I. NÉHÁNY FONTOS FOGALOM

1. Halmazok, relációk, függvények

A matematika alapfogalma a **halmaz**, amely szemléletesen dolgok összességét jelenti. Az alábbiakban az úgynevezett *naív halmazelmélet*et ismertetjük, a halmazelmélet rigorózus megalapozása a matematikai logika tárgykörébe tartozik. Kiindulásképpen adott halmaz az **univerzum** (alaphalmaz), amelyben minden dolog benne van, amit vizsgálunk. Ha adott egy A halmaz, akkor beszélünk annak **halmazelem**eiről, jelölés: $a \in A$, ha a egy dolog. Halmazról feltesszük, hogy bármely dologról egyértelműen eldönthető, hogy a halmazba tartozike avagy nem, és feltesszük, hogy az alaphalmaz elemei nem halmazok. Halmaz egy halmaz **hatványhalmaz**a, amelynek elemei a halmaz összes **részhalmaz**ai, azaz olyan halmazok, amelyeknek minden eleme szintén eleme a kiindulásként vett halmaznak. Jelölések: a B halmaz hatványhalmaza $\mathcal{P}(B)$, illetve $A \subseteq B$, az A halmaz a B halmaz részhalmaza illetve a B **halmaz tartalmazza** az A halmazt. Két **halmaz egyenlő** ha kölcsönösen tartalmazzák egymást, jelölés: $A = B$. Az A halmaz **valódi rész**e a B halmaznak ha részhalmaza B-nek, de nem egyenlő vele, jelölés: $A \subset B$. Kitüntetett halmaz az **üreshalmaz**, amelyre teljesül, hogy nincsen egyetlen eleme sem, jelölés: $\emptyset$. Ez része bármely halmaznak. Halmazt megadhatunk felsorolással, például ha az A halmaz elemei a_1, a_2, a_3, a_4, akkor a szokásos jelölés $A = \{a_1, a_2, a_3, a_4\}$, illetve kiválaszthatjuk halmazunk elemeit egy adott halmaz elemei közül valamely tulajdonsággal, jelölés: $A = \{a \in B | P(a)\}$, ahol a B halmaz elemei közül azok alkotják az A halmazt, amelyekre teljesül a P tulajdonság.

Tekintsük át a **halmazművelet**eket (a művelet pontos fogalmáról és a halmazműveletek tulajdonságairól később). Legyen A és B halmaz. **Unió**juk, $A \cup B$ az a halmaz, amelynek minden eleme eleme A-nak vagy B-nek. **Metszet**ük, $A \cap B$ az a halmaz, amelynek minden eleme eleme A-nak és B-nek is. **Különbség**ük, $A \setminus B$ az a halmaz, amelynek minden eleme eleme A-nak de nem eleme B-nek. Ha két halmaz metszete az üreshalmaz, akkor azt mondjuk, hogy **diszjunkt halmazok**. Ha az A halmaz része a B halmaznak, akkor A-nak B-re vonatkoztatott **komplementer**e, $\overline{A}$ az a halmaz, amelynek minden eleme eleme B-nek de nem eleme A-nak. **Szimmetrikus különbség**ük, $A \triangle B$ olyan halmaz, amelynek minden eleme eleme vagy A-nak vagy B-nek, de nem mindkettőnek. Ha $\mathcal{A}$ a $\mathcal{P}(B)$ hatványhalmaz nemüres részhalmaza, akkor képezhetjük a $\mathcal{A}$ **halmazrendszer** $\cup\mathcal{A}$, $\cup_{A\in\mathcal{A}} A$ **unió**ját, amely az a halmaz, amelynek minden eleme eleme legalább egy $\mathcal{A}$-beli A halmaznak. Képezhetjük a $\mathcal{A}$ **halmazrendszer** $\cap\mathcal{A}$, $\cap_{A\in\mathcal{A}} A$ **metszet**ét, amely az a halmaz, amelynek minden eleme eleme mindegyik $\mathcal{A}$-beli A halmaznak. Ha $\mathcal{A} = \{A_1, A_2, \dots, A_n\}$ véges n elemszámú halmazrendszer, akkor az unióra és a metszetre a szokásos jelölés $\cup_{i=1}^{n} A_i$ illetve $\cap_{i=1}^{n} A_i$.

Legyen A és B nemüres halmaz. Ekkor halmaz A és B **Descartes-szorzata**, amelynek elemei a **rendezett elempárok**. Egy A-beli a és egy B-beli b elem határoz meg egy $A \times B$ Descartes-szorzatbeli (a, b) elempárt, a-t az elempár első és b-t az elempár második tagjának nevezzük, két **elempár egyenlő**, ha megegyeznek első és második tagjaik is. Legyen $A_1, A_2, \dots, A_n$ halmaz. Ekkor halmaz $A_1, A_2, \dots, A_n$ **Descartes-szorzata**, amelynek elemei a **rendezett elem n-es**ek. A_i-beli a_i elemek $(i = 1, 2, \dots, n)$ határoznak meg egy $A_1 \times A_2 \times \cdots \times A_n$ Descartes-szorzatbeli $(a_1, a_2, \dots, a_n)$ elem n-est, a_i-t az elem n-es i-edik tagjának nevezzük $(i = 1, 2, \dots, n)$, két **elem n-es egyenlő**, ha rendre megegyeznek i-edik tagjaik $(i = 1, 2, \dots, n)$.

Az $A \times B$ halmaz részhalmazait **kétváltozós reláció**knak, az $A_1 \times A_2 \times \cdots \times A_n$ halmaz részhalmazait **n-változós reláció**knak nevezzük. Az $A \times A$ halmaz részhalmazait az A halmazon adott **kétváltozós homogén reláció**knak, az $\underbrace{A \times A \times \cdots \times A}_{n-\text{szer}}$ halmaz részhalmazait

az A halmazon adott **homogén n-változós reláció**knak nevezzük. Relációt, hasonlóan mint halmazt, felsorolással vagy tulajdonsággal adhatunk meg. Az $R \subseteq A \times B$ reláció esetén az $\{a \in A|$ létezik $b \in B$ úgy, hogy $(a,b) \in R\}$ halmazt az R reláció **értelmezési tartományának**, a B halmazt **érékkészletének**, az $R(A) = \{b \in B|$ létezik $a \in A$ úgy, hogy $(a,b) \in R\}$ halmazt **képhalmazának** nevezzük. Egy $a \in A$ **elem képe** a képhalmaz $R(a) = \{b \in B|\,(a,b) \in R\}$ részhalmaza. Az $R^{-1} = \{(b,a) \in B \times A|\,(a,b) \in R\}$ relációt az R **reláció inverzének** nevezzük.

Homogén kétváltozós relációknak az alábbi fontos típusait szokás vizsgálni. Lagyen $R \subset A \times A$ homogén reláció. Azt modjuk, hogy az R reláció **reflexív**, ha minden $a \in A$ esetén $(a,a) \in R$; **tranzitív**, ha $(a,b) \in R$ és $(b,c) \in R$ esetén $(a,c) \in R$; **szimmetrikus**, ha $(a,b) \in R$-ből $(b,a) \in R$ következik; **antiszimmetrikus**, ha $(a,b) \in R$ és $(b,a) \in R$ esetén $a = b$. **Rendezési reláció**nak nevezünk egy olyan kétváltozós homogén relációt, amely reflexív, antiszimmetrikus és tranzitív. Az A halmazon adott **rendezési reláció teljes (vagy lineáris)**, ha minden $a, b \in A$ elemre teljesül, hogy $(a,b) \in A$ vagy $(b,a) \in A$. Ha az A halmazon adott egy (lineáris) rendezési reláció, akkor azt is szoktuk mondani, hogy A **(lineárisan) rendezett halmaz**. **Ekvivalenciareláció**nak nevezünk egy olyan kétváltozós homogén relációt, amely reflexív, szimmetrikus és tranzitív. Ehhez szorosan kapcsolódó fogalom egy **halmaz osztályozása**: legyen A egy halmaz és $\mathcal{C}$ részhalmazainak egy nemüres rendszere, amely elemeit **osztály**oknak nevezünk, úgy, hogy az osztályok páronként diszjunktak és uniójuk az egész A halmaz. A két fogalom kapcsolatáról szól az alábbi

1.1. Állítás. *Legyen A egy nemüres halmaz. Ha adva van egy S ekvivalenciareláció A-n, akkor az ekvivalenciaosztályok megadásával, azaz egy osztályba sorolva egy adott elemmel relációban álló elemeket az A halmaz osztályozását kapjuk. Megfordítva, ha adva van egy $\mathcal{C}$ osztályozása az A halmaznak, akkor $\cup\{C \times C|C \in \mathcal{C}\}$ ekvivalenciareláció az A halmazon.*

Bizonyítás. Mivel ekvivalenciareláció reflexív, az ekvivalenciaosztályok uniója az egész A halmaz. Ha $(a,c),(b,c) \in S$ akkor a szimmetria miatt $(a,c),(c,b) \in S$ és a tranzitivitás miatt $(a,b) \in S$, és ismét a szimmetria miatt $(b,a) \in S$; így ha $(a,d) \in S$ akkor a tranzitivitás miatt $(b,d) \in S$ és $R(a) \subseteq R(b)$. Hasonlóan $R(b) \subseteq R(a)$. Kaptuk, hogy ha az a és b elemek ekvivalenciaosztályainak metszete nemüres, akkor egybeesnek.

Megfordítva, az $R = \cup\{C \times C|C \in \mathcal{C}\}$ reláció reflexív, mivel az osztályok uniója az egész A halmaz. Ha $(a,b),(b,c) \in R$ akkor a, b és c ugyanannak az osztálynak az elemei, így szükségképpen $(a,c) \in R$. Hasonlóan ha $(a, b \in R)$ akkor a és b ugyanannak az osztálynak az elemei, így szükségképpen $(b,a) \in R$. R valóban ekvivalenciareláció. □

Az R ekvivalenciareláció osztályainak halmazát **faktorhalmaz**nak nevezzük és A/R-rel jelöljük.

Az $f \subseteq A \times B$ relációról azt mondjuk, hogy (egyváltozós) **függvény** vagy **leképezés**, ha f értelmezési tartománya az egész A halmaz, és minden $a \in A$ elem $f(a) = \{b\}$ képe egyelemű halmaz. Azt mondjuk, hogy az f függvény az a **elemhez** az $f(a) = b$ **elemet rendeli**, illetve hogy az a **elem képe** a b elem. Jelölés: $f : A \to B, a \mapsto f(a) = b$. Analóg módon határozható meg a többváltozós függvény fogalma. Két **függvény egyenlő**, ha megegyeznek értelmezési tartományaik és értékkészleteik, és ugyanahhoz az elemhez ugyanazt az elemet rendelik. Legegyszerűbb függvény az $1_A : A \to A$, $a \mapsto a$ **identikus leképezés**. Az $f : A \to B$ függvényről azt mondjuk, hogy **injektív**, ha $f(a) = f(a')$-ből $a = a'$ következik; azt mondjuk, hogy **szürjektív**, ha az $f(A)$ képhalmaz az egész B értékkészlet; azt mondjuk, hogy **bijektív**, ha injektív és szürjektív.

Két függvény, $f : A \to B$ és $g : B \to C$ meghatározza a **kompozíciószorzat**ukat, a $g \circ f : A \to C$, $a \mapsto g \circ f(a) = g(f(a))$ függvényt. Az alábbi állítás bizonyítása gyakorlat.

1.2.Állítás. *Ha $f : A \to B$, $g : B \to C$ és $h : C \to D$ függvények, akkor $(h \circ g) \circ f = h \circ (g \circ f)$.*

Egy függvény inverze nem mindig függvény. Ha egy függvény (mint relćió) inverze is függvény, akkor azt mondjuk, hogy **invertálható függvény**. Az invertálhatóságot jellemzhetjük az alábbi módon.

1.3.Állítás. *Legyen $f : A \to B$ függvény. Az alábbi állítások ekvivalensek:*
(i) f invertálható függvény;
(ii) létezik $g : B \to A$ függvény úgy, hogy $f \circ g = 1_B$ és $g \circ f = 1_A$;
(iii) f bijektív függvény.

Bizonyítás. (i)$\Longrightarrow$(ii) Legyen g az f inverzfüggvénye, így nyilván teljesül a (ii)-ben szereplő két tulajdonság.

(ii)$\Longrightarrow$(iii) Ha $f(a) = f(a')$ akkor $g \circ f = 1_A$ miatt $a = 1_A(a) = g(f(a)) = g(f(a')) = 1_A(a') = a'$, és az injektivitás teljesül. Az $f \circ g = 1_B$ tulajdonság miatt $f(A) \supseteq f(g(B)) = 1_B(B) = B$, és a szürjektivitás világos.

(iii)$\Longrightarrow$(i) Mivel az f függvény szürjektív, az f^{-1} inverzreláció értelmezési tartománya az egész B halmaz. Az injektivitás miatt pedig az $f^{-1}(b)$ halmaz egyelemű. □

2. Műveletek, tulajdonságaik, algebrai struktúrák

Legyen A egy nemüres halmaz. A $* : A \to A$, $a \mapsto a^*$ függvényről azt mondjuk, hogy **egyváltozós (unér) művelet** az A halmazon. A $* : A \times A \to A$, $(a, b) \mapsto a * b$ függvényről azt mondjuk, hogy **kétváltozós (binér) művelet** az A halmazon. A $* : \underbrace{A \times A \times \cdots \times A}_{n-\text{szer}} \to A$, $(a_1, a_2, \dots, a_n) \mapsto *(a_1, a_2, \dots, a_n)$ függvényről azt mondjuk, hogy **n-változós (n-ér) művelet** az A halmazon. Ha az A halmazon adva van n darab $*, \circ, \dots$ művelet, akkor az $(A, *, \circ, \dots)$ rendezett elem $n+1$-est **n-műveletes algebrai struktúr**ának nevezzük.

Az alábbi műveleti tulajdonságokat szokás tanulmányozni. Ha másként nem említjük, művelet alatt kétváltozós műveletet fogunk érteni. Legyen $(A, *)$ algebrai struktúra. A $*$ műveletről azt mondjuk hogy

- **asszociatív**, ha minden $a, b, c \in A$ elemre $(a * b) * c = a * (b * c)$;
- **kommutatív**, ha minden $a, b \in A$ elemre $a * b = b * a$;
- **idempotens**, ha minden $a \in A$ elemre $a * a = a$;
- **invertálható**, ha minden $a, b \in A$ elemhez létezik $u, v \in A$ elem úgy, hogy $a * u = b$ és $v * a = b$.

Kitüntetett elem az

- $e \in A$ **neutrális elem**: minden $a \in A$ elem esetén $e * a = a * e = a$;
- $z \in A$ **zéruselem**: minden $a \in A$ elem esetén $z * a = a * z = z$;
- $a \in A$ **zérusosztó**: létezik $b \in A$ úgy, hogy $b \neq z$ és $a * b = z$ vagy $b * a = z$, ahol z zéruselem;
- az $a \in A$ **elem** $b \in A$ **inverze**: $a * b = b * a = e$, ahol e neutrális elem.

Azokat az elemeket, amelyeknek létezik inverzük, **invertálható elem**eknek vagy **egység**eknek nevezzük. Azt mondjuk, hogy egy zéruselemet tartalmazó struktúra **zérusosztómentes**, ha az egyedüli zérusosztó a zéruselem. Az $a \in A$ **elemmel lehet egyszerűsíteni**, ha minden $b, c \in A$ elem esetén abból, hogy $a * b = a * c$ vagy $b * a = c * a$ következik $b = c$.

Legyen $(A, *, \circ)$ algebrai struktúra. Azt mondjuk, hogy

- a $*$ művelet **disztributív** a $\circ$ műveletre nézve, ha minden $a, b, c \in A$ elemre $a * (b \circ c) = (a * b) \circ (a * c)$ és $(a \circ b) * c = (a * c) \circ (b * c)$;
- a $*$ művelet **abszorbtív** a $\circ$ műveletre nézve, ha minden $a, b, c \in A$ elemre $a * (a \circ b) = a$.

A következő nevezetes struktúratípusokat vizsgálják leggyakrabban. Egyműveletes struktúráról azt mondjuk, hogy
– **félcsoport**, ha a művelet asszociatív;
– **monoid**, ha félcsoport, és létezik neutrális eleme;
– **kommutatív félcsoport**, ha félcsoport, és a művelet kommutatív;
– **félháló**, ha kommutatív félcsoport és a művelet idempotens;
– **csoport**, ha monoid és minden elemnek van inverze;
– **Abel- (vagy kommutatív) csoport** ha csoport és a művelet kommutatív.

Legyen $(A, +, \cdot)$ kétműveletes algebrai struktúra, amelyben a két művelet az összeadás és a szorzás. Az $(A, +)$ struktúrát **additív**, az $(A, \cdot)$ struktúrát **multiplikatív struktúrá**nak nevezzük. Azt mondjuk, hogy az $(A, +, \cdot)$ struktúra
– **gyűrű**, ha az additív struktúra Abel-csoport, a multiplikatív struktúra félcsoport, és a szorzás disztributív az összeadásra nézve;
– **kommutatív gyűrű**, ha gyűrű és a szorzás kommutatív;
– **egységelemes gyűrű**, ha legalább kételemű gyűrű és a multiplikatív struktúrában létezik neutrális elem.

Gyűrűben szokás az additív neutrális elemet **nullá**nak nevezni és 0-val jelölni; az a elem additív inverzét **ellentett**jének nevezni és $-a$-val jelölni; a multiplikatív neutrális elemet (ha létezik) **egységelem**nek nevezni és 1-gyel jelölni; az a elem multiplikatív inverzét **reciprok**ának nevezni és a^{-1}-gyel jelölni.

Az asszociativitásból következő egyszerű tulajdonságok az alábbiak.

2.1. Állítás. *Legyen $(A, \cdot)$ félcsoport. Ekkor:*
(i) Tetszőleges számú tényezőből álló szorzat értéke független a zárójelezéstől.
(ii) Ha az $(A, \cdot)$ struktúra neutrális elemes, akkor egyetlen neutrális elem van az A félcsoportban, és ha az $a \in A$ elemnek létezik a^{-1} inverze, akkor az egyértelmű.

Bizonyítás. (i) Legyen az $a_1, \dots, a_n \in A$ elemek tetszőlegesen zárójelezett szorzata t_n, és legyen $l_n = (\dots((a_1a_2)a_3)\dots)a_n$ balrarendezett szorzat. Indukcióval n szerint belátjuk, hogy $t_n = l_n$. $n = 3$ esetén az állítás éppen a szorzás asszociativitása. Tegyük fel, hogy n-nél kisebb tényezős szorzatok ($n > 3$) tetszőlegesen zárójelezhetők. Ha $t_n \neq l_n$ akkor $t_n = t_k u$, ahol u az $a_{k+1}, \dots, a_n$ elemek valamely szorzata. Indukció alapján $t_k = l_k$ és $u = a_{k+1}(a_{k+2}(\dots(a_{n-1}a_n)\dots))$ jobbrarendezett szorzat, azaz az asszociativitás többszöri alkalmazásával

$$t_n = l_k(a_{k+1}(a_{k+2}(\dots(a_{n-1}a_n)\dots))) = (l_ka_{k+1})(a_{k+2}(a_{k+3}(\dots(a_{n-1}a_n)\dots))) =$$

$$l_{k+1}(a_{k+2}(\dots(a_{n-1}a_n)\dots)) = \dots = l_{n-2}(a_{n-1}a_n) = l_{n-1}a_n = l_n.$$

(ii) Legyen e, f neutrális elem. Ekkor mivel f neutrális elem, $ef = e$, de mivel e is neutrális elem, $ef = f$, azaz $e = f$. Ha $aa^{-1} = a^{-1}a = e$ és $ab = ba = e$, akkor $b = eb = (a^{-1}a)b = a^{-1}(ab) = a^{-1}e = a^{-1}$. □

Mivel (multiplikatíve írt) monoidban ha az a és b elemnek van inverze akkor az ab elemnek is van, $b^{-1}a^{-1}$, monoid egységei csoportot alkotnak (ellenőrizze!), az úgynevezett **egységcsoport**ot. Ha A egy halmaz, akkor az összes $A \to A$ függvény halmazán a kompozíciószorzás művelet, amelyre nézve a függvények halmaza félcsoport 1.2 alapján, amelyben az identikus leképezés neutrális elem. 1.3 alapján ezek közül az egységek a bijektív leképezések, a **permutációk**, ezeknek a csoportja az A halmaz **szimmetrikus csoport**ja.

Gyakorlatként lássa be, hogy kommutatív félcsoportban teljesülnek a hatványozás azonosságai. Gyakorlásképpen lássa be, hogy zéruselem csak egy lehet egy struktúrában,

monoidban egységgel lehet egyszerűsíteni, és hogy zéruselemes monoidban egység nem zérusosztó.

Legyen A egy halmaz, az úgynevezett **ábécé**, elemei a **betűk**. Képezzünk a betűkből (véges hosszú) szavakat, ezek közötti művelet legyen a **konkatenáció**, az egymásutánírás, amelyet asszociatívnak tekintünk. Kaptuk az úgynevezett **szabad félcsoportot**. Bővítsük ki az A ábécét újabb betűkkel az $A \cup A^{-1}$ ábécévé, ahol $A^{-1} = \{a^{-1} | \, a \in A\}$. Tekintsük az $A \cup A^{-1}$ ábécé betűiből képzett szavak W halmazát, amelybe beleértjük az üres szót is. Egy W-beli szót **redukált alakú**nak nevezünk, ha benne nem áll egymás mellett a illetve a^{-1} alakú betű. Tetszőleges W-beli szóhoz tartozik redukált alakú szó, az aa^{-1} illetve $a^{-1}a$ alakú szórészletek helyébe az üres szót írva, esetleg több lépésben. Legyen F a redukált alakú szavak halmaza (az üres szóval együtt). Két F-beli szó konkatenáltja legyen az egymásutánírt szó (ami W eleme) redukált alakja (ez már biztosan F-beli), a konkatenációt ismét asszociatívnak tekintve. Ekkor a konkatenáció művelet a redukált alakú szavak F halmazán, amely erre a műveletre nézve csoport (ellenőrizze!), amelyet az A ábécé feletti **szabad csoport**nak nevezünk.

A disztributivitást felhasználva kapjuk az alábbiakat.

2.2.Állítás. *Legyen az $(A, +, \cdot)$ struktúra gyűrű. Ekkor:*
(i) az additív neutrális elem multiplikatív zéruselem;
(ii) minden $a \in A$ elemre $(-a)b = a(-b) = -(ab)$ és $(-a)(-b) = ab$;
(iii) ha $(A, +, \cdot)$ egységelemes gyűrű, akkor minden $a \in A$ elemre $-a = (-1)a$.

Bizonyítás. (i) Legyen $a \in A$. Ekkor, mivel 0 additív neutrális elem, és a disztributív törvény teljesül, $0a = (0 + 0)a = 0a + 0a$, és mindkét oldalhoz hozzáadva $-0a$-t kapjuk, hogy $0 = 0a$. Hasonlóan adódik, hogy $0 = a0$.

(ii) Legyen $a, b \in A$. Ekkor, felhasználva a disztributivitást és (i)-et, $ab + (-a)b = (a + (-a))b = 0b = 0$, azaz ab ellentettje $(-a)b$. Hasonlóan ab az $a(-b)$ elem ellentettje is. Ezt a két tényt alkalmazva adódik, hogy $(-a)(-b) = ab$.

(iii) A (ii)-es állítás szerint $(-a)b = -ab$; legyen $a = 1$. □

Gyakorlásképpen lássa be, hogy kommutatív gyűrűben teljesül a binomiális tétel.

A kommutatív, egységelemes és zérusosztómentes gyűrűt **integritástartomány**nak nevezzük. A kommutatív, egységelemes gyűrűt, amelyben minden nemnulla elemnek van multiplikatív inverze, **testnek** nevezzük. Gyakorlásként bizonyítsa be, hogy test integritástartomány.

Az $(A, \vee, \wedge)$ struktúrát
- **háló**nak nevezzük, ha az $(A, \vee)$ és a $(A, \wedge)$ struktúra félháló, és mindkét művelet abszorbtív a másikra nézve.
- **disztributív háló**nak nevezzük, ha háló, és mindkét művelet disztributív a másikra nézve.

Szokás a $\vee$ műveletet **diszjunkció**nak, a $\wedge$ műveletet **konjunkció**nak nevezni.

A hálók és a rendezett struktúrák között szoros kapcsolat áll fenn. Legyen A rendezett halmaz a $\leq$ relációra nézve. Ha $a, b \in A$, és $\min\{a, b\}$ olyan elem, hogy $\min\{a, b\} \leq a$, $\min\{a, b\} \leq b$, és ha $c \leq a$, $c \leq b$ akkor $c \leq \min\{a, b\}$, akkor azt mondjuk, hogy $\min\{a, b\}$ az a és b elemek **minimum**a. Ha $a, b \in A$, és $\max\{a, b\}$ olyan elem, hogy $a \leq \max\{a, b\}$, $b \leq \max\{a, b\}$, és ha $a \leq c$, $b \leq c$ akkor $\max\{a, b\} \leq c$, akkor azt mondjuk, hogy $\max\{a, b\}$ az a és b elemek **maximum**a. Azt mondjuk, hogy a A **hálószerűen rendezett halmaz**, ha bármely két elemnek létezik minimuma és maximuma.

2.3.Állítás. *Legyen A egy halmaz. Ha $(A, \vee, \wedge)$ háló, akkor az*

$$a \leq b \;\; ha \;\; a \vee b = b$$

relációval A hálószerűen rendezett halmaz. Megfordítva, ha A hálószerűen rendezett halmaz a $\leq$ relációra nézve, akkor az $(A, \max, \min)$ struktúra háló.

Bizonyítás. Legyen $(A, \vee, \wedge)$ háló. Az idempotencia miatt $a \vee a = a$ és a $\leq$ reláció reflexív. Ha $a \leq b$ és $b \leq a$ azaz $a \vee b = b$ és $b \vee a = a$ akkor a kommutativitás miatt $a = b$, és a $\leq$ reláció antiszimmetrikus. Ha $a \leq b$, $b \leq c$ azaz $a \vee b = b$ és $b \vee c = c$ akkor $a \vee c = a \vee (b \vee c) = (a \vee b) \vee c = b \vee c = c$ és $a \leq c$, a tranzitivitás is világos. Legyen $\max\{a, b\} = a \vee b$. Ekkor $a \vee \max\{a, b\} = a \vee (a \vee b) = (a \vee a) \vee b = a \vee b = \max\{a, b\}$, és $a \leq \max\{a, b\}$; hasonlóan $b \leq \max\{a, b\}$. Ha $a \leq c$ és $b \leq c$ azaz $a \vee c = c$ és $b \vee c = c$ akkor $\max\{a, b\} \vee c = (a \vee b) \vee c = a \vee (b \vee c) = a \vee c = c$ és $\max\{a, b\} \leq c$, a maximalitás teljesül. Hasonlóan kapjuk, hogy $a \wedge b$ minimum (ellenőrizze!).

Megfordítva, legyen A hálószerűen rendezett halmaz. Az $(A, \min)$ pár nyilván algebrai struktúra.

Asszociativitás. Legyen $u = \min\{\min\{a, b\}, c\}$ és $v = \min\{a, \min\{b, c\}\}$. Ekkor $u \leq \min\{a, b\}$ és $u \leq c$, ahonnan $u \leq a$, $u \leq b$ és $u \leq c$. Innen $u \leq a$ és $u \leq \min\{b, c\}$, adódik, hogy $u \leq v$. Analóg módon $v \leq u$ (ellenőrizze!), és az antiszimmetria miatt $u = v$.

Kommutativitás, idempotencia. Ezek a tulajdonságok nyilvánvalóak a művelet definíciójából.

Az $(A, \min)$ pár valóban félháló. Hasonlóan kapjuk, hogy az $(A, \max)$ pár is félháló (ellenőrizze!).

A két abszorbtív tulajdonságból csak az egyiket tekintjük, a másik bizonyítása gyakorlat. Legyen $c = \min\{a, \max\{a, b\}\}$. Ekkor nyilván $c \leq a$. Továbbá $a \leq a$ és $a \leq \max\{a, b\}$ miatt $a \leq \min\{a, \max\{a, b\}\} = c$, így az antiszimmetriából adódik, hogy $a = c$. Beláttuk az összes hálótulajdonságot. □

Legyen 0 illetve 1 az $(A, \vee, \wedge)$ háló eleme úgy, hogy minden $a \in A$ elemre $0 \vee a = a$ illetve $1 \wedge a = a$. Ekkor 0-t a **háló zéruseleméne**k illetve 1-et a **háló egységeleméne**k nevezzük. Könnyen látható, hogy az indukált rendezésre nézve a 0 a legkisebb, 1 a legnagyobb elem. Ha $a, \overline{a} \in A$ olyan elemek, hogy $a \vee \overline{a} = 1$ és $a \wedge \overline{a} = 0$ akkor azt mondjuk, hogy $\overline{a}$ az a elem **komplementuma**. **Boole-algebrá**nak nevezzük az olyan disztributív hálót, amelyben létezik zéruselem és egységelem, és minden elemnek van komplementuma. Minimális Boole-algebra az igaz és hamis logikai értékek halmaza a ,,vagy" és az ,,és" műveletekkel. Gyakorlásképpen lássa be, hogy Boole-algebrában a komplementum egyértelmű.

Boole-algebrában teljesülnek az úgynevezett *De Morgan*-törvények:

2.4. Állítás. *Boole-algebra a, b elemeire $\overline{a \vee b} = \overline{a} \wedge \overline{b}$ és $\overline{a \wedge b} = \overline{a} \vee \overline{b}$.*

Bizonyítás. Csak az egyik azonosságot látjuk be, a másik bizonyítása gyakorlat:

$$(a \vee b) \vee (\overline{a} \wedge \overline{b}) = a \vee (b \vee \overline{a} \wedge \overline{b}) = a \vee ((b \vee \overline{a}) \wedge (b \vee \overline{b})) = a \vee ((b \vee \overline{a}) \wedge 1) = a \vee (b \vee \overline{a})$$

$$= (a \vee \overline{a}) \vee b = 1 \vee b = 1$$

illetve

$$(a \vee b) \wedge (\overline{a} \wedge \overline{b}) = ((a \vee b) \wedge \overline{a}) \wedge \overline{b}) = ((a \wedge \overline{a}) \vee (b \wedge \overline{a})) \wedge \overline{b} = (0 \vee (b \wedge \overline{a})) \wedge \overline{b}$$

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

Innen következik az első De Morgan-törvény. □

Legyen H egy halmaz. A $\mathcal{P}(H)$ hatványhalmaz nemüres részhalmazát az unió és a metszet műveletével együtt **halmaztest**nek nevezzük, ha zárt az unió, a metszet és a komplementer képzésére nézve. Alapvető fontosságú a

2.5.Tétel. *Halmaztest Boole-algebra.*

Bizonyítás. Legyen $\mathcal{H}$ a halmaztest. A $(\mathcal{H}, \cup)$ pár nyilván struktúra. Három halmaz uniójának elemei, akárhogyan zárójelezve, azok az elemek, amelyek legalább az egyik halmazban benne vannak, így az unióképzés asszociatív. Két halmaz uniójának elemei, bármilyen sorrendben, azok az elemek, amelyek legalább az egyik halmazban benne vannak, így az unióképzés kommutatív. Egy halmaznak önmagával vett uniójának elemei nyilván a halmaz elemei, így az unióképzés idempotens. A $(\mathcal{H}, \cup)$ struktúra félháló. Hasonlóan egyszerű meggondolásokkal a $(\mathcal{H}, \cap)$ struktúra is félháló.

A két abszorbtív tulajdonságból az egyiket tekintjük, a másik ellenőrzése gyakorlat. Legyen $a \in A \cup (A \cap B)$. Ekkor $a \in A$ vagy $a \in A \cap B$, de $A \cap B$ részhalmaza A-nak, így mindenképpen $a \in A$, azaz $A \cup (A \cap B) \subseteq A$. A fordított $A \subseteq A \cup (A \cap B)$ tartalmazás nyilvánvaló, és $A = A \cup (A \cap B)$. Eddig beláttuk, hogy $(\mathcal{H}, \cup, \cap)$ háló.

A két disztributivitásból csak az egyiket látjuk be, a másik gyakorlat. Legyen $a \in A \cup (B \cap C)$. Ekkor $a \in A$ vagy $a \in B \cap C$. Innen világos, hogy az a elem benne van az $A \cup B$ halmazban és az $A \cup C$-ben is. Így $A \cup (B \cap C) \subseteq (A \cup B) \cap (A \cup C)$. Legyen most $a \in (A \cup B) \cap (A \cup C)$. Ekkor $a \in A \cup B$ és $a \in A \cup C$. Ha $a \in A$ akkor nyilván $a \in A \cup (B \cap C)$. Ha $a \notin A$ akkor szükségképpen $a \in B$ és $a \in C$ is teljesül, azaz $a \in B \cap C \subseteq A \cup (B \cap C)$. Így $(A \cup B) \cap (A \cup C) \subseteq A \cup (B \cap C)$. A kétoldali tartalmazás miatt a két halmaz megegyezik. Az unió kommutativitása miatt $(A \cap B) \cup C = (A \cup C) \cap (B \cup C)$.

Nyilvánvaló, hogy az üreshalmaz illetve az egész H halmaz benne van a halmaztestben, és annak zéruseleme illetve egységeleme, továbbá egy halmaz és komplementerének uniója H, metszete az üreshalmaz. □

Ennek a tételnek bizonyos értelemben igaz a megfordítása is.

II. A SZÁMFOGALOM FELÉPÍTÉSE

3. A természetes és egész számok

Feltesszük, hogy adva van egy halmaz, a **természetes számok halmaza**, amelyet $\mathbb{N}$-nel jelölünk, elemei a **természetes számok**, és teljesülnek az alábbi úgynevezett *Peano*-axiómák:

(1) létezik egy nullának nevezett, 0-val jelölt eleme $\mathbb{N}$-nek;
(2) létezik egy $' : \mathbb{N} \to \mathbb{N}$, $a \mapsto a'$ injektív leképezés, ahol az a' természetes számot az a természetes szám rákövetkezőjének nevezzük, és amelyre teljesül az alábbi két tulajdonság:
(3) nem létezik $a \in \mathbb{N}$ természetes szám , amelyre $a' = 0$;
(4) (a teljes indukció axiómája) ha A az $\mathbb{N}$ halmaz részhalmaza, A-nak eleme a 0 és A tetszőleges elemével együtt tartalmazza annak rákövetkezőjét is, akkor $A = \mathbb{N}$.

A szokásos jelölések és elnevezések: 0'=1 egy, 1'=2 kettő, 2'=3 három, és így tovább. **Végtelen halmaz**nak nevezünk egy halmazt, ha létezik bijekció a halmaz és valódi részhalmaza között. A rákövetkezés leképezés bijekció az $\mathbb{N}$ és $\mathbb{N} \setminus \{0\}$ halmazok között (ellenőrizze!), ezért a természetes számok halmaza végtelen. Ellenkező esetben **véges halmaz**ról beszélünk.

Az utolsó Peano-axiómán alapul a **rekurzív definíció** módszere. Természetes számot, mint paramétert tartalmazó fogalmakat vagy elemeket határozunk meg oly módon, hogy megadjuk a 0-hoz tartozót, és azt, hogy tetszőleges n természetes szám esetén az n-hez tartozó fogalom illetve elem ismeretében hogyan határozható meg az n' rákövetkezőhöz tartozó. A **természetes számok közötti összeadás és szorzás** műveletét így definiáljuk: tetszőleges $a \in \mathbb{N}$ természetes számra legyen $a+0 = a$, $a \cdot 0 = 0$, továbbá ha $b \in \mathbb{N}$ természetes szám, akkor legyen $a + b' = (a + b)'$ és $ab' = ab + a$. Teljesülnek a megszokott műveleti tulajdonságok, mint azt látni fogjuk. A bizonyítás módszere a **teljes indukció**: egy állítást, amelyet az összes természetes számra látunk be, az utolsó Peano-axióma alapján elegendő igazolni 0-ra és, feltételezve, hogy igaz valamely n természetes számra, n'-re.

3.1.Tétel.

(i) *az $(\mathbb{N}, +)$ struktúra kommutatív félcsoport, amelyben lehet egyszerűsíteni, neutrális eleme a 0;*
(ii) *az $(\mathbb{N}, \cdot)$ struktúra kommutatív félcsoport, neutrális eleme az 1, nemnulla elemmel lehet egyszerűsíteni;*
(iii) *a szorzás az összeadásra nézve disztributív.*

Bizonyítás. Legyen a, b és c természetes szám.

(i) *Asszociativitás.* Nyilván $(a+b)+0 = a+b = a+(b+0)$, és tegyük fel, hogy $(a+b)+c = a+(b+c)$. Ekkor, a definíció és az indukciós feltétel alkalmazásával $(a+b)+c' = ((a+b)+c)' = a+(b+c)' = a+(b+c')$.

Neutrális elem. A definíció szerint $a + 0 = a$. Nyilván $0 + 0 = 0$, és tegyük föl, hogy $0 + a = a$. Ekkor $0 + a' = (0 + a)' = a'$.

Kommutativitás. Mivel 0 neutrális elem, $a + 0 = 0 + a$, és tegyük föl, hogy $a + b = b + a$. Ekkor $a + b' = (a + b)' = (b + a)' = b + a'$, így elegendő belátni, hogy $b + a' = b' + a$, újból indukcióval. Nyilván $b + 0' = (b + 0)' = b' = b' + 0$, és tegyük föl, hogy $b + a' = b' + a$. Ekkor $b + a'' = (b + a')' = (b' + a)' = b' + a'$.

Egyszerűsítés. A kommutativitás miatt elég a jobboldali egyszerűsítést belátni. Mivel 0 neutrális elem, $a + 0 = b + 0$-ból következik $a = b$. Tegyük föl, hogy $a + c = b + c$ esetén

$a = b$. Legyen $a + c' = b + c'$; ekkor $(a + c)' = (b + c)'$, és a rákövetkezés injektivitása miatt $a + c = b + c$, ahonnan az indukciós feltétel miatt $a = b$ következik.

A (ii) állítás belátása gyakorlat. A *disztributivitás*t is könnyen igazolhatjuk: $a(b+0) = ab = ab+0 = ab+a0$, és tegyük föl, hogy $a(b+c) = ab+ac$. Ekkor $a(b+c') = a(b+c)' = a(b+c)+a = (ab + ac) + a = ab + (ac + a) = ab + ac'$. Mivel a szorzás kommutatív, $(a + b)c = ac + bc$ is teljesül. □

Azt mondjuk, hogy az a **természetes szám kisebb vagy egyenlő** mint a b természetes szám, ha valamely c természetes számra $b = a+c$, jelölés: $a \leq b$, illetve az éles egyenlőtlenségé $a < b$. Gyakorlásképpen lássa be, hogy ez lineáris rendezés a természetes számok halmazán, és természetes számok tetszőleges nemüres halmazában van legkisebb elem. Nyilván a 0 minimális elem.

A természetes számok körében a négy alapművelet közül kettőt el lehet végezni. Ahhoz, hogy a kivonást is el lehessen végezni, bővíteni kell a számhalmazt. Legyen a_1 és a_2 természetes szám. Az $a_1 - a_2$ különbséget (ami nem biztos, hogy természetes szám) jelképezze az (a_1, a_2) kissebbítendő – kivonandó elempár. Ennek megfelelően két elempár megegyezik, ha ugyanannyi az $a_1 - a_2 = b_1 - b_2$ különbségük, azaz $a_1 + b_2 = a_2 + b_1$. Az összeadást és a szorzást is elvégezhetjük a kissebbítendő – kivonandó elempárok között: $(a_1-a_2)+(b_1-b_2) = (a_1+b_1)-(a_2+b_2)$ illetve $(a_1-a_2)(b_1-b_2) = (a_1b_1+a_2b_2)-(a_1b_2+a_2b_1)$. Ezeket az észrevételeket szem előtt tartva konstruálhatjuk meg az egész számokat.

3.2.Tétel. *Legyen $Z = \mathbb{N} \times \mathbb{N}$ Descartes-szorzat, és definiáljuk a ρ relációt a Z halmazon a következőképpen: $(a_1, a_2)\rho(b_1, b_2)$ ha $a_1 + b_2 = a_2 + b_1$, Ekkor ρ ekvivalencia-reláció, (a_1, a_2) ekvivalencia-osztályát jelölje $\overline{(a_1, a_2)}$, az ekvivalencia-osztályok faktorhalmazát jelölje $\mathbb{Z}$. Legyen továbbá*

$$\overline{(a_1, a_2)} + \overline{(b_1, b_2)} = \overline{(a_1 + b_1, a_2 + b_2)}, \quad \overline{(a_1, a_2)} \cdot \overline{(b_1, b_2)} = \overline{(a_1b_1 + a_2b_2, a_1b_2 + a_2b_1)}$$

az összeadás és a szorzás művelete. Ekkor a $(\mathbb{Z}, +, \cdot)$ struktúra integritástartomány.

Bizonyítás. A bizonyítás folyamán felhasználjuk külön hivatkozás nélkül a 3.1 tételt. Legyen $a_1, a_2, b_1, b_2, c_1, c_2, d_1, d_2$ természetes szám.

A ρ reláció ekvivalencia. A ρ reláció reflexív, mivel $a_1+a_2 = a_2+a_1$; szimmetrikus, mivel ha $((a_1, a_2), (b_1, b_2)) \in \rho$ azaz $a_1 + b_2 = a_2 + b_1$ akkor $b_1 + a_2 = b_2 + a_1$ azaz $((b_1, b_2), (a_1, a_2)) \in \rho$; tranzitív, mivel ha $((a_1, a_2), (b_1, b_2)) \in \rho$ és $((b_1, b_2), (c_1, c_2)) \in \rho$ azaz $a_1 + b_2 = a_2 + b_1$ és $b_1 + c_2 = b_2 + c_1$ akkor $a_1 + b_1 + c_2 = a_1 + b_2 + c_1$, ahonnan $a_1 + b_1 + c_2 = a_2 + b_1 + c_1$, és egyszerűsítés után $a_1 + c_2 = a_2 + c_1$ adódik, azaz $((a_1, a_2), (c_1, c_2)) \in \rho$.

A továbbiakban legyen $a = \overline{(a_1, a_2)}$, $b = \overline{(b_1, b_2)}$, $c = \overline{(c_1, c_2)}$, $d = \overline{(d_1, d_2)}$.

Az összeadás jóldefiniált. Legyen $a = c$ és $b = d$, azaz $a_1 + c_2 = a_2 + c_1$ és $b_1 + d_2 = b_2 + d_1$. Be kell látni, hogy $a + b = c + d$, azaz $a_1 + b_1 + c_2 + d_2 = a_2 + b_2 + c_1 + d_1$. Ez igaz, ha $a_2 + b_1 + c_1 + d_2 = a_2 + b_2 + c_1 + d_1$, ami teljesül, ha $a_2 + b_1 + d_2 = a_2 + b_2 + d_1$, ami pedig a második feltételből következik.

Az összeadás asszociatív és kommutatív. Nyilvánvaló, mivel a természetes számok összeadása is ilyen.

A $\overline{(0, 0)}$ elem neutrális elem, és a ellentettje $-a = \overline{(a_2, a_1)}$. Világos, hogy $\overline{(a_1, a_2)} + \overline{(0, 0)} = \overline{(0, 0)}+\overline{(a_1, a_2)} = \overline{(a_1, a_2)}$; továbbá $\overline{(a_1, a_2)}+\overline{(a_2, a_1)} = \overline{(a_2, a_1)}+\overline{(a_1, a_2)} = \overline{(a_1 + a_2, a_1 + a_2)} = \overline{(0, 0)}$.

Eddig beláttuk, hogy az additív struktúra Abel-csoport.

A szorzás jóldefiniált. Legyen $a = c$ és $b = d$, azaz $a_1 + c_2 = a_2 + c_1$ és $b_1 + d_2 = b_2 + d_1$. Be kell látni, hogy $ab = cd$, azaz $a_1b_1 + a_2b_2 + c_1d_2 + c_2d_1 = a_1b_2 + a_2b_1 + c_1d_1 + c_2d_2$.

Ez teljesül, ha $(a_1b_1 + c_2b_1) + a_2b_2 + c_1d_2 + c_2d_1 = a_1b_2 + a_2b_1 + c_1d_1 + (c_2b_1 + c_2d_2)$ azaz $(a_1 + c_2)b_1 + a_2b_2 + c_1d_2 + c_2d_1 = a_1b_2 + a_2b_1 + c_1d_1 + c_2(b_1 + d_2)$. A feltételeket felhasználva ez fennáll, ha $(a_2 + c_1)b_1 + a_2b_2 + c_1d_2 + c_2d_1 = a_1b_2 + a_2b_1 + c_1d_1 + c_2(b_2 + d_1)$, egyszerűsítve $c_1b_1 + a_2b_2 + c_1d_2 = a_1b_2 + c_1d_1 + c_2b_2$. Ez teljesül, ha $c_1(b_1 + d_2) + a_2b_2 = (a_1 + c_2)b_2 + c_1d_1$ azaz a feltételek miatt $c_1(b_2 + d_1) + a_2b_2 = (a_2 + c_1)b_2 + c_1d_1$, ami azonossághoz vezet.

A szorzás asszociativitása és kommutativitása és az a tény, hogy $\overline{(1,0)}$ *neutrális elem* egyszerűen látható be, gyakorlat.

Disztributivitás. A szorzás kommutativitása miatt elegendő belátni, hogy $a(b+c) = ab+ac$. Nyilván $a(b+c) = a\overline{(b_1 + c_1, b_2 + c_2)} = \overline{(a_1b_1 + a_1c_1 + a_2b_2 + a_2c_2, a_1b_2 + a_1c_2 + a_2b_1 + a_2c_1)}$, illetve $ab + ac = \overline{(a_1b_1 + a_2b_2, a_1b_2 + a_2b_1)} + \overline{(a_1c_1 + a_2c_2, a_1c_2 + a_2c_1)}$

$$= \overline{(a_1b_1 + a_1c_1 + a_2b_2 + a_2c_2, a_1b_2 + a_1c_2 + a_2b_1 + a_2c_1)}.$$

Eddig beláttuk, hogy a $(\mathbb{Z}, +, \cdot)$ struktúra kommutatív egységelemes gyűrű. Az $\overline{(a,0)}$ alakú elemeket azonosíthatjuk a természetes számokkal. Lássuk be, hogy $\mathbb{Z} = \{0, 1, 2, 3, \dots\} \cup \{-1, -2, -3, \dots\}$. Valóban, a rendezés linearitása miatt az a, b természetes számokra $a = b+c$ vagy $b = a + c$ valamely c természetes számmal, azaz $\overline{(a,b)} = \overline{(b+c,b)} = \overline{(c,0)}$ vagy $\overline{(a,b)} = \overline{(a,a+c)} = \overline{(0,c)} = -\overline{(c,0)}$. Ezután a zérusosztómentesség következik 2.2-ből és abból, hogy nemnulla természetes számmal a szorzásnál lehet egyszerűsíteni. □

A $(\mathbb{Z}, +, \cdot)$ struktúrát az **egész számok gyűrűjé**nek, elemeit **egész számok**nak nevezünk. A bizonyítás utolsó részében említett azonosítással a természetes számok $\mathbb{N}$ halmazát az egész számok $\mathbb{Z}$ halmazának részhalmazaként tekintjük. A rendezést nyilvánvaló módon kiterjesztve az egész számokra újból lineáris rendezést kapunk, amelyben már nincsen legkisebb elem. Az 1,2,3,... számokat **pozitív,** a -1,-2,-3,... számokat **negatív egész számok**nak nevezzük. Ellenőrizze, hogy ha $a \leq b$ és c egész számok, d pozitív egész szám, akkor $a + c \leq b + c$ és $ad \leq bd$.

4. A racionális és valós számok

Az egész számok körében a negyedik alapművelet, az osztás nem mindig végezhető el. Ezért a következő tételben bevezetjük a racionális szám fogalmát. A racionális számokat egész számokból alkotott számláló – nevező rendezett elempárnak tekintjük, ahol a nevező nem lehet nulla. Két tört, $\frac{a_1}{a_2}$ és $\frac{b_1}{b_2}$ egyenlő, ha $a_1b_2 = a_2b_1$. Az összeadás műveletét közös nevezőre hozás után végezhetjük el, a szorzást pedig a megszokott ,,számlálót a számlálóval, nevezőt a nevezővel" szabály szerint.

4.1.Tétel. *Legyen $Q = \mathbb{Z} \times \mathbb{Z} \setminus \{0\}$ Descartes-szorzat, és a $\rho \subseteq Q \times Q$ reláció legyen a következőképpen meghatározva: $((a_1, a_2), (b_1, b_2)) \in \rho$ ha $a_1b_2 = a_2b_1$. Ekkor ρ ekvivalenciareláció, az ekvivalenciaosztályok halmazát jelölje $\mathbb{Q}$, az (a_1, a_2) elempárral reprezentált ekvivalenciaosztályt jelölje $\frac{a_1}{a_2}$. Az osztályok közötti műveletek legyenek az alábbi módon megadva:*

$$\frac{a_1}{a_2} + \frac{b_1}{b_2} = \frac{a_1b_2 + a_2b_1}{a_2b_2}, \quad \frac{a_1}{a_2}\frac{b_1}{b_2} = \frac{a_1b_1}{a_2b_2}.$$

Ekkor a $(\mathbb{Q}, +, \cdot)$ struktúra test.

Bizonyítás. ρ ekvivalenciareláció. A ρ reláció nyilván reflexív és szimmetrikus. Ha $((a_1, a_2), (b_1, b_2)) \in \rho$ és $((b_1, b_2), (c_1, c_2)) \in \rho$ akkor $a_1b_2 = a_2b_1$ és $b_1c_2 = b_2c_1$. Ekkor $a_1c_2 = a_2c_1$ teljesül, ha $a_1b_2c_2 = a_2b_2c_1$ (mivel b_2 nemnulla) azaz a feltételekből $a_2b_1c_2 = a_2b_1c_2$, ami azonosság. Így $((a_1, a_2), (c_1, c_2)) \in \rho$, a tranzitivitás világos.

Legyen $\frac{a_1}{a_2}, \frac{b_1}{b_2}, \frac{c_1}{c_2}, \frac{d_1}{d_2} \in \mathbb{Q}$ ekvivalenciaosztály.

Az összeadás és a szorzás művelet, mivel nemnulla egész számok szorzata nemnulla.

Az összeadás jóldefiniált. Legyen $\frac{a_1}{a_2} = \frac{c_1}{c_2}$ és $\frac{b_1}{b_2} = \frac{d_1}{d_2}$, azaz $a_1c_2 = a_2c_1$ és $b_1d_2 = b_2d_1$. Be kell látni, hogy $\frac{a_1}{a_2} + \frac{b_1}{b_2} = \frac{c_1}{c_2} + \frac{d_1}{d_2}$, azaz $\frac{a_1b_2+a_2b_1}{a_2b_2} = \frac{c_1d_2+c_2d_1}{c_2d_2}$, azaz $(a_1b_2 + a_2b_1)c_2d_2 = a_2b_2(c_1d_2 + c_2d_1)$. A disztributivitást és a feltételeket felhasználva ez teljesül, ha $a_2b_2c_1d_2 + a_2b_2c_2d_1 = a_2b_2c_1d_2 + a_2b_2c_2d_1$, ami azonosság.

Az összeadás asszociatív. Nyilván

$$\left(\frac{a_1}{a_2} + \frac{b_1}{b_2}\right) + \frac{c_1}{c_2} = \frac{a_1b_2 + a_2b_1}{a_2b_2} + \frac{c_1}{c_2} = \frac{a_1b_2c_2 + a_2b_1c_2 + a_2b_2c_1}{a_2b_2c_2},$$

másrészről

$$\frac{a_1}{a_2} + \left(\frac{b_1}{b_2} + \frac{c_1}{c_2}\right) = \frac{a_1}{a_2} + \frac{b_1c_2 + b_2c_1}{b_2c_2} = \frac{a_1b_2c_2 + a_2b_1c_2 + a_2b_2c_1}{a_2b_2c_2}.$$

Az összeadás kommutatív. A definícióból látszik.

Neutrális elem, inverz. Nyilván $\frac{0}{1}$ neutrális elem, és az $\frac{a_1}{a_2}$ osztály additív inverze $\frac{-a_1}{a_2}$.

Eddig beláttuk, hogy az additív struktúra Abel-csoport.

A szorzás jóldefiniált. Legyen $\frac{a_1}{a_2} = \frac{c_1}{c_2}$ és $\frac{b_1}{b_2} = \frac{d_1}{d_2}$, azaz $a_1c_2 = a_2c_1$ és $b_1d_2 = b_2d_1$. Be kell látni, hogy $\frac{a_1}{a_2}\frac{b_1}{b_2} = \frac{c_1}{c_2}\frac{d_1}{d_2}$, azaz $\frac{a_1b_1}{a_2b_2} = \frac{c_1d_1}{c_2d_2}$, azaz $a_1b_1c_2d_2 = a_2b_2c_1d_1$, ami a két feltételt felhasználva azonossághoz vezet.

Közvetlen számolás belátni a szorzás asscociativitását, kommutativitását, azt, hogy $\frac{1}{1}$ neutrális elem, illetve a disztributivitást (gyakorlat!).

Eddig beláttuk, hogy a $(\mathbb{Q}, +, \cdot)$ struktúra kommutatív egységelemes gyűrű. Mivel $\frac{0}{1} = \{(0, a_2) |\, a_2 \in \mathbb{Z} \setminus \{0\}\}$ és $\frac{1}{1} = \{(a_1, a_1) |\, a_1 \in \mathbb{Z} \setminus \{0\}\}$, ha $\frac{a_1}{a_2}$ nemnulla elem, akkor multiplikatív inverze nyilván $\frac{a_2}{a_1}$, és a struktúra test. □

A $\mathbb{Q}$ testet a **racionális számok testé**nek, elemeit **racionális számok**nak nevezzük. Azonosíthatjuk az a egész számokat és az $\frac{a}{1}$ racionális számokat, így az egész számok $\mathbb{Z}$ halmaza részhalmaza a racionális számok $\mathbb{Q}$ halmazának, és a racionális számok közötti összeadás és szorzás az egész számok közötti összeadás és szorzás műveletének kiterjesztése, továbbá minden racionális szám előáll két egész szám hányadosaként. A **rendezés**t kiterjeszthetjük a **racionális számokra** nyilvánvaló módon, a rendezés továbbra is lineáris marad; világos az is, hogy mit értünk **abszolút érték** alatt. Gyakorlásképpen lássa be, hogy a, b racionális számokra $|ab| = |a||b|$ és $|a+b| \leq |a|+|b|$. Érdekes tulajdonság, hogy míg az egész számhoz van előző és rákövetkező egész szám, addig bármely két racionális szám között van egy harmadik racionális szám.

Geometriából tudjuk, hogy vannak nem összemérhető szakaszok, azaz amelyek hossza nem racionális szám, például az egységnégyzet átlójának hossza. Ez azt mutatja, hogy a számfogalom tovább bővíthető. Az alábbiakban ezt tesszük analitikus módszerrel.

Tekintsük a racionális **sorozat**okat, azaz az $a : \mathbb{N} \to \mathbb{Q}, n \mapsto a_n$ leképezéseket. Ezek között vannak **konvergensek**, azaz olyanok, amelyekhez létezik olyan u racionális szám, hogy tetszőlegesen kicsiny ε pozitív racionális számhoz létezik N természtes szám, hogy az $|u - a_n| < \varepsilon$ hacsak $n > N$. Ilyenkor azt mondjuk, hogy az a_n **sorozat határértéke** az u racionális szám, jelölés: $\lim_{n\to\infty} a_n = u$. **Nullsorozat**nak nevezzük a nullához konvergáló racionális sorozatot. Gyakorlásképpen lássa be, hogy a műveletek és a határátmenet sorrendje felcserélhető: ha a_n és b_n konvergens sorozatok, c racionális szám, akkor $a_n + b_n$, ca_n, a_nb_n, illetve $b_n \neq 0$, $\lim_{n\to\infty} b_n \neq 0$ esetén $\frac{a_n}{b_n}$ is konvergens sorozatok, és $\lim_{n\to\infty}(a_n + b_n) = \lim_{n\to\infty} a_n + \lim_{n\to\infty} b_n$, $\lim_{n\to\infty} ca_n = c \lim_{n\to\infty} a_n$, $\lim_{n\to\infty} \frac{a_n}{b_n} = \frac{\lim_{n\to\infty} a_n}{\lim_{n\to\infty} b_n}$.

Vannak racionális **Cauchy-sorozatok**: az a_n sorozat ilyen, ha minden ε tetszőlegesen kicsiny pozitív racionális számhoz létezik N természetes szám, hogy $|a_n - b_m| < \varepsilon$ hacsak $n, m > N$. Nyilvánvalóan konvergens sorozat Cauchy-tulajdonságú (ellenőrizze!), a megfordítás nem teljesül: bizonyos racionális Cauchy-sorozatok „irracionális számokhoz konvergálnak", azaz a racionális pontok nem fedik be teljesen a számegyenest. Az irracionális pontokkal kibővítve a számfogalmat, és a műveleteket a folytonos határátmenet segítségével értelmezve kapjuk a következő tételt.

4.2.Tétel. *Legyen R a racionális Cauchy-sorozatok halmaza, és legyen a $\rho \subseteq R \times R$ reláció a következőképpen meghatározva: $(a_n, b_n) \in \rho$ ha $a_n - b_n$ nullsorozat. Ekkor a ρ reláció ekvivalenciareláció, az ekvivalenciaosztályok halmazát jelölje $\mathbb{R}$. Az összeadás és a szorzás műveletét az $\mathbb{R}$ halmazon definiáljuk az alábbi módon: $\overline{a_n} + \overline{b_n} = \overline{a_n + b_n}$; $\overline{a_n}\,\overline{b_n} = \overline{a_n b_n}$. Ekkor az $(\mathbb{R}, +, \cdot)$ struktúra test.*

Bizonyítás. Legyen a_n, b_n, c_n, d_n racionális Cauchy-sorozat.

ρ ekvivalenciareláció. Nyilván a ρ reláció reflexív és szimmetrikus. Legyen $a_n - b_n$ és $b_n - c_n$ nullsorozat, és legyen ε pozitív racionális szám, N_1 és N_2 olyan természetes szám, hogy $|a_n - b_n| < \frac{\varepsilon}{2}$ hacsak $n > N_1$ és $|b_n - c_n| < \frac{\varepsilon}{2}$ hacsak $n > N_2$. Ekkor $|a_n - c_n| = |(a_n - b_n) + (b_n - c_n)| \le |a_n - b_n| + |b_n - c_n| < \frac{\varepsilon}{2} + \frac{\varepsilon}{2} = \varepsilon$ hacsak $n > \max\{N_1, N_2\}$, azaz $a_n - c_n$ nullsorozat, és a ρ reláció tranzitív.

Az összeadás és a szorzás művelet. Be kell látni, hoyg Cauchy-sorozatok összege és szorzata is Cauchy-tulajdonságú. Legyen az N_1 természetes szám olyan, hogy $|a_n - a_m| < \frac{\varepsilon}{2}$ hacsak $n, m > N_1$, és az N_2 olyan, hogy $|b_n - b_m| < \frac{\varepsilon}{2}$ hacsak $n, m > N_2$. Ekkor, ha $n, m > \max\{N_1, N_2\}$, $|(a_n + b_n) - (a_m + b_m)| = |(a_n - a_m) + (b_n - b_m)| \le |a_n - a_m| + |b_n - b_m| < \frac{\varepsilon}{2} + \frac{\varepsilon}{2} = \varepsilon$, és az $a_n + b_n$ sorozat Cauchy-tulajdonságú.

Most lássuk be, hogy az a_n Cauchy-sorozat korlátos, azaz van olyan A pozitív racionális szám, hogy $|a_n| \le A$ minden n természetes számra. Valóban, legyen az N termszetes szám olyan, hogy $|a_n - a_m| < 1$ hacsak $n, m > N$. Világos, hogy $A = \max\{|a_1|, |a_2|, \dots, |a_N|, |a_{N+1}| + 1\}$ megfelelő korlát.

Legyen az a_n sorozat korlátja az A racionális szám és a b_n sorozat korlátja a B racionális szám. Legyen továbbá az N_1 természetes szám olyan, hogy $|a_n - a_m| < \frac{\varepsilon}{2B}$ hacsak $n, m > N_1$, és az N_2 olyan, hogy $|b_n - b_m| < \frac{\varepsilon}{2A}$ hacsak $n, m > N_2$. Ekkor, ha $n, m > \max\{N_1, N_2\}$,

$$|a_n b_n - a_m b_m| = |a_n b_n - a_m b_n + a_m b_n - a_m b_m| = |(a_n - a_m) b_n + a_m (b_n - b_m)| \le$$

$$|(a_n - a_m) b_n| + |a_m (b_n - b_m)| = |a_n - a_m||b_n| + |a_m||b_n - b_m| < \frac{\varepsilon}{2B} B + A \frac{\varepsilon}{2A} = \varepsilon,$$

azaz az $a_n b_n$ sorozat is Cauchy-tulajdonságú.

Legyen $\alpha = \overline{a_n}$, $\beta = \overline{b_n}$, $\gamma = \overline{c_n}$, $\delta = \overline{d_n}$ az $\mathbb{R}$ halmaz elemei.

Az összeadás és a szorzás jóldefiniált. Be kell látni, hogy ha $\alpha = \gamma$, azaz $a_n - c_n$ nullsorozat, és $\beta = \delta$, azaz $b_n - d_n$ nullsorozat, akkor $\alpha + \beta = \gamma + \delta$, azaz $(a_n + b_n) - (c_n + d_n) = (a_n - c_n) + (b_n - d_n)$ nullsorozat; illetve $\alpha\beta = \gamma\delta$, azaz $a_n b_n - c_n d_n = a_n (b_n - d_n) + (a_n - c_n) d_n$ nullsorozat. Ez a két tulajdoság azokból a nyilvánvaló tényekből adódik, hogy nullsorozatok összege nullsorozat, és egy korlátos sorozat és egy nullsorozat szorzata nullsorozat (ellenőrizze!).

Az összeadás asszociatív. Nyilván $(\alpha + \beta) + \gamma = \overline{a_n + b_n} + \gamma = \overline{a_n + b_n + c_n}$ és $\alpha + (\beta + \gamma) = \alpha + \overline{b_n + c_n} = \overline{a_n + b_n + c_n}$.

Az összeadás kommutatív. Nyilván $\alpha + \beta = \overline{a_n + b_n} = \overline{b_n + a_n} = \beta + \alpha$.

Neutrális elem, ellentett. Nyilván a konstans 0 sorozat osztálya (azaz a nullsorozatok halmaza) neutrális elem, és $-\alpha = \overline{-a_n}$.

A szorzás asszociatív. Nyilván $(\alpha\beta)\gamma = \overline{a_n b_n}\gamma = \overline{a_n b_n c_n}$ és $\alpha(\beta\gamma) = \alpha\overline{b_n c_n} = \overline{a_n b_n c_n}$.

A szorzás kommutatív. Nyilván $\alpha\beta = \overline{a_n b_n} = \overline{b_n a_n} = \beta\alpha$.

Neutrális elem, inverz. Nyilván a konstans 1 sorozat osztálya (azaz az 1-hez konvergáló sorozatok halmaza) neutrális elem. Legyen α nemnulla elem, azaz nem a nullsorozatok halmaza. Be kell látni, hogy van olyan sorozat az α halmazban, amelynek egyik tagja sem 0. Valóban, vegyünk egy sorozatot az α halmazból. Nem lehet végtelen sok tagja 0, mivel azonnal látjuk, hogy ekkor, Cauchy sorozat lévén, konvergálna a 0-hoz. Így csak véges sok tagja 0, ezek mindegyike a sorozat N-nél kisebbik indexű tagja. Ekkor az az a_n sorozat, amelyik első N tagja 1, a többi megegyezik az eredeti sorozattal, eleme az α osztálynak, és egyik tagja sem 0. Nyilván $\frac{1}{a_n}$ is Cauchy-soroxat, és $\frac{1}{\alpha} = \overline{\frac{1}{a_n}}$ a keresett reciprok.

A disztributivitás nyilvánvaló, belátása gyakorlat. □

A $\mathbb{R}$ testet a **valós számok testé**nek, elemeit **valós számok**nak nevezzük. Azonosíthatjuk a racionális konstans sorozatok osztályait és a racionális számokat, így a racionális számok $\mathbb{Q}$ halmaza részhalmaza a valós számok $\mathbb{R}$ halmazának, és a valós számok közötti összeadás és szorzás a racionális számok közötti összeadás és szorzás műveletének kiterjesztése, továbbá minden valós szám valamely racionális sorozat határértéke, és minden valós Cauchy sorozat konvergens. A **rendezés**t kiterjeszthetjük a **valós számokra** nyilvánvaló módon: $\alpha \leq \beta$, ha létezik $a_n \in \alpha$, $b_n \in \beta$ sorozat, hogy $a_n \leq b_n$ minden n számra; a rendezés továbbra is lineáris marad.

Gyakorlásképpen lássa be, hogy bármely α, β pozitív valós számhoz létezik n természetes szám, hogy $\alpha \leq n\beta$; minden nemelfajuló nyílt intervallumban végtelen sok racionális szám van; zárt intervallumok csökkenő sorozatának közös része nemüres.

5. A komplex számok

Könnyen látható, hogy páratlan fokszámú valós együtthatós polinomnak mindig van valós gyöke, azonban például az $x^2 + 1$ polinomnak nincs valós gyöke. Jelölje az i szimbólum egy gyökét, és nevezzük el **képzetes egység**nek, mivel nem valós, hanem ,,elképzelt" számról van szó, hiszen négyzete -1. Tekintsük az $a_1 + a_2 i$ alakú formális összegeket, ahol az a_1 valós számot **valós rész**nek, az a_2 valós számot **képzetes rész**nek nevezzük. Az összeadás és a szorzás műveletét végezzük el ahogyan megszoktuk kéttagok esetén, a kapott struktúra minden, számoktól elvárt műveleti tulajdonsággal rendelkezik. Az $a_1 + a_2 i$ nemnulla elem reciprokának megkereséséhez vegyük észre, hogy $(a_1 + a_2 i)(a_1 - a_2 i) = a_1^2 + a_2^2$ nemnulla valós szám, így az egyenlőséget az $a_1^2 + a_2^2$ és $a_1 + a_2 i$ számmal elosztva kapjuk, hogy $\frac{1}{a_1 + a_2 i} = \frac{1}{a_1^2 + a_2^2}(a_1 - a_2 i)$. A precíz bizonyításhoz ezeket az ,,elképzelt" számokat valós rész – képzetes rész rendezett számpároknak tekintjük.

5.1.Tétel. *Legyen $\mathbb{C} = \mathbb{R} \times \mathbb{R}$ Descartes szorzat, és az összeadás és szorzás műveletét a következőképpen határozzuk meg:*

$$(a_1, a_2) + (b_1, b_2) = (a_1 + b_1, a_2 + b_2), \quad (a_1, a_2)(b_1, b_2) = (a_1 b_1 - a_2 b_2, a_1 b_2 + a_2 b_1).$$

Ekkor a $(\mathbb{C}, +, \cdot)$ struktúra test.

Bizonyítás. Legyenek $a = (a_1, a_2), b = (b_1, b_2), c = (c_1, c_2)$ a $\mathbb{C}$ halmaz elemei. Világos, hogy az összeadás és szorzás művelet. A bizonyítás során hivatkozás nélkül felhasználjuk a valós számok műveleti tulajdonságait.

Az additív struktúra Abel-csoport. Az asszociativitás és kommutativitás a valós számok összeadása megfelelő tulajdonságainak közvetlen következménye. Nyilván $(0, 0)$ neutrális elem, az a elem ellentettje $-a = (-a_1, -a_2)$.

Közvetlen számolással kapjuk, hogy egyrészt $a(bc) = a(b_1c_1 - b_2c_2, b_1c_2 + b_2c_1) =$

$$(a_1b_1c_1 - a_1b_2c_2 - a_2b_1c_2 - a_2b_2c_1, a_1b_1c_2 + a_1b_2c_1 + a_2b_1c_1 - a_2b_2c_2),$$

másrészt $(ab)c = (a_1b_1 - a_2b_2, a_1b_2 + a_2b_1)c =$

$$(a_1b_1c_1 - a_2b_2c_1 - a_1b_2c_2 - a_2b_1c_2, a_1b_1c_2 - a_2b_2c_2 + a_1b_2c_1 + a_2b_1c_1),$$

amely számpárok megegyeznek.

A szorzás kommutativitása a definícióból látszik.

Neutrális elem és inverz. Az $(1, 0)$ elem nyilván neutrális elem. Legyen a nemnulla elem, azaz a_1 vagy a_2 nemnulla valós szám. Ekkor $a_1^2 + a_2^2$ nemnulla, és

$$(a_1, a_2)(\frac{a_1}{a_1^2 + a_2^2}, \frac{-a_2}{a_1^2 + a_2^2}) = (1, 0),$$

azaz, a szorzás kommutativitását is felhasználva, a nemnulla a elem reciproka $(\frac{a_1}{a_1^2+a_2^2}, \frac{-a_2}{a_1^2+a_2^2})$.

A disztributivitás közvetlen számolás, gyakorlat. Beláttuk, hogy a struktúra test. □

A $\mathbb{C}$ struktúrát a **komplex számok testé**nek, elemeit **komplex számok**nak nevezzük. Azonosíthatjuk az $(a, 0)$ alakú komplex számokat az a valós számokkal, így a valós számok $\mathbb{R}$ halmaza részhalmaza a komplex számok $\mathbb{C}$ halmazának, és a komplex számok közötti összeadás és szorzás a valós számok közötti műveletek kiterjesztése. Legyen $i = (0, 1)$. Ekkor $a = (a_1, a_2) = (a_1, 0) + (a_2, 0)i$, illetve az $a_1 = (a_1, 0), a_2 = (a_2, 0)$ azonosítást felhasználva $a = a_1 + a_2i$, amely alakot a komplex szám **algebrai alak**jának nevezzük.

A reciprok megkeresésénél már alkalmaztuk a **komplex szám konjugáltját**: az $a = a_1+a_2i$ komplex szám konjugáltja az $\overline{a} = a_1 - a_2i$ komplex szám. Ennek a műveletnek a tulajdoságai az alábbiak.

5.2.Állítás. *Legyenek $a = a_1 + a_2i$ és $b = b_1 + b_2i$ tetszőleges komplex számok. Ekkor:*
(i) $\overline{a + b} = \overline{a} + \overline{b}$;
(ii) $\overline{ab} = \overline{a}\overline{b}$;
(iii) $\overline{\overline{a}} = a$;
(iv) $a\overline{a} = a_1^2 + a_2^2$ *valós szám, és* $a = \overline{a}$ *pontosan akkor, ha a valós szám.*

Bizonyítás. (i) Egyrészt

$$\overline{a + b} = \overline{(a_1 + b_1) + (a_2 + b_2)i} = (a_1 + b_1) - (a_2 + b_2)i,$$

másrészt

$$\overline{a} + \overline{b} = (a_1 - a_2i) + (b_1 - b_2i) = (a_1 + b_1) - (a_2 + b_2)i.$$

(ii) Egyrészt

$$\overline{ab} = \overline{(a_1b_1 - a_2b_2) + (a_1b_2 + a_2b_1)i} = (a_1b_1 - a_2b_2) - (a_1b_2 + a_2b_1)i,$$

másrészt

$$\overline{a}\overline{b} = (a_1 - a_2i)(b_1 - b_2i) = (a_1b_1 - a_2b_2) - (a_1b_2 + a_2b_1)i.$$

(iii),(iv). Az utolsó két állítás nyilvánvaló. □

Az $a = a_1 + a_2i$ komplex számra az $||a|| = a_1^2 + a_2^2$ nemnegatív valós számot a **komplex szám normájá**nak illetve az $|a| = \sqrt{a_1^2 + a_2^2}$ négyzetgyökét **abszolútértéké**nek nevezzük. Az abszolút érték tulajdonságai a megszokottak.

5.3.Állítás. *Legyen a és b tetszőleges komplex szám.*
(i) $|a| \geq 0$ *és* $a = 0$ *pontosan akkor, ha* $a = 0$*;*
(ii) (háromszög-egyenlőtlenség) $|a + b| \leq |a| + |b|$*;*
(iii) $|a - b| \geq ||a| - |b||$*;*
(iv) $|ab| = |a|\,|b|$.

Bizonyítás. (i) Nyilvánvaló.
(ii) Az egyenlőtlenség teljesül, ha $||a + b|| \leq (|a| + |b|)^2$, azaz

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

ehhez elegendő, hogy $a\overline{b}+\overline{a}b \leq 2|a||b|$ legyen. Ez az egyenlőtlenség fennáll, ha $4(a_1b_1+a_2b_2)^2 \leq 4||a||\,||b||$, azaz

$$a_1^2b_1^2 + a_2^2b_2^2 + 2a_1a_2b_1b_2 \leq a_1^2b_1^2 + a_2^2b_2^2 + a_1^2b_2^2 + a_2^2b_1^2.$$

Egyszerűsítés és átrendezés után a nyilvánvaló $0 \leq (a_1b_2 - a_2b_1)^2$ egyenlőtlenséget kapjuk.
(iii) A háromszög-egyenlőtlenségben először a helyére írjunk $a - b$-t: $|a| \leq |a - b| + |b|$. azaz $|a| - |b| \leq |a - b|$. Másodszor írjunk b helyére $b - a$-t: $|b| \leq |a| + |b - a|$. azaz $|b| - |a| \leq |a - b|$. A kapott két egyenlőtlenségből az állítás következik.
(iv) Elegendő belátni az $||ab|| = ||a||\,||b||$ egyenlőséget. Egyrészt

$$||ab|| = (a_1b_1 - a_2b_2)^2 + (a_1b_2 + a_2b_1)^2 = a_1^2b_1^2 + a_2^2b_2^2 + a_1^2b_2^2 + a_2^2b_1^2,$$

másrészt

$$||a||\,||b|| = (a_1^2 + a_2^2)(b_1^2 + b_2^2) = a_1^2b_1^2 + a_2^2b_2^2 + a_1^2b_2^2 + a_2^2b_1^2. \qquad \square$$

Azonosítsuk a Descartes-féle koordinátasík pontjait a valós rendezett számpárokkal, azaz a komplex számokkal, ilyenkor a síkot **Gauss-féle számsík**nak nevezzük. Ekkor a nemnulla komplex számot meghatározhatjuk az odamutató helyvektor hosszával és irányszögével, és kapjuk a **trigonometrikus alak**ot: $a = a_1+a_2i = r(\cos\alpha+i\sin\alpha)$ ahol a $r = \sqrt{a_1^2 + a_2^2} = |a|$ a helyvektor (és egyúttal a komplex szám) hossza, és $\alpha = \arg a$ a helyvektor irányszöge vagy a **komplex szám argumentuma**. Az áttérés a nemnulla $a = a_1 + a_2i$ komplex szám algebrai alakjáról a trigonometrikus alakra a következőképpen lehetséges. Nyilván $a = a_1 + a_2i = |a|(\frac{a_1}{|a|}+\frac{a_2}{|a|})i$, mivel az $\frac{a_1}{|a|}$ és az $\frac{a_2}{|a|}$ valós számok négyzetösszege 1, valamely α szög koszinuszával és szinuszával egyenlőek. Ha $a_1 = 0$ és $a_2 > 0$ akkor $\alpha = \frac{\pi}{2}$; ha $a_1 = 0$ és $a_2 < 0$ akkor $\alpha = \frac{3\pi}{2}$;

$$\alpha = \begin{cases} \operatorname{arctg}\frac{a_2}{a_1}, & \text{ha } a_1 > 0; \\ \pi + \operatorname{arctg}\frac{a_2}{a_1}, & \text{ha } a_1 < 0 \end{cases}$$

(Ez a visszakeresés $(-\frac{\pi}{2}, \frac{3\pi}{2}]$ intervallumbeli szöget ad meg.)
A trigonometrikus alakban egyszerűen végezhető el a szorzás, osztás, hatványozás és a **komplex gyökvonás** művelete: az a nemnulla komplex szám n-edik gyökének ($n \geq 2$) nevezzük az $x^n - a$ polinom komplex gyökeit, és $\sqrt[n]{a}$-val jelöljük. Nevezetes tény, hogy ilyen komplex gyök n darab különböző van.

5.4.Állítás. *Legyen a és b tetszőleges nemnulla komplex szám. Ekkor:*
(i) $|ab| = |a|\,|b|$ *és* $\arg ab = \arg a + \arg b$*;*
(ii) (Moivre képlete) $|a^n| = |a|^n$ *és* $\arg a^n = n \arg a$*, ahol n pozitív egész;*
(iii) $|\frac{a}{b}| = \frac{|a|}{|b|}$ *és* $\arg \frac{a}{b} = \arg a - \arg b$*;*
(iv) $|\sqrt[n]{a}| = \sqrt[n]{|a|}$ *(ez utóbbi valós n-edik gyökvonás) és* $\arg \sqrt[n]{a} = \frac{\arg a+2k\pi}{n}$ *($k = 1, 2, \ldots, n-1$), ahol $n > 1$ egész.*

Bizonyítás. (i) A hosszra vonatkozó állítás azonos 5.3.4-gyel. Az addíciós képleteket felhasználva $(\cos\alpha + i\sin\alpha)(\cos\beta + i\sin\beta) =$

$$(\cos\alpha\cos\beta - \sin\alpha\sin\beta) + i(\cos\alpha\sin\beta + \sin\alpha\cos\beta) = \cos(\alpha+\beta) + i\sin(\alpha+\beta),$$

ami az argumentumra vonatkozó állítást adja.

(ii) Világos az első állításból indukcióval.

(iii) Mivel $1 = b\frac{1}{b}$, kapjuk, hogy $1 = |1| = |b\frac{1}{b}| = |b|\,|\frac{1}{b}|$ az első állítást felhasználva, azaz $|\frac{1}{b}| = \frac{1}{|b|}$. Továbbá $0 = \arg 1 = \arg b\frac{1}{b} = \arg b + \arg\frac{1}{b}$ az első állítást felhasználva, azaz $\arg\frac{1}{b} = -\arg b$. Újból az első állítást alkalmazva kapjuk, amit be kellett látni.

(iv) A képlet n különböző komplex számot határoz meg, így elegendő belátni, hogy n-edik hatványuk a, ami Moivre képlete és a szinusz, koszinusz függvények periódusa alapján világos. □

Jelentősek az úgynevezett **n-edik komplex egységgyök**ök ($n \geq 2$): ezek az 1 komplex n-edik gyökei, azaz a

$$\varepsilon_k = \cos\frac{2k\pi}{n} + i\sin\frac{2k\pi}{n}$$

komplex számok, amelyek a Gauss-féle számsíkon az egységkörnek szabályos n-szöget alkotó pontjai. Ezek közül speciálisak azok, amelyek hatványaiként előáll az összes többi n-edik egységgyök: ezek a **primitív n-edik egységgyökök**. Nem nehéz belátni, hogy ε_k primitív pontosan akkor, ha k és n relatív prímek. Gyakorlásképpen bizonyítsa be, hogy az n-edik komplex egységgyökök a szorzásra nézve Abel-csoportot alkotnak, és az összegük zérus.

III. ELEMI SZÁMELMÉLET

6. Oszthatóság az egész számok körében

Azt mondjuk, hogy az a **egész szám osztja a** b **egész számot,** ha létezik c egész szám, hogy $b = ac$, jelölés: $a|b$. Azt mondjuk, hogy a b **egész szám az** a **egész szám asszociáltja,** ha $b = ac$, ahol c egység, azaz 1 vagy -1; jelölés: $a \sim b$. Nyilvánvaló, hogy az asszociáltság ekvivalenciareláció az egészek halmazán (általánosítva az asszociáltsági relációt tetszőleges integritástartományra ez érvényben marad). Oszthatósági szempontból elem és asszociáltja között különbséget tenni nem tudunk, így az oszthatósági tulajdonságok inkább az elem asszociált osztályának a sajátjai, azonban a kónnyebb érthetőség kedvéért nem fogjuk ezt a felfogást követni. Alapvető tulajdonságai az oszthatósági relációnak az alábbiak:

6.1.Állítás.

(i) Egész szám osztja önmagát;

(ii) ha az a egész szám osztja a b egész számot, és a b egész szám osztja a c egész számot, akkor a osztja a c egész számot;

(iii) ha az a egész szám osztja a b egész számot, és a b egész szám osztja az a egész számot akkor az a és b egész számok asszociáltak;

(iv) ha az a egész szám osztja a b egész számot, és a osztja a c egész számot akkor a osztja a $bu + cv$ egész számot, ahol u és v tetszőleges egész számok;

(v) ha az a egész szám osztja a c egész számot, és a b egész szám osztja a d egész számot akkor az ab szám osztja a cd számot.

Bizonyítás. (i) Nyilván $a = a1$.

(ii) Ha $b = as$ és $c = bt$, ahol s és t egész számok, akkor $c = (as)t = a(st)$, és a osztja a c egész számot.

(iii) Ha $b = as$ és $a = bt$, ahol s és t egész számok, akkor $b = bts$. Ha $b = 0$, akkor $a = bt = 0t = 0$; ha $b \neq 0$ akkor $b(1 - ts) = 0$ és a zérusosztómentesség miatt $1 - ts = 0$ és $ts = 1$, azaz t és s egységek, az a és b egész számok asszociáltak.

(iv) Ha $b = as$ és $c = at$, ahol s és t egész számok, akkor $bu + cv = asu + atv = a(su + tv)$ és a osztja a $bu + cv$ egész számot.

(v) Ha $c = as$ és $d = bt$, ahol s és t egész számok, akkor $cd = asbt = ab(st)$ és az ab szám osztja a cd számot. □

A fentiek tetszőleges integritástartományban igazak analóg bizonyítással. Az első három állítás azt jelenti, hogy az oszthatóság rendezési reláció az asszociáltsági osztályok halmazán; az egészek esetén a természetes számok halmazán.

Nagy fontossággal bír a maradékos vagy euklideszi osztás tétele.

6.2.Tétel. *A b és a nemnulla egész számokhoz egyértelműen létezik q és r egész szám úgy, hogy $b = aq + r$ és $0 \leq r < |a|$.*

Bizonyítás. Egzisztencia. Tekintsük azokat az u egész számokat, amelyekre $b - au \geq 0$. Ilyen egész számok léteznek, és ekkor a $\{b - au \in \mathbb{N} |\, u \in \mathbb{Z}\}$ halmaz természetes számok nemüres halmaza. Legyen ebben a halmazban $b - aq = r$ a legkisebb elem. Ahhoz, hogy az $r < |a|$ teljesülését belássuk, az úgynevezett indirekt bizonyítást alkamazzuk: feltesszük az ellenkezőjét, és ellentmondáshoz jutunk. Ha az $r \geq |a|$ egyenlőtlenség áll fenn, akkor $r - |a| = b - a(q \pm 1) \geq 0$ ellentmond r minimális voltának; ezért $r < |a|$ valóban teljesül.

Unicitás. Indirekte érvelünk. Legyen $b = aq+r$ és $b = aq'+r'$, ahol a q, q' különböző és r, r' egészek teljesítik a tétel feltételeit. Ekkor $0 = a(q-q')+(r-r')$ és $|a||q-q'| = |r-r'|$ fennáll, ahol a baloldal nem kisebb, mint $|a|$, a jobboldal pedig kisebb, mint $|a|$, ellentmodás. □

A maradékos osztás tételében szereplő a számot **osztó**nak, a b számot **osztandó**nak, a q számot **hányados**nak, az r számot **maradék**nak nevezzük. A maradékos osztáson alapul az **euklideszi algoritmus**. Legyen b és a nemnulla egész szám, a velük végzett maradékos osztás hányadosa legyen q_1, maradéka r_1. Az a és r_1 nemnulla egész számokon végzett maradékos osztás hányadosa legyen q_2, maradéka r_2. Az r_1 és r_2 nemnulla egész számokon végzett maradékos osztás hányadosa legyen q_3, maradéka r_3. És így tovább. Mivel a maradékok természetes számok szigorú monoton csökkenő sorozatát alkotják, véges sok lépés után a maradék 0 kell, hogy legyen: Az r_{n-2} és r_{n-1} nemnulla egész számokon végzett maradékos osztás hányadosa q_n, maradéka $r_n = 0$, amely az algoritmus utolsó lépése. Kaptuk a maradékos osztások következő sorozatát:

$$\begin{gathered}
b = aq_1 + r_1, \;\; 0 < r_1 < |a| \\
a = r_1q_2 + r_2, \;\; 0 < r_2 < r_1 \\
r_1 = r_2q_3 + r_3, \;\; 0 < r_3 < r_2 \\
\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\
r_{n-3} = r_{n-2}q_{n-1} + r_{n-1}, \;\; 0 < r_{n-1} < r_{n-2} \\
r_{n-2} = r_{n-1}q_n + r_n, \;\; 0 = r_n < r_{n-1}.
\end{gathered}$$

Ha a és b nemnulla egész számok, akkor **legnagyobb közös osztó**juknak nevezzük azt a d természetes számot, amelyre teljesül, hogy d osztja az a és a b számot is, és ha egy c egész szám szintén osztja az a és a b számot, akkor c osztja a d számot is. Jelölés: (a, b). A legnagyobb közös osztó létezését az euklideszi algoritmus biztosítja.

6.3. Állítás. *Bármely két nemnulla egész számnak létezik legnagyobb közös osztója, nevezetesen a rajtuk végrehajtott euklideszi algoritmus utolsó nemnulla maradéka.*

Bizonyítás. Legyen b és a nemnulla egész szám,

$$\begin{gathered}
b = aq_1 + r_1, \;\; 0 < r_1 < |a| \\
a = r_1q_2 + r_2, \;\; 0 < r_2 < r_1 \\
r_1 = r_2q_3 + r_3, \;\; 0 < r_3 < r_2 \\
\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\
r_{n-3} = r_{n-2}q_{n-1} + r_{n-1}, \;\; 0 < r_{n-1} < r_{n-2} \\
r_{n-2} = r_{n-1}q_n + r_n, \;\; 0 = r_n < r_{n-1}.
\end{gathered}$$

az euklideszi algoritmus. Az utolsó lépés miatt az r_{n-1} természetes szám osztja az r_{n-2} számot. Az utolsó előtti lépésben az egyenlőség jobb oldalát vizsgálva az r_{n-1} szám osztja az $r_{n-2}q_{n-1}$ és r_{n-1} számokat, így osztja az egyenlőség jobb oldalát, ezért osztja az r_{n-3} számot is. És így tovább, visszafelé haladva a lépésekben kapjuk, hogy az r_{n-1} szám osztja valamennyi maradékot. A második lépésben az egyenlőség jobb oldalát vizsgálva az r_{n-1} szám osztja r_1q_2 és r_2 számokat, így osztja az egyenlőség jobb oldalát, ezért osztja az a számot is. Az első lépésben az egyenlőség jobb oldalát vizsgálva az r_{n-1} szán osztja aq_1 és r_1 számokat, így osztja az egyenlőség jobb oldalát, ezért osztja a b számot is, azaz az r_{n-1} szám az a és b számok közös osztója.

Most legyen a c egész szám az a és b számok közös osztója. Ekkor az algoritmus első lépésében a c szám osztja az egyenlőség bal oldalát és az aq_1 számot, így osztja az r_1 számot is. A második lépésben a c szám osztja az egyenlőség bal oldalát és a r_1q_2 számot, így osztja az r_2 számot is. És így tovább, az algoritmusban előrefelé haladva kapjuk, hogy a c szám osztja az r_1, $r_2, \ldots, r_{n-2}$ számokat. Az utolsó előtti lépésben a c szám osztja az egyenlőség bal oldalát és a $r_{n-2}q_{n-1}$ számot, így osztja az r_{n-1} számot is. Az r_{n-1} szám valóban legnagyobb közös osztó. □

Világos, hogy legnagyobb közös osztó egyértelműen létezik (ellenőrizze!).

6.4.Állítás. *Az a és b nemnulla egész számok legnagyobb közös osztója felírható $au + bv$ alakban valamely u, v egészekre.*

Bizonyítás. Legyen b és a nemnulla egész szám,

$$\begin{gathered}
b = aq_1 + r_1, \;\; 0 < r_1 < |a| \\
a = r_1q_2 + r_2, \;\; 0 < r_2 < r_1 \\
r_1 = r_2q_3 + r_3, \;\; 0 < r_3 < r_2 \\
\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\
r_{n-3} = r_{n-2}q_{n-1} + r_{n-1}, \;\; 0 < r_{n-1} < r_{n-2} \\
r_{n-2} = r_{n-1}q_n + r_n, \;\; 0 = r_n < r_{n-1}.
\end{gathered}$$

az euklideszi algoritmus. Az első lépés alapján $r_1 = a(-q_1) + b$, azaz az r_1 maradék felírható a keresett alakban. A második lépés alapján $r_2 = a - r_1q_2 = a(1 + q_1q_2) + b(-q_2)$. Indukció alapján érvelünk. Tegyük fel, hogy $r_{k-2} = ae + bf$ és $r_{k-1} = ag + bh$ teljesül valamely e, f, g és h egészekre. Ekkor az algoritmus k-adik lépése alapján $r_{k-2} = r_{k-1}q_{k-1} + r_k$, amibe behelyettesítve a feltételeket kapjuk, hogy $r_k = a(e - gq_{k-1}) + b(f - hq_{k-1})$, ami a kívánt alak. Következésképpen a legnagyobb közös osztóval egyenlő r_{n-1} maradék is felírható a kívánt alakban. □

A legnagyobb közös osztó képzése művelet a nemnulla egész számokon. Tulajdonságai az alábbiak.

6.5.Állítás.

(i) A legnagyobb közös osztó képzésére nézve a nemnulla természetes számok félhálót alkotnak.

(ii) Minden nemnulla a, b, c természetes számra $(ac, bc) = (a, b)c$.

(iii) Minden nemnulla a, b, c természetes számra $(a, b) = (a + bc, b)$.

(iv) Minden nemnulla a, b, c természetes számra $(a, b) = a$ pontosan akkor, ha az a szám osztja a b számot.

Bizonyítás. (i) A *kommutativitás* a definíció szimmetriájából világos. Szintén nyilvánvaló az *idempotencia*. Az *asszociativitás* belátásához legyen a, b és c nemnulla természetes szám, és $u = ((a, b), c)$ illetve $v = (a, (b, c))$. Mivel u osztója az (a, b) legnagyobb közös osztónak, osztja az a és a b számot, továbbá a c számot is. Ezért osztja az a számot és a (b, c) legnagyobb közös osztót is. Ebből kapjuk, hogy osztja ezek v legnagyobb közös osztóját. Hasonlóan adódik, hogy v osztja az u számot, következésképp $u = v$.

(ii) Mivel az (a, b) legnagyobb közös osztó osztja az a számot és a b számot is, az $(a, b)c$ szám osztja az ac és bc számokat, következésképp osztja a legnagyobb közös osztójukat is, azaz $(ac, bc) = (a, b)ct$ valamely t természetes számra. Nyilván $(ac, bc)r = ac$ és $(ac, bc)s = bc$ valamely r, s természetes számokra, így $(a, b)ctr = ac$ és $(a, b)cts = bc$, ahonnan egyszerűsítés

után $(a,b)tr = a$ és $(a,b)ts = b$ adódik. Ekkor az $(a,b)t$ szám az a és b számok közös osztója, és osztania kell az (a,b) legnagyobb közös osztójukat is, azaz $(a,b)tw = (a,b)$ valamely w egész számra. Ez csak akkor lehetséges, ha $t = 1$.

(iii) Legyen $u = (a,b)$ és $v = (a+bc, b)$. Mivel az u szám osztja az a és a b számokat is, osztja az $a + bc$ és a b számokat, következésképp osztja a v legnagyobb közös osztójukat is. Mivel a v szám osztja az $a+bc$ és a b számokat is, osztja az a és a b számokat, következésképp osztja az u legnagyobb közös osztójukat is. Ez csak akkor lehetséges, ha $u = v$.

(iv) Legyen $(a,b) = a$. Ekkor nyilván az a szám osztja a b számot. Megfordítva, tegyük fel, hogy az a szám osztja a b számot. Ekkor a az a és b számok közös osztója. Egy másik közös osztó nyilván osztja az a számot, így ez legnagyobb közös osztó. □

Azt mondjuk, hogy az a és b nemnulla **egész számok relatív prímek**, ha legnagyobb közös osztójuk 1. Fontos tulajdonság az úgynevezett általánosított prímtulajdonság: ha az a egész osztja a bc szorzatot, és a és b számok relatív prímek, akkor az a szám osztja a c számot. Továbbá nyilvánvaló, hogy az $\frac{a}{(a,b)}$ és a $\frac{b}{(a,b)}$ számok relatív prímek. (Ellenőrizze ezeket az állításokat!).

A fenti tulajdonságok érvényben maradnak egész számokra is, ha a tulajdonságokban az egyenlőséget asszociáltság relációra cseréljük ki; illetve a nemnulla egészek asszociáltsági osztályai a legnagyobb közös osztó képzésére nézve félhálót alkotnak. A legnagyobb közös osztó fogalma és (létezés esetén) a tulajdonságai a nyilvánvaló módon általánosíthatók integritástartományokra.

Azt mondjuk, hogy az a és b nemnulla egész számok **legkisebb közös többszörös**e az m természetes szám, ha az a és a b szám is osztja az m számot, másszóval közös többszörösük, és ha a c szám szintén közös többszöröse az a és a b számoknak, akkor többszöröse az m számnak is. Jelölés: $[a,b]$.

A legkisebb közös többszörös nyilván egyértelmű, és a létezését 6.4-gyel együtt garantálja a

6.6. Állítás. *Az $m = \frac{|ab|}{(a,b)}$ szám az a és b nemnulla egész számok legkisebb közös többszöröse.*

Bizonyítás. Nyilván az $m = |a|\frac{|b|}{(a,b)} = |b|\frac{|a|}{(a,b)}$ szám közös többszörös.

Legyen a c egész az a és b egész számok közös többszöröse, azaz $c = as = bt$ valmely s és t egészekre. Ekkor az $\frac{a}{(a,b)}$ szám osztja a $\frac{b}{(a,b)}t$ számot, és, mivel az $\frac{a}{(a,b)}$ és a $\frac{b}{(a,b)}$ számok relatív prímek, az $\frac{a}{(a,b)}$ szám osztja a t számot, azaz $t = \frac{a}{(a,b)}u$ valamely u egészre. Kapjuk, hogy $c = b\frac{a}{(a,b)}u = \pm mu$, azaz az m szám osztja a c közös többszöröst. Az m szám valóban legkisebb közös többszörös. □

A művelet tulajdonságai az alábbiak.

6.7. Állítás.

(i) A nemnulla természetes számok a legkisebb közös többszörös képzésére nézve félhálót alkotnak;

(ii) Tetszőleges nemnulla a, b és c természetes számokra $[ac, bc] = [a,b]c$.

Bizonyítás. Legyenek a, b és c nemnulla természetes számok.

(i) A *kommutativitás* és az *idempotencia* a definíció közvetlen következménye. Legyen $u = [[a,b],c]$ és $v = [a,[b,c]]$. Belátjuk, hogy az u szám osztja a v számot, és megfordítva. Mivel az u szám közös többszörös, az $[a,b]$ és a c számok osztják u-t. Továbbá, mivel az $[a,b]$ szám közös többszörös, az u számot osztják az a illetve a b, c számok is. Mivel a $[b,c]$ szám legkisebb közös többszörös, innen kapjuk, hogy az u számot osztja az a és a $[b,c]$ szám is. Tekintve, hogy a v szám legkisebb közös többszörös, osztania kell az u számot. Hasonlóan érvelve adódik, hogy a v szám osztja az u számot, azaz $u = v$. Az *asszociativitás* világos.

(ii) Legyen $[ac, bc] = u$ és $[a, b]c = v$. Belátjuk, hogy az u szám osztja a v számot, és megfordítva. Mivel az a és b szám osztja az $[a, b]$ legkisebb közös többszöröst, az ac és bc szám osztja a $v = [a, b]c$ számot. Ennélfogva az u legkisebb közös többszörös osztja a v számot. Mivel az ac és bc számok osztják az u legkisebb közös többszöröst, $u = acs = bct$ valamely s és t egészekre. Egyszerűsítve kapjuk, hogy $as = bt$, és az a és b szám osztja az as számot. Ezért az $[a, b]$ legkisebb közös többszörös is osztja az as számot, így a $v = [a, b]c$ szám osztja az $asc = u$ számot. □

A fenti tulajdonságok érvényben maradnak egész számokra is, ha a tulajdonságokban az egyenlőséget asszociáltság relációra cseréljük ki; illetve a nemnulla egészek asszociáltsági osztályai a legkisebb közös többszörös képzésére nézve félhálót alkotnak. Gyakorlásképpen lássa be, hogy a nemnulla természetes számokon a legnagyobb közös osztó és a legkisebb közös többszörös műveletek kölcsönösen abszorbtívak, azaz az $(\mathbb{N} \setminus \{0\}, [], ())$ struktúra háló. Az indukált rendezés nyilván az oszthatóság. A legkisebb közös többszörös fogalma és (létezés esetén) a tulajdonságai a nyilvánvaló módon általánosíthatók integritástartományokra.

1-nél nagyobb természetes számról azt mondjuk, hogy **prímszám**, ha valahányszor oszt egy bc szorzatot (b és c egészek), akkor osztja legalább egyik tényezőjét is. 1-nél nagyobb u természetes számról azt mondjuk, hogy **törzsszám**, ha $u = ab$ (a és b egészek) egy faktorizációja, akkor valamelyik tényező egység, azaz 1 vagy -1. Ellentettjeikkel együtt **prímelem**ekről illetve **irreducibilis elem**ekről beszélünk.

6.8.Állítás. *A prímszám és a törzsszám fogalma egybeesik.*

Bizonyítás. Legyen u prímszám, és tegyük fel, hogy $u = ab$ alakban írható. Mivel az u prímszám osztja az ab szorzatot, osztja legalább egyik tényezőjét is. Ha az u szám osztja az a számot, azaz $a = us$ valamely s egészre, akkor az $u = usb$ egyenlőségből egyszerűsítés után $sb = 1$ következik, azaz s egység, az a és u számok asszociáltak és a b szám egység. Ha az u szám osztja a b számot, akkor hasonlóan kapjuk, hogy a b és u számok asszociáltak és az a szám egység. Az u szám törzsszám is.

Legyen most u törzsszám és osztója az ab szorzatnak. Feltehetjük, hogy az u szám nem osztja az a számot. Mivel u törzsszám, u és a ekkor relatív prímek, és az általánosított prímtulajdonság alapján az u számnak osztania kell a b számot. Beláttuk, hogy u prímszám. □

Ez alapján az egészeken nyilván a prímelem és az irreducibilis elem fogalma is egybeesik. Lényeges a következő, számelmélet alaptételeként említett

6.9.Tétel. *Tetszőleges 1-nél nagyobb természetes szám sorrendtől eltekintve egyértelműen bontható fel prímszámok szorzatára.*

Bizonyítás. Egzisztencia. Legyen a 1-nél nagyobb természetes szám. Lássuk be először, hogy létezik prímosztója. Ha maga a prímszám, akkor megtaláltuk a prímosztót. Ha nem, akkor nem törzsszám, ezért $a = a_1t_1$, ahol a_1, t_1 1-nél nagyobb természetes számok. Ha a_1 prímszám, megtaláltuk a prímosztót. Ha nem, akkor a_1 nem törzsszám, ezért $a_1 = a_2t_2$, ahol a_2, t_2 1-nél nagyobb természetes számok. És így tovább, ez az eljárás nem folytatható csak véges sok lépésig, mivel $a > a_1 > a_2 > \cdots$ természetes számok szigorú monoton csökkenő sorozata, amelynek előbb-utóbb az a szám egy prímosztójában kell végződjék.

Legyen u_1 az a szám prímosztója. Ekkor $a = u_1b_1$. Ha $b_1 = 1$ vagy prímszám, akkor megtaláltuk a prímtényezős felbontást. Ha nem, akkor b_1-nek van u_2 prímosztója, és $a = u_1u_2b_2$. Ha b_2 prímszám, akkor megtaláltuk a prímtényezős felbontást. És így tovább, ez az eljárás nem folytatható csak véges sok lépésig, mivel $a > b_1 > b_2 > \cdots$ természetes számok

szigorú monoton csökkenő sorozata, amelynek előbb–utóbb az a szám egy prímosztójában kell végződjék.

Unicitás. Legyen $a = u_1u_2\cdots u_r = v_1v_2\cdots v_s$ kétféle prímtényezős felbontás, $r \le s$. Mivel az u_1 prímszám, amely osztja a jobboldali szorzatot, osztja valamelyik v_{i_1} tényezőjét. Mivel v_{i_1} törzsszám, $u_1 = v_{i_1}$, átindexelés és egyszerűsítés után $u_1u_2\cdots u_{r-1} = v_1v_2\cdots v_{s-1}$, Ezt az eljárást folytatva $r-1$ lépés után kapjuk, hogy $u_1 = v_1v_2\cdots v_{s-r+1}$, Mivel u_1 törzsszám, ez csak úgy lehetséges, ha $r = s$ és (az átindexelések után) $u_1 = v_1$. □

Értelmeszerűen az egész számok prímtényezős felbontásában a tényezők lehetnek negatív prímelemek is, és a felbontás egyértelműségében az egységtényezőktől is el kell tekinteni. Általánosan is teljesül, hogy ha egy integritástartományban a maradékos osztást el lehet végezni, akkor teljesül az egyértelmű prímfaktorizáció.

Legyen a és b nemnulla nem egység egész szám, $|a| = p_1^{k_1}p_2^{k_2}\cdots p_r^{k_r}$ és $|b| = p_1^{l_1}p_2^{l_2}\cdots p_r^{l_r}$ felbontás, ahol $p_1, p_2, \dots, p_r$ különböző prímszámok, a nem közös prímosztók egyik kitevője zérus. Ekkor (ellenőrizze!):

$$(a,b) = p_1^{\min\{k_1,l_1\}}p_2^{\min\{k_2,l_2\}}\cdots p_r^{\min\{k_r,l_r\}}, \quad [a,b] = p_1^{\max\{k_1,l_1\}}p_2^{\max\{k_2,l_2\}}\cdots p_r^{\max\{k_r,l_r\}}.$$

Nevezetes tényt közöl a

6.10. Állítás. *Végtelen sok prímszám van.*

Bizonyítás. Indirekte érvelünk. Legyen az összes prímszám $p_1, p_2, \dots, p_r$, ahol r természetes szám. Ekkor az $1 + p_1p_2\cdots p_r$ számnak egyrészt létezik prímosztója a számelmélet alaptétele miatt, másrészt a $p_1, p_2, \dots, p_r$ prímszámok közül egyik sem osztja. □

7. Diofantoszi egyenlet, kongruencia

Egy egyenletet **diofantoszi egyenlet**nek nevezünk, ha egész megoldásait keressük. Sokféle ilyen egyenletet vizsgáltak, itt az **elsőfokú kétismeretlenes diofantoszi egyenlet**tel foglalkozunk. Általános alakja $ax + by = c$, ahol a, b nemnulla és c tetszőleges adott egész szám. A megoldás a következőképpen lehetséges:

7.1. Tétel. *Legyen a, b nemnulla egész szám és c tetszőleges egész szám. Az $ax + by = c$ diofantoszi egyenlet megoldható pontosan akkor, ha az (a, b) legnagyobb közös osztó osztja a c számot. Továbbá ha az (x_0, y_0) egész számpár megoldása a diofantoszi egyenletnek, akkor tetszőleges megoldás*

$$x = x_0 + \frac{b}{(a,b)}t$$
$$y = y_0 - \frac{a}{(a,b)}t$$

alakú valamely t egészre, és minden ilyen (x, y) számpár az egyenlet megoldása.

Bizonyítás. Tegyük fel, hogy az egyenletnek az (x_0, y_0) számpár megoldása, azaz $ax_0 + by_0 = c$ teljesül. Az egyenlőség baloldalát osztja az (a, b) legnagyobb közös osztó, ezért osztja a c számot is.

Megfordítva, tegyük fel most azt, hogy az (a, b) legnagyobb közös osztó osztja a c számot. A 6.4 állítás alapján $au + bv = (a, b)$ teljesül valamely u, v egészekre, amely egyenlőséget beszorozva a $\frac{c}{(a,b)}$ egész számmal kapjuk, hogy $a\frac{uc}{(a,b)} + b\frac{vc}{(a,b)} = c$, és a diofantoszi egyenlet megoldható.

Legyen $ax_0 + by_0 = c$ és az (x, y) egész számpár megoldás, azaz $ax + by = c$. A két egyenlőséget kivonva egymásból kapjuk, hogy $a(x - x_0) + b(y - y_0) = 0$. Elegendő tehát az $ax + by = 0$ úgynevezett homogén egyenlet általános megoldását megkeresni.

Nyilván $a\frac{b}{(a,b)}t + b\left(-\frac{a}{(a,b)}t\right) = 0$ tetszőleges t egész számra. Legyen az (x', y') számpár olyan, hogy $ax' + by' = 0$, azaz $ax' = -by'$. Leosztva az (a, b) legnagyobb közös osztóval kapjuk, hogy $\frac{a}{(a,b)}x' = -\frac{b}{(a,b)}y'$. Mivel a $\frac{b}{(a,b)}$ szám osztja a baloldalt, és relatív prím az $\frac{a}{(a,b)}$ számhoz, az általánosított prímtulajdonság miatt osztja az x' számot, azaz $x' = \frac{b}{(a,b)}t$ és $\frac{ab}{(a,b)}t = -\frac{b}{(a,b)}y'$. Egyszerűsítés után $y' = -\frac{a}{(a,b)}t$ adódik. □

A megoldhatóság ellenőrzése után a bizonyítás módszert ad az euklideszi algoritmus segítségével az (x_0, y_0) partikuláris megoldás megkeresésére. Az általános megoldást a képletbe való egyszerű behelyettesítés adja.

Legyen m 1-nél nagyobb természetes szám. Azt mondjuk, hogy az a **egész szám kongruens a** b **egész számmal modulo** m ha az m szám osztja a $b-a$ különbséget. Jelölés: $a \equiv b(\mod m)$. Az m számot a kongruencia **modulus**ának nevezzük. A modulo m kongruencia tulajdonságai a következők:

7.2.Állítás. *Legyen m, m' 1-nél nagyobb természetes szám, a, b, c, d tetszőleges egész számok. Ekkor az alábbi állítások teljesülnek:*

(i) A modulo m kongruencia ekvivalenciareláció az egész számok halmazán;

(ii) ha $a \equiv c(\mod m)$ és $b \equiv d(\mod m)$, akkor $a + b \equiv c + d(\mod m)$ és $ab \equiv cd(\mod m)$;

(iii) ha az m szám nem osztja a c számot és $ac \equiv bc(\mod m)$, akkor $a \equiv b(\mod \frac{m}{(m,c)})$;

(iv) ha $a \equiv b(\mod m)$ és $a \equiv b(\mod m')$, akkor $a \equiv b(\mod [m, m'])$

Bizonyítás. (i) A *reflexivitás* és a *szimmetria* világos. Legyen $a \equiv b(\mod m)$ és $b \equiv c(\mod m)$, azaz az m szám osztja a $b-a$ és $c-b$ számokat is. Ekkor, mivel $c-a = (c-b)+(b-a)$, az m szám osztja a $c - a$ számot is, azaz $a \equiv c(\mod m)$, ami a *tranzitivitás*t mutatja.

(ii) Legyen $a \equiv c(\mod m)$ és $b \equiv d(\mod m)$, azaz az m szám osztja a $c - a$ és a $d - b$ számokat. Ekkor, mivel $(c + d) - (a + b) = (c - a) + (d - b)$ és $cd - ab = cd - cb + cb - ab = c(d - b) + (c - a)b$, az m szám osztja a $(c + d) - (a + b)$ és a $cd - ab$ számot. Kaptuk, hogy $a + b \equiv c + d(\mod m)$ és $ab \equiv cd(\mod m)$.

(iii) Legyen $ac \equiv bc(\mod m)$, azaz az m szám osztja a $bc-ac = (b-a)c$ számot, $(b-a)c = ms$ valamely s egészre. Innen $(b - a)\frac{c}{(m,c)} = \frac{m}{(m,c)}s$, és az $\frac{m}{(m,c)}$ szám osztja a $b - a$ számot, azaz $a \equiv b(\mod \frac{m}{(m,c)})$.

(iv) Legyen $a \equiv b(\mod m)$ és $a \equiv b(\mod m')$, azaz az m és az m' szám osztja a $b - a$ számot. Ekkor, a legkisebb közös többszörös definíciója miatt az $[m, m']$ legkisebb közös többszörös is osztja a $b - a$ számot, azaz $a \equiv b(\mod [m, m'])$. □

A modulo m kongruencia ekvivalenciaosztályait **maradékosztály**oknak nevezzük. Egy osztályba azok az elemek tartoznak, amelyek ugyanazt a maradékot adják m-mel osztva maradékosan. Így a modulo m maradékosztályok száma éppen m: $\overline{0}, \overline{1}, \ldots, \overline{m-1}$.

7.3.Állítás. *Legyen m 1-nél nagyobb természetes szám. A modulo m maradékosztályok Z_m halmaza az $\overline{a}+\overline{b} = \overline{a+b}$ illetve az $\overline{a}\overline{b} = \overline{ab}$ műveletekre nézve kommutatív egységelemes gyűrűt alkot.*

Bizonyítás. A műveletek a 6.10.2 állítás szerint jóldefiniáltak, a műveleti tulajdonságok a műveletek definíciója és az egész számok megfelelő műveleti tulajdonságainak a következményei. (A részletes kifejtés gyakorlat.) □

A Z_m gyűrűt **modulo** m **maradékosztálygyűrű**nek nevezzük.

Az $ax \equiv b(\mod m)$ **egyismeretlenes elsőfokú kongruencia egyenlet** megoldását visszavezethetjük a kétismeretlenes diofantoszi egyenlet megoldására.

7.4.Tétel. *Legyen a nemnulla egész szám, b tetszőleges egész szám és m 1-nél nagyobb természetes szám. Az $ax \equiv b(\mod m)$ egyismeretlenes elsőfokú kongruencia egyenlet megoldható pontosan akkor, ha az (a,m) legnagyobb közös osztó osztja a b számot. A kongruencia egyenlet modulo m inkongruens összes megoldása $x = x_0 + \frac{m}{(a,m)}t$, ahol az x_0 egész a kongruencia egyenlet egy megoldása, és $t = 0, 1, \ldots, (a,m)-1$.*

Bizonyítás. Nyilván a kongruencia egyenlet ekvivalens az $ax + my = b$ diofantoszi egyenlettel, így a kongruencia megoldhatóságának szükséges és elegendő feltétele világos 7.1 alapján. Szintén innen következik, hogy a kongruencia tetszőleges megoldása $x = x_0 + \frac{m}{(a,m)}t$ alakú. Nyilván $0 \le t \le (a,m)-1$ esetén ezek az értékek inkongruensek modulo m, és az összes többi érték kongruens ezek közül valamelyikkel modulo m. □

7.5.Következmény. *A Z_m maradékosztálygyűrű test pontosan akkor, ha m prímszám.*

Bizonyítás. Ha a Z_m gyűrű test, akkor minden nemnulla eleme egység, azaz az $ax \equiv 1(\mod m)$ kongruencia megoldható ha m nem osztja az a számot. Azonban ha m nem törzsszám, akkor van w valódi (nem egység és nem asszociált) osztója, és ekkor a $wx \equiv 1(\mod m)$ kongruencia nem oldható meg, noha m nem osztja a w számot.

Megfordítva, ha m prímszám, akkor $1, 2, \ldots, m-1$ számok mindegyike relatív prím m-hez, és minden $1 \le a \le m-1$ egészre az $ax \equiv 1(\mod m)$ kongruencia megoldható, azaz nemnulla maradékosztálynak van multiplikatív inverze. Ez azt jelenti, hogy a Z_m maradékosztálygyűrű test. □

Ezeket a testeket prímelemű testeknek szokás nevezni.

Ha az a szám relatív prím az m modulushoz, akkor az $\overline{a}$ maradékosztályt **redukált maradékosztály**nak nevezzük. Számukat, azaz a $0, 1, 2, \ldots, m-1$ számok közül az m számhoz relatív prímek számát $\varphi(m)$-mel szokás jelölni, és a φ függvényt **Euler-féle φ-függvény**nek nevezni. Azt is mondhatjuk, hogy a modulo m maradékosztálygyűrű egységeinek száma $\varphi(m)$. Értékének meghatározásához szükség van az alábbi formulára, amelyben $|W|$ a W halmaz elemeinek a számát jelenti.

7.6.Állítás. *Legyen A véges halmaz, A_i az A halmaz részhalmaza ($i = 1, 2, \ldots, n$). Ekkor* $|\overline{A_1 \cup A_2 \cup \cdots \cup A_n}| =$

$$|\overline{A_1} \cup \overline{A_2} \cup \cdots \cup \overline{A_n}| = |A| - (|A_1| + |A_2| + \cdots + |A_n|) + (|A_1 \cap A_2| + |A_1 \cap A_3| + \cdots + |A_{n-1} \cap A_n|) - \cdots + \cdots$$

$$+ (-1)^k \sum_{1 \le i_1 < i_2 < \cdots < i_k \le n} |A_{i_1} \cap A_{i_2} \cap \cdot \cap A_{i_k}| + \cdots - \cdots + (-1)^n |A_1 \cap A_2 \cap \cdots \cap A_n|.$$

Bizonyítás. Indukció alapján érvelünk. Az $n = 2$ esetben a nyilvánvaló $|\overline{A_1 \cup A_2}| = |A| - (|A_1| + |A_2|) + |A_1 \cap A_2|$ összefüggést adja a formula. Jelölje a_n a formula jobb oldalának az értékét. Tegyük fel, hogy a formula teljesül $n-1$-re. Látjuk, hogy

$$a_{n-1} - a_n = |A_n| - (|A_1 \cap A_n| + |A_2 \cap A_n| + \cdots + |A_{n-1} \cap A_n|) + \cdots - \cdots +$$

$$(-1)^{k-1} \sum_{1 \le i_1 < i_2 < \cdots < i_{k-1} \le n-1} |A_{i_1} \cap A_{i_2} \cap \cdot \cap A_{i_{k-1}} \cap A_n| + \cdots - \cdots + (-1)^{n-1} |A_1 \cap A_2 \cap \cdots \cap A_n|.$$

Alkalmazva a formulát az $A = A_n$ halmazra és az $A_i \cap A_n$ részhalmazaira $(i = 1, 2, \dots, n-1)$ kapjuk, hogy $a_{n-1} - a_n$ a $B = A_n \setminus (A_1 \cup A_2 \cup \dots \cup A_{n-1})$ halmaz elemeinek a száma. Világos, hogy az $\overline{A_1 \cup A_2 \cup \dots \cup A_{n-1}}$ halmaz az $\overline{A_1 \cup A_2 \cup \dots \cup A_n}$ és a B halmazok diszjunkt uniója, és emiatt $a_{n-1} = |\overline{A_1 \cup A_2 \cup \dots \cup A_n}| + a_{n-1} - a_n$ azaz $a_n = |\overline{A_1 \cup A_2 \cup \dots \cup A_n}|$. $\square$

A formula alapján kiszámolhatjuk az $A = \{0, 1, \dots, m-1\}$ halmazban az $m = p_1^{k_1} p_2^{k_2} \cdots p_n^{k_n}$ természtes számhoz relatív prímek számát (itt a p_i számok különböző prímszámok, a k_i kitevők nemnulla természetes számok). Legyen A_i az A halmazban a p_i prímszám többszöröseinek a halmaza. Ekkor $\varphi(m) = |\overline{A_1 \cup A_2 \cup \dots \cup A_n}| =$

$$m - (\frac{m}{p_1} + \frac{m}{p_2} \cdots \frac{m}{p_n}) + (\frac{m}{p_1 p_2} + \frac{m}{p_1 p_3} \cdots \frac{m}{p_{n-1} p_n}) + \cdots - \cdots +$$

$$(-1)^k \sum_{1 \le i_1 < i_2 < \cdots < i_k \le n} \frac{m}{p_{i_1} p_{i_2} \cdots p_{i_k}} + \cdots - \cdots + (-1)^n \frac{m}{p_1 p_2 \cdots p_n},$$

amely kifejezést szorzattá alakítva kapjuk a

$$\varphi(m) = (p_1^{k_1} - p_1^{k_1 - 1})(p_2^{k_2} - p_2^{k_2 - 1}) \cdots (p_n^{k_n} - p_1^{k_n - 1})$$

összefüggést.

Euler-Fermat tételként ismert a következő

7.7.Tétel. *Legyen m 1-nél nagyobb természetes szám, és az a egész szám relatív prím az m számhoz. Ekkor $a^{\varphi(m)} \equiv 1 (\mod m)$.*

Bizonyítás. Nyilván redukált maradékosztályok szorzata redukált maradékosztály. Az $\overline{a}$ redukált maradékosztály összes pozitív egész kitevős hatványa nem lehet különböző, ezért $\overline{a}^k = \overline{a}^l$ valamely pozitív egész $k < l$ számra. Ekkor, felhasználva a 7.2.3 állítást, $\overline{a}^{l-k} = 1$ adódik. Legyen n a legkisebb pozitív egész, amelyre $\overline{a}^n = 1$. Ekkor az $\{1, \overline{a}, \overline{a}^2, \dots, \overline{a}^{n-1}\}$ n-elemű halmaz, és, mivel 7.2.3 szerint redukált maradékosztállyal lehet egyszerűsíteni, a redukált maradékosztályok halmaza előáll mint az $A = \{1, \overline{a}, \overline{a}^2, \dots, \overline{a}^{n-1}\}$, $A\overline{b_2} = \{\overline{b_2}, \overline{b_2}\overline{a}, \overline{b_2}\overline{a}^2, \dots, \overline{b_2}\overline{a}^{n-1}\}, \dots, A\overline{b_s} = \{\overline{b_s}, \overline{b_s}\overline{a}, \overline{b_s}\overline{a}^2, \dots, \overline{b_s}\overline{a}^{n-1}\}$ halmazok diszjunkt uniója, ahol a $\overline{b_i}$ elemek alkalmas redukált maradékosztályok. Összeszámlálva az elemeket kapjuk, hogy $\varphi(m) = sn$, és $\overline{a}^{\varphi(m)} = \overline{a}^{sn} = (\overline{a}^n)^s = 1^s = 1$, ami átírva kongruenciává a kívánt állítást adja. $\square$

8. Számrendszerek, racionális számok tizedes tört alakja

A természetes számok különféle alapú számrendszerekben való előállításáról szól a

8.1.Tétel. *Legyen u 1-nél nagyobb természetes szám és a nemnulla természetes szám. Ekkor egyértelműen létezik s természetes szám és $0 \le a_i \le u - 1$ természetes szám $(i = 0, 1, \dots, s)$, $a_s \neq 0$ úgy, hogy*

$$a = \sum_{i=0}^{s} a_i u^i.$$

Bizonyítás. Egzisztencia. Végezzük el maradékos osztások alábbi sorozatát:

$$a = uq_0 + a_0,\ 0 \le a_0 < u$$
$$q_0 = uq_1 + a_1,\ 0 \le a_1 < u$$
$$q_1 = uq_2 + a_2,\ 0 \le a_1 < u$$
$$\dots\dots\dots\dots\dots$$
$$q_{i-1} = uq_i + a_i,\ 0 \le a_i < u$$
$$\dots\dots\dots\dots\dots$$

Mivel $a > q_0 > q_1 > q_2 > \cdots > q_i > \cdots$ természetes számok szigorú monoton csökkenő sorozata, véges sok lépés után q_{s-1} kisebb lesz, mint u, és az utolsó lépésben $q_{s-1} = u0 + a_s$, az utolsó hányados $q_s = 0$. A végéről visszafelé haladva lépésenként kapjuk, hogy

$$\begin{gathered} q_{s-1} = a_s \\ q_{s-2} = a_s u + a_{s-1} \\ q_{s-3} = a_s u^2 + a_{s-1} u + a_{s-2} \\ \ldots\ldots\ldots\ldots\ldots\ldots \\ q_0 = a_s u^{s-1} + a_{s-1} u^{s-2} + \cdots + a_2 u + a_1 \\ a = a_s u^s + a_{s-1} u^{s-1} + \cdots + a_1 u + a_0 \end{gathered}$$

Unicitás. Ha $a = \sum_{i=0}^{t} a_i' u^i$ egy másik ilyen felírás, akkor szükségképpen az a_i' értékek rendre a fenti maradékos osztások maradékaival kell, hogy megegyezzenek, mivel $a = u \sum_{i=1}^{t} a_i' u^{i-1} + a_0'$, $\sum_{i=1}^{t} a_i' u^{i-1} = u \sum_{i=2}^{t} a_i' u^{i-2} + a_1$, és így tovább. Következésképp $s = t$ és $a_i = a_i'$. $\square$

A tételben szereplő u számot a **számrendszer alapjá**nak, az a_i számot az a szám u^i **helyiértékű számjegyé**nek nevezzük, és az $a = a_s a_{s-1} \ldots a_1 a_{0_{\underline{u}}}$ jelölést alkalmazzuk. Nevezetes számrendszerek a 2-alapú **bináris**, a 16-alapú **hexadecimális**, a 10-alapú **decimális**.

Nevezetesek a tizes számrendszerbeli oszthatósági szabályok:

- egy természetes szám osztható 2-vel illetve 4-gyel, ha az utolsó egy illetve kettő számjegyéből alkotott szám osztható 2-vel illetve 4-gyel;
- egy természetes szám osztható 5-tel illetve 25-tel, ha az utolsó egy illetve kettő számjegyéből alkotott szám osztható 5-tel illetve 25-tel;
- egy természetes szám osztható 3-mal illetve 9-cel, ha a számjegyeinek összege osztható 3-mal illetve 9-cel;
- egy természetes szám osztható 11-gyel ha a számjegyeinek váltakozó előjellel vett összege osztható 11-gyel.

  Ezek bizonyítása gyakorlat; példaként az utolsó belátásához vegyük észre, hogy $10 \equiv -1 (\mod 11)$, $10^i \equiv (-1)^i (\mod 11)$, és ennélfogva

$$a = \sum_{i=0}^{s} a_i 10^i \equiv \sum_{i=0}^{s} a_i (-1)^i (\mod 11).$$

Legyen a nemnulla racionális szám. Ekkor, mivel egyszerűsíthetünk a számláló és a nevező legnagyobb közös osztójával, előjeltől eltekintve egyértelműen létezik p és q relatív prím egész szám úgy, hogy $a = \frac{p}{q}$, a **racionális szám redukált közönséges tört alakja**. Legyen $0 < a < 1$ racionális szám redukált alakja $a = \frac{p}{q}$, ahol $p < q$ természetes számok. Végezzük el a maradékos osztások alábbi sorozatát:

$$\begin{gathered} 10p = qa_1 + r_1 \\ 10r_1 = qa_2 + r_2 \\ \ldots\ldots\ldots\ldots \\ 10r_{k-1} = qa_k + r_k \\ \ldots\ldots\ldots\ldots \end{gathered}$$

Nyilván a hányadosokra $0 \leq a_i \leq 9$ teljesül. Ekkor, lépésenként visszahelyettesítve,

$$\frac{p}{q} = a_1 10^{-1} + \frac{r_1}{10q} = a_1 10^{-1} + a_2 10^{-2} + \frac{r_2}{10^2 q} = \cdots =$$

$$a_1 10^{-1} + a_2 10^{-2} + \cdots + a_k 10^{-k} + \frac{r_k}{10^k q} = \cdots$$

Mivel az r_i maradékok 0 és q közé esnek, létezik egy legkisebb i index és t természetes szám, hogy $r_i = r_{i+t}$, és a többi maradék már ismétlődik, azaz $j \geq i$ indexekre $r_j = r_{j+t}$ teljesül. Ha $i = 1$ akkor azt mondjuk, hogy az a **racionális szám tiszta szakaszos tizedes tört alakba írható**, és az $a = 0, \dot{a_1}a_2 \ldots \dot{a_t}$ jelölést alkalmazzuk. A fenti összefüggésekből világos, hogy

$$a = \frac{a_1 10^{t-1} + a_2 10^{t-2} + \cdots + a_t}{10^t} \sum_{i=0}^{\infty} \frac{1}{10^{it}} = \frac{a_1 10^{t-1} + a_2 10^{t-2} + \cdots + a_t}{10^t} \frac{10^t}{10^t - 1} =$$

$$\frac{a_1 10^{t-1} + a_2 10^{t-2} + \cdots + a_t}{10^t - 1}$$

a mértani sor összegképlete alapján, azaz tiszta szakaszos tizedes törtet úgy írunk át közönséges tört alakba, hogy a számláló a szakasz számjegyeiből képzett szám, a nevező pedig annyi 9-esből képzett szám, ahány számjegyből áll a szakasz. Ha $i > 1$ akkor azt mondjuk, hogy az a **racionális szám vegyes szakaszos tizedes tört alakba írható**, és az $a = 0, a_1 a_2 \ldots a_{i-1}\dot{a_i}a_{i+1} \ldots \dot{a_{i+t-1}}$ jelölést alkalmazzuk, ahol $a_1 a_2 \ldots a_{i-1}$ az **előszakasz** illetve $\dot{a_i}a_{i+1} \ldots \dot{a_{i+t-1}}$ a **szakasz**. A fenti összefüggésekből világos, hogy

$$a = \frac{a_1 10^{i-2} + a_2 10^{i-3} + \cdots + a_{i-1}}{10^{i-1}} + \frac{a_i 10^{t-1} + a_{i+1} 10^{t-2} + \cdots + a_{i+t-1}}{10^{t+i-1}} \sum_{i=0}^{\infty} \frac{1}{10^{it}} =$$

$$\frac{a_1 10^{i-2} + a_2 10^{i-3} + \cdots + a_{i-1}}{10^{i-1}} + \frac{a_i 10^{t-1} + a_{i+1} 10^{t-2} + \cdots + a_{i+t-1}}{10^{t+i-1}} \frac{10^t}{10^t - 1} =$$

$$= \frac{a_1 10^{i+t-2} + \cdots + a_{i-1} 10^t + a_i 10^{t-1} + \cdots + a_{i+t-1} - (a_1 10^{i-2} + a_2 10^{i-3} + \cdots + a_{i-1})}{(10^t - 1)10^{i-1}}$$

azaz vegyes szakaszos tizedes törtet úgy írunk át közönséges tört alakba, hogy a számláló az előszakasz és a szakasz számjegyeiből képzett számból kivonva az előszakasz számjegyeiből képzett szám, a nevező pedig annyi 9-esből illetve utána annyi 0-ból képzett szám, ahány számjegyből áll a szakasz illetve az előszakasz.

Speciálisan ha a szakasz a 0 számjegy, akkor azt mondjuk, hogy a racionális szám **véges tizedes tört alakba írható**, és az $a = 0, a_1 a_2 \ldots a_{i-1}$ jelölést alkalmazzuk. Az előállítás nem egyértelmű, véges tizedes törteknek van végtelen tizedes tört alakjuk is, például $1,5 = 1,4\dot{9}$ (ellenőrizze!).

Nemnegatív racionális szám egész része a nála nem nagyobb legnagyobb természetes szám, törtrésze a szám és egészrészének különbsége. Az egész részt tizes számrendszerbe, a törtrészt tizedes tört alakba írva kapjuk a szám $a_s a_{s-1} \ldots a_0, a_{-1} a_{-2} \ldots$ tizedes tört alakját. Az előjelet eléírva határozhatjuk meg ellentettjének tizedes tört alakját.

8.2.Állítás. *Legyen $0 < a < 1$ racionális szám, redukált közönséges tört alakja $\frac{p}{q}$. Ekkor a következő állítások teljesülnek:*

(i) az a szám tiszta szakaszos tizedes tört alakba írható pontosan akkor ha a q természetes szám és 10 relatív prímek;

(ii) az a szám vegyes szakaszos tizedes tört alakba írható pontosan akkor ha a q természetes szám és 10 nem relatív prímek;

(iii) az a szám véges tizedes tört alakba írható pontosan akkor ha a q természetes számnak a 2 és 5 prímeken kívül más prímosztója nincsen.

Bizonyítás. Nyilván az a racionális szám vagy tiszta vagy vegyes szakaszos tizedes tört alakba írható.

Tegyük fel, hogy az $a = \frac{p}{q}$ racionális szám tiszta szakaszos tizedes tört alakba írható, szakaszának t darab számjegyéből képzett természetes szám legyen c. Ekkor $a = \frac{c}{10^t-1}$ és a q szám osztja a $10^t - 1$ számot; nyilván q és 10 relatív prímek.

Tegyük fel, hogy az $a = \frac{p}{q}$ racionális szám olyan, hogy q és 10 relatív prímek és az a szám mégis vegyes szakaszos tizedes tört alakba írható. Legyen az előszakasz s darab számjegyéből képzett természetes szám b, és szakaszának t darab számjegyéből képzett természetes szám c. Ekkor az $a = \frac{10^t b+c-b}{(10^t-1)10^s}$ közönséges törtnek egyszerűsíthetőnek kell lennie 10^s-nel, azaz 10^s-nek osztania kell a $10^t b + c - b$ számlálót. Ha $t \geq s$ akkor 10^s-nek osztania kell a $c - b$ számot, ami csak akkor lehetséges, ha a c szám utolsó s számjegye megegyezik b számjegyeivel, ami azt jelenti, hogy az előállítás tiszta szakaszos, a szakasz az első t tizedesjegy. Ha $t < s$ akkor a b szám utolsó $s-t$ számjegyének és a c szám számjegyeinek meg kell egyeznie a b szám számjegyeivel, ami szintén azt jelenti, hogy az előállítás tiszta szakaszos, a szakasz az első t tizedesjegy.

Az (i) állítást beláttuk, ennek a (ii) állítás közvetlen következménye. A (iii) állítás nyilvánvaló. □

Azt mondjuk, hogy az α **valós szám tizedes tört alakja** $c, a_1a_2\ldots$, ahol c egy decimális alakban felírt egész szám és $a_1, a_2, \ldots$ tizedesjegyek, ha az $u_0 = c, u_1 = c, a_1, u_2 = c, a_1a_2, \ldots$ racionális számsorozatot tartalmazza az α osztály (másszóval az u_n sorozat valós határértéke α).

8.4.Tétel. *Minden valós szám felírható tizedes tört alakban, ezek közül a racionálisak pontosan a szakaszos tizedes tört alakba írhatók.*

Bizonyítás. Nyilván elegendő a felírhatóságot pozitív valós α számra belátni. Legyen $u_0 = c$ a nála nem nagyobb legnagyobb egész szám; $u_1 = c, a_1$ a nála nem nagyobb legnagyobb szám a $\{c, 0; c, 1; \ldots c, 9\}$ számok közül; $u_2 = c, a_1a_2$ a nála nem nagyobb legnagyobb szám a $\{c, a_1 0; c, a_1 1; \ldots c, a_1 9\}$ számok közül; és így tovább. A kapott u_n sorozat nyilván tart az α valós számhoz.

Be kell még látni, hogy racionális számnak nem lehet nem szakaszos felírása. Legyen az a racionális számnak egyszerre szakaszos és nem szakaszos felírása; feltehetjük, hogy $0 < a < 1$. Az első különböző tizedesjegy legyen a t-edik, és legyen b illetve c az ezután következő tizedesjegyek levágásával keletkezett véges tizedes tört a szakaszos illetve a nem szakaszos felírásban. Ha $b < c$ akkor, mivel a nem szakaszos felírásban a levágott végtelen rész értéke nagyobb, mint 0, $a \leq b + 10^{-t} \leq c < a$, ami lehetetlen. Ha $c < b$ akkor, mivel a nem szakaszos felírásban a levágott végtelen rész értéke kisebb, mint 10^{-t}, $a < c + 10^{-t} \leq b \leq a$, ami lehetetlen. Kaptuk, hogy a nem szakaszos tizedes törtek éppen az irracionális számok előállításai. □

9. A polinomgyűrű

Legyen A kommutatív egységelemes gyűrű, $x \notin A$ határozatlannak nevezett szimbólum. Az $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots a_1 x + a_0$ alakú formális összeget, ahol az a_i együtthatók

az A gyűrű elemei, $a_n \neq 0$, n természetes szám, **az A gyűrű feletti egyhatározatlanú polinom**nak, n-et, ha nem minden együttható 0, a **polinom fokszám**ának nevezzük és f°-rel jelöljük. Ha az a_n együttható 1, akkor **főpolinom**ról beszélünk. A polinomok közötti összeadás és szorzás minden megszokott műveleti tulajdonság felhasználásával történik. Nem nehéz belátni, hogy ezekkel a műveletekkel a polinomok halmaza egységelemes kommutatív gyűrűt alkot. Precizírozott bizonyítással az alábbi tételt látjuk be.

9.1.Tétel. *Legyen A kommutatív egységelemes gyűrű. Jelölje $A[x]$ az olyan A-beli sorozatok halmazát, amelyeknek csak véges sok tagja nemnulla. Legyen $a, b \in A[x]$, összegüket és szorzatukat határozzuk meg az alábbi módon:*

$$(a+b)_n = a_n + b_n, \quad (ab)_n = \sum_{i=0}^{n} a_i b_{n-i}.$$

Ekkor az $(A[x], +, \cdot)$ struktúra kommutatív egységelemes gyűrű, továbbá ha az A struktúra integritástartomány, akkor az $A[x]$ struktúra is integritástartomány

Bizonyítás. Legyen a, b, c az $A[x]$ halmaz eleme. Nyilván az összeadás és szorzás művelet.

Az additív struktúra Abel-csoport. Nyilvánvaló az A gyűrű megfelelő tulajdonságaiból.

A multiplikatív struktúra asszociatív. Egyrészt

$$((ab)c)_n = \sum_{i=0}^{n} (ab)_i c_{n-i} = \sum_{i=0}^{n} \sum_{j=0}^{i} a_j b_{i-j} c_{n-i},$$

másrészt

$$(a(bc))_n = \sum_{i=0}^{n} a_i (bc)_{n-i} = \sum_{i=0}^{n} \sum_{j=0}^{n-i} a_i b_j c_{n-i-j}.$$

Mindkét kapott kifejezés egyenlő a $\sum_{i+j \leq n} a_i b_j c_{n-i-j}$ összeggel.

A *szorzás kommutativitása* nyilvánvaló. Az a sorozat, amelynek nulladik tagja 1 a többi 0 *egységelem.*

Disztributivitás. A kommutativitás miatt elegendő az egyik tulajdonságot belátni. Nyilván

$$((a+b)c)_n = \sum_{i=0}^{n} (a+b)_i c_{n-i} = \sum_{i=0}^{n} (a_i + b_i) c_{n-i} = \sum_{i=0}^{n} (a_i c_{n-i} + b_i c_{n-i}) =$$

$$\sum_{i=0}^{n} a_i c_{n-i} + \sum_{i=0}^{n} b_i c_{n-i} = (ac)_n + (bc)_n.$$

Zérusosztómentesség. Legyen a és b két nem konstans nulla sorozat olyan, hogy maximális indexű nemnulla tagjaik a_n és b_m. Ekkor $(ab)_{n+m} = a_n b_m \neq 0$. $\square$

A sorozatok fenti szorzatát szokás **konvolúciószorzás**nak nevezni. Jelölje 1 azt a sorozatot, amelynek nulladik tagja 1 a többi 0; jelölje x azt a sorozatot, amelynek első tagja 1 a többi 0; jelölje x^2 azt a sorozatot, amelynek második tagja 1 a többi 0, és így tovább. A fenti jelöléssel illetve azonosítva az A-beli skalárokat azokkal a sorozatokkal, amelyeknek nulladik tagja az adott elem a többi 0, az $f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots a_1 x + a_0$ formális összegekben levő „műveletek" az $A[x]$ gyűrűbeli műveletekként értelmezhetőek, és minden $A[x]$ halmazbeli sorozat felírható ilyen alakban. A továbbiakban a polinomokat ilyen előállításban fogjuk

tekinteni. Az $A[x]$ struktúrát **az A gyűrű feletti egyhatározatlanú polinomgyűrű**nek nevezzük.

Azt mondjuk, hogy az $a(x)$ $A[x]$ **polinom osztja a** $b(x) \in A[x]$ **polinomot**, ha létezik $c(x) \in A[x]$ polinom, hogy $b(x) = a(x)c(x)$, jelölés: $a(x)|b(x)$. Az oszthatóság tulajdonságai az egész számok esetével analóg módon bizonyíthatók (lásd 6.1.).

Az egységeket egyszerűen megkereshetjük a polinomok között.

9.2.Állítás. *Az $A[x]$ A integritástartomány feletti polinomgyűrű egységei az A gyűrű egységei.*

Bizonyítás. Nyilván az A-beli skalár egységek a polinomgyűrűben is egységek. Ha az $f(x), g(x)$ polinomokra $f(x)g(x) = 1$, akkor, mivel nyilván szorzatpolinom fokszáma a fokszámok összege, $f^\circ + g^\circ = 0$, ami csak úgy lehet, ha mindkét polinom fokszáma nulla, azaz skalár egységek. □

Azt mondjuk, hogy a $b(x) \in A[x]$ **polinom az** $a(x) \in A[x]$ **polinom asszociáltja,** ha $b(x) = a(x)c(x)$, ahol $c(x)$ egység, azaz egység az A polinomgyűrűben; jelölés: $a(x) \sim b(x)$. Az asszociáltság nyilván ekvivalenciareláció.

Ha az együtthatók struktúrája test, akkor elvégezhető benne a maradékos osztás az úgynevezett polinom osztása polinommal algoritmus alapján.

9.3.Tétel. *Legyen K test, $g(x), f(x)$ a $K[x]$ polinomgyűrű nemnulla elemei. Ekkor egyértelműen létezik $q(x), r(x)$ polinom a $K[x]$ polinomgyűrűből, hogy $g(x) = f(x)q(x) + r(x)$, és az $r(x)$ polinom a zéruspolinom, vagy $r^\circ < f^\circ$.*

Bizonyítás. Egzisztencia. Legyen az $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots a_1 x + a_0$ illetve $g(x) = b_m x^n + b_{m-1}x^{n-1} + \cdots b_1 x + b_0$ polinom fokszáma n illetve m. Ha $n > m$ akkor a $q(x) = 0$ és $r(x) = g(x)$ választás megfelelő. Legyen $c_{m-n} = \frac{b_m}{a_n}$. Ekkor a $g_{(1)}(x) = g(x) - f(x)c_{m-n}x^{m-n}$ polinom fokszáma kisebb, mint m, ha n-nél is kisebb, akkor $q(x) = c_{m-n}x^{m-n}$ és $r(x) = g_{(1)}(x)$ választással megkaptuk a hányadost és a maradékot. Legyen a $g_{(1)}(x)$ polinom $m-1$-edfokú tagjának (esetlegesen zérus) együtthatója u_1 és $c_{m-n-1} = \frac{u_1}{a_n}$. Ekkor a $g_{(2)}(x) = g_{(1)}(x) - f(x)c_{m-n-1}x^{m-n-1}$ polinom fokszáma kisebb, mint $m-1$, ha n-nél is kisebb, akkor $q(x) = c_{m-n}x^{m-n} + c_{m-n-1}x^{m-n-1}$ és $r(x) = g_{(2)}(x)$ választással megkaptuk a hányadost és a maradékot. És így tovább, legföljebb az $m-n$-edik lépésben az eljárás véget ér: a $g_{(m-n)}(x)$ polinom n-edfokú tagjának együtthatója legyem u_{m-n} és $c_0 = \frac{u_{m-n}}{a_n}$. Ekkor az $r(x) = g_{(m-n)}(x) - f(x)c_0$ polinom fokszáma kisebb, mint n, és a $q(x) = c_{m-n}x^{m-n} + c_{m-n-1}x^{m-n-1} + \cdots + c_0$ választással megkaptuk a hányadost és a maradékot.

Unicitás Indirekte érvelünk. Legyen $g(x) = f(x)q(x) + r(x)$ és $g(x) = f(x)t(x) + w(x)$ a feltételeknek megfelelő két maradékos osztás, $q(x) \neq t(x)$. A két egyenlőséget kivonva egymásból $0 = f(x)(q(x) - t(x)) + (r(x) - w(x))$ azaz $f(x)(t(x) - q(x)) = r(x) - w(x)$, ahol a bal oldal fokszáma legalább n, a jobboldal fokszáma kisebb, mint n, ami ellentmondás. □

Az egészekhez hasonló elnevezéseket használunk: **osztandó, osztó, hányados, maradék**. A maradékos osztáson alapuló **euklideszi algoritmus** is analóg módon végezhető el az $a(x), b(x) \in K[x]$ polinomokon:

$$
\begin{gathered}
b(x) = a(x)q_1(x) + r_1(x), \;\; r_1^\circ < a^\circ \\
a(x) = r_1(x)q_2(x) + r_2(x), \;\; r_2^\circ < r_1^\circ \\
r_1(x) = r_2(x)q_3(x) + r_3(x), \;\; r_3^\circ < r_2^\circ \\
\cdots\cdots\cdots\cdots\cdots\cdots \\
r_{n-3}(x) = r_{n-2}(x)q_{n-1}(x) + r_{n-1}(x), \;\; r_{n-1}^\circ < r_{n-2}^\circ \\
r_{n-2}(x) = r_{n-1}(x)q_n(x) + r_n(x), \;\; r_n(x) = 0.
\end{gathered}
$$

Ha $a(x) \in K[x]$ és $b(x) \in K[x]$ nemnulla polinomok, akkor **legnagyobb közös osztó**juknak nevezzük azt a $d(x) \in K[x]$ főpolinomot, amelyre teljesül, hogy $d(x)$ osztja az $a(x)$ és a $b(x)$ polinomot is, és ha egy $c(x) \in K[x]$ polinom szintén osztja az $a(x)$ és a $b(x)$ polinomot, akkor $c(x)$ osztja a $d(x)$ polinomot is. Jelölés: $(a(x), b(x))$. A legnagyobb közös osztó létezését az euklideszi algoritmus biztosítja. Bármely két nemnulla polinomnak a $K[x]$ testfölötti polinomgyűrűből létezik legnagyobb közös osztója, nevezetesen a rajtuk végrehajtott euklideszi algoritmus utolsó nemnulla maradékával asszociált főpolinom, a bizonyítás analóg a 6.3 állításával. A legnagyobb közös osztó képzésének tulajdonságai főpolinomokra megegyeznek a természetes számoknál kapottakkal, lásd a 6.4 és 6.5 állítást.

Azt mondjuk, hogy az $a(x), b(x) \in K[x]$ nemnulla polinomok **legkisebb közös többszörös**e az $m(x) \in K[x]$ főpolinom, ha az $a(x)$ és a $b(x)$ polinom is osztja az $m(x)$ polinomot, másszóval közös többszörösük, és ha a $c(x) \in K[x]$ polinom szintén közös többszöröse az $a(x)$ és a $b(x)$ polinomoknak, akkor többszöröse az $m(x)$ polinommnak is. Jelölés: $[a(x), b(x)]$.

Az $\frac{a(x)b(x)}{(a(x),b(x))}$ polinommal asszociált $m(x)$ főpolinom az $a(x), b(x) \in K[x]$ nemnulla polinomok legkisebb közös többszöröse, a bizonyítás analóg a 6.6 állításával. A legkisebb közös többszörös képzésének tulajdonságai főpolinomokra megegyeznek a természetes számoknál kapottakkal, lásd a 6.7 állítást.

Nemnulla és nem egység $K[x]$-beli polinomról azt mondjuk, hogy **prímpolinom**, ha valahányszor oszt egy $b(x)c(x)$ szorzatot ($b(x), c(x) \in K[x]$ polinomok), akkor osztja legalább egyik tényezőjét is. Nemnulla és nem egység $u(x) \in K[x]$ polinomról azt mondjuk, hogy **irreducibilis polinom**, ha $u(x) = a(x)b(x)$ ($a(x), b(x) \in K[x]$ polinomok) egy faktorizációja, akkor valamelyik tényező egység, azaz nemnulla nulladfokú polinom.

Testfeletti polinom prím akkor és akkor, ha irreducibilis, a bizonyítás analóg a 6.9 állításával. A 6.10. tételhez hasonlóan látható be a polinomelmélet alaptétele, a részletezés gyakorlat..

9.4.Tétel. *Tetszőleges nemnulla nem egység testfölötti polinom sorrendtől és egységtényezőtől eltekintve egyértelműen bontható fel prímpolinomok szorzatára.*

Az egészekéhez hasonló elmélet építhető fel a test fölötti polinomgyűrűben a diofantoszi egyenletekre, a kongruenciára és a kongruencia egyenletekre.

Euklideszi gyűrűnek nevezzük az A integritástartományt, ha létezik egy $\alpha : A \setminus \{0\} \to \mathbb{N}$ **euklideszi normá**nak nevezett leképezés úgy, hogy bármely $a, b \in A$ nemnulla elemhez létezik $q, r \in A$ elem, melyre teljesül, hogy $b = aq + r$, és $r = 0$ vagy $\alpha(r) < \alpha(a)$.

Az egészeknél az euklideszi norma az abszolútérték, a test fölötti polinomgyűrűben a fokszám, így ezek euklideszi gyűrűk. Mivel a bizonyítások során csak olyan tulajdonságokat használtunk fel, amelyek az euklideszi gyűrűkben teljesülnek, euklideszi gyűrűben az egészekével és a test fölötti polinomgyűrűével analóg oszthatóságelmélet építhető fel.