lambda\varphi + \mu\varphi$$

és

$$(\lambda\mu)\varphi = (\lambda\mu)e = \lambda(\mu e) = \lambda(e(\mu e)) = (\lambda e)(\mu e) = (\lambda\varphi)(\mu\varphi),$$

és ezért φ beágyazás. Végül ha $\lambda \in K$ és $a \in R$, akkor $(\lambda e)a = e(\lambda a) = \lambda a = (\lambda a)e = a(\lambda e)$, azaz $\lambda e \in \mathcal{C}(R)$. ■

10.4. Megjegyzés. A 10.3. Tétel az R egységelemes nem-triviális K -algebrákba oly módon ágyazta be a K testet, hogy a képelemek R centrumába estek, és K bármely λ elemével való szorzás megegyezik λ beágyazás melletti képével való szorzással. Így K elemeit azonosíthatjuk a beágyazás melletti képükkel, és ezért feltehetjük, hogy $K \subseteq R$. Tehát minden egységelemes nem-triviális algebra a 10.2. Példa speciális esete.

10.5. Tétel. Legyen $(R; +)$ egy n -dimenziós vektortér a K test felett, és a_1, \dots, a_n R egy bázisa. Legyenek továbbá adottak a $c_{ij} \in R$ ($i, j = 1, \dots, n$) elemek. Definiáljuk a szorzást R -en két lépésben:

$$a_i a_j = c_{ij}, \quad i, j = 1, \dots, n$$

és

$$\left(\sum_{i=1}^n \lambda_i a_i \right) \left(\sum_{i=1}^n \mu_i a_i \right) = \sum_{k=1}^n \sum_{l=1}^n (\lambda_k \mu_l) (a_k a_l), \quad \lambda_i, \mu_i \in K, \quad i = 1, \dots, n.$$

Ezzel a szorzással R egy K -algebra lett. Ha bármely $i \in \{1, \dots, n\}$ esetén $a_1 a_i = a_i a_1 = a_i$, akkor a_1 R multiplikatív egységeleme. Ha bármely $i, j, k \in \{1, \dots, n\}$ esetén $(a_i a_j) a_k = a_i (a_j a_k)$, akkor R szorzása asszociatív. Ha bármely $i, j \in \{1, \dots, n\}$ esetén $a_i a_j = a_j a_i$, akkor R szorzása kommutatív.

Bizonyítás. Az első állításhoz csak azt kell megmutatni, hogy bármely $a, b, c \in R$ és $\lambda \in K$ esetén $\lambda(ab) = (\lambda a)b = a(\lambda b)$, $a(b+c) = ac+bc$ és $(a+b)c = ac+bc$. Legyen

$$a = \sum_{i=1}^n \lambda_i a_i, \quad b = \sum_{i=1}^n \mu_i a_i \quad \text{és} \quad c = \sum_{i=1}^n \nu_i a_i, \quad \lambda_i, \mu_i, \nu_i \in K, \quad i = 1, \dots, n.$$

Ekkor

$$\begin{aligned} a(b+c) &= \left(\sum_{i=1}^n \lambda_i a_i \right) \left(\sum_{i=1}^n \mu_i a_i + \sum_{i=1}^n \nu_i a_i \right) = \left(\sum_{i=1}^n \lambda_i a_i \right) \left(\sum_{i=1}^n (\mu_i + \nu_i) a_i \right) = \\ &= \sum_{k=1}^n \sum_{l=1}^n (\lambda_k (\mu_l + \nu_l)) (a_k a_l) = \sum_{k=1}^n \sum_{l=1}^n (\lambda_k \mu_l + \lambda_k \nu_l) (a_k a_l) = \\ &= \sum_{k=1}^n \sum_{l=1}^n (\lambda_k \mu_l) (a_k a_l) + \sum_{k=1}^n \sum_{l=1}^n (\lambda_k \nu_l) (a_k a_l) = \\ &= \left(\sum_{i=1}^n \lambda_i a_i \right) \left(\sum_{i=1}^n \mu_i a_i \right) + \left(\sum_{i=1}^n \lambda_i a_i \right) \left(\sum_{i=1}^n \nu_i a_i \right) = ab + ac. \end{aligned}$$

Az $(a+b)c = ac+bc$ és $\lambda(ab) = (\lambda a)b = a(\lambda b)$ egyenlőségeket hasonlóan igazolhatjuk.

Tegyük fel, hogy bármely $i \in \{1, \dots, n\}$ esetén $a_1 a_i = a_i a_1 = a_i$, és legyen $a = \sum_{i=1}^n \lambda_i a_i \in R$. Ekkor

$$a_1 a = a_1 \left(\sum_{i=1}^n \lambda_i a_i \right) = \sum_{i=1}^n a_1 (\lambda_i a_i) = \sum_{i=1}^n \lambda_i (a_1 a_i) = \sum_{i=1}^n \lambda_i a_i = a$$

és

$$a a_1 = \left(\sum_{i=1}^n \lambda_i a_i \right) a_1 = \sum_{i=1}^n (\lambda_i a_i) a_1 = \sum_{i=1}^n \lambda_i (a_i a_1) = \sum_{i=1}^n \lambda_i a_i = a.$$

Tehát a_1 R multiplikatív egységeleme.

A szorzás asszociativitásának igazolásához tegyük fel, hogy bármely $i, j, k \in \{1, \dots, n\}$ esetén $(a_i a_j) a_k = a_i (a_j a_k)$, és legyen

$$U = \{(a, b, c) \in R^3 : (ab)c = a(bc)\}.$$

Vegyük észre, hogy ha $(a, b, c), (\bar{a}, b, c), (a, \bar{b}, c), (a, b, \bar{c}) \in U$ és $\lambda \in K$, akkor $(\lambda a, b, c), (a, \lambda b, c), (a, b, \lambda c), (a + \bar{a}, b, c), (a, b + \bar{b}, c), (a, b, c + \bar{c}) \in U$, mert

$$\begin{aligned} ((\lambda a)b)c &= (a(\lambda b))c = (\lambda(ab))c = (ab)(\lambda c) = \lambda((ab)c) = \\ &= \lambda(a(bc)) = (\lambda a)(bc) = a(\lambda(bc)) = a((\lambda b)c) = a(b(\lambda c)), \end{aligned}$$

$$(a + \bar{a})(bc) = a(bc) + \bar{a}(bc) = (ab)c + (\bar{a}b)c = (ab + \bar{a}b)c = ((a + \bar{a})b)c,$$

$$a((b + \bar{b})c) = a(bc + \bar{b}c) = a(bc) + a(\bar{b}c) = (ab)c + (a\bar{b})c = (ab + a\bar{b})c = (a(b + \bar{b}))c$$

és

$$a(b(c + \bar{c})) = a(bc + b\bar{c}) = a(bc) + a(b\bar{c}) = (ab)c + (ab)\bar{c} = (ab)(c + \bar{c}).$$

A feltevésünk szerint bármely $i, j, k \in \{1, \dots, n\}$ esetén $(a_i, a_j, a_k) \in U$. Továbbá R minden eleme megkapható az a_1, \dots, a_n báziselemekből az összeadás és K -beli elemekkel való szorzás véges számú alkalmazásával. Ezt és az előbbi észrevételt figyelembe véve adódik, hogy $U = R^3$, ami a szorzás asszociativitását jelenti.

Végül a szorzás kommutativitásának igazolásához tegyük fel, hogy bármely $i, j \in \{1, \dots, n\}$ esetén $a_i a_j = a_j a_i$, és legyen $a = \sum_{i=1}^n \lambda_i a_i$, $b = \sum_{i=1}^n \mu_i a_i \in R$. Ekkor

$$ab = \left(\sum_{i=1}^n \lambda_i a_i \right) \left(\sum_{i=1}^n \mu_i a_i \right) = \sum_{k=1}^n \sum_{l=1}^n (\lambda_k \mu_l) (a_k a_l) =$$

$$= \sum_{l=1}^n \sum_{k=1}^n (\mu_l \lambda_k) (a_l a_k) = \left(\sum_{i=1}^n \mu_i a_i \right) \left(\sum_{i=1}^n \lambda_i a_i \right) = ba.$$

■

10.6. Tétel. Legyen R és S két n rangú K -algebra. Legyen továbbá a_1, \dots, a_n és b_1, \dots, b_n R és S olyan bázisai, hogy bármely $i, j \in \{1, \dots, n\}$ esetén valahányszor $a_i a_j = \sum_{k=1}^n \lambda_k a_k$, mindannyiszor $b_i b_j = \sum_{k=1}^n \lambda_k b_k$. Ekkor R és S izomorf algebrák.

Bizonyítás. Lineáris algebra tanulmányainkból tudjuk, hogy a

$$\varphi: R \rightarrow S, \quad \sum_{i=1}^n \lambda_i a_i \mapsto \sum_{i=1}^n \lambda_i b_i$$

leképezés vektortér izomorfizmus. Legyen

$$a_i a_j = \sum_{k=1}^n \lambda_k^{ij} a_k, \quad i, j = 1, \dots, n$$

és $a = \sum_{i=1}^n \lambda_i a_i$, $b = \sum_{i=1}^n \mu_i a_i \in R$. Ekkor a tétel feltételei szerint

$$b_i b_j = \sum_{k=1}^n \lambda_k^{ij} b_k, \quad i, j = 1, \dots, n$$

és ezért

$$(ab)\varphi = \left(\left(\sum_{i=1}^n \lambda_i a_i \right) \left(\sum_{i=1}^n \mu_i a_i \right) \right) \varphi = \left(\sum_{i=1}^n \sum_{j=1}^n (\lambda_i \mu_j) (a_i a_j) \right) \varphi =$$

$$= \left(\sum_{i=1}^n \sum_{j=1}^n (\lambda_i \mu_j) \left(\sum_{k=1}^n \lambda_k^{ij} a_k \right) \right) \varphi = \left(\sum_{k=1}^n \left(\sum_{i=1}^n \sum_{j=1}^n (\lambda_i \mu_j \lambda_k^{ij}) a_k \right) \right) \varphi =$$

$$= \sum_{k=1}^n \left(\sum_{i=1}^n \sum_{j=1}^n (\lambda_i \mu_j \lambda_k^{ij}) \right) b_k = \sum_{i=1}^n \sum_{j=1}^n (\lambda_i \mu_j) \left(\sum_{k=1}^n \lambda_k^{ij} b_k \right) =$$

$$= \sum_{i=1}^n \sum_{j=1}^n (\lambda_i \mu_j) (b_i b_j) = \left(\sum_{i=1}^n \lambda_i b_i \right) \left(\sum_{i=1}^n \mu_i b_i \right) = (a\varphi)(b\varphi).$$

■

10.7. Megjegyzés. A 10.5 és a 10.6 tételek szerint egy végesrangú K -algebra definiálásához elegendő megadni a báziselemeket és bármely két báziselem szorzatát. Ugyanis, ha a báziselemek a_1, \dots, a_n , akkor az algebra tartóhalmaza a $\sum_{i=1}^n \lambda_i a_i$ kifejezések halmaza, mely természetes módon alkot n -dimenzós vektorteret, és a szorzás 10.5 Tételben megadott módon való kiterjesztésével K -algebra lesz.

10.8. Példa. Legyen K egy test és $(\{a_1, \dots, a_n\}; \cdot)$ egy n -elemű félcsoport. Legyen az algebra bázisa a_1, \dots, a_n , és a báziselemek szorzata legyen a félcsoportbeli szorzat. Ily módon egy asszociatív algebrát kapunk.

10.9. Definíció. Legyen K egy test és R egy K -algebra. Tetszőleges $a, b, c \in R$ esetén az

$$[a, b, c] = (ab)c - a(bc)$$

R -beli elemet az a, b, c elemek asszociátorának nevezzük. (Világos, hogy R pontosan akkor asszociatív, ha bármely $a, b, c \in R$ esetén $[a, b, c] = 0$.) Az R algebrát *alternatív algebrának* nevezzük, ha bármely $a, b, c \in R$ elemekre

$$[a, b, c] = -[b, a, c] = -[c, b, a] = -[a, c, b].$$

10.10. Tétel. Legyen R egy K -algebra. Tetszőleges $a, b, c, u \in R$ és $\lambda \in K$ esetén

$$[\lambda a, b, c] = [a, \lambda b, c] = [a, b, \lambda c] = \lambda [a, b, c], \quad [a + u, b, c] = [a, b, c] + [u, b, c],$$

$$[a, b + u, c] = [a, b, c] + [a, u, c], \quad \text{és} \quad [a, b, c + u] = [a, b, c] + [a, b, u].$$

Ha R alternatív algebra, és K karakterisztikája nem 2, akkor

$$a(ab) = (aa)b \quad \text{és} \quad a(bb) = (ab)b, \quad a, b \in R. \quad (*)$$

Megfordítva, ha R -re teljesül $(*)$, akkor alternatív algebra.

Bizonyítás. Az első állítás igazolása pusztán számolást igényel, s ezért az olvasóra bízunk. Tegyük fel, hogy R alternatív algebra, és K karakterisztikája nem 2. Ekkor felcserélve az első két tagot $[a, a, b]$ -ben azt kapjuk, hogy $[a, a, b] = -[a, a, b]$, $2[a, a, b] = 0$ és $[a, a, b] = 0$, azaz $(aa)b = a(ab)$. A másik egyenlőség hasonlóan igazolható.

Most tegyük fel, hogy $(*)$ teljesül. Ekkor $[a, a, b] = [a, b, b] = 0$ minden $a, b \in R$ -re. Ezért

$$\begin{aligned} [a, b, a] &= ([a, a, a] + [a, a, b]) + ([a, b, a] + [a, b, b]) = \\ &= [a, a, a + b] + [a, b, a + b] = [a, a + b, a + b] = 0, \end{aligned}$$

vagyis $(ab)a = a(ba)$. Ezt felhasználva

$$\begin{aligned} [a, b, c] + [a, c, b] &= ([a, b, b] + [a, b, c]) + ([a, c, b] + [a, c, c]) = \\ &= [a, b, b + c] + [a, c, b + c] = [a, b + c, a + b] = 0, \end{aligned}$$

és $[a, b, c] = -[a, c, b]$. Hasonlóan igazolható $[a, b, c] = -[c, b, a]$ és $[a, b, c] = -[a, c, b]$. ■

Az alternatív algebrákra fontos példa a Cayley-algebra, melyet a következő fejezetben adunk meg.

11. Hiperkomplex rendszerek

11.1. Definíció. Ha R egy egységelemes nem-triviális végesrangú \mathbf{R} -algebra, akkor röviden *hiperkomplex rendszernek*, elemeit pedig *hiperkomplex számoknak* nevezzük. A 10.4. Megjegyzés szerint R centruma tartalmazza \mathbf{R} -et úgy, hogy $1 \in \mathbf{R}$ egyben R -nek is multiplikatív egységeleme.

A 10.7. Megjegyzés szerint egy hiperkomplex rendszer definiálásához elegendő megadni a báziselemeket és bármely két báziselem szorzatát. Az egyszerűség kedvéért első báziselemnek mindig 1 -et, a multiplikatív egységelemet választjuk. Így csak a többi báziselem szorzatát kell megadni.

11.2. Tétel. *Bármely 2 rangú hiperkomplex rendszer izomorfiától eltekintve a következő három lehet:*

- (1) *A báziselemek $1, i$ és $i^2 = -1$ (ezek a komplex számok).*
- (2) *A báziselemek $1, i$ és $i^2 = 1$ (ezek a hiperbolikus komplex számok).*
- (3) *A báziselemek $1, i$ és $i^2 = 0$ (ezek a Study-féle számok).*

Bizonyítás. Legyen az R 2 rangú hiperkomplex rendszer egy bázisa $1, a$ és $a^2 = x + ya$, $x, y \in \mathbf{R}$. Az $a^2 = x + ya$ egyenlőségből átrendezéssel

$$\left(-\frac{y}{2} + a\right)^2 = x + \frac{y^2}{4}$$

adódik. Három eset lehetséges.

(1) $x + \frac{y^2}{4} = -u^2$, $u \in \mathbf{R}$, $u \neq 0$. Legyen $i = -\frac{y}{2u} + \frac{1}{u}a$. Ekkor $1, i$ is bázis és $i^2 = -1$. Tehát R izomorf a komplex számok testével.

(2) $x + \frac{y^2}{4} = u^2$, $u \in \mathbf{R}$, $u \neq 0$. Ha $i = -\frac{y}{2u} + \frac{1}{u}a$, akkor $1, i$ bázis és $i^2 = 1$. Tehát R izomorf a hiperbolikus komplex számok algebrájával.

(3) $x + \frac{y^2}{4} = 0$. Ha $i = -\frac{y}{2} + a$, akkor $1, i$ bázis és $i^2 = 0$. Tehát R izomorf a Study-féle számok algebrájával. ■

A komplex számok tulajdonságait elég részletesen elemeztük a nyolcadik és kilencedik fejezetben. A hiperbolikus komplex számok és a Study-féle számok szorzása a 10.5. Tétel szerint ugyan asszociatív és kommutatív, de nem zérusosztómentes. Így ők kevésbé érdekesek.

11.3. Példa. (A kvaterniók ferdeteste.) Legyen \mathbf{K} olyan 4 rangú hiperkomplex rendszer, melynek egy bázisa $1, i, j, k$, valamint $i^2 = j^2 = k^2 = -1$, $ij = -ji = k$, $jk = -kj = i$ és $ki = -ik = j$. Világos, hogy \mathbf{K} szorzása nem kommutatív, s könnyen ellenőrizhető, hogy a báziselemeken a szorzás asszociatív. Ezért a 10.5. Tétel szerint \mathbf{K} szorzása asszociatív. \mathbf{K} elemeit *kvaternióknak* nevezzük. Ha $a = \lambda + \mu i + \nu j + \tau k \in \mathbf{K}$, akkor λ -t a *valós részének*, $\mu i + \nu j + \tau k$ -t pedig a *képzetes részének* nevezzük, és őket rendre $\mathcal{R}(a)$ és $\mathcal{I}(a)$ jelöli. Ha $\lambda = 0$, akkor azt mondjuk, hogy a *tiszta képzetes kvaternió*.

Az $\bar{a} = \lambda - \mu i - \nu j - \tau k$ elemet a *konjugáltjának* nevezzük. Könnyű ellenőrizni, hogy $a\bar{a} = \bar{a}a = \lambda^2 + \mu^2 + \nu^2 + \tau^2$. Az a elem *abszolútértéke* legyen $|a| = \sqrt{a\bar{a}}$. Ha $a \neq 0$, akkor $|a|^2 \neq 0$, és így

$$a\left(\frac{1}{|a|^2}\bar{a}\right) = \frac{1}{|a|^2}(a\bar{a}) = 1 = \frac{1}{|a|^2}(\bar{a}a) = \left(\frac{1}{|a|^2}\bar{a}\right)a.$$

Ezért az a elemnek $\frac{1}{|a|^2}\bar{a}$ a multiplikatív inverze. Tehát \mathbf{K} ferdetest.

Összefoglaljuk a kvaterniók aritmetikájára vonatkozó legfontosabb tényeket.

11.4. Tétel. Bármely nullától különböző $a \in \mathbf{K}$ -ra az $a \in \mathbf{R}$, $\bar{a} = a$ és $a^2 \in \mathbf{R}^+$, illetve az $\mathcal{R}(a) = 0$, $\bar{a} = -a$ és $a^2 \in \mathbf{R}^-$ állítások ekvivalensek. Továbbá bármely $a, b, c \in \mathbf{K}$ és $\lambda \in \mathbf{R}$ esetén

$$\overline{\lambda a} = \lambda \bar{a}, \quad \overline{\bar{a}} = a, \quad |a| = |\bar{a}|, \quad a\bar{a} = \bar{a}a = |a|^2, \quad \overline{a+b} = \bar{a} + \bar{b},$$

$$\overline{ab} = \bar{b} \cdot \bar{a}, \quad |ab| = |a||b|, \quad \overline{\frac{1}{a}} = \frac{1}{\bar{a}} \quad (a \neq 0) \quad \text{és} \quad |a+b| \leq |a| + |b|.$$

Bizonyítás. Legyen $a \in \mathbf{K}$, $a \neq 0$. Az nyilvánvaló, hogy az $a \in \mathbf{R}$ és $\bar{a} = a$, illetve az $\mathcal{R}(a) = 0$ és $\bar{a} = -a$ állítások ekvivalensek. Továbbá egyrészt $\bar{a} = a$, illetve $\bar{a} = -a$ esetén $a^2 = |a|^2 \in \mathbf{R}^+$, illetve $a^2 = -a(-a) = -a\bar{a} = |a|^2 \in \mathbf{R}^-$. Másrészt, ha $a^2 \in \mathbf{R}$, akkor

$$(a - \bar{a})(a + \bar{a}) = a^2 + a\bar{a} - \bar{a}a - \bar{a}^2 = a^2 + |a|^2 - |a|^2 - \bar{a}^2 = a^2 - \bar{a}^2 = 0,$$

amiből $a = \bar{a}$ vagy $a = -\bar{a}$ következik, vagyis $a \in \mathbf{R}$ vagy $\mathcal{R}(a) = 0$. Ezért az előző megfontolásokat is figyelembe véve azt kapjuk, hogy $a^2 \in \mathbf{R}^+$ esetén a valós, $a^2 \in \mathbf{R}^-$ esetén pedig a tiszta képzetes.

A tétel első kiemelt sorába írt összefüggések egyszerű számolással adódnak, s ezért nem részletezzük őket. Legyen $a = x + yi + zi + ti$, $b = p + qi + rj + sk$ ($x, y, z, t, p, q, r, s, t \in \mathbf{R}$), $u = yi + zi + ti$ és $v = qi + rj + tk$. Ekkor

$$\begin{aligned} \overline{ab} - \bar{b}\bar{a} &= \overline{(x+u)(p+v)} - \overline{p+v} \cdot \overline{x+u} = \\ &= (\overline{xp} + \overline{xv} + \overline{up} + \overline{uv}) - (\bar{p} \cdot \bar{x} + \bar{p} \cdot \bar{u} + \bar{v} \cdot \bar{x} + \bar{v} \cdot \bar{u}) = \\ &= (xp + x\bar{v} + p\bar{u} + \bar{u}\bar{v}) - (xp + p\bar{u} + x\bar{v} + \bar{v} \cdot \bar{u}) = \bar{u}\bar{v} - (-v)(-u) = \bar{u}\bar{v} - vu = \\ &= ((-yq - zr - ts) + yr\bar{i}\bar{j} + ys\bar{i}\bar{k} + zq\bar{j}\bar{i} + zs\bar{j}\bar{k} + tq\bar{k}\bar{i} + tr\bar{k}\bar{j}) - vu = \\ &= ((-yq - zr - ts) + yrj\bar{i} + yski + zqij + zskj + tqik + trjk) - vu = vu - vu = 0 \end{aligned}$$

Tehát $\overline{ab} = \bar{b}\bar{a}$. Ezt felhasználva

$$|ab|^2 = ab\overline{ab} = ab\bar{b}\bar{a} = a|b|^2\bar{a} = a\bar{a}|b|^2 = |a|^2|b|^2.$$

Ha $a \neq 0$, akkor

$$\overline{\frac{1}{a}} = \frac{1}{\overline{a}} = \frac{1}{|a|^2}a = \frac{1}{\bar{a}}.$$

Most rátérünk az egyenlőtlenség igazolására. Emeljük mindkét oldalát négyzetre

$$a\bar{a} + b\bar{b} + a\bar{b} + b\bar{a} = (a+b)(\bar{a} + \bar{b}) \leq |a|^2 + |b|^2 + 2|a||b|,$$

majd a mindkét oldalon szereplő $|a|^2 + |b|^2$ rész elhagyása után emeljük ismét négyzetre:

$$(a\bar{b} + b\bar{a})^2 \leq 4|a|^2|b|^2.$$

Az utóbbi egyenlőtlenség igazolása céljából legyen $x \in \mathbf{R}$ és tekintsük az

$$f(x) = |a - xb|^2 = (a + xb)(\bar{a} + x\bar{b}) = x^2|b|^2 + x(a\bar{b} + b\bar{a}) + |a|^2$$

valós másodfokú formát. Mivel bármely valós x -re $f(x) \geq 0$, ezért diszkriminánsa nem pozitív, ami éppen az igazolandó egyenlőtlenséget jelenti. ■

11.5. Tétel. Legyen K az

$$\begin{pmatrix} x & y & z & t \\ -y & x & -t & z \\ -z & t & x & -y \\ -t & -z & y & x \end{pmatrix}, \quad x, y, z, t \in \mathbf{R},$$

alakú 4×4 -es mátrixok halmaza. Ekkor K olyan részalgebra a 4×4 -es mátrixok \mathbf{R} -algebrájában, mely izomorf a kvaterniók \mathbf{R} -algebrájával.

Bizonyítás. Tekintsük az

$$1 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \quad i = \begin{pmatrix} 0 & 1 & 0 & 0 \\ -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & 1 & 0 \end{pmatrix},$$

$$j = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ -1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \end{pmatrix} \quad \text{és} \quad k = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & -1 & 0 \\ 0 & 1 & 0 & 0 \\ -1 & 0 & 0 & 0 \end{pmatrix}$$

mátrixokat. Világos, hogy $1, i, j, k$ a $(K; +)$ vektortér bázisát alkotják, s könnyű ellenőrizni, hogy a szorzásban ugyanúgy viselkednek, mint a megfelelő kvaterniók. Ezért egyrészt nem vezet ki a mátrixszorzás K -ból, és így K valóban részalgebra, másrészt a 10.6. Tétel szerint K izomorf a kvaterniók \mathbf{R} -algebrájával. ■

11.6. Definíció. Jelölje R a valós számok, a komplex számok, illetve a kvaterniók \mathbf{R} -algebrája közül valamelyiket, és tekintsük az

$$R^{(2)} = \{a + bE : a, b \in R\},$$

halmazt, ahol $E \notin R$ egy szimbólum. Értelmezzük az összeadást és a szorzást $R^{(2)}$ -n, valamint az $R^{(2)}$ -beli elemeknek valós számmal való szorzását a következőképpen:

$$(a + bE) + (c + dE) = (a + c) + (b + d)E,$$

$$(a + bE)(c + dE) = (ac - \bar{d}b) + (da + b\bar{c})E$$

és

$$\lambda(a + bE) = \lambda a + (\lambda b)E, \quad a, b \in R, \lambda \in \mathbf{R}.$$

Az így nyert $R^{(2)}$ algebrai struktúrát az R algebra megkettőzöttjének nevezzük.

11.7. Tétel. A valós számok, a komplex számok, illetve a kvaterniók megkettőzöttje hiperkomplex rendszer. Speciálisan \mathbf{R} megkettőzöttje izomorf \mathbf{C} -vel, és \mathbf{C} megkettőzöttje izomorf \mathbf{K} -val.

Bizonyítás. Legyen R a valós számok, a komplex számok, illetve a kvaterniók \mathbf{R} -algebrája közül valamelyik, és tekintsük $R^{(2)}$ megkettőzöttjét. A definícióból azonnal adódik, hogy $(R^{(2)}; +)$ kommutatív csoport. $1 = 1 + 0E$ multiplikatív egységelem, mert, ha $a + bE \in R^{(2)}$, akkor

$$\begin{aligned} (1 + 0E)(a + bE) &= (1a - \bar{0}b) + (b1 + 0\bar{a})E = \\ &= a + bE = \\ &= (a1 - \bar{0}b) + (0a + b\bar{1})E = (a + bE)(1 + 0E). \end{aligned}$$

Legyen $a + bE, c + dE \in R^{(2)}$, és $\lambda \in \mathbf{R}$. Ekkor

$$(\lambda(a + bE))(c + dE) = ((\lambda a + \lambda bE)(c + dE) = ((\lambda a)c - \bar{d}(\lambda b)) + (d(\lambda a) + (\lambda b)\bar{c})E =$$

$$\begin{aligned}
&= \lambda((ac - \bar{d}b) + (da + b\bar{c})E) = \lambda((a + bE)(c + dE)) = \\
&= (a(\lambda c) - \overline{\lambda d}b) + ((\lambda d)a + b\overline{\lambda c})E = ((a + bE)(\lambda c + \lambda dE)) = (\lambda(a + bE))(c + dE).
\end{aligned}$$

Ahhoz, hogy $R^{(2)}$ hiperkomplex rendszer legyen, már csak a szorzás összeadásra való disztributivitását kell belátni. Legyen $a_1 + b_1E, a_2 + b_2E, c + dE \in R^{(2)}$. Ekkor

$$\begin{aligned}
((a_1 + b_1E) + (a_2 + b_2E))(c + dE) &= ((a_1 + a_2) + (b_1 + b_2)E)(c + dE) = \\
&= ((a_1 + a_2)c - \bar{d}(b_1 + b_2)) + (d(a_1 + a_2) + (b_1 + b_2)\bar{c})E = \\
&= ((a_1c - \bar{d}b_1) + (da_1 + b_1\bar{c})E) + ((a_2c - \bar{d}b_2) + (da_2 + b_2\bar{c})E) = \\
&= (a_1 + b_1E)(c + dE) + (a_2 + b_2E)(c + dE).
\end{aligned}$$

A baloldali disztributivitást hasonlóan igazolhatjuk felhasználva az $\overline{u+v} = \bar{u} + \bar{v}$ ($u, v \in R$) egyenlőséget.

Mivel minden $a \in \mathbf{R}$ esetén $\bar{a} = a$, az $\mathbf{R}^{(2)} \cong \mathbf{C}$ állítás nyilvánvaló. A $\mathbf{C}^{(2)} \cong \mathbf{K}$ állítás igazolásának első lépéseként vegyük észre, hogy

$$\mathbf{K} = \{a + bj : a, b \in \mathbf{C}\},$$

hiszen

$$x + yi + zj + tk = (x + yi) + (z + ti)j.$$

Ha $a, b, c, d \in \mathbf{C}$ és $\lambda \in \mathbf{R}$, akkor

$$(a + bj) + (c + dj) = (a + c) + (b + d)j \quad \text{és} \quad \lambda(a + bj) = \lambda a + (\lambda b)j$$

és

$$\begin{aligned}
(a + bj)(c + dj) &= ac + bjdj + adj + bjc = ac + b\bar{d}jj + adj + b\bar{c}j = \\
&= (ac - \bar{d}b) + (da + b\bar{c})j.
\end{aligned}$$

Az utóbbi egyenlőség igazolásánál kihasználtuk, hogy a komplex számok szorzása kommutatív, és minden $z = x + yi$ ($x, y \in \mathbf{R}$) esetén

$$zj = (x + yi)j = xj + yij = jx - jyi = j(x - yi) = j\bar{z}.$$

Végül a 10.6. Tételt alkalmazva kapjuk, hogy \mathbf{C} megkettőzöttje izomorf \mathbf{K} -val. ■

11.8. Definíció. A kvaterniók algebrájának megkettőzöttjét *Cayley-algebrának*, elemeit pedig *Cayley-számoknak* nevezzük. Értelmezzük a Cayley-számok konjugáltját. Ha $u = a + bE$ ($a, b \in \mathbf{K}$), akkor legyen

$$\bar{u} = \bar{a} - bE.$$

Ekkor

$$u\bar{u} = (a + bE)(\bar{a} - bE) = (a\bar{a} - \overline{(-b)b}) + ((-b)a + b\bar{a})E = a\bar{a} + \bar{b}b = |a|^2 + |b|^2,$$

s hasonlóan látható be, hogy $\bar{u}u = |a|^2 + |b|^2 = u\bar{u}$. Értelmezzük u abszolútértékét a szokásos módon:

$$|u| = \sqrt{u\bar{u}}.$$

Ha $u \neq 0$, akkor $|u|^2 \neq 0$, és így

$$u\left(\frac{1}{|u|^2}\bar{u}\right) = \frac{1}{|u|^2}(u\bar{u}) = 1 = \frac{1}{|u|^2}(\bar{u}u) = \left(\frac{1}{|u|^2}\bar{u}\right)u.$$

Ezért az u elemnek $\frac{1}{|u|^2}\bar{u}$ a multiplikatív inverze. A következő tételben megmutatjuk, hogy a Cayley-algebra zérusosztómentes. Ezt felhasználva könnyű belátni, hogy minden nullától különböző u Cayley-számnak csak egyetlen multiplikatív inverze van, s a hagyományokhoz híven $\frac{1}{u}$ -val jelöljük..

Most összefoglaljuk a Cayley-számok aritmetikájára vonatkozó legfontosabb tényeket.

11.9. Tétel.

(1) A Cayley-számok olyan zérusosztómentes alternatív algebrát alkotnak, melyben

$$1, i, j, k, E, I = iE, J = jE, K = kE$$

bázis, ahol $1, i, j, k$ a megfelelő kvaterniók.

(2) Bármely v, w és $u = x + yi + zj + tk + pE + qI + rJ + sK$ ($x, y, z, t, p, q, r, s \in \mathbf{R}$) Cayley-számok esetén

$$\begin{aligned} \bar{u} &= x - yi - zj - tk - pE - qI - rJ - sK, \\ \bar{u}u &= u\bar{u} = |u|^2 = x^2 + y^2 + z^2 + t^2 + p^2 + q^2 + r^2 + s^2, \\ \lambda\bar{u} &= \lambda\bar{u}, \quad \overline{\bar{u}} = u, \quad |u| = |\bar{u}|, \quad \overline{u + \bar{u}} = \bar{u} + u, \end{aligned}$$

$$\overline{uv} = \bar{v} \cdot \bar{u}, \quad |uv| = |u||v|, \quad \overline{\frac{1}{u}} = \frac{1}{\bar{u}} \quad (u \neq 0) \quad \text{és} \quad |a + b| \leq |a| + |b|.$$

(3) Bármely nullától különböző $a \in \mathbf{K}^{(2)}$ Cayley-számra az $a \in \mathbf{R}$, $\bar{a} = a$ és $a^2 \in \mathbf{R}^+$, illetve az $\mathcal{R}(a) = 0$, $\bar{a} = -a$ és $a^2 \in \mathbf{R}^-$ állítások ekvivalensek. (A Cayley-számok valós és képzetes részét a kvaterniókéhoz hasonlóan definiálhatjuk.)

Bizonyítás. Legyen $a + bE, c + dE$ ($a, b, c, d \in \mathbf{K}$) két Cayley-szám. Ekkor

$$\begin{aligned} (a + bE)((a + bE)(c + dE)) &= (a + bE)((ac - \bar{d}b) + (da + b\bar{c})E) = \\ &= (a(ac - \bar{d}b) + \overline{da + b\bar{c}} \cdot b) + (da + b\bar{c})a + b \cdot \overline{ac - \bar{d}b}E = \\ &= (a^2c - (a + \bar{a})\bar{d}b + c(\bar{b}b)) + (da^2 + b(\bar{c}(a + \bar{a})) - (b\bar{b})d)E = \\ &= (a^2c - \bar{d}b(a + \bar{a}) + (\bar{b}b)c) + (da^2 + b((a + \bar{a})\bar{c}) - d(\bar{b}b))E = \\ &= ((a^2 - \bar{b}b)c - \bar{d}(ba + b\bar{a})) + (d(a^2 - \bar{b}b) + (ba + b\bar{a})\bar{c})E = \\ &= ((a^2 - \bar{b}b) + (ba + b\bar{a})E)(c + dE) = ((a + bE)(a + bE))(c + dE). \end{aligned}$$

Az átalakítások során felhasználtuk az összeg és szorzat konjugálására vonatkozó összefüggéseket, valamint azt, hogy a $\bar{b}b = b\bar{b}$ és az $a + \bar{a}$ valós számok \mathbf{K} centrumában vannak. Az

$$(a + bE)((c + dE)(c + dE)) = ((a + bE)(c + dE))(c + dE)$$

egyenlőséget hasonlóan igazolhatjuk. Ezért a 10.10. Tétel szerint a Cayley-számok alternatív algebrát alkotnak.

A zérusosztómentesség igazolása céljából tegyük fel, hogy

$$(a + bE)(c + dE) = (ac - \bar{d}b) + (da + b\bar{c})E = 0.$$

azaz

$$ac - \bar{d}b = 0 \quad \text{és} \quad da + b\bar{c} = 0.$$

Az első egyenlőséget balról d -vel, a másodikat pedig jobbról c -vel szorozva

$$dac + |d|^2b = dac - d\bar{d}b = 0 \quad \text{és} \quad dac + |c|^2b = dac + b\bar{c}c = 0,$$

majd a második kivonva az elsőt

$$(|c|^2 + |d|^2)b = 0$$

adódik. Ha $|c|^2 + |d|^2 = 0$, akkor $c = d = 0$ és $c + dE = 0$. Ha $|c|^2 + |d|^2 \neq 0$, akkor $b = 0$ és $ac = da = 0$. Mivel c és d valamelyike különbözik nullától, az utolsó egyenlőségből $a = 0$ és $a + bE = 0$ következik. Tehát a Cayley-számok algebrája zérusosztómentes.

Ha $u = a + bE$ egy Cayley-szám, ahol $a = x + yi + zj + tk$, $b = p + qi + rj + sk \in \mathbf{K}$, akkor

$$\begin{aligned} u &= a + bE = (x + yi + zj + tk) + (p + qi + rj + sk)E = \\ &= x + yi + zj + tk + pE + qI + rJ + sK, \\ \bar{u} &= \bar{a} - bE = (x + yi + zj + tk) - (p + qi + rj + sk)E = \\ &= x - yi - zj - tk - pE - qI - rJ - sK \end{aligned}$$

és

$$|u|^2 = |a|^2 + |b|^2 = x^2 + y^2 + z^2 + t^2 + p^2 + q^2 + r^2 + s^2.$$

Ha valamely $x, y, z, t, p, q, r, t \in \mathbf{R}$ esetén

$$0 = x + yi + zj + tk + pE + qI + rJ + sK = (x + yi + zj + tk) + (p + qi + rj + sk)E,$$

akkor $x + yi + zj + tk = 0$, $p + qi + rj + sk = 0$ és $x = y = z = t = p = q = r = s = 0$. A fentiek szerint egyrészt $1, i, j, k, E, I, J, K$ független generátorrendszer, vagyis bázis, s ezzel az (1) állítást igazoltuk. Másrészt (2) első két állítása is teljesül.

Ha $u = a + bE$ és $v = c + dE$ ($a, b, c, d \in \mathbf{K}$) Cayley-számok, akkor

$$\begin{aligned} \overline{uv} &= \overline{(ac - \bar{d}b) + (da + b\bar{c})E} = \overline{(ac - \bar{d}b)} - (da + b\bar{c})E = \\ &= (\bar{c} \cdot \bar{c} - \bar{b}d) - (da + b\bar{c})E = (\bar{c} - dE)(\bar{a} - bE) = \bar{v} \cdot \bar{u}. \end{aligned}$$

A tétel további állításait az eddig igazoltakat felhasználva a kvaterniókra vonatkozó 11.4. Tétel analóg állításai bizonyításának szinte szó szerinti megismétlésével történhet. ■

12. Zérusosztómentes és normált algebrák

12.1. Frobenius-tétel. *Bármely memtriviális, végesrangú, zérusosztómentes és asszociatív \mathbf{R} -algebrára a következő három állítás egyike teljesül:*

- (a) Rangja 1, és izomorf a valós számok testével.
- (b) Rangja 2, és izomorf a komplex számok testével.
- (c) Rangja 4, és izomorf a kvaterniók ferdetestével.

Bizonyítás. Legyen R egy nemtriviális, végesrangú, zérusosztómentes és asszociatív \mathbf{R} -algebra. Mivel R nemtriviális, ezért a rang nem lehet 0. A bizonyítást négy állítás igazolásával kezdjük.

12.1.1. R ferdetest, azaz a nullától különböző elemei a szorzásra nézve csoportot alkotnak.

A csoportokra vonatkozó alapismereteink szerint elegendő azt megmutatni, hogy bármely $a, b \in R \setminus \{0\}$ elemekhez vannak olyan $x, y \in R$ elemek, hogy $ax = b$ és $ya = b$. Legyen a_1, \dots, a_n az R algebra egy bázisa. Megmutatjuk, hogy az aa_1, \dots, aa_n , illetve az a_1a, \dots, a_na elemek is bázist alkotnak. Csak azt kell belátni, hogy lineárisan független vektorrendszerek. Ha

$$\sum_{i=1}^n \lambda_i(aa_i) = 0, \quad \text{illetve} \quad \sum_{i=1}^n \lambda_i(a_i a) = 0,$$

akkor

$$a\left(\sum_{i=1}^n \lambda_i a_i\right) = 0, \quad \text{illetve} \quad \left(\sum_{i=1}^n \lambda_i a_i\right)a = 0,$$

amiből a zérusosztómentesség miatt $\sum_{i=1}^n \lambda_i a_i = 0$ következik. Mivel a_1, \dots, a_n bázis, ebből $\lambda_1 = \dots = \lambda_n = 0$ következik. Tehát valóban lineárisan független vektorrendszerek, és ezért bázisok. Emiatt vannak olyan $\mu_i, \nu_i \in \mathbf{R}$, $i = 1, \dots, n$, elemek, hogy

$$b = \sum_{i=1}^n \mu_i (aa_i) = a\left(\sum_{i=1}^n \lambda_i a_i\right), \quad \text{illetve} \quad b = \sum_{i=1}^n \nu_i (a_i a) = \left(\sum_{i=1}^n \lambda_i a_i\right)a,$$

amivel a 12.1.1 állítást beláttuk.

A 12.1.1 állítás szerint R hiperkomplex rendszer. Ekkor — mint azt már a 11. fejezet elején említettük — R tartalmazza \mathbf{R} -et úgy, hogy $1 \in \mathbf{R}$ egyben R -nek is multiplikatív egységeleme.

12.1.2. *Ha $a \notin \mathbf{R}$, akkor $a^2 = \xi_1 a + \xi_2$ valamely $\xi_1, \xi_2 \in \mathbf{R}$ esetén, és van olyan $\lambda, \mu \in \mathbf{R}$, $\lambda \neq 0$, hogy $(\lambda a + \mu)^2 = -1$.*

Tegyük fel, hogy $a \in R$ eleget tesz 12.1.2. feltételeinek. Az $1, a, a^2, \dots, a^n$ elemek lineárisan függő rendszert alkotnak, mert R dimenziójánál többen vannak. Ezért vannak olyan nem csupa nulla $\lambda_0, \lambda_1, \dots, \lambda_n$ valós számok, hogy $\lambda_0 + \lambda_1 a + \dots + \lambda_n a^n = 0$. Tekintsük az $f(x) = \lambda_0 + \lambda_1 x + \dots + \lambda_n x^n \in \mathbf{R}[x]$ polinomot, és bontsuk fel irreducibilis polinomok szorzatára: $f(x) = f_1(x)f_2(x) \cdots f_k(x)$. Mivel $0 = f(0) = f_1(0)f_2(0) \cdots f_k(0)$, a zérusosztómentesség miatt van olyan i , hogy $f_i(a) = 0$. Feltehető, hogy $f_i(x)$ főegyütthatója 1. Az a -ra vonatkozó feltevés miatt $f_i(x)$ nem lehet elsőfokú. Ezért $f_i(x) = x^2 - \xi_1 x - \xi_2$, hiszen minden irreducibilis valós együtthatós polinom legfeljebb másodfokú. Ebből $0 = f_i(a) = a^2 - \xi_1 a - \xi_2$ és $a^2 = \xi_1 a + \xi_2$ következik. Mivel $f_i(x)$ diszkriminánsa negatív $(x + \nu)^2 + \tau^2$, $\tau \neq 0$, alakban is írható. Ha $\lambda = \frac{1}{\tau}$ és $\mu = \frac{\nu}{\tau}$, akkor

$$(\lambda a + \mu)^2 = \left(\frac{1}{\tau} a + \frac{\nu}{\tau}\right)^2 = \frac{1}{\tau^2} (a + \nu)^2 = -1,$$

hiszen $0 = f_i(a) = (a + \nu)^2 + \tau^2$.

12.1.3. *Bármely $1, a_1, \dots, a_k$ lineárisan független rendszerhez, mely nem bázis R -ben, megadható olyan $a \in R$, hogy $a^2 = -1$ és $1, a_1, \dots, a_k, a$ lineárisan független.*

Ha $1, a_1, \dots, a_k$ olyan lineárisan független rendszer, mely nem bázis R -ben, akkor van olyan $b \in R$, hogy $1, a_1, \dots, a_k, b$ is lineárisan független. A 12.1.2. állítás szerint van olyan $\lambda, \mu \in \mathbf{R}$, $\lambda \neq 0$, hogy $(\lambda b + \mu)^2 = -1$. Legyen $a = \lambda b + \mu$. Ekkor $1, a_1, \dots, a_k, a$ is lineárisan független rendszer, hiszen az $1, a_1, \dots, a_k, b$ kineárisan független rendszerből két elemi átalakítással megkapható.

12.1.4. *Ha $1, a, b$ lineárisan független rendszer és $a^2 = b^2 = -1$, akkor van olyan $\lambda \in \mathbf{R}$, hogy $ab + ba = \lambda$.*

Tegyük fel, hogy $a, b \in R$ eleget tesz 12.1.4. feltételeinek. A függetlenség miatt $a + b, a - b \notin \mathbf{R}$. Ezért a 12.1.2. állítás szerint van olyan $\lambda_1, \lambda_2, \mu_1, \mu_2 \in \mathbf{R}$, hogy $(a + b)^2 = \lambda_1(a + b) + \lambda_2$ és $(a - b)^2 = \mu_1(a - b) + \mu_2$. Ezért

$$\lambda_1(a + b) + \lambda_2 = (a + b)^2 = a^2 + b^2 + ab + ba = -2 + ab + ba$$

és

$$\mu_1(a - b) + \mu_2 = (a - b)^2 = a^2 + b^2 - ab - ba = -2 - ab - ba,$$

amiből összeadással és átrendezéssel

$$(\lambda_1 + \mu_1)a + (\lambda_1 - \mu_1)b + (\lambda_2 + \mu_2 + 4) = 0$$

következik. A függetlenség miatt $\lambda_1 + \mu_1 = \lambda_1 - \mu_1 = 0$, azaz $\lambda_1 = \mu_1 = 0$. Ezért $ab + ba = \lambda_2 + 2$.

Most már hozzáfoghatunk a bizonyítás fő gondolatmenetéhez. Ha R 1 rangú, akkor $\mathbf{R} \subseteq R$ miatt $R = \mathbf{R}$. Ha R 2 rangú, akkor a 12.1.3. állítást felhasználva adódik egy olyan $i \in R$ elem, melyre $i^2 = -1$, és $1, i$ bázis. Ekkor R izomorf \mathbf{C} -vel.

Tegyük fel, hogy R rangja legalább három. A 12.1.3. állítást felhasználva adódik olyan $i, a \in R$, melyre $i^2 = a^2 = -1$, és $1, i, a$ lineárisan független rendszer. A 12.2.4. állítás szerint $ai + ia = 2\lambda$ valamely $\lambda \in \mathbf{R}$ -re. Legyen $b = a + \lambda i$. Ekkor $1, i, b$ is lineárisan független rendszer, és

$$b^2 = (a + \lambda i)^2 = -1 + \lambda(ai + ia) - \lambda^2 = \lambda^2 - 1.$$

$\lambda^2 - 1 < 0$, mert ellenkező esetben $0 = b^2 - (\lambda^2 - 1) = (b - \sqrt{\lambda^2 - 1})(b + \sqrt{\lambda^2 - 1})$, amiből azt kapjuk, hogy b valós szám. Ez pedig $1, i, b$ függetlensége miatt lehetetlen. Legyen

$$j = \frac{1}{\sqrt{1 - \lambda^2}}b \quad \text{és} \quad k = ij.$$

Ekkor

$$\begin{aligned} j^2 &= \frac{1}{1 - \lambda^2}b^2 = \frac{1}{1 - \lambda^2}(\lambda^2 - 1) = -1, \\ k &= ij = i \frac{1}{\sqrt{1 - \lambda^2}}b = i \frac{1}{\sqrt{1 - \lambda^2}}(a + \lambda i) = \frac{1}{\sqrt{1 - \lambda^2}}(ia - \lambda) = \\ &= \frac{1}{\sqrt{1 - \lambda^2}}(2\lambda - ai - \lambda) = \frac{1}{\sqrt{1 - \lambda^2}}(-ai + \lambda) = -\frac{1}{\sqrt{1 - \lambda^2}}(a + \lambda i)i = -ji, \\ k^2 &= ijij = -ijji = -i(-1)i = i^2 = -1, \\ jk &= jij = -jji = i = -ijj = -kj, \\ ki &= iji = -iij = j = -iij = -ik. \end{aligned}$$

Az $1, i, j, k$ elemek lineárisan független rendszert alkotnak, mert ellenkező esetben valamelyik elem az öt megelőzők lineáris kombinációja lenne. Az $1, i, j$ elemek lineáris függetlensége miatt ez csak k lehet. Ha $k = \lambda + \mu i + \nu j$, akkor j -vel jobbról szorozva

$$\begin{aligned} -i &= kj = (\lambda + \mu i + \nu j)j = \lambda j + \mu k - \nu = \lambda j + \mu(\lambda + \mu i + \nu j) - \nu = \\ &= (\lambda\mu - \nu) + \mu^2 i + (\lambda + \mu\nu)j \end{aligned}$$

adódik. Mivel független rendszerrel egy elem legfeljebb egyféleképpen írható fel lineáris kombinációként, ezért ebből $\mu^2 = -1$ következik, ami lehetetlen. Tehát $1, i, j, k$ lineárisan független, és így R rangja legalább 4. Ha a rang 4, akkor $1, i, j, k$ bázisa R -nek és közöttük a szorzást ugyanúgy kell elvégezni, mint a kvaterniókon. Ezért a 10.6. Tétel szerint R izomorf a kvaterniók algebrájával.

Most már csak azt kell belátni, hogy R rangja nem lehet 4-nél több. Ha R rangja legalább 5, akkor a 12.1.3. állítás szerint van olyan $l \in R$, hogy $l^2 = -1$, és $1, i, j, k, l$ lineárisan független rendszer. A 12.1.4 állítás szerint vannak olyan λ, μ, ν valós számok, hogy

$$il + lj = \lambda, \quad jl + lj = \mu \quad \text{és} \quad kl + lk = \nu.$$

Ezekből

$$\begin{aligned} lk &= lij = (\lambda - il)j = \lambda j - ilj = \lambda j - i(\mu - jl) = \lambda j - \mu i + ijl = \lambda j - \mu i + kl = \\ &= \lambda j - \mu i + \nu - lk \end{aligned}$$

és

$$2lk = \lambda j - \mu i + \nu$$

következik. Az utóbbit jobbról k -val szorozva

$$-2l = 2lkk = \lambda jk - \mu ik + \nu k = \lambda i + \mu j + \nu k$$

adódik, ami ellentmond annak, hogy i, j, k, l lineárisan független rendszer. ■

12.2. Tétel. *Bármely nemtriviális végesrangú, zérusosztómentes és asszociatív \mathbf{C} -algebra izomorf a komplex számok testével.*

Bizonyítás. Legyen R egy nemtriviális n rangú és zérusosztómentes \mathbf{C} -algebra. Ekkor R tekinthető \mathbf{R} -algebrának is. Megmutatjuk, hogy R -nek — mint \mathbf{R} -algebrának — $2n$ a rangja. Legyen a_1, \dots, a_n bázisa R -nek — mint \mathbf{C} -algebrának —, és tekintsük az $a_1, \dots, a_n, ia_1, \dots, ia_n$ elemeket, ahol $i \in \mathbf{C}$ a képzetes egység. Ha $a \in R$, akkor vannak olyan $\lambda_1 + i\mu_1, \dots, \lambda_n + i\mu_n \in \mathbf{C}$ számok, hogy

$$a = (\lambda_1 + i\mu_1)a_1 + \dots + (\lambda_n + i\mu_n)a_n = \lambda_1 a_1 + \dots + \lambda_n a_n + \mu_1(ia_1) + \dots + \mu_n(ia_n).$$

Tehát az $a_1, \dots, a_n, ia_1, \dots, ia_n$ elemek R -nek — mint \mathbf{R} -algebrának — generátorrendszere. Ha $\lambda_1\mu_1, \dots, \lambda_n, \mu_n \in \mathbf{R}$ és

$$\lambda_1 a_1 + \dots + \lambda_n a_n + \mu_1(ia_1) + \dots + \mu_n(ia_n) = 0,$$

akkor

$$(\lambda_1 + i\mu_1)a_1 + \dots + (\lambda_n + i\mu_n)a_n = 0.$$

Mivel a_1, \dots, a_n bázisa R -nek — mint \mathbf{C} -algebrának —, ezért mindegyik együttható nulla. Ebből pedig $\lambda_1 = \mu_1 = \dots = \lambda_n = \mu_n = 0$ következik. Tehát az $a_1, \dots, a_n, ia_1, \dots, ia_n$ elemek R -ben — mint \mathbf{R} -algebrában — lineárisan független rendszert, és így bázist alkotnak. Tehát R -nek — mint \mathbf{R} -algebrának — $2n$ a rangja. Ezért Frobenius-tétel szerint R izomorf \mathbf{C} -vel vagy \mathbf{K} -val. Az utóbbi esetben a 10.3. Tétel és a 10.4. Megjegyzés szerint azt kapnánk, hogy \mathbf{C} része \mathbf{K} centrumának, ami nem igaz. Így csak az első lehetőség marad. ■

Bizonyítás nélkül megadjuk a Frobenius-tétel általánosabb alkját.

12.3. Általános Frobenius-tétel. *Bármely nemtriviális, végesrangú, zérusosztómentes és alternatív \mathbf{R} -algebrára a következő négy állítás egyike teljesül:*

- (a) Rangja 1, és izomorf a valós számok testével.
- (b) Rangja 2, és izomorf a komplex számok testével.
- (c) Rangja 4, és izomorf a kvaterniók ferdetestével.
- (d) Rangja 8, és izomorf a Cayley-számok alternatív algebrájával.

12.4. Definíció. Legyen R egy \mathbf{R} -algebra. Egy $\sigma: R^2 \rightarrow \mathbf{R}$ leképezést *skaláris szorzatnak* nevezzük, ha bármely $a, b, c \in R$ és $\lambda \in \mathbf{R}$ esetén

$$\begin{aligned} \sigma(a, b) &= \sigma(b, a), & \sigma(\lambda a, b) &= \lambda \sigma(a, b), & \sigma(a + b, c) &= \sigma(a, c) + \sigma(b, c), \\ \sigma(a, a) &\geq 0 & \text{és} & \sigma(a, a) = 0 & \Leftrightarrow a = 0. \end{aligned}$$

Azt mondjuk, hogy R *normált algebra* a σ -skaláris szorzással, ha

$$\sigma(ab, ab) = \sigma(a, a) \cdot \sigma(b, b)$$

minden $a, b \in R$ esetén.

12.5. Tétel. Jelölje R a valós számok, a komplex számok, a kvaterniók illetve a Cayley-féle számok \mathbf{R} -algebrája közül valamelyiket. Legyen

$$\sigma: R^2 \rightarrow \mathbf{R}, (a, b) \mapsto \frac{1}{2}(a\bar{b} + b\bar{a}).$$

Ekkor σ olyan skaláris szorzás, mellyel R normált algebra.

Bizonyítás. A skaláris szorzás definíciójában szereplő első három egyenlőség egyszerű számolással, a többi tulajdonság pedig $\sigma(a, a) = |a|^2$ felhasználásával igazolható. ■

12.6. Hurwitz-tétel. *Bármely nem-triviális végesrangú, egységelemes és normált \mathbf{R} -algebrára a következő négy állítás egyike teljesül:*

- (a) Rangja 1, és izomorf a valós számok testével.
- (b) Rangja 2, és izomorf a komplex számok testével.
- (c) Rangja 4, és izomorf a kvaterniók ferdetestével.
- (d) Rangja 8, és izomorf a Cayley-számok alternatív algebrájával.