4. fejezet

Példák

Struktúrák vagy struktúraosztályok vizsgálatát minden esetben azzal kezdjük, hogy megadjuk azok hasonlósági típusait, vagyis azokat a függvény- és relációjeleket, melyeknek megfelelő függvények és relációk tulajdonságaival kívánunk foglalkozni. Magukat a struktúrákat csak ezután lehet definiálni. Így például a gráfelmélet olyan *gráfok*nak nevezett struktúrákat vizsgál, melyek típusa egyetlen $\acute{E}$ kétváltozós relációjelet tartalmaz. A struktúra alaphalmazát a gráf *szögpont*jainak vagy *csúcs*ainak nevezzük, és a két szögpont *él*lel van összekötve, ha a belőlük alkotott párra az $\acute{E}$ reláció (interpretáltja) fennáll. A csoportelmélet struktúráinak típusa az e konstansjelet (egységelem), a $^{-1}$ egyváltozós és a $\cdot$ kétváltozós függvényjelet tartalmazza. Ezt a típust egyszerűen $\langle e, ^{-1}, \cdot \rangle$ hármassal jelöljük, hasonlóan más típusokat is, ha a jelekről világos (vagy előtte megmondtuk), hogy függvény- vagy relációjelek, és hogy hány változósak.

A t hasonlósági típus rögzítésével automatikusan egy elsőrendű nyelv, a t típusú formulák halmaza is rendelkezésünkre áll, ezt a vizsgálandó elmélet *nyelv*ének szokás nevezni. Amennyiben fel tudunk írni olyan formulákat, melyek egyértelműen jellemzik a vizsgálandó struktúraosztályt, a felírt formulákat *axiómák*nak, a struktúraosztályt pedig *axiomatizálható*nak nevezzük.

4.1. Definíció Legyen $\mathcal{K}$ egy t típusú struktúrákból álló osztály. $\mathcal{K}$-ról azt mondjuk, hogy *axiomatizálható*, ha van formuláknak olyan $\Gamma \subset F(t)$ halmaza, hogy tetszőleges t-típusú $\mathfrak{A}$ struktúrára $\mathfrak{A} \in \mathcal{K}$ pontosan akkor, ha minden $\varphi \in \Gamma$-ra $\mathfrak{A} \models \varphi$. A $\mathcal{K}$ *végesen axiomatizálható* ha véges ilyen formulahalmaz is van.

Az axiomatizálhatóság a legtöbb algebrai struktúraosztályban automatikusan teljesül, hiszen ezeket az osztályokat általában úgy jelölik ki, hogy bizonyos feltételeket szabnak, melyeket egy struktúrának ki kell elégítenie ahhoz, hogy csoport, gyűrű, test stb. legyen. Amit ellenőrizni kell az, hogy ezek a feltételek éppen egy-egy formula igazságát követelik meg. Teljesen más a helyzet, ha egy konkrét struktúra axiomatizálásáról van szó. Ezek közül is kettő emelkedik ki fontosságával: a természetes számok elmélete és a halmazelmélet. Ezek axiomatizálása, pontosabban az erre irányúló kisérletek vezettek végül is a modern halmazelmélet és a matematikai logika kialakulásához. Mint látni fogjuk, ezek a kisérletek eleve kudarcra voltak ítélve.

A továbbiakban különböző struktúraosztályokat mutatunk be (elsősorban az algebra területéről), melyek jól illusztrálják az eddigieket.

1. Gráfok

Egy $\langle \acute{E} \rangle$ típusú $\mathcal{G}$ struktúra (irányítatlan, hurokmentes) *gráf*, ha az $\acute{E}$ kétváltozós reláció irreflexiv és szimmetrikus (az első a hurokmentességet, a másik az irányítatlanságot jelenti), és ez akkor van így, ha $\mathcal{G}$-ben a következő két formula teljesül (emlékezzünk rá, hogy x és y változójelek):

(i)	$\neg \acute{E}(x,x)$	(irreflexivitás)
(ii)	$\acute{E}(x,y) \to \acute{E}(y,x)$	(szimmetria)

A gráfok osztálya tehát végesen axiomatizálható: ez a két formula megteszi ezt a szívességet. Gráfok különböző tulajdonságai is megfogalmazhatók ezen a nyelven, például az, hogy a gráf nem tartalmaz háromszöget. Tetszőleges $\mathcal{G}$ gráfra

$$\mathcal{G} \models \forall x\, \forall y\, \forall z\, (\neg \acute{E}(x,y) \vee \neg \acute{E}(y,z) \vee \neg \acute{E}(z,x))$$

pontosan akkor, ha tetszőleges x, y, z szögpontokra nincs mind a három x, y és z között vezető él behúzva, vagyis ha a gráf háromszögmentes. Gráfok más (igazán fontos) tulajdonságai sajnos ezen az egyszerű nyelven már nem fogalmazhatók meg. Például azokból a gráfokból álló struktúrák, melyek összefüggők, 3-kromatikusak, stb, nem axiomatizálhatók az $\langle \acute{E} \rangle$ típusú nyelv fölött.

2. Rendezés

Tegyük fel, hogy az $\mathfrak{A}$ struktúra hasonlósági típusában szerepel a $\leq$ kétváltozós relációjel. Ezt a relációt *parciális rendezésnek*, vagy *részbenrendezésnek* nevezzük, ha reflexív, antiszimmetrikus és tranzitív, vagyis ha $\mathfrak{A}$-ban igazak a következő formulák:

(i)	$x \leq x$	(reflexív)
(ii)	$x \leq y \wedge y \leq x \to x = y$	(antiszimmetrikus)
(iii)	$x \leq y \wedge y \leq z \to x \leq z$	(tranzitív)

Korábbi megállapodásaink értelmében x, y, z változójelek, és $\leq(x,y)$ helyett írhatunk $x \leq y$-t is, tehát ezek valóban formulák.

Ha ezeken kívül még az is igaz, hogy bármely két elem összehasonlítható, azaz $\mathfrak{A}$-ban még az

(iv) $$x \leq y \vee y \leq x$$

formula is teljesül, akkor *lineáris rendezésről*, vagy egyszerűen csak rendezésről beszélünk, (i)-(iv) a *rendezés* axiómái. Ha ezekhez hozzátesszük a következő axiómát:

(v) $$\forall x\, \forall y\, [(x \leq y \wedge x \neq y) \to \exists z\, (x \leq z \wedge z \leq y \wedge x \neq z \wedge z \neq y)],$$

akkor a *sűrű rendezést* axiomatizáltuk: bármely két (különböző) elem között van még elem. Ilyen például a racionális vagy valós számok nagyság szerinti rendezése. Ha csak azokat a sűrű rendezéseket akarjuk vizsgálni, melyeknek sem kezdő, sem végpontjuk nincs, még a

(vi) $$\begin{gathered} \forall x\, \exists y\, (y \leq x \wedge y \neq x) \\ \forall x\, \exists y\, (x \leq y \wedge x \neq y) \end{gathered}$$

axiómákat is hozzá kell vennünk az előzőkhöz.

Egy lineáris rendezés *diszkrét*, ha a sűrű rendezéssel ellentétben bármely elemnek, ha az nem az első, van közvetlen megelőzője és ha nem az utolsó, akkor van közvetlen rákövetkezője. Ennek axiomatizálásához (i)-(iv)-hez a következő két formulát kell hozzátenni:

$$\text{(vii)}\quad \begin{array}{l} \forall x\left(\exists y\,(y \le x \wedge y \neq x) \to \exists y\,(y \le x \wedge y \neq x \wedge \forall z(z \le x \to z = x \vee z \le y))\right), \\ \forall x\left(\exists y\,(x \le y \wedge y \neq x) \to \exists y\,(x \le y \wedge x \neq y \wedge \forall z(x \le z \to x = z \vee y \le z))\right). \end{array}$$

A diszkrét rendezések között fontosak a kezdőponttal rendelkező, végpont nélküli rendezések, ilyen a természetes számok szokásos nagyság szerinti rendezése. Ezt (i)-(iv) és (vii) mellett a

$$\text{(viii)}\quad \begin{array}{c} \exists x\,\forall y\,(y \le x \to y = x) \\ \forall x\,\exists y\,(x \le y \wedge x \neq y) \end{array}$$

formulák hozzáadásával axiomatizálhatjuk.

Egy $\mathfrak{A}$ struktúra $\le$ parciális rendezéséről azt mondjuk, hogy *jól fundált*, ha A bármely nem-üres B részhalmazában van minimális elem, vagyis olyan $a \in B$, hogy tetszőleges $b \in B$-re $b \le a \to b = a$. Ha a $\le$ rendezés lineáris és jól fundált, akkor azt mondjuk, hogy *jólrendezés*. Egy lineáris rendezésben bármely két elem összehasonlítható, azért egy jólrendezett halmaz minden nem-üres B részében van legkisebb elem, azaz olyan $a \in B$, hogy minden $b \in B$-re $a \le b$. Sem a jól fundált parciális rendezés, sem a jólrendezés nem axiomatizálható, azaz nincs a $\langle \le \rangle$ típusú formuláknak olyan részhalmaza, ami egyértelműen jellemezné az egyik vagy a másik fajta rendezett halmazokat.

3. Csoportok

A csoportok $\langle 0, -, + \rangle$ típusú struktúrák, ahol 0 konstansjel, a $-$ egyváltozós, a $+$ pedig kétváltozós függvényjel, és persze a szabályos $-(x)$ függvényjelölés helyett egyszerűen $(-x)$-et írunk. Egy $\langle 0, -, + \rangle$ típusú $\mathcal{G}$ struktúra *csoport*, ha $\mathcal{G}$-ben a következők teljesülnek:

(i)	$(x+y)+z = x+(y+z)$	(asszociatív)
(ii)	$0 + x = x$	(a 0 baloldali nullelem)
(iii)	$(-x) + x = 0$	(a $-x$ bal inverze x-nek)

Ezek a formulák alkotják a *csoportaxiómákat*. Ha egy struktúrában ezek igazak, akkor ott további állításoknak is teljesülniük kell, többek között annak, hogy 0 jobb oldali nullelem is, és hogy $-x$ jobb inverz is, azaz $\mathcal{G} \models x + 0 = x$ és $\mathcal{G} \models x + (-x) = 0$ minden $\mathcal{G}$ csoportra. Ez utóbbi formulákról azt mondjuk, hogy az (i)–(iii) formulák *következményei*: valahányszor (i)–(iii) igaz, szükségképpen igazak azok következményei is.

A csoportok osztályának fontos részosztályát alkotják a *kommutatív* vagy *Abel-csoportok*, ezekben (i)–(iii) mellett teljesül a

$$\text{(iv)}\quad x + y = y + x$$

formula is.

Egy csoport x elemének *rendje* a legkisebb olyan $n > 0$ egész szám, amire $x + x + \ldots + x = 0$ (n-tagú összeg), illetve ha ilyen nincs, az elem rendje végtelen. Rögzített $n > 0$-ra az alábbi n-tagú összeget $(\ldots((x + x) + x) + \ldots) + x$ röviden csak $n \cdot x$-nek írjuk. Így $n \cdot x$ egy kifejezés rövidítése. Ha egy Abel-csoport minden elemének rendje egy p prímszám, akkor a fenti (i)-(iv) formulákon kívül a

(v)$_p$
$$p \cdot x = 0$$

formula is teljesül, ezzel axiomatizáltuk azt az Abel-csoportokból álló osztályt, melyben a csoport minden 0-tól különböző eleme p-ed rendű. Hasonlóan azokat az Abel-csoportokat, melyekben nincs véges rendű elem, vagyis a *torziómentes* Abel-csoportokat úgy axiomatizálhatjuk, hogy (i)-(iv)-hez minden $n \geq 1$-re hozzávesszük a

(vi)$_n$
$$x \neq 0 \to n \cdot x \neq 0$$

formulát. Természetesen ez nem véges axiómarendszer, és látni fogjuk, hogy ez az osztály nem is axiomatizálható végesen. Ha a fentieken kívül még minden $n \geq 1$-re hozzávesszük a

(vii)$_n$
$$\forall x\, \exists y\, (n \cdot y = x)$$

formulát, akkor az *osztható* torziómentes Abel-csoportok osztályát axiomatizáltuk.

Végül egy csoport *torziócsoport*, ha benne minden elem rendje véges. A torziócsoportok osztálya nem axiomatizálható.

4. Testek

Végesen axiomatizálható osztályt alkotnak a testek is. Ezek $\langle 0, 1, -, ^{-1}, +, \cdot \rangle$ típusú struktúrák, ahol 0 és 1 konstansjelek, a $-$ és a $^{-1}$ egyváltozós, a $+$ és a $\cdot$ pedig kétváltozós függvényjelek. $\mathcal{F}$ test, ha $\mathcal{F}$-ben csak a $\langle 0, -, + \rangle$ jeleket tartva meg, Abel-csoportot kapunk, az $\langle F - \{0\}, 1, ^{-1}, \cdot \rangle$ struktúra csopotot alkot, végül a $+$ és $\cdot$ műveleteket a disztributivitási szabályok kötik össze:

$$x \cdot (y + z) = (x \cdot y) + (x \cdot z)$$
$$(x + y) \cdot z = (x \cdot z) + (y \cdot z)$$

Ha egy testben a szorzás kommutatív, azt *kommutatív testnek* nevezik. Mivel mi csak kommutatív testekkel foglalkozunk, ezt a jelzőt nem tesszük ki, test alatt kommutatív testet értünk.

Testre példa a racionális, a valós vagy a komplex számok halmaza a szokásos műveletekkel, de test az a struktúra is, melynek alaphalmaza mindössze a 0 és 1 elemeket tartalmazza, és rajta az összeadást és a szorzást a következő táblázatokkal definiáljuk:

$+$	0	1
0	0	1
1	1	0

$\cdot$	0	1
0	0	0
1	0	1

A véges testeket *Galois-testeknek* nevezik, ezeket egyértelműen (az izomorfia erejéig) meghatározza elemszámuk, ami csak prímhatvány lehet. Ha p prímszám, a p^n-elemű Galois testet $\mathcal{GF}(p^n)$ jelöli.

Egy test *karakterisztikája* az a legkisebb p szám, amire a test 1 elemét p-szer önmagához adva 0-t kapunk. Ha ilyen p nincs, a testet 0-karakterisztikájúnak szokás nevezni. Így a fenti két elemű test, a $\mathcal{GF}(2)$, karakterisztikája 2, a általában $\mathcal{GF}(p^n)$ karakterisztikája éppen p. A racionális, valós vagy komplex számok 0 karakterisztikájúak. Karakterisztika csak prímszám lehet, s a p karakterisztikájú testeket úgy axiomatizálhatjuk, hogy a test axiómákhoz még a

(i)$_p$ $$(\ldots(1+1)+\ldots)+1=0 \qquad (p \text{ darab 1-es})$$

formulát is hozzávesszük, ha pedig minden p prímre a

(ii)$_p$ $$(\ldots(1+1)+\ldots)+1\neq 0 \qquad (p \text{ darab 1-es})$$

axiómákat tesszük a test axiómákhoz, akkor a 0 karakterisztikájú testek axiómarendszerét kapjuk.

Egy test *algebrailag zárt*, ha benne minden polinomnak van gyöke. Ezt a feltételt legegyszerűbben úgy fogalmazhatjuk meg, hogy minden $n \geq 1$-re igaz a következő formula:

(iii)$_p$ $$x_n = 0 \vee \exists y\,(x_n \cdot y^n + x_{n-1}\cdot y^{n-1} + \ldots + x_1 \cdot y + x_0 = 0),$$

természetesen y^n az $(\ldots((y\cdot y)\cdot y)\ldots)$ kifejezés rövidítése.

Egy test *valósan zárt*, ha olyan mint a valós számok testje, azaz ha -1 nem áll elő két négyzetszám összegeként; ha bármely számra vagy ő vagy az ellentettje négyzetszám; végül ha minden páratlan fokú polinomnak van gyöke. Ez utóbbi feltételt éppen (iii)$_n$ írja le páratlan n-ekre, az előbbi kettő pedig a következőképpen formalizálható:

(vi) $$\begin{gathered}\forall x\,\forall y\,(x\cdot x + y\cdot y + 1 \neq 0)\\ \forall x\,\exists y\,(y\cdot y + x = 0 \vee y \cdot y = x)\end{gathered}$$

Egy $\langle 0,1,-,^{-1},+,\cdot,\leq\rangle$ típusú struktúra *rendezett test*, ha az első hat szimbólumra nézve (kommutatív) test, a $\leq$-re nézve lineáris rendezés, és még teljesülnek a következők is:

(vii) $$\begin{gathered}x\leq y \to x+z \leq y+z\\ 0\leq x \wedge 0 \leq y \to 0 \leq x\cdot y\end{gathered}$$

A valósan zárt testeken mindig lehet olyan rendezést definiálni, amivel rendezett testté válik: $x \leq y$ pontosan akkor, ha $\exists z\,(y = x + z\cdot z)$. Egy rendezett test *archimédeszi*, ha teljesül benne az ún. archimédeszi axióma, vagyis minden pozitív elem kisebb az 1, $1+1$, $1+1+1, \ldots$ elemek valamelyikénél. Az archimédeszi testek osztálya nem axiomatizálható.

5. Hálók, Boole algebrák

Egy $\leq$ részbenrendezésről azt mondjuk, hogy *hálószerű*, ha bármely két elemnek létezik legkisebb felső és legnagyobb alsó korlátja:

(i) $\forall x\, \forall y\, \exists z\, (x \leq z \wedge y \leq z \wedge \forall z_1\, (x \leq z_1 \wedge y \leq z_1 \rightarrow z \leq z_1))$

(ii) $\forall x\, \forall y\, \exists z\, (z \leq x \wedge z \leq y \wedge \forall z_1\, (z_1 \leq x \wedge z_1 \leq y \rightarrow z_1 \leq z))$

Az x és y elemek legkisebb felső korlátját $(x \cup y)$-nal, legnagyobb alsó korlátját $(x \cap y)$-nal jelölve* könnyen látható, hogy ezekre a következő tulajdonságok teljesülnek:

(iii)

$x \cup x = x,$	$x \cap x = x$	(idempotens)
$x \cup y = y \cup x,$	$x \cap y = y \cap x$	(kommutatív)
$x \cup (y \cup z) = (x \cup y) \cup z,$	$x \cap (y \cap z) = (x \cap y) \cap z$	(asszociatív)
$(x \cup y) \cap x = x,$	$(x \cap y) \cup x = x$	(elnyelés)

Egy $\langle \cup, \cap \rangle$ típusú struktúrát *hálónak* nevezünk, ha benne az (iii) alatt felsorolt nyolc formula mindegyike igaz. Így ha adott egy hálórendezés, abban az $\cup$ és $\cap$ függvényeket mint argumentumaik legkisebb felső illetve legnagyobb alsó korlátjaiként definiáljuk, majd elfelejtkezünk a rendezésről, egy hálót kapunk. Ez fordítva is így van: tetszőleges hálón definiálható, mégpedig egyértelműen olyan hálórendezés, melyből a hálóműveleteket visszakaphatjuk. Először is az elnyelési tulajdonságok alapján a háló tetszőleges x, y elemeire $x \cup y = y$ pontosan akkor igaz, ha egyúttal $x \cap y = x$ is áll. Definiáljuk a háló elemein a $\leq$ kétváltozós relációt a következőképpen:

$$x \leq y \quad \text{pontosan akkor, ha} \quad x \cup y = y, \quad \text{azaz ha} \quad x \cap y = x.$$

Nem nehéz belátni, hogy ez a keresett hálórendezés.

Érdekességképpen megjegyezzük, hogy a műveletek idempotenciája következik az elnyelési tulajdonságokból, így azokat fölösleges külön kikötni.

Egy hálót *modulárisnak* neveznek, ha benne az

(iv) $$x \cup z = x \rightarrow (x \cap y) \cup z = z \cap (y \cup z)$$

formula is teljesül, és *disztributívnak*, ha mindkét művelet disztributív a másikra nézve, azaz ha

(v) $$(x \cup y) \cap z = (x \cap z) \cup (y \cap z), \quad (x \cap y) \cup z = (x \cup z) \cap (y \cup z).$$

Disztributív hálók egyúttal modulárisak is.

Legyen X egy halmaz, és álljon $\mathcal{A}$ az X bizonyos részhalmazaiból úgy, hogy $x, z \in \mathcal{A}$ esetén x és y egyesítése és metszete is tartozzon $\mathcal{A}$-hoz. Ekkor az $\mathfrak{A} = \langle \mathcal{A}, \cup, \cap \rangle$ struktúra, ahol $x \cup y$ az x és y egyesítése, $x \cap y$ pedig a metszete, disztributív háló. Ezeket a hálókat *halmazhálóknak* szokás nevezni. Disztributív hálókra érvényes az ún. Stone féle reprezentációs tétel:

* Az $\cup$ illetve $\cap$ jelek helyett, hogy a halmazelméleti unióval illetve metszettel ne legyen összekeverhető, szokás a $\vee$, $\wedge$ jeleket, újabban pedig az $\sqcup$, $\sqcap$ jeleket használni.

4.2. Tétel *Minden disztributív háló izomorf egy halmazhálóval.* ■

Hálótulajdonságokat nem csak erősíteni, hanem gyengíteni is lehet. A $\leq$ részbenrendezés felső-félháló (egyesítés félháló) rendezés, ha benne bármely két x, y elemről csak annyit követelünk meg, hogy létezzen legkisebb felső korlátjuk, azaz (i) teljesüljön.

Ezt az elemet $(x \cup y)$-nal jelölve az (iii) alatti formulák közül mindazok, melyekben a $\cap$ jel nem szerepel, továbbra is érvényben maradnak. Egy $\langle \cup \rangle$ típusú struktúra *felső félháló*, ha benne ezek a formulák megkaphatók egy egyértelműen meghatározott részbenrendezésből.

A Boole algebrák hasonlósági típusa a 0 és 1 konstansjelekből, a $^-$ (felülhúzás) egyváltozós, és $\cup, \cap$ kétváltozós függvényjelekből áll, természetesen $\overline{x}$ jelöli azt, hogy a felülhúzás függvényt alkalmaztuk az x-re. Egy $\mathfrak{B} = \langle B, 0, 1, ^-, \cup, \cap \rangle$ struktúra *Boole algebra*, ha $\langle B, \cup, \cap \rangle$ egy disztributív háló, továbbá fennállnak még az

$$\text{(vi)} \quad \begin{array}{ll} \overline{x \cup y} = \overline{x} \cap \overline{y}, \quad \overline{x \cap y} = \overline{x} \cup \overline{y} & \text{(deMorgan szabályok)} \\ \overline{\overline{x}} = x & \\ \overline{0} = 1 & \\ x \cup 0 = x, \ x \cap 0 = 0, \ x \cup \overline{x} = 1, \ x \cap \overline{x} = 0 & \end{array}$$

formulák is.

Legyen X egy halmaz, jelölje $x \subset X$ komplementerét, vagyis az $X \setminus x$ halmazt $\overline{x}$, $x, y \subset X$ egyesítését, metszetét $x \cup y$ és $x \cap y$. Álljon $\mathcal{A}$ az X bizonyos részhalmazaiból, és tegyük fel, hogy $\mathcal{A}$ zárt a komplementerképzésre, egyesítésre és metszetre, továbbá hogy $X \in \mathcal{A}$ (és ekkor persze $\overline{X} = \emptyset$ miatt $\emptyset \in \mathcal{A}$ is igaz). Az

$$\mathfrak{A} = \langle \mathcal{A}, \emptyset, X, ^-, \cup, \cap \rangle$$

struktúrát *halmazalgebrának* nevezzük, ez könnyen láthatóan Boole algebra.

4.3. Tétel (Boole algebrák reprezentációs tétele) *Minden Boole algebra izomorf egy halmazalgebrával.* ■

A $\mathfrak{B}$ Boole algebra speciálisan háló is, így elemein egy részbenrendezést tudunk definiálni: $x \leq y$ akkor, ha $x \cap y = x$. Az algebra egy $b \in B$ elemét *atomnak* nevezzük, ha 0-tól különbözik, és közte és 0 között nincs más elem:

$$\forall x \, (x \leq b \rightarrow (x = 0 \vee x = b)).$$

Egy Boole algebra *atomos*, ha benne minden 0-tól különböző elem alatt van atom, azaz ha

$$\forall x \, \left[x \neq 0 \rightarrow \exists y \, (y \neq 0 \wedge y \leq x \wedge \forall z \, (z \leq y \rightarrow z = 0 \vee z = y)) \right],$$

itt persze $y \leq x$ és $z \leq y$ helyett $y \cap x = y$ illetve $z \cap y = z$-t kellett volna írnunk. Ezzel az atomos Boole algebrák osztályát sikerült axiomatizálnunk. Végül a Boole algebra *atommentes*, ha nincs benne atom, azaz ha $\mathfrak{B}$-ben a

$$\forall x \, (\forall y \, (y \leq x \rightarrow y = 0 \vee y = x) \rightarrow x = 0)$$

formula igaz. Nyilván minden véges Boole algebra atomos, és vannak Boole algebrák, melyek nem atomosak és nem atommentesek.

6. Aritmetika, Peano axiómák

Eddigi példáinkban struktúraosztályokat definiáltunk, most egy konkrét struktúráról lesz szó: a természetes számokéról. Még a múlt század hetvenes éveiben *R. Dedekind* fogalmazta meg azokat az „axiómákat,” melyek feladata – a geometria Euklidesz-féle axiómáihoz hasonlóan – az volt, hogy ezt a struktúrát definiálják. Dedekind definícióinak pontosított, elsőrendű formulákkal leírt változata a természetes számoknak az az axiómarendszere, melyet *Peano axiómák* néven ismerünk. Az axiómarendszer jelkészlete a 0 és 1 konstansjelekből, a $+$ és $\cdot$ kétváltozós függvényjelekből áll, ezt a hasonlósági típust t^{PA} jelöli. Az axiómarendszer, melyet *PA*-val jelölünk, a következő formulákból áll:

(P1) $x+1 \neq 0$
(P2) $x+1 = y+1 \to x = y$
(P3) $x+0 = x$
(P4) $x+(y+1) = (x+y)+1$
(P5) $x \cdot 0 = 0$
(P6) $x \cdot (y+1) = x \cdot y + x$

Végül tetszőleges $\varphi(x) \in F(t^{PA})$ formulára

(P7) $\big[\varphi(0) \wedge \forall x\,(\varphi(x) \to \varphi(x+1))\big] \to \forall x\,\varphi(x).$

Az $x+1$ számot x *rákövetkezőjének* nevezzük, P1 és P2 ennek tulajdonságait mondják ki: a 0 semminek sem a rákövetkezője, és ha két szám rákövetkezője megegyezik, akkor a számoknak is meg kell egyezniük. P3 és P4 az összeadást, P5 és P6 pedig a szorzást definiálja. Végül P7 alatt az ún. *indukciós axiómákat* soroltuk fel, ezek hétköznapi nyelvre lefordítva a következőket jelentik: ha φ a természetes számok valamely tulajdonsága, ami igaz a 0-ra továbbá minden x-ről öröklődik a rákövetkezőjére, akkor minden természetes szám φ tulajdonságú. A P7 típusú formulahalmazokat *axiómasémának* szokás nevezni, esetünkben P7 az indukciós axiómaséma.

A természetes számok „valamiféle tulajdonságán” azok egy részhalmazát szokás érteni. Az aritmetika nyelvén azonban részhalmazokról nem beszélhetünk, így meg kell elégednünk azzal, hogy az összes ezen a nyelven definiálható részhalmazt sorra vesszük és mindegyikre külön-külön felírjuk az indukciót. Ám részhalmazból kontinuum sok van, formulából pedig csak megszámlálható, így P7 kevesebbet mond, mint a teljes indukció intuitív fogalma.

Azt a t^{PA} típusú struktúrát, melynek alaphalmazát a természetes számok alkotják, az egyes jelek interpretáltja pedig az, amit elvárunk: 0 a nullának, 1 az egynek, $+$ az összeadásnak és $\cdot$ a szorzásnak felel meg, $\mathfrak{N}$-nel jelöljük. $\mathfrak{N}$-ben természetesen igazak a Peano axiómák, ezt nevezzük a *PA sztenderd modelljének*. Az összes többi modellt, azaz mindazokat az $\mathfrak{N}$-nel nem izomorf t^{PA} típusú struktúrákat, melyekben *PA* igaz, *nemsztenderd modelleknek* hívjuk. Az lenne az igazi, ha nemsztenderd modellek egyáltalán nem volnának, mert ekkor *PA* egyértelműen leírná az $\mathfrak{N}$ struktúrát.

Bár az axiómák az összeadásról és szorzásról nagyon keveset mondanak, azok sok fontos tulajdonsága minden Peano modellben igaz.

4.4. Lemma *Legyen $\mathfrak{A}$ egy t^{PA} típusú struktúra, melyre $\mathfrak{A} \models PA$. Ekkor $\mathfrak{A}$-ban igazak a következő formulák is:*

(i)	$x + y = y + x,$	$x \cdot y = y \cdot x$	(kommutatív)
(ii)	$(x + y) + z = x + (y + z),$	$(x \cdot y) \cdot z = x \cdot (y \cdot z)$	(asszociatív)
(iii)	$(y + z) \cdot x = y \cdot x + z \cdot x$		(disztributív)
(iv)	$x + z = y + z \to x = y$		
(v)	$x + y = 0 \to x = 0 \wedge y = 0,$	$x \cdot y = 0 \to x = 0 \vee y = 0$	
(vi)	$x \neq 0 \to \exists y\,(x = y + 1)$		

Bizonyítás Csak a disztributivitást bizonyítjuk, a többi formula igazsága hasonlóan látható be. A P7 indukciós axiómasémát akarjuk használni a következő $\varphi(x) \in F(t^{PA})$ formulára:

$$(y + z) \cdot x = y \cdot x + z \cdot x.$$

Először is, $\mathfrak{A} \models \varphi(0)$. Valóban, P5 szerint $(y + z) \cdot 0 = 0$, $y \cdot 0 = 0$ és $z \cdot 0 = 0$ a változójelek tetszőleges $\mathfrak{A}$-beli értékelése mellett, továbbá P3 szerint $0 + 0 = 0$, ahonnan $\mathfrak{A} \models (y + z) \cdot 0 = y \cdot 0 + z \cdot 0$, ahogyan kívántuk.

Másodjára $\mathfrak{A} \models \varphi(x) \to \varphi(x + 1)$. Ennek igazolásához rögzítsük a változójelek egy tetszőleges e értékelését. Azt kell megmutatnunk, hogy $\mathfrak{A} \models (\varphi(x) \to \varphi(x + 1))[e]$, azaz ha $\mathfrak{A} \models \varphi(x)[e]$, akkor $\mathfrak{A} \models \varphi(x + 1)[e]$. Ha most (elég szabálytalanul, de szokás szerint) az x, y, z változójelekhez rendelt A-beli elemeket is x, y, z-vel jelöljük, az $\mathfrak{A}$-beli összeadást $+$-szal, a szorzást $\cdot$ jellel, akkor ez utóbbi éppen azt jelenti, hogy

$$(*) \qquad (y + z) \cdot (x + 1) = y \cdot (x + 1) + z \cdot (x + 1)$$

Mivel $\mathfrak{A}$-ban igaz a P6 formula, azért azt a megfelelő értékelésekre alkalmazva adódik, hogy

$$(y + z) \cdot (x + 1) = (y + z) \cdot x + (y + z),$$

valamint

$$y \cdot (x + 1) = y \cdot x + y, \qquad z \cdot (x + 1) = z \cdot x + z.$$

Így a $(*)$ bal oldala $(y + z) \cdot x + (y + z)$, jobb oldala pedig $(y \cdot x + y) + (z \cdot x + z)$, ami az összeadás kommutativitása és asszociativitása miatt (a tétel (i) és (ii) pontjai) $(y \cdot x + z \cdot x) + (y + z)$-vel egyenlő. Így *ha* $\mathfrak{A} \models \varphi(x)[e]$, azaz $(y + z) \cdot x = y \cdot x + z \cdot x$, *akkor* persze

$$(y + z) \cdot x + (y + z) = (y \cdot x + z \cdot x) + (y + z)$$

is igaz (a $+$ függvény argumentumai mindkét oldalon egyenlők, tehát a függvényértékek is egyenlők), tehát ekkor $\mathfrak{A} \models \varphi(x + 1)[e]$ is teljesül. Ezzel beláttuk, hogy $\mathfrak{A} \models \varphi(x) \to \varphi(x + 1)$ a változók tetszőleges értékelése mellett, és így $\mathfrak{A} \models \forall x\,(\varphi(x) \to \varphi(x + 1))$.

Végül $\mathfrak{A}$-ban a P7 axiómasémát a fenti $\varphi(x)$ formulára felírva

$$\mathfrak{A} \models [\varphi(0) \wedge \forall x\,(\varphi(x) \to \varphi(x + 1))] \to \forall x\,\varphi(x).$$

Mivel a változójelek tetszőleges értékelése mellett a szögletes zárójelben álló formula igaz, azért igaznak kell lennie a konklúziónak is, tehát $\mathfrak{A} \models \forall x\,\varphi(x)$, ami éppen a kívánt állítást adja. ■

Tetszőleges $\mathfrak{A}$ Peano-modell alaphalmazán definiálhatjuk a következő kétváltozós relációt: $a, b \in A$ esetén $a \leq b$, ha van olyan $c \in A$, melyre $c + a = b$. Világos, hogy $\mathfrak{N}$-en a $\leq$ reláció egybeesik a természetes számok szokásos rendezésével.

4.5. Lemma *A $\leq$ reláció végpont nélküli diszkrét rendezés A-n.*

Bizonyítás Először azt mutatjuk meg, hogy a $\leq$ parciális rendezés, azaz reflexív, antiszimmetrikus és tranzitív. Az előző lemma szerint $\mathfrak{A}$-ban az összeadás kommutatív, így tetszőleges $a \in A$-ra $a + 0 = 0 + a$, és ez P3 szerint a-val egyenlő: $0 + a = a$. Ezért $a \leq a$, ami a reflexivitást adja. Tegyük fel most, hogy $a \leq b$ és $b \leq a$, azaz vannak olyan c_0 és $c_1 \in A$ elemek, hogy $c_0 + a = b$ és $c_1 + b = a$. Ekkor az összeadás asszociativitása miatt $a = c_1 + b = c_1 + (c_0 + a) = (c_1 + c_0) + a$, tehát az előző lemma (iv) pontja alapján $0 = c_1 + c_0$, ahonnan $c_0 = c_1 = 0$, és ezért $a = b$, ami az antiszimmetriát adja. Végül a tranzitivitás azonnal következik az összeadás asszociativitásából és kommutativitásából.

Azt, hogy A-nak bármely két eleme összehasonlítható, P7 felhasználásával igazoljuk. Az, hogy $a, b \in A$ összehasonlíthatók, azt jelenti, hogy van olyan $c \in A$ melyre vagy $c + a = b$, vagy $c + b = a$. Ez viszont azonnal adódik abból, hogy a következő $\varphi(x)$ formula igaz $\mathfrak{A}$-n:

$$\exists z\,(z + x = y \vee z + y = x).$$

Így feladatunk annak igazolása, hogy $\mathfrak{A} \models \varphi(x)$. Először $\mathfrak{A} \models \varphi(0)$, hiszen P3 alapján $\mathfrak{A} \models y + 0 = y$, így tényleg van olyan z, amire $\mathfrak{A} \models z + 0 = y \vee z + y = 0$. Az $\mathfrak{A} \models \varphi(x) \to \varphi(x + 1)$ igazolásához megint rögzítsük a változók egy e értékelését, ami mellett $\mathfrak{A} \models \varphi(x)[e]$. Most van olyan A-beli elem, amit a kvantor mögötti formulában z helyébe téve az igaz lesz, jelöljük azt az elemet z-vel, x és y értékeit pedig (mi mással?) x-szel és y-nal. E szerint vagy $z + x = y$, vagy $z + y = x$ teljesül, esetleg mindkettő, és olyan $z' \in A$-t kell keresnünk, amire vagy $z' + (x + 1) = y$, vagy $z' + y = x + 1$. Tegyük fel elsőként, hogy $z + y = x$ teljesült. Ekkor P4 szerint $(z + 1) + y = (z + y) + 1 = x + 1$, és így $z' = z + 1$ megfelelő. Ha $z + x = y$ teljesült és $z \neq 0$, akkor 4.4. lemma (vi) pontja alapján van olyan $z' \in A$, amire $z = z' + 1$, és ekkor $y = z + x = (z' + 1) + x = z' + (x + 1)$, és ismét készen vagyunk. Végül ha $z = 0$, akkor $x = y$ és $1 + y = x + 1$, azaz most $z' = 1$ megteszi. Így mindenképpen van olyan $z' \in A$, amire vagy $z' + (x + 1) = y$, vagy $z' + y = x + 1$, vagyis $\mathfrak{A} \models \varphi(x + 1)[e]$. A P7 indukciós séma alapján ekkor $\mathfrak{A} \models \forall x\, \varphi(x)$, ahogyan kívántuk.

Azonnal látható, hogy a rendezésben a 0 minimális elem. Végül, hogy a $\leq$ diszkrét végpont nélküli rendezés abból következik, hogy minden $a, b \in A$-ra $b \leq b + 1$, és $a \leq b + 1$ esetén vagy $a \leq b$ vagy $a = b + 1$, vagyis b és $b + 1$ között nincs egyetlen elem sem. ■

Legyen $\varphi(x, y) \equiv \exists z\,(z + x = y) \in F(t^{PA})$. Vegyük észre, hogy tetszőleges $\mathfrak{A}$ Peano-modellben $a \leq b$ pontosan akkor áll, ha arra az e értékelésre, melyre $e(x) = a$ és $e(y) = b$, $\mathfrak{A} \models \varphi(x, y)[e]$. Azt mondjuk, a $\leq$ reláció *formulával definiálható PA* modelljein. Ha most t^{PA}-t kibővítjük a $\leq$ kétváltozós relációjellel, és további axiómaként *PA*-hoz hozzávesszük az

$$x \leq y \leftrightarrow \exists z\,(z + x = y)$$

formulát, akkor ezzel lehetővé tettük, hogy a rendezésről explicite is beszélhessünk, ne kelljen minduntalan a $\exists z\,(z + x = y)$ formulát használnunk, s elmondani, hogy az általa definiált relációról van tulajdonképpen szó. Egy nyelvnek az ilyen típusú bővítéseit — vagyis mikor új reláció- vagy függvényjeleket vezetünk be implicite, azaz formulával definiálható relációk és függvények jelölésére — *konzervatív bővítéseknek* nevezzük. Ezek a vizsgálandó axiómarendszer kifejezőerejét, erősségét, a benne definiálható fogalmakat nem befolyásolják, mindössze lerövidítik, kényelmesebbé, olvashatóbbá teszik a formulákat. Konzervatív bővítéseknek különösen fontos szerep jut az axiomatikus halmazelméletben, ahol az alapnyelv szegényességét ellensúlyozandó rendkívül sok új jelet definiálnak.

Mindezek alapján mostantól kezdve a $\leq$ jelet csakúgy mint a $<$, $>$, $\geq$ jeleket hozzágondoljuk a t^{PA} típushoz, és a Peano formulák felírásakor ezeket szabadon használjuk értelemszerű interpretációikkal egyetemben. Minden esetben világos, hogyan lehet ezeket a formulákat visszaírni e relációjelek nélküli alakjukba. Például azt a formulát, ami az összeadás monotonitását fejezi ki, a $\leq$ jelet használva a következőképpen írhatjuk fel:

$$x_0 \leq x_1 \wedge y_0 \leq y_1 \rightarrow x_0 + y_0 \leq x_1 + y_1,$$

míg ugyanez a $\leq$ relációjel nélkül így néz ki:

$$\exists x_2\,(x_2 + x_0 = x_1) \wedge \exists y_2\,(y_2 + y_0 = y_1) \rightarrow \exists z\,(z + (x_0 + y_0) = x_1 + y_1).$$

Innen mellékesen az is látszik, miért is igaz ez minden Peano-modellben: z-nek az x_2+y_2 megfelelő választás.

Szokás vizsgálni az aritmetikának csak az összeadást tartalmazó részét, amit *additív-* vagy *Presburger aritmetikának* neveznek. Ennek hasonlósági típusa $t^+ = \langle 0, 1, + \rangle$ abban különbözik t^{PA}-tól, hogy a szorzásjel nincs benne. A Presburger aritmetika axiómarendszerét, amit úgy kapunk PA-ból, hogy töröljük mindazokat a formulákat, melyekben szerepel a szorzásjel – magyarul a P5 és P6 axiómákat –, és P7-et csak $\varphi(x) \in F(t^+)$ esetén használjuk. PA^+ sztenderd modelljét nem túl meglepő módon $\mathfrak{N}^+$ jelöli, ez úgy áll elő $\mathfrak{N}$-ből, hogy a szorzásról „elfelejtkezünk."

Az eddig felsorolt, PA modelljeire vonatkozó állítások, melyekben a szorzásjel nem szerepelt, PA^+ modelljeire is érvényben maradnak. Többek között a $\exists z\,(z + x = y)$ formulával definiált reláció most is diszkrét lineráris rendezés, amire nézve az összeadás monoton művelet. Érdekes módon azonban a PA^+ és PA axiómarendszerek bármennyire is hasonlónak látszanak az első pillanatban, alapvetően különböznek egymástól. PA^+ a „legegyszerűbb," PA pedig a „legbonyolultabb" rendszerek közé tartozik.

7. Halmazelmélet

Az aritmetika axiómarendszerét azzal az elképzeléssel fogalmazták meg, hogy az minél pontosabban írja le a természetes számok intuitív fogalmát. A halmazelmélet axiómái viszont azt a célt szolgálják, hogy annak a „halmazvilágnak" a tulajdonságait foglalják össze, amely bizonyos értelemben otthont ad minden matematikai fogalomnak. Az axiómák így nem egy struktúráról vagy struktúraosztályról szólnak, hanem azt az intuitív képet teszik pontossá, ami a halmazokról, azok tulajdonságairól kialakult. A halmazelméletnek nincs „sztenderd" modellje, mint az aritmetikának, hanem úgy képzeljük, hogy az axiómák a halmazok világát írják le.

Magát az axiomatizálást a naiv halmazelméletben felbukkanó ellentmondások kényszerítették ki. Bizonyos halmazok létezésének feltételezése ellentmondásra vezet, így biztosítani kell, hogy ezek a halmazok „ne létezzenek." Ugyanakkor a rendszernek elég bőnek kell maradnia ahhoz, hogy benne a szokásos matematikai fogalmak, bizonyítási eljárások egyszerűen leírhatók legyenek. E két ellentétes követelmény eredményeképpen született meg az 1900-as évek elejére a halmazelméletnek ma általánosan elfogadott Zermelo-Fraenkel féle axiómarendszere. Ennek nyelve az egyenlőségjelen kívül egyetlen kétváltozós relációjelet tartalmaz, amit szokás szerint $\in$-nel jelölünk. A könnyebb olvashatóság kedvéért használni fogjuk a $\notin$ jelet is: $\neg(x \in y)$ helyett $x \notin y$-t írunk. Az axiómarendszer, melyet $\boldsymbol{ZF}$-fel szokás jelölni, a következő formulákból áll:

A0 *üres halmaz axiómája*: $\exists x\, \forall u\, (u \notin x)$.
Van olyan halmaz, aminek nincsenek elemei.

A1 *meghatározottsági axióma*: $\forall x\, \forall y\, (\forall u\, (u \in x \leftrightarrow u \in y) \rightarrow x = y)$.
Ha két halmaznak ugyanazok az elemei, akkor a két halmaz megegyezik. Ez többek között azt is jelenti, hogy legfeljebb egy olyan halmaz lehet, aminek nincsenek elemei. Az A0 axióma szerint viszont ilyen van, tehát a korábban mondottak szerint $\boldsymbol{ZF}$ jelkészletét kiegészíthetjük egy nullváltozós függvényjellel — azaz konstansjellel — ami ezt a meghatározott halmazt jelöli. Ez a jel a $\emptyset$, és definíciójaként a következő formulát írhatjuk fel: $\forall u\, (u \notin \emptyset)$.

A2 *pár axióma*: $\forall x\, \forall y\, \exists z\, \forall u\, (u \in z \leftrightarrow u = x \vee u = y)$.
Minden x, y párhoz van olyan halmaz, melynek pontosan ezek az elemei. A meghatározottsági axióma miatt csak egy ilyen lehet. Megint bővítjük a nyelvet, most egy kétváltozós $\{\}$ függvényjellel. Ez x-hez és y-hoz ezt az egyértelműen meghatározott halmazt rendeli. Persze $\{\}(x, y)$ helyett $\{x, y\}$-t írunk. Könnyű látni, hogy $\{x, y\} = \{y, x\}$ továbbá $\{x, x\}$ helyett az $\{x\}$ jelölés használatos.

Újabb bővítés: a $\subset$ kétváltozós relációjelet vezetjük be annak jelölésére, hogy az első halmaz minden eleme egyúttal eleme a második halmaznak is, azaz

$$x \subset y \leftrightarrow \forall v\, (v \in x \rightarrow v \in y).$$

Ha $x \subset y$, akkor azt mondjuk, hogy x részhalmaza y-nak.

A3 *hatványhalmaz axióma*: $\forall x\, \exists y\, \forall u\, (u \in y \leftrightarrow u \subset x)$.
Minden x halmazra létezik x összes részhalmazainak halmaza, amit x hatványhalmazának nevezünk. A1 szerint ez megint egyértelmű, és persze új egyváltozós függvényjelet vezetünk be ennek jelölésére: $u \in \mathcal{P}(x) \leftrightarrow u \subset x$.

A4 *egyesítési halmaz axióma*: $\forall x\, \exists y\, \forall u\, (u \in y \leftrightarrow \exists v\, (u \in v \wedge v \in x))$.
E szerint létezik az x elemeiből álló halmaz. Ez A1 szerint egyértelmű, és $\cup x$-szel jelöljük. Az $\cup\{x, y\}$ halmazt még $x \cup y$-ként is szokás írni, ennek elemei x és y elemei együtt, tehát $x \cup y$ éppen x és y egyesítése vagy uniója.

A5 *végtelen halmaz axiómája*: $\exists x\, (\emptyset \in x \wedge \forall y\, (y \in x \rightarrow y \cup \{y\} \in x))$.
Ez A0-on kívül az egyetlen axióma, mely egy halmaz létezését állítja, a többiek csak már létező halmazok mellé garantálják más halmazok létezését. A5 felírásában már használtuk a bevezetett jeleket, lássuk hogyan néz ki azok nélkül:

$$\exists x\, (\exists y\, (y \in x \wedge \forall v\, (v \notin y)) \wedge \forall y\, (y \in x \rightarrow \exists u\, (\forall v\, (v \in u \leftrightarrow v = y \vee v \in y) \wedge u \in x))).$$

Gondoljuk el, mi lenne, ha még a $\rightarrow$, $\leftrightarrow$, $\wedge$, $\forall$ rövidítéseket sem használhatnánk! Az axióma által szolgáltatott halmaznak eleme az üres halmaz, azután eleme az $\emptyset \cup \{\emptyset\} = \{\emptyset\}$

halmaz is, ami persze különbözik $\emptyset$-től, hiszen egy eleme van, míg az $\emptyset$ halmaznak egy sincs. A $\{\emptyset\}$ halmazt jelöljük $\underline{1}$-gyel, s általában ha egy n természetes számra definiáltuk az $\underline{n}$ halmazt, legyen $\underline{n+1} = \underline{n} \cup \{\underline{n}\}$. Ha az $\underline{n}$ halmaznak n eleme volt, akkor az $\underline{n+1}$-nek $n+1$ eleme lesz, ezért az $\underline{n}$ alakú halmazok mind különbözőek. Az axióma szerint $\underline{n} \in x$ minden természetes n-re, így x valóban végtelen.

A6 *helyettesítési axiómaséma*: az indukciós axiómasémához hasonlóan minden $\varphi(u, v) \in F(\langle\in\rangle)$ formulához tartozik egy axióma:

$$\begin{gathered}\left[\forall u\, \exists v\, \varphi(u, v) \wedge \forall u\, \forall v_0 \forall v_1\, (\varphi(u, v_0) \wedge \varphi(u, v_1) \rightarrow v_0 = v_1)\right] \rightarrow \\ \forall x\, \exists y\, \forall v\, (v \in y \leftrightarrow \exists u\, (u \in x \wedge \varphi(u, v))).\end{gathered}$$

A szögletes zárójelben álló premissza azt mondja ki, hogy minden u-hoz pontosan egy olyan v tartozik, amire $\varphi(u, v)$ igaz. Ezt a $\forall u\, \exists! v\, \varphi(u, v)$ jelöléssel szokás rövidíteni. A konklúzió szerint ekkor minden x halmazra, ha alkalmazzuk x elemeire a $\varphi(u, v)$ által definiált „függvényt," a képpontok is halmazt alkotnak. Bár az axiómát csak olyan formulákra mondtuk ki, melyek $F(\langle\in\rangle)$ elemei, az igaz marad a bevezetett jelekkel felírt formulákra is, hiszen azokat visszaírhatjuk a rövidítés nélküli alakjukba, majd arra alkalmazzuk a megfelelő helyettesítési axiómát.

A7 *regularitási axióma*: $\forall x\, (\exists y\, (y \in x) \rightarrow \exists y\, (y \in x \wedge \forall u\, (u \in x \rightarrow u \notin y)))$.
E szerint minden nem-üres halmaznak van az $\in$ relációra nézve minimális eleme, vagyis olyan $y \in x$, hogy x egyetlen u eleme sem áll $\in$ relációban y-nal. A regularitási axiómából következik többek között az is, hogy egyetlen halmaz sem lehet eleme önmagának.

Az A0 - A7 axiómák többé kevésbé világos intuitív tartalommal rendelkeznek (talán a regularitási axiómát kivéve, melynek felvétele nem szükségszerű, csak a tárgyalást egyszerűsíti le), igazságukat, mármint azt, hogy a „valódi halmazok" ténylegesen eleget tesznek ezeknek, az elmélet axiomatizálása óta a matematikusok legnagyobb része minden további nélkül elfogadja. Annál nagyobb volt a vita különösen a 30-as évek végén az ún. „kiválasztási" axióma körül. Az axiómát *E. Zermelo* fogalmazta meg először egy 1904-ben megjelent cikkében, s lényegében azt mondja ki, hogy egy halmaz minden nem-üres eleméből „egyszerre" ki tudunk venni egy-egy elemet. Ennek pontos megfogalmazásához először a rendezett pár fogalmát kell definiálnunk. Az $\langle x, y\rangle$ kétváltozós függvény az x, y halmazokhoz az $\{\{x\}, \{x, y\}\}$ halmazt rendeli, $\langle x, y\rangle$-t nevezzük az x és y-ból alkotott rendezett párnak. Nem nehéz belátni, hogy $\langle x, y\rangle = \langle u, v\rangle$ pontosan akkor, ha $x = u$ és $y = v$, így az elnevezés jogos. Ezek után lássuk az axiómát:

A8 *kiválasztási axióma*: $\forall x\, \exists y$ (y elemei rendezett párok és x minden eleme pontosan egy y-beli rendezett pár első eleme, továbbá x minden u elemére, ha $u \neq \emptyset$ és $\langle u, v\rangle \in y$, akkor $v \in u$).

Az axióma pontos felírása meglehetősen hosszadalmas, de nem okozna különösebb gondot. A8-at $\boldsymbol{C}$-vel szokás jelölni (a choice - választás szóból), az A0 - A8 axiómákat együtt pedig $\boldsymbol{ZFC}$-vel.

A kíválasztási axiómával szembeni kezdeti idegenkedés valószínűleg onnan ered, hogy más jellegű, mint a többi axióma. A „kiválasztási függvény," melynek létezését az axióma garantálja, nem „konstruktíven” áll elő az adott halmazból, mint a pár, unió vagy hatványhalmaz. Fizikai szóhasználattal élve A8 egy „szimmetriasértő” axióma: nélküle például a valós számok végtelen részhalmazai valamilyen értelemben szimmetrikus csoportokra bomlanak, amiket lehetetlen „szétszabdalni” egy kiválasztási függvénnyel. Az A8-cal szemben felhozott további érv az, hogy kellemetlen következményei vannak, sőt olyanok is, amik egyenesen ellentmondanak a józan észnek. Az egyik leghíresebb paradoxon *S. Banach*tól és *A. Tarski*tól származik 1924-ből. Legyen X és Y a közönséges háromdimenziós Euklideszi tér két részhalmaza. Azt mondjuk, hogy X és Y *egymásba darabolható*, ha X és Y külön-külön felbontható véges sok, mondjuk *m* diszjunkt halmaz uniójára:

$$X = X_0 \cup \ldots \cup X_{m-1}, \quad Y = Y_0 \cup \ldots \cup Y_{m-1}$$

úgy, hogy minden $i < m$-re X_i és Y_i térbeli mozgással egymásba vihető (tehát speciálisan egybevágó is).

4.6. Tétel *Legyen G a zárt egységgömb. G felbontható két diszjunkt X és Y részre úgy, hogy G és X valamint G és Y is átdarabolható egymásba.* ■

Ezek szerint egy gömböt szét tudunk vágni véges sok részre úgy, hogy a darabokból kettő, az eredetivel egybevágó gömb rakható össze! A paradoxon megjelenése után nem sokkal *Neumann János* bebizonyította, hogy síkban csak egyenlő területű alakzatokat lehet a fenti módon egymásba darabolni (feltéve persze, hogy az alakzatoknak van területe). Ám síkbeli „paradox” átdarabolást csak nemrégiben talált *Laczkovich Miklós*:

4.7. Tétel (Laczkovich Miklós tétele) *Síkban egyenlő területű kör és négyzet átdarabolható egymásba.* ■

A kiválasztási axiómával kapcsolatos viták, ha nem is zárultak le, mindenesetre nyugvópontra jutottak. Az axióma ekvivalenseivel együtt (Zorn lemma, Tukey–Teichmüller lemma, jólrendezési tétel stb.) bevonult a matematikusok mindennapi fegyvertárába. Ebben fontos szerepe volt annak, hogy tisztázódott a kiválasztási axiómának valamint számos gyengített változatának egymással és a többi axiómával való kapcsolata.