Juhász Tibor

Diszkrét matematika

ÚJ SZÉCHENYI TERV

Eszterházy Károly Főiskola
Matematikai és Informatikai Intézet

Juhász Tibor

Diszkrét matematika

Eger, 2013

Bíráló:
???

Készült a TÁMOP-4.1.2.A/1-11/2011-0038 támogatásával.

Nemzeti Fejlesztési Ügynökség
www.ujszechenyiterv.gov.hu
06 40 638 638

MAGYARORSZÁG MEGÚJUL

A projekt az Európai Unió támogatásával, az Európai Szociális Alap társfinanszírozásával valósul meg.

Tartalomjegyzék

Előszó

Ez a jegyzet az Eszterházy Károly Főiskola Programtervező Informatikus hallgatói számára tartott Diszkrét matematika I. előadások könnyebb követhetőségét szolgálja. Az anyag felépítésekor figyelembe vettük, hogy a kurzus hallgatói már rendelkeznek felsőbb matematikai ismeretekkel, hiszen a megelőző félévben a Kalkulus I. keretein belül az alapvető halmazelméleti és függvénytani ismeretek elhangzanak, de a jegyzet nagy része stabil középiskolai ismeretek birtokában is követhető.

A matematika lényegében fogalomalkotásból és a fogalmak közötti logikai kapcsolatok felderítéséből áll. Itt amikor új fogalom értelmezése történik, magát a fogalmat *dőlt* betűvel írjuk. Ezek a definíciók a lehetőségekhez képest precízek. Az állítások megfogalmazására több esetben a környező szöveg részeként, de van amikor tételként kiemelve kerül sor. A matematikai állítások általában bizonyításra szorulnak, itt azonban – a célcsoport igényére és felkészültségére, valamint a rendelkezésre álló időkeretre való tekintettel – a bizonyításokat nem minden esetben közöljük.

A fejezetek végén lévő feladatok a tárgyalt anyag elmélyítésének mérését segítik: azt javasoljuk, hogy az olvasó addig ne tekintsen feldolgozottnak egy fejezetet, amíg az ott kitűzött feladatokkal gondjai vannak.

A jegyzet célja nem a matematika lehetséges informatikai alkalmazásainak bemutatása, csupán az ahhoz szükséges matematikai alapok a tárgyhoz tartozó részének biztosítása.

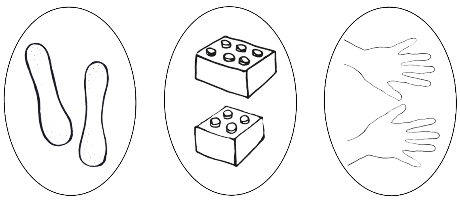
1. A természetes számoktól a valós számokig

„A számok a formalizálás és az eltávolítás eszközei. [...] Van például az asztalon öt alma, de az öt fogalma nincs az asztalon. Csak annak tudatában létezik, aki megszámolja az almákat."[*]

Életünk első matematikai élményei a számok megismeréséhez köthetők, már kisgyermekként is tudtunk velük valamilyen módon bánni. Ennek ellenére a számok fogalmának precíz matematikai megalapozása túlmutat az elemi matematika szintjén. A „kettő" jelentéséről mindenkinek stabil elképzelése van, de sokan bajban lennének, ha pontos meghatározást kellene rá adni. A számfogalom egzakt felépítését ezen jegyzet keretein belül sem tudjuk ígérni, csupán annak „hangulatát" kíséreljük meg e fejezetben érzékeltetni. Célunk a középiskolában megismert nevezetes számhalmazok számunkra fontos tulajdonságainak összefoglalása.

1.1. A természetes számok

Gyermekkorban a számok megismerése egyfajta elvonatkoztatás eredményeképpen történik: a körülöttünk lévő tárgyak számosságának állandóságát érzékelve a „kettő" fogalma 2 darab babapiskóta, két építőkocka, vagy éppen két kezünk közös tulajdonságaként körvonalazódik. Ezt a felismerést ragadja meg a természetes szá-



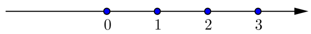
1.1. ábra. Mi a közös a három halmazban?

mok halmazelméletből származó definíciója, mely szerint *természetes számoknak* a véges halmazok számosságait tekintjük. Kalkulusból ismert, hogy az üres halmaz véges, ennek számosságát jelöljük 0-val. Az 1 annak a halmaznak a számosságát jelöli, melynek az üres halmaz az egyetlen eleme, a 2 pedig a $\{\emptyset, \{\emptyset\}\}$ halmaz számosságaként értelmezhető, és így tovább. A természetes számok halmaza tehát az

$$\mathbb{N} = \{0, 1, 2, 3, 4, \dots\}$$

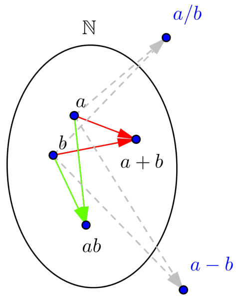
[*] Borbély Szilárd: Nincstelenek, Kaligram, 2013.

halmaz. Tudjuk, hogy a természetes számok körében korlátlanul elvégezhető az



1.2. ábra. Természetes számok a számegyenesen

összeadás és a szorzás. Ez alatt azt értjük, hogy bármely két természetes szám



1.3. ábra. Két természetes szám összege és szorzata is természetes szám, de nem mondható el ugyanez a természetes számok különbségeiről és hányadosairól

összeadható, illetve összeszorozható, és az eredmény is minden esetben egy jól meghatározott természetes szám lesz. A számolást nagymértékben könnyíti az a tény, hogy ezek a műveletek mindegyike az alábbi „jó” tulajdonságokkal rendelkezik.

1. A természetes számok halmazán értelmezett összeadás és szorzás is *kommutatív*, vagyis az eredmény független a tagok, illetve tényezők sorrendjétől. Formálisan:
$$a + b = b + a \quad \text{és} \quad ab = ba$$
teljesül minden a és b természetes számra.

2. Mindkét művelet *asszociatív*, azaz
$$(a + b) + c = a + (b + c) \quad \text{és} \quad (ab)c = a(bc)$$
teljesül bármely $a, b, c \in \mathbb{N}$ esetén. Ez a tulajdonság úgy értelmezhető, hogy ha három számot kell összeadnunk, mindegy, hogy először az első kettőt adjuk össze, majd az összeghez hozzáadjuk a harmadikat, vagy éppen a két második szám összegét adjuk hozzá az elsőhöz. Mivel a zárójelezés tetszőleges, a zárójeleket általában elhagyjuk.

Mint azt később látni fogjuk, a két tulajdonság együtt garantálja, hogy véges sok szám összege és szorzata független a tagok, illetve tényezők sorrendjétől és a zárójelezéstől. A következő tulajdonság a két művelet kapcsolatáról árulkodik.

3. A szorzás az összeadásra nézve *disztributív*, azaz bármely a, b, c természetes számok esetén igaz az
$$(a + b)c = ac + bc$$
egyenlőség.

Felhívjuk még a figyelmet a 0-nak az összeadáshoz, és az 1-nek a szorzáshoz fűződő viszonyára: a nullát bármelyik számhoz hozzáadva az a szám nem változik, továbbá bármelyik szám változatlan marad, ha azt eggyel szorozzuk.

Az összeadás segítségével a természetes számok között rendezés is értelmezhető: azt mondjuk, hogy $a \leqslant b$ (kiolvasva: a kisebb, vagy egyenlő, mint b), ha van olyan c természetes szám, hogy $a + c = b$. Továbbá, $a < b$ (a kisebb, mint b), ha $a \leqslant b$ de $a \neq b$. Gyakran ki fogjuk használni azt a tényt, hogy a természetes számok minden nemüres részhalmazának van legkisebb eleme.

1.1.1. Teljes indukció

Az is világos, hogy ha n egy természetes szám, akkor $n + 1$ is az. Sőt, ha H a természetes számok halmazának egy olyan részhalmaza, amely tartalmazza a 0-t, és amennyiben tartalmazza n-et, úgy tartalmazza $n + 1$-et is, akkor H szükségképpen az összes természetes számot tartalmazza. Ezen az állításon alapszik egy fontos bizonyítási módszer, a *teljes indukció*, amely természetes számokkal kapcsolatos állítások igazolására alkalmas, és a következő két lépésből áll:

1. Először azt bizonyítjuk az állítás igaz a nullára (vagy a legkisebb olyan természetes számra, melyre az állítás értelmes).

2. Utána belátjuk, hogy amennyiben az állítás érvényes valamely n természetes számra, akkor érvényes $n + 1$-re is. Ezt nevezzük indukciós lépésnek.

A két lépés együtt biztosítja, hogy az állítás minden természetes számra igaz: az első lépés szerint igaz nullára, de ekkor a második lépés szerint egyre is, majd újra a második lépést alkalmazva kettőre is, stb. Szemléletesen szólva, biztosan fel tud menni a lépcsőn az, akiről tudjuk, hogy fel tud állni a lépcső legelső fokára, és annak bármelyik fokáról fel tud lépni a következőre.

Példaként megmutatjuk, hogy

$$1^2 + 2^2 + 3^2 + \cdots + n^2 = \frac{n(n+1)(2n+1)}{6}$$

teljesül minden $n \geqslant 1$ természetes számra.

Először az $n = 1$ esetet kell ellenőriznünk, melyhez csupán behelyettesítésre van szükség:

$$1^2 = \frac{1 \cdot 2 \cdot 3}{6}$$

valóban igaz. Most feltesszük, hogy igaz az állítás valamely $k \geqslant 1$ természetes számra, azaz

$$1^2 + 2^2 + 3^2 + \cdots + k^2 = \frac{k(k+1)(2k+1)}{6}, \tag{1.1}$$

és ebből kellene bizonyítani, hogy $k+1$ esetén is igaz, vagyis

$$1^2 + 2^2 + 3^2 + \cdots + k^2 + (k+1)^2 = \frac{(k+1)((k+1)+1)(2(k+1)+1)}{6}. \tag{1.2}$$

Alkalmazva az (1.1) feltevést,

$$\begin{aligned} 1^2 + 2^2 + 3^2 + \cdots + k^2 + (k+1)^2 &= \frac{k(k+1)(2k+1)}{6} + (k+1)^2 = \\ &= \frac{k(k+1)(2k+1) + 6(k+1)^2}{6} = \\ &= \frac{(k+1)(k(2k+1) + 6(k+1)}{6} = \\ &= \frac{(k+1)(2k^2 + 7k + 6)}{6}. \end{aligned}$$

Könnyű ellenőrizni, hogy (1.2) jobb oldala is pont ugyanezzel egyenlő. A fent elmondottak szerint az állítás ezzel bizonyítva van. Még egyszer nyomatékosítjuk, hogy az (1.1) egyenlőség csupán feltevés, ha azt közvetlenül bizonyítani tudnánk, nem lett volna szükség a teljes indukcióra. Sőt, akár még azt is feltehettük volna, hogy az állítás nemcsak k-ra, hanem a nála kisebb természetes számokra is igaz. Itt most erre nem volt szükség, de van olyan, amikor az $n = k+1$ esetre csak így tudunk következtetni (lásd 1.2. tétel).

Most pedig bebizonyítjuk, hogy minden ló ugyanolyan színű. Ezt a lovak száma szerinti teljes indukcióval tesszük. Ha a világon csak egyetlen ló lenne, akkor az állítás nyilván igaz lenne. Most tegyük fel, hogy k darab ló esetén igaz az állítás, és tekintsünk egy $k+1$ lóból álló ménest. Számozzuk meg ebben a lovakat:

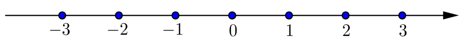
$1, 2, \ldots, k+1$. Az $1, 2, \ldots, k$ és $2, 3, \ldots, k+1$ sorszámú lovak egy-egy k lóból álló ménest alkotnak, így a feltevésünk szerint mindkét ménes lovai azonos színűek. Mivel a 2. ló tagja mindkét ménesnek, ezért mind a $k+1$ ló színe azonos.
Az állítás, melyet éppen most igazoltunk, nyilvánvalóan hamis. Ez az úgynevezett lóparadoxon nem a teljes indukciót hivatott támadni, csupán egy annak alkalmazása közben elkövethető hibára igyekszik felhívni a figyelmet. A hiba igen egyszerű: az indukciós lépésében alkalmazott gondolatmenet csak akkor helyes, ha k legalább 2, ugyanis csak ekkor lehet közös ló a két k tagú ménesben. Tehát az indukciós lépésünk megköveteli, hogy az $n = 1$ eseten túl az $n = 2$ esetet is külön kezeljük. Két tetszőleges lóról pedig senki nem mondhatja, hogy biztosan azonos színűek.

1.2. Egész számok

Aki már a jegyzetben előrelapozott, láthatta, hogy előbb-utóbb egyenleteket szeretnénk megoldani. A természetes számok körében azonban már az $x + 1 = 0$ egyenlet megoldása is gondot okoz, hiszen nincs olyan természetes szám, melyhez egyet hozzáadva nullát kaphatnánk, vagy ha úgy tetszik, a nullából nem tudunk kivonni egyet. A természetes számok halmazának bővítésére van tehát szükség. Ezt úgy tesszük meg, hogy a $-n$ szimbólumot, ahol n nullánál nagyobb természetes szám, is számnak tekintjük, és ezt az n negatívjának nevezzük. Az így kapott

$$\mathbb{Z} = \{\ldots, -4, -3, -2, -1, 0, 1, 2, 3, 4, \ldots\}$$

halmazt az *egész számok halmazának*, elemeit pedig *egész számoknak* hívjuk. A



1.4. ábra. Egész számok a számegyenesen

bővítés akkor lesz eredményes, ha a természetes számoknál megismert műveleteket is kiterjesztjük erre a bővebb halmazra. A kiterjesztés arra utal, hogy az „új” művelet a „régi” számokon a megszokott eredményt kellene, hogy produkálja. Azt, hogy ez sikerült, általános iskolában mindenki láthatta: a 2 és a 3 egész számok összege ugyanúgy 5 lesz, mintha természetes számokként adtuk volna össze őket. Sőt, az összeadás és a szorzás „jó” tulajdonságai, a kommutativitás és az asszociativitás is megmaradnak. A bővítés nyeresége abban áll, hogy minden x egész számhoz található olyan szintén egész szám (ezt hívjuk *x ellentettjének*), hogy a kettő összege éppen 0. Így elmondhatjuk, hogy az egész számok körében a kivonás is elvégezhető, a kivonás ugyanis nem más, mint az ellentett hozzáadása.

A rendezés is kiterjeszthető az egész számok halmazára: azt mondjuk, hogy $a \leqslant b$, ha $b - a$ természetes szám. Ha $0 < a$, akkor a-t *pozitív*, ha pedig $a < 0$, akkor a-t *negatív* egész számnak nevezzük.

Korábbi tanulmányainkból ismert, hogy az osztás az egész számok körében általában nem végezhető el. Ez alatt azt értjük, hogy vannak olyan egészek (pl. a 12 és az 5) melyek hányadosa nem egész szám. Viszont az osztásnak az a változata, melyben maradék képződését is megengedjük, az egész számokkal is elvégezhető.

1.1. Tétel (Maradékos osztás tétele)**.** *Bármely a és b ($b \neq 0$) egészek esetén egyértelműen léteznek olyan q és r egészek, amelyekre $a = bq + r$ teljesül úgy, hogy $0 \leqslant r < |b|$.*

A bizonyítás előtt megjegyezzük, hogy a tételben szereplő a-t osztandónak, a b-t osztónak, a q-t hányadosnak, az r-et pedig maradéknak nevezzük. A maradékra vonatkozó $0 \leqslant r < |b|$ feltétel az egyértelműség miatt szükséges, nélküle azt is joggal mondhatnánk, hogy „ha a 20-at osztjuk maradékosan 7-tel, akkor az így keletkező hányados 1, a maradék pedig 13".

Bizonyítás. Tekintsük az

$$\ldots,\ a-(-2)b,\ a-(-1)b,\ a,\ a-b,\ a-2b,\ \ldots,$$

azaz az $a - kb$ ($k \in \mathbb{Z}$) alakú egészeket. Ezek között biztosan van nemnegatív, nemnegatív egészek között pedig van legkisebb: legyen ez r. Ekkor $r = a - kb$ valamely k egész esetén; legyen $q = k$. Innen az $a = bq + r$ egyenlőség egyszerű átrendezéssel adódik. Megmutatjuk, hogy $0 \leqslant r < |b|$. Valóban, ha nem így volna, akkor

$$r > r - |b| = a - qb - |b| \geqslant 0$$

teljesülne, mely ha b negatív, akkor az $r > a - (q-1)b \geqslant 0$, ellenkező esetben pedig az $r > a - (q+1)b \geqslant 0$ egyenlőtlenséghez vezetne. Ez viszont ellentmond annak, hogy a fenti egészek között $a - qb$ volt a legkisebb nemnegatív.

Most tegyük fel, hogy q_1, q_2, r_1, r_2 olyan egészek, melyekre

$$a = bq_1 + r_1, \qquad 1 \leqslant r_1 < |b|,$$

és

$$a = bq_2 + r_2, \qquad 1 \leqslant r_2 < |b|$$

teljesülnek. Az első egyenlőségből a másodikat kivonva, átrendezés és b kiemelése után a

$$b(q_1 - q_2) = r_2 - r_1$$

egyenlőséghez jutunk. Vegyük mindkét oldal abszolút értékét (a bal oldalon lévő szorzatét tényezőnként):

$$|b||q_1 - q_2| = |r_2 - r_1|.$$

Az r_1 és r_2-re vonatkozó feltevés miatt az egyenlőség jobb oldala kisebb, mint $|b|$. A bal oldalra ugyanez csak akkor teljesülhet, ha $q_1 = q_2$. Ekkor viszont a bal oldal 0, így a jobb oldalnak is annak kell lenni, tehát $r_1 = r_2$, ami azt jelenti, hogy q és r egyértelműen meghatározott. □

Az 1.5. ábrán néhány példát láthatunk maradékos osztásra.

osztandó	osztó	hányados	maradék
20	7	2	6
20	-7	-2	6
-20	7	-3	1
-20	-7	3	1
0	7	0	0
7	0	-	-

1.5. ábra. Néhány példa maradékos osztásra

Megjegyezzük, hogy az r maradékra a $0 \leqslant r < |b|$ helyett más feltétel is adható úgy, hogy a maradékos osztás egyértelműsége nem sérül. A MAPLE rendszer például a maradékra az $|r| < |b|$ és $0 \leqslant a \ldots r$ feltételeket szabja. Ezzel az osztással hogyan alakul az 1.5 táblázat utolsó két oszlopa? Fennáll így is a hányados és a maradék egyértelműsége? A kérdések megválaszolását az olvasóra bízzuk.

Maradékos osztások sorozatát alkalmazzuk akkor is, amikor egy egész számot valamilyen más alapú számrendszerbe konvertálunk át.

1.2.1. Oszthatóság

Először az oszthatóság fogalmát tisztázzuk. Legyenek a és b egész számok. Azt, hogy a b *osztója az a-nak* (vagy másképpen: a osztható b-vel, vagy: a többszöröse b-nek), ha van olyan c szintén egész szám, hogy $a = bc$. Jelölésben: $a \mid b$.

Az alábbi állítások a definíció egyszerű következményei.

1. A nullának minden egész szám osztója.

2. A nulla csak önmagának osztója.

3. A -1 és 1 számok minden egész számnak osztói. Ezeket *egységeknek* nevezzük.

4. Ha $a \mid b$ és $b \mid a$, akkor $a = b$ vagy $a = -b$.

Az oszthatóság és az egész számokon értelmezett összeadás és szorzás között a következő kapcsolat áll fenn.

5. Ha $a \mid b$ és $a \mid c$, akkor $a \mid (b + c)$.

6. Ha $a \mid b$ és $c \mid d$, akkor $ac \mid bd$.

Példaként bebizonyítjuk az 5. állítást. Ha $a \mid b$ és $a \mid c$, akkor az oszthatóság definíciója szerint vannak olyan k és l egész számok, hogy $b = ak$ és $c = al$. Ekkor $b + c = ak + al = a(k + l)$, ahonnan, lévén $k + l$ egész, $a \mid (b + c)$ következik. A többi állítás is hasonlóan igazolható.

Most a legnagyobb közös osztó fogalmával folytatjuk. A d egész számot az a és a b egészek *közös osztójának* nevezzük, ha d az a-nak és a b-nek is osztója. Könnyű belátni, hogy ha $a \neq 0$ és $d \mid a$, akkor $|d| \leqslant |a|$, melyből az következik, hogy minden nullától különböző egésznek csak véges sok osztója lehet. Tehát ha a és b olyan egészek, melyek közül legalább az egyik nem nulla, akkor véges sok közös osztójuk van, így ezek között van egy legnagyobb. Ennek ellenére a legnagyobb közös osztó fogalmát másképp definiáljuk: az a és b *legnagyobb közös osztója* alatt a és b azon közös osztóját értjük, mely minden közös osztónak többszöröse. Például a 28 és a 12 közös osztói a $\pm 1, \pm 2, \pm 4$ számok, közülük a -4 és 4 azok, melyek mindegyik többszörösei, tehát ezek a legnagyobb közös osztók.

Először belátjuk, hogy ha az a és b egészeknek létezik legnagyobb közös osztója, akkor az előjeltől eltekintve egyértelmű. Ugyanis ha d_1 és d_2 is legnagyobb közös osztó, akkor egyrészt $d_1 \mid d_2$, másrészt pedig $d_2 \mid d_1$; azaz $d_1 = d_2$ vagy $d_1 = -d_2$. Másrészt, ha d az a és b egészek legnagyobb közös osztója, akkor $-d$ is az. Ezek közül a nemnegatívat $\text{lnko}(a, b)$ fogja jelölni. Tehát $\text{lnko}(28,12) = 4$.

Most megmutatjuk, hogy bármely két egésznek létezik legnagyobb közös osztója, és egyúttal azt is, hogy az hogyan határozható meg. Legyenek a és b egész számok, és legyen $b \neq 0$. Ha $b \mid a$, akkor nyilvánvaló, hogy $\text{lnko}(a, b) = b$. Ellenkező esetben a maradékos osztás tétele szerint a felírható

$$a = bq_1 + r_1 \tag{1.3}$$

alakban, ahol $0 < r_1 < |b|$. Folytassuk a maradékos osztást úgy, hogy a következő lépésben mindig az előző lépés osztóját osztjuk az ott keletkezett maradékkal:

$$b = r_1 q_2 + r_2, \tag{1.4}$$

$$r_1 = r_2 q_3 + r_3, \tag{1.5}$$

$$\vdots$$

ahol $|b| > r_1 > r_2 > r_3 > \cdots \geqslant 0$. Mivel a keletkező maradékok csökkennek, előbb-utóbb el kell, hogy érjék a nullát:

$$r_{n-2} = r_{n-1} q_n + r_n, \tag{1.6}$$

$$r_{n-1} = r_n q_{n+1} + 0. \tag{1.7}$$

Ezt az eljárást nevezzük az a és b egészeken végrehajtott *euklideszi algoritmusnak*, az r_n egész számot pedig *az euklideszi algoritmus utolsó zérustól különböző maradékának*. Azt állítjuk, hogy r_n legnagyobb közös osztója a-nak és b-nek. Valóban, az (1.3)-(1.7) egyenlőségeken visszafelé haladva látható, hogy

$$r_n \mid r_{n-1},\ r_n \mid r_{n-2},\ \ldots,\ r_n \mid r_1,\ r_n \mid b,\ r_n \mid a,$$

tehát r_n közös osztója a-nak és b-nek. De ha d is közös osztó, akkor ugyanazon egyenlőségek fentről lefelé való bejárásával kapjuk, hogy $d \mid r_n$, vagyis r_n valóban legnagyobb közös osztó.

Példaként végrehajtjuk az euklideszi algoritmust az $a = 34$ és $b = 12$ számokkal:

$$34 = 12 \cdot 2 + 10$$

$$12 = 10 \cdot 1 + 2$$

$$10 = 2 \cdot 5 + 0,$$

ahol az utolsó zérustól különböző maradék 2, és ez pontosan $\mathrm{lnko}(34, 12)$.

A legnagyobb közös osztó fogalmának hű társa a legkisebb közös többszörös fogalma. Az a és b egészek *legkisebb közös többszörösén* azt az m egész számot értjük, amely egyrészt *közös többszöröse* a-nak és b-nek, azaz $a \mid m$ és $b \mid m$, másrészt a és b minden közös többszörösének osztója, azaz ha $a \mid m'$ és $b \mid m'$, akkor $m \mid m'$. Ez utóbbi tulajdonság a „legkisebb” jelző egyfajta megkerülése. Belátható, hogy bármely két egész számnak létezik legkisebb közös többszöröse, mely előjeltől eltekintve egyértelmű. Az a és b legkisebb közös többszörösei közül a pozitívat $\mathrm{lkkt}(a, b)$ fogja jelölni. A legnagyobb közös osztó és a legkisebb közös többszörös közötti összefüggés az

$$\mathrm{lkkt}(a, b) \cdot \mathrm{lnko}(a, b) = ab$$

képlettel írható le. Innen például

$$\mathrm{lkkt}(34, 12) = \frac{34 \cdot 12}{\mathrm{lnko}(34, 12)} = \frac{34 \cdot 12}{2} = 204.$$

1.2.2. Prímszámok

Korábbi tanulmányainkból ismert, hogy *prímszámoknak* azokat az egész számokat nevezzük, melyeknek pontosan két pozitív osztójuk van. Ez a két osztó nyilván az 1 és a szóbanforgó szám abszolút értéke lehet. Definíció szerint a $-1, 0, 1$ számok egyike sem prím, hiszen a 0-nak végtelen sok, míg a másik kettőnek pedig csak egyetlen pozitív osztója van. A következő állítások azt mutatják, hogy a prímszámokat többféleképpen is lehet jellemezni.

1. Egy 0-tól és ± 1-től különböző egész szám pontosan akkor prím, ha csak úgy bontható fel két egész szám szorzatára, hogy az egyik tényező -1 vagy 1.

2. Egy 0-tól és ± 1-től különböző egész szám pontosan akkor prím, ha $p \mid ab$-ből $p \mid a$ vagy $p \mid b$ következik.

A 2. állítás úgy is megfogalmazható, hogy egy prímszám csak úgy lehet osztója egy szorzatnak, ha a szorzat valamelyik tényezőjének osztója. Példával illusztrálva, a 6 nem prím, ugyanis $6 \mid 2 \cdot 15$ teljesül, de a 6 sem a 2-nek, sem a 15-nek nem osztója.

A következő tétel arra utal, hogy a prímszámok bizonyos értelemben az egész számok építőköveinek tekinthetők.

1.2. Tétel (A számelmélet alaptétele)**.** *Minden 0-tól és ± 1-től különböző egész szám sorrendtől és előjelektől eltekintve egyértelműen felírható véges sok prímszám szorzataként. (Jelen esetben az egytényezős szorzat is megengedett, és az magát az egész számot jelenti.)*

A tételben mondottak értelmében a 10-nek a $(-2) \cdot (-5)$, $2 \cdot 5$, $5 \cdot 2$ és $(-5) \cdot (-2)$ felbontásai közt nem teszünk különbséget.

Bizonyítás. A tételt először természetes számokra bizonyítjuk: megmutatjuk, hogy minden egynél nagyobb természetes szám sorrendtől eltekintve egyértelműen felírható véges sok pozitív prímszám szorzataként. A felbonthatóságot teljes indukcióval igazoljuk. Az első eset, ami szóba jöhet az $n = 2$. Mivel a 2 prím, így az egytényezős szorzatra tett engedménynek megfelelően a tétel igaz ebben az esetben. Most tegyük fel, hogy az állítás 2-től kezdődően valamely k-val bezárólag minden természetes számra teljesül. Megmutatjuk, hogy a tétel $k + 1$-re is igaz. Ez nyilván így van, ha $k+1$ prím. Ha nem, léteznek olyan k_1 és k_2 természetes számok, hogy $k + 1 = k_1k_2$, $2 \leqslant k_1 \leqslant k$ és $2 \leqslant k_2 \leqslant k$. Az indukciós feltevés szerint k_1 és k_2 prímszámok szorzatára bontható, de ekkor nyilván $k + 1$ is.

Az egyértelműség bizonyítása pedig indirekt módon történik: feltesszük, hogy valamely $n > 1$ természetes szám kétféleképpen is prímszámok szorzatára bontható:

$$n = p_1p_2 \cdots p_k = q_1q_2 \cdots q_t, \tag{1.8}$$

és tegyük fel, hogy $k \leqslant t$. Ekkor $p_1 \mid q_1q_2 \cdots q_t$, és mivel p_1 prím, így p_1 osztója a $q_1q_2 \cdots q_t$ szorzat valamely tényezőjének; legyen ez mondjuk q_1. Mivel q_1 is prím, így $p_1 = q_1$, és (1.8)-ból

$$p_2 \cdots p_k = q_2 \cdots q_t$$

következik. Hasonlóan láthatjuk be, hogy $p_2 = q_2$, $p_3 = q_3, \ldots,$ $p_k = q_k$, és így az

$$1 = q_{k+1}q_{k+2} \cdots q_t$$

egyenlőséghez jutunk. Mivel az 1 nem lehet prímek szorzata, ezért a jobb oldalon maradt prímek „nem létezhetnek”, tehát csak $k = t$ teljesülhet. Ez viszont azt jelenti, hogy nincs két különböző prímfelbontás.

Adósak vagyunk még azzal az esettel, amikor n egy -1-nél kisebb egész szám. Ez esetben $-n$ 1-nél nagyobb természetes szám, így a fent bizonyítottak szerint $-n$ véges sok pozitív prím szorzatára bontható: $-n = p_1p_2 \cdots p_k$. Innen $n = (-p_1)p_2 \cdots p_k$ egy lehetséges prímfelbontás. Továbbá, ha n-nek lenne két olyan prímtényezős felbontása, amely nem csak a prímek sorrendjében és azok előjelében különbözne, akkor $-n$-nek is lenne két, nem csupán a prímek sorrendjében eltérő felbontása, ami ellentmond a fentieknek. $\square$

Ha $n > 1$ és az $n = p_1 p_2 \cdots p_k$ felbontásban az azonos prímtényezőket hatvány alakban írjuk fel, akkor az n természetes szám

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$$

alakban is írható, ahol $p_1, p_2, \ldots, p_r$ különböző prímszámok és $\alpha_1, \alpha_2, \ldots, \alpha_n$ pedig pozitív egész számok. Ezt szokás az n *kanonikus alakjának* nevezni.

Nyilvánvaló, hogy ha $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$ és $d \mid n$, akkor d kanonikus alakja

$$d = p_1^{\beta_1} p_2^{\beta_2} \cdots p_r^{\beta_r},$$

ahol $0 \leqslant \beta_1 \leqslant \alpha_1,\ 0 \leqslant \beta_2 \leqslant \alpha_2, \ldots,\ 0 \leqslant \beta_r \leqslant \alpha_r$. Más szóval, d kanonikus alakjában csak olyan prímek lehetnek jelen, melyek n kanonikus alakjában is jelen vannak, és legfeljebb akkora kitevőn. Az állítás megfordítása is igaz: minden ilyen kanonikus alakú természetes szám osztója n-nek. Ezek következménye, hogy ha n és m egynél nagyobb egészek, akkor $\mathrm{lnko}(n, m)$ megkapható úgy, hogy vesszük n és m kanonikus alakjaiból a közös prímtényezőket az előforduló kisebbik hatványon, majd azokat összeszorozzuk. Így például $56 = 2^3 \cdot 7$ és $140 = 2^2 \cdot 5 \cdot 7$, ezért $\mathrm{lnko}(56, 140) = 2^2 \cdot 7{=}28$.

A számelmélet alaptételből az is következik, hogy egy 0-tól és ± 1-től különböző egész szám mindig osztható valamely prímszámmal.

Ha már a prímek ilyen fontos szerephez jutottak, nézzünk még néhány velük kapcsolatos állítást. Először megmutatjuk, hogy végtelen sok prímszám van. Valóban, ha csak véges sok lenne, és mondjuk $p_1, p_2, \ldots, p_n$ lennének az összes, akkor nézzük meg mit mondhatunk az $N = p_1 p_2 \cdots p_n + 1$ egész számról. Egy biztos: a számelmélet alaptétele szerint N prímek szorzatára bontható. Ebben a felbontásban viszont biztosan nem szerepel a felsorolt prímek egyike sem, hiszen N bármelyikkel osztva egyet ad maradékul, ami ellentmond annak, hogy $p_1, p_2, \ldots, p_n$ tényleg az összes prím.

Ha az $n > 1$ egész számról el szeretnénk dönteni, hogy prím-e vagy sem, elég azt megnézni, hogy van-e 1-től és önmagától különböző pozitív osztója. Legyen az n legkisebb pozitív osztója p. Ekkor $n = pc$ valamely c egészre. Mivel c is osztója n-nek, így $c \geqslant p$, és $n = pc \geqslant pp = p^2$. Innen $p \leqslant \sqrt{n}$ adódik, ami azt jelenti, hogy az $n > 1$ egész szám legkisebb egytől különböző pozitív osztója nem lehet nagyobb $\sqrt{n}$-nél.

Például ahhoz, hogy az 1007-ről megállapítsuk, hogy prím-e vagy sem, elegendő

$\sqrt{1007} \approx 31{,}73$-ig osztókat keresni. Sőt, az osztók keresését elég a prímek körében elvégezni, így csupán a $3, 5, 7, 11, 13, 17, 19, 23, 29$ és 31 számokkal való oszthatóságot kell vizsgálni. Ezeket sorban ellenőrizve kiderül, hogy a 19 osztója az 1007-nek, így az 1007 nem lehet prím.

Végül egy algoritmust mutatunk arra, hogyan állíthatjuk elő adott n pozitív egész számig az összes prímeket. Írjuk fel az egész számokat 2-től n-ig:

$$2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, \ldots, n.$$

Ezen számok közül az elsőt bekeretezzük, majd a többszöröseit kihúzzuk:

$$\boxed{2}, 3, \cancel{4}, 5, \cancel{6}, 7, \cancel{8}, 9, \cancel{10}, 11, \cancel{12}, 13, \cancel{14}, 15, \ldots$$

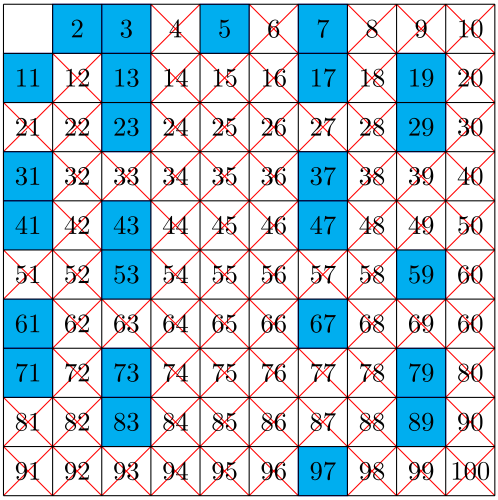
A listán lévő első olyan számot mely még sem bekeretezve, sem kihúzva nincsen, jelen esetben a 3-at, bekeretezzük, majd kihúzzuk a többszöröseit (amelyiket már korábban áthúztuk, azt nem kell még egyszer):

$$\boxed{2}, \boxed{3}, \cancel{4}, 5, \cancel{6}, 7, \cancel{8}, \cancel{9}, \cancel{10}, 11, \cancel{12}, 13, \cancel{14}, \cancel{15}, \ldots$$

A módszer ugyanígy folytatódik: az első át nem húzott és még be nem keretezett számot bekeretezzük, a többszöröseit pedig kihúzzuk. A bekeretezett számokról elmondható, hogy nem oszthatók egyetlen nála kisebb, egynél nagyobb számmal sem, tehát prímek. Amiket kihúztunk, pedig a többszörösei valamelyik bekeretezettnek, így azok nem lehetnek prímek. Ezt az algoritmust nevezzük az *eratosztheneszi szita* módszerének. Az előzőekben elmondottakból az is következik, hogy ha $\sqrt{n}$-ig már az összes prímeket bekereteztük, akkor az eredeti lista minden olyan eleme, ami még nincs áthúzva prím lesz.

1.3. A racionális számok

Jóllehet az egész számokról sokmindent elmondtunk, de még olyan egyszerű egyenletet, mint a $2x - 1 = 0$ sem lehet körükben megoldani. Világos, hiszen ide olyan szám kellene, melyet 2-vel megszorozva egyet kapunk, de ilyen egész szám nem létezik. Ismét építkeznünk kell, az eddig felállított szabályainkat betartva. Az $\frac{a}{b}$ alakú szimbólumokat, ahol a és b egész számok, és $b \neq 0$, *törteknek* nevezzük. Továbbá a-t a tört *számlálójának*, míg b-t a tört *nevezőjének* mondjuk. Az $\frac{a}{b}$ és $\frac{c}{d}$ törteket



1.6. ábra. A prímek listája 100-ig

egyenlőeknek tekintjük, ha $ad = bc$. Ily módon

$$\frac{1}{2} = \frac{2}{4} = \frac{3}{6} = \dots$$

Következik továbbá az is, hogy egy tört számlálóját és nevezőjét ugyanazzal a nullától különböző egész számmal osztva vagy szorozva vele egyenlő törtet kapunk. Amennyiben egy tört számlálójának és nevezőjének a legnagyobb közös osztója 1, akkor a törtet *redukált törtnek* nevezzük. Minden törtnek pontosan egy olyan redukált alakja van, ahol a nevező pozitív. Az összes törtek halmazát *racionális számok halmazának nevezzük*, melynek jelölésére a $\mathbb{Q}$ betűt használjuk.

A racionális számokon az összeadást és a szorzást a következőképpen értelmezzük:

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

Megjegyezzük, hogy az első formulában az egyenlőség bal és jobb oldalain lévő + jel nem ugyanaz. A bal oldalon a + a racionális számok összeadását jelenti, melyről éppen ezzel a formulával akarjuk elmondani, hogy mit is értünk alatta, míg a jobb oldalon álló + egy tört számlálójában van, így az az egész számok összeadását jelképezi, amit már korábbról ismerünk. A második formulában a szorzással ugyanez a helyzet.

Természetesen azt szeretnénk, ha ezek a műveletek rendelkeznének mindazon tulajdonságokkal, amit eddig tőlük megszoktunk: az összeadás is és a szorzás is legyen kommutatív és asszociatív. Könnyű látni, hogy ezek mind teljesülnek, például az összeadás asszociativitását nézzük meg:

$$\begin{aligned}\left(\frac{a}{b}+\frac{c}{d}\right)+\frac{e}{f} &= \frac{ad+bc}{bd}+\frac{e}{f}=\frac{(ad+bc)f+(bd)e}{(bd)f}= \\ &= \frac{adf+bcf+bde}{bdf}\end{aligned}$$

és

$$\begin{aligned}\frac{a}{b}+\left(\frac{c}{d}+\frac{e}{f}\right) &= \frac{a}{b}+\frac{cf+de}{df}=\frac{a(df)+b(cf+de)}{b(df)}= \\ &= \frac{adf+bcf+bde}{bdf}.\end{aligned}$$

Mindkét egyenlőség ugyanahhoz a formulához vezetett, így a bal oldalon lévő formulák is egyenlők kell legyenek, tehát a törtek összeadása valóban asszociatív. Vegyük észre, hogy menet közben a számlálóban az egész számok közötti összeadás és szorzás szinte minden korábban említett tulajdonságát kihasználtuk.

Hasonlóan igazolhatjuk azt is, hogy a szorzás az összeadásra nézve disztributív.

De hogyan lesz a racionális számok halmaza az egész számok halmazának bővítése? Hogyan érhetők tetten az egész számok a racionális számok között? A válasz egyszerű: az a egész számnak megfeleltetjük az $\frac{a}{1}$ törtet. Ez egy kölcsönösen egyértelmű hozzárendelés az egész számok halmaza és a racionális számok

$$\left\{\frac{a}{1}: a \in \mathbb{Z}\right\}$$

részhalmaza között. Továbbá, ha az a és b egész számok helyett a nekik megfelelő $\frac{a}{1}$ és $\frac{b}{1}$ racionális számokat adjuk illetve szorozzuk össze, akkor összeg és a szorzat $\frac{a+b}{1}$ és $\frac{ab}{1}$ lesz, melyek pontosan az $a+b$, illetve ab egész számoknak felelnek meg. Ez azt jelenti, hogy ha egész számokat „racionális számokként” adunk, illetve szorzunk össze, az eredmény ugyanaz lesz, mintha egész számokként tettük volna velük ugyanezt. Mindezek alapján megállapodunk abban, hogy az $\frac{a}{1}$ tört helyett ezentúl egyszerűen a-t is írhatunk.

Az is igaz, hogy a 0 (azaz a $\frac{0}{1}$ tört) olyan racionális szám, melyet bármelyik másikhoz hozzáadva, az a másik nem változik. Továbbá, az $\frac{a}{b}$ racionális számhoz

$\frac{-a}{b}$-t hozzáadva az összeg 0 lesz, így minden racionális számnak van ellentettje. Az ellentett létezése a kivonás lehetőségét kínálja, a kivonás ugyanis nem más, mint az ellentett hozzáadása. Könnyű látni, hogy az $\frac{1}{1}$ törtet bármely törttel megszorozva ez utóbbi nem változik, tehát az 1 a racionális számok körében a szorzásra nézve pontosan úgy viselkedik, mint az egész számok körében. De míg az egészek körében az 1 csak önmagával és -1-gyel volt osztható, az $\frac{1}{1}$-et minden $\frac{0}{1}$-től különböző tört osztja, vagyis minden $\frac{a}{b} \neq 0$ törthöz van olyan tört, nevezetesen a $\frac{b}{a}$, hogy a kettő szorzata éppen 1-gyel egyenlő. A $\frac{b}{a}$ törtet az $\frac{a}{b}$ reciprokának mondjuk. Ha osztásnak a reciprokkal való szorzást tekintjük, akkor megállapíthatjuk, hogy bármely racionális számot bármely nullától különböző racionális számmal el lehet osztani, és az eredmény is racionális szám lesz.

Megállapítható tehát, hogy a racionális számok körében az összeadás, a kivonás és a szorzás korlátlanul elvégezhető, sőt az osztás is azzal a megkötéssel, hogy a nullával való osztást nem értelmezzük.

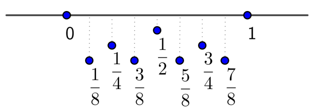
Végül a racionális számoknak egy újabb, az egész számokétól eltérő tulajdonságára hívjuk fel a figyelmet: bármely két különböző racionális szám között van további racionális szám. Valóban, legyenek $\frac{a}{b}$ és $\frac{c}{d}$ racionális számok, és tegyük fel, hogy $\frac{a}{b} < \frac{c}{d}$. Ekkor a számtani közepük

$$\frac{\frac{a}{b} + \frac{c}{d}}{2} = \frac{ad + bc}{2bd}$$

is racionális szám, továbbá

$$\frac{a}{b} < \frac{ad + bc}{2bd} < \frac{c}{d}.$$

A racionális számoknak ez a tulajdonsága azt jelenti, hogy a racionális számok

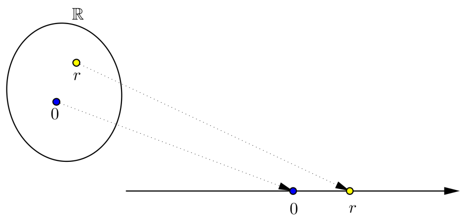


1.7. ábra. A $[0; 1]$ intervallum felezésével, majd a keletkezett intervallumok tovább felezésével kapott felezőpontok „látszólag lefedik” az intervallumot

sűrűn helyezkednek el a számegyenesen, azaz a számegyenes bármely pontjának bármely környezetében van racionális szám. De ebből még nem következik, hogy a számegyenes minden pontja racionális számnak felel meg. Középiskolai tanulmányainkból ismert, hogy például az egységnégyzet átlójának hosszához tartozó szám nem lesz racionális.

1.4. A valós számok

Az egyenletek megoldhatóságára visszatérve megállapíthatjuk, hogy az $ax + b = 0$ alakú egyenletek, ahol a és b racionális számok, és $a \neq 0$ mind megoldhatók a racionális számok körében, és az egyetlen megoldás $x = -\frac{b}{a}$. Más a helyzet akkor, ha az egyenletben már az x ismeretlen négyzete is megjelenik: az $x^2 - 2 = 0$ egyenletnek már nincs megoldása a racionális számok körében. A számegyenes minden nem racionális számot reprezentáló pontjához rendeljük hozzá annak a 0-tól való (előjellel ellátott) távolságát, és ezekkel az úgynevezett irracionális számokkal egészítsük ki a racionális számok halmazát. Szemléletesen így jutunk el a *valós számok halmazáig*, melyben a fenti egyenletnek már két megoldása is van: $\sqrt{2}$ és $-\sqrt{2}$. A valós számok halmazában a négy alapművelet korlátlanul elvégezhető (a nullával való osztás kivételével), és minden nemnegatív számból tudunk négyzetgyököt vonni. Negatív számoknak azonban nem létezik valós négyzetgyöke, így például az $x^2 + 1 = 0$ egyenlet megoldása még a valós számok körében sem lehetséges.



1.8. ábra. A valós számok és a számegyenes pontjai között kölcsönösen egyértelmű leképezés létesíthető

1.5. Feladatok

1.1. Feladat. Igazolja, hogy

a) az első n pozitív egész összege $\frac{n(n+1)}{2}$;

b) az első n páratlan természetes szám összege n^2;

c) az első n pozitív egész köbeinek az összege

$$\left(\frac{n(n+1)}{2}\right)^2!$$

1.2. Feladat. Igazolja, hogy

$$(1+1)\left(1+\frac{1}{2}\right)\left(1+\frac{1}{3}\right)\cdots\left(1+\frac{1}{n}\right)=n+1$$

minden $n \geqslant 1$ természetes számra!

1.3. Feladat. Elevenítse fel a Kalkulusból ismert rendezési reláció fogalmát, majd igazolja, hogy az egész számok halmazán az oszthatóság rendezési reláció!

1.4. Feladat. Végezze el a maradékos osztást az összes lehetséges módon a ± 82 és ± 18 egészeken!

1.5. Feladat. Mivel egyenlők $\operatorname{lnko}(0,0)$ és $\operatorname{lkkt}(0,0)$?

1.6. Feladat. Hajtsa végre az euklideszi algoritmust az $a = 68$ és $b = 44$ számokon, majd állapítsa meg a és b legnagyobb közös osztóit, és legkisebb közös többszöröseit!

1.7. Feladat. Bizonyítsuk be, hogy

$$11 \mid (6^{2n} + 3^{n+2} + 3^n)!$$

1.8. Feladat. Egy természetes szám pozitív osztóinak száma mikor lesz páros, illetve páratlan?

1.9. Feladat. Két pozitív prímszám különbsége 2001. Hány pozitív osztója van a két prím összegének?

2. Komplex számok

Célunk egy olyan (szám)halmaz felépítése, amely eleget tesz a következő kívánalmaknak:

– elvégezhető benne a négy alapművelet a „megszokott” műveleti tulajdonságokkal;

– tartalmazza a valós számok halmazát oly módon, hogy az alapműveletek a valós számokon úgy „működjenek”, ahogy azt megszoktuk;

– korlátlanul lehessen benne gyököt vonni.

Mivel a valós számok és a számegyenes pontjai között kölcsönösen egyértelmű leképezés létesíthető, a számfogalom további bővítése egy dimenzióban már nem lehetséges.

2.1. Műveletek a sík pontjain

Tekintsük a sík pontjainak $\mathbb{R}^2 = \mathbb{R} \times \mathbb{R} = \{(a, b) \quad : \quad a, b \in \mathbb{R}\}$ halmazát, és definiáljuk rajta az összeadást és a szorzást a következőképpen:

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

Ez az összeadás és szorzás mindig elvégezhető, tehát a sík bármely két pontjának összege és szorzata is a sík valamely pontja lesz. Mindkét művelet kommutatív és asszociatív, azaz bármely $u, v, w \in \mathbb{R}^2$ esetén teljesülnek az alábbi egyenlőségek:

$$\begin{aligned} u + v &= v + u \qquad \text{és} \qquad u \cdot v = v \cdot u; \\ (u + v) + w &= u + (v + w) \qquad \text{és} \qquad (u \cdot v) \cdot w = u \cdot (v \cdot w). \end{aligned}$$

Az összeadás ezen tulajdonságait a valós számoktól örökli, hiszen a pontok összeadásakor tulajdonképpen valós számokat adunk össze, koordinátánként. A szorzás asszociatív tulajdonságát bebizonyítjuk, mely után a kommutativitás ellenőrzése már nem jelenthet gondot. Legyen $u = (a, b), v = (c, d)$ és $w = (e, f)$. Kiszámítva a $(u \cdot v) \cdot w$ és $u \cdot (v \cdot w)$ szorzatokat (és felhasználva, hogy a valós számok összeadása kommutatív) láthatjuk, hogy mindkettő ugyanazt a pontot adja eredményül:

$$\begin{aligned} (u \cdot v) \cdot w &= \big((a, b) \cdot (c, d)\big) \cdot (e, f) = (ac - bd, ad + bc) \cdot (e, f) = \\ &= \big((ac - bd)e - (ad + bc)f, (ac - bd)f + (ad + bc)e\big) = \end{aligned}$$

$$= (ace - bde - adf - bcf, acf - bdf + ade + bce)$$

és

$$\begin{aligned} u \cdot (v \cdot w) &= (a,b) \cdot \big((c,d) \cdot (e,f)\big) = (a,b) \cdot (ce - df, cf + de) = \\ &= \big(a(ce - df) - b(cf + de), a(cf + de) + b(ce - df)\big) = \\ &= (ace - adf - bcf - bde, acf + ade + bce - bdf). \end{aligned}$$

Érvényes továbbá a zárójel-felbontási szabály, vagyis a szorzás az összeadásra nézve disztributív: $(u + v) \cdot w = u \cdot w + v \cdot w$ teljesül bármely u, v és w pontokra. Ennek ellenőrzése az olvasó feladata.

Az origó olyan pont, melyet bármely másik ponthoz hozzáadva az a másik pont nem változik, ez lesz az úgynevezett zéruselem. Továbbá, bármely (a, b) ponthoz található olyan pont, nevezetesen a $(-a, -b)$ pont, mellyel összeadva az eredmény éppen a zéruselem, más szóval, minden pontnak van ellentettje. Ennek köszönhetően a kivonás, mint az ellentett hozzáadása, a sík pontjain korlátlanul elvégezhető. Az $(1, 0)$ pont olyan tulajdonságú, hogy bármely (a, b) pontot vele megszorozva az eredmény (a, b) lesz, ez az úgynevezett egységelem. Most pedig megmutatjuk, hogy minden (a, b) origótól különböző pontnak van reciproka, azaz van olyan (x, y) pont, mellyel (a, b)-t megszorozva eredményül az $(1, 0)$ pontot kapjuk. Valóban, az $(a, b) \cdot (x, y) = (1, 0)$ egyenlőségből a szorzást elvégezve $(ax - by, ay + bx) = (1, 0)$ adódik. Két rendezett elempár pontosan akkor egyenlő, ha megfelelő komponensei megegyeznek. Innen az

$$\begin{aligned} ax - by &= 1 \\ ay + bx &= 0 \end{aligned} \tag{2.1}$$

egyenletrendszert nyerjük, melynek megoldása könnyedén leolvasható, ha a vagy b egyike nulla. Ellenkező esetben az első egyenletet a-val, a másodikat b-vel szorozva kapjuk, hogy

$$\begin{aligned} a^2x - aby &= a \\ aby + b^2x &= 0, \end{aligned}$$

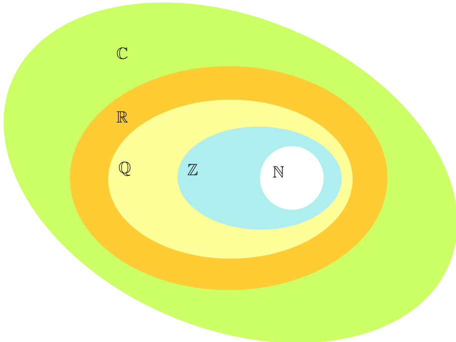
majd a két egyenletet összeadva az $a^2x + b^2x = a$ egyenlethez jutunk. Innen kapjuk,

hogy
$$x = \frac{a}{a^2+b^2}.$$
Ha (2.1)-ben a szorzást fordított szereposztással végezzük el, azaz az első egyenletet szorozzuk b-vel, a másodikat a-val, majd a két egyenletet egymásból kivonjuk, azt kapjuk, hogy
$$y = \frac{-b}{a^2+b^2}.$$
Összegezve, az (a,b) origótól különböző pont reciproka
$$\frac{1}{(a,b)} = \left(\frac{a}{a^2+b^2}, \frac{-b}{a^2+b^2}\right).$$
A reciprok létezése az osztás elvégezhetőségét jelenti. Az első kívánalom tehát maradéktalanul teljesül.

A rendezett valós számpárok $\mathbb{R}^2$ halmazát a fent definiált összeadással és szorzással ellátva a *komplex számok* halmazának nevezzük és jelölésére a $\mathbb{C}$ szimbólumot használjuk. A $z = (a,b)$ komplex szám első komponensét a z *valós részének*, második komponensét pedig a *képzetes részének* nevezzük. Jelölés: $\mathrm{Re}(z) = a$ és $\mathrm{Im}(z) = b$.

Tekintsük a komplex számok halmazának az $R = \{(a,0) : a \in \mathbb{R}\}$ részhalmazát. Két R-beli elem összege és szorzata szintén eleme R-nek:
$$(x,0)+(y,0) = (x+y,0) \qquad \text{és} \qquad (x,0)\cdot(y,0) = (xy,0).$$
Az első komponenseket nézve (melyek nyilván valós számok) megállapíthatjuk, hogy R-ben a műveletek úgy „működnek” ahogy azt a valós számok körében megszoktuk. Továbbá, az $f : \mathbb{R} \to R$, $f(x) = (x,0)$ függvény kölcsönösen egyértelmű leképezés a valós számok és az R halmaz elemei között, tehát R elemei azonosíthatók a valós számokkal.

A harmadik kívánalmunk teljesülésének igazolása később fog megtörténni, előljáróban annyit elárulhatunk, hogy például az egységelem ellentettje, mely a $(-1,0)$ komplex szám (amit az imént éppen a -1-gyel azonosítottunk), „négyzetszám” lesz:
$$(0,1)\cdot(0,1) = (-1,0).$$
Jelöljük ezt a $(0,1)$ komplex számot i-vel, továbbá – a fentebb említett beágyazás által motiválva – az $(a,0)$ alakú komplex számot egyszerűen csak a-val. Ekkor az



2.1. ábra. Számhalmazok

(a, b) komplex szám felírása az

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

felbontás miatt $a + bi$ alakban is lehetséges, melyet a komplex szám *algebrai alakjának* nevezünk.

2.2. Műveletek algebrai alakban adott komplex számokkal

Algebrai alakban felírt komplex számokkal az összeadást, a kivonást és a szorzást úgy kell elvégezni, mint általában a többtagú kifejezésekkel, emlékezetben tartva, hogy $i^2 = -1$:

$$(a + bi) \pm (c + di) = (a + c) \pm (b + d)i$$

és

$$(a + bi) \cdot (c + di) = ac + adi + bci + bdi^2 = ac + adi + bci - bd =$$
$$= (ac - bd) + (ad + bc)i.$$

A szemléletesség kedvéért álljon itt néhány példa:

$$(-1 + i) + (3 - 2i) = 2 - i,$$
$$(-1 + i) - (3 - 2i) = -4 + 3i,$$
$$(-1 + i) \cdot (3 - 2i) = -3 + 2i + 3i - 2i^2 = -3 + 5i + 2 = -1 + 5i,$$
$$(-5 - 3i) \cdot 2i = -10i - 6i^2 = 6 - 10i.$$

Mielőtt rátérnénk az osztásra, megjegyezzük, hogy a $z = a + bi$ komplex szám *konjugáltján* a $\overline{z} = a - bi$ komplex számot értjük. Eszerint $\overline{1+i} = 1 - i$, $\overline{3-2i} = 3 + 2i$, $\overline{2{,}45} = 2{,}45$, $\overline{-4i} = 4i$. Könnyen ellenőrizhető, hogy tetszőleges z és w komplex számok esetén:

- $\overline{z} = z$ akkor és csak akkor, ha z valós szám;
- $\overline{\overline{z}} = z$;
- $\overline{z + w} = \overline{z} + \overline{w}$;
- $\overline{z \cdot w} = \overline{z} \cdot \overline{w}$;
- $z + \overline{z} = 2\,\mathrm{Re}(z)$;
- ha $z = a + bi$, akkor $z \cdot \overline{z} = a^2 + b^2$.

Most határozzuk meg az $a + bi$ és a nullától különböző $c + di$ komplex számok hányadosát. Az alapgondolat az, hogy egy tört számlálóját és nevezőjét a nevező konjugáltjával szorozva megszabadulhatunk a nevezőben lévő komplex számtól úgy, hogy a tört értéke nem változik:

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

Nézzük meg ugyanezt konkrét komplex számokkal, majd az eredményt vessük össze a szorzásnál látott példákkal:

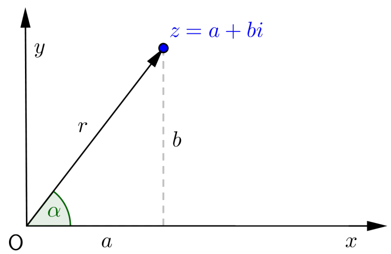
$$\frac{-1+5i}{3-2i} = \frac{-1+5i}{3-2i} \cdot \frac{3+2i}{3+2i} = \frac{-13+13i}{13} = -1 + i,$$

$$\frac{6-10i}{2i} = \frac{6-10i}{2i} \cdot \frac{-2i}{-2i} = \frac{-20-12i}{4} = -5 - 3i.$$

Hatványozáshoz és gyökvonáshoz azonban az algebrai alak csak nehézkesen használható.

2.3. Komplex számok trigonometrikus alakja

Világos, hogy az (a, b), vagy ha úgy tetszik, $a + bi$ komplex szám egy derékszögű koordináta-rendszer rögzítése után jellemezhető az (a, b) pont origótól való távolságával, és azzal a α szöggel, mellyel a vízszintes tengely pozitív felét az origó körül pozitív (az óramutató járásával ellentétes) irányba el kell forgatni ahhoz, hogy az áthaladjon az (a, b) ponton. Ezt az α szöget nevezzük a komplex szám *argumentumának*. Például, az $1 + i$ komplex szám argumentuma $45°$, az $1 - i$ komplex számé pedig $315°$. Általában véve, az argumentum meghatározásához a $\operatorname{tg} \alpha = \frac{b}{a}$ egyenlet megoldása elégséges, feltéve, hogy $a \neq 0$. Ne feledjük, hogy a tangens függvény periódusa $180°$, így az egyenletnek végtelen sok megoldása van; ebből az argumentum kiválasztásához elég megnézni, hogy a szóbanforgó komplex szám melyik síknegyedben van. Ha van elég bátorságunk radiánban számolni, akkor az argumentumot a



2.2. ábra. Komplex szám ábrázolása a síkon

tangens függvény inverzének segítségével a következőképpen határozhatjuk meg:

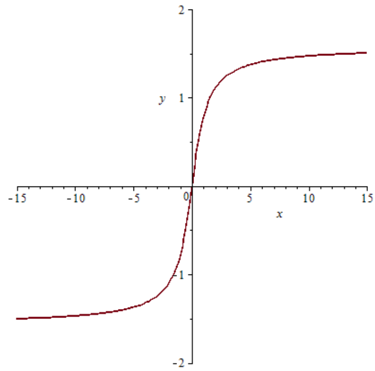
$$\arg(z) = \begin{cases} \operatorname{arctg}(b/a) & \text{ha } a > 0 \text{ és } b \geqslant 0; \\ 2\pi + \operatorname{arctg}(b/a) & \text{ha } a > 0 \text{ és } b < 0; \\ \pi/2 & \text{ha } a = 0 \text{ és } b > 0; \\ 3\pi/2 & \text{ha } a = 0 \text{ és } b < 0; \\ \pi + \operatorname{arctg}(b/a) & \text{ha } a < 0. \end{cases}$$

Az (a, b) komplex szám origótól való távolsága a Pitagorasz-tétel alapján $\sqrt{a^2 + b^2}$; ezt a nemnegatív valós számot nevezzük a komplex szám *abszolút értékének*. Ez a fogalom is szinkronban van a valós számok köréből ismert abszolút értékkel, és minden $z, w \in \mathbb{C}$ esetén igazak az alábbi tulajdonságok:

– $|zw| = |z||w|$;

– $\left|\frac{z}{w}\right| = \frac{|z|}{|w|}$.

Világos, hogy két, nullától különböző, abszolút értékével és argumentumával adott komplex szám pontosan akkor egyenlő, ha az abszolút értékeik megegyeznek, argumentumaik különbsége pedig $360°$ valamely egész számú többszöröse. Továbbá, ha adott a $z = a + bi \neq 0$ komplex szám origótól való r távolsága, és α argumentuma,



2.3. ábra. Az arctg függvény gráfja

akkor a 2.2. ábra szerint $a = r\cos\alpha$ és $b = r\sin\alpha$, ezért

$$z = a + bi = r\cos\alpha + (r\sin\alpha)i = r(\cos\alpha + i\sin\alpha).$$

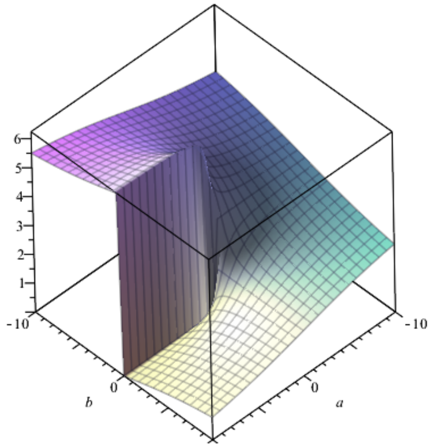
Az egyenlőség jobb oldalán lévő formulát a z komplex szám trigonometrikus alakjának nevezzük. A 0 komplex számhoz nem rendelünk trigonometrikus alakot.

Példaként írjuk fel a $z = 1 + i$ komplex számot trigonometrikus alakban. Ekkor $r = |z| = \sqrt{1^2 + 1^2} = \sqrt{2}$, az argumentum pedig a komplex számot a síkon ábrázolva könnyen le is olvasható: $\alpha = 45°$. A trigonometrikus alak tehát $z = \sqrt{2}(\cos 45° + {} + i\sin 45°)$. Legyen most $z = -\sqrt{3} + i$. Ekkor $r = |z| = \sqrt{(\sqrt{3})^2 + 1^2} = \sqrt{4} = 2$. Az argumentum meghatározása pedig a $\operatorname{tg}\alpha = -\frac{1}{\sqrt{3}}$ egyenlet megoldásával lehetséges. Innen kapjuk, hogy $\alpha = -30° + k \cdot 180°$, ahol k teszőleges egész. Tekintettel arra, hogy z most a második síknegyedben van, így $90° < \alpha < 180°$, tehát $\alpha = 150°$ és z trigonometrikus alakja: $z = 2(\cos 150° + i\sin 150°)$.

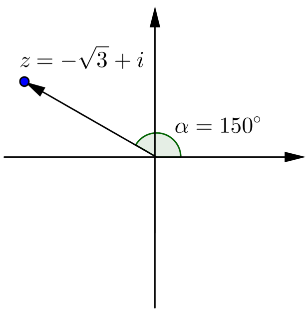
2.4. Műveletek trigonometrikus alakban adott komplex számokkal

A komplex számok trigonometrikus alakjának jelentősége abban rejlik, hogy ilyen alakban adott komplex számokkal bizonyos műveletek sokkal hatékonyabban végezhetők el. Legyenek $z = r(\cos\alpha + i\sin\alpha)$ és $w = s(\cos\beta + i\sin\beta)$ trigonometrikus alakban adott komplex számok. A

$$\sin(\alpha + \beta) = \sin\alpha\cos\beta + \cos\alpha\sin\beta$$



2.4. ábra. Az $f\colon \mathbb{R}^2 \to [0, 2\pi[,\ f(a,b) = \arg(a+bi)$ függvény által leírt felület



2.5. ábra. A $z = -\sqrt{3} + i$ komplex szám argumentuma

és

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

addíciós képletek felidézése után könnyen ellenőrizhető, hogy

$$z \cdot w = rs(\cos(\alpha + \beta) + i\sin(\alpha + \beta)),$$

azaz trigonometrikus alakban adott komplex számok szorzásakor az abszolút értékek összeszorzódnak, míg az argumentumok összeadódnak. Lévén a pozitív egész kitevőre történő hatványozás ismételt szorzás, a $z = r(\cos\alpha + i\sin\alpha)$ komplex szám

n-edik hatványa, ahol n pozitív egész,

$$z^n = \underbrace{r \cdot r \cdot \ldots \cdot r}_{n \text{ db}} \big(\cos(\underbrace{\alpha + \alpha + \cdots + \alpha}_{n \text{ db}}) + i \sin(\underbrace{\alpha + \alpha + \cdots + \alpha}_{n \text{ db}})\big) =$$
$$= r^n(\cos n\alpha + i \sin n\alpha).$$

Ezt a formulát *Moivre-képletnek* nevezzük, jelentése pedig az, hogy trigonometrikus alakban adott komplex szám hatványozásakor az abszolút értéket, mint valós számot az adott kitevőre emeljük, és az argumentumot pedig a kitevővel szorozzuk.

Példaként kiszámítjuk az $1-i$ komplex szám tizedik hatványát. Előtte megállapodunk abban, hogy algebrai alakban kitűzött feladatnál az eredményt is algebrai alakban várjuk. A Moivre-képlet alkalmazásához viszont át kell váltanunk trigonometrikus alakra: $1 - i = \sqrt{2}(\cos 315^\circ + i \cos 315^\circ)$. Innen

$$(1-i)^{10} = (\sqrt{2})^{10}(\cos(10 \cdot 315^\circ) + i \sin(10 \cdot 315^\circ)) = 32(\cos 270^\circ + i \sin 270^\circ) =$$
$$= 32(0 + (-1)i) = -32i.$$

Könnyű belátni, hogy a $z = r(\cos\alpha + i \sin\alpha)$ komplex szám reciproka

$$\frac{1}{z} = \frac{1}{r}(\cos(-\alpha) + i \sin(-\alpha)),$$

ugyanis ekkor $z \cdot \frac{1}{z} = 1(\cos 0^\circ + i \sin 0^\circ) = 1$. A szorzás és a reciprok felhasználásával a $z = r(\cos\alpha + i \sin\alpha)$ és $w = s(\cos\beta + i \sin\beta) \neq 0$ komplex számok hányadosa a következőképpen határozható meg:

$$\frac{z}{w} = z \cdot \frac{1}{w} = r(\cos\alpha + i \sin\alpha) \cdot \frac{1}{s}(\cos(-\beta) + i \sin(-\beta)) =$$
$$= \frac{r}{s}(\cos(\alpha - \beta) + i \sin(\alpha - \beta).$$

Más szóval, trigonometrikus alakban adott komplex számok osztásánál az abszolút értékeiket elosztjuk, argumentumaikat pedig kivonjuk. Ennélfogva a Moivre-képlet tetszőleges egész kitevőre érvényes, továbbá teljesülnek a hatványozás valós számok köréből is ismert tulajdonságai.

2.5. Gyökvonás komplex számból

Célunkat teljes mértékben akkor érjük el, ha megmutatjuk, hogy a komplex számok körében korlátlanul elvégezhető a gyökvonás. Ehhez azonban tisztáznunk kell mit is értünk egy komplex szám n-edik gyökén. Legyen n adott pozitív egész. A z *komplex szám n-edik gyökén* mindazon komplex számokat értjük, melyek n-edik hatványa z. Vigyázat! A valós számok körében a 9 négyzetgyöke a 3, a komplex számok körében viszont a fenti definíciónak a 3 mellett a -3 is eleget tesz. Tehát a z komplex szám n-edik gyöke általában nem egyetlen komplex szám, hanem komplex számok egy halmaza. Az ebből fakadó zavarok elkerülése végett a $\sqrt[n]{\cdot}$ jelet kizárólag valós számok n-edik gyökének jelölésére fogjuk használni.

Legyen $z = r(\cos\alpha + i\sin\alpha)$ tetszőleges komplex szám, és keressük z n-edik gyökeit trigonometrikus alakban. Ha $x = u(\cos\varphi + i\sin\varphi)$ egy n-edik gyöke z-nek, akkor $x^n = z$ teljesül. Alkalmazva a Moivre-képletet

$$u^n(\cos(n\cdot\varphi) + i\sin(n\cdot\varphi)) = r(\cos\alpha + i\sin\alpha)$$

adódik. Az egyenlőség mindkét oldalán egy-egy trigonometrikus alakban adott komplex szám szerepel, tehát az egyenlőség csak úgy teljesülhet, ha

$$u^n = r \qquad \text{és} \qquad n\cdot\varphi = \alpha + k\cdot 360^\circ,$$

valamely k egészre. Az első egyenlet az abszolút értékek miatt a valós számok körében értendő, így egyetlen megoldása $u = \sqrt[n]{r}$. A második egyenletből pedig $\varphi = \frac{\alpha + k\cdot 360^\circ}{n}$ adódik. A z komplex szám n-edik gyökei tehát az

$$\sqrt[n]{r}\left(\cos\frac{\alpha + k\cdot 360^\circ}{n} + i\sin\frac{\alpha + k\cdot 360^\circ}{n}\right), \tag{2.2}$$

alakú komplex számok, ahol $k \in \mathbb{Z}$. Ezek szerint minden nemnulla komplex számnak végtelen sok n-edik gyöke lenne? Próbaképpen határozzuk meg a -8 harmadik gyökeit! A -8 trigonometrikus alakja $8(\cos 180^\circ + i\sin 180^\circ)$. A k alábbi értékeire a fenti képlet a következő eredményt adja.

$$\begin{aligned}
k = 0: &\quad \sqrt[3]{8}\,(\cos 60^\circ + i\sin 60^\circ) = 1 + \sqrt{3}i\\
k = 1: &\quad \sqrt[3]{8}\,(\cos 180^\circ + i\sin 180^\circ) = -2\\
k = 2: &\quad \sqrt[3]{8}\,(\cos 300^\circ + i\sin 300^\circ) = 1 - \sqrt{3}i
\end{aligned}$$

Folytatva ezt, a $k = 3$ esetben $\sqrt[3]{8}\,(\cos 420^\circ + i\sin 420^\circ) = 1 + \sqrt{3}i$ adódik, ugyanaz tehát mint a $k = 0$ esetben.

Legyenek u és v tetszőleges egészek, és osszuk el az $u - v$ egész számot maradékosan n-nel: $u - v = nq + t$, ahol q és t egészek, valamint $0 \leqslant t < n$. Ekkor

$$\frac{\alpha + u \cdot 360^\circ}{n} = \frac{\alpha + (v + nq + t) \cdot 360^\circ}{n} = \frac{\alpha + v \cdot 360^\circ}{n} + \frac{(nq + t) \cdot 360^\circ}{n} = \\ = \frac{\alpha + v \cdot 360^\circ}{n} + \left(q + \frac{t}{n}\right) \cdot 360^\circ.$$

Ebből látszik, hogy a $\frac{\alpha+u\cdot 360^\circ}{n}$ és $\frac{\alpha+v\cdot 360^\circ}{n}$ szögek közötti eltérés pontosan a $t = 0$ esetben lesz 360° egész számú többszöröse, vagyis a (2.2) képlet által meghatározott komplex számok a $k = u$ és $k = v$ esetekben akkor és csak akkor egyeznek meg, ha $u - v$ osztható n-nel. Tehát a (2.2) képlet $k = 0, 1, \ldots, n-1$ esetekre történő alkalmazásával n darab különböző komplex számot kapunk, és k semmilyen más értékére nem kapunk ezektől különböző eredményt. Ezáltal azt bizonyítottuk, hogy minden nullától különböző komplex számnak pontosan n darab n-edik gyöke van.

Visszatérve a példához, a -8-nak 3 különböző harmadik gyöke létezik: -2 és $1 \pm \sqrt{3}i$. Megállapíthatjuk továbbá, hogy a komplex számok körében a gyökvonás valóban korlátlanul elvégezhető, így a komplex számok halmaza eleget tesz a kezdeti követelményeinknek.

Az 1 is komplex szám, így neki is pontosan n darab n-edik gyöke van, ezeket *n-edik egységgyököknek* nevezzük. Ezek kiszámítása ugyancsak a (2.2) képlet alkalmazásával történhet. Mivel az 1 trigonometrikus alakja $\cos 0^\circ + i \sin 0^\circ$ (az $r = 1$ szorzót elhagytuk), (2.2) alapján az n-edik egységgyökök a következők:

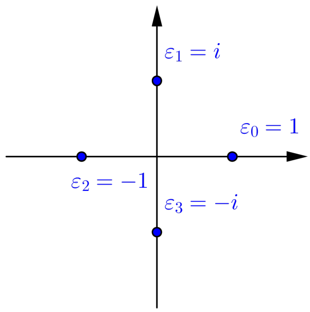
$$\varepsilon_k = \cos \frac{k \cdot 360^\circ}{n} + i \sin \frac{k \cdot 360^\circ}{n},$$

ahol $k = 0, 1, \ldots, n-1$. A negyedik egységgyökök például:

$$\begin{aligned} \varepsilon_0 &= \cos 0^\circ + i \sin 0^\circ = 1, \\ \varepsilon_1 &= \cos 90^\circ + i \sin 90^\circ = i, \\ \varepsilon_2 &= \cos 180^\circ + i \sin 180^\circ = -1, \\ \varepsilon_3 &= \cos 270^\circ + i \sin 270^\circ = -i. \end{aligned}$$

Világos, hogy ε_0 mindig 1, és belátható az is, hogy az n-edik egységgyökök mindegyike előállítható oly módon, hogy ε_1-et $0, 1, \ldots, n-1$ kitevőkre emeljük. A fenti példát tekintve tehát a negyedik egységgyökök megkaphatók, mint i hatványai: $i^0 = 1,\ i^1 = i,\ i^2 = -1$ és $i^3 = -i$.

Az n-edik egységgyökök ismeretében az n-edik gyökvonás tetszőleges z komplex



2.6. ábra. Negyedik egységgyökök

számból könnyebben elvégezhető: ha w a z egy n-edik gyöke, akkor z összes n-edik gyöke

$$w\varepsilon_0, w\varepsilon_1, \dots, w\varepsilon_{n-1},$$

vagyis elég w-t végigszorozni az összes n-edik egységgyökkel. Ennek bizonyítását az olvasóra bízzuk.

A tétel alkalmazásával kiszámítjuk a $-4 = 4(\cos 180° + i \sin 180°)$ negyedik gyökeit. Alkalmazva a (2.2) képletet a $k = 0$ esetre, azt kapjuk, hogy $\sqrt{2}(\cos 45° + {} + i \sin 45°) = 1+i$ az egyik negyedik gyök. Fejben tartva a negyedik egységgyököket, a maradék három a következő: $(1+i)i, (1+i)(-1), (1+i)(-i)$, azaz $-1+i, -1-i$ és $1-i$.

Végül megjegyezzük, hogy a valós számok n-edik gyökének középiskolából ismert tulajdonságai (pl. $\sqrt[n]{ab} = \sqrt[n]{a} \cdot \sqrt[n]{b}$) a komplex számok n-edik gyökére általában nem terjeszthetők ki.

2.6. Feladatok

2.1. Feladat. Töltse ki az alábbi táblázatot!

z	$\mathrm{Re}(z)$	$\mathrm{Im}(z)$	$\overline{z}$
$-5-i$			
1			
0			
			$2+3i$
			i
			π
	0	-5	

2.2. Feladat. Hol helyezkednek el a síkon azok a pontok, melyeknek megfelelő komplex számokra igaz, hogy

1. $\mathrm{Re}(z) + \mathrm{Im}(z) = 1$;
2. $\arg(z) = 45°$;
3. $z = \frac{1}{z}$?

2.3. Feladat. Adja meg az i^2, i^3, i^4, i^5 és i^{15342} értékét! Mivel egyenlő $\frac{1}{i^3}$? Mivel egyenlő i^k, ha n tetszőleges egész szám?

2.4. Feladat. Hozza algebrai alakra a

$$\frac{2}{(1-i)(3+i)}$$

komplex számot!

2.5. Feladat. Legyen $z = -1 + i$ és $w = -3 - 4i$. Határozza meg a

$$\frac{(w+z)^2 \cdot \overline{w}}{\overline{w-z}}$$

kifejezés pontos értékének algebrai alakját!

2.6. Feladat. Adja meg a

$$-2+i, \quad 3+i, \quad -1-2i, \quad 8{,}192-5{,}736i, \quad 3i, \quad 1-\sqrt{3}i$$

komplex számokat trigonometrikus alakban!

2.7. Feladat. Fejezze ki a

$$\frac{\cos 60° + i \sin 60°}{\cos 150° + i \sin 150°}$$

komplex számot algebrai alakban!

2.8. Feladat. Adja meg a

$$\frac{(1+i)^7}{(1-i)^5}$$

komplex számot algebrai alakban!

2.9. Feladat. Számítsa ki a második és a harmadik egységgyököket!

2.10. Feladat. Határozza meg a $\sqrt{3}(\cos 30° + i \sin 30°)$ komplex szám nyolcadik hatványát és harmadik gyökeit!

2.11. Feladat. Legyen a tetszőleges valós szám. Adja meg a komplex négyzetgyökeit!

2.12. Feladat. Számítsa ki a $-2i$ és a $-7 - 24i$ komplex számok négyzetgyökeit!

2.13. Feladat. Számítsa ki a $-2i$ és a $-7 - 24i$ komplex számok négyzetgyökeit trigonometrikus alak használata nélkül! (Útmutatás: keressük a $-2i$ négyzetgyökeit $a + bi$ alakban; ekkor $(a + bi)^2 = -2i$.)

2.14. Feladat. Oldja meg a komplex számok halmazán a

$$z \cdot \overline{z} + z - (10 + i) = 0$$

és a

$$z^2 - \overline{z} = 0$$

egyenleteket!

3. Polinomok

Legyen T a racionális, valós, illetve komplex számok halmaza közül az olvasó szívéhez legközelebb álló. Tekintsük T elemeit, az x úgynevezett „határozatlant”, és nézzük meg, hogy ezekből az összeadás és a szorzás segítségével véges sok lépésben milyen kifejezéseket állíthatunk elő. Könnyen látható, hogy ezek a kifejezések tartalmazhatják x bármilyen nemnegatív kitevőjű hatványát, azok bármilyen T-beli elemmel való szorzatát, illetve az ilyenek összegét. Más szóval, az esetleges zárójelek felbontása, összevonás és rendezés után egy

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 \tag{3.1}$$

alakú kifejezést kapunk, ahol $a_0, a_1, \ldots, a_n$ a T elemei, és n természetes szám. Az ilyen alakú kifejezéseket T feletti *polinomnak* nevezzük, az $a_0, a_1, \ldots, a_n$ számokat a polinom *együtthatóinak* mondjuk. Az $a_j x^j$ kifejezést a polinom *j-ed fokú tagjának* nevezzük. Jelölésben $f(x)$ helyett írhatunk f-et is, ha nem kívánjuk hangsúlyozni, hogy x a határozatlan. A polinomot definiáló képlet bonyolultságát az okozza, hogy az x határozatlan egy T-beli elemmel való szorzatát nem tudjuk ténylegesen elvégezni, így például az x kétszeresét csak formálisan, $2x$-ként tudjuk kezelni, továbbá a különböző fokú tagokat is csak formálisan tudjuk összeadni. Az x-ről mindössze annyit feltételezünk, hogy rá is igaz az, ami T minden elemére, így például $0 \cdot x = 0$. Ebből $0 \cdot x^k = 0$ következik, így az ilyen alakú tagokat általában elhagyjuk. A (3.1) képletben például n-nél magasabb fokú tag nem szerepel, így azok együtthatóit mind nullának tekintjük. Egy polinomban tehát csak véges sok nullától különböző együttható lehet. A definíció szerint az is megtörténhet, hogy egy polinom mindegyik együtthatója nulla, az ilyen polinomot *azonosan nulla polinomnak* nevezzük és 0-val jelöljük.

Ha $f \neq 0$, keressük meg azt a legnagyobb k egész számot, melyre $a_k \neq 0$. Ezt a k számot az *f polinom fokának* nevezzük, és $\deg(f)$-fel jelöljük. Az azonosan nulla polinom fokát nem szokás értelmezni. Ahhoz, hogy ne kelljen az azonosan nulla polinomot mindig kivételként kezelni, mi az azonosan nulla polinom fokát létezőnek, és minden más polinom fokánál kisebbnek tekintjük: legyen az azonosan nulla polinom foka $-\infty$.

A T feletti összes polinomok halmazát $T[x]$ fogja jelölni.

Két polinomot *egyenlőnek* tekintünk, ha az együtthatóik rendre megegyeznek, vagyis minden $k \geqslant 0$ esetén az x^k együtthatója a két polinomban ugyanaz. Világos, hogy egyenlő polinomok fokai is megegyeznek.

3.1. Műveletek polinomokkal

A T feletti polinomok körében értelmezhetünk összeadást és szorzást a következőképpen. Az összeadást az azonos fokú tagok összeadásával végezzük, míg a szorzásnál minden tagot minden taggal szorzunk úgy, hogy az $a_i x^i$ és a $b_j x^j$ tagok szorzata $a_i b_j x^{i+j}$ lesz, majd az azonos fokú tagokat összevonva a kapott összeget x hatványai szerint csökkenő sorrendbe rendezzük. Legyen például $f(x) = 3x^2 - 2x + 1$ és $g(x) = 2x^3 + 5x^2 - 1$. Ekkor

$$f(x) + g(x) = 2x^3 + 8x^2 - 2x$$

és

$$\begin{aligned} f(x) \cdot g(x) &= 6x^5 + 15x^4 - 3x^2 - 4x^4 - 10x^3 + 2x + 2x^3 + 5x^2 - 1 = \\ &= 6x^5 + 11x^4 - 8x^3 + 2x^2 + 2x - 1. \end{aligned}$$

Az összeg- és szorzatpolinomok fokáról az összeadandók, illetve a szorzótényezők fokának ismeretében a következőt mondhatjuk: Az összeg foka nem lehet nagyobb egyik összeadandó fokánál sem, azaz

$$\deg(f + g) \leqslant \max\{\deg(f), \deg(g)\}.$$

Az egyenlőség csak akkor nem teljesül, ha az f és g azonos fokúak, és a legmagasabb fokú tagjaik együtthatóinak összege nulla. Továbbá,

$$\deg(f \cdot g) = \deg(f) + \deg(g),$$

vagyis a szorzat polinom foka mindig a tényezők fokainak összegével egyenlő. Itt kihasználtuk, hogy T-beli elemek szorzata csak úgy lehet nulla, ha valamelyik tényezője nulla. Hogy ez a komplex számok körében is így van, majd egy későbbi fejezetben, általánosabb körülmények között fogjuk belátni.

A polinomokon értelmezett összeadás kommutatív, asszociatív, zéruseleme az azonosan nulla polinom, továbbá minden f polinomnak létezik ellentettje, a $-f$ polinom, melynek együtthatói éppen az f együtthatóinak ellentettjei. Így tehát a polinomok körében a kivonás, mint az ellentett hozzáadása, szintén elvégezhető. A kommutativitás és asszociativitás a szorzásra is igaz, az egységelem szerepét az $f(x) = 1$ polinom tölti be. Egyetlen legalább elsőfokú polinomnak sem létezik reciproka, hiszen szorzáskor a fokok összeadódnak, így legalább elsőfokú polinom egyetlen polinommal való szorzata sem lehet a nulladfokú $f(x) = 1$ polinom. Reciproka tehát csak a nulladfokú polinomoknak lehet, és van is, mivel azok pontosan a T nullától különböző elemei.

Az egész számoknál látottakhoz hasonlóan, reciprok hiányában osztás helyett csak maradékos osztásról tudunk beszélni.

3.1. Tétel (Polinomok maradékos osztásának tétele)**.** *Bármely f és g ($g \neq 0$) T feletti polinomhoz egyértelműen léteznek olyan q és r szintén T feletti polinomok, amelyekre $f = g \cdot q + r$, ahol r foka kisebb a g fokánál.*

Bizonyítás. Először megmutatjuk, hogy ha q és r valóban léteznek, akkor egyértelműen meghatározottak. Ezzel ellentétben tegyük fel, hogy léteznek olyan q_1, q_2, r_1 és r_2 polinomok, melyekre

$$f = g \cdot q_1 + r_1 \quad \text{és} \quad f = g \cdot q_2 + r_2,$$

ahol $\deg(r_1)$ és $\deg(r_2)$ is kisebb mint $\deg(g)$, és $q_1 \neq q_2$. Kivonva a második egyenlőséget az elsőből, átrendezés után a

$$g \cdot (q_2 - q_1) = r_1 - r_2 \tag{3.2}$$

egyenlőséget kapjuk. Mivel $q_1 \neq q_2$, a bal oldalon álló polinom foka legalább annyi, mint g foka, a jobb oldalon álló $r_1 - r_2$ polinom viszont g-nél kisebb fokú, ami ellentmondás. Tehát $q_1 = q_2$, és így a (3.2) bal oldalán álló polinom azonosan nulla. Ekkor viszont $r_1 - r_2$ is azonosan nulla kell legyen, ahonnan $r_1 = r_2$ következik.

Most megmutatjuk, hogyan konstruálhatók meg a q és r polinomok. Legyenek

$$f = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$$

és

$$g = b_m x^m + b_{m-1} x^{m-1} + \cdots + b_1 x + b_0 \neq 0$$

n, illetve m-ed fokú polinomok. Ha $n < m$, akkor a $q = 0$ és $r = f$ szereposztással igaz az állítás: $f = g \cdot 0 + f$. Az $n \geqslant m$ esetben osszuk el f legmagasabb fokú tagját

g legmagasabb fokú tagjával, majd ezt a

$$q_1 = \frac{a_n x^n}{b_m x^m} = \frac{a_n}{b_m} x^{n-m}$$

hányadost szorozzuk meg g-vel és a szorzatot vonjuk ki f-ből! Jelölje ezt a különbséget f_1:

$$f_1 = f(x) - q_1(x) \cdot g(x).$$

Világos, hogy a kivonásnál f legmagasabb fokú tagja kiesik, így f_1 foka kisebb, mint f foka. Ha $\deg(f_1) < \deg(g)$, akkor készen vagyunk: $q = q_1$ és $r = f_1$. Ellenkező esetben ismételjük meg az eljárást úgy, hogy f helyett az f_1 polinomot vesszük: megkonstruáljuk az f_2 polinomot, melyre igaz, hogy $\deg(f_2) < \deg(f_1) < < \deg(f)$. Ha $\deg(f_2) < \deg(g)$, megállunk, egyébként újból ismétlünk, de most f_1 helyett f_2-vel. Mivel az $f_1, f_2, \ldots$ polinomok fokai egyre kisebbek, véges sok lépésben (mondjuk a k-adikban) eljutunk arra az esetre, amikor már $\deg(f_k) < < \deg(g)$. Könnyen látható, hogy

$$f = (q_1 + q_2 + \cdots + q_{k-1}) \cdot g + f_k,$$

tehát a polinomok maradékos osztásának tétele igaz. □

A tételben szereplő q polinomot az f és a g *hányadosának*, míg az r polinomot az osztás *maradékának* nevezzük.

Konkrét példán keresztül talán a bizonyítás is könnyebben megérthető. Osszuk el az $f = -x^5 - 5x^3 + 4x - 1$ polinomot maradékosan a $g = x^3 + 2x - 1$ polinommal! Először elosztjuk f legmagasabb fokú tagját g legmagasabb fokú tagjával: $-x^5/x^3 = -x^2$, ezt a hányadost írjuk az egyenlőségjel jobb oldalára:

$$(-x^5 - 5x^3 + 4x - 1) \ : \ (x^3 + 2x - 1) = -x^2$$

A g polinomot megszorozzuk az előbb kapott hányadossal ($-x^2$-nel), és a szorzatot f alá írjuk:

$$\begin{aligned} &(-x^5 - 5x^3 + 4x - 1) \ : \ (x^3 + 2x - 1) = -x^2 \\ &\ - x^5 - 2x^3 + x^2 \end{aligned}$$

Vonjuk ki f-ből az alatta lévő szorzatot:

$$\begin{aligned}
&(-x^5 - 5x^3 + 4x - 1) \ : \ (x^3 + 2x - 1) = -x^2 \\
-&(\underline{-x^5 - 2x^3 + x^2}) \\
&-3x^3 - x^2 + 4x - 1
\end{aligned}$$

A vonal alatt lévő polinom foka még nem kisebb, mint g foka, így azt f_1-nek tekintve folytatjuk az eljárást. Az f_1 és g polinomok legmagasabb fokú tagjainak hányadosa $-3x^3/x^3 = -3$, ezt hozzáadjuk az egyenlőség jobb oldalán lévő polinomhoz, majd g -3-szorosát az f_1 alá írjuk, amit végül ki is vonunk f_1-ből:

$$\begin{aligned}
&(-x^5 - 5x^3 + 4x - 1) \ : \ (x^3 + 2x - 1) = -x^2 - 3 \\
-&(\underline{-x^5 - 2x^3 + x^2}) \\
&-3x^3 - x^2 + 4x - 1 \\
-&(\underline{-3x^3 - 6x + 3}) \\
&-x^2 + 10x - 4
\end{aligned}$$

A bizonyítás jelöléseit követve a legalul lévő polinom f_2, melynek foka már kisebb g fokánál, így az eljárás véget ért. Az eredmény: $q = -x^2 - 3$ és $r = -x^2 + 10x - 4$. A számolás helyességéről a

$$-x^5 - 5x^3 + 4x - 1 = (x^3 + 2x - 1)(-x^2 - 3) + (-x^2 + 10x - 4)$$

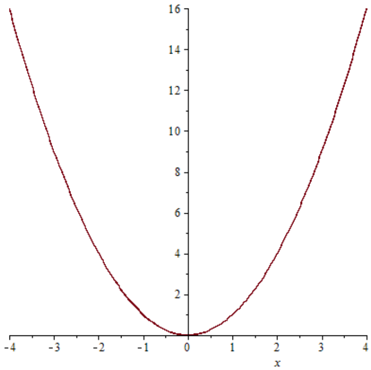
egyenlőség ellenőrzésével győződhetünk meg.

3.2. Polinomok helyettesítési értéke

Legyen $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ egy T feletti polinom, és t adott eleme T-nek. Az

$$f(t) = a_n t^n + a_{n-1}t^{n-1} + \cdots + a_1 t + a_0$$

T-beli számot az $f(x)$ polinom t *helyen vett helyettesítési értékének* nevezzük. Hangsúlyozzuk, hogy a fenti kifejezés már nem formális összeg, itt a műveletek már ténylegesen elvégezhetők. Az f polinomba akár T összes elemét behelyettesíthetjük, melynek eredményeként egy $f^*\colon T \to T$ függvényt kapunk, melyet az *f-hez tartozó polinomfüggvénynek* nevezünk. Gyakorlati szempontból egy polinom (mint formális összeg) és a hozzá tartozó polinomfüggvény között lényegi különbség nincs, később azonban látni fogjuk, hogy ha a polinomok együtthatóit nem a komplex számok köréből vesszük, előfordulhat, hogy nem egyenlő polinomokhoz tartozó polinomfüggvények egyenlők. A polinomok adott helyen vett helyettesítési értékének kiszá-



3.1. ábra. Az $f(x) = x^2$ valós számok feletti polinomhoz tartozó polinomfüggvény gráfja, melyet középiskolai tanulmányaiból mindenki ismer

mításához elvégzendő műveletek számának csökkentésére alkalmas az úgynevezett *Horner-elrendezés*, melynek alapja, hogy az $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ polinomban a legalább elsőfokú tagokból x kiemelhető:

$$f(x) = (a_n x^{n-1} + a_{n-1}x^{n-2} + \cdots + a_1)x + a_0.$$

A zárójelen belül újra és újra kiemelve x-et azokból a tagokból, melyekből lehetséges,

$$\begin{aligned} f(x) &= (a_n x^{n-1} + a_{n-1}x^{n-2} + \cdots + a_1)x + a_0 = \\ &= ((a_n x^{n-2} + a_{n-1}x^{n-3} + \cdots + a_2)x + a_1)x + a_0 = \cdots = \\ &= (\cdots(((a_n x + a_{n-1})x + a_{n-2})x + a_{n-3})x + \cdots + a_1)x + a_0 \end{aligned} \tag{3.3}$$

adódik. Helyettesítsünk most x helyére t-t! A jobb oldalon lévő kifejezés kiértékeléséhez létrehozunk egy táblázatot úgy, hogy

- a táblázat felső sorába a polinom együtthatói kerülnek, rendre a legmagasabb fokú tagtól a konstansig, a nullákat is beleértve;
- a második sor fejlécébe a behelyettesítendő értéket írjuk, majd a főegyüttható alá magát a főegyütthatót másoljuk;

– a második sor többi celláját balról jobbra haladva töltjük ki úgy, hogy a következő cellába az azt megelőzőbe írt szám t szeresének, és a fölötte lévő együtthatónak az összegét írjuk.

Jelölje a második sorba írt elemeket rendre $c_n, c_{n-1}, \ldots, c_0$. Könnyen látható, hogy

$$\begin{aligned}
c_n &= a_n;\\
c_{n-1} &= a_n t + a_{n-1};\\
c_{n-2} &= (a_n t + a_{n-1})t + a_{n-2};\\
&\vdots\\
c_0 &= (\cdots(((a_n t + a_{n-1})t + a_{n-2})t + a_{n-3})t + \cdots + a_1)t + a_0.
\end{aligned}$$

Ekkor (3.3) szerint $c_0 = f(t)$, azaz a táblázat utolsó cellájába írt érték éppen az f polinom t helyen vett helyettesítési értéke.

Például a 3.2. ábrán látottak szerint az $f(x) = 3x^4 - 2x^2 + x + 1$ polinomba $x = 2$-t helyettesítve $f(2) = 43$ adódik. A táblázatból az is látszik, hogy $f(2)$ meghatározásához mindössze 4 darab szorzást és ugyanennyi összeadást használtunk, míg ha a behelyettesítést a „hagyományos” módszerrel végeznénk, akkor csupán a $3x^4$ tag kiértékelése máris 5 szorzásba kerülne.

	3	0	-2	1	1
2	3	$3 \cdot 2 + 0 = 6$	$6 \cdot 2 + (-2) = 10$	$10 \cdot 2 + 1 = 21$	$21 \cdot 2 + 1 = 43$

3.2. ábra. Horner-táblázat az $f(x) = 3x^4 - 2x^2 + x + 1$ polinom $x = 2$ helyen vett helyettesítési értékének meghatározására

Könnyen igazolható a Horner-elrendezés egy másik hozadéka: ha az f polinomot maradékosan osztjuk az $x - t$ elsőfokú polinommal, akkor a hányados együtthatói éppen a táblázat alsó sorában szereplő $c_n, c_{n-1}, \ldots, c_1$ számok, $c_0 = f(t)$ pedig az osztás maradéka, azaz

$$f(x) = (x - t)(c_n x^{n-1} + c_{n-1}x^{n-2} + \cdots + c_2 x + c_1) + f(t). \tag{3.4}$$

A példánkban tehát

$$3x^4 - 2x^2 + x + 1 = (x - 2)(3x^3 + 6x^2 + 10x + 21) + 43,$$

ami a szorzás elvégzésével könnyen ellenőrizhető.

3.3. Polinomok gyökei

Azt mondjuk, hogy $t \in T$ *gyöke* az $f \in T[x]$ polinomnak, ha $f(t) = 0$. Itt T szerepe már fontosabb, mint az eddigiekben. Például az $f(x) = x^2 + 1$ polinom tekinthető akár $\mathbb{R}$, akár $\mathbb{C}$ feletti polinomnak is. Az első esetben f-nek nincs gyöke, hiszen nem létezik olyan t valós szám, melyre $t^2 + 1 = 0$ teljesülne, míg a második esetben f gyökei az i és a $-i$ komplex számok.

(3.4) alapján könnyen látszik, hogy t pontosan akkor gyöke az f polinomnak, ha f felírható

$$f(x) = (x - t)q(x)$$

alakban, ahol q eggyel alacsonyabb fokú polinom, mint f. Ekkor az $x - t$ elsőfokú polinomot az f polinom t-hez tartozó *gyöktényezőjének* nevezzük.

Tegyük fel, hogy az $f(x)$ polinom szorzattá alakítható, azaz vannak olyan $g(x)$ és $h(x)$ szintén T feletti polinomok, hogy $f(x) = g(x)h(x)$. Ha t gyöke az f polinomnak, akkor $f(t) = g(t)h(t) = 0$. Mivel T-beli elemek szorzata csak úgy lehet nulla, ha valamelyik tényező nulla, $g(t) = 0$ vagy $h(t) = 0$ következik; vagyis t pontosan akkor gyöke az f polinomnak, ha vagy g-nek, vagy h-nak (esetleg mindkettőnek) gyöke.

Legyen t_1 az f nem azonosan nulla polinom egy gyöke, és legyen $f(x) = (x - t_1)q_1(x)$. Ha q_1-nek van gyöke, és az mondjuk t_2, akkor a hozzá tartozó gyöktényező q_1-ből ugyanúgy kiemelhető, és ekkor

$$f(x) = (x - t_1)(x - t_2)q_2(x),$$

ahol q_2 már f-nél kettővel alacsonyabb fokú polinom. Az eljárást tovább folytathatjuk a q_2 polinommal, feltéve, hogy van gyöke. Mivel a $q_1, q_2, \dots$ polinomok foka egyre csökken, előbb vagy utóbb eljutunk az

$$f(x) = (x - t_1)(x - t_2)\cdots(x - t_k)q_k(x) \tag{3.5}$$

felíráshoz, ahol a q_k polinomnak már nincsen gyöke, ha másért nem, azért, mert az már nulladfokú. Könnyen látható, hogy ekkor $t_1, t_2, \dots, t_k$ mindegyike gyöke f-nek, és f-nek nincsenek további gyökei. Továbbá, az egyenlőség két oldalán a fokokat összehasonlítva kapjuk, hogy $k \leqslant \deg(f)$. Igaz tehát a következő állítás:

3.2. Tétel. *Minden nem azonosan nulla polinomnak legfeljebb annyi gyöke van, mint amennyi a foka.*

A teljesség kedvéért megemlítjük, hogy az azonosan nulla polinomnak T minden elemét gyökének tekintjük.

Ha a (3.5) gyöktényezős alakban a $t_1, t_2, \ldots, t_k$ gyökök között valamely t_i többször is előfordul, akkor azt mondjuk, hogy t_i *többszörös gyöke* f-nek. Pontosabban, ha t_i előfordulásainak száma s, akkor t_i-t f *s-szeres gyökének* mondjuk.

3.3. Tétel (Polinomok azonossági tétele)**.** *Ha két legfeljebb n-ed fokú polinom helyettesítési értékei több mint n különböző helyen megegyeznek, akkor a két polinom egyenlő.*

Bizonyítás. Ha az f és g polinomok b helyen vett helyettesítési értékei megegyeznek, akkor $f(b) = g(b)$, azaz $f(b) - g(b) = 0$. Ez utóbbit úgy is mondhatjuk, hogy b gyöke az $f - g$ polinomnak. Ha f és g helyettesítési értékei több, mint n különböző helyen megegyeznek, az azt jelenti, hogy az $f - g$ polinomnak több, mint n különböző gyöke van. De ha f és g legfeljebb n-ed fokú polinomok, akkor $f - g$ is az, így az előző tétel értelmében $f - g$-nek csak úgy lehet n-nél több gyöke, ha $f - g$ az azonosan nulla polinom, vagyis $f = g$. □

A tételből következik, hogy minden legfeljebb n-ed fokú polinom egyértelműen megadható az által, hogy megmondjuk $n + 1$ különböző helyen a helyettesítési értékét. Arról, hogy hogyan lehet megtalálni egy így megadott polinomot, a Numerikus módszerek című tantárgyban fog szó esni.

A fejezet zárásaként megemlítjük, hogy az egész számoknál látottakhoz hasonlóan értelmezhetnénk a polinomok körében is az oszthatóságot, majd a prímpolinomok, a legnagyobb közös osztó, a legkisebb közös többszörös fogalmait. Végül a számelmélet alaptételéhez hasonló egyértelmű prímfaktorizációs tételt is bizonyíthatnánk. Jóllehet ezt itt nem tesszük meg, de az egész számoknál az említett fogalmakat úgy vezettük be, hogy minden további nélkül általánosítható legyen akár polinomokra is (például a legnagyobb közös osztó fogalmában megkerültük a $\leqslant$ relációt, stb.). Az érdeklődő olvasó erről a témakörről például a [3] és az [5] művekből tájékozódhat.

3.4. Feladatok

3.1. Feladat. Adjon meg két negyedfokú polinomot, melyek összege másodfokú!

3.2. Feladat. Osszuk el maradékosan az f polinomot a g-vel!

a) $f(x) = 7x^4 + 2x^3 + 9x^2 + 5$ és $g(x) = x^3 - x + 1$

b) $f(x) = -x^3 + 2x^2 + x + 1$ és $g(x) = 2x^2 + 1$

3.3. Feladat. Ellenőrizze Horner-elrendezéssel, hogy a -3 gyöke-e az

$$f(x) = x^3 - 2x^2 - 11x + 12$$

polinomnak! Ha igen, emelje ki a hozzá tartozó gyöktényezőt!

3.4. Feladat. Végezze el Horner-elrendezés segítségével a

$$(2x^5 - 3x^2 + 5ix - 3) : (x - i)$$

polinomosztást!

3.5. Feladat. Határozza meg a c értékét úgy, hogy az $f(x) = 4x^3 - 3x^2 - x + c$ polinom helyettesítési értéke az $x = 1$ helyen 3 legyen!

3.6. Feladat. Általában hány összeadásra és szorzásra van szükség egy n-ed fokú polinom helyettesítési értékének kiszámításához a Horner-elrendezéssel?

3.7. Feladat. Adjon meg olyan harmadfokú polinomot, melynek a gyökei: $1, 2$ és i!

4. Algebrai egyenletek

Egyenlet alatt egy $F(x) = G(x)$ szimbólumot értünk, ahol F és G valamilyen függvényei x-nek, és ennek *megoldáshalmaza* alatt mindazon t-k halmazát értjük, melyek beletartoznak mind az F, mind a G függvény értelmezési tartományába, és fennáll rájuk az $F(t) = G(t)$ egyenlőség. Az egyenlet megoldáshalmazának elemeit az egyenlet *megoldásainak* nevezzük. Ha két egyenlet megoldáshalma megegyezik, akkor a két egyenletet *ekvivalensnek* mondjuk. Azokat az „eljárásokat”, melyeket egy adott egyenleten végrehajtva vele ekvivalens egyenletet kapunk, az egyenlet *ekvivalens átalakításainak* nevezzük. Egy egyenlet megoldásainak megkeresése általában úgy történik, hogy az egyenletet ekvivalens átalakítások egymásutánjával olyan egyenletre vezetjük vissza, amely megoldásainak megkeresése már kevesebb gondot jelent.

Mi most csak azzal az esettel foglalkozunk, amikor $F(x)$ is és $G(x)$ is komplex együtthatós polinomok, pontosabban polinomfüggvények. Ekkor az egyenlet mindkét oldalának ugyanazzal a nullától különböző komplex számmal való szorzása, valamint az egyenlet mindkét oldalához ugyanannak a polinomnak a hozzáadása nyilván ekvivalens átalakítások. Ez utóbbi segítségével az $F(x) = G(x)$ egyenlet $f(x) = 0$ alakra hozható, ahol $f(x)$ természetesen az $F(x) - G(x)$ polinom. Ha f legalább elsőfokú (komplex együtthatós) polinom, akkor az $f(x) = 0$ egyenletet *algebrai egyenletnek* nevezzük. Az *algebrai egyenlet fokán* az f polinom fokát értjük. Világos, hogy a t komplex szám pontosan akkor lesz megoldása az egyenletnek, ha t az f polinom gyöke, azaz $f(t) = 0$. Emiatt az egyenlet megoldásait az egyenlet *gyökeinek* is szokás nevezni.

A következő tétel garantálja, hogy minden algebrai egyenletnek van megoldása a komplex számok halmazában.

4.1. Tétel (Az algebra alaptétele)**.** *Minden legalább elsőfokú komplex együtthatós polinomnak van gyöke.*

A tétel és (3.5) szerint tehát az

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$$

komplex együtthatós legalább elsőfokú polinom felírható

$$f(x) = a_n (x - t_1)(x - t_2) \cdots (x - t_n) \tag{4.1}$$

alakban, ahol a $t_1, t_2, \ldots, t_n$ komplex számok az f gyökei. Az f polinom ezen alakját f *gyöktényezős alakjának* nevezzük. Az is világos, hogy $t_1, t_2, \ldots, t_n$ megoldásai az $f(x) = 0$ egyenletnek, és a 3.2. tétel szerint más megoldás nincs. Természetesen a $t_1, t_2, \ldots, t_n$ számok nem feltétlenül páronként különbözők, ami azt jelenti, hogy egy algebrai egyenlet megoldáshalmazának számosságáról csak annyit állíthatunk, hogy az nem lehet nagyobb az egyenlet fokánál. Az viszont igaz, hogy minden, legalább elsőfokú komplex együtthatós polinom pontosan annyi (nem feltétlenül különböző) elsőfokú polinom szorzatára bomlik, mint amennyi a polinom foka.

Az $(x - t_1)(x - t_2) \cdots (x - t_n)$ szorzatot kifejtve, egy olyan

$$b_0 x^n - b_1 x^{n-1} + \cdots + (-1)^{n-1} b_{n-1} x + (-1)^n b_n$$

polinomot kapunk, ahol:

$$\begin{aligned} b_0 &= 1; \\ b_1 &= t_1 + t_2 + \cdots + t_n; \\ b_2 &= t_1 t_2 + \cdots + t_1 t_n + t_2 t_3 + \cdots + t_{n-1} t_n; \\ &\vdots \\ b_n &= t_1 t_2 \cdots t_n. \end{aligned}$$

Szavakba öntve, a b_k számot úgy kapjuk, hogy a $t_1, t_2, \ldots, t_n$ gyökök közül kiválasztunk k darabot az összes lehetséges módon úgy, hogy egyet csak egyszer választunk, majd a kiválasztottakat összeszorozzuk, a kapott szorzatokat pedig összeadjuk. A (4.1) egyenlőség bal és jobb oldalán álló polinomok együtthatóit összevetve azt kapjuk, hogy

$$b_k = (-1)^k \frac{a_{n-k}}{a_n}.$$

Erre a képletre a *polinom gyökei és együtthatói közötti összefüggésként* szokás hivatkozni.

Ha például az $ax^2 + bx + c = 0$ másodfokú egyenlet megoldásai x_1 és x_2, akkor a fenti képletből a jól ismert

$$x_1 + x_2 = -\frac{b}{a} \qquad \text{és} \qquad x_1 \cdot x_2 = \frac{c}{a}$$

formulákat kapjuk.

4.1. Algebrai egyenletek megoldóképlete

A következőkben azt vizsgáljuk, hogyan lehet egy általános algebrai egyenlet megoldásait megtalálni. Egy algebrai egyenlet *megoldóképletén* olyan formulát értünk, amely a négy alapművelet és a gyökvonás segítségével az egyenlet együtthatóiból előállítja az összes megoldást. Például az $ax+b=0$ elsőfokú egyenlet esetén csupán kivonás és osztás segítségével megkapható az egyetlen megoldás:

$$x = -\frac{b}{a},$$

tehát ez a megoldóképlet.

4.1.1. Másodfokú algebrai egyenletek

A másodfokú egyenletek megoldóképletével már középiskolában is találkoztunk, ott azonban az egyenlet együtthatói valós számok voltak, és a képlet csak akkor működött, ha nem negatív számból kellett négyzetgyököt vonni.

Tekintsük most az

$$ax^2 + bx + c = 0$$

másodfokú egyenletet (itt a, b, c már komplex számok), és szorozzuk meg mindkét oldalát $4a$-val:

$$4a^2x^2 + 4abx + 4ac = 0.$$

A bal oldalon teljes négyzetté egészítést végezve kapjuk, hogy

$$(2ax + b)^2 - b^2 + 4ac = 0,$$

amiből

$$(2ax + b)^2 = b^2 - 4ac$$

adódik. Ebből látható, hogy $2ax + b$ a $D = b^2 - 4ac$ komplex szám valamely négyzetgyökével kell, hogy egyenlő legyen. Ha $D = 0$, akkor $2ax + b = 0$, így

$$x = -\frac{b}{2a}$$

az egyetlen megoldás, ha pedig $D \neq 0$, akkor a következő két megoldás létezik:

$$x_1 = \frac{-b+z}{2a} \qquad \text{és} \qquad x_2 = \frac{-b-z}{2a},$$

ahol z a D egyik négyzetgyöke.

Az $x^2 - 2x + 2 = 0$ egyenlet esetén például $D = (-2)^2 - 4 \cdot 1 \cdot 2 = -4$, a -4 egyik négyzetgyöke $2i$, így az egyenlet két megoldása

$$x_1 = \frac{2+2i}{2} = 1 + i \qquad \text{és} \qquad x_2 = \frac{2-2i}{2} = 1 - i,$$

melyek helyességéről visszahelyettesítéssel könnyedén meggyőződhetünk. Módszerünk természetesen olyan másodfokú egyenletek megoldására is alkalmas, melynek együtthatói nem valós komplex számok. Ilyen esetben a megoldások meghatározása nyilván több számolással jár.

4.1.2. Harmadfokú algebrai egyenletek

Ebben a részben az

$$ax^3 + bx^2 + cx + d = 0$$

harmadfokú egyenlet megoldását tűzzük ki célul. Első lépésben osszuk el az egyenlet mindkét oldalát a-val:

$$x^3 + \frac{b}{a}x^2 + \frac{c}{a}x + \frac{d}{a} = 0,$$

majd vezessük be az $y = x + b/3a$ új ismeretlent, vagyis írjunk x helyére $y - b/3a$-t! Ekkor a hatványozások és a lehetséges összevonások elvégzése után az

$$y^3 + \left(\frac{c}{a} - \frac{b^2}{3a^2}\right)y + \left(\frac{2b^3}{27a^3} - \frac{bc}{3a^2} + \frac{d}{a}\right) = 0.$$

egyenlethez jutunk. Látható, hogy ebben az egyenletben már nincsen másodfokú tag, így az

$$y^3 + py + q = 0 \tag{4.2}$$

alakba írható, ahol p és q az eredeti egyenlet együtthatóiból alapműveletek segítségével kifejezhető komplex számok. Elegendő tehát a (4.2) egyenletet megoldanunk, hiszen annak megoldásaiból $b/3a$ kivonásával megkaphatjuk az eredeti egyenlet megoldásait. Ha $q = 0$, akkor (4.2) bal oldalán y kiemelhető, és azt kapjuk, hogy a 0 és a $-p$ négyzetgyökei lesznek a megoldások. A $p = 0$ esetben pedig a megoldások pontosan a $-q$ köbgyökei. Marad tehát az az eset, amikor sem p, sem q nem nulla. Legyenek u és v tetszőleges komplex számok. Ekkor

$$(u + v)^3 = u^3 + 3u^2v + 3uv^2 + v^3,$$

ahonnan rendezés után

$$(u+v)^3 - 3uv(u+v) - (u^3+v^3) = 0$$

adódik. Összevetve ezt a (4.2) egyenlettel arra a következtetésre jutunk, hogy ha sikerülne az u és v komplex számokat megválasztani, hogy $-3uv = p$ és $-(u^3 + v^3) = q$ egyidejűleg teljesül, akkor $y = u+v$ a (4.2) egyenlet megoldása lenne. Az első egyenlet köbre emelése, majd rendezése, valamint a második egyenlet rendezése után az

$$\begin{aligned} u^3v^3 &= \left(-\frac{p}{3}\right)^3 \\ u^3+v^3 &= -q \end{aligned}$$

egyenletrendszerhez jutunk. A másodfokú egyenletek gyökei és együtthatói közötti összefüggés alapján elmondható, hogy a

$$z^2 + qz - \left(\frac{p}{3}\right)^3 = 0$$

olyan másodfokú egyenlet, melynek megoldásai pontosan u^3 és v^3. Nincs más hátra tehát, mint ezt a másodfokú egyenletet megoldani, majd a megoldásokból köbgyököt vonni. Ha w a $q^2 - 4(p/3)^3$ komplex szám egyik négyzetgyöke, akkor a másodfokú egyenletek megoldóképlete szerint

$$z_1 = u^3 = \frac{-q+w}{2} \qquad \text{és} \qquad z_2 = v^3 = \frac{-q-w}{2}.$$

Köbgyökvonás után u-ra is és v-re is 3-3 értéket kapunk, így a (4.2) egyenlet $y = u+v$ megoldására látszólag 9 komplex szám pályázik. Tudjuk, hogy 3-nál több megoldás nem lehet, ezért e 9 között biztosan vannak egybeesők. De így akár az is megtörténhetne, hogy az egybeesők száma már oly sok, hogy a módszer végül nem is adja meg (4.2) összes megoldásait. Ezen kérdések precíz tárgyalására a jegyzet keretei között nem vállalkozunk, csupán a végeredményt közöljük. Igazolható, hogy ha az u_1, u_2, u_3 komplex számok az u különböző köbgyökei, akkor

$$v_1 = -\frac{p}{3u_1}, \quad v_2 = -\frac{p}{3u_2}, \quad v_3 = -\frac{p}{3u_3},$$

választással az

$$y_1 = u_1 + v_1, \quad y_2 = u_2 + v_2, \quad y_3 = u_3 + v_3$$

komplex számok a (4.2) összes megoldásai.

A módszer elmélyítése érdekében oldjuk meg az

$$x^3 + 6x^2 + 6x - 13 = 0$$

egyenletet! Először végrehajtjuk az $x = y - 6/3 = y - 2$ helyettesítést, azaz tekintjük az

$$(y-2)^3 + 6\,(y-2)^2 + 6\,(y-2) - 13 = 0$$

egyenletet, melyből a hatványozások és a lehetséges összevonások elvégzése után az

$$y^3 - 6y - 9 = 0 \tag{4.3}$$

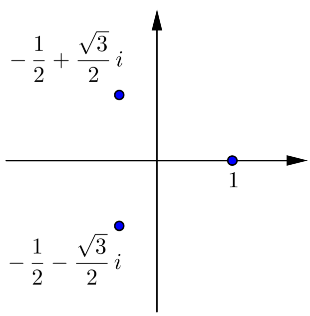
egyenlethez jutunk. A (4.2) jelöléseit követve most $p = -6$ és $q = -9$. A következő lépés a

$$z^2 - 9z - \left(\frac{-6}{3}\right)^3 = z^2 - 9z + 8 = 0$$

másodfokú egyenlet megoldása; a megoldások: $z_1 = 1$ és $z_2 = 8$. Igazából nekünk csak az egyik megoldásra van szükségünk, jobbanmondva annak a köbgyökeire. A 1 komplex köbgyökei, más szóval a harmadik egységgyökök pedig

$$u_1 = 1, \quad u_2 = -\frac{1}{2} + \frac{\sqrt{3}}{2}i, \quad u_3 = -\frac{1}{2} + \frac{\sqrt{3}}{2}i.$$

Innen



4.1. ábra. A harmadik egységgyökök

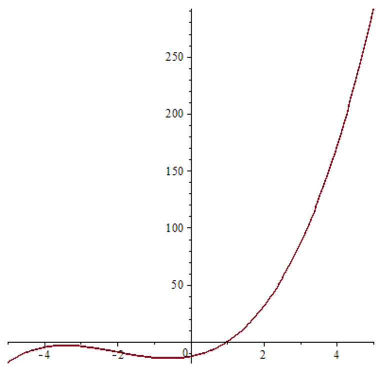
$$v_1 = -\frac{p}{3u_1} = -\frac{-6}{3 \cdot 1} = 2,$$
$$v_2 = -\frac{p}{3u_2} = -\frac{-6}{3\left(\frac{-1}{2} + \frac{\sqrt{3}}{2}i\right)} = \frac{4}{-1+\sqrt{3}i} = \frac{4(1-\sqrt{3}i)}{4} = -1-\sqrt{3}i,$$

és hasonlóan kapjuk, hogy $v_3 = -1 + \sqrt{3}i$. A (4.3) egyenlet megoldásai tehát

$$y_1 = u_1 + v_1 = 1 + 2 = 3,$$
$$y_2 = u_2 + v_2 = \left(-\frac{1}{2} + \frac{\sqrt{3}}{2}i\right) + \left(-1 - \sqrt{3}i\right) = -\frac{3}{2} - \frac{\sqrt{3}}{2}i,$$
$$y_3 = u_3 + v_3 = \left(-\frac{1}{2} - \frac{\sqrt{3}}{2}i\right) + \left(-1 + \sqrt{3}i\right) = -\frac{3}{2} + \frac{\sqrt{3}}{2}i,$$

és innen az eredeti egyenlet megoldásait úgy kapjuk, hogy mindegyikből kivonunk 2-t:

$$x_1 = 1, \quad x_2 = -\frac{7}{2} - \frac{\sqrt{3}}{2}i, \quad x_3 = -\frac{7}{2} + \frac{\sqrt{3}}{2}i.$$



4.2. ábra. Az $f\colon \mathbb{R} \to \mathbb{R}$, $f(x) = x^3 + 6x^2 + 6x - 13$ polinomfüggvény gráfja

4.1.3. Magasabb fokú egyenletek

A másod- és harmadfokú egyenletekhez hasonlóan negyedfokú egyenletekhez is lehetséges megoldóképletet konstruálni, ám annak bonyolultsága miatt inkább csak a megoldásokat a négy alapművelet és gyökvonás segítségével előállító algoritmust szokás közölni. Sajnos magasabbfokú egyenletek esetén már ez sem lehetséges.

4.2. Tétel (Ruffini-Abel-tétel)**.** *Ötöd, vagy annál magasabb fokú általános algebrai egyenletnek nincs megoldóképlete.*

Mit tehetünk mégis? Nyilván, ha az $f(x) = 0$ algebrai egyenlet bal oldalán álló f polinom az f_1 és f_2 polinomok szorzata, akkor az egyenlet összes megoldása megkapható az $f_1(x) = 0$ és $f_2(x) = 0$ egyenletek megoldásával. Ha a két tényező közül az egyik legalább elsőfokú, akkor az egyenlet megoldása így két alacsonyabb fokú egyenlet megoldására redukálható. Speciálisan, ha valahogyan sikerülne megsejtenünk az $f(x) = 0$ algebrai egyenlet egy t megoldását, akkor a hozzá tartozó gyöktényezőt kiemelve az $f(x) = (x - t) \cdot q(x)$ egyenlőséghez jutunk, így az $f(x) =$ $= 0$ egyenlet megoldását az eggyel alacsonyabb fokú $q(x) = 0$ egyenlet megoldására vezethetjük vissza. Mivel a q polinom előállítása akár a maradékos osztás elvégzésével, akár a Horner-elrendezéssel lehetséges, a kérdés már csak az, hogy hogyan sejthető meg az egyenlet egy megoldása. Erre csak speciális esetekben, a következő alfejezetben adunk választ.

4.2. Valós együtthatós egyenletek

Ebben a részben olyan algebrai egyenletekkel fogunk foglalkozni, melyek együtthatói valós számok. Először azt fogjuk megmutatni, hogy az ilyen egyenletek nem valós megoldásai „párosával” fordulnak elő.

4.3. Tétel. *Ha a t komplex szám megoldása az $f(x) = 0$ valós együtthatós egyenletnek, akkor $\overline{t}$ is az.*

Bizonyítás. Ha t megoldás, akkor $f(t) = 0$, melyből mindkét oldal konjugálásával kapjuk, hogy $\overline{f(t)} = 0$, azaz

$$\overline{a_n t^n + a_{n-1} t^{n-1} + \cdots + a_1 t + a_0} = 0.$$

Felhasználva, hogy összeg konjugáltja a konjugáltak összege, valamint szorzat konjugáltja a konjugáltak szorzata,

$$\overline{a_n}\,\overline{t}^n + \overline{a_{n-1}}\,\overline{t}^{n-1} + \cdots + \overline{a_1}\,\overline{t} + \overline{a_0} = 0$$

adódik. Az együtthatók most valós számok, azok konjugáltja pedig önmaga, így

$$a_n \overline{t}^n + a_{n-1} \overline{t}^{n-1} + \cdots + a_1 \overline{t} + a_0 = 0,$$

amely pontosan azt jelenti, hogy $\bar{t}$ gyöke az $f(x)$ polinomnak, azaz $f(\bar{t}) = 0$. $\square$

A tétel ismeretében vizsgáljuk fölül a legalább elsőfokú valós együtthatós f polinom (4.1) gyöktényezős alakját. Ha a t_i gyök egy valós szám, akkor a hozzá tartozó $x - t_i$ gyöktényező egy valós együtthatós elsőfokú polinom. Ha pedig t_i nem valós szám, akkor a tétel szerint t_i konjugáltja is ott van a gyökök között: legyen az mondjuk t_j. Ekkor a t_i-hez és t_j-hez tartozó gyöktényezők szorzata

$$(x - t_i)(x - t_j) = x^2 - (t_i + t_j)x + t_i t_j = x^2 - (t_i + \overline{t_i})x + t_i \overline{t_i},$$

ahol a konjugálás tulajdonságai szerint $t_i + \overline{t_i}$ és $t_i \overline{t_i}$ már valós számok. Tehát a két gyöktényező szorzata egy valós együtthatós másodfokú polinomot eredményez. Az eljárás megismételhető minden nem valós gyökpárra, így igaz a következő állítás.

4.4. Tétel. *Minden legalább elsőfokú $\mathbb{R}$ feletti polinom felírható első- és másodfokú $\mathbb{R}$ feletti polinomok szorzataként úgy, hogy a másodfokú polinomok egyikének sincs gyöke a valós számok halmazában.*

Ha az f valós együtthatós polinom páratlan fokú, akkor (4.1) szerint gyöktényezőinek száma is páratlan. Mivel a nem valós gyökökhöz tartozó gyöktényezők párokba rendezhetők, így lennie kell olyan gyöktényezőnek is, ami pár nélkül marad, más szóval létezik valós gyök.

4.5. Tétel. *Minden páratlan fokú valós együtthatós algebrai egyenletnek van valós megoldása (vagyis olyan megoldása, amely valós szám).*

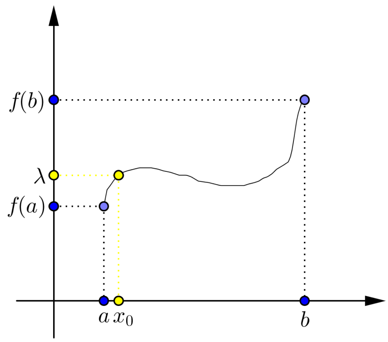
Ha jól meggondoljuk, ez az állítás következik az alábbi, kalkulusból ismert tételből is.

4.6. Tétel (Bolzano-tétel)**.** *Legyen $f\colon [a, b] \to \mathbb{R}$. Ha f folytonos, és $f(a) \neq f(b)$, akkor minden olyan λ valós számhoz, amely az $f(a)$ és az $f(b)$ által meghatározott nyílt intervallumban van, létezik olyan $x_0 \in]a, b[$, amelyre $f(x_0) = \lambda$.*

Nyilván, az f valós együtthatós polinomfüggvény folytonos, és ha f páratlan fokú, akkor $\lim_{x\to-\infty} f(x) = -\infty$ és $\lim_{x\to+\infty} f(x) = +\infty$ miatt vannak olyan a és b valós számok, hogy $f(a) < 0$ és $f(b) > 0$. Ekkor $\lambda = 0$ választással a Bolzano-tétel állítása pontosan az, hogy az f függvénynek van zérushelye az $]a, b[$ nyílt intervallumban, azaz az $f(x) = 0$ egyenletnek van ott megoldása.

4.7. Tétel (Racionális gyökteszt)**.** *Az*

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 = 0$$



4.3. ábra. A Bolzano-tétel szemléltetése

egész együtthatós algebrai egyenletnek az r racionális szám csak akkor megoldása, ha r felírható $\frac{u}{v}$ alakban, ahol u az a_0-nak, v pedig az a_n-nek osztója.

Bizonyítás. Minden r racionális szám felírható $\frac{u}{v}$ alakban, ahol u és v egész számok, $v \neq 0$, továbbá $\operatorname{lnko}(u, v) = 1$. Tegyük fel, hogy r megoldása a fenti egyenletnek, azaz

$$a_n\left(\frac{u}{v}\right)^n + a_{n-1}\left(\frac{u}{v}\right)^{n-1} + \cdots + a_1\frac{u}{v} + a_0 = 0.$$

Mindkét oldalt szorozva v^n-nel az

$$a_n u^n + a_{n-1}u^{n-1}v + \cdots + a_1 uv^{n-1} + a_0 v^n = 0$$

egyenlőséget kapjuk. Az egyenlőség jobb oldala osztható v-vel, így a bal oldal is. Ott viszont a másodiktól kezdődően minden tag osztható v-vel, így az elsőnek is oszthatónak kell lennie v-vel. Mivel a feltevés szerint u és v relatív prímek, ez csak úgy lehet, ha v osztója a_n-nek. Ugyanezt az analízist elvégezve az u-val való oszthatóságra, kapjuk, hogy u osztója kell legyen az a_0-nak. □

Megjegyezzük, hogy a racionális gyökteszt racionális együtthatós algebrai egyenletekre is alkalmazható, ugyanis az egyenlet mindkét oldalát a nevezők legkisebb közös többszörösével megszorozva vele ekvivalens egész együtthatós algebrai egyenletet kapunk.

Alkalmazva a racionális gyöktesztet az

$$x^4 - 2x^3 - x + 2 = 0$$

negyedfokú egyenlet racionális gyökeinek megkeresésére azt kapjuk, hogy ha az egyenletnek van racionális megoldása, akkor annak tovább nem egyszerűsíthető alakja csak olyan $\frac{u}{v}$ tört lehet, ahol $u \mid 2$ és $v \mid 1$. Tehát

$$u \in \{-2, -1, 1, 2\} \qquad \text{és} \qquad v \in \{-1, 1\},$$

melyből

$$\frac{u}{v} \in \{-2, -1, 1, 2\}$$

adódik. Hogy ezek közül melyik lesz valóban megoldás, arról a Horner-elrendezés segítségével győződünk meg:

	1	-2	0	-1	2	Megoldás?
-2	1	-4	8	-17	36	–
-1	1	-3	3	-4	6	–
1	1	-1	-1	-2	0	✓
2	1	0	0	-1	0	✓

Az egyenlet összes racionális megoldásai tehát az 1 és 2. Reménykedünk abban, hogy az olvasóban is felmerült az igény az egyenlet összes megoldásának megkeresésére. Ehhez először kiemeljük az $x-1$ és $x-2$ gyöktényezőket. Az $x-1$ kiemelése a fenti táblázat 1-hez tartozó sora segítségével történhet:

$$x^4 - 2x^3 - x + 2 = (x-1)(x^3 - x^2 - x - 2). \tag{4.4}$$

Az $x-2$ gyöktényező $x^3 - x^2 - x - 2$ harmadfokú polinomból történő kiemeléséhez egy újabb Horner-táblát készítünk:

	1	-1	-1	-2
2	1	1	1	0

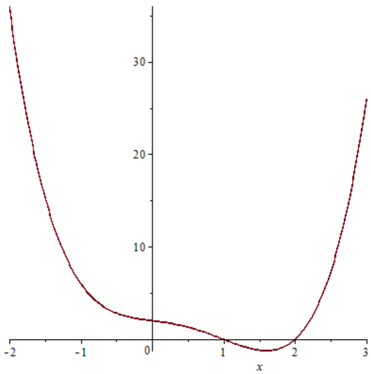
Innen következik, hogy

$$x^3 - x^2 - x - 2 = (x-2)(x^2 + x + 1),$$

melyet (4.4)-be helyettesítve végül

$$x^4 - 2x^3 - x + 2 = (x-1)(x-2)(x^2 + x + 1)$$

adódik. Az egyenlet további megoldásai tehát pontosan az $x^2+x+1 = 0$ másodfokú egyenlet megoldásai, melyek megkeresését már nyugodt szívvel bízzuk az olvasóra.

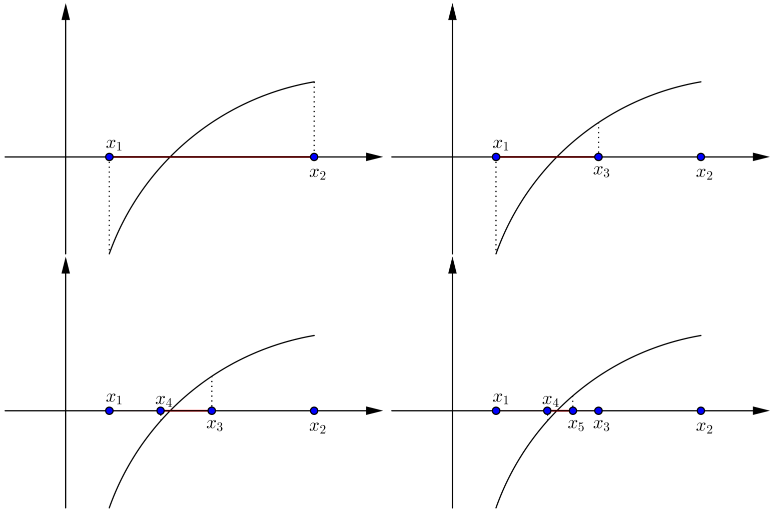


4.4. ábra. Az $f\colon \mathbb{R} \to \mathbb{R}$, $f(x) = x^4 - 2x^3 - x + 2$ polinom-függvény gráfja

4.2.1. Egy közelítő módszer

A fejezetet egy olyan módszer ismertetésével zárjuk, mely már nemcsak algebrai egyenletekre alkalmazható, hanem minden olyan $f(x) = 0$ egyenletre, ahol f egy $[a; b]$ intervallumon értelmezett, valós értékű, folytonos függvény. Ez a módszer már kivezet a diszkrét matematika tárgyköréből, célunk vele csupán példát adni arra, hogy céljaink elérése érdekében a diszkrét matematika és a kalkulus hogyan léptethető párbeszédbe.

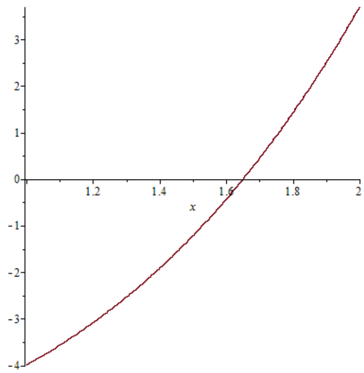
Keressünk olyan x_1 és x_2 pontokat az $[a; b]$ intervallumban, melyekre $f(x_1)$ és $f(x_2)$ előjele különböző. Ha nincsenek ilyen pontok, akkor az egyenletnek nyilván nincs megoldása az $[a, b]$ intervallumban. Ha vannak, akkor a Bolzano-tétel értelmében az x_1 és x_2 végpontú nyílt intervallum tartalmaz megoldást. Vegyük az intevallum felezőpontját: legyen $x_3 = \frac{x_1+x_2}{2}$. Az $f(x_3)$ előjele az $f(x_1)$ és $f(x_2)$ előjeleinek egyikétől biztosan különbözik, így a Bolzano-tétel szerint vagy az x_1 és x_3, vagy az x_2 és x_3 végpontú nyílt intervallumban van megoldása az egyenletnek, és ezen intervallum hossza fele az x_1 és x_2 végpontú intervallum hosszának. Megismételve az eljárást, az n-edik lépésben már egy $\frac{|x_1-x_2|}{2^{n-1}}$ hosszúságú intervallumot kapunk, amely biztosan tartalmazza az egyenlet egy megoldását. Világos, hogy ha n tart a végtelenbe, akkor az intervallumok hosszainak sorozata tart nullához, azaz az $\langle x_n \rangle$ sorozat az egyenlet egy megoldásához konvergál. Fontos megjegyezni, hogy ez az úgynevezett *intervallumfelezés módszere* véges sok lépésben általában nem



4.5. ábra. Az intervallumfelezéses eljárás első négy lépése

vezet pontos megoldáshoz, csak közelíti azt. Emiatt előírunk egy pontosságot, és az iterációt mindaddig végezzük, amíg a keletkező intervallum hossza (és ezáltal az intervallum bármely pontjának a pontos megoldástól való távolsága) kisebb nem lesz, mint az előírt pontosság.

Példaként keressünk az $f(x) = x^3 + \ln x - 5 = 0$ egyenletnek megoldását az $[1;2]$ intervallumon, 0,1 pontossággal! Mivel $f(1) = -4$ és $f(2) = 3{,}6931$, így valóban van megoldás az $]1;2[$ intervallumon. Legyen $x_1 = 1$, $x_2 = 2$ és x_3 pedig a felezőpont: $x_3 = 1{,}5$. Ekkor $f(1{,}5) = -1{,}2195$, és lévén $f(1{,}5)$ negatív, $f(2)$ pedig pozitív, így az $]1{,}5;2[$ intervallum biztosan tartalmazza az egyenlet egy megoldását. Legyen $x_4 = \frac{1{,}5+2}{2} = 1{,}75$ az $]1{,}5;2[$ intervallum felezőpontja. Most az $f(1{,}75) = 0{,}919$ előjelét figyelve megállapítható, hogy a $]1{,}5;1{,}75[$ intervallumban garantáltan van megoldás; az eljárást ennek az intervallumnak a felezésével folytatjuk: legyen $x_6 = \frac{1{,}5+1{,}75}{2} = 1{,}625$. Mivel $f(1{,}625) = -1{,}1944$, most újra az intervallum kezdőpontját cseréljük le: az $]1{,}625;1{,}75]$ lesz a megoldást biztosan tartalmazó intervallum. Ennek felezőpontja $x_7 = 1{,}6875$, és mivel $f(1{,}6875) = -0{,}7178$, így a megoldást tartalmazó intervallum az $]1{,}6875;1{,}75[$ nyílt intervallumra szűkül. Ennek az intervallumnak a hossza már kisebb, mint 0,1, így megállhatunk: az intervallum bármelyik pontja közelebb van az egyenlet egy megoldásához, mint 0,1.



4.6. ábra. Az $f\colon \mathbb{R} \to \mathbb{R}$, $f(x) = x^3 + \ln x - 5$ függvény gráfja az $[1; 2]$ intervallum fölött

4.3. Feladatok

4.1. Feladat. Oldjuk meg a komplex számok halmazán az alábbi egyenleteket!

a) $3x^2 - 2x + 1 = 0$

b) $x^2 + 2x + 5 = 0$

c) $x^2 + (-4 + 3i)x + 1 - 5i = 0$

d) $(2 + i)x^2 - (5 - i)x + 2 - 2i = 0$

e) $x^3 - 9x^2 + 18x + 28 = 0$

f) $x^3 - 3ix^2 + 3x - i = 0$

g) $x^3 - 6x + 4 = 0$

4.2. Feladat. Határozzuk meg a következő egyenletek racionális gyökeit!

a) $x^3 - 2x^2 + x - 2 = 0$

b) $2x^4 - 3x^2 + 5x - 4 = 0$

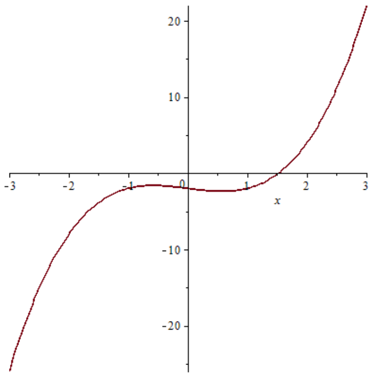
c) $x^4 - \frac{3}{2}x^3 + 3x^2 - 6x - 4 = 0$

4.3. Feladat. Oldja meg az alábbi egyenleteket a komplex számok halmazán!

a) $x^4 - 8x^3 + 18x^2 - 27 = 0$

a) $x^4 - 4x^3 - 8x + 32 = 0$

4.4. Feladat. Oldja meg az $x^3 - x - 2 = 0$ egyenletet algebrai és intervallum-felezéses módszerekkel, az utóbbinál 0,1 pontossággal! Hány további lépésre lenne még szükség a 0,01 pontosság eléréséhez? Segítségül megmutatjuk az $f\colon \mathbb{R} \to \mathbb{R}$, $f(x) = x^3 - x - 2$ polinomfüggvény gráfját (4.7. ábra).



4.7. ábra. Az $f\colon \mathbb{R} \to \mathbb{R}$, $f(x) = x^3 - x - 2$ polinomfüggvény gráfja

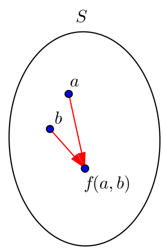
5. Algebrai struktúrák

Az előző fejezetekben gyakran előfordult, hogy bevezettünk valamilyen új objektumot (számot, polinomot, stb.), majd azokon műveleteket értelmeztünk. Ebben a fejezetben megpróbálunk az objektumoktól elvonatkoztatni, és csak a műveletekre, valamint azok tulajdonságaira koncentrálni.

Először azt tisztázzuk, mit is értünk műveleten. A matematikában műveletvégzéskor tulajdonképpen az történik, hogy egy halmazból veszünk két elemet (ettől lesz kétváltozós a művelet), és ahhoz hozzárendeljük ugyanazon halmaz valamely elemét. Az S nemüres halmazon értelmezett *kétváltozós műveleten* tehát egy

$$f\colon S \times S \to S$$

függvényt értünk. Ily módon az egész számok halmazán az összeadáson, a szor-



5.1. ábra. Az S halmazon értelmezett kétváltozós művelet S bármely két eleméhez egyértelműen hozzárendel egy szintén S-beli elemet

záson, és a kivonáson kívül művelet lesz például a legnagyobb közös osztó képzése is. De nem lesz művelet az osztás, hiszen az nem hajtható végre bármely két egész számmal. Megjegyezzük, hogy f helyett általában valamilyen „műveleti jelet" ($+, \cdot, \cup, \cap, \star, *, \dots$) írunk, és ekkor $f(a, b)$ helyett pedig az $a + b, a \cdot b, a \cup b, a \cap b, a \star b, a * b, \dots$ szimbólumot használjuk.

Az S halmazt a rajta értelmezett $f_1, f_2, \dots$ műveletekkel együtt *algebrai struktúrának* nevezzük, és erre az $(S, f_1, f_2, \dots)$ jelölést alkalmazzuk. Legutóbb például a $(T[x], +, \cdot)$ algebrai struktúrát ismertük meg, ahol $T[x]$ a T feletti (T alatt egyelőre még mindig a racionális, valós, vagy komplex számok halmazának valamelyikét értjük) összes polinomok halmazát jelöli, a $+$ és a $\cdot$ szimbólumok pedig a rajta értelmezett összeadást, illetve szorzást.

Azt mondjuk, hogy az S halmazon értelmezett $*$ művelet *asszociatív*, ha minden

$a, b, c \in S$ esetén

$$(a * b) * c = a * (b * c)$$

teljesül.

Asszociatív művelet például az összeadás és a szorzás az egész számok halmazán, az összeadás és a szorzás a polinomok halmazán, az összeadás és a szorzás a komplex számok halmazán, az unió egy nemüres halmaz hatványhalmazán, a függvények kompozíciója, stb. Viszont a kivonás az egész számok halmazán, az osztás a nemnulla valós számok halmazán, a vektoriális szorzás a 3 dimenziós euklideszi tér vektorain már nem asszociatív műveletek.

A következő tétel azt állítja, hogy asszociatív művelet esetén a zárójelezés szabadsága nemcsak három, hanem tetszőleges számú elemre fennáll.

5.1. Tétel. *Ha az S halmazon értelmezett $*$ művelet asszociatív, akkor véges sok elemen végrehajtott művelet eredménye független a zárójelezéstől.*

Bizonyítás. Legyen $n \geqslant 3$ és $a_1, a_2, \ldots, a_n \in S$, és legyen

$$A = (\ldots((a_1 * a_2) * a_3) * \cdots) * a_n,$$

továbbá jelölje az $a_1, a_2, \ldots, a_n$ elemeknek egy tetszőleges zárójelezés melletti műveleti eredményét B. Az n szerinti teljes indukcióval megmutatjuk, hogy $A = B$. Ez $n = 3$-ra az asszociativitás következménye. Most tegyük fel, hogy $n > 3$, és az állítás igaz minden háromnál nagyobb vagy egyenlő és n-nél kisebb természetes számra. Világos, hogy B felírható $C * D$ alakban, ahol C és D legfeljebb $n-1$ elem valamilyen zárójelezés melletti eredménye. Ha a D kifejezés csak az a_n elemet tartalmazza, akkor $B = C * a_n$, és az indukciós feltevést alkalmazva C-re $B = A$ adódik. Ha pedig D legalább 2 elemet tartalmaz, akkor az indukciós feltevés szerint $D = E * a_n$, ahol E-ben az elemek száma már csak legfeljebb $n-2$. Alkalmazva az asszociativitást, majd az indukciós feltevést $C * E$-re, kapjuk, hogy

$$B = C * D = C * (E * a_n) = (C * E) * a_n =$$
$$= (\ldots((a_1 * a_2) * a_3) * \cdots) * a_n = A.$$

□

Azt mondjuk, hogy az $(S, *)$ algebrai struktúra *félcsoport*, ha $*$ asszociatív. Ilyen például az $(\mathbb{N}, +)$ és az $(\mathbb{N}, \cdot)$, stb.

Legyen $*$ az S halmazon értelmezett művelet. Ha S-ben van olyan e elem, hogy $e * a = a$ és $a * e = a$ teljesülnek minden $a \in S$ esetén, akkor ezt az e elemet (a $*$ műveletre vonatkozó) *neutrális elemnek* nevezzük. Ha a művelet összeadás, akkor a neutrális elemet *zéruselemnek*, míg szorzás esetén *egységelemnek* is nevezzük. Például

– az $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ halmazokon értelmezett összeadás és szorzás neutrális elemei rendre a 0 és az 1;

– a T feletti polinomok körében értelmezett összeadás és szorzás neutrális elemei rendre az azonosan nulla polinom és az $f(x) = 1$ polinom;

– egy H halmaz hatványhalmaza felett értelmezett unió műveletének a neutrális eleme az üres halmaz;

– az egész számok körében értelmezett legnagyobb közös osztó műveletének neutrális eleme a 0.

Könnyen belátható, hogy egy algebrai struktúrában műveletenként legfeljebb egy neutrális elem lehet, ugyanis ha e és f is neutrális elemek volnának a $*$ műveletre nézve, akkor egyrészt $e * f = e$, másrészt $e * f = f$, melyekből a művelet eredményének egyértelműsége miatt $e = f$ következik.

Legyen $*$ az S halmazon értelmezett művelet, melyre vonatkozó neutrális elem az e. Azt mondjuk, hogy az S halmaz a elemének létezik inverze, ha van olyan $x \in S$, hogy $a * x = x * a = e$ teljesül. Ekkor az x elemet az a *inverzének* nevezzük és a^{-1}-nel jelöljük. Ha a művelet összeadás, akkor az a elem inverzét szokás $-a$ val is jelölni és az a *ellentettjének* nevezni. Ha a művelet a szorzás, akkor az inverz elemet gyakran *reciproknak* hívjuk.

A $(\mathbb{Z}, +)$ és $(\mathbb{Z}, \cdot)$ félcsoportok közül az elsőben a 2 inverze a -2, a másodikban azonban a 2 elemnek nem létezik inverze. Könnyű látni, hogy $(\mathbb{Z}, +)$ algebrai struktúrában minden elemnek van inverze, a $(\mathbb{Z}, \cdot)$-ban csak a -1 és 1 elemeknek létezik inverzük, és mindkettőnek az inverze önmaga.

5.2. Tétel. *Legyen $(S, *)$ neutrális elemmel rendelkező félcsoport. Ekkor:*

1. *S minden elemének legfeljebb egy inverze van.*

2. *Ha az $a \in S$-nek létezik inverze, akkor a^{-1}-nek is és $(a^{-1})^{-1} = a$.*

3. *Ha az a és b S-beli elemeknek létezik inverzük, akkor $a * b$-nek is és $(a * b)^{-1} = b^{-1} * a^{-1}$.*

Bizonyítás.

1. Tegyük fel, hogy b és c az a elem inverzei. Ekkor $b * a = a * b = e$ és $c * a = a * c = e$ és

$$c = c * e = c * (a * b) = (c * a) * b = e * b = b.$$

2. Mivel $a * a^{-1} = a^{-1} * a = e$, így a tényleg inverze a^{-1}-nek, és az előző pont értelmében nem létezik másik inverz.

3. Az asszociativitás miatt

$$\begin{aligned}(a * b) * (b^{-1} * a^{-1}) = a * ((b * b^{-1}) * a^{-1}) = \\ = a * (e * a^{-1}) = a * a^{-1} = e,\end{aligned}$$

és hasonlóan kapjuk azt is, hogy $(b^{-1} * a^{-1}) * (a * b) = e$. □

Az S halmazon értelmezett $*$ művelet *kommutatív*, ha minden $a, b \in S$ esetén

$$a * b = b * a.$$

Ahogy azt a következő tétel mutatja, a kommutativitás és asszociativitás együtt egy igen kényelmes számolási lehetőséget biztosít.

5.3. Tétel. *Kommutatív félcsoportban véges sok elemen végrehajtott művelet eredménye sem a zárójelezéstől, sem az elemek sorrendjétől nem függ.*

Bizonyítás. Nyilván, ha a műveletet véges sok elemen hajtjuk végre, abban bármely két szomszédos elem sorrendje felcserélhető, ugyanis az előző tétel miatt a zárójelezést irányíthatjuk úgy, hogy először a szóban forgó két elemen kelljen a műveletet elvégezni, majd arra a két elemre alkalmazhatjuk a kommutativitást. Mivel szomszédos elemek véges sokszori felcserélésével az elemek bármely sorrendjéhez el lehet jutni (lásd buborékrendezés), az állítás igaz. □

Azt mondjuk, hogy az $(S, *)$ algebrai struktúra *csoport*, ha $*$ asszociatív, S-nek van neutrális eleme és S minden elemének létezik inverze. Ha az $(S, *)$ csoportban $*$ kommutatív, akkor a csoportot *kommutatív csoportnak* vagy *Abel-csoportnak* nevezzük. Például a $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{Q} \setminus \{0\}, \cdot)$ (Miért kell kivenni a nullát?), $(T[x], +)$ algebrai struktúrák mindegyike Abel-csoport. Nemkommutatív csoportokra a későbbiekben fogunk példát mutatni.

Megjegyezzük, hogy az 5.2. tétel 3. része miatt egy neutrális elemmel rendelkező S félcsoport invertálható elemeinek halmaza csoportot alkot a félcsoport műveletére nézve. Ezt a félcsoport egységcsoportjának nevezzük, és $U(S)$-sel jelöljük. Például $U(\mathbb{Z}) = \{-1, 1\}$.

Könnyen látható, hogy ha csak a páros (2-vel osztható) egészek halmazát tekintjük, az szintén csoportot alkot az egész számok összeadására nézve, ugyanis két páros szám összege is páros, a 0 is páros, és minden páros szám ellentettje is páros. Legyen $(G, *)$ csoport és H egy részhalmaza a G-nek. Azt mondjuk, hogy H *részcsoportja G-nek*, ha $(H, *)$ is csoport, azaz H maga is csoportot alkot a G-beli csoportműveletre nézve. Mint az imént láttuk, a $(\mathbb{Z}, +)$ csoportnak a páros számok halmaza részcsoportja. Annak eldöntése, hogy egy részhalmaz részcsoport-e vagy sem, általában az alábbi tétel segítségével történik:

5.4. Tétel (Részcsoport-kritérium)**.** *A $(G, *)$ csoport H nemüres részhalmaza akkor és csak akkor részcsoport, ha $a^{-1} * b \in H$ bármely $a, b \in H$ esetén.*

Bizonyítás. Definíció szerint, ha H részcsoport, akkor bármely $a, b \in H$ esetén a^{-1}, továbbá $a^{-1} * b$ szintén elemei H-nak.

Fordítva, tegyük fel, hogy $a^{-1} * b \in H$ tetszőleges $a, b \in H$ esetén. A b helyett a-t választva kapjuk, hogy $e = a^{-1} * a$ is benne van a H-ban, és ha b helyett e-t írunk, akkor azt kapjuk, hogy $a^{-1} * e = a^{-1}$ is a H-ban van, tehát H minden elemének az inverze is H eleme. Ekkor viszont választhatunk a helyett a^{-1}-t, így $a * b \in H$ adódik, tehát $*$ művelet a H halmazon. Mivel az asszociativitás öröklődik G-ből, a bizonyítás készen van. □

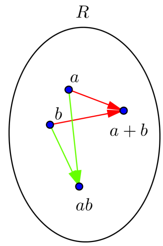
A következőkben olyan algebrai struktúrákkal foglalkozunk, melyekben már két kétváltozós művelet van. Az $(S, +, \cdot)$ algebrai struktúrát *gyűrűnek* nevezzük, ha a következő tulajdonságok mindegyike teljesül:

1. $(S, +)$ Abel-csoport;
2. minden $a, b, c \in S$ esetén

   $$a \cdot (b + c) = a \cdot b + a \cdot c \qquad \text{és} \qquad (b + c) \cdot a = b \cdot a + c \cdot a,$$

   azaz a szorzás az összeadásra nézve *mindkét oldalról disztributív.*

Megjegyezzük, hogy a gyűrűműveletek nem feltétlenül az összeadás és a szorzás kell, hogy legyenek, de mivel a legtöbb esetben mégis azok, nem tartottuk indokoltnak a definícióban absztrakt műveleti jelek használatát. Gyűrűk például a $(\mathbb{Z}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, $(T[x], +, \cdot)$ és a $(P(H), \triangle, \cap)$ algebrai struktúrák. Ez utóbbinál H egy nemüres halmaz, $P(H)$ a H hatványhalmaza, $\triangle$ pedig a halmazok szimmetrikus különbsége, azaz $A \triangle B = (A \setminus B) \cup (B \setminus A)$. Itt most a szimmetrikus különbség játssza az összeadás, míg a metszet pedig a szorzás szerepét.



5.2. ábra. Gyűrűben bármely két elem összege mellett azok szorzata is eleme a gyűrűnek

Teljes indukcióval könnyen bizonyítható, hogy egy gyűrű tetszőleges $a_1, \ldots, a_m$, $b_1, \ldots, b_n$ elemeire érvényes, hogy

$$\left(\sum_{i=1}^{m} a_i\right) \cdot \left(\sum_{j=1}^{n} b_j\right) = \sum_{i=1}^{m} \sum_{j=1}^{n} a_i \cdot b_j.$$

Azt mondjuk, hogy a gyűrű asszociatív, ha a $\cdot$ asszociatív; kommutatív, ha a $\cdot$ kommutatív; egységelemes, ha $(S, \cdot)$-nak van neutrális eleme.

A részcsoportokéhoz hasonlóan értelmezzük a részgyűrű fogalmát. Azt mondjuk, hogy az R gyűrű egy H részhalmaza *részgyűrűje R-nek*, ha maga is gyűrű az R-beli gyűrűműveletre nézve.

5.5. Tétel (Részgyűrű-kritérium)**.** *A $(R, +, \cdot)$ gyűrű H nemüres részhalmaza akkor és csak akkor részgyűrű, ha bármely $a, b \in H$ esetén $a - b$ és $a \cdot b$ is elemei H-nak.*

Részgyűrűje például a páros számok halmaza az egész számoknak, az egész számok a valós számoknak, a valós számok a komplex számoknak a szokásos műveletekre nézve.

Most az egész számok bizonyos részhalmazai segítségével konstruálunk újabb gyűrűket. Legyen m egy rögzített, egynél nagyobb egész szám, és legyen

$$\mathbb{Z}_m = \{0, 1, \ldots, m-1\}.$$

Definiáljuk a Z_m halmazon az összeadást és a szorzást a következőképpen: $a +_m b$, illetve $a \cdot_m b$ alatt az $a + b$, illetve ab egész m-mel való osztási maradékát értjük. Az egész számokra vonatkozó maradékos osztás tétele és annak következményei miatt $+_m$ és $\cdot_m$ műveletek a $\mathbb{Z}_m$ halmazon, sőt, $\mathbb{Z}_m$ kommutatív és asszociatív egységelemes gyűrű, melyet az *egész számok modulo m szerinti maradékosztály gyűrűjének* hívunk. Az 5.3. ábrán megmutatjuk $\mathbb{Z}_2$, az 5.4. ábrán pedig a $\mathbb{Z}_6$ összeadó- és szorzótábláját.

$+_2$	0	1
0	0	1
1	1	0

$\cdot_2$	0	1
0	0	0
1	0	1

5.3. ábra. $\mathbb{Z}_2$ összeadó- és szorzótáblája

$+_6$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

$\cdot_6$	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

5.4. ábra. $\mathbb{Z}_6$ összeadó- és szorzótáblája

Az $(R, +, \cdot)$ gyűrű egy nullától különböző a elemét *nullosztónak* nevezzük, ha van olyan nullától különböző $b \in R$, hogy $a \cdot b = 0$ vagy $b \cdot a = 0$. Az R gyűrű *nullosztómentes*, ha nem tartalmaz nullosztót.

Könnyű látni, hogy a $\mathbb{Z}_6$ gyűrűben $2 \cdot_6 3 = 0$, tehát a 2 és a 3 nullosztók. A kommutatív, asszociatív, egységelemes, nullosztómentes gyűrűket *integritás-tartományoknak* is nevezzük.

Emlékezzünk vissza, hogy a valós számok nullosztómentességét erősen kihasználtuk például az $x^3 - x = 0$ egyenlet megoldásakor. Ugyanis a bal oldalt szorzattá alakítva $x(x^2 - 1) = 0$ adódik, ahonnan, mivel a valós számok körében egy szorzat csak akkor 0, ha valamelyik tényezője 0, mondtuk, $x = 0$ vagy $x^2 - 1 = 0$ következik. A gondolatmenet helyessége abból következik, hogy ha egy R gyűrű valamely a elemének van inverze a szorzásra nézve, akkor az nem lehet nullosztó. Ugyanis ha a mégis nullosztó lenne, akkor lenne olyan $b \in R \setminus \{0\}$ elem, hogy $ab = 0$. Az egyenlet mindkét oldalát a^{-1}-nel balról megszorozva $b = 0$ adódik, ami ellentmondás. Mivel a valós számok körében minden nullától különböző elemnek van inverze, ezért $\mathbb{R}$ tényleg nem tartalmaz nullosztót.

Az $(R, +, \cdot)$ gyűrűt *testnek* nevezzük, ha $(R \setminus \{0\}, \cdot)$ Abel-csoport. A Komplex számok című fejezet elején tulajdonképpen azt igazoltuk, hogy az $\mathbb{R} \times \mathbb{R}$ halmaz a rajta bevezetett összeadással és szorzással testet alkot. Belátható az is, hogy $\mathbb{Z}_m$ pontosan akkor test, ha m prím.
Legyen T egy test, és T egységelemét jelölje 1. Azt a legkisebb n pozitív egész számot, melyre

$$\underbrace{1 + \cdots + 1}_{n \text{ db}} = 0,$$

a T *test karakterisztikájának* nevezzük. Ha nincs ilyen n, akkor azt mondjuk, hogy a T *test karakterisztikája nulla.* Világos, hogy a $\mathbb{Q}, \mathbb{R}$ és a $\mathbb{C}$ testek karakterisztikája 0, míg a $\mathbb{Z}_p$ test karakterisztikája p. A test nullosztómentességét kihasználva könnyen igazolható, hogy egy test karakterisztikája vagy 0, vagy prím.

Ha a T test egy részhalmaza maga is testet alkot a T-beli műveletekkel, akkor azt a részhalmazt T *résztestének* mondjuk.

A polinomok témakörén belül mindvégig rögzítve volt egy T számhalmaz, melyből a polinomok együtthatóit vettük. Ott azt mondtuk, hogy legyen T a $\mathbb{Q}, \mathbb{R}$ vagy $\mathbb{C}$ halmazok egyike. Most utólag már azt is mondhatnánk: legyen T egy test. Az olvasóra bízzuk annak ellenőrzését, hogy a Polinomok című fejezet állításai akkor is igazak maradnak, ha T alatt a fent felsoroltaktól különböző testet értünk.
Legyen most $T = \mathbb{Z}_2$, és tekintsük e fölött az $f(x) = x$ és a $g(x) = x^2$ polinomokat. Mivel a $\mathbb{Z}_2$ test összesen két elemet tartalmaz, az f-hez és g-hez tartozó polinomfüggvények az

$$f^*(0) = 0,\ f^*(1) = 1, \quad \text{és} \quad g^*(0) = 0^2 = 0,\ g^*(1) = 1^2 = 1$$

egyenlőségek által adottak. Ezzel a példával azt akarjuk érzékeltetni, hogy különböző polinomokhoz tartozhat ugyanaz a polinomfüggvény, tehát vannak olyan körülmények, amikor polinom és polinomfüggvény között különbséget kell tenni. Könnyű belátni, hogy $\mathbb{Z}_2$ felett végtelen sok polinom van (pl. $x, x^2, x^3, \dots$) de csak négy különböző polinomfüggvény.

Végül említést teszünk egy, az informatikában különösen fontos algebrai struktúráról. Az $(S, \cup, \cap)$ algebrai struktúrát *hálónak* nevezzük, ha az alábbi tulajdonságok mindegyike teljesül:

1. $(S, \cup)$ és $(S, \cap)$ kommutatív félcsoport,

2. teljesül a úgynevezett elnyelési törvény, azaz

$$a \cup (a \cap b) = a \quad \text{és} \quad a \cap (a \cup b) = a$$

fennállnak bármely $a, b \in S$-re.

Hálót alkot például a H nemüres halmaz összes részhalmazaiból álló $P(H)$ hatványhalmaz a halmazok uniójára és metszetére nézve. Sőt, ekkor az is elmondható, hogy mindkét műveletre nézve van neutrális elem ($\emptyset$ és H), mindkét művelet disztributív a másikra nézve, továbbá $P(H)$ minden eleméhez van olyan $\overline{A}$, szintén $P(H)$-beli elem (ez nem lesz más, mint az $H \setminus A$), melyre igaz, hogy $A \cup \overline{A} = H$ és $A \cap \overline{A} = \emptyset$. Az ilyen tulajdonságú hálót *Boole-algebrának* nevezzük, az $A \mapsto \overline{A}$ egyváltozós műveletet pedig komplementer-képzésnek.

5.1. Feladatok

5.1. Feladat. Igazolja, hogy tetszőleges nemüres H halmaz félcsoport az $a * b = b$ művelettel! Van-e mindig neutrális eleme?

5.2. Feladat. Igazolja, hogy $(\mathbb{Q}^+, *)$ félcsoport, ahol $\mathbb{Q}^+$ a pozitív racionális számok halmaza és

$$a * b = \frac{ab}{a+b}!$$

Van-e neutrális eleme?

5.3. Feladat. Csoport-e a $(\mathbb{Z}, *)$, ahol

$$a * b = \begin{cases} a + b & \text{ha } a \text{ páros,} \\ a - b & \text{ha } a \text{ páratlan?} \end{cases}$$

5.4. Feladat. Csoport-e a $(\mathbb{R} \setminus \{-1\}, *)$, ahol $a * b = a + b + ab$?

5.5. Feladat. Legyen c egy rögzített pozitív valós szám. Igazolja, hogy $(]-c, c[, *)$ csoport, ahol

$$a * b = \frac{a+b}{1 + \frac{ab}{c^2}}!$$

5.6. Feladat. Igazolja, hogy az

$$(A \cup B) \setminus C = (A \setminus C) \cup (B \setminus C) \quad \text{és} \quad C \setminus (A \cup B) = (C \setminus A) \cup (C \setminus B)$$

egyenlőségek közül az egyik igaz tetszőleges A, B és C halmazokra, a másik nem! Ez indokolja, hogy a gyűrű fogalmában a disztributivitást mindkét oldalról megköveteljük.

5.7. Feladat. Legyen H egy nemüres halmaz, és jelölje $P(H)$ a H összes részhalmazainak halmazát. Igazolja, hogy $P(H)$ gyűrű, ha az összeadás a szimmetrikus differencia, a szorzás pedig a metszetképzés!

5.8. Feladat. Írja fel $\mathbb{Z}_4$ és $\mathbb{Z}_5$ összeadó- és szorzótábláját! Keressen nullosztókat és invertálható elemeket ezekben a gyűrűkben!

5.9. Feladat. Mutassa meg, hogy minden kettőtől különböző karakterisztikájú testben az $x + x = 0$ egyenletnek az $x = 0$ az egyetlen megoldása!

5.10. Feladat. Igazolja, hogy $\{a + b\sqrt{5} \ : \ a, b \in \mathbb{Z}\}$ részgyűrűje $(\mathbb{R}, +, \cdot)$-nak!

5.11. Feladat. Vegyen egy tetszőleges négyelemű halmazt, majd vezessen be rajta olyan összeadást és szorzást, melyre nézve testet alkot!

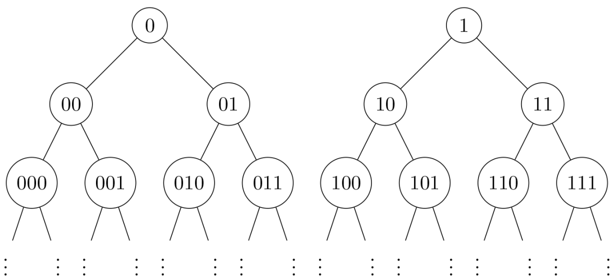
5.12. Feladat. Vezessen be a $H = \{0, 1\}$ halmazon két kétváltozós műveletet és egy komplementer-képzést úgy, hogy az így kapott algebrai struktúra Boole-algebra legyen!

6. Kombinatorikai alapok

Ebben a fejezetben a „hányféleképpen lehet” kezdetű kérdésekre keressük a választ.

6.1. Variáció, permutáció, kombináció

Jól ismert, hogy 1 biten két különböző állapot ábrázolható, jelölje ezeket 0 és 1. Egy bájt pedig 8 bitből áll. Hány különböző állapot ábrázolható egy bájton? A



6.1. ábra. Az 1 bájton ábrázolható összes állapotok

feladat egyszerű. A bájt első bitje 0 és 1 lehet, ez két lehetőség. Ugyanez igaz a második bitre is, így az első két biten ábrázolható különböző állapotok: 00, 01, 10 és 11. Folytatva a harmadik helyiértékkel, az előzőleg kapott elem után kerülhet 0 is és 1 is, ez 8 lehetőséget jelent. Folytatva az eljárást könnyen láthatjuk, hogy 8 biten $2^8 = 256$ különböző állapot ábrázolható. A probléma a következőképpen általánosítható:

Ha n darab különböző elemből kiválasztunk k darabot úgy, hogy a kiválasztás sorrendje számít, és egy elemet többször is kiválaszthatunk, akkor az *n elem egy k-ad osztályú ismétléses variációját* kapjuk.

A fenti példában mutatott módszerrel könnyedén igazolható, hogy n elem k-ad osztályú ismétléses variációinak száma:

$$V_{n,\mathrm{ism}}^{k} = n^k.$$

Egy jelenleg forgalomban lévő CD lemez tárolókapacitása 700 MB. Ez

$$t = 700 \cdot 1024 \cdot 1024 \cdot 8 = 5\,872\,025\,600$$

bit, melyen 2^t különböző állapot ábrázolható, vagy más szóval 2^t darab különböző tartalommal megírt CD lemez létezik. Érdekes belegondolni, hogy mi történne, ha ezt mind legyártanánk. Nagyrészt olyan lemezeket kapnánk, melyek tartalmát semmi nem tudná értelmezni, de köztük lenne a kedvenc lemezünk, és valamelyiken rajta lenne a jövő évszázad slágere is, melyet még meg sem írtak. Ennek a különös jelenségnek nyilván az az oka, hogy 2^t egy szokatlanul nagy szám.

Kicsit másabb, de hasonló gondolatmenettel kezelhető az a probléma, hogy hány különböző autó azonosítására alkalmas a Magyarországon jelenleg használatos, három betűből és három számból álló forgalmi rendszám, feltéve, hogy minden rendszám kiadható. Ha úgy vesszük, itt egy 6 hosszúságú karakter-sorozat előállítása a cél, melynek első, második és harmadik elemét 26 (az angol ábécé betűinek száma), a maradék hármat pedig 10 (a lehetséges számjegyek száma) lehetőség közül választhatjuk ki. Erre pedig $26^3 \cdot 10^3 = 17\,576\,000$ lehetőség van. Nyilván a 6, 26 és 10 számoknak nincs speciális jelentősége, így ismét próbálkozhatunk általánosítással. Ha kiválasztunk k darab elemet úgy, hogy az elsőt n_1, a másodikat n_2, és így tovább, a k-adikat n_k darab elem közül választhatjuk, akkor ezen k darab elem kiválasztására $n_1 n_2 \cdots n_k$ lehetőség van. Az elemek kiválasztásának sorrendje nyilván számít.

Ha n darab különböző elemből kiválasztunk k darabot úgy, hogy a kiválasztás sorrendje számít, és egy elemet csak egyszer választhatunk, akkor az n elem egy *k-ad osztályú ismétlés nélküli variációját* kapjuk.

Most meghatározzuk n elem k-ad osztályú ismétlés nélküli variációinak számát. Az első elemet n darab, a másodikat már csak a maradék $n-1$ elem közül választhatjuk ki. A harmadikra $n-2$, az utolsó, k-adik elem kiválasztására már csak $n-(k-1)$ lehetőségünk marad. Az eredmény tehát:

$$V_n^k = n(n-1)\cdots(n-(k-1)).$$

Az n nemnegatív egész *faktoriálisának* az

$$n! = \begin{cases} 1 & \text{ha } n \leqslant 1; \\ 1 \cdot 2 \cdot 3 \cdots n & \text{ha } n > 1 \end{cases}$$

egész számot nevezzük. Megjegyezzük, hogy $n!$ rekurzívan is értelmezhető az $(n+$ $+1)! = n!(n+1)$ és $0! = 1$ előírásokkal. Alkalmazva ezt a jelölést,

$$V_n^k = \frac{n!}{(n-k)!}.$$

Ha a kiválasztásnál mind az n darab elemet felhasználjuk (tehát $k = n$), akkor tulajdonképpen az n elem egy sorrendjéhez jutunk, amely nem más, mint az elemek kiválasztásának sorrendje.

n darab különböző elem egy rögzített sorrendjét az n darab elem egy (ismétlés nélküli) *permutációjának* nevezzük.

Az előbb elmondottak szerint n darab elem permutációinak száma:

$$P_n = V_n^n = n!.$$

Tehát egy 32 lapos magyarkártya-pakli megkeverésekor 32! különböző sorrend állhat elő, amely már egy 36 jegyű szám. Ha azonban olyan kártyajátékot játszunk, melyben csak a lapok színe számít, az értéke nem, akkor egy adott keverés után azonos színű lapok sorrendjének változtatásával a lapok egy másik, de a játék szempontjából az eredetivel lényegében azonos sorrendjét kapjuk. Négy szín van, mindegyik színből nyolc lap, így a lapok egy rögzített sorrendjéhez $8!8!8!8! = (8!)^4$ a játék szempontjából azonos sorrend rendelhető. Ekkor a játék szempontjából különböző sorrendek száma:

$$\frac{32!}{8!8!8!8!}.$$

Ha n darab elem között van $k_1, k_2, \ldots, k_m$ egymással megegyező, akkor ezen n darab elem egy rögzített sorrendjét az n darab elem egy $k_1, k_2, \ldots, k_m$ *típusú ismétléses permutációjának* nevezzük.

n darab elem $k_1, k_2, \ldots, k_m$ típusú ismétléses permutációinak száma:

$$P_n^{k_1, k_2, \ldots, k_m} = \frac{n!}{k_1! k_2! \cdots k_m!}.$$

Az eddigi feladatokban a kiválasztás sorrendje fontos volt. Van azonban, amikor ez nem számít. Például az ötöslottón lényegtelen, hogy milyen sorrendben húzzuk le a számokat, csak az a fontos, hogy pont arra az ötre tippeljünk, amit majd kihúznak. Az első elemet 90 közül, a másodikat a maradék 89-ből, és így tovább, az 5. számot már csak 86 közül választhatjuk, így az öt szám kiválasztására $V_{90}^5 =$ $= 90 \cdot 89 \cdot 88 \cdot 87 \cdot 86$ lehetőségünk van. Azonban ugyanazt az 5 számot $P_5 = 5! = 120$ sorrendben jelölhetjük meg, és ez nyilván ugyanazon tippnek számít, így ha biztos öttalálatost szeretnék, legalább

$$\frac{V_{90}^5}{P_5} = \frac{90 \cdot 89 \cdot 88 \cdot 87 \cdot 86}{5!} = \frac{90!}{5!85!} = 43\,949\,268$$

darab lottószelvény kitöltése szükséges.

Ha n darab különböző elemből kiválasztunk k darabot úgy, hogy a kiválasztás sorrendje nem számít, és egy elemet csak egyszer választhatunk (vagyis egy n elemű halmaznak kiválasztjuk egy k elemű részhalmazát), akkor az n elem egy *k-ad osztályú ismétlés nélküli kombinációját* kapjuk.

n elem összes k-ad osztályú ismétlés nélküli kombinációinak száma:

$$C_n^k = \frac{V_n^k}{P_k} = \frac{n!}{k!(n-k)!}.$$

Az $\frac{n!}{k!(n-k)!}$ szám jelölésére, ahol $0 \leqslant k \leqslant n$, az $\binom{n}{k}$ jelölést is használjuk, melyet „n alatt a k"-nak olvasunk. Ha pedig $0 \leqslant n < k$, akkor $\binom{n}{k}$ értékét 0-nak tekintjük, ami összhangban van azzal, hogy n különböző elem közül n-nél többet ismétlés nélkül nem lehet (0-féleképpen lehet) kiválasztani.

Adósok vagyunk még azzal az esettel, amikor egy elemet többször is kiválaszthatunk.

Ha n darab különböző elemből kiválasztunk k darabot úgy, hogy a kiválasztás sorrendje nem számít, és egy elemet többször is kiválaszthatunk, akkor az n elem egy *k-ad osztályú ismétléses kombinációját* kapjuk.

n elem k-ad osztályú ismétléses kombinációinak $C_{n,\mathrm{ism}}^k$ száma már nem kapható meg a fentiekhez hasonló, egyszerű okoskodással. Az általánosság nyilván nem sérül, ha azt feltételezzük, hogy az n darab elem, melyből választunk éppen az $1, 2, \ldots, n$ számok. Válasszunk ki ezekből k darabot úgy, hogy egy elem többször is szerepelhet! Jelölje a legkisebb kiválasztott elemet a_1, a következőt a_2, és így tovább, végül a legnagyobbat a_k! Ekkor

$$1 \leqslant a_1 \leqslant a_2 \leqslant a_3 \leqslant \cdots \leqslant a_k \leqslant n,$$

ahol az ismétlés miatt egyenlőség is előfordulhat. Továbbá, a

$$b_1 = a_1, \quad b_2 = a_2 + 1, \quad b_3 = a_3 + 2, \quad \ldots, \quad b_k = a_k + (k-1)$$

elemek között már nincsenek egyenlőek és

$$1 \leqslant b_1 < b_2 < b_3 < \cdots < b_k \leqslant n + k - 1,$$

tehát a $b_1, b_2, \ldots, b_k$ elemek tekinthetők úgy, mintha az $1, 2, \ldots, n+k-1$ elemek közül választottuk volna ki őket ismétlés nélkül. Az olvasó könnyen beláthatja, hogy ez a hozzárendelés megfordítható, azaz n darab elem minden k-ad osztályú ismétléses kombinációja $n+k-1$ darab elem pontosan egy k-ad osztályú ismétlés nélküli kombinációjához tartozik. Így

$$C^k_{n,\mathrm{ism}} = C^k_{n+k-1} = \binom{n+k-1}{k}.$$

A hanyag postás tehát, aki a szórólapok kiosztását esetlegesen végzi, 6 egyforma szórólapot 10 postaládába

$$C^6_{10,\mathrm{ism}} = C^6_{15} = \binom{15}{6} = 5005$$

-féleképpen tud elhelyezni, ugyanis mind a 6 szórólap elhelyezéséhez a 10 postaláda közül választ egyet, nem törődve azzal, hogy esetleg valamelyikbe többet is dob, így valóban 10 elem 6-od osztályú ismétléses kombinációjáról van szó.

6.2. Binomiális és polinomiális tétel

Az $(x+y)^2 = x^2 + 2xy + y^2$ azonosság jól ismert, és könnyen ellenőrizhető. Most képletet adunk $(x+y)^n$ kiszámítására tetszőleges n nemnegatív egész esetén. Világos, hogy $(x+y)^n$ olyan n tényezős szorzat, melynek minden tényezője $x+y$:

$$\underbrace{(x+y)(x+y)\cdots(x+y)}_{n \text{ darab tényező}}. \tag{6.1}$$

Ha alkalmazzuk a disztributivitást, és minden tagot minden taggal megszorzunk, az eredmény egy olyan összeg lesz, melynek minden tagja $x^k y^l$ alakú, ahol $k + l = n$. Most megszámoljuk, hány esetben kapjuk az $x^k y^{n-k}$ szorzatot. Ilyen tag úgy áll elő, ha (6.1) pontosan k darab tényezőjéből választunk x-et, a maradék $n-k$ tényezőből pedig az y-t, és azokat szorozzuk össze. n darab tényezőből k darabot pedig C^k_n-féleképpen választhatunk, ugyanis a szorzás kommutatív, és így a kiválasztás sorrendje nem számít. A következő tételt bizonyítottuk.

6.1. Tétel (Binomiális tétel)**.** *Legyenek x, y valamely T test elemei, és legyen n nemnegatív egész. Ekkor*

$$(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}.$$

A fenti formula magyarázatot ad arra, miért is nevezik az $\binom{n}{k}$ számokat binomiális együtthatóknak.

A binomiális tétel kiterjeszthető többtagú összeg hatványozására. Legyen $k \geqslant 2$ egész, és legyenek $x_1, x_2, \ldots, x_k$ valamely test elemei. Számítsuk ki az $(x_1 + x_2 + + \cdots + x_k)^n$ hatványt, ahol $n \geqslant 0$ egész! Ez egy n-tényezős szorzat:

$$(x_1 + x_2 + \cdots + x_k)^n = \underbrace{(x_1 + x_2 + \cdots + x_k) \cdots (x_1 + x_2 + \cdots + x_k)}_{n \text{ darab tényező}}. \tag{6.2}$$

A zárójelek felbontása után a tagok $x_1^{i_1} x_2^{i_2} \cdots x_k^{i_k}$ alakúak, ahol $i_1 + i_2 + \cdots + i_k = n$. Pontosan ezt a tagot kapjuk, ha (6.2) jobb oldalán álló szorzat n tényezője közül i_1-ből x_1-et választunk, a maradék $n - i_1$ tényező közül i_2-ből választunk x_2-t, és így tovább. Tehát összesen

$$\begin{aligned}
&\binom{n}{i_1}\binom{n-i_1}{i_2} \cdots \binom{n - i_1 - i_2 - \cdots - i_{k-1}}{i_k} = \\
&= \frac{n!}{i_1!(n-i_1)!} \frac{(n-i_1)!}{i_2!(n-i_1-i_2)!} \cdots \frac{(n-i_1-i_2-\cdots-i_{k-1})!}{i_k! \underbrace{(n-i_1-i_2-\cdots-i_k)!}_{=0!=1}} = \\
&= \frac{n!}{i_1! i_2! \cdots i_k!}
\end{aligned}$$

esetben kapjuk az $x_1^{i_1} x_2^{i_2} \cdots x_k^{i_k}$ tagot.

6.2. Tétel (Polinomiális tétel)**.** *Legyenek $k \geqslant 2$ és $n \geqslant 0$ egészek, és $x_1, x_2, \ldots, x_k$ valamely test elemei. Ekkor*

$$(x_1 + x_2 + \cdots + x_k)^n = \sum_{i_1 + i_2 + \cdots + i_k = n} \frac{n!}{i_1! i_2! \cdots i_k!} x_1^{i_1} x_2^{i_2} \cdots x_k^{i_k}.$$

A $k = 2$ estben nyilván a binomiális tételt láthatjuk viszont.

Példaként megnézzük $(a + b + c + d)^8$ esetén az $a^2 b c^3 d^2$ tag együtthatóját. A tétel szerint ez

$$\frac{8!}{2!1!3!2!} = 1680.$$

6.3. A binomiális együtthatók tulajdonságai

Most áttekintjük a binomiális együtthatók néhány alapvető tulajdonságát. Legyen n nemnegatív egész, és $0 \leqslant k \leqslant n$.

n elem közül k darabot úgy is kiválaszthatunk, hogy megmondjuk, melyik az az $n-k$ darab elem, melyet nem választunk. Erre reflektál az

$$\binom{n}{k} = \binom{n}{n-k} \tag{6.3}$$

egyenlőség, mely algebrai úton is könnyen igazolható:

$$\binom{n}{n-k} = \frac{n!}{(n-k)!(n-(n-k))!} = \frac{n!}{(n-k)!k!} = \frac{n!}{k!(n-k)!} = \binom{n}{k}.$$

Most vegyünk a meglévő n elemünkhöz egy újabb, $n+1$-edik elemet, és válasszunk ki belőle visszatevés nélkül $k+1$ elemet! Ez kétféleképpen történhet: vagy közte van az új elem a kiválasztottaknak (és k darab pedig az eredeti n elem közül való), vagy mind a $k+1$ elem a régiek közül való. Az elsőre C_n^k, a másodikra C_n^{k+1} lehetőségünk van. Kaptuk tehát, hogy $C_{n+1}^{k+1} = C_n^k + C_n^{k+1}$, azaz

$$\binom{n+1}{k+1} = \binom{n}{k} + \binom{n}{k+1}. \tag{6.4}$$

Ez az egyenlőség is nyilván bizonyítható algebrai úton: a bal oldal

$$\binom{n+1}{k+1} = \frac{(n+1)!}{(k+1)!(n+1-(k+1))!} = \frac{(n+1)!}{(k+1)!(n-k)!},$$

míg a jobb oldal

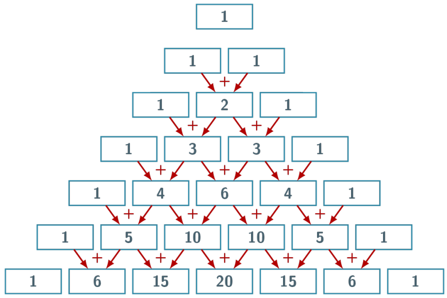
$$\binom{n}{k} + \binom{n}{k+1} = \frac{n!}{k!(n-k)!} + \frac{n!}{(k+1)!(n-(k+1))!},$$

melyből közös nevezőre hozás után

$$\begin{aligned}\binom{n}{k} + \binom{n}{k+1} &= \frac{n!(k+1) + n!(n-k)}{(k+1)!(n-k)!} = \\ &= \frac{n!(k+1+n-k)}{(k+1)!(n-k)!} = \frac{(n+1)!}{(k+1)!(n-k)!}\end{aligned}$$

adódik, tehát a bal és jobb oldalak közötti egyenlőség fennáll.

Felhasználva ezt a tulajdonságot, a binomiális együtthatók könnyen felírhatók a 6.2. ábrán látható háromszög alakú elrendezésben. A háromszög sorainak és a sorok elemeinek számozása nullával kezdődik, a nulladik sor csak az 1-et tartalmazza. A következő sorokban minden elem a felette balra és felette jobbra találha-



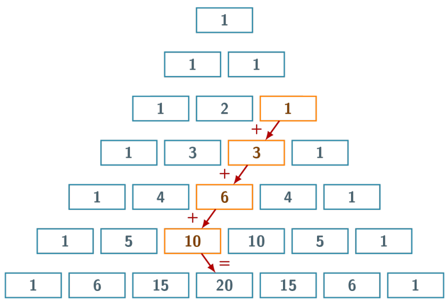
6.2. ábra. A Pascal-háromszög

tó két szám összege (a sor széleinél a hiányzó elemet nullának tekintjük). Például a második sorban az első szám $0 + 1 = 1$, a második szám pedig $1 + 1 = 2$. Az így szerkesztett háromszöget *Pascal-háromszögnek* nevezzük, mely n-edik sorának k-adik eleme éppen $\binom{n}{k}$. A (6.3) azonosság a Pascal-háromszög szimmetrikus tulajdonságára utal.

Az

$$\binom{n+1}{k+1} = \binom{n}{k} + \binom{n-1}{k} + \cdots + \binom{k}{k} \tag{6.5}$$

egyenlőség azt állítja, hogy a Pascal-háromszög $n+1$-edik sorának $k+1$-edik eleme a fölötte lévő sorok k-adik elemeinek összege. Bizonyítása (6.4) többszöri alkalma-



6.3. ábra. A (6.5) azonosság az $n = 5$, $k = 2$ esetben zásával könnyen elvégezhető:

$$\begin{aligned}\binom{n+1}{k+1} &= \binom{n}{k} + \binom{n}{k+1} = \\ &= \binom{n}{k} + \binom{n-1}{k} + \binom{n-1}{k+1} = \\ &\ \ \vdots \\ &= \binom{n}{k} + \binom{n-1}{k} + \dots + \binom{k}{k}.\end{aligned}$$

Végül bebizonyítjuk, hogy

$$\binom{n+1}{k+1} = \frac{n+1}{k+1}\binom{n}{k}.$$

Valóban,

$$\begin{aligned}\binom{n+1}{k+1} &= \frac{(n+1)!}{(k+1)!(n+1-(k+1))!} = \frac{n!(n+1)}{k!(k+1)(n-k)!} = \\ &= \frac{n+1}{k+1}\frac{n!}{k!(n-k)!} = \frac{n+1}{k+1}\binom{n}{k}.\end{aligned}$$

6.4. Feladatok

6.1. Feladat. Hány darab hatjegyű szám van a 10-es számrendszerben? Ebből hány darab nem osztható 10-zel?

6.2. Feladat. Egy lifthez 5 ember érkezik, de egyszerre csak 3 ember fér be. Hányféleképpen választhatjuk ki az első menet utasait?

6.3. Feladat. Egy 15 tagú klub elnököt, titkárt és jegyzőt választ. Hányféleképpen tehetik ezt meg? És ha Kovács úrnak mindenképp szeretnének valami tisztséget adni?

6.4. Feladat. Hányféleképpen ültethető le egy padra 10 gyerek? És egy kerekasztal köré? (Ez utóbbinál az egymásba forgatással átvihető ülésrendeket azonosnak tekintjük.)

6.5. Feladat. Hány különböző számsorozatot kapunk, ha tízszer dobunk egy kockával?

6.6. Feladat. 10 egyforma sört, 6 egyforma röviditalt és 9 egyforma üdítőt osztunk ki 25 ember között úgy, hogy mindenki pontosan egyvalamit kap. Hányféleképpen tehetjük ezt meg?

6.7. Feladat. Hány olyan hatjegyű szám van, melyben pontosan két számjegy azonos?

6.8. Feladat. Hány olyan hatjegyű szám létezik, amelyben van két azonos számjegy? És hány ilyen tizenötjegyű szám létezik?

6.9. Feladat. Hányféleképpen tölthető ki egy hatoslottó szelvény? Hány 5, 4 és 3 találatos kitöltés van?

6.10. Feladat. Egy 8 férfiból és 5 nőből álló társaságból hányféleképpen választhatunk 6 főt úgy, hogy legalább két nő legyen köztük?

6.11. Feladat. Ötfajta szeletelt csokit árulnak. Hányféleképpen vehetünk 12 szeletet?

6.12. Feladat. Egy 14 mérkőzéses TOTÓ első négy meccséről tudjuk, hogy biztosan nem végződhet döntetlennel. Legalább hány szelvényt kell kitölteni ahhoz, hogy biztosan legyen telitalálatos?

6.13. Feladat. Igazolja kombinatorikai megfontolással, hogy egy n elemű halmaznak 2^n darab részhalmaza van!

6.14. Feladat. A (6.5) összefüggés alapján adjon rekurzív formulát az $\binom{n}{k}$ binomiális együttható kiszámítására!

6.15. Feladat. A binomiális tétel alkalmazásával állapítsa meg, hogy a $(2x^2 + \frac{3}{x})^9$ kifejezésben, a hatványozás és a lehetséges összevonások elvégzése után, mi lesz az x^6 együtthatója!

6.16. Feladat. A hatványozás és a lehetséges összevonások elvégzése után mennyi lesz az $x^5y^2z^2$ tag együtthatója az $(x + 3y + 2z)^9$ kifejezésben?

6.17. Feladat. Igazolja, hogy a Pascal-háromszög n-edik sorában lévő számok összege 2^n! Útmutatás: a binomiális tételt alkalmazva számítsuk ki az $(1 + 1)^n$ hatványt!

6.18. Feladat. Igazolja, hogy a Pascal-háromszög n-edik sorában lévő számok váltakozó előjellel összeadva (pozitív előjellel kezdve) nullát eredményeznek!

6.19. Feladat. Legyen n nemnegatív egész, és $0 \leqslant k \leqslant m \leqslant n$. Igazolja, hogy

$$\binom{n}{m}\binom{m}{k} = \binom{n}{k}\binom{n-k}{m-k}!$$

7. Determinánsok

Ebben a fejezetben egy olyan fogalommal ismerkedünk meg, amely a továbbiakban hasznos algebrai segédeszköz lesz. Ehhez azonban a permutációk tulajdonságainak alaposabb ismerete szükséges.

7.1. Permutáció, mint bijektív leképezés

Legyen $M = \{1, 2, \ldots, n\}$, ahol $n \geqslant 1$ egész, és legyen $i_1, i_2, \ldots, i_n$ az $1, 2, \ldots, n$ számok egy permutációja. Ekkor az az f függvény, melyre

$$f(1) = i_1,\ f(2) = i_2,\ \ldots,\ f(n) = i_n,$$

az M halmaz egy önmagára való kölcsönösen egyértelmű leképezése. Például, ha $M = \{1, 2, 3, 4, 5\}$, akkor a $2, 5, 4, 1, 3$ sorrendhez tartozó $f\colon M \to M$ függvény a következő:

$$f(1) = 2,\ f(2) = 5,\ f(3) = 4,\ f(4) = 1,\ f(5) = 3,$$

melyet majd úgy fogunk jelölni, hogy

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 4 & 1 & 3 \end{pmatrix}.$$

A gondolatmenet megfordítható: ha f az M halmaz egy önmagára való kölcsönösen egyértelmű leképezése, akkor $f(1), f(2), \ldots, f(n)$ az $1, 2, \ldots, n$ elemek egy átrendezése, vagyis permutációja. Az $1, 2, \ldots, n$ számok helyett n darab különböző elemet tekintve bizonyítást nyert, hogy n különböző elem egy permutációja nem más, mint az n elemből álló halmaz egy önmagára való kölcsönösen egyértelmű leképezése.

Jelölje S_M az M halmaz összes permutációinak halmazát. Könnyen meggyőződhetünk arról, hogy $(S_M, \cdot)$ csoport, ahol a $\cdot$ művelet a leképezések kompozíciója. Ezt a csoportot az M halmaz *teljes transzformáció-csoportjának* nevezzük. Abban a speciális esetben, mikor $M = \{1, 2, \ldots, n\}$, *n-ed fokú szimmetrikus csoportról* beszélünk, melyet S_n-nel jelölünk. Mint fentebb már előrevetítettük, S_n egy f elemét a következő alakban fogjuk megadni:

$$f = \begin{pmatrix} 1 & 2 & \cdots & n \\ f(1) & f(2) & \cdots & f(n) \end{pmatrix}.$$

Az alábbi példa S_6 két elmének szorzását szemlélteti:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 5 & 6 & 1 & 3 & 4 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 3 & 2 & 4 & 5 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 6 & 5 & 1 & 3 & 2 \end{pmatrix}.$$

A szorzást – mint a leképezések szorzását – jobbról balra végezzük el: például a második permutáció az 1-hez a 6-ot, az első permutáció a 6-hoz a 4-et rendeli, ezért rendel a szorzat 1-hez 4-et.

Azt mondjuk, hogy az

$$f = \begin{pmatrix} 1 & 2 & \cdots & n \\ f(1) & f(2) & \cdots & f(n) \end{pmatrix}$$

permutációban *a k és l elemek inverzióban állnak*, ha $k < l$, de $f(k) > f(l)$. Jelölje $I(f)$ az f permutáció összes inverzióinak a számát. Azt mondjuk, hogy az f permutáció *páros*, ha $I(f)$ páros, egyébként f *páratlan*.

Például az

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 5 & 6 & 1 & 3 & 4 \end{pmatrix}$$

permutációban az 1 és 4, a 2 és 4, a 2 és 5, a 2 és 6, a 3 és 4, a 3 és 5, valamint a 3 és 6 elemek állnak inverzióban. Tehát $I(f) = 7$, így f páratlan permutáció.

Most megmutatjuk, hogy ha egy permutációban két elem képét felcseréljük, akkor a permutáció paritása az ellenkezőjére változik. Valóban, cseréljük fel az

$$f = \begin{pmatrix} 1 & \cdots & i & \cdots & j & \cdots & n \\ f(1) & \cdots & f(i) & \cdots & f(j) & \cdots & f(n) \end{pmatrix}$$

permutációban az i és a j képét. Ekkor a

$$g = \begin{pmatrix} 1 & \cdots & i & \cdots & j & \cdots & n \\ f(1) & \cdots & f(j) & \cdots & f(i) & \cdots & f(n) \end{pmatrix}$$

permutációhoz jutunk. A csere után az i és a j elemek egymás közötti inverziója biztosan megváltozik. Továbbá, könnyen látható, hogy az i elem inverziója egy i és j között lévő x számmal pontosan akkor változik meg (azaz ha nem voltak inverzióban, akkor abban lesznek, ha abban voltak, nem lesznek), ha az x és j közötti inverzió is megváltozik. Más inverziókban nem történik változás, így végül a változások száma páratlan. Páros permutációból tehát páratlan lesz, és fordítva.

Belátható, hogy az

$$I = \begin{pmatrix} 1 & 2 & \cdots & n \\ 1 & 2 & \cdots & n \end{pmatrix}$$

identikus permutációból kiindulva bármely permutációhoz eljuthatunk csak elempárok egymás utáni cseréjével. Például ha

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 4 & 1 & 3 \end{pmatrix},$$

akkor a

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix} \to \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 3 & 4 & 5 \end{pmatrix} \to \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 3 & 4 & 1 \end{pmatrix} \to$$
$$\to \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 4 & 3 & 1 \end{pmatrix} \to \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 4 & 1 & 3 \end{pmatrix}$$

cseresorozat alkalmas. Az identikus permutációban egyetlen inverzió sincs, így az páros. Mivel elemek cseréjekor a paritás ellentettjére változik, így páros permutációhoz páros számú elempár-cserével, míg páratlanhoz páratlan számú cserével juthatunk. Mi történik, ha két páros permutációt összeszorzunk? Mivel a permutációk szorzása leképezések egymás után való elvégzését jelenti, így páros számú elemcsere után még páros számú elemcserét végzünk, tehát a szorzat is páros lesz. Ugyanígy kapjuk, hogy páratlan permutációk szorzata is páros, ellentétes paritású permutáció szorzata pedig páratlan. Legyen f egy páros permutáció, és legyen f^{-1} az inverze. Ekkor $ff^{-1} = I$, I páros, tehát f^{-1}-nek is párosnak kell lennie. A fent leírtak igazolják, hogy a páros permutációk S_n-ben részcsoportot alkotnak.

7.2. Mátrixok értelmezése

Legyenek m és n adott pozitív egész számok, és legyenek a_{ij}, ahol $1 \leqslant i \leqslant m$ és $1 \leqslant j \leqslant n$, egy rögzített T test elemei. Az

$$A = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{bmatrix}$$

táblázatot $m \times n$ típusú (T test feletti) *mátrixnak* nevezzük. Ezek szerint egy $m \times$ $\times\, n$ típusú mátrix egy olyan táblázat, melyben T-beli elemek m számú sorban és n számú oszlopban vannak elrendezve. Például a

$$B = \begin{bmatrix} 1 & -3 & 0 & \pi \\ 2 & 7{,}5 & 83 & 11 \end{bmatrix}$$

táblázat tekinthető úgy, mint egy valós számok feletti 2×4 típusú mátrix.

Az $a_{11}, a_{22}, a_{33}, \ldots$ elemeket a mátrix *főátlójának*, az $a_{m1}, a_{m-1,2}, a_{m-2,3}, \ldots$ elemeket pedig a mátrix *mellékátlójának* mondjuk. A főátló tehát a bal felső sarokból indulva átlósan lefelé, a mellékátló pedig a bal alsó sarokból átlósan felfelé indulva járható be. A B mátrix főátlóját az 1 és a 7,5, míg mellékátlóját a 2 és -3 elemek alkotják.

Az A mátrix *transzponáltján* az

$$A^T = \begin{bmatrix} a_{11} & a_{21} & \cdots & a_{m1} \\ a_{12} & a_{22} & \cdots & a_{m2} \\ \vdots & \vdots & & \vdots \\ a_{1n} & a_{2n} & \cdots & a_{mn} \end{bmatrix}$$

$n \times m$ típusú mátrixot értjük, ami úgy is felfogható, mint az a mátrix, melyet az A mátrix sorainak és oszlopainak felcserélésével kapunk. Az előző példában szereplő B mátrix transzponáltja

$$B^T = \begin{bmatrix} 1 & 2 \\ -3 & 7{,}5 \\ 0 & 83 \\ \pi & 11 \end{bmatrix}.$$

Két mátrixot *egyenlőnek* tekintünk, ha azonos típusúak, és azonos indexű elemeik megegyeznek.

Az $n \times n$ típusú mátrixokat *négyzetes mátrixoknak* is nevezzük.

A fent leírt A mátrixot röviden úgy is írhatjuk, hogy $[a_{ij}]$, illetve $[a_{ij}]_{m \times n}$, ha a típusát is hangsúlyozni akarjuk, továbbá az i-edik sorának j-edik elemét néha $(A)_{ij}$-vel is jelöljük.

7.3. A determináns értelmezése

Vegyünk egy $n \times n$ típusú $A = [a_{ij}]$ mátrixot, és vegyük az S_n szimmetrikus csoport egy tetszőleges

$$f = \begin{pmatrix} 1 & 2 & \cdots & n \\ f(1) & f(2) & \cdots & f(n) \end{pmatrix}$$

elemét! Tekintsük az első sor $f(1)$-edik elemét: $a_{1f(1)}$, a második sor $f(2)$-edik elemét: $a_{2f(2)}$, és így tovább, végül az n-edik sor $f(n)$-edik elemét: $a_{nf(n)}$. Jól látszik, hogy minden sorból és minden oszlopból pontosan egy elemet vettünk. Szorozzuk ezeket az elemeket össze:

$$a_{1f(1)}a_{2f(2)}\cdots a_{nf(n)},$$

majd változtassuk a szorzat előjelét az ellentettjére, ha az f permutáció páratlan! Ha f páros, a szorzat változatlan marad. Ezen előjelkorrekció után a szorzatunk

$$(-1)^{I(f)}a_{1f(1)}a_{2f(2)}\cdots a_{nf(n)}$$

alakú. Készítsük el ezeket a szorzatokat S_n összes elemére, majd adjuk őket össze! Az így kapott összeget nevezzük az A mátrix determinánsának.

Precízebben: *determinánson* azt a T test feletti négyzetes mátrixok halmazán értelmezett, a T testbe képező det függvényt értjük, amely az

$$A = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{bmatrix}$$

mátrixhoz a

$$\det A = \sum_{f \in S_n} (-1)^{I(f)}a_{1f(1)}a_{2f(2)}\cdots a_{nf(n)}$$

elemet rendeli. A $\det A$ elemet az *A mátrix determinánsának* nevezzük. Még egyszer hangsúlyozzuk, hogy a determináns egy függvény, míg egy adott mátrix determinánsa a T test egy eleme (ami általában egy szám).

A $(-1)^{I(f)}a_{1f(1)}a_{2f(2)}\cdots a_{nf(n)}$ szorzatot az A mátrix determinánsa (f permutációhoz tartozó) *tagjának* nevezzük.

Könnyű belátni, hogy egy 1×1 típusú mátrix determinánsa definíció szerint nem más, mint a mátrix egyetlen eleme. Most megnézzük, hogyan számítható ki egy 2×2 típusú mátrix determinánsa. Legyen

$$A = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix}.$$

Az $1, 2$ elemeknek 2 permutációja van:

$$f_1 = \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix} \quad \text{és} \quad f_2 = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix};$$

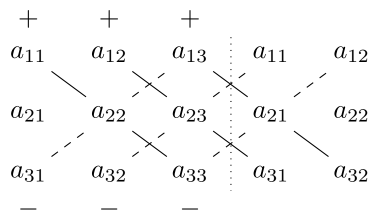
f_1 inverzióinak száma 0, míg f_2 inverzióinak száma 1, ezért az f_1-hez tartozó tag $(-1)^0 a_{11}a_{22} = a_{11}a_{22}$, az f_2-höz tartozó tag pedig $(-1)^1 a_{12}a_{21} = -a_{12}a_{21}$. Az A mátrix determinánsa ezek összege: $\det A = a_{11}a_{22} - a_{12}a_{21}$. Igazoltuk tehát, hogy egy 2×2 típusú mátrix determinánsát úgy is megkaphatjuk, hogy a főátlón lévő elemek szorzatából kivonjuk a mellékátlón lévő elemek szorzatát. Csupán a teljesség kedvéért álljon itt egy példa:

$$\det \begin{bmatrix} 3 & -2 \\ 1 & 5 \end{bmatrix} = 3 \cdot 5 - (-2) \cdot 1 = 17.$$

Legyen most

$$A = \begin{bmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{bmatrix}$$

egy adott 3×3 típusú mátrix. Az A determinánsának kiszámításához szükségünk van az S_3 csoportra, melynek elemeit az alábbi táblázat első oszlopa tartalmazza.



7.1. ábra. 3×3 típusú mátrix determinánsának kiszámítása

f	$I(f)$	$\det A$ f-hez tartozó tagja
$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$	0	$a_{11}a_{22}a_{33}$
$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$	1	$-a_{11}a_{23}a_{32}$
$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$	1	$-a_{12}a_{21}a_{33}$
$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$	2	$a_{12}a_{23}a_{31}$
$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$	2	$a_{13}a_{21}a_{32}$
$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$	3	$-a_{13}a_{22}a_{31}$

Az A mátrix determinánsa tehát a táblázat harmadik oszlopában lévő elemek összege:

$$\begin{aligned} \det A = a_{11}a_{22}a_{33} + a_{12}a_{23}a_{31} + a_{13}a_{21}a_{32} - \\ - a_{11}a_{23}a_{32} - a_{12}a_{21}a_{33} - a_{13}a_{22}a_{31}. \end{aligned} \tag{7.1}$$

Valószínűleg senkinek sem támadt kedve ezt a képletet fejben tartani. Van azonban egy módszer, mely segítségével a képlet könnyen rekonstruálható. Írjuk az A mátrix mellé az első két oszlopát még egyszer, majd adjuk össze a főátlón és a vele párhuzamos átlókon lévő elemek szorzatait, és ebből az összegből vonjuk ki a mellékátlón, és a vele párhuzamos átlókon lévő elemek szorzatait (lásd: 7.1. ábra)! Ekkor (7.1) szerint éppen az A mátrix determinánsát kapjuk.

Egy konkrét példa erre:

$$\det\begin{bmatrix}2 & -1 & 3\\ 1 & 4 & -2\\ 5 & 1 & -1\end{bmatrix} = 2\cdot 4\cdot(-1) + (-1)\cdot(-2)\cdot 5 + 3\cdot 1\cdot 1-$$
$$-\,3\cdot 4\cdot 5 - 2\cdot(-2)\cdot 1 - (-1)\cdot 1\cdot(-1) = -52.$$

Nagyon fontos, hogy az itt bemutatott módszerek csak 2×2, illetve 3×3 típusú mátrixokon működnek. Ha például egy 4×4 típusú mátrix determinánsát szeretnénk definíció szerint kiszámolni, akkor már az S_4 mind a $4! = 24$ eleme paritásának vizsgálata is elég fárasztó lenne. Ahhoz, hogy nagyobb mátrixok determinánsa is barátibb mennyiségű számolással elérhetővé váljon, a determinánst jobban meg kell ismernünk.

7.4. A determináns tulajdonságai

Ebben a részben mátrix alatt minden esetben egy T test feletti $n\times n$ típusú mátrixot értünk, konstanson pedig T egy tetszőleges elemét.

7.1. Tétel. *Transzponált mátrix determinánsa megegyezik az eredeti mátrix determinánsával.*

Bizonyítás. Tekintsük az $A = [a_{ij}]_{n\times n}$ és $B = [b_{ij}]_{n\times n}$ mátrixokat. Ekkor

$$\det A = \sum_{f\in S_n} (-1)^{I(f)} a_{1f(1)} a_{2f(2)} \cdots a_{nf(n)}$$

és

$$\det B = \sum_{g\in S_n} (-1)^{I(g)} b_{1g(1)} b_{2g(2)} \cdots b_{ng(n)}.$$

Tegyük fel, hogy $B = A^T$. Ekkor

$$\det A^T = \det B = \sum_{g\in S_n} (-1)^{I(g)} a_{g(1)1} a_{g(2)2} \cdots a_{g(n)n}.$$

Mivel transzponáláskor csupán sor-oszlop csere történik, a determináns értékének kiszámításakor pedig olyan szorzatokkal dolgozunk, melyhez minden sorból és oszlopból pontosan egy elemet veszünk, következik, hogy a $\det A^T$ kiszámításához használt összes szorzat megjelenik az A determinánsának kiszámításánál is. A kérdés csak az, hogy az előjelük ugyanaz marad-e. Tegyük fel, hogy az $a_{1f(1)}a_{2f(2)}\cdots a_{nf(n)}$ és $a_{g(1)1}a_{g(2)2}\cdots a_{g(n)n}$ szorzatok ugyanazokat a tényezőket tartalmazzák, csak más sorrendben. Keressük meg azt a j-t, melyre $g(j)=1$; ekkor $j=f(1)$ is teljesül. Végignézve ugyanezt a $2,\dots,n$ számokra is, láthatjuk, hogy az f és g permutációk egymás inverzei. Ekkor viszont a paritásuk megegyezik. $\square$

A tétel szerint tehát

$$\det\begin{bmatrix}1 & 2 & 3\\ 3 & -2 & 4\\ 1 & 1 & 2\end{bmatrix} = \det\begin{bmatrix}1 & 3 & 1\\ 2 & -2 & 1\\ 3 & 4 & 2\end{bmatrix},$$

melynek ellenőrzése az eddig elmondottak jó gyakorlása lehet az olvasó számára.

A fenti tétel értelmében a determináns kiszámításával kapcsolatos további tételekben a „mátrix sora” helyett mindig mondhatunk „mátrix oszlopát” is.

7.2. Tétel. *Ha egy mátrix egy sorának minden eleme nulla, akkor a mátrix determinánsa is nulla.*

Bizonyítás. A definícióból látszik, hogy ha egy sor minden eleme nulla, akkor a mátrix determinánsát adó összeg minden tagjában egy szorzótényező biztosan nulla. $\square$

7.3. Tétel. *Ha egy mátrix egy sorát úgy változtatjuk meg, hogy a sor elemeihez konstansokat adunk hozzá, akkor az így kapott mátrix determinánsa egyenlő az eredeti mátrix determinánsának, és azon mátrix determinánsának az összegével, melynek a szóban forgó sorába csak a hozzáadott konstansokat írjuk, a többi sort pedig* *változatlanul hagyjuk. Formálisan:*

$$\det\begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ \vdots & \vdots & & \vdots \\ a_{i1}+c_1 & a_{i2}+c_2 & \cdots & a_{in}+c_n \\ \vdots & \vdots & & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{bmatrix} =$$

$$= \det\begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ \vdots & \vdots & & \vdots \\ a_{i1} & a_{i2} & \cdots & a_{in} \\ \vdots & \vdots & & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{bmatrix} + \det\begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ \vdots & \vdots & & \vdots \\ c_1 & c_2 & \cdots & c_n \\ \vdots & \vdots & & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{bmatrix},$$

ahol a jobb oldalon lévő összeg második tagjában a $c_1, c_2, \ldots, c_n$ elemek az i-edik sorban vannak, és minden más sorban az eredeti elemek szerepelnek.

Bizonyítás. Írjuk fel az eredeti mátrix determinánsát, majd alkalmazzuk a disztributivitást:

$$\sum_{f\in S_n}(-1)^{I(f)}a_{1f(1)}\cdots(a_{if(i)}+c_{f(i)})\cdots a_{nf(n)} =$$
$$= \sum_{f\in S_n}(-1)^{I(f)}a_{1f(1)}\cdots a_{if(i)}\cdots a_{nf(n)}+$$
$$+ \sum_{f\in S_n}(-1)^{I(f)}a_{1f(1)}\cdots c_{f(i)}\cdots a_{nf(n)}.$$

□

7.4. Tétel. *Ha egy mátrix egy sorának minden elemét megszorozzuk ugyanazzal a c konstanssal, akkor a mátrix determinánsa is c-szeresére változik.*

Bizonyítás. Szorozzuk meg egy mátrix egy sorának minden elemét ugyanazzal a c konstanssal! Ekkor a mátrix determinánsának minden tagja pontosan c-szeresére változik, ugyanis a szóbanforgó sorból minden tag pontosan egy elemet tartalmaz. Az összegből c-t kiemelve a maradó rész nyilván az eredeti mátrix determinánsa. □

7.5. Tétel. *Ha egy mátrix két azonos sort tartalmaz, akkor a determinánsa nulla.*

Bizonyítás. Tegyük fel, hogy az $A = [a_{ij}]_{n\times n}$ mátrixban az i-edik és j-edik sorok megegyeznek. Tekintsük az A mátrix determinánsának egy adott f permutációhoz tartozó

$$a_{1f(1)} \cdots a_{if(i)} \cdots a_{jf(j)} \cdots a_{nf(n)}$$

tagját, így előjelkorrekció nélkül. Az i-edik és j-edik sorok egyenlősége miatt

$$a_{1f(1)} \cdots a_{if(i)} \cdots a_{jf(j)} \cdots a_{nf(n)} = a_{1f(1)} \cdots a_{jf(i)} \cdots a_{if(j)} \cdots a_{nf(n)},$$

és ez utóbbi szorzat pontosan a

$$g = \begin{pmatrix} 1 & \cdots & i & \cdots & j & \cdots & n \\ f(1) & \cdots & f(j) & \cdots & f(i) & \cdots & f(n) \end{pmatrix}$$

permutációhoz tartozó tag, előjelkorrekció nélkül. Mivel az f és g permutációk pontosan két elem képében térnek el, paritásuk ellentétes. Tehát két azonos sort tartalmazó mátrix determinánsának minden tagjához hozzárendelhető egy másik, hogy a kettő összege nulla, így a determináns maga is nulla. □

7.6. Tétel. *Ha egy mátrix egyik sora egy másik sorának konstansszorosa, akkor a mátrix determinánsa nulla.*

Bizonyítás. Használva az előző tételeket

$$\det \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ \vdots & \vdots & & \vdots \\ a_{i1} & a_{i2} & \cdots & a_{in} \\ \vdots & \vdots & & \vdots \\ ca_{i1} & ca_{i2} & \cdots & ca_{in} \\ \vdots & \vdots & & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{bmatrix} = c \cdot \det \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ \vdots & \vdots & & \vdots \\ a_{i1} & a_{i2} & \cdots & a_{in} \\ \vdots & \vdots & & \vdots \\ a_{i1} & a_{i2} & \cdots & a_{in} \\ \vdots & \vdots & & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{bmatrix} = 0$$

□

7.7. Tétel. *A determináns értéke nem változik, ha egy mátrix egy sorához hozzáadjuk egy másik sor konstansszorosát.*

Bizonyítás. Szintén az előző tételek következménye, hogy

$$\det \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ \vdots & \vdots & & \vdots \\ a_{i1} & a_{i2} & \cdots & a_{in} \\ \vdots & \vdots & & \vdots \\ a_{j1}+ca_{i1} & a_{j2}+ca_{i2} & \cdots & a_{jn}+ca_{in} \\ \vdots & \vdots & & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{bmatrix} =$$

$$= \det \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ \vdots & \vdots & & \vdots \\ a_{i1} & a_{i2} & \cdots & a_{in} \\ \vdots & \vdots & & \vdots \\ a_{j1} & a_{j2} & \cdots & a_{jn} \\ \vdots & \vdots & & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{bmatrix} + \det \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ \vdots & \vdots & & \vdots \\ a_{i1} & a_{i2} & \cdots & a_{in} \\ \vdots & \vdots & & \vdots \\ ca_{i1} & ca_{i2} & \cdots & ca_{in} \\ \vdots & \vdots & & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{bmatrix} =$$

$$= \det \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ \vdots & \vdots & & \vdots \\ a_{i1} & a_{i2} & \cdots & a_{in} \\ \vdots & \vdots & & \vdots \\ a_{j1} & a_{j2} & \cdots & a_{jn} \\ \vdots & \vdots & & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{bmatrix}$$

□

Ennek a tételnek majd fontos szerepe lesz az úgynevezett eliminációs módszerben. Emellett jól használható a mátrixban lévő „nagy" számok csökkentésére is a következő értelemben: ha az

$$A = \begin{bmatrix} 30 & 20 & 15 & 12 \\ 20 & 15 & 12 & 10 \\ 105 & 84 & 70 & 60 \\ 170 & 140 & 120 & 105 \end{bmatrix}$$

mátrix első oszlopából kivonjuk a másodikat (vagy ha úgy tetszik, a mátrix első oszlopához hozzáadjuk a második -1-szeresét), a második oszlopból kivonjuk a harmadikat, végül a harmadikból a negyediket, akkor az

$$A_1 = \begin{bmatrix} 10 & 5 & 3 & 12 \\ 5 & 3 & 2 & 10 \\ 21 & 14 & 10 & 60 \\ 30 & 20 & 15 & 105 \end{bmatrix}$$

mátrixot kapjuk, melynek determinánsa a fenti tétel értelmében megegyezik az A mátrixéval. A hatást tovább fokozhatjuk, ha az A_1 mátrix első oszlopából ismételten kivonjuk a másodikat, a másodikból a harmadikat, majd a negyedikből a harmadik négyszeresét, de ennek elvégzése már az olvasó feladata.

7.8. Tétel. *Ha egy mátrix két sorát felcseréljük, akkor a mátrix determinánsa előjelet vált.*

Bizonyítás. Vegyünk egy négyzetes mátrixot! Adjuk hozzá az i-edik sorhoz a j-ediket, majd a j-edik sorból vonjuk ki az i-ediket! Végül az i-edik sorhoz adjuk hozzá a j-ediket! A 7.6. és 7.7. tételek szerint

$$\det\begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ \vdots & \vdots & & \vdots \\ a_{i1} & a_{i2} & \cdots & a_{in} \\ \vdots & \vdots & & \vdots \\ a_{j1} & a_{j2} & \cdots & a_{jn} \\ \vdots & \vdots & & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{bmatrix} = \det\begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ \vdots & \vdots & & \vdots \\ a_{i1}+a_{j1} & a_{i2}+a_{j2} & \cdots & a_{in}+a_{jn} \\ \vdots & \vdots & & \vdots \\ a_{j1} & a_{j2} & \cdots & a_{jn} \\ \vdots & \vdots & & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{bmatrix} =$$

$$= \det\begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ \vdots & \vdots & & \vdots \\ a_{i1}+a_{j1} & a_{i2}+a_{j2} & \cdots & a_{in}+a_{jn} \\ \vdots & \vdots & & \vdots \\ -a_{i1} & -a_{i2} & \cdots & -a_{in} \\ \vdots & \vdots & & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{bmatrix} = \det\begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ \vdots & \vdots & & \vdots \\ a_{j1} & a_{j2} & \cdots & a_{jn} \\ \vdots & \vdots & & \vdots \\ -a_{i1} & -a_{i2} & \cdots & -a_{in} \\ \vdots & \vdots & & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{bmatrix} =$$

$$= -\det\begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ \vdots & \vdots & & \vdots \\ a_{j1} & a_{j2} & \cdots & a_{jn} \\ \vdots & \vdots & & \vdots \\ a_{i1} & a_{i2} & \cdots & a_{in} \\ \vdots & \vdots & & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{bmatrix}.$$

□

7.5. Kifejtési tételek

Egy $m \times n$ típusú mátrix egy *k-ad rendű aldeterminánsán* egy olyan $k \times k$ típusú mátrix determinánsát értjük, melyet az eredetiből úgy kapunk, hogy kiválasztunk k darab sort és k darab oszlopot, és vesszük a kiválasztott sorok és oszlopok metszéspontjain lévő elemeket. Az $n \times n$ típusú A mátrix *d aldeterminánshoz tartozó d^* komplementer aldeterminánsán* azon $(n-k) \times (n-k)$ típusú mátrix determinánsát értjük, melynek alkotóelemei nem szerepelnek a kijelölt sorokban illetve oszlopokban. Ha a kijelölt sorok illetve oszlopok indexei $i_1, \ldots, i_k$ és $j_1, \ldots, j_k$, akkor a *d-hez tartozó adjungált komplementer aldetermináns*

$$d^+ = (-1)^{i_1+\cdots+i_k+j_1+\cdots+j_k} d^*.$$

Például az

$$A = \begin{bmatrix} 2 & 0 & 0 & 3 \\ 1 & -1 & 3 & 4 \\ -3 & 2 & 1 & -5 \\ 1 & 1 & 2 & -1 \end{bmatrix}$$

mátrixban az 1. és 2. sorokat, valamint a 1. és 3. oszlopokat kiválasztva, azok metszéspontjain a

$$\begin{bmatrix} 2 & 0 \\ 1 & 3 \end{bmatrix}$$

mátrix keletkezik, melynek determinánsa 6. Ez tehát az A egy másodrendű aldeterminánsa. Az ehhez tartozó komplementer aldetermináns

$$\det \begin{bmatrix} 2 & -5 \\ 1 & -1 \end{bmatrix} = 3,$$

az adjungált komplementer aldetermináns pedig $(-1)^{1+2+1+3} \cdot 3 = -3$.

Talán sejthető, hogy egy négyzetes mátrix aldeterminánsaiból valahogyan előállítható kell legyen az eredeti mátrix determinánsa. Az alábbiakban azt nézzük meg, hogyan.

7.9. Lemma. *Tekintsünk egy $n \times n$ típusú A mátrixot és annak egy d k-ad rendű aldeterminánsát. Ha d egy tetszőleges tagját megszorozzuk d^+ egy tetszőleges tagjával, akkor* $\det A$ *egy tagját kapjuk.*

Bizonyítás. Először az $i_1 = 1, \ldots, i_k = k$ és $j_1 = 1, \ldots, j_k = k$ esetet tekintjük, vagyis amikor az aldeterminánshoz tartozó mátrix kiválasztásához az első k darab sort és oszlopot választjuk. Legyen $f \in S_n$ olyan permutáció, ami a $k+1, \ldots, n$ elemeket fixen hagyja. Ez nyilván felfogható mint egy S_k-beli permutáció, és d ehhez tartozó tagja

$$(-1)^{I(f)} a_{1f(1)} \cdots a_{kf(k)}$$

alakú. Hasonlóan, ha $g \in S_n$ az $1, \ldots, k$ elemeket hagyja fixen, akkor d^* g-hez tartozó tagja

$$(-1)^{I(g)} a_{k+1,g(k+1)} \cdots a_{ng(n)}$$

alakú, ami $(1 + \cdots + k) + (1 + \cdots + k)$ páros volta miatt éppen d^+-nak is tagja. A kettő szorzata

$$(-1)^{I(f)+I(g)} a_{1f(1)} \cdots a_{kf(k)} a_{k+1,g(k+1)} \cdots a_{ng(n)},$$

ami pontosan a $\det A$ fg permutációhoz tartozó tagja.

Tekintsük most az általános esetet, amikor a kiválasztott sorok és oszlopok $i_1, \ldots, i_k$ és $j_1, \ldots, j_k$ indexei tetszőlegesek. Ekkor az i_1 indexű oszlopot az összes őt megelőzővel megcserélve $i_1 - 1$ lépésben elérhetjük, hogy az első helyre kerüljön. Ugyanígy, az i_2 indexű oszlop $i_2 - 2$ oszlopcserével kerülhet a második helyre. Folytatva az eljárást az összes sorra és oszlopra,

$$t = (i_1 - 1) + \cdots + (i_k - k) + (j_1 - 1) + \cdots + (j_k - k)$$

számú sor- illetve oszlopcserével elérhetjük, hogy a kiválasztott aldetermináns a bal felső sarokban jelenjen meg. Ha B jelöli az így átrendezett mátrixot, akkor

$$\det A = (-1)^t \det B = (-1)^{i_1 + \cdots + i_k + j_1 + \cdots + j_k} \det B,$$

ahol a kitevőből a biztosan páros tagokat már elhagytuk. Ha α tagja d-nek, β pedig d^*-nak, akkor az előzőekben igazoltak miatt $\alpha\beta$ tagja $\det B$-nek és így

$$(-1)^{i_1 + \cdots + i_k + j_1 + \cdots + j_k} \alpha\beta$$

tagja $\det A$-nak. □

7.10. Tétel (Laplace-féle kifejtési tétel)**.** *Ha egy négyzetes mátrixból kiválasztunk k darab sort, és ezen sorok segítségével képezzük az összes k-ad rendű aldeterminánst, majd azokat mind megszorozzuk a saját adjungált komplementer aldeterminánsával, akkor ezen szorzatok összege éppen a mátrix determinánsa lesz.*

Bizonyítás. Ha veszünk egy k-ad rendű d aldeterminánst az A négyzetes mátrixból, akkor az előző lemma szerint d és d^+ tagjainak szorzatai tagjai $\det A$-nak. Ez $k!(n-k)!$ darab tagot jelent aldeterminánsonként. A kiválasztott k darab sor segítségével viszont

$$\binom{n}{k} = \frac{n!}{k!(n-k)!}$$

k-ad rendű aldetermináns képezhető, tehát összesen $n!$ tagot kapunk. Mivel ezek a tagok különbözőek, és mind tagjai a $\det A$-nak, az összegük nem lehet más, mint $\det A$. □

Ha a fenti A mátrix determinánsát a mátrix első két sora szerint fejtjük ki, a következőt kapjuk:

$$
\begin{aligned}
\det A = &\det \begin{bmatrix} 2 & 0 \\ 1 & -1 \end{bmatrix} \cdot (-1)^{1+2+1+2} \cdot \det \begin{bmatrix} 1 & -5 \\ 2 & -1 \end{bmatrix} + \\
&+ \det \begin{bmatrix} 2 & 0 \\ 1 & 3 \end{bmatrix} \cdot (-1)^{1+2+1+3} \cdot \det \begin{bmatrix} 2 & -5 \\ 1 & -1 \end{bmatrix} + \\
&+ \det \begin{bmatrix} 2 & 3 \\ 1 & 4 \end{bmatrix} \cdot (-1)^{1+2+1+4} \cdot \det \begin{bmatrix} 2 & 1 \\ 1 & 2 \end{bmatrix} + \\
&+ \det \begin{bmatrix} 0 & 0 \\ -1 & 3 \end{bmatrix} \cdot (-1)^{1+2+2+3} \cdot \det \begin{bmatrix} -3 & -5 \\ 1 & -1 \end{bmatrix} + \\
&+ \det \begin{bmatrix} 0 & 3 \\ -1 & 4 \end{bmatrix} \cdot (-1)^{1+2+2+4} \cdot \det \begin{bmatrix} -3 & 1 \\ 1 & 2 \end{bmatrix} + \\
&+ \det \begin{bmatrix} 0 & 3 \\ 3 & 4 \end{bmatrix} \cdot (-1)^{1+2+3+4} \cdot \det \begin{bmatrix} -3 & 2 \\ 1 & 1 \end{bmatrix} + \\
= &(-2) \cdot 9 + 6 \cdot (-1) \cdot 3 + 5 \cdot 3 + 0 + 3 \cdot (-1) \cdot (-7) + (-9) \cdot (-5) = 45.
\end{aligned}
$$

A negyedik összeadandó helyére azért írtunk csak 0-t, mert az aldeterminánst kiszámolva 0-t kaptunk, és ha egy szorzat egyik tényezője 0, akkor már a szorzat a további tényezőktől függetlenül 0. Ezáltal megkíméltük magunkat egy újabb 2×2 típusú mátrix determinánsának kiszámításától.

Gyakran előfordul, hogy a Laplace-féle kifejtési tételt csak egy sorra alkalmazzuk. Ezt a verziót külön tételként is szokás megemlíteni:

7.11. Tétel (Kifejtési tétel)**.** *Ha egy négyzetes mátrix egy sorának minden elemét megszorozzuk a hozzá tartozó adjungált komplementer aldeterminánssal, majd ezeket a szorzatokat összeadjuk, eredményül a mátrix determinánsát kapjuk.*

Bizonyítás. Mivel egy mátrix elsőrendű aldeterminánsai éppen a mátrix elemei, ez a tétel nem más, mint a Laplace-féle kifejtési tétel $k = 1$ esetén. □

Ha most az A mátrix determinánsát annak egy sora szerint szeretnénk kifejteni, akkor azt a sort célszerű választani, ami a legtöbb nullát tartalmazza, ugyanis a sor elemei determinánsok előtti szorzótényezőként jelennek meg, és amikor azok nullák, a hozzájuk tartozó determinánsok kiszámítása szükségtelenné válik. Tehát esetünkben a kifejtést az első sor szerint érdemes megtenni:

$$\det A = 2 \cdot (-1)^{1+1} \cdot \det \begin{bmatrix} -1 & 3 & 4 \\ 2 & 1 & -5 \\ 1 & 2 & -1 \end{bmatrix} + 0 + 0 + 3 \cdot (-1)^{1+4} \cdot \det \begin{bmatrix} 1 & -1 & 3 \\ -3 & 2 & 1 \\ 1 & 1 & 2 \end{bmatrix}.$$

A számolás befejezését (melynek lényegi része a két 3×3 típusú mátrix determinánsának valamilyen módszerrel való meghatározása) az olvasóra bízzuk.

A következő tétel pedig inkább elméleti jelentőségű.

7.12. Tétel (Ferde kifejtési tétel)**.** *Ha egy négyzetes mátrix egy sorának minden elemét megszorozzuk egy másik sor ugyanazon oszlopában lévő eleméhez tartozó adjungált komplementer aldeterminánssal, majd ezeket a szorzatokat összeadjuk, eredményül nullát kapunk.*

Bizonyítás. Szorozzuk meg az $A = [a_{ij}]_{n \times n}$ mátrix i-edik sorának minden elemét az i-től különböző j-edik sor megfelelő elemeihez tartozó adjungált komplementer aldeterminánsokkal, és legyen mindezek összege t; ekkor

$$t = a_{i1}A_{j1} + \cdots + a_{in}A_{jn},$$

ahol A_{jk} jelöli az a_{jk} elemhez tartozó adjungált komplementer aldeterminánst. Könnyen látható, hogy t értéke független a j-edik sor elemeitől. Írjuk a j-edik sor elemei helyére az i-edik sor elemeit, legyen az így kapott mátrix B. Ekkor t nem változik, és alkalmazva a kifejtési tételt a j-edik sorra, kapjuk, hogy $t = \det B$. De mivel B két azonos sort tartalmaz, $t = 0$ adódik, amit bizonyítani kellett. □

Még egyszer megjegyezzük, hogy mivel mátrixnak és transzponáltjának a determinánsa megegyezik, így a kifejtési tételekben is mondhatunk sor helyett oszlopot. Összefoglalva, a kifejtési tételek arra kínálnak lehetőséget, hogy egy $n \times n$ típusú mátrix determinánsára „kisebb” mátrixok determinánsaiból következtessünk. Segítségükkel a determináns függvény rekurzívan is megadható. Látható azonban, hogy „nagy” mátrixok determinánsának a kiszámítása még mindig nagyon sok számolást igényel.

7.6. A determináns értékének kiszámítása eliminációval

Egy négyzetes mátrixot *felső háromszögmátrixnak* nevezünk, ha főátlója alatt minden elem nulla:

$$\begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ 0 & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & a_{nn} \end{bmatrix},$$

azaz $a_{ij} = 0$ teljesül minden olyan esetben, amikor $i > j$; továbbá *alsó háromszögmátrixnak*, ha a főátlója felett minden elem nulla:

$$\begin{bmatrix} a_{11} & 0 & \cdots & 0 \\ a_{21} & a_{22} & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{bmatrix},$$

vagyis ha $a_{ij} = 0$ bármely $i < j$ esetén.

7.13. Tétel. *Ha egy mátrix felső vagy alsó háromszögmátrix, akkor determinánsa egyenlő a főátlón lévő elemek szorzatával.*

Bizonyítás. Mivel a felső háromszögmátrixok megkaphatók mint az alsó háromszögmátrixok transzponáltjai, a 7.1. tétel értelmében elég csak alsó háromszögmátrixokra igazolni az állítást. Alkalmazva a kifejtési tételt az első sorra

$$\det \begin{bmatrix} a_{11} & 0 & \cdots & 0 \\ a_{21} & a_{22} & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{bmatrix} = a_{11} \det \begin{bmatrix} a_{22} & 0 & \cdots & 0 \\ a_{32} & a_{33} & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ a_{n2} & a_{n3} & \cdots & a_{nn} \end{bmatrix},$$

ahonnan az eljárást ismételve kapjuk az állítást. □

Az eliminációs módszer lényege, hogy egy négyzetes mátrixon bizonyos átalakításokat végzünk, mígnem egy olyan felső háromszögmátrixot kapunk, melynek determinánsából következtethetünk az eredeti mátrix determinánsára. A felső háromszögmátrixszá alakítást oszloponként végezzük. Tekintsük először a mátrix első oszlopát! Ha abban minden főátló alatti elem nulla, akkor az már eleve olyan alakú, mint egy felső háromszögmátrix első oszlopa, tehát áttérhetünk a második oszlopra. Ha nem, akkor pedig sorcserével elérhető, hogy az első sor első eleme ne nulla legyen (nem biztos, hogy szükség van sorcserére, ha igen, ügyeljünk az előjelváltozásra, lásd: 7.8. tétel). Ekkor az első sor megfelelő konstansszorosait a második, harmadik, stb. sorokhoz hozzáadva elérhetjük, hogy az első oszlop második, harmadik, stb. eleme nulla legyen. Ekkor – a 7.7. tétel értelmében – a determináns értéke nem változik. Nézzük most a második oszlopot! Ha ebben a harmadiktól kezdődően minden elem nulla, akkor ez az oszlop formailag megfelel egy felső háromszögmátrix második oszlopának, így nincs semmi tennivalónk, folytathatjuk a 3. oszloppal. Ellenkező esetben esetleges sorcserével elérhető, hogy a második sor második eleme ne legyen nulla. (Ehhez a második sort csak az alatta lévő sorok valamelyikével érdemes cserélni, hiszen az első sorral felcserélve elrontanánk a sor első oszlopában előbb kialakított nullát.) Ezután a második sor megfelelő konstansszorosait hozzáadva a harmadik, negyedik, stb. sorokhoz elérhető, hogy a második oszlopban a főátló alatti elemek mind nullák legyenek. Hasonlóan folytatjuk az eljárást a harmadik, negyedik, majd legvégül az utolsó előtti oszloppal. A végeredmény egy olyan felső háromszögmátrix lesz, melynek determinánsa legfeljebb előjelben tér el az eredeti mátrix determinánsától.

Ez az algoritmus ebben a formában is korrekt, kézi végrehajtásakor azonban a számítás könnyítése érdekében még beiktathatunk néhány extra lépést.

A fejezet zárásaként kiszámítjuk az

$$A = \begin{bmatrix} 2 & 0 & 0 & 3 \\ 1 & -1 & 3 & 4 \\ -3 & 2 & 1 & -5 \\ 1 & 1 & 2 & -1 \end{bmatrix}$$

mátrix determinánsát eliminációs módszerrel is:

$$\det A = -\det \begin{bmatrix} 1 & -1 & 3 & 4 \\ 2 & 0 & 0 & 3 \\ -3 & 2 & 1 & -5 \\ 1 & 1 & 2 & -1 \end{bmatrix} = -\det \begin{bmatrix} 1 & -1 & 3 & 4 \\ 0 & 2 & -6 & -5 \\ 0 & -1 & 10 & 7 \\ 0 & 2 & -1 & -5 \end{bmatrix} =$$

$$= -\det \begin{bmatrix} 1 & -1 & 3 & 4 \\ 0 & 2 & -6 & -5 \\ 0 & 0 & 7 & 4{,}5 \\ 0 & 0 & 5 & 0 \end{bmatrix} = \det \begin{bmatrix} 1 & -1 & 4 & 3 \\ 0 & 2 & -5 & -6 \\ 0 & 0 & 4{,}5 & 7 \\ 0 & 0 & 0 & 5 \end{bmatrix} = 45.$$

Most pedig leírjuk, hogy az egyes lépésekben pontosan mit csináltunk.

1. A fentieket követve, először az első oszlop első elemével kellene az alatta lévőket eliminálni. Ehhez kényelmi okokból célszerű az első két sort felcserélni, ugyanis ekkor az első oszlop első eleme 1 lesz, melynek minden alatta lévő elem többszöröse (extra lépés!). Ekkor a determináns előjelet vált.

2. Kivonjuk az első sor kétszeresét a másodikból, hozzáadjuk az első sor háromszorosát a harmadikhoz, végül kivonjuk az első sort a negyedikből. Ekkor a determináns nem változik.

3. Az első oszloppal készen vagyunk, most a második oszlop főátló alatti elemeinek kinullázása következik. Itt most a következő két lehetőséget érdemes mérlegelni: vagy hozzáadjuk a 2. sor felét a harmadikhoz (ekkor törtek is megjelennek), és kivonjuk a második sort a negyedikből; vagy mint az első lépésben, először megcseréljük a második és a harmadik sorokat és utána eliminálunk. Mi az első mellett voksolunk, ekkor a determináns nyilván nem változik.

4. A harmadik oszlop következik, de ott az elimináció elkerülhető, ha megcseréljük a negyedik oszloppal. A determináns újra előjelet vált.

5. A jobb oldalon most már egy felső háromszögmátrix determinánsa áll, mely értéke a főátlón lévő elemek szorzata, azaz $1 \cdot 2 \cdot 4{,}5 \cdot 5$.

7.7. Feladatok

7.1. Feladat. Előfordulhat-e, hogy egy csupa egész számokat tartalmazó négyzetes mátrix determinánsa nem egész szám? Válaszát indokolja!

7.2. Feladat. Az $[a_{ij}]_{6\times 6}$ mátrix determinánsában milyen előjellel szerepelnek az

a) $a_{23}a_{31}a_{42}a_{56}a_{14}a_{65}$

b) $a_{32}a_{43}a_{14}a_{51}a_{66}a_{25}$

szorzatok?

7.3. Feladat. Számítsa ki az alábbi mátrixok determinánsait:

$$A = \begin{bmatrix} 2 & 3 \\ 1 & 4 \end{bmatrix}, \qquad B = \begin{bmatrix} 2 & 1 \\ -1 & 2 \end{bmatrix}, \qquad C = \begin{bmatrix} \sin x & \cos x \\ -\cos x & \sin x \end{bmatrix},$$

$$D=\begin{bmatrix}1+\sqrt{2} & 2-\sqrt{3}\\ 2+\sqrt{3} & 1-\sqrt{2}\end{bmatrix},\qquad E=\begin{bmatrix}1 & 1 & 1\\ -1 & 0 & 1\\ -1 & -1 & 0\end{bmatrix},\qquad F=\begin{bmatrix}0 & 1 & 1\\ 1 & 0 & 1\\ 1 & 1 & 0\end{bmatrix},$$

$$G=\begin{bmatrix}1 & -2 & 3\\ 2 & -4 & 1\\ 3 & -5 & 2\end{bmatrix}!$$

7.4. Feladat. Mi a kapcsolat az A és B mátrixok determinánsa között?

$$A=\begin{bmatrix}a_{11} & a_{12} & a_{13}\\ a_{21} & a_{22} & a_{23}\\ a_{31} & a_{32} & a_{33}\end{bmatrix}\qquad B=\begin{bmatrix}2a_{11} & 3a_{12} & 5a_{13}\\ 2a_{21} & 3a_{22} & 5a_{23}\\ 2a_{31} & 3a_{32} & 5a_{33}\end{bmatrix}$$

7.5. Feladat. Hogyan változik egy mátrix determinánsa, ha a sorait fordított sorrendben írjuk fel?

7.6. Feladat. Hogyan változik egy mátrix determinánsa, ha minden elemét ugyanazzal a konstanssal szorozzuk?

7.7. Feladat. Határozza meg x értékét, ha

$$\det\begin{bmatrix}1 & 1 & 1 & 1\\ 1 & 1-x & 1 & 1\\ 1 & 1 & 2-x & 1\\ 1 & 1 & 1 & 3-x\end{bmatrix}=0!$$

7.8. Feladat. Számítsa ki az alábbi mátrixok determinánsait kifejtés segítségével!

$$A=\begin{bmatrix}0 & 0 & 5 & 1\\ 0 & 0 & 6 & 2\\ 5 & 6 & 7 & 3\\ 1 & 2 & 3 & 4\end{bmatrix},\quad B=\begin{bmatrix}8 & 6 & 0 & 0 & 0\\ 1 & 8 & 6 & 0 & 0\\ 0 & 1 & 8 & 6 & 0\\ 0 & 0 & 1 & 8 & 6\\ 0 & 0 & 0 & 1 & 8\end{bmatrix},\quad C=\begin{bmatrix}2 & -1 & 1 & 7 & 2\\ 0 & 2 & 0 & 2 & 0\\ 1 & 1 & 1 & 3 & 1\\ 0 & 2 & 0 & -2 & 0\\ 3 & 3 & 2 & 1 & 1\end{bmatrix}.$$

7.9. Feladat. Számítsa ki az

$$A=\begin{bmatrix}4 & 6 & 4 & 4\\ 2 & 1 & 0 & 0\\ 0 & 3 & 1 & 3\\ 2 & 2 & 3 & 5\end{bmatrix}$$

mátrix determinánsát eliminációs módszerrel!

7.10. Feladat. Határozza meg az alábbi $n \times n$ típusú mátrixok determinánsait!

$$A = \begin{bmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & 0 & 1 & \cdots & 1 \\ 1 & 1 & 0 & \cdots & 1 \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & 1 & 1 & \cdots & 0 \end{bmatrix}$$

$$V = \begin{bmatrix} 1 & 1 & 1 & \cdots & 1 \\ a_1 & a_2 & a_3 & \cdots & a_n \\ a_1^2 & a_2^2 & a_3^2 & \cdots & a_n^2 \\ \vdots & \vdots & \vdots & & \vdots \\ a_1^{n-1} & a_2^{n-1} & a_3^{n-1} & \cdots & a_n^{n-1} \end{bmatrix}$$

A V mátrix determinánsa (*Vandermonde-determináns*) mikor egyenlő nullával?

8. Műveletek mátrixokkal

Most az előző fejezetben bevezetett mátrixok körében értelmezünk műveleteket. Először az összeadást, mely csak azonos típusú mátrixokkal végezhető el: az $A = [a_{ij}]_{m\times n}$ és $B = [b_{ij}]_{m\times n}$ *mátrixok összegén* azt az $A + B = [c_{ij}]_{m\times n}$ mátrixot értjük, melyre $c_{ij} = a_{ij} + b_{ij}$ minden $1 \leqslant i \leqslant m$ és $1 \leqslant j \leqslant n$ esetén. Az $A + B$ mátrix kiszámításához tehát a megfelelő indexű elemeket kell összeadni. Például:

$$\begin{bmatrix} 1 & -2 \\ 2 & 4 \\ -3 & 5 \end{bmatrix} + \begin{bmatrix} 0 & 3 \\ -1 & 2 \\ -3 & -3 \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 6 \\ -6 & 2 \end{bmatrix}.$$

Különböző típusú mátrixok összegét nem értelmezzük.

Jelölje $\mathcal{M}_{m\times n}(T)$ az összes T test feletti $m \times n$ típusú mátrixok halmazát. A fenti definíció szerint $+$ művelet az $\mathcal{M}_{m\times n}(T)$ halmazon, és mivel a mátrixok összege a T testbeli összeadásra van visszavezetve, $+$ asszociatív és kommutatív. A zéruselem az az $m \times n$ típusú mátrix, melynek minden eleme nulla (*zérómátrix*), és az $A = [a_{ij}]_{m\times n}$ mátrix ellentettje az a $B = [b_{ij}]_{m\times n}$ mátrix, melyre $b_{ij} = -a_{ij}$ minden $1 \leqslant i \leqslant m$ és $1 \leqslant j \leqslant n$ esetén. Tehát $(\mathcal{M}_{m\times n}(T), +)$ Abel-csoport.

Kicsit komplikáltabb lesz a mátrixok szorzása. Először is, az A és B mátrixok AB szorzatát csak akkor értelmezzük, ha az A mátrix oszlopainak száma megegyezik a B mátrix sorainak számával. Ekkor, ha az A mátrixból kiválasztunk egy sort (mondjuk az i-ediket), a B mátrixból pedig egy oszlopot (legyen ez a j-edik), akkor ennek a sornak és oszlopnak pontosan ugyanannyi eleme van. Szorozzuk ezt a sort és oszlopot oly módon össze, hogy az első elemet az elsővel, a másodikat a másodikkal, és így tovább, végül az utolsót az utolsóval. Ezen szorzatok összege lesz a szorzatmátrix i-edik sorának j-edik eleme (8.1. ábra). Ugyanez precízen: az $A = [a_{ij}]_{m\times n}$ és $B = [b_{ij}]_{n\times k}$ *mátrixok szorzatán* azt az $AB = [c_{ij}]_{m\times k}$ mátrixot értjük, melyre

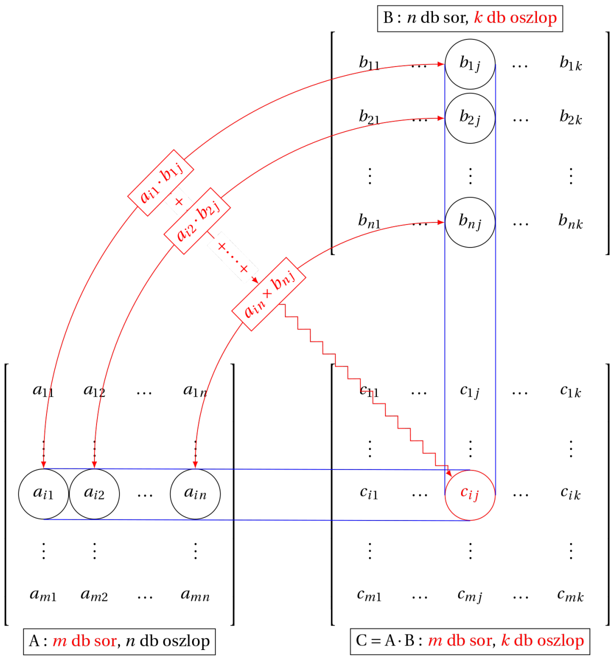
$$c_{ij} = a_{i1}b_{1j} + a_{i2}b_{2j} + \cdots + a_{in}b_{nj}$$

minden $1 \leqslant i \leqslant m$ és $1 \leqslant j \leqslant k$ esetén.

Legyenek

$$A = \begin{bmatrix} 1 & 2 & 0 \\ -1 & 3 & 4 \end{bmatrix} \quad \text{és} \quad B = \begin{bmatrix} 2 & 1 \\ -3 & 2 \\ -5 & 7 \end{bmatrix}.$$

Az AB szorzat kiszámításának talán legszemléletesebb módszere, amikor a két



8.1. ábra. Mátrixok szorzása

mátrixot egy táblázatba helyezzük a következőképpen:

			2	1
			-3	2
			-5	7
1	2	0		
-1	3	4		

A beírt mátrixok sorait illetve oszlopait elválasztó vonalak behúzása után kirajzolódó négyzetrács szépen mutatja, hogy a szorzat egy 2×2 típusú mátrix lesz, amely

– első sorának első eleme: $1 \cdot 2 + 2 \cdot (-3) + 0 \cdot (-5) = -4$,

– első sorának második eleme: $1 \cdot 1 + 2 \cdot 2 + 0 \cdot 7 = 5$,

– második sorának első eleme: $(-1) \cdot 2 + 3 \cdot (-3) + 4 \cdot (-5) = -31$,

– második sorának második eleme: $(-1) \cdot 1 + 3 \cdot 2 + 4 \cdot 7 = 33$.

Tehát

$$AB = \begin{bmatrix} -4 & 5 \\ -31 & 33 \end{bmatrix}.$$

Az alábbi állítás következménye, hogy $(\mathcal{M}_{n\times n}(T), \cdot)$ félcsoport.

8.1. Tétel. *Ha $A = [a_{ij}]_{m\times n}$, $B = [b_{ij}]_{n\times k}$ és $C = [c_{ij}]_{k\times l}$, akkor*

$$(AB)C = A(BC).$$

Bizonyítás. A mátrixszorzás definíciója szerint az AB szorzat létezik, és $m \times k$ típusú, és ekkor az $(AB)C$ szorzat is létezik, mely egy $m\times l$ típusú mátrix. Ugyanígy látható be, hogy az $A(BC)$ szorzat is létezik, ami szintén egy $m \times l$ típusú mátrix. Most megmutatjuk, hogy ez a két mátrix elemenként megegyezik. Valóban, felhasználva, hogy T test,

$$\begin{aligned}
((AB)C)_{ij} &= \sum_{u=1}^{k}(AB)_{iu}(C)_{uj} = \sum_{u=1}^{k}\left(\sum_{v=1}^{n}(A)_{iv}(B)_{vu}\right)(C)_{uj} \\
&= \sum_{u=1}^{k}\sum_{v=1}^{n}((A)_{iv}(B)_{vu})(C)_{uj} = \sum_{u=1}^{k}\sum_{v=1}^{n}(A)_{iv}((B)_{vu}(C)_{uj}) \\
&= \sum_{v=1}^{n}\sum_{u=1}^{k}(A)_{iv}((B)_{vu}(C)_{uj}) = \sum_{v=1}^{n}(A)_{iv}\sum_{u=1}^{k}(B)_{vu}(C)_{uj} \\
&= \sum_{v=1}^{n}(A)_{iv}(BC)_{vj} = (A(BC))_{ij}.
\end{aligned}$$

□

8.2. Tétel. $(\mathcal{M}_{n\times n}(T), +, \cdot)$ *nemkommutatív, asszociatív, egységelemes gyűrű.*

Bizonyítás. Ahhoz, hogy $(\mathcal{M}_{n\times n}(T), +, \cdot)$ asszociatív gyűrű, már csak a disztributivitást kell belátni. Ha $A = [a_{ij}]$, $B = [b_{ij}]$ és $C = [c_{ij}]$ mind $n\times n$ típusú mátrixok, akkor a T-beli disztributivitás miatt

$$\begin{aligned}
(A(B+C))_{ij} &= \sum_{k=1}^{n} a_{ik}(B+C)_{kj} = \sum_{k=1}^{n} a_{ik}(b_{kj}+c_{kj}) \\
&= \sum_{k=1}^{n}(a_{ik}b_{kj} + a_{ik}c_{kj}) = \sum_{k=1}^{n} a_{ik}b_{kj} + \sum_{k=1}^{n} a_{ik}c_{kj} \\
&= (AB+AC)_{ij}.
\end{aligned}$$

A jobb oldali disztributivitás is hasonlóan igazolható. Az egységelem szerepét az az $n \times n$ típusú mátrix tölti be, melynek a főátlójában minden eleme 1, máshol pedig minden eleme 0:

$$E_n = \begin{bmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & 1 \end{bmatrix}.$$

Ezt a mátrixot $n \times n$ *típusú egységmátrixnak* nevezzük, és E_n-nel jelöljük.

Legyen például

$$A = \begin{bmatrix} 1 & 2 \\ 1 & 1 \end{bmatrix} \quad \text{és} \quad B = \begin{bmatrix} -1 & 0 \\ 2 & 1 \end{bmatrix}.$$

Kiszámítva az AB és BA szorzatokat, láthatjuk, hogy a szorzás nem kommutatív.

□

8.3. Tétel (Determinánsok szorzástétele)**.** *Ha A és B $n \times n$ típusú mátrixok, akkor*

$$\det(AB) = \det A \cdot \det B.$$

Bizonyítás. Legyenek $A = [a_{ij}]$ és $B = [b_{ij}]$ $n \times n$ típusú mátrixok, és legyen C az a $(2n) \times (2n)$ típusú mátrix, melynek

- bal felső sarkában az A mátrix,
- jobb felső sarkában az $n \times n$ típusú zérómátrix,
- bal alsó sarkában az az $n \times n$ típusú mátrix, melynek főátlójában minden elem -1, máshol minden elem nulla,
- jobb alsó sarkában pedig a B mátrix van:

$$C = \begin{bmatrix} a_{11} & \cdots & a_{1n} & 0 & \cdots & 0 \\ \vdots & & \vdots & \vdots & & \vdots \\ a_{n1} & \cdots & a_{nn} & 0 & \cdots & 0 \\ -1 & \cdots & 0 & b_{11} & \cdots & b_{1n} \\ \vdots & & \vdots & \vdots & & \vdots \\ 0 & \cdots & -1 & b_{n1} & \cdots & b_{nn} \end{bmatrix}.$$

A Laplace-féle kifejtési tétel első n sorra történő alkalmazásával kapjuk, hogy

$$\det C = \det A \cdot (-1)^{(1+\cdots+n)+(1+\cdots+n)} \det B = \det A \cdot \det B.$$

Most adjuk hozzá az első sorhoz az $(n+1)$-edik sor a_{11}-szeresét, majd az $(n+2)$-edik sor a_{12}-szeresét, és így tovább, végül a $(2n)$-edik sor a_{1n}-szeresét! Utána adjuk hozzá a második sorhoz az $(n+1)$-edik sor a_{21}-szeresét, majd az $(n+2)$-edik sor a_{22}-szeresét, és így tovább, végül a $(2n)$-edik sor a_{2n}-szeresét! Az eljárást folytatva a többi sorra végül az n-edik sorhoz adjuk az $(n+1)$-edik sor a_{n1}-szeresét, majd az $(n+2)$-edik sor a_{n2}-szeresét, stb., végül a $(2n)$-edik sor a_{nn}-szeresét. Az így keletkezett mátrix a

$$C_1 = \begin{bmatrix} 0 & \cdots & 0 & (AB)_{11} & \cdots & (AB)_{1n} \\ \vdots & & \vdots & \vdots & & \vdots \\ 0 & \cdots & 0 & (AB)_{1n} & \cdots & (AB)_{nn} \\ -1 & \cdots & 0 & b_{11} & \cdots & b_{1n} \\ \vdots & & \vdots & \vdots & & \vdots \\ 0 & \cdots & -1 & b_{n1} & \cdots & b_{nn} \end{bmatrix},$$

és a 7.7. tétel miatt $\det C_1 = \det C$. Alkalmazva ismét a Laplace-féle kifejtési tételt a C_1 mátrix első n sorára, azt kapjuk, hogy

$$\det C_1 = \det(AB) \cdot (-1)^{((n+1)+\cdots+2n)+(1+\cdots+n)} \cdot (-1)^n.$$

Mivel a -1 kitevőjében lévő összeg páros, ezért $\det C_1 = \det(AB)$, és így $\det(AB) =$ $= \det A \cdot \det B$. □

Az alábbi tétel szerint az osztás még a négyzetes mátrixok körében sem végezhető el korlátlanul.

8.4. Tétel. *Egy négyzetes mátrixnak pontosan akkor létezik inverze a szorzásra nézve, ha determinánsa nem nulla.*

Bizonyítás. Tegyük fel először, hogy az A $n \times n$ típusú mátrixnak létezik inverze, és legyen ez B. Ekkor $AB = E_n$, és a determinánsok szorzástétele miatt

$$\det A \cdot \det B = \det(AB) = \det E_n = 1,$$

tehát $\det A \neq 0$.

Fordítva, ha $A = [a_{ij}]_{n \times n}$ olyan mátrix, melynek determinánsa nem nulla, akkor legyen $B = [b_{ij}]_{n\times n}$ az a mátrix, melyre

$$b_{ji} = \frac{A_{ij}}{\det A},$$

ahol A_{ij} az A mátrix a_{ij} eleméhez tartozó adjungált komplementer aldeterminánsa. Ha ezzel a mátrixszal bármelyik oldalról megszorozzuk A-t, a kifejtési tétel garantálja, hogy a szorzat főátlójában csak egyesek lesznek, a ferde kifejtési tétel pedig azt, hogy máshol mindenütt nulla. Tehát $AB = E_n$, azaz B valóban az A inverze. $\square$

A bizonyításból az is kiderült, hogy ha egy négyzetes mátrixnak létezik inverze, akkor az inverzmátrix hogyan állítható elő. Például ha

$$A = \begin{bmatrix} 1 & -2 & 0 \\ 1 & -1 & 1 \\ -1 & 0 & -3 \end{bmatrix},$$

akkor $\det A = -1 \neq 0$ miatt A-nak létezik inverze, és

$$A^{-1} = \begin{bmatrix} \frac{(-1)^{1+1}\begin{bmatrix} -1 & 1 \\ 0 & -3 \end{bmatrix}}{-1} & \frac{(-1)^{2+1}\begin{bmatrix} -2 & 0 \\ 0 & -3 \end{bmatrix}}{-1} & \frac{(-1)^{3+1}\begin{bmatrix} -2 & 0 \\ -1 & 1 \end{bmatrix}}{-1} \\ \frac{(-1)^{1+2}\begin{bmatrix} 1 & 1 \\ -1 & -3 \end{bmatrix}}{-1} & \frac{(-1)^{2+2}\begin{bmatrix} 1 & 0 \\ -1 & -3 \end{bmatrix}}{-1} & \frac{(-1)^{3+2}\begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}}{-1} \\ \frac{(-1)^{1+3}\begin{bmatrix} 1 & -1 \\ -1 & 0 \end{bmatrix}}{-1} & \frac{(-1)^{2+3}\begin{bmatrix} 1 & -2 \\ -1 & 0 \end{bmatrix}}{-1} & \frac{(-1)^{3+3}\begin{bmatrix} 1 & -2 \\ 1 & -1 \end{bmatrix}}{-1} \end{bmatrix} =$$

$$= \begin{bmatrix} -3 & 6 & 2 \\ -2 & 3 & 1 \\ 1 & -2 & -1 \end{bmatrix}.$$

Hogy a kapott mátrix valóban az A inverze, arról az $AA^{-1} = E_3$ egyenlőség ellenőrzésével győződhetünk meg.

Megjegyezzük, hogy azon $n \times n$ típusú mátrixok, melyek determinánsa nem nulla, csoportot alkotnak a mátrixok szorzására nézve.

8.1. Feladatok

8.1. Feladat. Végezze el az alábbi műveleteket!

$$\begin{bmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{bmatrix} \cdot \begin{bmatrix} 1 \\ 2 \\ -1 \end{bmatrix}, \qquad \begin{bmatrix} 4 & -5 \\ 2 & -1 \end{bmatrix}^3, \qquad \begin{bmatrix} a & 1 \\ 0 & a \end{bmatrix}^n, \qquad \begin{bmatrix} \sin x & \cos x \\ -\cos x & \sin x \end{bmatrix}^n,$$

$$\begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{bmatrix} \cdot \begin{bmatrix} 1 & -2 & 3 \\ 2 & -4 & 1 \\ 3 & -5 & 2 \end{bmatrix}, \qquad \begin{bmatrix} 1 & -2 & 3 \\ -1 & 0 & 5 \end{bmatrix} \cdot \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix}$$

8.2. Feladat. Legyen

$$A = \begin{bmatrix} -2 & 0 \\ 3 & 2 \end{bmatrix}, \qquad B = \begin{bmatrix} -1 & 1 \\ 2 & 0 \end{bmatrix}, \qquad C = \begin{bmatrix} 1 & 1 & 2 \\ 2 & -1 & -1 \end{bmatrix}.$$

Adja meg az

$$((A - B) \cdot C)^T$$

mátrixot!

8.3. Feladat. Igazolja, hogy ha $A = [a_{ij}]_{m \times n}$ és $B = [b_{ij}]_{n \times k}$ típusú mátrix, akkor $(AB)^T = B^T A^T$!

8.4. Feladat. Keressen az $(\mathcal{M}_{n \times n}(T), +, \cdot)$ gyűrűben nullosztókat!

8.5. Feladat. Keresse meg azokat a 2×2 típusú mátrixokat, melyek a szorzásra nézve felcserélhetők az

$$\begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix}$$

mátrixszal!

8.6. Feladat. Legyen

$$G = \left\{ \begin{bmatrix} a & a \\ b & b \end{bmatrix} \ : \ a, b \in \mathbb{R} \right\}.$$

Van-e G-nek neutrális eleme a mátrixszorzásra nézve? Igazolja, hogy $a \neq b$ megszorítással G csoportot alkot a mátrixszorzásra nézve!

8.7. Feladat. Keresse meg az alábbi mátrixok inverzeit!

$$A = \begin{bmatrix} 1 & 1 & -1 \\ 2 & -1 & 4 \\ 3 & -2 & -1 \end{bmatrix}, \qquad B = \begin{bmatrix} a & b \\ c & d \end{bmatrix}, \qquad C = \begin{bmatrix} \sin x & \cos x \\ -\cos x & \sin x \end{bmatrix}$$

8.8. Feladat. Igazolja, hogy ha A invertálható mátrix, akkor A^T is invertálható és $(A^T)^{-1} = (A^{-1})^T$.

8.9. Feladat. Oldja meg a

$$\begin{bmatrix} 4 & 1 \\ -6 & 2 \end{bmatrix} \cdot X = \begin{bmatrix} 4 & -1 \\ 2 & 3 \end{bmatrix}$$

mátrixegyenletet!

8.10. Feladat. Igazolja, hogy mindazon $n \times n$ típusú mátrixok, melyek determinánsa 1, csoportot alkotnak a mátrixok szorzására nézve!

8.11. Feladat. Csoportot alkot-e a mátrixok szorzására nézve a

$$H = \left\{ \begin{bmatrix} x & y \\ -y & x \end{bmatrix} \; : \; x, y \in \mathbb{R}, x^2 + y^2 \neq 0 \right\}$$

halmaz?

8.12. Feladat. Legyen A egy olyan négyzetes mátrix, melyre $A^n = 0$ valamely n esetén. Mutassa meg, hogy $\det A = 0$!

Irodalomjegyzék

[1] Freud Róbert: Lineáris algebra. ELTE Eötvös Kiadó, Budapest, 1996.

[2] Gaál István, Kozma László: Lineáris algebra. Kossuth Egyetemi Kiadó, Debrecen, 2009.

[3] Kiss Emil: Bevezetés az algebrába. Typotex, 2007.

[4] Kovács Zoltán: Feladatgyűjtemény lineáris algebra gyakorlatokhoz. Kossuth Egyetemi Kiadó, Debrecen, 2002.

[5] Kiss Péter, Mátyás Ferenc: A számelmélet elemei. EKTF Líceum Kiadó, 1997.

[6] Lovász László, Pelikán József, Vesztergombi Katalin: Diszkrét matematika. Typotex, 2010.

[7] Székelyhidi László: Halmazok és függvények. Palotadoktor Bt., 2009.