1. Absztrakt algebrai bevezető

Legyen A nemüres halmaz, n pedig nemnegatív egész szám. Az $f\colon A^n \to A$ leképezéseket A–n értelmezett n–változós műveleteteknek nevezzük. Az $(a_1, \ldots, a_n) \in A^n$ elem f szerinti képét $f(a_1, \ldots, a_n)$ 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 *műveletjelek*nek. Tegyük fel, hogy $\mathcal{F}$ minden f eleméhez egy n nemnegatív egész szám van rendelve. Ekkor $\mathcal{F}$–et *algebratípus*nak, f–et pedig *n–változós műveletjel*nek nevezzük. Azt mondjuk, hogy az $(A; F)$ rendezett elempár *$\mathcal{F}$–típusú algebrai struktúra* (vagy röviden *algebra*), ha A nemüres halmaz (az *algebra alaphalmaza*) $F = \{f^A\colon\ f \in \mathcal{F}\}$ 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. $\mathcal{F} = \{f_1, \ldots, f_k\}$, akkor $(A; F)$ helyett az $(A; f_1, \ldots, f_k)$ jelölést is használjuk, többnyire úgy, hogy $f_1, \ldots, f_k$ 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 *grupoid*nak nevezünk, ha egyetlen kétváltozós művelettel rendelkezik. Ha a műveletnek van egységeleme, illetve a művelet kommutativ, akkor *egységelemes*, illetve *kommutatív* grupoidról beszélünk. Az asszociatív műveletű grupoidokat *félcsoport*oknak, az olyan egységelemes félcsoportokat pedig, melyekben minden elemnek van inverze, *csoport*oknak nevezzük.

Azt mondjuk, hogy egy $(R; +, \cdot)$ algebrai struktúra *félgyűrű*, ha $(R; +)$ kommutatív és egységelemes félcsoport, $(R; \cdot)$ félcsoport, és a szorzás disztributív az összeadásra nézve. Az $(R; +, \cdot)$ félgyűrűt *gyűrű*nek nevezzük, ha $(R; +)$ csoport. Ha egy félgyűrű vagy gyűrű szorzása egységelemes, illetve kommutatív akkor egységelemes, illetve kommutatív félgyűrűnek 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), *test*eknek nevezzük. Ha R a szorzás kommutativitását esetleg leszámítva a testek minden tulajdonságával rendelkezik, akkor *ferdetest*nek nevezzük. Ha $(R; +, \cdot)$ a szorzás asszociatívitását leszámítva minden gyűrű axiómát teljesít, akkor *nem-asszociatív gyűrű*nek 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 $\varphi\colon\ A \to B$ leképezést *homomorfizmus*nak nevezünk, ha felcserélhető a műveletekkel, azaz tetszőleges $f \in F$ n–változós ($n \geq 0$) művelet és $a_1, \ldots, a_n \in A$ esetén

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

Ha φ szürjektív, akkor a második struktúrát az első *homomorf képé*nek nevezzük. A bijektív homomorfizmust *izomorfizmus*nak, az injektívet pedig *beágyazás*nak hívjuk. Homomorfizmusok szorzata homomorfizmus, és izomorfizmusok inverze is izomorfizmus.

Számos művelettulajdonság öröklődik szürjektív homomorfizus esetén. Ilyen tulajdonságok például a kommutativitás, az asszociativitás, a disztributivitás, valamint az egységelem és inverz elem létezése. Így csoport, félgyűrű, illetve gyűrű homomorf képe is csoport, félgyűrű, 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 $a_1, b_1 \ldots, a_n, b_n \in A$ esetén

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

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,

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

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 $\overline{a}$ jelölést is használjuk. Minden $f \in F$ n–változós ($n \geq 0$) művelet segítségével természtes módon értelmezhetünk egy ugyancsak f-fel jelölt n–változós műveletet az A/ρ halmazon: Tetszőleges $a_1/\rho, \ldots, a_n/\rho \in A/\rho$ esetén legyen

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

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

Egy nemüres A halmazon értelmezett kétváltozós ρ relációt *részbenrendezés*nek 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 *rendezés*nek vagy *lineáris rendezés*nek 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 $\{a \in G\colon\ 1 \leq a\}$ halmazt a részbenrendezett csoport *pozitívitási tartomány*ának 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)⇒(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)⇒(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)⇒(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)⇒(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 antiszimmetria 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:*

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

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 $\{a \in R\colon\ 0 \leq a\}$ halmazt a részbenrendezett gyűrű *pozitívitási tartomány*ának 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)⇒(3) és (3)⇒(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. Definiáljunk egy $\leq$ relációt R–en a következőképpen:*

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

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.*

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*

$$\mathcal{R} \to \mathcal{P},\ \leq \mapsto \{x \in G\colon 1 \leq x\}$$

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

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 $|a+b| = -(a+b) = (-a)+(-b) \leq |a| + |b|$. ∎

3. Természetes számok

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

(P1) N nemüres halmaz és van egy $0 \in N$ kitüntetett eleme.
(P2) Adott egy $'\colon N \to N$ 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

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

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

A Peano-féle axiómrendszer 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 $^*\colon A \to A$ egy leképezés. Tegyük fel továbbá, hogy $(N;',0)$ teljesíti a Peano-féle axiómákat. Ekkor létezik pontosan egy olyan $\varphi\colon N \to A$ 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 $\psi\colon N \to A$ leképezésre is $0\psi = a_0$, és $n'\psi = (n\psi)^*$ minden $n \in N$ esetén. Legyen $U = \{n \in N\colon\ n\varphi = n\psi\}$. 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 $\varphi\colon N \to M$ és $\psi\colon M \to N$ 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 $U = \{n \in N\colon\ n(\varphi\psi) = n\}$. 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. Igy (P5) miatt $U = N$, azaz $\varphi\psi = \mathrm{id}_N$. Hasonlóan látható be $\psi\varphi = \mathrm{id}_M$ 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 axiómá*jának 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. $\mathbf{N} = \{n'\colon\ n \in \mathbf{N}_0\}$.

Bizonyítás. Világos, hogy az $U = \{0\} \cup \{n'\colon\ n \in \mathbf{N}_0\}$ 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 $U = \{n \in \mathbf{N}_0\colon\ n' \neq n\}$. (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 álltás: (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 egyszerűsítéses 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 asszociatívitását és kommutatívitását többször kihasználva kapjuk, hogy $(k+m)n' = (k+m)n+(k+m) = (kn+mn)+(k+m) = \cdots = (kn + k) + (mn + m) = kn' + mn'$. ∎

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 kommutatívitása 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 félgyűrű, 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

$$m \leq n \quad \overset{\text{def}}{\Leftrightarrow} \quad \exists k \in \mathbf{N}_0 \colon\ m + k = n.$$

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

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

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:*

(a) 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 $m+k<n+l$.

(b) 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 $mk<nl$.

(c) Ha $m+k\leq n+k$, akkor $m\leq n$. Ha $m+k<n+k$, akkor $m<n$.

(d) Ha $mk\leq nk$ és $k\neq 0$, akkor $m\leq n$, Ha $mk<nk$ és $k\neq 0$, akkor $m<n$.

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 $(R\,;+,\cdot)$ félgyűrű és ρ részbenrendezés R-en. Azt mondjuk, hogy $(R;+,\cdot)$ *részbenrendezett félgyűrű* 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* félgyűrűnek nevezzük.

3.25. Tétel. *A természetes számok félgyűrűje rendezett a $\leq$ relációra nézve. A természetes számok félgyűrűjének két rendezése van: a $\leq$ és a $\geq$ rendezés.*

Bizonyítás. Az első állítás lényegében összeloglalja néhány korábbi állításunkat. Legyen $\preceq$ a természetes számok félgyűrűjének egy rendezése. Vegyük észre, hogy ekkor a természetes számok félgyűrűjének $\succeq$ is 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 $U_m=\{x\in\mathbf{N}_0\colon m\preceq m+x\}$ halmaz megegyezik $\mathbf{N}_0$-lal. Világos, hogy $0\in U_m$. Ha $n\in U_n$, 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: Teszőleges $(a,b),(c,d)\in\mathbf{N}_0^2$ 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

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

4.2. Tétel.

(1) Az $(\mathbf{N}_0^2;+,\cdot)$ algebrai struktúra kommutatív és egységelemes félgyűrű, melynek ρ kongruenciarelációja.

(2) Az $(\mathbf{N}_0^2/\rho;+,\cdot)$ faktorstruktúra olyan integritástartomány, melyre az $\mathbf{N}_0\to\mathbf{N}_0^2/\rho;\ n\mapsto\overline{(n,0)}$ leképezés az $(\mathbf{N}_0;.+,\cdot)$ félgyűrűnek $(\mathbf{N}_0^2/\rho;+,\cdot)$–ba való beágyazása.

(3) $\mathbf{N}_0^2/\rho=\{-\overline{(n,0)}\colon\ n\in\mathbf{N}\}\cup\{\overline{(0,0)}\}\cup\{\overline{(n,0)}\colon\ n\in\mathbf{N}\}$, 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 disztributiv 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

$$((a,b)\cdot(c,d))\cdot(e,f)=(ac+bd,ad+bc)\cdot(e,f)=$$

$$=((ac+bd)e+(ad+bc)f,(ac+bd)f+(ad+bc)e)=$$

$$=(a(ce+df)+b(cf+de),a(cf+de)+b(ce+df))=$$

$$=(a,b)\cdot(ce+df,cf+de)=(a,b)\cdot((c,d)\cdot(e,f))$$

és

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

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

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

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

Most megvizsgáljuk a ρ reláció tulajdonságait. A definícóból 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 $\mathbf{N}_0^2 \to \mathbf{N}_0^2/\rho,\ (a,b) \mapsto \overline{(a,b)}$ leképezés homomorfizmus, az $(\mathbf{N}_0^2/\rho;+,\cdot)$ faktorstruktúra is kommutatív és egységelemes félgyűrű, melynek $\overline{(0,0)}$ az additív, $\overline{(1,0)}$ 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

$$\varphi\colon\ \mathbf{N}_0 \to \mathbf{N}_0^2/\rho,\ \ a \mapsto \overline{(a,0)}$$

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

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

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 $\mathbf{N}_0^2/\rho$ halmazt $\mathbf{Z}$–vel, és az $\overline{(n,0)},\ n \in \mathbf{N}_0$, alakú elemeket pedig egyszerűen n-nel. $\mathbf{Z}$ elemeit *egész számok*nak nevezzük. Értelmezzünk a $\leq$ relációt $\mathbf{Z}$-n a következőképpen:

$$a \leq b \quad \overset{\text{def}}{\Leftrightarrow} \quad b - a \in \mathbf{N}_0$$

.

4.4. Tétel. *A $(\mathbf{Z};+,\cdot)$ olyan integritásrtartomány, melynek $(\mathbf{N}_0;+,\cdot)$ részfélgyűrűje, és minden eleme $a-b$, $a,b \in \mathbf{N}_0$, alakú. Továbbá $(\mathbf{Z};+,\cdot)$ lineárisan rendezett gyűrű a $\leq$ relációra nézve az $\mathbf{N}_0$ pozitivitási 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.*

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

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

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

és

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

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 $\mathbf{Z} \to S/\rho,\ n \mapsto \overline{(n, 1)}$ leképezés az egész számok gyűrűjének beágyazása $(S/\rho, +, \cdot)$-ba.

(4) $S/\rho = \{-\overline{(m, n)}\colon\ m, n \in \mathbf{N}\} \cup \{\overline{(0, 1)}\} \cup \{\overline{(m, n)}\colon\ m, n \in \mathbf{N}\}$ 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

$$((a, b) + (c, d)) + (e, f) = (ad + bc, bd) + (e, f) = ((ad + bc)f + (bd)e, (bd)f) =$$

$$= (a(df) + b(cf + de), b(df)) = (a, b) + (cf + de, df) = (a, b) + ((c, d) + (e, f)).$$

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 $adcf = bcde$, 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 $(a,b)\cdot(e,f)=(ae,bf)\ \rho\ (ce,df)=\overline{(c,d)}\cdot(e,f)$. Tehát ρ valóban kongruenciareláció.

Mivel az $S\to S/\rho,\ (a,b)\mapsto\overline{(a,b)}$ 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 $a\neq0$, 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

$$(\overline{(a,b)}+\overline{(c,d)})\cdot\overline{(e,f)}=\overline{(ad+bc,bd)}\cdot\overline{(e,f)}=\overline{((ade+bce,bdf)}=$$

$$=\overline{(adef+bcef,bdf^2)}=\overline{(ae,bf)}+\overline{(ce,df)}=\overline{(a,b)}\cdot\overline{(e,f)}+\overline{(c,d)}\cdot\overline{(e,f)},$$

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

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

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

$$(a+b)\varphi=\overline{(a+b,1)}=\overline{(a\cdot1+1\cdot b,1\cdot1)}=\overline{(a,1)}+\overline{(b,1)}=a\varphi+b\varphi$$

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 $a\neq0$. 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 $\overline{(a,b)}=-\overline{(-a,b)}\in\{-\overline{(m,n)}\colon\ m,n\in\mathbf{N}\}$. Ha $a\in\mathbf{N}$, akkor $\overline{(a,b)}\in\{\overline{(m,n)}\colon\ m,n\in\mathbf{N}\}$. 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 számok*nak nevezzük. Ha $a,b\in\mathbf{Q}$ és $b\neq0$, akkor ab^{-1} helyett $\frac{a}{b}$-t vagy a/b-t is írunk. Legyen továbbá $\mathbf{Q}^+=\{\overline{(m,n)}\colon\ m,n\in\mathbf{N}\}$ és $\mathbf{Q}^-=\{-\overline{(m,n)}\colon\ m,n\in\mathbf{N}\}$. $\mathbf{Q}^+$ elemeit *pozitív racionális számok*nak, $\mathbf{Q}^-$ elemeit pedig *negatív racionális számok*nak hívjuk. Értelmezzünk a $\leq$ relációt $\mathbf{Q}$-n a következőképpen:

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

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* $n\leq a<n+1$.

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.*

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 *alapsorozat*nak vagy *Cauchy–sorozat*nak 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 *nullsorozat*nak 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

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

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 definícó szerint van olyan $n_0 \in \mathbf{N}$, hogy $|r_n| < \dfrac{\varepsilon}{2}$ 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 másodszor $(r_i) \in R$. A definícó 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 $K_1 = \min(r_0 \ldots, r_{n_0-1}, r_{n_0} - 1)$, $K_2 = \max(r_0 \ldots, r_{n_0-1}, r_{n_0} + 1)$ és $K = \max(|K_1|, |K_2|)$, akkor $|r_i| < K$ minden $i \in \mathbf{N}$ esetén. ∎

6.3. Segédtétel. *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 $|r_n - r_m| < \dfrac{\varepsilon}{2}$ valahányszor $m, n \geq n_1$. Az előbbiek szerint van olyan $n_0 \geq n_1$, hogy $|r_{n_0}| \geq \varepsilon$. Legyen $t = \dfrac{\varepsilon}{2}$. 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 kissebbítendőt csökkentettük a kivonandót pedig növeltük. Az világos, hogy a két állítás egyszerre nem teljesülhet, és a nullsorozatok egyik állítást sem teljesítik. ∎

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

6.5. Következmény. *$R = R^+ \cup R^- \cup I$ és az egyesítésben szereplő három halmaz páronlént 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 $(-q_i), (q_i r_i) \in R^+$.

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 $\mathbf{Q} \to R/I$, $r \mapsto \overline{(r)} = I + (r)$ leképezés a $(\mathbf{Q}, +, \cdot)$ test beágyazása $(R/I, +, \cdot)$-be.

(3) $R/I = \{\overline{(r_i)}\colon\ (r_i) \in R^+\} \cup \{\overline{(0)}\} \cup \{\overline{(r_i)}\colon\ (r_i) \in R^-\}$, *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 $(q_i)(s_i) \in I$ bámely $(q_i) \in R$ 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 $R \to R/I,\ (r_i) \mapsto \overline{(r_i)} = I + (r_i)$ 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. Segédtétel 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. Definiáljuk 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

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

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

$$\varphi\colon\ \mathbf{Q} \to R/I,\ r \mapsto \overline{(r)}$$

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 $(r_i) \in I$. Tegyük fel, hogy $\overline{(r_i)} \neq \overline{(0)}$, vagyis $(r_i) \notin I$. Ekkor a 6.3. Segédtétel és a 6.4. Definíció szerint $\overline{(r_i)} \in \{\overline{(r_i)}\colon\ (r_i) \in R^+\}$ vagy $\overline{(r_i)} \in \{\overline{(r_i)}\colon\ (r_i) \in R^-\}$. 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. Segédtétel 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 számok*nak nevezzük. Legyen továbbá $\mathbf{R}^+ = \{\overline{(r_i)}\colon\ (r_i) \in R^+\}$ és $\mathbf{R}^- = \{\overline{(r_i)}\colon\ (r_i) \in R^-\}$. $\mathbf{R}^+$ elemeit *pozitív valós számok*nak $\mathbf{R}^-$ elemeit pedig *negatív valós számok*nak hívjuk. Értelmezzünk a $\leq$ relációt $\mathbf{R}$-n a következőképpen:

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

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* $n \leq a < n+1$.

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.*

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 számnál 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 sorozat*nak nevezzük. A racionális számsorozatokhoz hasonlóan egy a_n, $n \in \mathbf{N}$, valós számsorozatot *Cauchy–sorozat*nak 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 pozitívok, 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 $|r_m - r_n| < \dfrac{\varepsilon}{2}$ 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 $q_i = r_{i'}^i$, $i \in \mathbf{N}$. Megmutatjuk, hogy (q_i) alapsorozat, és az $a = \overline{(q_i)}$ valós szám az a_n, $n \in \mathbf{N}$, sorozat határértéke.

Az $r_{n'}^n - a_n$, $n \in \mathbf{N}$ 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

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

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

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

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

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

8. Komplex számok

8.1. Definíció. Az $\mathbf{R}^2$ halmazon értelmezzük az összeadás és a szorzás műveleteket a következőképpen: Teszőleges $(a, b), (c, d) \in \mathbf{R}^2$ 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 $\mathbf{R} \to \mathbf{R}^2$, $a \mapsto (a, 0)$ 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 disztributiv 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

$$((a, b) \cdot (c, d)) \cdot (e, f) = (ac - bd, ad + bc) \cdot (e, f) =$$

$$= ((ac - bd)e - (ad + bc)f, (ac + bd)f + (ad + bc)e) =$$

$$= ((a(ce - df) - b(cf + de), a(cf + de) + b(ce + df)) =$$

$$= (a, b) \cdot (ce - df, cf + de) = (a, b) \cdot ((c, d) \cdot (e, f))$$

és

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

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

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

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

Most tekintsük a

$$\varphi\colon\ \mathbf{R}\to\mathbf{R}^2,\ a\mapsto(a,0)$$

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 számok*nak 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 $\overline{z}$ *konjugált*ját és $|z|$ *abszolút érték*ét a következőképpen értelmezzük:

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

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*

$$\overline{\overline{z}}=z,\quad |z|=|\overline{z}|,\quad z\overline{z}=|z|^2,\quad \frac{1}{z}=\frac{\overline{z}}{|z|^2}\ (z\neq 0),$$

$$|z_1z_2|=|z_1||z_2|,\quad \overline{z_1+z_2}=\overline{z_1}+\overline{z_2},\quad \overline{z_1z_2}=\overline{z_1}\cdot\overline{z_2},$$
$$\overline{\frac{z_1}{z_2}}=\frac{\overline{z_1}}{\overline{z_2}}\ (z_2\neq 0)\quad \text{és}\quad |z_1+z_2|\leq|z_1|+|z_2|.$$

Az alábbiakban két olyan konstrukciót ismertetünk, melynek ereménye 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

$$\varphi\colon\ \mathbf{C} \to C,\ a + bi \mapsto \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$$

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

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

és

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

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*

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

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

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

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 legleljebb 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

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

és

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

Tehát φ felcserélető a műveletekkel, és ezért izomorfizmus. ∎

9. Irracionális, algebrai és transzcendens számok

A $\mathbf{R} \setminus \mathbf{Q}$ elemeit *irracionális számok*nak 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 prímek, ezért p^k és q^k is relatív prímek. Ismert, hogy ha egy egész szám osztója egy szorzatnak, és a szorzat egyik tényezőjéhez relatív prím, akkor osztója a másik tényezőnek. Ezért a második egyenlőségből $n|p^k$, $p^k|n$ 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 a számláló jegyeiből kifogytunk, a hányadosban kitesszük 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 perodikus.

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

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

és

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

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 irracionalitását 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 pozitiv. Legyen továbbá $f_1(x), f_2(x), \dots$ egy olyan függvénysorozat, 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 $f_1(x), f_2(x), \ldots$ teljesítik a tétel feltételeit. Legyen

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

ahol $g^{(k)}$ a g polinom k–adik de4riváltja.

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

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

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 $c = \dfrac{m}{n}$, ahol m és n pozitív egész számok. Könnyen ellenőrizhető, hogy

$$m - 2nx\ \in P. \tag{$*$}$$

Legyen

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

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

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

Ez az integrál 9.3.1 miatt egész szám, és így

$$\int_0^c f(x)g_k(x)dx \geq 1, \quad k = 0, 1, \ldots. \tag{$**$}$$

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

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

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 érdekesség 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

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

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

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

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

9.6. Definíció. Egy a komplex számot *algebrai szám*nak 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 szám*nak 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

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

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. ∎

9.10. 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.*

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.

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

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 algebrá*nak nevezzük.

Valamely R K–algebra egy nemüres S részhalmazát *részalgebrá*jának 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 részalgebrá*nak nevezzük. Az R algebra (illetve gyűrű) *centrum*ának az

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

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 algebrá*nak 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 $\{a+b\sqrt{2}\colon\ a,b \in \mathbf{Q}\}$ 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 $\{fg\colon\ g \in K[x_1,\dots,x_n]\}$ 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 $K \to K_{n\times n},\ \lambda \mapsto \lambda E$, 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 $\varphi\colon\ K \to R,\ \lambda \mapsto \lambda e$ 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. Igy 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 $a_1, \ldots, a_n$ R egy bázisa. Legyenek továbbá adottak a $c_{ij} \in R$ $(i, j = 1, \ldots, n)$ elemek. Definiáljuk a szorzást R–en két lépésben:*

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

és

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

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

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

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 $a_1, \ldots, a_n$, 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 $(\{a_1, \ldots, a_n\}; \cdot)$ egy n–elemű félcsoport. Legyen az algebra bázisa $a_1, \ldots, a_n$, 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 *asszociátor*ának nevezzük. (Világos, hogy R pontosan akkor asszociatív, ha bármely $a, b, c \in R$ esetén $[a, b, c] = 0$.) Az R algebrát *alternatív algebrá*nak 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

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

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

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 rendszer*nek, elemeit pedig *hiperkomplex szám*oknak 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) $x + \dfrac{y^2}{4} = -u^2$, $u \in \mathbf{R}$, $u \neq 0$. Legyen $i = -\dfrac{y}{2u} + \dfrac{1}{u}a$. Ekkor $1, i$ is bázis és $i^2 = -1$. Tehát R izomorf a komplex számok testével.

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

(3) $x + \dfrac{y^2}{4} = 0$. Ha $i = -\dfrac{y}{2} + a$, 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

K szorzása nem kommutatív, s könnyen ellenőrizhető, hogy a báziselemeken a szorzás asszociatív. Ezért a 10.5. Tétel szerint **K** szorzása asszociatív. **K** elemeit *kvaterniók*nak 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 $\overline{a} = \lambda - \mu i - \nu j - \tau k$ elemet *a konjugáltjának* nevezzük. Könnyű ellenőrizni, hogy $a\overline{a} = \overline{a}a = \lambda^2 + \mu^2 + \nu^2 + \tau^2$. Az a elem *abszolútértéke* legyen $|a| = \sqrt{a\overline{a}}$. Ha $a \neq 0$, akkor $|a|^2 \neq 0$, és így

$$a\Big(\frac{1}{|a|^2}\overline{a}\Big) = \frac{1}{|a|^2}(a\overline{a}) = 1 = \frac{1}{|a|^2}(\overline{a}a) = \Big(\frac{1}{|a|^2}\overline{a}\Big)a.$$

Ezért az a elemnek $\dfrac{1}{|a|^2}\overline{a}$ a multiplikatív inverze. Tehát **K** ferdetest.

Összefoglaljuk a kvaterniók aritmetikájára vonatkozó legfontosabb tényeket.

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

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

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

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 **R**–algebrájában, mely izomorf a kvaterniók **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 **R**–algebrájával. ∎

11.6. Definíció. Jelölje R a valós számok, a komplex számok, illetve a kvaterniók **R**–algebrája közül valamelyiket, és tekintsük az

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

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:

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

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

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.*

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

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

Ekkor

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

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

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

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

$$u\Big(\frac{1}{|u|^2}\overline{u}\Big) = \frac{1}{|u|^2}(u\overline{u}) = 1 = \frac{1}{|u|^2}(\overline{u}u) = \Big(\frac{1}{|u|^2}\overline{u}\Big)u.$$

Ezért az u elemnek $\dfrac{1}{|u|^2}\overline{u}$ 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 $\dfrac{1}{u}$–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*

$$\overline{u} = x - yi - zj - tk - pE - qI - rJ - sK,$$

$$\overline{u}u = u\overline{u} = |u|^2 = x^2 + y^2 + z^2 + t^2 + p^2 + q^2 + r^2 + s^2,$$

$$\overline{\lambda u} = \lambda\overline{u}, \quad \overline{\overline{u}} = u, \quad |u| = |\overline{u}|, \quad \overline{u+u} = \overline{u} + \overline{u},$$

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

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

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 komlex számok testével.
(c) Rangja 4, és izomorf a kvaterniók ferdetestével.

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 komlex 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 $\sigma\colon R^2 \to \mathbf{R}$ leképezést *skaláris szorzat*nak nevezzük, ha bármely $a, b, c \in R$ és $\lambda \in \mathbf{R}$ esetén

$$\sigma(a,b) = \sigma(b,a), \quad \sigma(\lambda a, b) = \lambda\sigma(a,b), \quad \sigma(a+b,c) = \sigma(a,c) + \sigma(b,c),$$
$$\sigma(a,a) \geq 0 \quad \text{és} \quad \sigma(a,a) = 0 \;\Leftrightarrow\; a = 0.$$

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

$$\sigma\colon R^2 \to \mathbf{R}, \;\; (a,b) \mapsto \frac{1}{2}(a\overline{b} + b\overline{a}).$$

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 komlex számok testével.

(c) Rangja 4, és izomorf a kvaterniók ferdetestével.

(d) Rangja 8, és izomorf a Cayley–számok alternatív algebrájával.