Fried Ervin

ALGEBRA I.
Elemi és lineáris algebra

Fried Ervin

ALGEBRA I.

Elemi és lineáris algebra

TYPOTEX

A mű digitális formában történő megjelenését a Nemzeti Kulturális Alap támogatta.

Bírálók: dr. Csákány Béla egyetemi tanár és dr. Pálfy Péter Pál egyetemi tanár

ISBN 978 963 279 993 3

Kedves Olvasó!
Köszönjük, hogy kínálatunkból választott olvasnivalót!
Újabb kiadványainkról, akcióinkról a *www.typotex.hu*
és a *facebook.com/typotexkiado* oldalakon értesülhet.

Typotex Kiadó
Alapította Votisky Zsuzsa, 1989
A kiadó az 1795-ben alapított Magyar Könyvkiadók
és Könyvterjesztők Egyesülésének tagja.
Felelős kiadó: Németh Kinga
Főszerkesztő: Horváth Balázs
Műszaki szerkesztő: Fried Katalin

TARTALOM

ELŐSZÓ

Ez a tankönyv elsődlegesen az Eötvös Loránd Tudományegyetem elsőéves matematikus és alkalmazott matematikus hallgatói számára készült, e szakoknak a tematikáját követi; az elemi algebrai és a lineáris algebrai ismeretek a matematika szinte minden területén és az alkalmazásokban is nélkülözhetetlenek. Emellett a lineáris algebra szükségszerűen absztrakt tárgyalása jó átmenetet nyújt a tervezett második kötetben szereplő algebrai struktúrákhoz is.

Ma már Magyarországon (is) sok egyetemi szintű jegyzet és tankönyv foglalkozik az elemi és lineáris algebra tárgyalásával. Ezek mindegyike más felfogásban tárgyalja a fenti tananyagot, ezért nem lehet e tankönyveket rangsorolni; tulajdonképpen jól kiegészítik egymást. Ez a tankönyv az 1977-ben megjelent *Klasszikus és lineáris algebra* c. tankönyvem pótlására készült, amelynek legutóbbi kiadása is elfogyott. Tekintettel arra, hogy az idézett tankönyvhöz képest lényeges változtatásokat éreztem szükségesnek (többek között szerettem volna egységesíteni az ugyancsak nem kapható *Általános algebra* c. tankönyvemmel), ezért nem tartottam jónak a fenti tankönyv újabb — lényegében változatlan — kiadását. Nem változtattam a könyv „szellemén”, a tananyagot is főleg bővítettem. A tételek bizonyításában a leglényegesebb változás az, hogy az ottani formalizmust igyekeztem elkerülni, arra törekedve, hogy a definíciók ne „ügyesek”, hanem a lényeget jobban megmutatók legyenek.

A kötet két részre oszlik. Az első rész tárgya a klasszikus vagy elemi algebra. A középiskolában tanult számfogalom átismétlése és néhány általános algebrai fogalom (elnevezés) bevezetése után a komplex számok ismertetése következik. Ezek után a mátrixok, majd a determináns bevezetésére kerül sor. E résznek a befejezéseként az egy- és többhatározatlanú polinomokat tárgyaljuk. Itt alapvető szempont a fogalmak minél tisztább, minél precízebb bevezetése. Csak ezután kerülhet sor az érdemi tárgyalásra.

A második rész a lineáris algebra. A lineáris algebra eredetileg elsősorban a lineáris egyenletrendszerekkel foglalkozott. Ehhez a mátrixok és ezekhez kapcsolódva a koordináták szolgáltatták a módszert. E felfogással szemben nagy változást jelentett a tömör jelölésmód, amelyben a vektorterek és a lineáris leképezések jutottak szóhoz. Ennek megfelelően a fogalmak geometriai jelentést kaptak; ezáltal sokkal világosabbá váltak. Éles ellentétként a fogalmak absztraktabbak lettek, ami az elvontabb tárgyalásmódot tette szükségessé. A fentebb említett tankönyvhöz képest igyekeztem ezen enyhíteni, ahol tudtam (mind a definíciókban, mind a tárgyalás sorrendjében). A könyvben ■ jelöli a bizonyítások, illetve definíciók és □ jelöli a megjegyzések végét.

Remélem, hogy ezt a tankönyvet sikerrel használhatják más szakok és más egyetemek hallgatói is. Elsősorban természetesen azokra a hallgatókra gondolok, akik matematikus szakra járnak. Úgy vélem, hogy egyéb matematikát tanuló egyetemi hallgatók is tanulhatnak e könyvből; mindenekelőtt algebrai módszereket.

Természetesen egyetlen könyv (de az internet sem) sem pótolhatja az élő előadás élményét. A matematikát csak úgy lehet megtanulni, ha (lehetőleg aktívan) nyomon követjük a gondolkodásmódot, az esetleges hibákat; és a tételeket, a fogalmakat és a bizonyításokat *in statu nascendi* (a születés pillanatában) láthatjuk. Semmi sem pótolhat egy vitát az előadóval. Az írott segédanyagra az ismeretek felfrissítésekor van szükség. Ettől függetlenül célszerűnek tartom azt, hogy a tankönyv a közölt tananyagon kívül lehetőleg gondolkozni is tanítson és magyarázzon. Természetesen ehhez szükséges, hogy a fogalmak, tételek és a bizonyítások (eltekintve néhány hosszadalmas és mechanikus bizonyítástól) mind megtalálhatóak legyenek a tankönyvben.

A szereplő fogalmak és tételek az elméleti és az alkalmazott matematika legkülönbözőbb területeiről származnak. Ezeknek a fogalmaknak a motivációjáról azért mondtam le, mert ez az egész tárgyalást igen hosszadalmassá és esetleg érthetetlenebbé tenné. Megmaradtam az algebrai keretek között, és az alkalmazásokra való utalást a megfelelő szaktárgyakra hagytam.

Köszönetnyilvánítás. E könyv készítésében hálával tartozom azoknak, akik velem a matematikai gondolkozásmódot megismertették és megszerettették. Így NEUKOMM GYULA gimnáziumi tanáromnak, GEHÉR ISTVÁN egyetemi diáktársamnak, FUCHS LÁSZLÓ, RÉNYI ALFRÉD, PÉTER RÓZSA és mindenekfelett TURÁN PÁL egyetemi tanáraimnak. Hálával tartozom diákjaimnak és tanítványaimnak, akik állandó javító célzattal bírálták munkáimat; és akiktől ugyancsak nagyon sokat tanultam. Ezeknek a diákoknak a száma olyan nagy, hogy őket felsorolva óhatatlanul kimaradna jó néhány, akiket nem szeretnék megbántani. Ezért inkább egyetlen nevet sem írok ide; ők úgyis tudják, hogy róluk van szó. Hálával tartozom algebrista kollégáimnak, akik jelenlétükkel erősítették a magyar algebrista közösséget.

Vannak, akik a könyv közvetlen megjelenését is elősegítették. Hálával és köszönettel tartozom két lektoromnak, CSÁKÁNY BÉLÁnak és PÁLFY PÉTER PÁLnak, akik magukra vállalták az átnézés keserveit, számos értelemzavaró hibától mentve meg a könyvet. Ha valami benne maradt, az nem az ő munkájukat, hanem az enyémet minősíti.

Hálával tartozom a könyv előállításában való részvételéért FRIED KATALINnak a szedésért, a Nemzeti Tankönyvkiadóban PALOJTAY MÁRIÁnak és BALASSA ZSÓFIÁnak, akik a könyvet gondozták. Hálával tartozom az anyagi háttér biztosításáért a SZÉCHENYI PROFESSZORI ÖSZTÖNDÍJnak, valamint a **T 023186** és **T 029525** számú OTKA-nak. Végül, de nem utolsósorban hálával tartozom feleségemnek, HAY ERZSÉBETnek, az erkölcsi háttér biztosításáért, türelméért és a könyv átolvasásában nyújtott segítségéért.

Budapesten a 2000. évben

Fried Ervin

I. rész

ELEMI ALGEBRA

ELSŐ FEJEZET

KOMPLEX SZÁMOK

1. A természetes számoktól a valós számokig

A komplex számok vizsgálata előtt tekintsük át a valós számok alapvető algebrai tulajdonságait. A valós számokat — mint középiskolai tananyagot — tárgyalásaink során ismerteknek tételezzük fel. Ennek megfelelően a felsorolt algebrai tulajdonságokat sem fogjuk bizonyítani. (A későbbiek során ezekre bizonyos értelemben majd sor kerül.) A valós számoknak nagyon sok fontos tulajdonsága van; itt azonban csak olyanokra lesz szükségünk, amelyekben csupán e számok közötti műveletek és relációk szerepelnek. Ezeket nevezzük algebrai tulajdonságoknak.

Tárgyalni fogjuk az összeadás, kivonás, szorzás és osztás, valamint a hatványozás, gyökvonás és logaritmálás alapvető azonosságait; továbbá az oszthatósági és rendezési relációkat.

Bármely két a és b valós számnak létezik az $a + b$ *összege* és az ab ($a \cdot b$, vagy más jelöléssel $a \times b$) *szorzata*. a és b az összeg *tagjai*, illetve a szorzat *tényezői*. Mindkét műveletre, az *összeadásra* és a *szorzásra* érvényes a *kommutativitás (felcserélhetőség)* és az *asszociativitás (társíthatóság)*; azaz bármely a, b, c valós számokra:

$$a + b = b + a, \quad ab = ba, \qquad (a + b) + c = a + (b + c), \quad (ab)c = a(bc).$$

A szorzás az összeadásra nézve *disztributív (szétosztó)*, azaz $c(a+b) = ca+cb$, tetszőleges a, b, c valós számok esetében. Ebből következik az $(a+b)(c+d) = ac+ad+bc+bd$, speciálisan az $(a + b)(a + b) = aa + ab + ab + bb$ összefüggés.

Ezeket a műveleteket *direkt műveleteknek* is szokták nevezni.

Az összeg és az egyik tag ismeretében egyértelműen meghatározható a másik tag, ennek a meghatározását *kivonásnak* nevezzük. Ha $a + b = c$, akkor a $b = c - a$ jelölést használjuk, c a *kisebbítendő*, a a *kivonandó* és b a *különbség*. Bármely a valós számra a $0 = a - a$ szám ugyanaz, ezt *nullának* nevezik. 0 azzal jellemezhető, hogy tetszőleges b valós szám esetén $0 + b = b$. A $-a = 0 - a$ szám csak a-tól függ, ez az a *ellentettje* (vagy *negatívja*, vagy *additív inverze*). Érvényesek az

$$(a+b)-c = a+(b-c), \ (a-b)+c = a-(b-c), \ (a-b)-c = a-(b+c), \ a+(-b) = a-b$$

összefüggések. A kivonást nem kell új műveletnek tekinteni, mert az összeadással meghatározható. A kivonást *inverz műveletnek* is szokták nevezni.

A disztributivitást felhasználva kapjuk, hogy $(a-b)c = ac - bc$, $(a+b)(a-b) = aa - bb$; továbbá $(-a)b = a(-b) = -ab$, $(-a)(-b) = ab$, valamint $0a = 0$. Ez utóbbi tulajdonsággal egyedül a 0 rendelkezik.

Ugyancsak inverz művelet az osztás, amikor a szorzat és az egyik tényező ismeretében keressük a másikat. Az osztás nem mindig végezhető el:

0-val nem lehet osztani!

Ha ugyanis létezne $\frac{a}{0}$, akkor $a = 0\left(\frac{a}{0}\right) = 0$ volna, bármely a valós számra.

Ha $c = ab$, akkor $b = \frac{c}{a}$ (vagy $b = c/a$); itt c az *osztandó*, a az *osztó* és b a *hányados*. $a \neq 0$ esetén $1 = \frac{a}{a}$ mindig ugyanaz, 1 neve *egy*; és jellemezhető azzal, hogy bármely b valós számra $1b = b$ igaz. Ha $a \neq 0$, akkor $\frac{1}{a}$ az a *reciproka* vagy *multiplikatív inverze*. Az osztás, valamint az összeadás és a kivonás között $c \neq 0$ esetén érvényesek az alábbi kapcsolatok:

$$\frac{a+b}{c} = \frac{a}{c} + \frac{b}{c}, \quad \frac{a-b}{c} = \frac{a}{c} - \frac{b}{c}, \quad \frac{-a}{c} = \frac{a}{-c} = -\frac{a}{c}, \quad \frac{-a}{-c} = \frac{a}{c}.$$

Ezek után speciális (ismert) számköröket fogunk nézni.

A természetes számok. Az emberekben eredendően „természetesen” kialakult számfogalom. Ezek azok a számok, amelyeket az 1-ből számlálással nyerhetünk: $1, 2, 3, 4, \ldots$ soha abba nem hagyva a számlálást és mindig újabb és újabb számokat nyerve. Ezt az alábbi módon fogalmazhatjuk meg pontosabban:

1. 1 természetes szám.
2. Minden n természetes számnak van egy n' rákövetkezője.
3. $n' \neq 1$.
4. Ha $n' = k'$, akkor $n = k$.

Ezekkel még nem írtuk le teljesen a természetes számokat, mert a természetes számoknak alapvető tulajdonsága a *teljes indukció*. Ez azt mondja ki, hogy:

Ha

1. *az* 1 *számnak megvan egy* T *tulajdonsága és*
2. *valahányszor egy természetes számnak megvan* e *tulajdonsága, akkor a rákövetkezőnek is megvan;*

úgy minden természetes szám rendelkezik e *tulajdonsággal.*

A teljes indukció segítségével *definiálhatjuk* az összeadást és a szorzást, valamint a *kisebb* relációt is.

Megjegyzések

1. Noha 0 sem történelmileg, sem „érzelmileg” nem természetes szám, matematikai szempontból sokszor hasznos annak tekinteni. Ez különösen akkor van így, ha egy teljes indukciós bizonyításnál a két lépés bizonyítása lényegében ugyanúgy történhet, míg az állítás a 0 esetére szinte bizonyítást sem igényel.

2. A teljes indukcióval való definiálás az valójában nem bizonyítás, de ez is megtehető. Ebben az esetben *rekurzióról* beszélünk.

3. Nem definiáltuk a „tulajdonság”-ot. Ilyenképpen szinte minden értelmetlen állítás bizonyítható volna. Valójában csak olyan tulajdonságokat engedhetünk meg, amelyeket „logikai formulával” lehet megadni. Például ilyen az, hogy bármely számot a rákövetkezővel szorozva páros számot kapunk.

4. Miután „tudjuk”, mik a természetes számok, ezért nem definiálhatjuk őket, mert csak úgy lehetne definiálni, hogy valami sokkal bonyolultabbat használunk fel. Ezért a fentiekben csupán azt fogalmaztuk meg, hogy a természetes számoknak melyek az alaptulajdonságaik. Ha ebben egyetértünk, akkor ugyanazt a matematikát „űzzük”. A fenti *axiómarendszert* bevezetőjük nevéről *Peano-axiómáknak* nevezzük. □

A természetes számok körében mindig elvégezhető az összeadás és a szorzás, de általában sem a kivonás, sem az osztás nem végezhető el. A természetes számok *halmazát* $\mathbb{N}$-nel fogjuk jelölni. Azokat az 1-től különböző természetes számokat, amelyek felírhatók két 1-től különböző természetes szám szorzataként, *összetett számoknak* nevezzük, amelyek nem írhatók így fel, azoknak a neve *prímszám*. A *számelmélet alaptétele* kimondja, hogy minden összetett szám egyértelműen (azaz a tényezők sorrendjétől eltekintve) felbontható prímszámok szorzatára. (Ha „egytényezős” szorzatot is megengedünk, akkor csak az 1-et kell kizárnunk.)

Az egész számok. Noha történetileg a pozitív racionális, sőt az irracionális számokat is korábban ismerték, egyszerűbb előbb az egész számokat tárgyalni. Ezek a számok a természetes számokból úgy nyerhetők, hogy a fenti műveleteken kívül a kivonást is megengedjük. Az így kapott „új” számok tehát $0, -1, -2, -3, -4, \ldots$; egy új szám a 0, és minden természetes számhoz „ugyanaz”, de egy $-$ jelet téve eléje. Könnyen (de hosszadalmasan) belátható, hogy a műveleteket a „megszokott” módon értelmezve, azokra a már tárgyalt összefüggések igazak. Az egész számok halmazát $\mathbb{Z}$-vel fogjuk jelölni; ez a halmaz az összeadáson és szorzáson kívül még a kivonásra is zárt (azaz ezek a műveletek sem vezetnek ki e számkörből). Ha az egész számok körében csak az összeadást és a kivonást nézzük, akkor erre a $\mathbb{Z}^+$ jelölést fogjuk használni.

Érdemes megtanulni a következő elnevezéseket:

Ha egy számhalmaz az összeadásra és a kivonásra is *zárt* (vagyis ezek a műveletek nem vezetnek ki a halmazból), akkor azt mondjuk, hogy e számhalmaz az *összeadásra nézve csoport*. Ugyanígy, ha egy számhalmaz a szorzásra és az osztásra zárt, akkor ez a *szorzásra nézve csoport*. Ha csak az összeadásra (szorzásra) való zártságot tudjuk, akkor az összeadásra (szorzásra) vonatkozó *félcsoportról* beszélünk.

$\mathbb{N}$ az összeadásra és a szorzásra nézve is félcsoport. Ha egy számhalmaz az összeadásra nézve csoport és a szorzásra nézve félcsoport, akkor ez az *összeadásra és a szorzásra nézve gyűrű*. Ilyen például $\mathbb{Z}$.

$\mathbb{Z}$-ben két relációt értelmezünk, az egyik az *oszthatóság*, a másik a *rendezés*.

Az $a \mid b$ reláció azt fejezi ki, hogy a a b-nek *osztója*, illetve b az a-nak többszöröse, ami azt jelenti, hogy létezik egy olyan c *egész* szám, amire $b = ac$. E relációnak a következő alapvető tulajdonságai vannak:

Az $a \mid b$, $a \mid (-b)$, $(-a) \mid b$, $(-a) \mid (-b)$ feltételek ekvivalensek.

Az oszthatóság *reflexív* ($a \mid a$), *antiszimmetrikus* (ha $a \mid b$ és $b \mid a$, akkor vagy $a = b$, vagy $a = -b$) és *tranzitív* (ha $a \mid b$ és $b \mid c$, akkor $a \mid c$).

Ha $a \mid b$ és $a \mid c$, akkor $a \mid (b + c)$ és $a \mid (b - c)$; továbbá tetszőleges d egész szám esetén $a \mid (bd)$.

Az a egész szám pontosan akkor osztója minden egész számnak, ha $a = 1$ vagy $a = -1$. Egy a egész számnak pontosan akkor osztója minden egész szám, ha $a = 0$. (Noha $\frac{0}{0}$ értelmetlen, a $0 \mid 0$ reláció igaz.)

Az a és b egész számoknak létezik $d = (a, b)$ *legnagyobb közös osztójuk* és $c = [a, b]$ *legkisebb közös többszörösük*. Ezekre $d \mid a$, $d \mid b$, $a \mid c$, $b \mid c$ teljesül úgy, hogy az $u \mid a$, $u \mid b$, illetve $a \mid v$, $b \mid v$ feltételekből $u \mid d$, illetve $c \mid v$ következik. Ha feltesszük, hogy c is, d is vagy természetes szám, vagy 0, akkor ezek a számok egyértelműen meghatározottak. Ha $(a, b) = 1$, akkor *relatív prím* számokról beszélünk.

A másik reláció a *rendezés*, ezt a kivonással definiáljuk:

a *nagyobb*, mint b (jelben $a > b$), ha $a - b$ természetes szám. Ekkor azt is mondjuk, hogy b *kisebb*, mint a ($b < a$). Ha $a > 0$, akkor a *pozitív*, ha $a < 0$, akkor a *negatív*.

A rendezés *irreflexív* ($a > a$ soha sem teljesül), *antiszimmetrikus* ($a > b$ és $b > a$ egyszerre nem teljesülhet, és *tranzitív* (ha $a > b$ és $b > c$, akkor $a > c$). (Vigyázat! Az itt szereplő antiszimmetria nem egészen ugyanaz, mint az előző; ez azért van, mert itt az egyenlőséget is kizárjuk.)

A rendezés *teljes*, azaz bármely a és b számokra $a > b$, $a = b$ és $a < b$ közül pontosan az egyik igaz. A „hozzáadás” és a pozitív számmal való szorzás *monoton*, azaz $a > b$ és tetszőleges c, továbbá pozitív d mellett $a+c > b+c$ és $ad > bd$. (Ha $d = 0$, akkor $ad = bd$, ha $d < 0$, akkor $ad < bd$ következik.)

Használatos ezzel kapcsolatban még a *nagyobb-egyenlő*, illetve *kisebb-egyenlő* ($a \geq b$, illetve $b \leq a$), ami azt jelenti, hogy vagy $a > b$, vagy $a = b$. Ennek a relációnak a tulajdonságai az előzőéből leolvashatók. Ha $a \geq b$, akkor ezek *maximuma*, illetve *minimuma*: $\max(a, b) = a$, illetve $\min(a, b) = b$.

Az a és $-a$ közül csak egyik lehet pozitív. Ezt az a abszolút értékének nevezzük és $|a|$-kel jelöljük. Külön definíció az, hogy $|0| = 0$. Az abszolút értékre az alábbiak teljesülnek:

$$|ab| = |a| \cdot |b|, \qquad |a + b| \leq |a| + |b|, \qquad |a - b| \geq \big||a| - |b|\big|.$$

Az abszolút érték segítségével megfogalmazható a *maradékos osztás*:

Bármely a egész és bármely 0-tól különböző b egész számokhoz léteznek olyan q és r egész számok, amelyekre:

$$a = bq + r \qquad \text{és} \qquad |r| < |b|. \qquad \text{(Negatív } r \text{ is megengedett.)}$$

A maradékos osztás biztosítja, hogy elvégezhető az úgynevezett *euklideszi algoritmus*, amelynek segítségével előállítható két szám legnagyobb közös osztója és bizonyítható a számelmélet alaptétele.

A racionális számok. Ezeket a számokat úgy kapjuk, hogy még a nemnulla egész számmal való osztást is megengedjük. A racionális számok tehát $\frac{a}{b}$ alakú *törtek*. Itt a a tört *számlálója*, b a tört *nevezője*. Az őket elválasztó vízszintes vonal neve *törtvonal*. Különböző törtek is jelölhetik ugyanazt a racionális számot: $\frac{a}{b} = \frac{c}{d}$ pontosan akkor, ha $ad = bc$. Ezek körében elvégezhető az összeadás, kivonás, szorzás és a nemnulla racionális számmal való osztás (amit : jelöl):

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}, \quad \frac{a}{b} - \frac{c}{d} = \frac{ad - bc}{bd}, \quad \frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}, \quad \frac{a}{b} : \frac{c}{d} = \frac{ad}{bc},$$

amennyiben a fellépő nevezők egyike sem 0. Itt is érvényesek az egész számokra látott azonosságok. A racionális számok körében elvégezhető az osztás is (persze 0-val nem!). Ilyen esetben a számgyűrűt *számtestnek* nevezzük. A racionális számtestet $\mathbb{Q}$-val fogjuk jelölni. Ha a racionális számokat mint additív csoportot nézzük, akkor erre a $\mathbb{Q}^+$ jelölést fogjuk használni. Vigyázat! A matematikai analízisben $\mathbb{Q}^+$ a pozitív racionális számokat jelöli.

A racionális számok körében is beszélhetünk rendezésről; erre is hasonlóak érvényesek, mint az egészek körében. Jó tudni, hogy $\frac{a}{b} > 0$ akkor és csak akkor igaz, ha $ab > 0$. Az egész számok körében bármely egész számnál volt „közvetlenül” kisebb is és nagyobb is. A racionális számoknál ez nincs így, bármely két különböző racionális szám között van újabb: Ha $r < s$, akkor $r < \frac{r+s}{2} < s$.

Érdemes megjegyezni, hogy a pozitív racionális számok a szorzásra nézve csoportot alkotnak.

Megjegyzések

1. A racionális szó nem azt jelenti, hogy ésszerű, hanem azt, hogy viszonyszám. A régi görögök csak a „mérőrúd” egész számú többszöröseinek a mértékét tekintették számnak; a racionális számok csak úgy jelentkeztek náluk, mint két ilyen távolságnak az aránya.

2. Érdemes észrevenni, hogy csak a természetes számok esetében soroltunk fel axiómákat, a többi számfajtát ezekből építettük fel. A Peano-axiómarendszerről senki sem tudja bebizonyítani, hogy ellentmondásmentes. Ha az újabb, bővebb számfajtákat is axiómákkal definiálnánk, akkor egyre kellemetlenebb helyzetbe jutnánk. Ezen úgy segítünk, hogy „tudva”, mik azok az egészek, illetve racionálisak, ezekre a természetes számok segítségével egy „modell”-t építünk fel. Ha tehát a természetes számok körében nincs ellentmondás, akkor ezekben a bővebb számkörökben sincs.

Általában azokat az axiómarendszereket fogadjuk el ellentmondásmenteseknek, amelyekre létezik véges modell.

3. A törtszámok között nincsenek ott az egész számok, mert „más az alakjuk”. Ezzel szemben vannak e számkörben olyan számok, amelyeket úgy tekinthetünk, mintha ők egész számok lennének. Nevezetesen az $\frac{a}{1}$ helyett azt képzelhetjük, hogy az a egész szám áll. A velük való műveletek pontosan úgy végezhetők, mint az egészekkel. □

A valós számok. A valós számokat nem származtathatjuk a racionális számokból „algebrai módon”. Ezek szemléletesen a következőképpen kaphatók. A rendezés tulajdonságai alapján a racionális számokat úgy képzelhetjük el, hogy ezek egy egyenesen, a *számegyenesen* helyezkednek el. Közöttük azonban „kimaradnak” pontok. Ezt a tulajdonságot pontosabban a következőképpen fejezhetjük ki: Legyen P és Q a racionális számok két olyan részhalmaza, hogy bármely racionális szám e két részhalmaz közül pontosan az egyiknek eleme; továbbá, ha p egy P-beli és q egy Q-beli szám, akkor $p < q$. Ezen felül még azt is feltesszük, hogy P-ben nincs legnagyobb racionális szám. (Ha m ilyen volna, akkor P helyett vegyük azt a P_1 halmazt, amelyet az m elhagyásával nyerünk, míg Q helyett azt a Q_1 halmazt, amelyet úgy kapunk, hogy Q-hoz hozzávesszük m-et is. P_1 és Q_1 is eleget tesznek a kirótt feltételeknek, de P_1-ben nincs legnagyobb szám, hiszen bármely két különböző racionális szám között van tőlük különböző.) Minden ilyen úgynevezett *szelet* meghatároz pontosan egy valós számot, amely minden P-beli számnál nagyobb, de egyik Q-belinél sem. Ez a valós szám pontosan akkor „tekinthető” racionálisnak, ha Q-nak van legkisebb eleme; méghozzá ekkor pontosan ezt a racionális számot jellemeztük. Ezek alapján a valós számokra is értelmezhető a rendezés, amire a már szerepelt tulajdonságok teljesülnek. A valós számokról már említettük, hogy számtestet alkotnak. Ezt a számtestet $\mathbb{R}$ fogja jelölni. Ha a valós számok additív csoportját nézzük, akkor az $\mathbb{R}^+$ jelölést fogjuk használni. Itt is vigyázni kell, mert analízisben ez a pozitív valós számok halmazát jelöli. Itt is érvényesek a már tárgyalt műveleti azonosságok, valamint a rendezésnek és az abszolút értéknek a műveletekkel kapcsolatos tulajdonságai. (Valójában éppen ez az elv teszi lehetővé az összeadás és a szorzás definícióját.)

1-nél nagyobb n természetes számmal való szorzás megegyezik a másik tényező n példányban vett összegével: $n \cdot a = \overbrace{a + \cdots + a}^{n\text{-szer}}$. Külön értelmezendő az $1 \cdot a = a$ és a $0 \cdot a = 0$. Negatív egész számmal való szorzás is értelmezhető; ha n természetes szám, akkor $(-n) \cdot a = n \cdot (-a)$. Ennek analógiájára definiálható a *hatványozás*.

Ha $n > 1$ természetes szám, akkor legyen $a^n = \overbrace{a \cdot \ldots \cdot a}^{n\text{-szer}}$. Legyen $a^1 = a$ és $a^0 = 1$.

Ha n természetes szám, akkor legyen $a^{-n} = \dfrac{1}{a^n}$ (feltéve, hogy $a \neq 0$).

Igen fontos speciális eset az $n = 2$. Az a^2 számot az a szám *négyzetének* nevezzük. Egyedül a 0 négyzete 0, *minden más valós szám négyzete pozitív*. Fontos összefüggés, hogy $(-a)^2 = a^2$.

Az $n = 3$ esetben is szokásos külön elnevezés: a^3 az a szám *köbe*. Könnyen belátható, hogy különböző számok köbe is különböző, pozitívaké pozitív, negatívaké negatív.

Az $a \mapsto a^2$ megfeleltetés neve *négyzetre emelés*; az $a \mapsto a^3$ megfeleltetésé *köbre emelés*.

Ha $a^b = c$, akkor a neve *alap*, b neve *kitevő* és c neve *hatvány*. Az eddigiekben a kitevő egész szám volt; más kitevő esetén mindig feltesszük, hogy az alap pozitív szám.

Ha n természetes szám, akkor az $a^n = b$ kapcsolatot $a = \sqrt[n]{b}$ is jelöli. Az a pozitivitása következtében itt a egyértelműen meghatározott. E jelölésnél *gyökvonásról* beszélünk; b a gyök *alapja*, n a *gyökkitevő* és a a *gyök*.

Az $n = 1$ esetben nem szoktak gyökvonásról beszélni. Az $n = 2$ esetben a gyökkitevőt elhagyva $a = \sqrt[2]{b}$ helyett $\sqrt{b}$ szerepel. Ebben az esetben *négyzetgyökvonásról* beszélünk. Mint a négyzetre emelésnél láttuk, valós szám négyzete nem lehet negatív; így negatív valós számnak nincs négyzetgyöke (a valós számok körében).

Legyen $r = \dfrac{p}{q}$ tetszőleges racionális szám, ahol feltehető, hogy $q > 0$. Definíció szerint legyen $a^r = \sqrt[q]{a^p}$. Az alap pozitivitásából következik, hogy a racionális hatvány egyértelműen meghatározott pozitív szám. Pozitív alap esetén a racionális kitevőjű hatványra az alábbiak teljesülnek:

$$a^{r+s} = a^r \cdot a^s, \qquad a^{rs} = (a^r)^s, \qquad (ab)^r = a^r \cdot b^r.$$

Ha $a < b$ és $r > 0$, akkor $a^r < b^r$; ha $r < s$ és $a > 1$, akkor $a^r < a^s$. Ezeket az összefüggéseket a hatványozás *monotonitásának* nevezzük. Ez a tulajdonság és a valós számoknak a racionális számokkal való leírása lehetőséget ad arra, hogy a valós kitevőjű a^b hatványt is definiálhassuk. Erre is érvényesek a már ismertetett összefüggések. Ez pozitív alapra speciális esetként tartalmazza a gyökvonást. Mivel a hatványozás nem kommutatív, ezért egy másik inverz művelete is van, a *logaritmálás*, amikor az alapból és a hatványból határozzuk meg a kitevőt. Az $a^b = c$ esetben a következő elnevezések használatosak: a az *alap*, c a *logaritmálandó* vagy *numerus* és b a *logaritmus*. Ebben az esetben a $\log_a c = b$ jelölés használatos.

Halmaz, reláció, függvény. Ezek a fogalmak nem tartoznak ugyan a számfogalom körébe, de szerepelnek a középiskolai tananyagban, és a továbbiakban itt is szükség lesz rájuk. A halmazokról van szemléletes képünk. A halmazokat még annyira sem írjuk itt le, mint amennyire a természetes számokkal tettük a Peano-axiómáknál. Ennek az az oka, hogy a természetes szám fogalma és azoknak számlálás útján való nyerése valóban természetes; míg a halmazok „absztrakt” tulajdonságai sokkal nehezebben beláthatóak.

A halmazokat általában latin nagybetűkkel fogjuk jelölni. A halmazoknak „eredendő” tulajdonsága, hogy elemeik vannak. Ezeket az elemeket általában latin kisbetűkkel jelöljük. Azt, hogy x *eleme* az A halmaznak, úgy fogjuk jelölni, hogy $x \in A$. Van egyetlen halmaz, amelynek egyetlen eleme sincs; ezt úgy nevezik, hogy *üres halmaz*; ezt $\emptyset$ jelöli. Azt mondjuk, hogy B *részhalmaza* A-nak ($B \subseteq A$), ha $b \in B$ esetén $b \in A$ is teljesül. Az A és B halmazok *direkt szorzatán* azt az $A \times B$ halmazt értjük, amelynek elemei azok az (a, b) párok, amelyekre $a \in A$ és $b \in B$. Több halmaznak is képezhető a direkt szorzata: $A \times B \times C$ az (a, b, c) hármasokból áll, ahol $a \in A, b \in B, c \in C$. Megemlítjük, hogy ezt sokszor ugyanannak fogjuk tekinteni, mint az $A \times (B \times C)$ vagy az $(A \times B) \times C$ halmazt; noha formálisan az előbbinek az elemei az $(a, (b, c))$ elemek, az utóbbinak pedig az $((a, b), c)$ alakú elemek.

Ha a halmazt elemei felsorolásával adjuk meg, akkor a felsorolt elemeket kapcsos zárójelek közé tesszük. Például az $\{1, 2, 5\}$ halmaz elemei a felsorolt három szám, míg az

$\{1, 2, 5, a, b\}$ halmazé ezeken kívül még az a és a b betű is. A felsorolásnál mindegy, hogy az elemeket milyen sorrendben írjuk, a halmaz nem változik. A halmaz elemei különbözőek, így az $\{1, 2, 5, 2, 2, 1\}$ halmaznak is csak három eleme van.

Ha a halmazt úgy akarjuk megadni, hogy egy halmaz elemeiből valamilyen „utasítással" választunk ki elemeket, akkor is kapcsos zárójelet használunk, de közöttük húzunk egy függőleges vonalat. Ettől balra szerepelnek az elemek és az, hogy honnan választjuk ki őket; míg jobbra az, hogy milyen módon történik a kiválasztás. Például az $A = \{i \in \in \mathbb{N} \mid 3 < i \leq 7\}$ azt jelenti, hogy a természetes számok közül azokat tekintjük, amelyek 3-nál nagyobbak, de 7-nél nem. Ez a halmaz tehát a $\{4, 5, 6, 7\}$.

Az A halmazon értelmezett *reláció* egy „kapcsolat" az A elemei között. Azt, hogy egy ϱ reláció fennáll az a és b elemek között, általában úgy jelöljük, hogy $a\varrho b$ (mint például $a < b$). Használatos még a $\varrho(a, b)$ jelölés is. Mivel itt két elem szerepel, ezért ilyenkor *kétváltozós relációról* beszélünk. Léteznek még *többváltozós relációk* és *egyváltozós reláció* is.

Ugyancsak nem magyarázzuk, hogy mi a *függvény* vagy *leképezés*. Ha az f függvény az A halmazt képezi le a B halmazra, akkor ezt $f : A \to B$ vagy $A \xrightarrow{f} B$ fogja jelölni. Azt mondjuk, hogy $A = D(f)$ az f *értelmezési tartománya* és $B = R(f)$ az f *értékkészlete*. (Általában csak az $f(a)$ alakú elemek halmazát szokták értékkészletnek nevezni.) Ha f az A-beli a elemet a B-beli b elemre képezi le, ezt $b = f(a)$ vagy $f : a \mapsto b$ jelöli (figyeljük meg, hogy itt a nyílnak „talpa" van). (Néha a b elem kiírása nélkül csak $a \mapsto f(a)$ szerepel.)

Ha B minden eleme $f(a)$ alakú, akkor azt mondjuk, hogy $f : A \to B$ *szürjektív*. Ha különböző A-beli elemek képe is különböző, azaz minden $b \in B$ elemhez legfeljebb egy olyan $a \in A$ található, amelyre $b = f(a)$, akkor *injektív* függvényről beszélünk. Ha mindkét feltétel teljesül, akkor a függvény *bijektív*. Bijektív függvényre igen fontos példa egy-egy halmaz *identitása*, az a függvény, amely a szóban forgó halmaz minden elemének önmagát felelteti meg. Természetesen az identitás(függvény) minden halmaznál más. Az A halmaz identitását 1_A fogja jelölni (erre tehát $D(1_A) = R(1_A)$ és ha $a \in A$, akkor $1_A : a \mapsto a$).

A függvények körében nagyon fontos művelet a *kompozíció*: Ha $f : A \to B$ és $g : B \to C$, akkor a $g \circ f$, vagy röviden $gf : A \to C$ függvény definíció szerint legyen az $a \mapsto g(f(a))$. Könnyen látható, hogy például a fenti f függvényre $f \circ 1_A = 1_B \circ f = f$.

Az identitások segítségével könnyen jellemezhetők a szereplő különféle függvényfajták. Legyen $f : A \to B$. Az f függvény pontosan akkor injektív, ha van olyan $g : B \to A$ függvény, amelyre $g \circ f = 1_A$, pontosan akkor szürjektív, ha van olyan $g : B \to A$ függvény, amelyre $f \circ g = 1_B$, és pontosan akkor bijektív, ha van olyan $g : B \to A$ függvény, amely mindkét feltételt kielégíti. Az első esetben g szürjektív, a második esetben injektív, a harmadik esetben pedig bijektív lesz. Az első két esetben a g függvény nem feltétlenül egyértelmű (csak ha f bijektív); a harmadik esetben viszont csak egy ilyen g függvény létezik. Ekkor ezt a függvényt $g = f^{-1}$ jelölheti és azt mondjuk, hogy g az f *inverz függvénye*.

Az algebrában alapvető jelentőségűek azok a leképezések, amelyek *művelettartók*. Ilyenekkel már találkoztunk is: Művelettartó az a leképezés, amely az a egész számnak

megfelelteti az $\frac{a}{1}$ törtet. Ugyancsak művelettartó leképezést nyertünk, amikor az r racionális számnak azt a P, Q részhalmazpárt (tehát valós számot) feleltettük meg, amelynél r a Q-nak a legkisebb eleme. (Gondoljuk meg, miképpen adjuk össze a valós számoknál említett részhalmazpárokat.) Ezek a leképezések teszik lehetővé, hogy az újabb számkörben „felfedezhessük" a régit.

A művelettartó leképezéseket *homomorfizmusoknak* nevezik. A függvények tulajdonságának megfelelően beszélünk *injektív homomorfizmusról*, illetve *szürjektív homomorfizmusról*. Fontossága miatt a bijektív homomorfizmus külön nevet kapott, ezt *izomorfizmusnak* hívjuk. Könnyen belátható, hogy ha $f : A \to B$ izomorfizmus, akkor $f^{-1} : B \to A$ is az.

Megjegyzések

1. A relációkat tekinthetjük úgy, mint az $A \times A$, vagy általánosabban, mint az $A \times B$ részhalmazait; nevezetesen a ϱ relációval együtt tekinthetjük azokat az $(a, b) \in A \times B$ párokat, amelyekre $a \varrho b$ teljesül. Mivel „ennél több" egyetlen relációra sem mondható, ezért relációnak nevezhetjük az $A \times A$ — vagy általában tetszőleges direkt szorzat — részhalmazait.

2. A függvényeket viszont értelmezhetjük úgy, mint speciális relációkat. Egy $f : A \to B$ függvényt akkor „ismerünk", ha ismerjük az összes $(a, f(a)) \in A \times B$ elemet. Világos, hogy ez egy φ reláció, amely azzal a tulajdonsággal rendelkezik, hogy ha (a, b_1) és (a, b_2) mindegyike a „relációhoz tartozik", akkor $b_1 = b_2$.

3. Érdemes észrevenni, hogy ha az $f : A \to B$ és $g : B \to A$ függvényekre $g \circ f = 1_A$, akkor f biztosan injektív és g biztosan szürjektív. Ebben az esetben azt mondjuk, hogy g az f *balinverze* és f a g *jobbinverze*. Ha még $f \circ g = 1_B$ is teljesül, akkor mindkét függvény bijektív; egymás inverzei. □

Szumma és produktum. (Noha középiskolában nem kötelező anyag, mégis szükségünk lesz két „rövidítésre".)

Legyen $I = \{i \in \mathbb{N} \mid k \leq i \leq n\}$ és tegyük fel, hogy adott egy $f : I \to A$ függvény. Ilyen esetben $f(i)$ helyett használatos az a_i jelölés; az i neve *index* és I egy *indexhalmaz*.

k-tól és n-től függően a következőképpen értelmezzük az

$$S = \sum_{i=k}^{n} a_i, \qquad \text{illetve} \qquad P = \prod_{i=k}^{n} a_i$$

jeleket:

1. Ha $k < n$: $S = a_k + \ldots + a_n$ és $P = a_k \cdot \ldots \cdot a_n$ ($n - k + 1$ tag, illetve tényező).
2. Ha $k = n$: $S = P = a_k$.
3. Ha $k = n + 1$: $S = 0$ és $P = 1$.
4. Ha $k > n + 1$: $S = -\left(\sum_{i=n+1}^{k-1} a_i\right)$, illetve $P = \left(\prod_{i=n+1}^{k-1} a_i\right)^{-1}$.

Az S, illetve P jeleket a következőképpen olvassák: szumma i egyenlő k-tól n-ig a_i, illetve produktum i egyenlő k-tól n-ig a_i. A fenti definícióval érvényes a $\sum_{i=k}^{n} a_i = \sum_{i=k}^{r} a_i + \sum_{i=r+1}^{n} a_i$ összefüggés, illetve ennek a produktumra vonatkozó analogonja.

Ha az $\{a_i \mid i \in \mathbb{N}\}$ számok közül csak véges sok különbözik 0-tól (illetve 1-től), akkor a megfelelő végtelen összeget, illetve szorzatot is értelmezhetjük: csak a 0-tól (illetve 1-től) különbözőket adjuk (illetve szorozzuk) össze.

Ha a k és n „határok" az adatokból világosak, akkor nem írjuk ki őket. Ugyancsak nem írjuk ki az indexeket sem, ha azok elhagyása nem okoz zavart.

A produktumnak igen fontos speciális esete a következő: $n! = \prod_{i=1}^{n} i$ (olv.: *n faktoriális*). A definícióból következik, hogy $0! = 1! = 1$; míg $n > 1$ esetén $n!$ az n-ig terjedő természetes számok szorzata.

Műveletek maradékokkal. Végezetül néhány példát adunk olyan halmazokra, amelyeknek az elemei nem számok, de a műveletek természetes módon definiálhatók rájuk. Továbbá az is igaz, hogy ezekre a műveletekre teljesülnek a számokra megismert műveleti szabályok. (De nem értelmezhetők e halmazon a tárgyalt relációk.)

Tekintsünk egy rögzített, 1-nél nagyobb m természetes számot. A vizsgált halmaz elemei az egész számok részhalmazai lesznek. Két egész szám akkor tartozzék ugyanabba a részhalmazba, ha a különbségük osztható m-mel. Az oszthatóság tulajdonságai alapján ekkor minden szám pontosan egy ilyen halmazba esik, amelyeket modulo m vett *maradékosztályoknak* nevezünk. Így ezeket bármely elemük egyértelműen meghatározza; jelölje az i-t tartalmazó maradékosztályt $[i]$.

Az oszthatósági tulajdonságokból könnyen látható, hogy az $[i + j]$, illetve $[i \cdot j]$ maradékosztály nem az i, illetve j számoktól, hanem csupán az $[i]$ és $[j]$ maradékosztályoktól függ. Éppen ezért ezek tekinthetők az $[i]$ és $[j]$ maradékosztályok összegének, illetve szorzatának: $[i] + [j] = [i + j]$ és $[i] \cdot [j] = [i \cdot j]$. A műveleti azonosságok teljesülnek, és elvégezhető a kivonás: $[i] - [j] = [i - j]$. Ezeket a maradékosztályokat az adott műveletekre nézve *gyűrűnek*; pontosabban *modulo m vett maradékosztály-gyűrűnek* nevezzük. Ezt a gyűrűt $\mathbb{Z}_m$ jelöli. Ebben a gyűrűben pontosan akkor végezhető el az osztás, ha $m = p$ prímszám. Azt mondjuk, hogy a *modulo p vett maradékosztályok testet alkotnak*.

A $\mathbb{Q}$ vagy az $\mathbb{R}$ esetében a maradékosztályok szorzata problémát jelent, az összeadás és a kivonás viszont nem. Különösen fontos az az eset, amikor „modulo" 1 tekintjük e számokat, azaz két racionális számot akkor veszünk ugyanabba a „maradékosztály"-ba, ha különbségük egész szám.