10. fejezet

Utószó: Mi az algebra?

Ha végigpillantunk a tudomány történetén, beláthatjuk: nagyon valószínűvé teszi, hogy a jövő képét az határozza meg, amit ma nem tudunk, és ami nem látható előre.

Stanisław Lem: *Az Úr hangja (Murányi Beatrix fordítása)*

A címben föltett kérdésre nagyon sokféle válasz lehetséges. Aki végigolvassa ezt a könyvet (és remélhetőleg más matematika-könyveket is), annak kialakul a képe az algebráról. Mégis megkísérelünk egyfajta — szükségszerűen szubjektív — összefoglalót adni. Ez egyaránt szól azoknak, akik most nyitják ki először a könyvet, és azoknak, aki már végigrágták magukat rajta. Az alábbiakat érdemes többször is elolvasni, hiszen a fölsorolt elvek konkrét tudás birtokában újabb és újabb értelmet nyernek, egyre érthetőbbekké válnak.

Középiskolai tapasztalatunk az, hogy az algebrában számolni szoktunk. Ha például egy geometriapéldát akarunk megoldani, és sikerül fölírni egy egyenletet, akkor ennek megoldása már az algebra témakörébe tartozik. Az algebrista dolga az, hogy az embereknek megkönnyítse a számolások elvégzését.

A számolás fogalma egészen általános. A mindennapi életben mondhatjuk ezt olyankor is, ha el akarjuk dönteni, melyik úton haladva jutunk el leggyorsabban a Magas-Tátrába, vagy hogy beáldozzuk-e a vezérünket egy sakkpartiban a mattadás érdekében. Az algebrában számoláson elsősorban azt értjük, hogy *műveleteket végzünk*. Ezek lehetnek a klasszikus műveletek: összeadás, kivonás, szorzás, osztás, de más is, például két egész szám legnagyobb közös osztójának a meghatározása.

Műveleteket nem csak számokkal végzünk. Középiskolában megtanultunk egyenleteket rendezni, és ilyenkor ismeretlent tartalmazó (formális) kifejezésekkel számolunk. Beszélünk függvények összegéről is, például a $\sin x + \cos x$ függvényről. Szükséges lehet annak kiszámítása, hogy a síkon egy tükrözés és egy forgatás egymás utáni elvégzése milyen transzformációt eredményez. Ilyenkor geometriai transzformációkkal végzünk műveletet: az egymás után alkalmazás, más néven *kompozíció* műveletét. A matematikában, a fizikában a fentieken kívül még sok olyan dolgot fedeztek föl (például vektorokat, tenzorokat, kvaterniókat), amelyekkel számolni érdemes.

Amikor sok ember mindenfélével számolni akar, az a jó, ha az algebrista egyszerre tud segíteni nekik, olyan általánosan, ahogy csak lehet. Ha valakinek sok olyan feladatot kell megoldania, amely mind másodfokú egyenletre vezet, akkor nem érdemes minden egyenlettel az algebristához szaladnia, jobban jár, ha az algebrista megmutatja neki a megoldóképletet. A lineáris algebra a geometriai transzformációk kompozíciójának kiszámítását úgy könnyíti meg, hogy minden síkbeli transzformációhoz egy számnégyest (úgynevezett mátrixot) rendel, és megadja, hogy a két transzformáció kompozíciójának mátrixát milyen szabályokkal határozhatjuk meg.

A matematika erős oldala mindig is az volt, hogy sok hasonló problémát *egyszerre* tudott megoldani, alkalmas módszerek kidolgozásával. Az ezt elősegítő egyik alapvető eszköz az *absztrakció*. Ez azt jelenti, hogy sok hasonló dolognak megragadjuk a közös vonásait, ezekből kiindulva valami érdekeset fedezünk föl, amit azután a kiinduló dolgok mindegyikére alkalmazhatunk (olyanokra is, amire korábban nem is gondoltunk).

♫ Amikor az ősember rájött, hogy két tigris meg két tigris az négy tigris, de ugyanúgy két dárda meg két dárda az négy dárda, akkor hatalmas lépést tett a szám fogalmának megalkotása felé. Az „egész szám” tehát egy absztrakt fogalom, a $2 + 2 = 4$ pedig egy absztrakt tétel. Ez azt is maga után vonja, hogy két űrhajó meg két űrhajó az négy űrhajó (amire az ősember feltehetőleg nem gondolt). Hasonlóképpen absztrakció eredménye a másodfokú egyenlet fogalma is, a megoldóképlet pedig egy absztrakt tételnek tekinthető.

Az absztrakciót a matematika minden ága alkalmazza. Az algebra abban speciális, hogy *struktúrákban* gondolkodik, és ezek szerkezetét akarja földeríteni. Ezt először az egész számok példáján érzékeltetjük (amelyek ugyan nem struktúrák a szó algebrai értelmében, de mint láttuk, absztrakció eredményei).

♫ Középiskolából tudjuk, hogy minden egynél nagyobb egész szám egyértelműen fölbontható (pozitív) prímszámok szorzatára. Ez megadja a számok „szerkezetét”, tehát egyfajta struktúratételnek tekinthető. Lehetővé teszi bizonyos kérdések gyors megválaszolását (például hogy egy számnak hány osztója van, mi két szám legkisebb közös többszöröse). Persze nem minden probléma megoldásában segít (például azokéban kevésbé, amelyekben összeadás is szerepel).

Mi az, hogy algebrai struktúra? A számok szorzása *asszociatív*, vagyis bármely három számra $(ab)c = a(bc)$ teljesül. Ez a szabály érvényes akkor is, ha függvényeket, vagy ha mátrixokat szorzunk. Ilyenkor az algebrista a következőt mondja.

♫ „Ne foglalkozzunk azzal, hogy *miket* szorzunk össze, csak azzal, hogy a szorzásnak mik a tulajdonságai. Nevezzük el félcsoportnak azt a struktúrát, amelyről csak annyit tudunk, hogy az elemeit asszociatív módon össze lehet szorozni. Az én dolgom az, hogy az ilyen struktúrákat vizsgáljam, minél többet, mélyebbet tudjak mondani róluk, a legjobb esetben teljesen le tudjam írni a szerkezetüket. Mivel az elemekről semmit sem tettem föl, mindenki tudja majd alkalmazni az eredményeimet, aki egy asszociatív művelettel találkozik.”

Természetesen nagyon sokféle struktúra és tulajdonság van, amit ily módon vizsgálni lehet. Két olyan fontos feltétel van, amelynek teljesülnie kell ahhoz, hogy egy struktúrát érdemes is legyen vizsgálni.

- Elég speciális legyen ahhoz, hogy nemtriviális eredményeket lehessen bizonyítani.
- Elég általános legyen ahhoz, hogy a kapott eredmények sokféleképpen alkalmazhatók legyenek.

Az algebrában szereplő fogalmak ennek megfelelően származhatnak az alkalmazásokból, de eredhetnek abból a belső szükségszerűségből is, hogy az algebrai vizsgálatokat hatékonnyá, áttekinthetővé, egyszerűvé tegyük.

Ha egy struktúra szerkezetét teljesen föl lehet deríteni, akkor *struktúratételről* beszélünk. Ilyen a véges Abel-csoportok alaptétele, a véges egyszerű csoportok klasszifikációja, a véges testek leírása, vagy a Wedderburn–Artin-tétel. Ide tartozó egyszerűbb eredmény a ciklikus csoportok és a prímtestek *osztályozása* is.

Az imént hangsúlyoztuk, hogy a vizsgált struktúrákban csak a műveletek tulajdonságai számítanak, az elemek mibenléte nem. Ha az elemeket kicseréljük, de a műveleteket „ugyanúgy” végezzük, akkor a két struktúrát azonosnak tekintjük. Ezt pontosabban úgy fogalmazhatjuk, hogy a két struktúra elemei között van egy olyan kölcsönösen egyértelmű megfeleltetés, amely *tartja a műveleteket*. Más szóval a két struktúra *izomorf*, a szerkezetük ugyanaz.

Általában két struktúra között egy „szerkezettartó” leképezést *homomorfizmusnak* nevezünk. Ez talán az algebra legfontosabb fogalma, mert lehetővé teszi, hogy a struktúrákat ne önmagukban, hanem egymáshoz való viszonyaikban vizsgáljuk. Az izomorfizmusok fontosságát már láttuk. Sokszor előfordul az is, hogy egy bonyolult struktúrában föltett kérdés megválaszolásához elegendő egy olyan egyszerűbb struktúra vizsgálata, amelybe a bonyolult struktúrából homomorfizmus vezet, azt *reprezentálja*.

♫ Például ha a kérdés az, hogy az 100000000007 számot elő lehet-e állítani két négyzetszám összegeként, akkor minden számot reprezentáljunk a néggyel való osztási maradékával. Összeg maradéka a maradékok összege, szorzat maradéka a maradékok szorzata, ezért ez a leképezés „szerkezettartó” (tartja az összeadást és a szorzást). Mivel négyzetszám néggyel osztva nullát vagy egyet ad maradékul, két négyzetszám összegének maradéka három biztosan nem lehet, és így a fenti szám nem áll elő két négyzetszám összegeként.

Homomorfizmusnak tekinthetjük a mérés aktusát is a természettudományokban, hiszen a mérőszám a vizsgált dolog egy egyszerűen kezelhető reprezentánsa. A mérőszám hozzárendelése „szerkezettartó” leképezés, ezt fejezik ki a természeti törvények. Például ha két biliárdgolyó összeütközik, akkor a tömegek, a mozgásmennyiségek összeadódnak. Egy fizikai kérdést, mondjuk azt, hogy a biliárdasztalon lévő golyók ütközések sorozata után kerülhetnek-e egy megadott állapotba, megválaszolhatunk negatívan úgy, hogy kiszámítjuk a rendszer energiáját a kezdő és a végső állapotban. Ha más mennyiséget kapunk, akkor a végső állapot nem jöhet létre. Ez a fenti, négyzetszámokról szóló feladat analogonja. A mérések eredményei általában az algebra legfontosabb objektumainak elemei (számok, vektorok), és az ezekkel végzendő műveletek motivációja is sokszor a fizikából származik (például a vektorok összeadását levezethetjük az erők viselkedéséből is).

♫ Ennél még általánosabb elvként magát az absztrakció folyamatát is homomorfizmusnak képzelhetjük. Amikor elvonatkoztatunk az elemek mibenlététől, ugyanolyan egyszerűsítést hajtunk végre, mint az előbbi két példában, és ez lehetővé teszi, hogy a lényegre koncentráljunk. A valós számok esetében elhagyhatjuk a műveleteket, és csak arra figyelhetünk, hogy mely számok vannak egymáshoz „közel”. Ekkor az analízis *topológiai* szemléletmódjához jutunk. Ha viszont a rendezést és a távolságot hanyagoljuk el, és a műveletekre figyelünk, akkor a valós számok összességét, mint algebrai struktúrát, azaz mint *testet* vizsgálhatjuk.

„Szerkezettartó” hozzárendelésre fontos példa az *invariánsok* fogalma is. Az invariáns olyan dolog, ami egy rendszernek jellemzője, a rendszer átalakulásai során nem változik. Ilyen például az energia, a mozgásmennyiség a fizikában. Ha gyerekek dobálnak labdákat egymásnak, akkor az változhat, hogy kinél éppen hány labda van, de a labdák össz-száma invariáns marad. Az algebrában az invariánsok szerepe különösen fontos, ha azt akarjuk megállapítani, hogy két struktúra izomorf-e.

♫ Például két vektortér akkor és csak akkor izomorf, ha a dimenziójuk megegyezik. Ezért a vektorterek teljes osztályozásához szükséges egyetlen invariáns a dimenzió. Csoportoknál invariáns a huszadrendű elemek száma a csoportban, hiszen izomorfizmusnál ez is megőrződik.

Néha olyan szerencsénk van, hogy a megismerni kívánt bonyolult struktúrából rengeteg homomorfizmust találunk egyszerűbb struktúrákba, eleget ahhoz, hogy a kiinduló struktúra szerkezetét ezek teljesen meghatározzák. Például egy pont egy koordinátájának kiszámítása homomorfizmus, de ha a pont „összes” koordinátáit megadjuk, akkor ezzel a pontot is meghatároztuk. Ugyanígy egy részecske állapotát leírhatjuk hat „koordináta” segítségével (három hely- és három sebesség-koordináta). Ha egy algebrai struktúrát sikerül az így leírt módon megfognunk, akkor *szubdirekt felbontásról* beszélünk. (Szerencsésebb esetben direkt szorzatra való felbontást kapunk.)

Az algebrában a *fogalmak* és a *módszerek* legalább annyira fontosak, mint a tételek. Egy-egy tételt el lehet felejteni, de az alkalmazott módszerek megragadnak, és így lehetővé válik, hogy az erre alkalmas problémákat „algebrista” gondolkodásmóddal támadjuk meg. A helyes fogalmak felismerésének módját az alábbi, klasszikus hindu történet példázza.

♫ Vak fakírok az erdőben sétálva találkoztak egy állattal. Az egyik felkiáltott: „Ez egy kígyó!”, mikor megsimogatta az ormányát. „Nem, ez egy fa!”, mondta egy másik, aki a lábát tapogatta. A harmadik az állat testét falnak érzékelte, a negyedik a fülét papírnak, az ötödik a farkát kötélnek. Amikor azonban este elbeszélgettek a tapasztalataikról, egész jó képet sikerült kialakítaniuk az elefántról (amit korábbi tapasztalataik segítségével „mértek” meg).

Azt, hogy egy fogalmat az általánosság melyik szintjén érdemes vizsgálni, magától a fogalomtól, és a felvetett kérdéstől függ. Ezt úgy kell elképzelni, mint amikor megismerünk egy hegységet, ahová kirándulni járunk. A konkrét problémák megoldása annak felel meg, hogy le kell küzdenünk meredek emelkedőket, bozótos részeket. Eleinte ezeket ki sem tudjuk kerülni. Csak évek során jön meg az az áttekintési képességünk, hogy már minden pillanatban tudjuk: a hegység egészéhez képest hol vagyunk, merre mi van, milyen távolságban, és az hogyan érhető el. Ez a megismerési folyamat az egyéni tanulásra éppen úgy vonatkozik, mint magának a matematikának a fejlődésére. A jobb áttekintés a matematikában sokszor az általánosság szintjének emelkedését jelenti. Minderre fontos példát szolgáltatnak az alábbiak.

- Elem rendjével először a komplex egységgyökök kapcsán találkozunk, amikor azt vizsgáljuk, hogy egy komplex szám mely hatványai lesznek 1-gyel egyenlők. Kiderül, hogy ezek a „jó” kitevők mindig egy alkalmas egész szám összes többszörösei. Ugyanez a jelenség lép föl akkor is, ha azt kérdezzük, hogy egy geometriai transzformációt hányszor kell alkalmazni ahhoz, hogy minden pontot önmagába vigyen. Az „elefánt” ebben az esetben a csoportelméleti elemrend lesz. Az újabb fakír azonban észreveszi, hogy a lineáris transzformációknál tanult minimálpolinomnak is vannak a fentiekhez hasonló tulajdonságai. A végső, „még magasabb szintű elefánt” tehát az elemrendnek az a fogalma, ami a modulusok elméletében szerepel.
- A véges Abel-csoportok alaptétele és a Jordan-féle normálalakról szóló tétel esetében a „helyes” (közös) általánossági szint a főideálgyűrűk fölötti modulusok alaptétele.
- A számelmélet alaptételét tárgyalhatjuk külön az egész számokra, és test fölötti polinomokra. Közös általánosításként szerepel az euklideszi gyűrű, illetve a főideálgyűrű fogalma. Ennél is tovább léphetünk, ha ideálok primér felbontásait nézzük (Noether–Lasker-tétel), vagy akár ennek a hálóelméleti általánosítását (Kuros–Ore-tétel).
- A direkt szorzat fogalmának legáltalánosabb definíciója a kategóriaelméletből származik. A direkt szorzat belső jellemzése általános algebrákban kongruenciákkal történik. Csoportokban és gyűrűkben is módosítanunk kell ezen, hogy a normálosztókkal, illetve ideálokkal történő jellemzést megtaláljuk.

- A generált részstruktúra megkapható úgy, mint a generátorokat tartalmazó részstruktúrák metszete (ez a teljes hálók szintje). Az elemeit le lehet írni úgy, mint a generátoroknak a kifejezésfüggvényeknél fölvett értékeit (ez az általános algebrák szintje). Konkrét struktúrákban mindig új feladat, hogy ez a leírás milyen formában lehetséges (lineáris kombinációkkal a vektorterekben, modulusokban, szavakkal a csoportokban, normálformákkal a Boole-algebrákban).

Az algebrai módszerek alapja az, hogy, mint már említettük, struktúrákban gondolkodunk. A teljesség igénye nélkül megemlítünk néhány további, tipikus algebrai módszert.

- A *direkt szorzatra bontás* során a struktúrákat egyszerűbb alkotóelemekből állítjuk össze. Olyanokból, amelyekben már könnyebb számolni. A *szubdirekt szorzat* szerkezete nehezebben kezelhető, de több struktúrát bonthatunk szubdirekt szorzatra, mint direkt szorzatra.
- Hasonló fontosságú a *faktorstruktúra* fogalma is, amely azt teszi lehetővé, hogy hasonló tulajdonságú elemeket egymással azonosítsunk. Példa erre az a technika, amelynek segítségével a törteket bevezetjük a hányadostest nevű konstrukció révén (és a $2/4$ és $3/6$ törteket egyenlővé tesszük).
- A *reprezentációk* olyan homomorfizmusok, amelyek egy struktúrából egy másfajta struktúrába képeznek, ahol általában már jól lehet számolni. Például egy csoport elemeihez mátrixokat vagy permutációkat, egy Boole-algebra elemeihez halmazokat rendelhetünk.
- Ennek ellentéteképpen sokszor *szabadon* építünk bizonyos objektumokat, és ezekből kapjuk meg a vizsgált struktúrát egy homomorfizmus képeként.
- A *Gauss-elimináció* egy konkrét algoritmus, amit eredetileg lineáris egyenletrendszerek megoldására fejlesztettek ki. Alkalmas azonban mátrixok inverzének, determinánsának és Jordan-alakjának, továbbá kvadratikus alakok négyzetösszeg alakjának kiszámítására is.

A most leírt szemléletmód különösen alkalmas arra, hogy az egyes problémák megoldására egy másik területről származó módszereket alkalmazzunk. Az ilyen „interdiszciplináris” hozzáállás mindig nagyon megtermékenyítő.

♫ Például egyenletek megoldásainak vizsgálatára testeket, ezek megértéséhez pedig csoportokat használunk a Galois-elmélet keretében. Hasonló fontosságú a Pontrjagin-dualitás, amely a diszkrét és kompakt topologikus csoportok elméletét kapcsolja össze.

Végül egy általános megjegyzést teszünk a matematikáról. A matematika fejlődése nem olyan egyszerű folyamat, hogy megoldjuk a gyakorlatban, vagy a más tudományokban fölmerülő problémákat. Azért nem, mert sokszor előfordul, hogy nem vagyunk elég okosak, és ezért ezeket a problémákat nem tudjuk megoldani azonnal. Gyakori tapasztalat, hogy ilyenkor segíthet a megoldásban a matematika egy másik területe, egy olyan terület, amelyet eredetileg egészen más célból, más problémák megoldása végett fejlesztettek ki. Példaként megemlítjük az RSA titkosítási rendszert, amelyet manapság állandóan alkalmaznak, és amely annak köszönheti a megszületését, hogy az emberiség egy másik, teljesen elvontnak és alkalmazhatatlannak tűnő problémát vizsgált: azt, hogy nagyon nagy számokat milyen eljárással lehet gyorsan prímtényezőkre bontani.

♫ A jó problémák azok, amelyek új, még feltáratlan területekre, új jelenségek megértésére vezetnek. A keletkező elméletek azután már sokszor gyakorlati alkalmazásokat is adnak. Jó példa erre, hogy az egyenletek megoldóképletének vizsgálata a Galois-elmélet kifejlődéséhez vezetett, ennek segítségével értettük meg a véges testek szerkezetét, ezeket pedig, szinte váratlan módon, alkalmazni lehet a híradástechnikában, pontosabban a kódelméletben.

A matematika most leírt fejlődési folyamata hasonlít ahhoz, ahogy az Élet terjeszkedik, és egyre újabb területeket vesz birtokába. Eleinte a véletlenen, például mutációkon, tengeráramlatok szeszélyein múlik, hogy egy-egy organizmus „megpróbálkozik-e” valami újdonsággal. Azután „követői” is akadnak, akik közül nagyon sok elpusztul. De lassan kiderül az „igazság”: a helyes stratégia, amivel az új körülményekhez alkalmazkodni lehet. Ugyanígy számos matematikai kísérletet kell tennünk, problémákat megoldanunk, tételt bizonyítanunk, elméletet készítenünk, míg végül a helyes irányra rábukkanunk, és az „elefántot” megtaláljuk.

A matematikát tehát nem egy (tétel)gyárhoz vagy csirkefarmhoz érdemes hasonlítani, hanem inkább a természethez, ahol minden mindennel összefügg. Egy-egy terület életképességét nemcsak az eredményei szabják meg, hanem az is, hogy hogyan tud beilleszkedni az egészbe, milyen kapcsolatokat tud teremteni. A fejlődést sokszor belső törvényszerűségek szabályozzák, ezek egy kifejeződési formája a matematika *esztétikuma*. A matematikusok által izgalmasnak, érdekesnek, szépnek tartott kérdések megválaszolása számtalanszor vezetett döntő áttöréshez. Olyan ötletek merülhetnek így föl, amelyekhez máshogy el sem juthattunk volna. A matematikát alkalmazni szándékozók azután meglátogathatják a természetet, és megtalálhatják azt az erdei gyümölcsöt, gombát, amire éppen szükségük van.

Ha kirándulunk a természetben, akkor meg is erősödünk. A matematikával való foglalkozás pedig megerősíti az általános emberi gondolkodásnak egy nagyon fontos fajtáját: azt, amikor szisztematikusan végig kell gondolnunk valamit. Ez lehet köznapi dolog, mondjuk bútortologatási stratégia egy zsúfolt lakásban, de lehet számítástechnikai probléma, vagy akár jogi kérdés is. Mindezt problémamegoldással, fogalmak, bizonyítások megértésével edzhetjük. A matematikának része a matematikai logika, amely ezt a fajta gondolkodásmódot vizsgálja, és teljes megbízhatósággal kezeli.