# E. függelék

# Az előismeretek összefoglalása

*Még a tudomány látszólag legelvontabb, színtisztán elméleti és matematikai eredményei is csupán egy-két lépésre távolodtak el a környező világ történelem előtti, primitíven érzéki, antropomorf felfogásától.*

***Stanisław Lem:*** *Solaris*
*(Murányi Beatrix fordítása)*

Ebben a fejezetben összefoglaltunk néhány olyan, a középiskolai tananyagon túlmutató konkrét állítást, amelyre a könyvben hivatkozunk. Mindegyik témakör esetében megadtunk egy ajánlott bevezető tankönyvet is. Kivétel a halmazelmélet és logika alapjait bemutató E.1. szakasz: azt javasoljuk, hogy ezt az Olvasó több ízben is fussa át, miközben az algebrával ismerkedik.

## E.1. Halmazelmélet és logika

♫ Az alábbi halmazelméleti fogalmak egy része középiskolából ismerős, a többit pedig a szövegben menet közben vezetjük be, amikor egyúttal példákat is mutatunk rájuk. Az alábbi összefoglalóban meg lehet találni a tömör definíciókat. Szót ejtünk néhány olyan szabályról is, amelyek segíthetnek abban, hogy elkerüljük a legtipikusabb, tapasztalatlanságból eredő logikai hibákat.

A halmaz összességet, kollekciót jelent, olyan dolgot, amelynek elemei vannak (mindegyik elem egyszer szerepelhet, és a sorrendjük nem számít). A matematikában a „halmaz” és a „halmaz eleme” alapfogalmak, nem definiáljuk őket (de az összes többi fogalmat ezekre vezethetjük vissza). Azt, hogy $h$ eleme a $H$ halmaznak úgy jelöljük, hogy $h \in H$ (vagy $H \ni h$). A halmazok elemeit kapcsos zárójelek között sorolhatjuk föl, például $\{1, 2, 3\}$ az a halmaz, amelynek elemei 1, 2 és 3,

$$\{x \in \mathbb{Z} : x^2 = 1\}$$

pedig azokat az egész számokat jelöli, amelyek négyzete 1. Itt $\mathbb{Z}$ az egész számok halmaza, a : jel után pedig bármilyen másmilyen feltételt is írhatunk. Ha $X$ véges halmaz, akkor az elemeinek számát $|X|$ fogja jelölni.

Azt mondjuk, hogy a $B$ halmaz *részhalmaza* az $A$ halmaznak, jelben $B \subseteq A$ (vagy $A \supseteq B$), ha $B$ minden eleme $A$-nak is eleme. Minden halmaznak részhalmaza önmaga, továbbá a $\emptyset$-val jelölt *üres halmaz*, amelynek egyetlen eleme sincs, ezek a *triviális részhalmazok*. Az $X$-től különböző részhalmazokat *valódi részhalmaznak* nevezzük.

A halmazok között műveleteket értelmezhetünk. Az $A$ és $B$ halmazok *uniója* (egyesítése) azokból az elemekből áll, amelyek $A$ és $B$ valamelyikében benne vannak, jele $A \cup B$. Az $A$ és $B$ halmazok *metszete* azokból az elemekből áll, amelyek mind $A$-ban, mind $B$-ben benne vannak, jele $A \cap B$. Két halmaz *diszjunkt*, ha metszetük az üres halmaz, azaz ha nincs közös elemük.

Az $A$ és $B$ halmazok *különbsége* azokból az elemekből áll, amelyek $A$-ban benne vannak, de $B$-ben nincsenek benne, jele $A - B$ (vagy néhány könyvben $A \setminus B$). Ennek speciális esete a komplementum fogalma. Ha $A$ részhalmaza $X$-nek, akkor $A$ *komplementuma* az $X - A$ halmaz, jele $A'$ (vagy néha $\overline{A}$). Ezt olyankor szokás használni, ha $X$ rögzített, és ennek a részhalmazait vizsgáljuk. Két halmaz *szimmetrikus differenciáján* azoknak az elemeknek a halmazát értjük, amelyek a két halmazból pontosan egyben vannak benne. Az $A$ és $B$ szimmetrikus differenciája tehát $(A - B) \cup (B - A)$.

Az unió műveletének fontos tulajdonsága, hogy *asszociatív*, azaz tetszőleges $A$, $B$, és $C$ halmazok esetén

$$(A \cup B) \cup C = A \cup (B \cup C)\,.$$

Valóban, mindkét halmazban azok az elemek vannak benne, amelyek $A$, $B$ és $C$ valamelyikében benne vannak. Ezt szokás zárójelek nélkül, $A \cup B \cup C$-vel jelölni. Végtelen sok halmaz uniójáról is beszélhetünk, ebben azok az elemek vannak, amelyek a résztvevő halmazok valamelyikének elemei. Ugyanígy asszociatív a metszet művelete is, végtelen sok halmaz metszetét analóg módon definiálhatjuk.

Másik fontos műveleti tulajdonság a *kommutativitás*, ami azt jelenti, hogy

$$A \cup B = B \cup A \quad \text{és} \quad A \cap B = B \cap A\,.$$

tetszőleges $A$ és $B$ halmazokra. Végül tetszőleges $A$, $B$ és $C$ halmazokra teljesül kétféle *disztributivitás* is:

$$(A \cup B) \cap C = (A \cap C) \cup (B \cap C) \quad \text{és} \quad (A \cap B) \cup C = (A \cup C) \cap (B \cup C)\,.$$

További fontos, halmazok közötti művelet a *Descartes-szorzat.* Az $(a, b)$ *rendezett pár* abban különbözik az $\{a, b\}$ halmaztól, hogy $(a, b)$ esetében számít az $a$ és $b$ elemek sorrendje (vagyis $a \neq b$ esetén $(a, b) \neq (b, a)$), és $a = b$ is lehetséges (míg az $\{a, a\}$ halmaz csak egyeleműnek számít). Az összes $(a, b)$ párok halmazát, ahol $a \in A$ és $b \in B$, az $A$ és $B$ halmazok Descartes-szorzatának nevezzük, és $A \times B$-vel jelöljük. Nyilván $A \times B$ elemszáma az $A$ és $B$ elemszámának a szorzata. Ha kettőnél több halmaz adott, például $A_1, \ldots, A_n$, akkor

beszélünk az $A_1 \times \ldots \times A_n$ Descartes-szorzatról is, ennek elemei az $(a_1, \ldots, a_n)$ *rendezett n-esek*, ahol $a_i \in A_i$ mindegyik $i$-re. Az analóg fogalmat végtelen sok tényező esetében is használni fogjuk.

Azt, hogy $f$ az $A$ halmazból a $B$ halmazba vezető függvény, úgy írjuk, hogy $f : A \to B$. Ha $f(a) = b$, akkor alkalmazzuk az $f : a \mapsto b$ jelölést is. Az $f$ függvény *értékkészlete* azoknak a $b \in B$ elemeknek a halmaza, amelyeket $f$ értékként fölvesz, vagyis van olyan $a \in A$, hogy $f(a) = b$. Az $f : A \to B$ *szürjektív*, ha értékkészlete az egész $B$ (másképp fogalmazva $f$ az egész $B$-re képez). Az $f$ *injektív* (más néven 1–1-értelmű), ha $A$ különböző elemeihez $B$ különböző elemeit rendeli, vagyis tetszőleges $a_1 \neq a_2$ esetén $f(a_1) \neq f(a_2)$. Az injektív függvényeket (különösen algebrai struktúrák között a művelettartókat) szokás *beágyazásnak* is hívni. Az $f : A \to B$ *bijektív* vagy *kölcsönösen egyértelmű,* ha injektív is és szürjektív is.

Ha $H$ véges halmaz, akkor minden $f : X \to X$ leképezésre $f$ akkor és csak akkor szürjektív, ha injektív. Ha viszont $H$ végtelen halmaz, akkor létezik olyan $f : H \to H$ leképezés, ami injektív, de nem szürjektív, és olyan is, ami szürjektív, de nem injektív.

♫ Két véges halmaz nyilván akkor és csak akkor egyenlő elemszámú, ha van közöttük kölcsönösen egyértelmű megfeleltetés. Ezt a definíciót Georg Cantor végtelen halmazokra is kiterjesztette, ilyenkor nem elemszámról, hanem *számosságról* beszélünk. *Megszámlálhatóan végtelennek* nevezzük azokat a halmazokat, amelyek kölcsönösen egyértelmű megfeleltetésben állnak a pozitív egész számok halmazával. Meg lehet mutatni, hogy az összes egész számok, sőt az összes racionális számok halmaza is megszámlálhatóan végtelen, de a valós számoké már nem az. Az $X$ halmaz számosságát $|X|$ fogja jelölni.

Az $X$ halmaz *identikus leképezése* az az $id_X$ függvény, amely $X$ mindegyik eleméhez önmagát rendeli. Ha $f : A \to B$ és $g : B \to A$, akkor $f$ és $g$ egymás *inverzei*, ha mindegyik „visszacsinálja”, amit a másik elvégez, azaz ha $f\big(g(b)\big) = b$ minden $b \in B$-re, és $g\big(f(a)\big) = a$ minden $a \in A$-ra. Az $f$ függvénynek akkor és csak akkor van inverze, ha bijekció. A függvények között a legfontosabb művelet a kompozíció (lásd 2.2.3. Definíció), amely szintén asszociatív (2.2.4. Gyakorlat).

Egy $X$ halmazon *relációt* értelmezünk, ha bármely két eleméről megmondjuk, hogy relációban állnak-e. Ilyen például az oszthatóság vagy a $\leq$ az egész számok halmazán. Formailag egy reláció az $X \times X$ egy részhalmaza. Azt, hogy $x$ és $y$ az $R$ relációban áll, $x\ R\ y$ vagy $(x, y) \in R$ jelöli. Az $R$ reláció

(1) *reflexív*, ha $x\ R\ x$ minden $x \in X$-re;
(2) *szimmetrikus*, ha $x\ R\ y$-ból $y\ R\ x$ következik minden $x, y \in X$-re;
(3) *tranzitív*, ha $x\ R\ y$-ból és $y\ R\ z$-ből következik, hogy $x\ R\ z$ tetszőleges $x, y, z \in X$ esetén.

Ha mind a három tulajdonság teljesül, akkor $R$ *ekvivalenciareláció*.

Az ekvivalenciarelációk az $X$ halmaz *partícióival* (vagyis páronként diszjunkt halmazokra, úgynevezett ekvivalenciaosztályokra való felosztásaival) állnak kölcsönösen egyértelmű megfeleltetésben (lásd 4.4.9. Tétel).

A halmazelmélet nevezetes tétele Zorn lemmája, amit algebrában is, analízisben is sokat használnak. Mi bizonyítás nélkül idézzük. Tegyük föl, hogy $X$ egy halmaz, és legyen $\mathcal{L}$ egy halmazrendszer az $X$ halmazon (ez azt jelenti, hogy $\mathcal{L}$ elemei az $X$ bizonyos részhalmazai).

**E.1.1. Definíció.** Egy $\mathcal{L}$ halmazrendszert *láncnak* hívunk, ha bármely két $L_1$ és $L_2$ elemére $L_1 \subseteq L_2$ vagy $L_2 \subseteq L_1$.

Például ha minden $r$ valós számra a $H_r$ halmaz az $r$-nél kisebb valós számokból áll, akkor a $\{H_r \,:\, r \in \mathbb{R}\}$ halmazrendszer egy lánc. Az Olvasót megkérjük, hogy az állítás elolvasása előtt ismételje át a maximális elem fogalmát (4.6.4. Definíció).

**E.1.2. Tétel** [Zorn-lemma]. *Legyen $\mathcal{X}$ az $X$ halmaz részhalmazaiból álló nem üres halmazrendszer, amely rendelkezik a következő tulajdonsággal: bárhogyan is választjuk ki $\mathcal{X}$ egy olyan nem üres $\mathcal{L}$ részrendszerét, amelyik lánc, az $\mathcal{L}$ elemeinek uniója is eleme az $\mathcal{X}$ halmazrendszernek. Ekkor az $\mathcal{X}$-nek van maximális eleme.*

A Zorn-Lemma feltételeit kielégítő halmazrendszereket *induktívnak* nevezik.

♫ Például a Zorn-lemma segítségével mutatható meg, hogy minden vektortérben van bázis. Ebben a bizonyításban $\mathcal{X}$ a lineárisan független halmazokból álló halmazrendszer.

Bertrand Russel az 1900-as évek elején jött rá arra, hogy a halmaz naiv fogalmával probléma van, ellentmondásra, paradoxonokra vezet. Egy példa a következő. Ha bármit betehetünk egy halmazba, akkor speciálisan beszélhetünk az összes halmazok halmazáról is. Ez persze halmaz, tehát eleme önmagának. Már ez önmagában is problematikusnak látszik. Konkrétan ellentmondásra is lehet jutni, ha az összes olyan halmazok $H$ halmazát tekintjük, amelyek nem elemei önmaguknak (próbálja meg az Olvasó: abból is ellentmondást kap, ha $H$ eleme önmagának, és abból is, ha $H$ nem eleme önmagának).

A kiutat az jelenti, hogy a most kapott „ellentmondást” a következőképpen fogjuk föl: beláttuk, hogy azok a halmazok, amelyek nem elemei önmaguknak, nem alkotnak halmazt! Tehát nem minden összességet, kollekciót tekintünk halmaznak. Pontos axiómákkal lehet szabályozni, hogy mik is a halmazok, ilyen például a *Zermelo–Fraenkel-féle* axiómarendszer, amelyből az egész matematika fölépíthető. Ezek az axiómák megengedik a matematikában megszokott halmazokat (halmazok uniója is halmaz, egy halmaz összes részhalmaza is halmazt alkot, és így tovább). Vezérlő elvként talán azt lehet mondani, hogy ami túl „nagy” lenne (összes halmazok, összes csoportok), az nem lesz halmaz.

Vannak helyzetek, amikor ezekről a nagyon nagy „nem-halmazokról” mégiscsak beszélni szeretnénk. Például szeretnénk tételeket kimondani, amelyek minden halmazra érvényesek (vagy minden vektortérben igazak). Az ilyen esetekben nem halmazról, hanem *osztályról*, például az összes halmazok osztályáról beszélünk. Az osztály pontosan definiált fogalom, amelyből nem kapunk ellentmondást a fenti értelemben (feltéve, hogy maga a halmazelmélet is ellentmondásmentes). Egy algebrai struktúra (például egy gyűrű) alaphalmaza csakis halmaz lehet, osztály nem.

♫ Kurt Gödel szenzációs tétele, hogy a halmazelmélet ellentmondásmentességét nem lehet bebizonyítani a halmazelmélet axiómarendszerén belül (ami a jelenlegi matematikát magában foglalja). Általában belátta, hogy minden valamirevaló axiómarendszerben van *megoldhatatlan* probléma, amit se bizonyítani, se megcáfolni nem lehet. Ezek a (logikához tartozó) tételek a huszadik század talán legfontosabb eredményei, mert nem valamiféle technikai problémáról, hanem magáról az emberi gondolkodásról, annak a határairól szólnak.

A halmazelméletből szükséges tudnivalók ismertetése után a matematikai logikára térünk. A mindennapi beszédben is használunk logikai műveleteket. Jelölje $A$ azt a mondatot, hogy „esik az eső”, $B$ pedig azt, hogy „felhős az ég”. Ekkor azt a mondatot, hogy „esik az eső és felhős az ég” így rövidíthetjük: „$A$ és $B$”. Hasonlóan értjük azt is, hogy „$A$ vagy $B$”, vagy azt, hogy „nem $A$” (ez tehát azt rövidíti, hogy „nem esik az eső”). Ez utóbbit $\neg A$-nak írjuk.

Az „$A$ és $B$” jelentése egyértelmű: ez akkor igaz, ha $A$ is és $B$ is igaz. A „vagy” műveletet azonban sokféle értelemben használjuk a köznapi életben. Gondoljunk csak az alábbi mondatokra:

„Ez a villamos átmegy a Petőfi-hídon, vagy a Margit-hídon.”

„Vagy fagyit kapsz, vagy perecet.”

„Vagy eszel, vagy olvasol.”

Ezek egészen másképp kapcsolják össze a két részállítást. Az első igaz, ha a villamos akármelyik hídon is átmegy, de akkor is igaz, ha mindkettőn átmegy. A második állítás kizárja azt, hogy a gyerek fagyit és perecet is kapjon, de az egyiket biztosan megkapja. Tehát ez az összetett állítás akkor igaz, ha a két részállítás közül pontosan az egyik teljesül. A harmadik állítás is kizárja, hogy a két részállítás egyszerre teljesüljön, de megengedi, hogy egyik se legyen igaz (hiszen nem muszáj minden pillanatban vagy enni, vagy olvasni, az állítás azt kívánja csak, hogy egyszerre ne történjen a kettő).

A matematikában zavart keltene, ha nem tudnánk pontosan, hogy a „vagy” szót melyik értelemben használjuk. Ezért megállapodunk abban, hogy a „vagy” mindig a fenti legelső, megengedő értelemben szerepel. Tehát az „$A$ vagy $B$” csak akkor hamis, ha $A$ is és $B$ is hamis, különben igaz.

Az első fontos tudnivaló a tagadás szabályaira vonatkozik. Ha $C$ azt jelenti, hogy „ez a gyerek lány”, $D$ pedig azt, hogy „ez a gyerek szőke”, akkor az, hogy

„nem igaz, hogy ez a gyerek lány és szőke”

így rövidíthető: $\neg(C \text{ és } D)$”. Ez ***nem azt jelenti,*** hogy „ez a gyerek nem lány ***és*** nem szőke”, hanem azt, hogy „ez a gyerek nem lány ***vagy*** nem szőke”. Gondoljunk csak bele: a fent kiemelt mondat a szőke fiúkra és a barna lányokra is teljesül. Ugyanígy a

„nem igaz, hogy ez a gyerek lány vagy szőke”

azt jelenti, hogy „ez a gyerek nem lány és nem szőke”, és nem azt, hogy „ez a gyerek nem lány vagy nem szőke”. Ezt az észrevételt általánosítják De Morgan szabályai:

„$C$ és $D$” tagadása „$\neg C$ vagy $\neg D$”,

„$C$ vagy $D$” tagadása „$\neg C$ és $\neg D$”.

Nagyon fontos a „ha $A$, akkor $B$” típusú mondat is, annyira, hogy erre is bevezetünk jelölést: $A \implies B$-vel fogjuk rövidíteni (ezt a műveletet *implikációnak* hívják). Az $A \implies B$ akkor hamis, ha $A$ igaz, de $B$ mégis hamis. Erről ismét példamondatokkal győzhetjük meg magunkat. Legyen $A$ az az állítás, hogy az $n$ szám hattal osztható, $B$ pedig az, hogy $n$ páros. Az $A \implies B$ következtetés ekkor azt mondja, hogy „ha egy szám hattal osztható, akkor páros”. Ezt igaznak érezzük, hiszen ha egy számból 6-ot ki tudunk emelni, akkor 2-t is. Ha $n = 6$, akkor $A$ és $B$ is igaz. Ha $n = 2$, akkor $A$ nem igaz, de $B$ igaz. Ha $n = 7$, akkor sem $A$, sem $B$ nem igaz, de ez még mindig nem rontja el a következtetést. Csak akkor lenne baj, ha találnánk egy 6-tal osztható páratlan számot, tehát amire $A$ igaz, de $B$ mégis hamis.

♫ ***Hamis állításból tehát minden következik!*** Ha $0 = 1$, akkor minden ember örökké él. Ugyanígy az üres halmazban található minden szám egyszerre páros és páratlan; az üres halmazban található mindegyik háromszög szabályos és derékszögű is.

Az Olvasónak érdemes meggondolnia, hogy az $A \implies B$ ugyanazt jelenti, mint hogy „nem $A$, vagy $B$”. Ismét egy példamondattal érvelve: „ha elmész, megharagszom” ugyanazt jelenti, mint hogy „nem mész el, vagy megharagszom”. Azt, hogy $A \implies B$, szokás úgy is mondani, hogy $A$ *elégséges feltétele* $B$-nek, vagy hogy $B$ *szükséges feltétele* $A$-nak.

Egy implikációt nem lehet büntetlenül megfordítani! Abból, hogy $A \implies B$, általában nem következik, hogy $B \implies A$. A fenti példát folytatva: nem igaz, hogy minden páros szám hattal osztható, hiszen például az $n = 2$ ellenpélda. Ugyanakkor érvényes a következő szabály:

Ha $A \implies B$ igaz, akkor $\neg B \implies \neg A$ is igaz.

Például igaz az, hogy „ha egy szám páratlan, akkor nem osztható hattal”. Másképp fogalmazva: ha egy implikációt meg akarunk fordítani, akkor mindkét tagját tagadnunk kell. Ezt a *kontrapozíció* szabályának nevezzük.

Ha $A \implies B$ és $B \implies A$ is teljesül, akkor ezt úgy írjuk, hogy $A \iff B$, és azt mondjuk, hogy $A$ *ekvivalens* $B$-vel. Ezt úgy szokás fogalmazni, hogy „$A$ akkor és csak akkor, ha $B$”, vagy rövidebben „$A$ pontosan akkor, ha $B$”.

Sokszor hallunk ilyesfajta mondatokat is: „az osztályban van barna gyerek”, vagy „mindegyik fa beteg”. Ezeket a $\exists$ („létezik”) és $\forall$ („minden”) jelek segítségével rövidíthetjük. Például $(\forall x)(\exists y)(x < y)$ így fordítható le: „minden számnál van nagyobb szám”. E két jelet *kvantoroknak* hívjuk, az első az egzisztenciális, a második az univerzális kvantor.

Az „és” és a „vagy” műveletekhez hasonlóan a kvantorokat tartalmazó állítások tagadása is külön figyelmet érdemel. A szabály is hasonló: ahogy az „és” és a „vagy” jelek kicserélődnek, ugyanúgy a kvantorokat is meg kell cserélni, amikor a „nem” műveletet átvisszük rajtuk. Például annak az állításnak, hogy „mindegyik fa beteg”, a tagadása az, hogy „van olyan fa, amelyik nem beteg”. Ugyanígy annak, hogy „az osztályban van barna gyerek”, a tagadása az, hogy „az osztályban mindegyik gyerek nem barna”, vagy köznapibban „az osztályban egyik gyerek sem barna”. Általában a szabály a következő:

$$\text{„}(\forall x)F(x)\text{” tagadása „}(\exists x)\neg F(x)\text{”},$$
$$\text{„}(\exists x)F(x)\text{” tagadása „}(\forall x)\neg F(x)\text{”}.$$

Érdemes még megemlíteni kétféle bizonyítási módszert. Ha azt akarjuk bebizonyítani, hogy $A \implies B$, akkor a kontrapozíció szabálya szerint elég azt megmutatni, hogy $\neg B$-ből következik $\neg A$, vagy másképpen: ha feltesszük, hogy $A$ és $\neg B$ is igaz, akkor ellentmondást kapunk. Vagyis feltesszük a bizonyítandó állítás tagadását, és ellentmondásra jutunk. Ezt *indirekt bizonyításnak* nevezzük.

A másik bizonyítási módszer a teljes indukció. Ha egy állítást minden pozitív egész $n$ számra be akarunk látni, akkor elég megmutatni $n = 1$ esetén, továbbá annak feltételezésével, hogy $n-1$-re igaz, megmutatni $n$-re is. Praktikusan: az állítás $n$-re való megmutatásához felhasználhatjuk, hogy igaz $n-1$-re.

A teljes indukció azért működik, mert természetes számok minden nem üres halmazában van legkisebb szám (ez a halmazelmélet axiómarendszerből következik). Ezért a teljes indukciót indirekt bizonyítássá alakíthatjuk a következőképpen. Tegyük föl, hogy az állítás nem igaz. Legyen $n$ a legkisebb olyan szám, amire az állítás hamis. Ez azt jelenti, hogy az összes $n$-nél kisebb számra már igaz. Ellentmondásra kell jutnunk ezekből a feltevésekből.

Vagyis az indukciós bizonyítás során nemcsak $n-1$-re, hanem az összes $n$-nél kisebb számra is feltehetjük, hogy az állítás igaz, miközben $n$-re próbáljuk igazolni azt! Példaként érdemes elolvasni a polinomok maradékos osztásáról szóló 3.2.1. Tétel bizonyítását.

## E.2. Véges matematika

Az ajánlott irodalom Elekes György és Brunczel András [5] tankönyve, illetve Lovász László, Pelikán József és Vesztergombi Katalin [6] műve.

**E.2.1. Tétel.** *Ha van $n$ tárgyunk, akkor ezeket*

$$n! = 1 \cdot 2 \cdot \ldots \cdot (n-1) \cdot n = \prod_{i=1}^{n} i$$

*különböző módon tudjuk sorba rakni. Az itt szereplő $n!$ szám neve: $n$* faktoriális. *Megállapodás szerint $0! = 1$ (lásd a 2.2.42. Gyakorlatot).*

**E.2.2. Tétel.** *Ha van $n$ tárgyunk, és ebből $k$ darabot akarunk kiválasztani (a sorrendre való tekintet nélkül), akkor ezt*

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

*különböző módon tehetjük meg. Az itt szereplő kifejezés az „$n$ alatt a $k$”* binomiális együttható. *Megállapodás szerint ennek értéke nulla, ha $k > n$, vagy ha $k < 0$.*

**E.2.3. Állítás.** *Egy $k$ elemű halmazból egy $n$ elemű halmazba képző függvények száma $n^k$.*

**E.2.4. Tétel.** *Egy $n$ elemű halmaz összes részhalmazainak száma $2^n$. Ha $n \geq 1$, akkor a páros, illetve páratlan elemszámú részhalmazok száma egyaránt $2^{n-1}$ (lásd az 1.5.23. Feladat megoldását).*

Használni fogjuk az alábbi két gráfelméleti tételt is. A gráfokkal kapcsolatos elemi fogalmakat ismertnek tételezzük föl (ezek csak kevés helyen jönnek az anyagban elő).

**E.2.5. Tétel.** *Egy $n$ csúcsú összefüggő gráfnak legalább $n-1$ éle van, és pontosan akkor van ennyi, ha a gráf fa, vagyis nincsen benne kör.*

**E.2.6. Definíció.** A $G = (A, B, E)$ *páros gráf*, ha a csúcshalmaza a diszjunkt $A$ és $B$ halmazok uniója, és sem $A$-n, sem $B$-n belül nem megy él.

Az előbbi jelölésben $E$ az élek halmazát szokta jelenteni. Könnyű belátni, hogy egy gráf akkor és csak akkor páros, ha minden köre páros hosszúságú. Az alábbi jóval nehezebb, de igen hasznos tétel.

**E.2.7. Tétel** [König–Hall–Ore-tétel]. *Legyen $G$ páros gráf. Pontosan akkor léteznek olyan diszjunkt élek, amelyek az $A$ minden elemét lefedik, ha tetszőleges $X \subseteq A$ esetén az $X$-beli pontok $B$-beli szomszédainak száma legalább annyi, mint az $X$ elemszáma.*

## E.3. Analízis

Az ajánlott irodalom Laczkovich Miklós és T. Sós Vera [3] tankönyve.

**E.3.1. Tétel.** *Minden valós együtthatós polinomhoz tartozó polinomfüggvény folytonos.*

**E.3.2. Tétel** [Bolzano tétele]. *Legyen $f$ folytonos függvény az $[a, b]$ zárt intervallumon. Ha $f(a) < 0$ és $f(b) > 0$, akkor van olyan $a < c < b$, melyre $f(c) = 0$.*

**E.3.3. Lemma.** *Legyen $f$ valós együtthatós polinom, melynek főegyütthatója pozitív. Ekkor van olyan $c$ valós szám, hogy $x > c$ esetén $f(x) > 0$ (azaz „elég nagy" $x$ értékekre $f(x)$ már pozitív lesz).*

*Bizonyítás.* Legyen $f(x) = a_0 + \ldots + a_n x^n$, ahol $a_n > 0$. A háromszög-egyenlőtlenséget (1.4.3. Tétel) felhasználva $x \geq 1$ esetén

$$|a_0 + a_1 x + \ldots + a_{n-1}x^{n-1}| \leq \big(|a_0| + \ldots + |a_{n-1}|\big)x^{n-1}\,.$$

Ez kisebb, mint $a_n x^n$, ha még $x > \big(|a_0| + \ldots + |a_{n-1}|\big)/a_n$ is teljesül. Ezért az ilyen $x$-ekre $f(x) > 0$. □

Az alábbi tételt érdemes összevetni a 3.3.9. Tétellel, és az azt követő megjegyzésekkel.

**E.3.4. Tétel.** *Páratlan fokú valós együtthatós polinomnak van valós gyöke.*

*Az algebra alaptételétől független bizonyítás.* Mivel $f$-nek és $-f$-nek ugyanazok a gyökei, feltehetjük, hogy $f$ főegyütthatója pozitív. Az előző lemma szerint $f$ felvesz pozitív értéket. Most tekintsük a $-f(-x)$ polinomot. Mivel $f$ páratlan fokú, ennek a főegyütthatója szintén pozitív. Az előző lemma szerint van olyan $d$ valós szám, hogy $-x > d$ esetén $-f(-x) > 0$. Vagyis $x$ helyébe $-x$-et írva $x < -d$ esetén $f(x) < 0$. Beláttuk tehát, hogy $f$ pozitív és negatív értéket is felvesz, és így Bolzano tétele miatt van valós gyöke. □

## E.4. Számelmélet

Feltételezzük, hogy az Olvasó ismeri az elemi számelmélet alapfogalmait (oszthatóság, egység, legnagyobb közös osztó, legkisebb közös többszörös, prímszám), és a hozzájuk kapcsolódó szokásos jelöléseket (például $b \mid c$ azt jelöli, hogy $b$ osztója $c$-nek, $a \equiv b\ (n)$ pedig azt, hogy $a$ kongruens $b$-vel modulo $n$, vagyis hogy $n \mid b - a$). Ezek megtalálhatók Freud Róbert és Gyarmati Edit [1] könyvének első fejezetében. E fogalmak részletes elemzéséről és általánosításairól szót ejtünk a 3.1. szakaszban is. Most azokat a tudnivalókat foglaljuk össze, amelyeket felhasználunk majd, az Euler-függvénnyel, a Möbius-függvénnyel és a kvadratikus maradékokkal kapcsolatban.

**E.4.1. Definíció.** Legyen $n$ pozitív egész. Ekkor a $\varphi(n)$ *Euler-függvény* megadja a $0, 1, \ldots, n-1$ számok közül az $n$-hez relatív prímek számát.

Természetesen ha a $0, 1, \ldots, n-1$ helyett az $1, 2, \ldots, n$ számok között (vagy bármely más teljes maradékrendszerben) számoljuk meg az $n$-hez relatív prím számokat, akkor ugyanazt az eredményt kapjuk.

**E.4.2. Tétel.** *Az Euler-függvény multiplikatív, azaz ha $n$ és $m$ relatív prím pozitív egészek, akkor $\varphi(nm) = \varphi(n)\varphi(m)$. Innen következik, hogy ha $n$ kanonikus alakja $n = p_1^{\alpha_1} \ldots p_k^{\alpha_k}$, ahol egyik $\alpha_i$ kitevő sem nulla, akkor*

$$\varphi(n) = \left(p_1^{\alpha_1} - p_1^{\alpha_1 - 1}\right) \ldots \left(p_k^{\alpha_k} - p_k^{\alpha_k - 1}\right).$$

Elemi számelméleti okoskodásokkal adódik a fenti képletből az alábbi két állítás, amit a könyvben felhasználunk.

**E.4.3. Állítás.** *Legyen $n$ pozitív egész.*

(1) *A $\varphi(n)$ értéke akkor és csak akkor 1, ha $n = 1$ vagy $n = 2$.*
(2) *A $\varphi(n)$ értéke akkor és csak akkor páratlan, ha $n = 1$ vagy $n = 2$.*

Azt, hogy az Euler-függvény multiplikatív, most be fogjuk bizonyítani, mert a bizonyításból egy olyan összefüggés adódik, amire szükségünk lesz. Ehhez emlékeztetjük az Olvasót néhány definícióra. A 2.2. szakaszban láttuk, hogy amikor a $0, 1, \ldots, n-1$ számokkal modulo $n$ végezzük a műveleteket, akkor egy $\mathbb{Z}_n$ egységelemes gyűrűt kapunk, amelynek az invertálható elemei pontosan azok a $0 \leq i < n$ számok, amelyek $n$-hez relatív prímek. Ezeknek a halmazát $\mathbb{Z}_n^\times$-tel jelöltük. Vagyis $\mathbb{Z}_n^\times$ elemszáma pontosan $\varphi(n)$. A $\mathbb{Z}_n^\times \times \mathbb{Z}_m^\times$ az olyan $(a, b)$ rendezett párok halmazát jelöli, amelyekre $a \in \mathbb{Z}_n^\times$ és $b \in \mathbb{Z}_m^\times$. Ennek a halmaznak az elemszáma tehát $\varphi(n)\varphi(m)$.

**E.4.4. Tétel.** *Tegyük föl, hogy $n$ és $m$ relatív prím pozitív egészek. Ekkor létezik olyan $g : \mathbb{Z}_n^\times \times \mathbb{Z}_m^\times \to \mathbb{Z}_{nm}^\times$ kölcsönösen egyértelmű megfeleltetés, hogy tetszőleges $a, a' \in \mathbb{Z}_n$ és $b, b' \in \mathbb{Z}_m$ esetén*

$$g(a *_n a', b *_m b') = g(a, b) *_{mn} g(a', b').$$

*(ebben a képletben $*_n$ a modulo $n$ szorzás műveletét jelöli, lásd 1.1.4. Definíció). Speciálisan $\varphi(nm) = \varphi(n)\varphi(m)$.*

*Bizonyítás.* Kényelmesebb a $g$ megfeleltetés $f$ inverzét megkonstruálni. Ha $c \in \mathbb{Z}_{nm}^\times$, akkor jelölje $a$ a $c$ szám $n$-nel való osztási maradékát. Hasonlóképpen legyen $b$ a $c$ szám $m$-mel való osztási maradéka, és $f(c) = (a, b)$.

A definíció szerint $0 \leq a < n$. Megmutatjuk, hogy $a$ és $n$ relatív prímek. Valóban, ha volna egy $d > 1$ közös osztójuk, akkor $a \equiv c \ (n)$ miatt $d$ osztaná $c$-t is, ami lehetetlen, mert $c$ és $nm$ relatív prímek. Ezért $a \in \mathbb{Z}_n^\times$. Ugyanígy adódik, hogy $b \in \mathbb{Z}_m^\times$. Az $f$ tehát a $\mathbb{Z}_{nm}^\times$ halmazt a $\mathbb{Z}_n^\times \times \mathbb{Z}_m^\times$ halmazba képzi.

Ahhoz, hogy belássuk, hogy bijektív, meg kell mutatnunk, hogy $f$ szürjektív és injektív.

Legyen $(a, b) \in \mathbb{Z}_n^\times \times \mathbb{Z}_m^\times$, és tekintsük az

$$\left.\begin{aligned} x &\equiv a\ (n) \\ x &\equiv b\ (m) \end{aligned}\right\}$$

szimultán kongruenciarendszert. Ennek a kínai maradéktétel szerint van megoldása, és ez egyértelmű modulo $nm$. Ezért pontosan egy olyan $c$ megoldás van, amelyre $0 \leq c < nm$. Belátjuk, hogy $c \in \mathbb{Z}_{nm}^\times$, azaz hogy $(c, nm) = 1$. Tegyük föl ennek ellenkezőjét. Ekkor van olyan $q$ prím, melyre $q \mid c$ és $q \mid nm$. Ezért vagy $q \mid n$, vagy $q \mid m$. Az első esetben $c \equiv a\ (n)$ miatt $q \mid a$ is teljesül, azaz $q$ közös osztója $a$-nak és $n$-nek. Ez lehetetlen, mert $a \in \mathbb{Z}_n^\times$, azaz $(a, n) = 1$. A második esetben, amikor $q \mid m$, a $(b, m) = 1$ feltétellel kerülünk ellentmondásba. Tehát tényleg $c \in \mathbb{Z}_{nm}^\times$. A maradékos osztás egyértelműsége miatt $f(c) = (a, b)$. Tehát $f$ tényleg szürjektív.

Az, hogy $f$ injektív, a kínai maradéktétel egyértelműségi állításából következik. Ha ugyanis $f(c) = f(c') = (a, b)$, akkor $c$ is és $c'$ is megoldása a fenti szimultán kongruenciarendszernek. Tehát $c \equiv c'\ (nm)$. Mivel $0 \leq c, c' < nm$, ezért $c = c'$. Tehát $f$ bijektív, és ezzel $\varphi$ multiplikativitását beláttuk.

Legyen $g$ az $f$ függvény inverze. Ha tehát $g(a, b) = c$ és $g(a', b') = c'$, akkor $f(c) = (a, b)$ és $f(c') = (a', b')$. Szeretnénk kiszámítani $f(c *_{nm} c')$ értékét, azaz a $c *_{nm} c'$ szám maradékát modulo $n$ és modulo $m$. A modulo $nm$ szorzás definíciója az, hogy az egész számok között kiszámított szorzatot még redukálni kell modulo $nm$. Így viszont $c *_{nm} c' \equiv cc'\ (n)$ is teljesül, tehát elegendő a $cc'$ maradékát kiszámolni. Tudjuk, hogy $c \equiv a\ (n)$ és $c' \equiv a'\ (n)$, ezért $cc' \equiv aa\ (n)$. Így $cc'$ maradéka ugyanaz, mint $aa'$ maradéka, azaz $a *_n a'$. Hasonló számolással kapjuk, hogy $c *_{nm} c'$ mod $m$ vett maradéka $b *_m b'$. Tehát $f(c *_{nm} c') = (a *_n a', b *_m b')$. Másképp fogalmazva $g(a *_n a', b *_m b') = c *_{nm} c'$, és ezzel az állítást beláttuk. □

**E.4.5. Definíció.** A $\mu(m)$ *Möbius-függvényt* a következőképpen definiáljuk: ha az $m$ pozitív egész szám $s$ darab különböző prím szorzata, akkor $\mu(m) = (-1)^s$, egyébként pedig $\mu(m) = 0$.

Természetesen $\mu(1) = (-1)^0 = 1$, hiszen az 1 nulla darab prím szorzata (üres szorzat). A Möbius-függvény egy fontos tulajdonságát fogalmazza meg a következő állítás.

**E.4.6. Állítás.** *Tetszőleges $m$ pozitív egészre*

$$\sum_{d \mid m} \mu(d) = \begin{cases} 1 & \text{ha } m = 1, \\ 0 & \text{ha } m \neq 1. \end{cases}$$

*Bizonyítás.* Az állítás $m = 1$ esetén nyilvánvaló. Tegyük föl, hogy $m > 1$, és legyenek $p_1, \ldots, p_s$ az $m$ szám különböző prímosztói. A $\mu(d)$ értéke 0, kivéve ha $d$ különböző prímek szorzata, azaz $p_1 \cdot \ldots \cdot p_s$ egy rész-szorzata. Ha páratlan sok prímet szorzunk össze, akkor $\mu(d) = -1$, ha páros sokat, akkor $\mu(d) = 1$. Vagyis a fenti összeg értéke akkor lesz nulla, ha a $\{p_1, \ldots, p_s\}$ halmaznak ugyanannyi páratlan elemű részhalmaza van, mint páros elemű. Ez $s \geq 1$ (vagyis $m > 1$) esetén igaz az E.2.4. Tétel miatt. □

**E.4.7. Definíció.** Legyen $n$ pozitív egész. Egy $n$-hez relatív prím szám akkor *kvadratikus maradék* mod $n$, ha egy alkalmas másik szám négyzetével kongruens mod $n$.

**E.4.8. Tétel.** *Legyen $p$ páratlan prímszám. Ekkor a kvadratikus maradékok száma $(p-1)/2$. Ha a $p$ prím $4k+1$ alakú, akkor a $-1$ kvadratikus maradék. Ebben az esetben egy $p$-hez relatív prím szám akkor és csak akkor kvadratikus maradék, ha az ellentettje az. Ha a $p$ prím $4k-1$ alakú, akkor a $-1$ nem kvadratikus maradék. Ebben az esetben minden $p$-hez relatív prím $b$ számra igaz, hogy $b$ és $-b$ közül az egyik kvadratikus maradék, a másik nem az.*

A bizonyítás megtalálható az [1] könyv 4.1. szakaszában. Ha az Olvasó már megismerkedett a csoportelmélet alapjaival, akkor a kvadratikus maradékok elméletét a következőképpen szemlélheti.

A kvadratikus maradékok a $\mathbb{Z}_n^\times$ csoport négyzetelemei. Tegyük föl, hogy $p$ páratlan prím. Ekkor a kvadratikus maradékok száma azért $(p-1)/2$, mert a négyzetre emelés csoporthomomorfizmus, melynek magja $\{1, -1\}$, vagyis kételemű. A kvadratikus maradékok tehát egy 2 indexű részcsoportot alkotnak. Tudjuk, hogy létezik primitív gyök modulo $p$ (4.3.22. Tétel), ennek pontosan a páros kitevőjű hatványai lesznek kvadratikus maradékok. A hatvány rendjének képlete szerint tehát azok az $r$ számok kvadratikus maradékok, melyekre $(p-1)/o_p(r)$ páros szám (itt $o_p(r)$ az $r$ rendje $\mathbb{Z}_p^\times$-ben).

## E.5. Lineáris algebra

Általában Freud Róbert [2] könyvének terminológiáját követjük, azonban a vektorokat egyszerűen kisbetűkkel, a mátrixokat és a lineáris leképezéseket pedig nagybetűkkel jelöljük: $u$, $M$, $A$. Az $m \times m$-es egységmátrix $E_m$ (néha csak $E$), egy vektortér identikus transzformációjának jele általában $I$. A $T$ test fölötti $k$ sorból és $n$ oszlopból álló mátrixok halmaza $T^{k\times n}$. Az $M$ négyzetes mátrix determinánsa $\det(M)$, nyoma, azaz a főátlóban álló elemek összege (és egyúttal a sajátértékeinek összege) $\mathrm{tr}(M)$. A $V$ vektortér dimenzióját $\dim(V)$ jelöli.

**E.5.1. Tétel** [A determinánsok szorzástétele]. *Legyen $T$ test, és $M$, $N$ a $T$ fölötti $n \times n$-es mátrixok. Ekkor $\det(MN) = \det(M)\det(N)$. Egy $M$ (négyzetes) mátrix akkor és csak akkor invertálható, ha determinánsa nem nulla. Ha $M$ és $N$*

*négyzetes mátrixok, és $MN$ az egységmátrix, akkor $M$ és $N$ egymás kétoldali inverzei, vagyis $NM$ is az egységmátrix.*

**E.5.2. Tétel.** *Ha $T$ test, $M \in T^{m\times m}$, $N \in T^{n\times n}$, $X \in T^{n\times m}$, $O$ az $m \times n$-es nullmátrix, akkor például az első sor szerinti kifejtéssel igazolható, hogy*

$$\det \begin{bmatrix} M & O \\ X & N \end{bmatrix} = \det(M)\det(N)\,.$$

*A transzponált determinánsra vonatkozó tétel miatt az állítás akkor is igaz, ha a nullák nem a jobb fölső, hanem a bal alsó sarokban vannak.*

**E.5.3. Definíció.** Az alábbi determináns a *Vandermonde-determináns:*

$$V(z_1,\ldots,z_n) = \begin{vmatrix} z_1^{n-1} & \ldots & z_n^{n-1} \\ \vdots & \ldots & \vdots \\ z_1 & \ldots & z_n \\ 1 & \ldots & 1 \end{vmatrix}\,.$$

Ugyanígy hívjuk az ebből transzponálással, valamint a sorok (oszlopok) sorrendjének megfordításával kapható determinánsokat is.

**E.5.4. Tétel.** *A fenti Vandermonde-determináns értéke*

$$\prod_{1\le i<j\le n} (z_i - z_j)\,.$$