Komjáth Péter

# Matematikai logika

Budapest, 2000

# Előszó

> Egyszerre beszélek (tudom, tudom: csupán ,,beszélek") a természetet legyőzni akaró de legalábbis mindenestül megismerni szándékozó természettudományokról, a matematika elvi korlátaira rámutató Gödelről, a totális háborúról és Heisenberg bizonytalansági relációjáról, Auschwitzról, a lyukról a történelemben, mely a történelem szükségképpeni része, és a fénysebességről, melyről kiderült, kiderítettük, nem érhetjük el soha.
> Szegény Puskás.
> (Esterházy Péter: Puskás, Gödel, passz.)

E jegyzet célja az ELTE matematika tanárszakosainak segítséget adni ,,A matematika alapjai" című tárgy logika részének tanulásához. Ennek megfelelően bevezetést ad a matematikai logika gondolatvilágába, megvilágítja, hogyan lehet matematikai módszerekkel a matematikai bizonyítás, tétel és más fogalmakat vizsgálni. Kimondjuk és néhány esetben bizonyítjuk a legjelentősebb eredményeket, köztük (nagyon vázlatosan) Gödel nem-teljességi tételét.

Az olvasótól feltesszük a matematikai bizonyításokban való jártasságot, és ezenfelül a matematika különböző ágainak ismeretét, mivel az axiomatikus módszer példáiként szerepeltetjük az algebra ágait, a számelméletet, a halmazelméletet, stb.

A jegyzet az ,,Alapítvány a Magyar Felsőoktatásért és Kutatásért" alapítvány támogatásával készült.

# 1 Bevezetés

Hilbert a következőképpen fogalmazta meg a matematika axiomatizálásának programját: a matematika egy adott ágát úgy axiomatizáljuk, hogy a kapott rendszer legyen *kategórikus* (azaz csak egy modellje legyen), *ellentmondástalan* (ne lehessen belőle ellentmondást levezetni), és *teljes* (minden, az adott rendszeren belül megfogalmazható kérdés eldönthető legyen).

E jegyzet egyik célja annak bemutatása, hogyan lehet a matematika különböző ágai axiomatizálásának keretét (az elsőrendű nyelveket) megadni, a másik pedig a fenti program kitűzéseinek eredményéről beszámolni. Az utóbbi beszámoló nagyobbrészt negatív: a Löwenheim-Skolem-Tarski tétel szerint, ha egy axiómarendszernek van modellje, akkor van akármilyen nagy számosságú modellje is (néhány nyilvánvaló esettől eltekintve). A Gödel-féle nemteljességi tétel szerint, ha a számelméletet vagy a halmazelméletet (egy jólmeghatározott értelemben) „ésszerűen" axiomatizáljuk, akkor mindig adódnak eldönthetetlen problémák.

# 2 Kijelentéslogika, igazságfüggvények

Először azt vizsgáljuk, hogyan épülnek fel egyszerű matematikai állításokból bonyolultabbak a logikai összekötőjelek segítségével. Mivel itt nem érdekes, hogy melyek ezek az egyszerű állítások, csak azok igaz vagy hamis volta döntő, úgy tekintjük, hogy azok az „igaz" vagy „hamis" (jelben i, h) értéket felvevő úgynevezett *igazságváltozók* (szokásos elnevezés még: *Boole-változók*).

Ha $f$ az $\{\mathrm{i}, \mathrm{h}\}$ halmazon értelmezett, akárhányváltozós függvény, ami ugyanebbe a halmazba képez, akkor $f$-et *igazságfüggvény*nek nevezzük. Az igazságfüggvényeket az úgynevezett *igazságtáblázat*okkal adjuk meg: egy $n$-változós igazságfüggvény igazságtáblázata $n+1$ oszlopból és $2^n$ sorból áll. Az első $n$ oszlopban minden lehetséges módon sorravesszük az $n$ változó összes kombinációját és az utolsó oszlopban megadjuk a függvény értékét. Például, az $\wedge$ („és") függvény megadása:

| $x$ | $y$ | $\wedge$ |
|---|---|---|
| i | i | i |
| i | h | h |
| h | i | h |
| h | h | h |

Hasonlóan adható meg a $\vee$ („vagy") és a $\rightarrow$ („ha, akkor") függvény:

| $x$ | $y$ | $\vee$ | $\rightarrow$ |
|---|---|---|---|
| i | i | i | i |
| i | h | i | h |
| h | i | i | i |
| h | h | h | i |

További példák az $\leftrightarrow$ (ekvivalencia), $\oplus$ (mod 2 összeadás, antivalencia), $|$ (Sheffer művelet).

| $x$ | $y$ | $\leftrightarrow$ | $\oplus$ | $\mid$ |
|---|---|---|---|---|
| i | i | i | h | h |
| i | h | h | i | i |
| h | i | h | i | i |
| h | h | i | h | i |

Az igazságtáblázatok segítségével az igazságfüggvények közötti azonosságokat, például $A \rightarrow B = (\neg A) \vee B$-t, egyszerűen ellenőrizhetjük, mivel csak véges sok eset van.

Lássuk a műveleti azonosságokat!

$$\begin{aligned}
A \wedge B &= B \wedge A \\
A \vee B &= B \vee A \quad \text{(kommutativitás)} \\
A \wedge A &= A \\
A \vee A &= A \\
(A \wedge B) \wedge C &= A \wedge (B \wedge C) \\
(A \vee B) \vee C &= A \vee (B \vee C) \quad \text{(asszociativitás)} \\
(A \vee B) \wedge A &= A \\
(A \wedge B) \vee A &= A \quad \text{(elnyelés)} \\
A \wedge (B \vee C) &= (A \wedge B) \vee (A \wedge C) \\
A \vee (B \wedge C) &= (A \vee B) \wedge (A \vee C) \quad \text{(disztributivitás)}
\end{aligned}$$

Ilyenek még a jólismert de Morgan azonosságok.

$$\begin{aligned}
\neg(A \wedge B) &= \neg A \vee \neg B \\
\neg(A \vee B) &= \neg A \wedge \neg B
\end{aligned}$$

Vagy általánosabban:

$$\begin{aligned}
\neg(A_1 \wedge \cdots \wedge A_n) &= \neg A_1 \vee \cdots \vee \neg A_n \\
\neg(A_1 \vee \cdots \vee A_n) &= \neg A_1 \wedge \cdots \wedge \neg A_n
\end{aligned}$$

A tagadással kapcsolatos azonosságok még:

$$\begin{aligned} \neg\neg A &= A \\ A \wedge \neg A &= \mathrm{i} \\ A \vee \neg A &= \mathrm{h} \end{aligned}$$

Az $f(A_1, \ldots, A_n)$ igazságfüggvény *teljes diszjunktív normálformájá*nak nevezzük azt a felírását, amelyben bizonyos tagokat $\vee$-gyal kötünk össze a tagokon belül csak logikai „és" szerepelhet, és minden tagban minden változó pontosan egyszer szerepel: vagy eredeti formájában, vagy negálva.

Például:

$$A \to B = (\neg A \wedge B) \vee (\neg A \wedge \neg B) \vee (A \wedge B)$$

Vagy:

$$f(A_1, A_2, A_3) = (A_1 \wedge A_2 \wedge \neg A_3) \vee (\neg A_1 \wedge A_2 \wedge A_3) \vee (A_1 \wedge \neg A_2 \wedge \neg A_3)$$

**Tétel.** *Minden nem azonosan hamis igazságfüggvénynek van teljes diszjunktív normálformája.*

**Bizonyítás.** A bizonyítás kiindulópontja az az észrevétel, hogy az $A_1 \wedge \cdots \wedge A_n$ kifejezés a változók egyetlen értékeloszlása mellett igaz: ha $A_1 = \cdots = A_n = \mathrm{i}$. Ha egy olyan kifejezést veszünk, amiben az előzőhöz hasonlóan minden változó pontosan egyszer szerepel és $\wedge$-ekkel vannak összekötve, akkor ugyanez igaz, csak ezúttal az egyetlen i-t adó értékeloszlás az, amelyben a $\neg$-t kapó értékek h igazságértéket adnak (és csak azok).

Ezzel rögtön kapjuk a tételt arra az esetre, amikor a szóban forgó igazságfüggvény pontosan egyszer veszi fel az i értéket: az igazságtáblázatból vesszük a megfelelő sort, és annak alapján elkészítjük az (egytagú) teljes diszjunktív normálformát.

| i | i | h | h | i | h | $\Longrightarrow (A_1 \wedge A_2 \wedge \neg A_3 \wedge \neg A_4 \wedge A_5 \wedge \neg A_6)$ |
|---|---|---|---|---|---|---|

Ha a függvény többször veszi fel az i értéket, akkor az igazságtáblázat minden ilyen sorához elkészítjük a fenti módon a megfelelő kifejezést és ezeket $\vee$-gyal kötjük össze. Ez éppen a megfelelő eljárás, mert így olyan képletet kapunk, amely az előírt helyek mindegyikén az i, a többi helyen a h értéket veszi fel.

Például:

| $A_1$ | $A_2$ | $A_3$ | $f(A_1, A_2, A_3)$ | t.d.n.f. |
|---|---|---|---|---|
| i | i | i | h | |
| i | i | h | h | |
| i | h | i | i | $(A_1 \wedge \neg A_2 \wedge A_3)\vee$ |
| i | h | h | i | $(A_1 \wedge \neg A_2 \wedge \neg A_3)\vee$ |
| h | i | i | h | |
| h | i | h | i | $(\neg A_1 \wedge A_2 \wedge \neg A_3)$ |
| h | h | i | h | |
| h | h | h | h | |

□

Érdemes észrevenni, hogy az azonosan h függvénynek nem is lehet teljes diszjunktív normálformája, a fenti eljárással nem kapunk semmit. Pontosabban sehány tagot kapunk, és formálisan tekinthetjük a tagok nélküli kifejezést a megfelelő felírásnak (hasonlóan ahhoz, hogy az üres összeget 0-nak definiáljuk).

Analóg módon definiálhatjuk a teljes konjunktív normálforma fogalmát, amikor a tagokon belül $\vee$-okkal kötjük össze a változókat, a tagokat viszont $\wedge$-k kötik össze. Itt az azonosan igaz igazságfüggvény az, aminek nincs normálformája.

**Feladat.** Írjuk fel $A \vee B$-t az implikáció és a tagadás segítségével !

# 3 Teljes rendszerek

Igazságfüggvények egy halmazát *teljes rendszer*nek nevezzük, ha elemeiből kompozícióval minden igazságfüggvény előáll.

A teljes diszjunktív normálforma létezésének következménye, hogy $\{\wedge, \vee, \neg\}$ teljes. A de Morgan azonosság segítségével a $\vee$ minden előfordulását kiküszöbölhetjük: $\alpha \vee \beta = \neg(\neg\alpha \wedge \neg\beta)$, ezért $\{\wedge, \neg\}$ is teljes rendszer. Hasonlóképpen adódik, hogy $\{\vee, \neg\}$ teljes rendszer. $\{\wedge, \vee\}$ viszont nem teljes rendszer. Például, $\neg$ olyan igazságfüggvény, amely nem kompozíciója ezeknek. Ezt úgy lehet belátni, hogy megadunk egy olyan tulajdonságot, amely teljesül $\wedge$-re és $\vee$-ra, öröklődik a kompozícióra és a $\neg$ nem rendelkezik vele. Ilyen tulajdonság például az, hogy i-t i-be viszi. Tehát tulajdonképpen azt csináltuk, hogy definiáltuk igazságfüggvények $\mathcal{K}_\mathrm{i}$ osztályát, azokét, amelyek i-t i-be viszik, és beláttuk, hogy az osztály kompozícióra zárt, de nem tartalmaz minden igazságfüggvényt.

Összesen öt ilyen speciális részosztályt definiálunk:

$$
\begin{aligned}
\mathcal{K}_\mathrm{i} &= \{f : f(\mathrm{i},\ldots,\mathrm{i}) = \mathrm{i}\} \\
\mathcal{K}_\mathrm{h} &= \{f : f(\mathrm{h},\ldots,\mathrm{h}) = \mathrm{h}\} \\
\mathcal{U} &= \{f : f(\neg A_1,\ldots,\neg A_n) = \neg f(A_1,\ldots,A_n)\} \quad \text{(önduális függvények)} \\
\mathcal{L} &= \{f : f(x_1,\ldots,x_n) = c_0 \oplus c_1 x_1 \oplus \cdots \oplus c_n x_n\} \quad \text{(lineáris függvények)} \\
\mathcal{M} &= \{f : f \text{ monoton}\}
\end{aligned}
$$

ahol az utolsó két esetben elvégezzük a $h = 0$, $i = 1$ azonosítást és $\oplus$ a modulo 2 összeadás. A szorzást is mod 2 értelmezzük, de észrevehető, hogy ez azonos az $\wedge$-sel.

Könnyen meggondolható, hogy ezek az osztályok valóban zártak a kompozícióra, továbbá $\neg \notin \mathcal{K}_i$, $\neg \notin \mathcal{K}_h$, $\wedge \notin \mathcal{U}$, $\wedge \notin \mathcal{L}$ és $\neg \notin \mathcal{M}$. A következő, némileg meglepő tétel azt mondja ki, hogy ezek a maximális fenti típusú osztályok.

**Post-Jablonszkij-tétel.** *Igazságfüggvényeknek egy $\mathcal{F}$ rendszere teljes és csak akkor teljes, ha nem részrendszere $\mathcal{K}_i$, $\mathcal{K}_h$, $\mathcal{U}$, $\mathcal{L}$, $\mathcal{M}$ közül egyiknek sem.* □

A tétel egyik iránya könnyen adódik abból, hogy e rendszerek mind zártak a kompozícióra és valódi részrendszerei az összes igazságfüggvények halmazának. A másik irány jóval nehezebb és nem is bizonyítjuk.

**Következmény.** *Ha az $\mathcal{F}$ rendszer teljes, akkor van legfeljebb ötelemű teljes részrendszere.*

**Bizonyítás.** Mivel $\mathcal{F}$ teljes, a Post-Jablonszkij-tétel könnyű irányát használva ki tudjuk választani az

$$f_1 \in \mathcal{F} - \mathcal{K}_i, f_2 \in \mathcal{F} - \mathcal{K}_h, f_3 \in \mathcal{F} - \mathcal{U}, f_4 \in \mathcal{F} - \mathcal{L}, f_5 \in \mathcal{F} - \mathcal{M}$$

elemeket. De ekkor a Post-Jablonszkij-tétel másik irányát alkalmazva adódik, hogy az $\mathcal{F}' = \{f_1, f_2, f_3, f_4, f_5\} \subseteq \mathcal{F}$ rendszer nem teljes. □

Megjegyezzük, hogy az utóbbi következmény állítása valójában 4-gyel is teljesül. A bizonyítás azonban másképp halad; nem a Post-Jablonszkij-tételt használja.

**Feladat. 1.** Lássuk be, hogy $\{\rightarrow, \neg\}$ teljes rendszer !

**2.** Lássuk be, hogy $\{|\}$ teljes rendszer !

# 4 Következtetések

Ha $\alpha$, $\beta$, $\gamma$ (összetett) állítások, akkor vannak bizonyos kézenfekvő következtetések az ezekből felépített állítások között.

Például, ha van két állításunk, az egyik szerkezete $\alpha \rightarrow \beta$ a másiké $\beta \rightarrow \gamma$ alakú, akkor szabad az $\alpha \rightarrow \gamma$ állításra következtetnünk. Ezt régebben így jelölték:

$$\frac{\alpha \rightarrow \beta, \beta \rightarrow \gamma}{\alpha \rightarrow \gamma}$$

mai jelölése (feltehetőleg nyomdatechnikai okokból) ez:

$$\alpha \rightarrow \beta, \beta \rightarrow \gamma \models \alpha \rightarrow \gamma.$$

Tehát a $\models$ jel baloldalán a feltevéseket (premisszákat), jobboldalán a következményt (konklúzió) adjuk meg.

Következtetési szabályok:

1. $\alpha,\ \alpha \to \beta \models \beta$ (modus ponens, MP, levágás),
2. $\neg\alpha \to \neg\beta,\ \beta \models \alpha$ (indirekt),
3. $\alpha \to \beta \models \neg\beta \to \neg\alpha$ (kontrapozíció),
4. $\alpha \to \beta,\ \beta \to \gamma \models \alpha \to \gamma$ (hipotetikus szillogizmus),
5. $\neg\alpha \to \beta,\ \neg\alpha \to \neg\beta \models \alpha$ (reductio ad absurdum).

Logikai axiómák:

1. $\alpha \to (\beta \to \alpha)$
2. $\big(\alpha \to (\beta \to \gamma)\big) \longrightarrow \big((\alpha \to \beta) \to (\alpha \to \gamma)\big)$
3. $\big(\neg\beta \to \neg\alpha\big) \longrightarrow \big((\neg\beta \to \alpha) \to \beta\big)$

A logikai axómákat az $\alpha$, $\beta$, $\gamma$ igazságfüggvények minden választásával felírjuk, tehát valójában három végtelen csoportról van szó.

Ha $\Gamma$ kijelentések halmaza, $\psi$ kijelentés, akkor $\psi$ *levezethető* $\Gamma$-ból, jelben $\Gamma \vdash \psi$, ha van olyan $\varphi_1, \varphi_2, \ldots, \varphi_n = \psi$ sorozat (a levezetés), hogy minden $\varphi_i$ kijelentés, mégpedig: vagy $\Gamma$-beli, vagy logikai axióma, vagy két korábbi $\varphi_i$-ből a levágás segítségével keletkezett. Ha $\Gamma = \emptyset$, azaz valamit kizárólag a logikai axiómák segítségével vezetünk le, akkor $\emptyset \vdash \psi$ helyett $\vdash \psi$-t írunk.

Tehát ahelyett, hogy a fenti következtetési szabályok mindegyikét megengednénk, csak a levágást engedjük meg, cserébe bevezetjük a logikai axiómák csoportjait. Hogy ez elég, az ötödik következtetési szabálynál nyilvánvaló (csak a harmadik logikai axiómát kell használni). Belátjuk ezt a második következtetési szabályra is.

**1. Állítás.** $\neg\alpha \to \neg\beta, \beta \vdash \alpha$.

**Bizonyítás.** Az alábbiakban megadjuk a levezetést.

1. $\beta$ (feltevés)
2. $\beta \to (\neg\alpha \to \beta)$ (1. logikai axióma)
3. $\neg\alpha \to \beta$ (levágással 1,2-ből)
4. $\neg\alpha \to \neg\beta$ (feltevés)
5. $\big(\neg\alpha \to \neg\beta\big) \to \big((\neg\alpha \to \beta) \to \alpha\big)$ (1. log. ax.)
6. $(\neg\alpha \to \beta) \to \alpha$ (MP 4,5-ből)
7. $\alpha$ (MP 4,6-ból)

□

**2. Állítás.** $\vdash \varphi \to \varphi$ *minden* $\varphi$*-re.*

**Bizonyítás.** Megadjuk a levezetést.

1. $\varphi \longrightarrow \big((\varphi \to \varphi) \to \varphi\big)$ (1. logikai axióma)
2. $(\varphi \to ((\varphi \to \varphi) \to \varphi)) \longrightarrow ((\varphi \to (\varphi \to \varphi)) \longrightarrow (\varphi \to \varphi))$ (2. log. ax.)
3. $\big(\varphi \to (\varphi \to \varphi)\big) \longrightarrow (\varphi \to \varphi)$ (levágás)
4. $\varphi \to (\varphi \to \varphi)$ (1. logikai axióma)
5. $\varphi \to \varphi$ (levágás)

□

**3. Állítás.** *Ha* $\Gamma \vdash \varphi, \neg\varphi$ *akkor* $\Gamma \vdash \psi$ *minden* $\psi$*-re.*

**Bizonyítás.** Elég persze $\{\varphi, \neg\varphi\} \vdash \psi$-t igazolni. Megadjuk a levezetést.

1. $\neg\varphi$ (mert eleme $\Gamma$-nak)
2. $\neg\varphi \to (\neg\psi \to \neg\varphi)$ (1. logikai axióma)
3. $\neg\psi \to \neg\varphi$ (modus ponens 1,2-ből)
4. $\varphi$ (mert eleme $\Gamma$-nak)
5. $\varphi \to (\neg\psi \to \varphi)$ (1. logikai axióma)
6. $\neg\psi \to \varphi$ (modus ponens 4,5-ből)
7. $\big(\neg\psi \to \neg\varphi\big) \longrightarrow \big((\neg\psi \to \varphi) \to \psi\big)$ (3. logikai axióma)
8. $\big((\neg\psi \to \varphi) \to \psi\big)$ (levágás 3,5-ből)
9. $\psi$ (levágás 6,8-ból)

□

Az Állítás meglepő, látszólag paradoxongyanús dolgot állít: ha egy rendszerben van egyetlen egy ellentmondás, akkor mindent (és így minden ellentettjét is) be lehet bizonyítani, tehát egy ponton való megkettőzés ($\varphi$ és $\neg\varphi$) mindenütt való megkettőzésre vezet. De itt nincs semmi, ami ellentmondana szokásos matematikai okoskodásainknak: ha $\Gamma$-ból $\varphi$-t is, $\neg\varphi$-t is le tudnánk vezetni, akkor $\psi$ levezetéséhez indirekt módon járunk el; feltesszük $\neg\psi$-t, eseteket különböztetünk meg. Ha (első eset) $\varphi$ igaz, akkor levezetjük $\neg\varphi$-t, kész az ellentmondás, az első esetben készen vagyunk. A második esetben, ha $\neg\varphi$ igaz, ugyanígy vezetjük ellentmondásra a feltevéseket.

**4. Állítás.** $\neg\neg\varphi \vdash \varphi$.

**Bizonyítás.** Megadjuk a levezetést.

1. $\neg\neg\varphi$ (mert eleme $\Gamma$-nak)
2. $\neg\neg\varphi \to (\neg\varphi \to \neg\neg\varphi)$ (1. logikai axióma)
3. $\neg\varphi \to \neg\neg\varphi$ (modus ponens 1,2-ből)
4. $\big(\neg\varphi \to \neg\neg\varphi\big) \longrightarrow \big((\neg\varphi \to \neg\varphi) \to \varphi\big)$ (3. logikai axióma)
5. $(\neg\varphi \to \neg\varphi) \to \varphi$ (modus ponens 3,4-ből)
6. $\neg\varphi \to \neg\varphi$ (ennek levezetését láttuk)
7. $\varphi$ (modus ponens 5,6-ból)

□

**A dedukció tétel.** (Herbrand, 1930) *Ha* $\Gamma \cup \{\varphi\} \vdash \psi$, *akkor* $\Gamma \vdash \varphi \to \psi$.

**Bizonyítás.** Legyen $\varphi_1, \ldots, \varphi_n = \psi$ levezetés $\Gamma \cup \{\varphi\}$-ből. $1 \leq i \leq n$-re indukcióval bebizonyítjuk, hogy $\Gamma \vdash \varphi \to \varphi_i$. Ez $i = n$-re éppen a bizonyítandó állítást adja. Négy eset lehetséges, aszerint, hogy $\varphi_i$ hogyan keletkezik.

Ha $\varphi_i \in \Gamma$, akkor, mivel $\varphi_i \to (\varphi \to \varphi_i)$ logikai axióma, $\varphi \to \varphi_i$-t le tudjuk vezetni $\Gamma$-ból. Hasonló az okoskodás, ha $\varphi_i$ logikai axióma. Ha $\varphi_i = \varphi$, $\vdash \varphi \to \varphi$-t már láttuk.

Tegyük fel végül, hogy $\varphi_i$ modus ponensszel keletkezik két korábbi kijelentésből, $\varphi_j$-ből és $\varphi_k$-ból. Tehát $j, k < i$ és (mondjuk) $\varphi_k = \varphi_j \to \varphi_i$. Indukciós feltevésünk szerint már tudjuk, hogy $\Gamma \vdash \varphi \to \varphi_j, \varphi \to (\varphi_j \to \varphi_i)$. Mivel a 2. logikai axióma egyik esete

$$\big(\varphi \to (\varphi_j \to \varphi_i)\big) \longrightarrow \big((\varphi \to \varphi_j) \to (\varphi \to \varphi_i)\big)$$

levágásokkal $\varphi \to \varphi_i$-t le tudjuk vezetni. □

Jegyezzük meg, hogy a dedukció tétel megfordítása nyilvánvaló.

Bár a dedukció tétel mesterkéltnek tűnhet, igen hasznos alkalmazásai vannak.

**Állítás.** $\alpha \to \beta, \beta \to \gamma \vdash \alpha \to \gamma$.

**Bizonyítás.** A levágási szabály alkalmazásával $\{\alpha, \alpha \to \beta, \beta \to \gamma\} \vdash \gamma$. Innen a dedukció tétellel adódik az állítás. □

**Állítás.** $\varphi \vdash \neg\neg\varphi$.

**Bizonyítás.** Az előzőekben láttuk $\neg\neg\neg\varphi \vdash \neg\varphi$-t. A dedukció tétel miatt ebből $\vdash \neg\neg\neg\varphi \to \neg\varphi$ következik. A 3. logikai axióma egyik esete

$$\big(\neg\neg\neg\varphi \to \neg\varphi\big) \to \big((\neg\neg\neg\varphi \to \varphi) \to \neg\neg\varphi\big).$$

Ennek az előtagját levezettük, s mivel $\varphi \to (\neg\neg\neg\varphi \to \varphi)$ az 1. logikai axióma egyik esete, végső soron $\varphi$-ből $\neg\neg\varphi$-t le tudjuk vezetni. □

# 5 Elsőrendű nyelvek

Az elsőrendű nyelvek fogalmának nagy újítása a kijelentéslogika fölött a *kvantorok* bevezetése. A $\forall$, „minden" és a $\exists$, „létezik" jelek segítségével már ilyen állításokat is felírhatunk:

$$\forall x \forall y [xy = yx]$$

azaz a csoportkommutativitást. A kvantorok tehát nem állhatnak magukban, mindig változónak kell követnie, a kiolvasás pedig $\forall x$ esetén „$x$ minden értékére (igaz, hogy ...)", $\exists x$ esetén „van $x$-nek olyan értéke (amire igaz, hogy ...)". Tehát az, hogy a csoportban van egységelem, így fogalmazható meg:

$$\exists x \forall y [xy = yx = y].$$

A különböző kvantorok sorrendje nem cserélhető fel: az előző képlettől lényegesen különbözőt mond ki $\forall y \exists x [xy = yx = y]$. Az azonos kvantorok viszont felcserélhetők: $\forall x \forall y [xy = yx]$ és $\forall y \forall x [xy = yx]$ egyaránt a csoport kommutativitását mondja ki.

**Definíció.** *Elsőrendű nyelv*nek nevezünk egy $L$ halmazt, ha a következő részekből áll:

- Változójelek egy végtelen halmaza: $v_0, v_1, \ldots$.
- Konstansjelek véges vagy megszámlálhatóan végtelen halmaza: $c_0, c_1, \ldots$.
- Függvényjelek véges vagy megszámlálhatóan végtelen halmaza: $f_0, f_1, \ldots$.
- Relációjelek véges vagy megszámlálhatóan végtelen halmaza: $R_0, R_1, \ldots$.
- Logikai jelek: $\neg, \wedge, \vee, \rightarrow$
- Kvantorok: $\exists, \forall$
- Segédjelek:(,),, (tehát a zárójelek és a vessző).

Feltesszük, hogy minden függvényjelhez és minden relációjelhez hozzá van rendelve egy pozitív egész szám, a változóinak száma. Kikötjük, hogy van legalább egy relációjel és az első relációjel, $R_0$, mindenképpen kétváltozós. (Ennek az az oka, hogy ez fogja az egyenlőség szerepét játszani, ez teszi lehetővé, hogy a formulákban egyenlőségjeleket írjunk.) Mivel a logikai jelek a már látott módon redukálhatók például a $\neg$-ra és a $\vee$-ra, vagy a $\neg$-ra és az $\rightarrow$-ra, tulajdonképpen felírhattuk volna úgy is a definíciót, hogy csak ez a kettő (vagy az a kettő) szerepel, és valóban ilyen a legtöbb szakkönyvben szereplő definíció.

Annak, hogy rögtön végtelen sok változójelet vezetünk be (és ezzel, meglehetősen kényelmetlenül, a nyelv végtelenné válik), az az oka, hogy nem tudhatjuk előre, hány változóra lesz szükség egy bizonyítás leírásához. Mivel a nyelv

menetközbeni kiegészítésére nincs mód, be kell vezetnünk végtelen sok változójelet. A továbbiakban, az elvileg helyes, de meglehetősen kényelmetlen $v_0, v_1, \ldots$ jelek helyett a szokásos $x$, $y$, stb. használjuk.

A kvantorok használata: ha $\varphi(x)$ egy $x$-re vonatkozó állítás, $\exists x\varphi(x)$ jelentése: „létezik $x$, amelyre $\varphi(x)$", $\forall x\varphi(x)$ jelentése: „minden $x$-re $\varphi(x)$". A logikai jelekhez hasonlóan, az egyik kvantort visszavezethetjük a másikra: $\forall x\varphi(x)$ egyenértékű azzal, hogy $\neg\exists x\neg\varphi(x)$, ennek megfelelően, a formális definíciókba csak az egyik kvantort veszik be.

Egy hasonló képlet lehetővé teszi, hogy használjuk a megszokott $\exists!$ jelet:

$$\exists x!\varphi(x) \iff \exists x\varphi(x) \wedge \forall x\forall y\big[\big(\varphi(x) \wedge \varphi(y)\big) \to (x = y)\big].$$

A függvényszimbólumok valójában a műveleti jelek, mindössze szokásból hívjuk függvényjeleknek.

Megemlítem, hogy a bevezetett szabályoktól sokszor eltérünk: az egyenlőség relációt a szabályos $=(x, y)$ helyett $x = y$-nal, az összeadást, szorzást szintén szabálytalanul $x + y$, $xy$-nal jelöljük. (A helyes jelölés $+(x, y)$, $\cdot(x, y)$ lenne.)

**Definíció.** *Kifejezés*nek nevezük az alábbiakat:

1. Minden változójel kifejezés.
2. Minden konstansjel kifejezés.
3. Ha $t_1, \ldots, t_n$ kifejezés, $f_i$ pedig $n$-változós függvényjel, akkor $f_i(t_1, \ldots, t_n)$ is kifejezés.
4. Más kifejezés nincs, csak amit a fenti eljárások tetszőleges sok alkalmazásával megkaphatunk.

Hasonlóképpen rekurzív a *formulák* definíciója.

**Definíció.** *Formulák*nak nevezük az alábbiakat:

1. (Prímformulák.) Ha $t_1, \ldots, t_n$ kifejezés, $R_i$ pedig $n$-változós relációjel, akkor $R_i(t_1, \ldots, t_n)$ formula.
2. Ha $\varphi$ és $\psi$ formula, akkor $\varphi \vee \psi$ is az.
3. Ha $\varphi$ formula, akkor $\neg\varphi$ is az.
4. Ha $\varphi$ formula, $v_i$ változójel, akkor $\exists v_i\varphi$ is formula.
5. Más formula nincs, csak amit a fenti eljárások tetszőleges sok alkalmazásával megkaphatunk.

**Példák: 1. Csoportelmélet.** A csoportelmélet nyelve egyetlen műveleti jelből áll (a kötelezően megadott jeleken kívül) a szorzás $\cdot$ jeléből. Az egységelem létezése a következőképpen írható fel:

$$\exists x \forall y (xy = yx = y).$$

Gondot okoz az inverz létezésének megfogalmazása, ugyanis azt általában úgy csináljuk, hogy „jelöljük az egységelemet 1-gyel, és ekkor ...” stb. Ezt azonban nem tehetjük, nem lehet a nyelvbe új jeleket bevezetni. Ehelyett „beírjuk” 1 definícióját:

$$\exists x \big[ \big( \forall y (xy = yx = y) \big) \wedge \big( \forall y \exists z (yz = zy = x) \big) \big].$$

Megjegyzem, kicsit csaltam, a csoportelmélet elsőrendű nyelve általában az 1 konstansjelét, az inverz egyváltozós, és a szorzás kétváltozós műveletét tartalmazza. Szabályosan $xy = yx = y$-t sem írhatunk, a helyes $(xy = yx) \wedge (yx = y)$ lett volna.

**2. Gyűrűelmélet.** A gyűrűelmélet nyelve egy konstansjelből: 0, és két kétváltozós függvényjelből: $+$, $\cdot$ áll. Itt azt érdemes megjegyezni, hogy a kifejezések tulajdonképpen a (többváltozós) polinomok.

**3. Rendezett halmazok elmélete.** Ez egyetlen kétváltozós relációjelből áll (a kötelezőt leszámítva) a rendezés $<$ jeléből. Az axiómák a szokásosak:
$\forall x \neg (x < x)$;
$\forall x \forall y \forall z \big( (x < y \wedge y < z) \to (x < z) \big)$;
$\forall x \forall y \big( (x < y) \vee (x = y) \vee (y < x) \big)$.
Az ezeknek az axiómáknak megfelelő struktúrák éppen a rendezett halmazok.

**4. Halmazelmélet.** A halmazelmélet nyelve egyetlen kétváltozós relációjelből áll: az „elemének lenni” $\in$ jeléből. A fentihez hasonló módon oldható meg a szokásos jelölések kiküszöbölése: $\emptyset \in x$ helyett azt írjuk, hogy

$$\exists y \big( \forall z (z \notin y) \wedge y \in x \big);$$

ahelyett, hogy $x = P(y)$ ($x$ az $y$ hatványhalmaza) azt írjuk, hogy

$$\forall z \big[ z \in x \longleftrightarrow \big( \forall u (u \in z \to u \in y) \big) \big];$$

ahelyett, hogy $\{P(x), P(y)\} \in z$, azt írjuk, hogy

$$\exists u \exists v \exists w \Bigg( \underbrace{\big[ \forall x \big( (x \in w) \leftrightarrow (x = u \vee x = v) \big) \big]}_{w = \{u,v\}} \wedge \big( u = P(x) \big) \wedge \big( v = P(y) \big) \wedge \big( w \in z \big) \Bigg)$$

itt persze be kell írni a fenti részformulákat $u = P(x)$-re és $v = P(y)$-ra.

# 6 A Peano-axiómák

Ebben a részben bemutatjuk a számelmélet axiomatizálásához használt Peano-féle nyelvet. Ez (a kötelező, minden nyelvben közös jeleken kívül) egy 0 konstansjelből áll, ezenkívül három műveleti jel van benne: a rákövetkezés egyváltozós $S$, az összeadás kétváltozós $+$ és a szorzás kétváltozós $\cdot$ jele. (A rákövetkezést $S(x)$ helyett szokásos még $x'$-vel is jelölni.)

**N1** $\forall x\big(S(x) \neq 0\big)$

**N2** $\forall x \forall y\big([S(x) = S(y)] \to [x = y]\big)$

**N2,5** $\forall x\big([x \neq 0] \to \exists y(S(y) = x)\big)$

**N3**$_\varphi$ $\varphi_x[0] \wedge \forall y\big[\varphi_x[y] \to \varphi_x[S(y)]\big] \longrightarrow \forall x \varphi(x)$

**N4** $\forall x(x + 0 = x)$

**N5** $\forall x \forall y\big(x + S(y) = S(x + y)\big)$

**N6** $\forall x(x0 = 0)$

**N7** $\forall x \forall y\big(xS(y) = xy + x\big)$

A továbbiakban az $S(0)$ kifejezést $\overline{1}$-sal, $S\big(S(0)\big)$-t $\overline{2}$-sal, stb jelöljük. Hangsúlyozom, hogy ezek „nemlétező" jelek, mivel a nyelv megadásakor lerögzítettük, milyen jelek szerepelhetnek, azokhoz már nem tehetünk újabbakat. Ezek házi használatú rövidítések, valahogy úgy, ahogy a $\forall x$ jeleket is használjuk egy hosszabb jelsorozat rövidítésére.

Mielőtt pontosan megadnánk a levezetés elsőrendű nyelvekre vonatkozó definícióját, megadunk néhány Peano-axiómarendszerbeli „levezetést".

**1. Állítás.** $\overline{2} + \overline{2} = \overline{4}$.

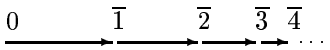
**Bizonyítás.** N4-et és N5-öt alkalmazva kapjuk, hogy $\overline{2} + 0 = \overline{2}$, $\overline{2} + \overline{1} = \overline{3}$, $\overline{2} + \overline{2} = \overline{4}$. □

Az N3 axióma valójában axiómák végtelen serege. Minden $\varphi$ formulára felírtuk a teljes indukció axiómáját: **ha** $\varphi$ igaz nullára, abból, hogy $y$-ra igaz, következik, hogy $S(y)$-ra is, **akkor** $\varphi$ minden $y$-ra igaz. Itt $\varphi_x[0]$, $\varphi_x[y]$, $\varphi_x[S(y)]$ azt jelenti, hogy a $\varphi$ formulában az $x$ változó helyébe rendre a 0, $y$, $S(y)$ kifejezéseket helyettesítettük. Azért kellett minden formulára kiírni az axiómát, mert nem tudunk $\forall$ kvantort alkalmazni a formulákra.

A N2,5 axióma neve azért ilyen különös, mert levezethető a többi axiómából, de a teljes indukció segítségével (ezért valójában elhagyható). Ha ugyanis $\varphi(x)$-nek a

$$(x = 0) \vee \exists y\big(x = S(y)\big)$$

formulát vesszük, akkor igaz $\varphi(0)$ (az első tag) és minden $x$-re $\varphi\big(S(x)\big)$ (a második tag), tehát $\mathrm{N3}_\varphi$ szerint minden $x$-re $\varphi(x)$ teljesül, és ezt akartuk.




Az N1, N2 és az N2,5 axióma együttesen azt mondja ki, hogy 0-n kívül minden elem rákövetkezője valaminek, de csak egyvalaminek. Tehát 0-ból kiindul egy végtelen „fonál". Azt nem válaszolják meg az axiómák, vannak-e ezeken kívül elemek, de az igaz, hogy az N1, N2, N2,5 axiómarendszer modelljei úgy néznek ki, hogy van egy, 0-ból kiinduló, egyirányban végtelen „fonál", valahány (esetleg sehány) irányított kör, és valahány (esetleg sehány) mindkét irányban végtelen „fonál".

**2. Állítás.** $\forall x(0 + x = x)$.

**Bizonyítás.** Jelölje $\varphi(x)$ a $0 + x = x$ állítást. Az indukció axiómáját felhasználva elég lenne belátni $\varphi(0)$-t és $\forall y\big[\varphi(y) \to \varphi\big(S(y)\big)\big]$-t. $\varphi(0)$-t azaz $0 + 0 = 0$-t N4-ből tudjuk. Ha $0 + x = x$, akkor N5 szerint $0 + S(x) = S(x)$, így az indukciós lépést is láttuk. □

**3. Állítás.** $\forall x[x\overline{1} = x]$.

**Bizonyítás.** $x\overline{1} = xS(0) = x0 + x = 0 + x = x$. □

**4. Állítás.** $\forall x \forall y(x + y = y + x)$.

**Bizonyítás.** Ezt megpróbáljuk, az előzőhöz hasonlóan $x$-re indukcióval belátni. Az $x = 0$ eset, tehát $\forall y(0+y = y+0)$ N4-ből és a 2. Állításból adódik. Gondoljuk át, mi az indukciós lépés. Igazolnunk kell, hogy ha $\forall y(x + y = y + x)$ akkor $\forall y\big(S(x) + y = y + S(x)\big)$. Ez utóbbit $y$-ra való indukcióval célszerű igazolni. Az $y = 0$ eset, $S(x) + 0 = 0 + S(x)$ igaz (N4 és az előző állítás miatt). Le kell tehát vezetnünk $S(x) + y = y + S(x)$-ből $S(x) + S(y) = S(y) + S(x)$-t. Mivel tudjuk $x + y = y + x$-et, végezzük a következő átalakításokat:

$$\begin{aligned} S(S(x + y)) &= S(x + S(y)) \quad \text{(N5 miatt)} \\ &= S(S(y) + x) \quad \text{(mert } x\text{-re tudjuk az állítást)} \\ &= S(y) + S(x) \quad \text{(N5 miatt)} \end{aligned}$$

Hasonlóan

$$\begin{aligned} S\big(S(y + x)\big) &= S\big(y + S(x)\big) \quad \text{(N5 miatt)} \\ &= S\big(S(x) + y\big) \quad \text{(mivel feltettük)} \\ &= S(x) + S(y) \quad \text{(N5 miatt)} \end{aligned}$$

□

Hasonló módon igazolhatóak a szokásos egyéb műveleti azonosságok:

$$\forall x \forall y \forall z \big((x+y)+z = x+(y+z)\big),$$
$$\forall x (0x = 0),$$
$$\forall x \forall y (xy = yx),$$
$$\forall x \forall y \forall z \big((xy)z = x(yz)\big),$$
$$\forall x \forall y \forall z \big((x+y)z = xz+yz\big).$$

Trükkösebb az $x < y$ reláció definiálása. Jelöljük ezzel azt, hogy $\exists z\big(S(x) + x = y\big)$. Ekkor már annak a levezetéséhez, hogy $x < x$ sohasem teljesül, fel kell használnunk a teljes indukció axiómáját. Levezethetjük a rendezés szokásos többi tulajdonságát is. Ezután megfogalmazhatjuk és levezethetjük a maradékos osztás tételét:

$$\forall x \forall y \big[(y \neq 0) \longrightarrow \exists! q \exists! r \big((x = yq + r) \wedge (r < y)\big)\big].$$

Tovább is mehetünk, és formulával felírhatjuk, hogy valami prímszám, vagy például hogy minden 0-nál nagyobb szám és kétszerese között van prímszám.

Az axiómákról könnyen láthatjuk, hogy a természetes számok „igazi" struktúrája kielégíti azokat, messze nem világos azonban (és nem is igaz) hogy más megfelelő struktúra nincs.

A teljes indukció axiómasémájához hasonló a halmazelmélet axiómarendszerében a részhalmazaxióma és a pótlás axiómájának megfogalmazása. A részhalmazaxióma formája:

$$\forall x \exists y \big(\forall z (z \in y) \longleftrightarrow \big(z \in x \wedge \varphi(z, u_1, \ldots, u_n)\big)\big)$$

ahol $u_1, \ldots, u_n$ paraméterek és $\varphi(z, u_1, \ldots, u_n)$ $(n+1)$-változós formula.

**Feladatok. 1.** Vezessük le a Peano-axiómákból, hogy $n = 1, 2, 3, \ldots$-ra nincs olyan $x$ elem, amire $S^n(x) = x$ (tehát nincs „kör").

**2.** Bizonyítsuk be, hogy minden $x$-re $x + \overline{1} = S(x)$.

**3.** Írjuk fel a Peano-axiómák nyelvén azt, hogy $x$ és $y$ relatív prímek !

**4.** Lássuk be, hogy a Peano-axiómáknak megfelelő struktúra, ha nem azonos (helyesebben nem izomorf) a természetes számok szokásos struktúrájával, akkor nem is lehet jólrendezett!

# 7 Az elsőrendű logika

Ebben a részben felépítjük az elsőrendű nyelvek használatához szükséges fogalmakat.

Definiáljuk kifejezések és formulák *szabad változó*it. Ha $t$ kifejezés, szabad változóinak $V(t)$ halmazát $t$ felépítése szerinti indukcióval adjuk meg. Először is, $V(v_i) = \{v_i\}$ minden $v_i$ változójelre és $V(c_i) = \emptyset$ minden $c_i$ konstansjelre. Ha pedig $t = f_i(t_1, \ldots, t_n)$, ahol $f_i$ $n$-változós függvényjel, $t_1, \ldots, t_n$ pedig (már meglevő) kifejezések, akkor legyen $V(t) = V(t_1) \cup \cdots \cup V(t_n)$. Így tehát $V(t)$ a $t$-ben szereplő szabad változók halmaza.

Ha $\varphi$ az $R_i(t_1, \ldots, t_n)$ prímformula, akkor legyen $V(\varphi) = V(t_1) \cup \cdots \cup V(t_n)$. Ha a $\varphi$ formulára $V(\varphi)$ már definiálva lett, akkor legyen $V(\neg\varphi) = V(\varphi)$. Ha a $\varphi$, $\psi$ formulákra a szabad változók halmaza definiálva lett, akkor legyen $V(\varphi \vee \psi) = V(\varphi) \cup V(\psi)$. Végül pedig legyen $V(\exists v_i \varphi) = V(\varphi) - \{v_i\}$. Ha egy $\varphi$ formulára $V(\varphi) = \emptyset$ teljesül, akkor $\varphi$ *zárt formula*, vagy *mondat*. Zárt formula például $\forall v_0 \forall v_1 [v_0 v_1 = v_1 v_0]$, vagy $0 + 0 = 0$.

Tehát a kvantorok csökkentik a szabad változók halmazát. Az azonban nem igaz, hogy ha egy változó kvantorral le van kötve, akkor nem szabad változó, ugyanis szerepelhet a formula másik részén: $\big(\exists v_1 [v_0 = v_1]\big) \wedge [v_1 = v_1]$ -ben $v_1$ szabad és kötött változó egyszerre. Azt lehet mondani, hogy az első előfordulása „véletlen", ha más változóra cseréljük, azonos értelmű formulát kapunk: $\big(\exists v_4 [v_0 = v_4]\big) \wedge [v_1 = v_1]$.

Következő fogalmunk az adott elsőrendű nyelvnek megfelelő *struktúra*. Tételezzük fel, hogy az $L$ elsőrendű nyelv a $c_i$ konstansjeleket, $f_i$ függvényjeleket, $R_i$ relációjeleket tartalmazza. (A többi eleme ugyanis egyértelműen elő van írva.) Ekkor egy $L$-nek megfelelő $\mathcal{A}$ struktúra a következő elemekből áll: egy nemüres $A$ halmaz, minden $c_i$ konstansjelhez egy $C_i \in A$ kitüntetett elem, minden $f_i$ függvényjelhez, ha az $n$-változós, egy $n$-változós $F_i$ függvény $A$-n, tehát $F_i : A^n \to A$, minden $R_i$ relációjelhez, ha az $n$-változós, egy $n$-változós $r_i$ reláció, tehát $r_i \subseteq A^n$. A kötelezően előírt kétváltozós $R_0$ relációjelnél azonban ragaszkodunk ahhoz, hogy $r_0$ az igazi egyenlőség legyen.

A fentiekben is látható, hogy meg kell különböztetnünk (például) a függvényjelet a hozzátartozó függvényektől, a valóságban ezt azonban, érthető okokból mégsem tesszük. Így például, ha gyűrűkről van szó, a + jel egyszerre jelöli az összeadás műveletének *jelét* és (esetleg) végtelen sok gyűrű egyik műveletét.

Ezután definiáljuk a kifejezések és formulák *kiértékelés*ét. Ehhez legyen adva egy elsőrendű nyelv $c_i, f_i, R_i$ jeleivel. Legyen szintén adva egy $\mathcal{A}$ struktúra az $A \neq \emptyset$ halmazon, $C_i \in A$ elemekkel, $F_i$ függvényekkel és $r_i$ relációkkal. Tételezzük fel, hogy rögzítve van $A$ elemeinek egy $a_0, a_1, \ldots$ sorozata. Ekkor a kifejezések és formulák felépítése szerinti indukcióval definiáljuk a $H$ kiértékelést a következőképpen. Kifejezések: $H(v_i) = a_i$, $H(c_i) = C_i$, $H(f_i(t_1, \ldots, t_n)) = F_i(H(t_1), \ldots, H(t_n))$. Formulák: $H(R_i(t_1, \ldots, t_n)) = \mathrm{i}$, ha $r_i(H(t_1), \ldots, H(t_n))$

fennáll,

$$H(\neg\varphi) = \begin{cases} \text{i}, & \text{ha } H(\varphi) = \text{h} \\ \text{h}, & \text{ha } H(\varphi) = \text{i}, \end{cases}$$

$$H(\varphi \vee \psi) = \begin{cases} \text{i}, & \text{ha } H(\varphi) = \text{i vagy } H(\psi) = \text{i} \\ \text{h}, & \text{különben}, \end{cases}$$

végül pedig, ha $\varphi$ a $\exists v_i \psi$ formula, akkor $H(\varphi)$-t a következőképpen definiáljuk: $H(\varphi) = \text{i}$ pontosan akkor, ha van olyan $H'$ kiértékelés, amire $H'(\psi) = \text{i}$ és $H'$ úgy keletkezik, hogy az eredetileg adott $a_0, a_1, \ldots$ sorozat $a_i$ elemét $A$ valamelyik $a$ elemére cseréljük.

Jól látható hogy az előző definíció egyszerű alapgondolata, hogy „kiolvassuk", amit a kifejezések és formulák „mondanak", csak $v_i$ helyett $a_i$-t, $c_i$ helyett $C_i$-t, stb kell értenünk. Végrehajtjuk a formális utasításokat. A gondot csak a kvantorok jelentik, ekkor ugyanis nem azt nézzük meg, hogy az adott $a_i$ érték megfelel-e, hanem, hogy található-e az $i$-edik változóhelyére olyan érték, ami igazzá teheti a formulát. Ebből rögtön látható, hogy $H(t)$, $H(\varphi)$ csak azoktól az $a_i$-ktől függ, amik $V(t)$, $V(\varphi)$-ben vannak, magyarán a formula értéke csak szabad változóitól függ. Zárt formula igazságértéke nem függ az $a_0, a_1, \ldots$ elemektől, azért voltunk kénytelenek mégis így definiálni a kiértékelést, mert a zárt formulákat, a formulafelépítés szabályai szerint csak nem-zárt formulákonkeresztül tudtuk felépíteni.

Érdemes leszögezni, hogy a kiértékelésnél válik világossá, amit korábban is éreztünk, hogy kifejezés elemet jelöl, formula igazságértéket kap.

Ha $L$ elsőrendű nyelv, $\Gamma$ ennek formulahalmaza, $\mathcal{A}$ pedig struktúra ebben a nyelvben, azt mondjuk, hogy $\mathcal{A}$ *modellje* $\Gamma$-nak, vagy $\mathcal{A}$ *modellezi* $\Gamma$-t, ha minden $\varphi \in \Gamma$ formulára és $a_0, a_1, \ldots \in A$ elemekre a $H(\varphi)$ kiértékelés eredménye i. Ezt így jelöljük: $\mathcal{A} \models \Gamma$. Ha $\Gamma$ csak a $\varphi$ formulából áll, $\mathcal{A} \models \{\varphi\}$ helyett $\mathcal{A} \models \varphi$-t is írunk. Felhívjuk a figyelmet arra, hogy ha $\varphi$ nem zárt formula, akkor előfordulhat, hogy sem $\mathcal{A} \models \varphi$ sem $\mathcal{A} \models \neg\varphi$ nem teljesül. ($\varphi$ „időnként" igaz, „időnként" nem.)

A továbbiakban kidolgozzuk az elsőrendű nyelvekbeli levezetésekkel kapcsolatos alapfogalmakat. Ezek a kijelentéslogika hasonló fogalmaira épülnek, a többlet, természetszerűleg, a kvantorok és a műveleti/relációjelek kezelésével kapcsolatos.

*Helyettesítés*nek nevezzük, ha egy $\varphi$ formulában a $v_i$ változójel minden előfordulása helyébe a $t$ kifejezést írjuk. Jelben: $\varphi_{v_i}[t]$. *Megengedett helyettesítést* mondunk, ha ekkor $t$ azonos $v_i$-vel (azaz nem történik semmi) vagy minden olyan esetben, ha $v_j \in V(t)$, akkor $\varphi$ felépítése során $v_i$ egyik előfrodulása sem áll $\exists v_j$ alakú kvantor hatókörében. A különbségtétel oka a következő. Érezhető, hogy „igaz" formula helyettesítéskor is igaz, mert „specializálunk". Például az $xy = yx$ formulát egy $x \to x^2$ cserével az $x^2y = yx^2$ formulává cseréljük. Nem megengedett helyettesítéskor viszont olyasmi történhet, amit nem akarunk:

a $\exists x\big[x = S(y)\big]$ formulából (ami a természetes számokon mindig igaz), az $y$ helyébe $x$-et írva $\exists x\big[x = S(x)\big]$ adódik, ami nagyon nem igaz.

A logikai axiómákat két további csoporttal egészítjük ki:

4. $\forall v_i \varphi \to \varphi_{v_i}[t]$, ha a helyettesítés megengedett,
5. $\big(\forall v_i(\varphi \to \psi)\big) \to \big(\varphi \to \forall v_i \psi\big)$, ha $v_i \notin V(\varphi)$.

Egy újabb csoport az egyenlőségaxiómáké.

1. $v_i = v_i \quad (i = 0, 1, \ldots)$
2. $(v_i = v_j) \to (v_j = v_i) \quad (i, j = 0, 1, \ldots)$
3. $\big((v_i = v_j) \wedge (v_j = v_k)\big) \to \big(v_i = v_k\big) \quad (i, j, k = 0, 1, \ldots)$
4. $\big((v_{i_1} = v_{j_1}) \wedge \cdots \wedge (v_{i_n} = v_{j_n})\big) \to \big(R(v_{i_1}, \ldots, v_{i_n}) \to R(v_{j_1}, \ldots, v_{j_n})\big)$ ($R$ $n$-változós relációjel)
5. $\big((v_{i_1} = v_{j_1}) \wedge \cdots \wedge (v_{i_n} = v_{j_n})\big) \to \big(f(v_{i_1}, \ldots, v_{i_n}) = f(v_{j_1}, \ldots, v_{j_n})\big)$ ($f$ $n$-változós függvényjel)

Az elsőrendű nyelvekbeli levezetéseket ezekután ugyanúgy definiáljuk, mint a kijelentéslogikában, csak az új logikai és az egyenlőségaxiómákon túl a modus ponens mellé egy új következtetési szabályt is hozzáveszünk: a generalizációt (GEN), ami lehetővé teszi, hogy a $\varphi$ formulából, tetszőleges $v_i$ változó esetén a $\forall v_i$ formulát levezessük.

Ekkor, ha egy $\Gamma$ formulahalmazból sikerül levezetni a $\varphi$ formulát, azt $\Gamma \vdash \varphi$-vel jelöljük. Ha $\Gamma$ egyelemű, általában elhagyjuk a kapcsos zárójeleket.

Lássunk egy példát elsőrendű nyelvben való levezetésre!

**Állítás.** $\forall x \forall y \varphi \vdash \forall y \forall x \varphi$.

**Bizonyítás.** Megadjuk a levezetést.

1. $\forall x \forall y \varphi$ (eleme $\Gamma$-nak)
2. $(\forall x \forall y \varphi) \to (\forall y \varphi)$ (4. logikai axióma)
3. $\forall y \varphi$ (modus ponens 1,2-ből)
4. $\forall y \varphi \longrightarrow \varphi$ (4. logikai axióma)
5. $\varphi$ (modus ponens 3,4-ből)
6. $\forall x \varphi$ (GEN 5-ből)
7. $\forall y \forall x \varphi$ (GEN 6-ból)

□

# 8 A modellelmélet tételei

Tegyük fel, hogy $L$ elsőrendű nyelv, $T$ benne felírt zárt formulák bármilyen halmaza (az ilyen halmazokat *elmélet*nek nevezzük).

**Igazság tétel.** *Ha $T$-nek van modellje, akkor ellentmondásmentes.*

**Bizonyítás.** Persze, mert, ha $T$-ből le tudnánk vezetni a $\varphi$ zárt formulát és annak tagadását is, akkor az állítólagos modellen mindkettő igaz lenne. □

**Teljességi tétel.** *Ha $T$ ellentmondásmentes, akkor van modellje.*

E nevezetes tétel bizonyítását annak bonyolultsága miatt nem adjuk.

**Kompaktsági tétel** *Ha $T$ minden véges részének van modellje, akkor $T$-nek is van.*

**Bizonyítás.** Ha $T$-nek nincs modellje, akkor a teljességi tétel szerint levezethető belőle ellentmondás. Ez a levezetés (mivel véges sorozat) $T$-nek csak egy véges $T'$ részét használja. Ekkor már $T'$-ből is ellentmondást tudunk levezetni (ugyanazzal a levezetéssel), tehát az igazság tétel szerint $T'$-nek nem lehet modellje. □

**Löwenheim-Skolem-Tarski tétel.** *Ha egy $T$ elméletnek van végtelen modellje, akkor minden végtelen a számosságra van a számosságú modellje.*

Itt fontos annak kikötése, hogy végtelen modell van, mert minden $n$ természetes számra van olyan zárt formula, amelynek csak $n$-elemű modelljei vannak. Például $n = 3$-ra ilyen

$$\exists x \exists y \exists z \big[ (x \neq y) \wedge (x \neq z) \wedge (y \neq z) \wedge \forall u \big( (u = x) \vee (u = y) \vee (u = z) \big) \big].$$

A tétel azt állítja, hogy az elsőrendű logika eszközeivel Hilbert célkitűzései kivitelezhetetlenek: a számelmélet bármilyen axiomatizálásához van (például) kontinuum számosságú modell. Hasonlóan, ha a valós számokon értelmezett bármilyen struktúrát axiomatizálunk, annak van megszámlálható modellje, stb. Fontos azonban, hogy elsőrendű logikáról van szó, ha például hivatkozhatunk a részhalmaz fogalmára (másodrendű logika), akkor bevezethetjük a valós számokon a limesz fogalmát és elvégezhetjük a szokásos axiomatizálást.

A tételnek egy fontos speciális esetét bizonyítjuk.

**Löwenheim-Skolem tétel.** *Ha egy $T$ elméletnek van végtelen modellje, akkor van $\aleph_0$ számosságú modellje.*

**Bizonyítás.** Legyen adva az $L$ elsőrendű nyelv valamely $T$ elméletének $\mathcal{A}$ modellje, tehát egy végtelen $A$ halmaz, benne a $C_i \in A$ konstansok, rajta az $F_i$ függvények, $r_i$ relációk, valamennyi az $L$ által előírt változószámmal. Célunk egy másik, $\mathcal{B}$ modell felépítése, ami megszámlálható és rajta $T$ formulái igazak. Mivel két modellel kell dolgoznunk, a modellekhez kötődő fogalmaknál időnként jelölni fogjuk, hogy melyik modellről van szó.

**1. Állítás.** *$L$-nek $\aleph_0$ formulája van.*

**Bizonyítás.** A definíció alapján $|L| = \aleph_0$. Minden formula $L$-beli elemek véges sorozata, így számuk legfeljebb $\aleph_0 + \aleph_0^2 + \cdots = \aleph_0$. Legalább $\aleph_0$ formula pedig mindenképpen van: $v_0 = v_0$, $v_1 = v_1$, stb. □

Vegyük azokat a formulákat, amelyek nem zártak, tehát van legalább egy szabad változójuk. Mindegyiknél (minden lehetséges módon) elkülönítjük az egyik szabad változót, tehát ezen $\varphi$ formulák mindegyike így néz ki: $\varphi(x_1, \ldots, x_n, y)$. Ezekhez a fomulákhoz készítsük el a következő függvényeket:

$$g_\varphi(a_1, \ldots, a_n) = \begin{cases} \text{ha van } a \in A, \text{ amire } \varphi(a_1, \ldots, a_n, a), \text{ egy ilyen } a, \\ \text{akármi, ha nincs.} \end{cases}$$

Ezzel tehát definiáltunk megszámlálható sok $A$-n értelmezett, különböző változószámú függvényt.

Ezután definiáljuk a leendő $\mathcal{B}$ modell alaphalmazát, ami $A$ részhalmaza lesz. Legyen $B_0$ $A$-nak tetszőleges olyan $\aleph_0$ számosságú részhalmaza, amely minden $C_i^{\mathcal{A}}$-t tartalmaz. (Vegyük ezek halmazát, ha végtelen sokan vannak, ha csak véges sok van belőlük, esetleg egy sincs, tegyünk melléjük még végtelen sok elemet.)

Definiáljuk a $B_1, B_2, \ldots$ halmazokat a következőképpen:

$$B_1 = B_0 \cup \{F_i(a_1, \ldots, a_n) : a_1, \ldots, a_n \in B_0\} \cup \{g_\varphi(a_1, \ldots, a_n) : a_1, \ldots, a_n \in B_0\},$$

$$B_2 = B_1 \cup \{F_i(a_1, \ldots, a_n) : a_1, \ldots, a_n \in B_1\} \cup \{g_\varphi(a_1, \ldots, a_n) : a_1, \ldots, a_n \in B_1\},$$

és így tovább. Legyen végül $B = B_0 \cup B_1 \cup \cdots$, halmazaink növő úniója.

**2. Állítás.** *$B_0$, $B_1, \ldots$, $B$ mind $\aleph_0$ számosságú.*

**Bizonyítás.** $B_{i+1}$ úgy keletkezik $B_i$-ből, hogy $B_i$-hez hozzáadjuk megszámlálható sok függvény megszámlálható sok helyen felvett értékét. Ezért $|B_{i+1}| = \aleph_0$. Innen $|B| = \aleph_0 + \aleph_0 + \cdots = \aleph_0$ adódik. □

**3. Állítás.** *$B$ zárt mind az $F_i$, mind a $g_\varphi$ függvényekre.*

**Bizonyítás.** Legyen adva $F_i$ és $b_1, \ldots, b_n \in B$. Mivel $B$ a $B_j$ halmazok növő úniója, van olyan $j$, hogy $b_1, \ldots, b_n \in B_j$. Ekkor $F_i(b_1, \ldots, b_n) \in B_{j+1} \subseteq B$. Hasonlóan kapjuk a zártságot a $g_\varphi$ függvényekre. □

Mint mondtuk, $B$ lesz megszámlálható $\mathcal{B}$ modellünk alaphalmaza. A struktúrát a következőképpen definiáljuk: a konstansok: $C_i^{\mathcal{B}} = C_i$; a függvények: $F_i^{\mathcal{B}} = F_i$ megszorítása $B$-re; a relációk: $r_i^{\mathcal{B}} = r_i$ megszorítása $B$-re. Láthatjuk, nincs baj a konstansok definiálásával, mert $B$-t úgy választottuk, hogy benne van minden $C_i$. Hasonlóan, az $F_i^{\mathcal{B}}$-k függvények lesznek $B$-n, mert $B$-t ezekre zártaknak választottuk.

A következőkben azt vizsgáljuk meg, hogy ha adott egy $b_0, b_1, \ldots \in B$ sorozat, akkor az ehhez a sorozathoz tartozó két kiértékelés, $H^{\mathcal{A}}$ és $H^{\mathcal{B}}$ hogyan viszonyul egymáshoz.

**4. Állítás.** *Ha $b_0, b_1, \ldots \in B$, $t$ kifejezés, akkor $H^{\mathcal{B}}(t) = H^{\mathcal{A}}(t)$.*

**Bizonyítás.** A kifejezés felépítése szerinti indukcióval. Ha $t$ valamelyik $c_i$ konstansjel, akkor $H^{\mathcal{A}}(t) = C_i$, míg $H^{\mathcal{B}}(t) = C_i^{\mathcal{B}}$ de ez azonos az előbbivel. Ha $t$ valamelyik $v_i$ változójellel egyezik meg, akkor $H^{\mathcal{A}}(t) = b_i$, és $H^{\mathcal{B}}(t)$ is $b_i$-vel egyezik meg, tehát az azonosság fennáll.

Tegyük most fel, hogy $t = f_i(t_1, \ldots, t_n)$ alakú kifejezés és a $t_1, \ldots, t_n$ kifejezésekre már tudjuk az állítást. Ekkor a bizonyítandó egyenlőség így alakítható:

$$\begin{aligned} H^{\mathcal{B}}(t) &= H^{\mathcal{A}}(t) \\ H^{\mathcal{B}}(f_i(t_1, \ldots, t_n)) &= H^{\mathcal{A}}(f_i(t_1, \ldots, t_n)) \\ F_i^{\mathcal{B}}\big(H^{\mathcal{B}}(t_1), \ldots, H^{\mathcal{B}}(t_n)\big) &= F_i\big(H^{\mathcal{A}}(t_1), \ldots, H^{\mathcal{A}}(t_n)\big) \end{aligned}$$

ez pedig fennáll, mert az utolsó egyenlőség argumentumai az indukció miatt azonosak a két oldalon, $F_i^{\mathcal{B}}$ pedig ugyanúgy hat, mint $F_i$, legalábbis $B$ elemein. □

**5. Állítás.** *Ha $b_0, b_1, \ldots \in B$, $\varphi$ formula, akkor $H^{\mathcal{B}}(\varphi)$ akkor és csak akkor igaz, ha $H^{\mathcal{A}}(\varphi)$ igaz.*

**Bizonyítás.** Legyen először $\varphi = R_i(t_1, \ldots, t_n)$ prímformula. Ekkor $H^{\mathcal{B}}(\varphi) = \mathrm{i}$ akkor és csak akkor, ha $b$-nek a $H^{\mathcal{B}}(t_1), \ldots, H^{\mathcal{B}}(t_n)$ elemei az $r_i^{\mathcal{B}}$ relációban állnak. A 4. Állítás szerint ezek azonosak rendre a $H^{\mathcal{A}}(t_1), \ldots, H^{\mathcal{A}}(t_n)$ elemekkel. Ezek pedig akkor és csak akkor állnak az $r_i^{\mathcal{B}}$ relációban ha az $r_i^{\mathcal{B}}$ relációban, $r_i^{\mathcal{B}}$ definíciója szerint. Ezért $H^{\mathcal{B}}(\varphi) = \mathrm{i}$ akkor és csak akkor teljesül, ha $H^{\mathcal{A}}(\varphi) = \mathrm{i}$.

Legyen $\varphi = \neg\psi$ alakú, és $\psi$-re már tudjuk az állítást. Ekkor

$$H^{\mathcal{B}}(\varphi) = \mathrm{i} \iff H^{\mathcal{B}}(\psi) = \mathrm{h} \iff H^{\mathcal{A}}(\psi) = \mathrm{h} \iff H^{\mathcal{A}}(\varphi) = \mathrm{i}.$$

Legyen $\varphi = \psi_1 \vee \psi_2$ alakú, és $\psi_1$, $\psi_2$-re már tudjuk az állítást. Ekkor

$$\begin{aligned} H^{\mathcal{B}}(\varphi) = \mathrm{i} &\iff \big(H^{\mathcal{B}}(\psi_1) = \mathrm{i}\big) \vee \big(H^{\mathcal{B}}(\psi_2) = \mathrm{i}\big) \\ &\iff \big(H^{\mathcal{A}}(\psi_1) = \mathrm{i}\big) \vee \big(H^{\mathcal{A}}(\psi_2) = \mathrm{i}\big) \\ &\iff H^{\mathcal{A}}(\varphi) = \mathrm{i}. \end{aligned}$$

Tegyük végül fel, hogy elérkeztünk egy $\psi = \exists y \varphi(x_1, \ldots, x_n, y)$ alakú formulához és $\varphi$-re már beláttuk az állítást. Írjuk ki pontosan $\varphi$ változóit:

$$\psi = \exists v_k \varphi(v_{i_1}, \ldots, v_{i_n}, v_k).$$

Tegyük fel először, hogy $H^{\mathcal{B}}(\psi) = \mathrm{i}$. Ekkor, $H^{\mathcal{B}}$ definíciója szerint, van $b \in B$, hogy $H^{\mathcal{B}}\big(\varphi(b_{i_1}, \ldots, b_{i_n}, b)\big) = \mathrm{i}$. Mivel indukciós feltevésünk szerint $\varphi$-re igaz az állítás, $H^{\mathcal{A}}\big(\varphi(b_{i_1}, \ldots, b_{i_n}, b)\big) = \mathrm{i}$, tehát $H^{\mathcal{A}}(\psi) = \mathrm{i}$.

Tegyük végül fel, hogy $H^{\mathcal{A}}(\psi) = \mathrm{i}$. Azaz, van $a \in A$, hogy

$$H^{\mathcal{A}}\big(\varphi(b_{i_1}, \ldots, b_{i_n}, a)\big) = \mathrm{i}.$$

Ezek szerint, $g_\varphi(b_{i_1}, \ldots, b_{i_n})$ definíciójában az első eset áll fenn, tehát $b = g_\varphi(b_{i_1}, \ldots, b_{i_n})$-re az $\mathcal{A}$ modellben

$$H^{\mathcal{A}}\big(\varphi(b_{i_1}, \ldots, b_{i_n}, b)\big) = \mathrm{i}$$

teljesül. A 2. Állítás szerint $b \in B$. Az indukciót ismét használva

$$H^{\mathcal{B}}\big(\varphi(b_{i_1}, \ldots, b_{i_n}, b)\big) = \mathrm{i}$$

innen $H^{\mathcal{B}}(\psi) = \mathrm{i}$. □

Az utolsó állításból következik a tétel, mivel minden $\varphi \in T$ zárt formulára $H^{\mathcal{B}}(\varphi) = H^{\mathcal{A}}(\varphi) = \mathrm{i}$. □

# 9 Primitív rekurzív függvények

A továbbiakban az $\mathbf{N} = \{0, 1, \ldots\}$-en értelmezett, ugyanide képező, egy- és többváltozós függvényekkel foglalkozunk.
**Alapfüggvények.** $0(x) = 0$, $S(x) = x + 1$, $I_m^n(x_1, \cdots, x_m) = x_m$.
**Operációk.**

**Kompozíció.** Az $f$ függvény kompozícióval készül a $g, h_1, \ldots, h_m$ függvényekből, ha $f(x_1, \ldots, x_n = g(h_1(x_1, \ldots, x_n), \ldots, h_m(x_1, \ldots, x_n))$.

**Primitív rekurzió** Az $f(x_1, \ldots, x_n, y)$ függvény primitív rekurzióval készül a $g(x_1, \ldots, x_n)$ és a $h(x_1, \ldots, x_n, y, z)$ függvényekből, ha $f(x_1, \ldots, x_n, 0) = g(x_1, \ldots, x_n)$ és $f(x_1, \ldots, x_n, y + 1) = h(x_1, \ldots, x_n, y, f(x_1, \ldots, x_n, y))$.

**Definíció.** *Primitív rekurzívaknak* nevezzük az alapfüggvényekből a fenti operációk tetszés számú alkalmazásával nyert függvényeket.

**Példák primitív rekurzív függvényekre.**

1. A konstans $n$ függvény.

$$f(x) = \underbrace{S(S(\cdots(S}_{n}(0(x)))\cdots))$$

2. $x \dot{-} 1 = \begin{cases} 0, & \text{ha } x = 0 \\ x - 1, & \text{ha } x \geq 0. \end{cases}$ $f(0) = 0$. $f(y + 1) = y$.

3. $sg(x) = \begin{cases} 0, & \text{ha } x = 0 \\ 1, & \text{ha } x \geq 0. \end{cases}$

4. $\overline{\mathrm{sg}}(x) = \begin{cases} 1, & \text{ha } x = 0 \\ 0, & \text{ha } x \geq 0. \end{cases}$

5. $x \dot{-} y = \begin{cases} x - y, & \text{ha } x \geq y \\ 0, & \text{ha } x < y. \end{cases}$

6. $f(x,y) = x + y$. $f(x,0) = x$, $f(x,y+1) = S(f(x,y))$.

7. $f(x,y) = xy$. $f(x,0) = 0$, $f(x,y+1) = f(x,y) + x$.

8. $f(x,y) = x^y$. $f(x,0) = 1$, $f(x,y+1) = f(x,y)x$.

9. $|x - y| = (x \dot{-} y) + (y \dot{-} x)$

10. A maradékos osztás függvénye. $\mathrm{rem}(y,a) = r$, ahol $y = aq + r$, $0 \leq r < a$. $\mathrm{rem}(0,a) = 0$, $\mathrm{rem}(y+1,a) = (r+1)h(r+1)$, ahol $r = \mathrm{rem}(y,a)$, $h(x) = \mathrm{sg}(|x - a|)$. Jegyezzük meg, hogy $\mathrm{rem}(y,0) = y$.

11. $f(x_1,\ldots,x_n,y) = \sum_{z=0}^{y} g(x_1,\ldots,x_n,z)$. Hiszen

$$f(x_1,\ldots,x_n,0) = g(x_1,\ldots,x_n,0),$$

$$f(x_1,\ldots,x_n,y+1) = f(x_1,\ldots,x_n,y) + g(x_1,\ldots,x_n,y+1).$$

12. $f(x_1,\ldots,x_n,y) = \prod_{z=0}^{y} g(x_1,\ldots,x_n,z)$. Ez ugyanúgy megy:

$$\begin{aligned} f(x_1,\ldots,x_n,0) &= g(x_1,\ldots,x_n,0), \\ f(x_1,\ldots,x_n,y+1) &= f(x_1,\ldots,x_n,y)g(x_1,\ldots,x_n,y+1). \end{aligned}$$

13. Az osztást leíró függvény. $\mathrm{div}(y,x) = \begin{cases} 1, & \text{ha } y|x \\ 0, & \text{ha } y \not| x. \end{cases}$ Ugyanis $\mathrm{div}(y,x) = 1 \dot{-} \mathrm{rem}(x,y)$

14. Az osztók száma.

$$d(x) = \sum_{y=0}^{x} \mathrm{div}(y,x)$$

15. A prímek száma $x$-ig.

$$\pi(x) = \sum_{y=0}^{x} \overline{\mathrm{sg}}(|d(x) - 2|)$$

16. $t(x,n) = \begin{cases} 1, & \text{ha } x < \sqrt{2}\cdot 2^n \\ 0, & \text{ha } x > \sqrt{2}\cdot 2^n. \end{cases}$

$s(x,n) = \begin{cases} 1, & \text{ha } x+1 > \sqrt{2}\cdot 2^n \\ 0, & \text{ha } x+1 < \sqrt{2}\cdot 2^n. \end{cases}$

Ugyanis $t(x,n) = \mathrm{sg}(2^{2n+1} \dot{-} x^2)$, $s(x,n) = \mathrm{sg}((x+1)^2 \dot{-} 2^{2n+1})$.

17. $g(n) = [\sqrt{2}\cdot 2^n]$. Ugyanis

$$g(n) = \sum_{x=0}^{2^{n+1}} x \cdot t(x,n) \cdot s(x,n).$$

18. $f(n) = \sqrt{2}$ $n$-edik bináris jegye. Ugyanis $f(n) = \mathrm{rem}(g(n), 2)$.

19. Legvégül belátjuk, hogy a Fibonacci-sorozat:

$$\begin{aligned} F(0) &= 0, \\ F(1) &= 1, \\ F(y+1) &= F(y) + F(y-1) \end{aligned}$$

is primitív rekurzív függvény. Itt a nehézség az, hogy a függvény értéke nem az előző, hanem az előző két értékből lett definiálva. Ezért előkészületeket csinálunk. Minden $x > 0$ szám egyértelműen írható $x = 2^y(2z+1)$ alakban. Először megmutatjuk, hogy a $x = 2^{\alpha(x)}(2\beta(x)+1)$ segítségével definiált $\alpha(x)$, $\beta(x)$ függvények primitív rekurzívak.

$$\alpha(x) = \sum_{y=0}^{x} \sum_{z=0}^{x} y\, \overline{\mathrm{sg}}(|2^y(2z+1) - x|)$$

és hasonlóan

$$\beta(x) = \sum_{y=0}^{x} \sum_{z=0}^{x} z\, \overline{\mathrm{sg}}(|2^y(2z+1) - x|)$$

Legyen most $G(x) = 2^{F(x)}(2F(x+1)+1)$. Ha belátjuk, hogy $G(x)$ primitív rekurzív, akkor készen vagyunk, hiszen $F(x) = \alpha(G(x))$. $G(0) = 3$. Ha $G(x) = y$, akkor

$$\begin{aligned} G(x+1) &= 2^{F(x+1)}(2F(x+2)+1) \\ &= 2^{F(x+1)}(2(F(x)+F(x+1))+1) \\ &= 2^{\beta(y)}(2(\alpha(y)+\beta(y))+1), \end{aligned}$$

primitív rekurzív függvénye $y$-nak.

**Feladat.** Lássuk be, hogy az $f(n) = p_n$, az $n$-edik prímszám függvénye primitív rekurzív!

# 10 Az Ackermann-függvény

Az előző fejezet példáiból úgy tűnhet, hogy minden, valamilyen algoritmussal kiszámítható függvény egyben primitív rekurzív is. Ez azonban nincs így. A nevezetes ellenpélda Ackermanntól ered, itt példájának Péter Rózsa által egyszerűsített változatát ismertetjük.

A kétváltozós $A(x,y)$ függvényt a következőképpen definiáljuk. $A(0,y) = 2^y$, $A(x+1,0) = A(x,1)$, $A(x+1,y+1) = A\big(x, A(x+1,y)\big)$.

Az $A(x,y)$ függvény néhány értékét az alábbi táblázat adja:

| $x\backslash y$ | 0 | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|
| 0 | 1 | 2 | 4 | 8 | 16 | 32 |
| 1 | 2 | 4 | 16 | 65536 | $2^{65536}$ | $2^{2^{65536}}$ |
| 2 | 4 | $2^{65536}$ | $A$ | $B$ | ... | ... |

ahol $A = 2^{2^{\cdot^{\cdot^{\cdot^{2}}}}}\Big\}\, 2^{65536}+1$ és $B = 2^{2^{\cdot^{\cdot^{\cdot^{2}}}}}\Big\}\, A+1$.

Vegyük észre, hogy az $A(x,y)$ kiszámítására szolgáló három képlet közül mindig pontosan egy volt hasznunkra. Továbbá, $x$-re vonatkozó indukcióval látható, hogy minden $y$-ra $A(x,y)$ értelmezett (tehát sorról sorra belátjuk, hogy a sor végig ki van töltve értékekkel) és hasonlóan látható, hogy minden rögzített $x$-re $A(x,y)$, mint egyváltozós függvény, primitív rekurzív. Belátjuk, hogy az $A(x,x)$ egyváltozós függvény nem primitív rekurzív.

**Tétel.** *Ha $f(x_1,\ldots,x_n)$ primitív rekurzív függvény, akkor van olyan a természetes szám, hogy mindig fennáll $f(x_1,\ldots,x_n) \le A(a,z)$, ahol $z = \max(x_1,\ldots,x_n)$.*

**Bizonyítás.** Az állítást $f(x_1,\ldots,x_n)$ felépítését követő indukcióval bizonyítjuk.

**1.Állítás.** $A(x,y) < A(x,y+1)$.

**Bizonyítás.** $x = 0$-ra ez $2^y < 2^{y+1}$, ami igaz. Általában pedig $x$-re vonatkozó indukciót alkalmazunk. Ha tudjuk, hogy $x$-re az állítás igaz, akkor $A(x,y) \ge A(x,y-1)+1 \ge \cdots \ge A(x,0)+y > y$-t írhatunk. Innen $A(x+1,1) = A(x,A(x+1,0)) > A(x+1,0)$. Innen tovább:

$$A(x+1,y+2) = A(x,A(x+1,y+1)) > A(x,A(x+1,y)) = A(x+1,y+1),$$

mert $x$-re az indukciós feltevés szerint már tudjuk, hogy igaz az állítás. □

**2.Állítás.** $A(x,y) < A(x+1,y)$.

**Bizonyítás.** $y = 0$-ra ez $A(x+1,0) = A(x,1) > A(x,0)$. Ez pedig igaz az előző állítás miatt. A definícióból látható, hogy $A(X,y)$ mindig 2-hatvány és $A(0,0)$ kivételével sosem 1. Ezért

$$A(x+1,y) \ge 2A(x+1,y-1) \ge \cdots \ge 2^y A(x+1,0) \ge 2^{y+1}.$$

Innen $A(x+1,y+1) = A(x,A(x+1,y)) \ge A(x,2^{y+1}) > A(x,y+1)$ (mivel $A(x,y)$ $y$-ban monoton). □

**3.Állítás.** $A(x+1, y+1) \leq A(x+2, y)$.

**Bizonyítás.** $y = 0$-ra ez $A(x+1, 1) = A(x+2, 0)$, a definíció miatt. Ha egy adott $y$-ra igaz, akkor $A(x+1, y+2) = A(x, A(x+1, y+1)) \leq A(x+1, A(x+2, y)) = A(x+2, y+1)$. □

**4. Állítás.** *Legyen $f$ a $g$ és a $h_i$ függvények kompozíciója. Ha $g$, $h_i \leq A(a, z)$ ($z$ mindig az aktuális változók maximuma), akkor $f \leq A(a+2, z)$.*

**Bizonyítás.** $f(x_1, \ldots, x_n) = g(h_1, \ldots, h_m) \leq A\big(a, A(a, z)\big) \leq A\big(a, A(a+1, z)\big) = A(a+1, z+1) \leq A(a+2, z)$. □

**5. Állítás.** *Tegyük fel, hogy $f = f(x_1, \ldots, x_n, y)$ primitív rekurzióval adódik $g$, $h$-ból. Ha $g$, $h \leq A(a, z)$, akkor $f \leq A(a+2, z)$ ($z$ mindig az aktuális változók maximuma).*

**Bizonyítás.** Először belátjuk, hogy $f(x_1, \ldots, x_n, y) \leq A(a+1, z+y)$, ahol $z = \max(x_1, \ldots, x_n)$. $y = 0$-ra ez $g(x_1, \ldots, x_n) \leq A(a, z) \leq A(a+1, z)$. Tegyük fel, hogy $y$-ra már tudjuk az állítást. $f\big(x_1, \ldots, x_n, y+1\big) = h\big(x_1, \ldots, x_n, y, f(x_1, \ldots, x_n, y)\big) \leq A\big(a, A(a+1, z+y)\big) = A\big(a+1, z+y+1\big)$, mert $z,\ y \leq z+y \leq A(a+1, z+y)$.

Legyen ezután $t = \max(z, y) = \max(x_1, \ldots, x_n, y)$. Mivel $z+y \leq 2t$, $A(a+1, z+y) \leq A(a+1, 2t)$. A továbbiakhoz először is belátjuk, hogy $2t \leq A(a+2, t-1)$, ha $t \geq 1$. Azt már láttuk, hogy $A(a+2, t-1) \geq \cdots \geq A(a+2, 0)2^{t-1} \geq 2t$. Ezért $A(a+1, 2t) \leq A\big(a+1, A(a+2, t-1)\big) = A(a+2, t)$, ha $t \geq 1$. Ha pedig $t = 0$, akkor nyilván $A(a+1, 2t) \leq A(a+2, t)$. □

A tétel bizonyítása ezután egész egyszerű, az alapfüggvényekre $a = 0$ vehető, mert $x+1 \leq 2^x$. A többi primitív rekurzív függvényre indukcióval a megelőző két állítással adódik az egyenlőtlenség. □

**Következmény.** *Az egyváltozós $A(x, x)$ függvény nem primitív rekurzív.*

**Bizonyítás.** Ha az lenne, akkor $A(x, x) + 1$ is az lenne, de ekkor lenne olyan $a$ természetes szám, hogy $A(x, x) + 1 \leq A(a, x)$ teljesül minden $x$-re, ami viszont $x = a$-ra nem igaz. □

# 11 Kiszámítható függvények

A továbbiakban olyan függvényekkel dolgozunk, amelyek esetleg nincsenek mindenütt értelmezve.

**Definíció.** Egy $f(x_1, \ldots, x_n)$ függvény *parciális*, ha értelmezési tartománya a természetes számokból álló $n$ hosszúságú sorozatok bármilyen részhalmaza, értékeit természetes számokból veszi. Ha minden szám-$n$-esre értelmezve van, akkor $f$ *totális*.

**Definíció.** (*Minimalizáció, $\mu$-operáció.*) Ha $f(x_1, \ldots, x_n, y)$ parciális függvény, akkor

$$g(x_1, \ldots, x_n) = \mu y\big[f(x_1, \ldots, x_n, y) = 0\big]$$

jellel a következő függvényt jelöljük: $g(x_1, \ldots, x_n) = y$, ha $f(x_1, \ldots, x_n, 0)$, $\ldots$, $f(x_1, \ldots, x_n, y)$ mind értelmezett és csak a legutolsó 0, ha ilyen $y$ nem létezik, akkor $g(x_1, \ldots, x_n)$ nem definiált.

**Definíció.** Egy $f(x_1, \ldots, x_n)$ parciális függvényt *parciálisan rekurzívnak* nevezünk, ha előáll az alapfüggvényekből kompozícióval, primitív rekurzióval és minimalizációval. Ha $f$ totális, akkor *rekurzív* függvénynek nevezzük.

A minimalizáció kivezet a totális függvények osztályából: $g(x) = \mu y[x - y^2 = 0]$ csak a négyzetszámokon van értelmezve. De vissza is vezethet: $f(x) = \mu y[g(y) = 0]$ azonosan nulla.

A tapasztalat azt mutatja, hogy bármilyen algoritmussal kiszámítható függvényt veszünk, az parciálisan rekurzív. Könnyű látni, hogy fordítva is igaz; minden parciálisan rekurzív függvény algoritmussal kiszámítható.

Ezt, az intuitív tényt fogalmazza meg az alábbi, úgynevezett Church-Turing-tézis.

| A parciálisan rekurzív függvények azonosak a kiszámítható függvényekkel. |
|---|

Vegyük észre, hogy ez nem precíz matematikai állítás. De azzá válik, ha konkrét definíciót adunk a „kiszámítható függvény" fogalmára, például valamilyen programnyelven programozható függvényét. A továbbiakban ezt az ekvivalenciát (a Church-Turing tézist) ki fogjuk használni, sőt vissza fogunk élni vele, mert bizonyos esetekben úgy érvelünk parciálisan rekurzív függvényekre vonatkozó állítások igazolásakor, hogy átgondoljuk a megfelelő állítást kiszámítható függvényekre. Ezek szigorú értelemben véve nem jó bizonyítások.

Van univerzális parciálisan rekurzív függvény.

**Tétel.** *Van olyan $\varphi(x, y)$ parciálisan rekurzív függvény, hogy minden $g(y)$ (tehát egyváltozós) parciálisan rekurzív függvényhez létezik olyan $e$ index, hogy $\varphi(e, y) = g(y)$ minden $y$-ra, azaz vagy egyik sincs definiálva, vagy mindkettő és egyenlőek.*

**Bizonyítás.** Legyen $x$ egy program valamilyen módszerrel nyert kódja, $\varphi(x, y)$ pedig az outputja az $x$-szel kódolt program eredményének, ha $y$ inputtal futatjuk. □

**Tétel.** *Nincs univerzális rekurzív függvény, tehát olyan kétváltozós $\varphi(x, y)$ rekurzív függvény, hogy minden egyváltozós $f(y)$ rekurzív függvényhez van olyan $e$ természetes szám, hogy $\varphi(e, y) = f(y)$ áll fenn minden $y$ természetes számra.*

**Bizonyítás.** Tegyük fel, hogy $\varphi(x, y)$ rekurzív. Ekkor $f(x) = \varphi(x, x) + 1$ is az. De ehhez nyilván nincs olyan $e$, hogy $\varphi(e, x) = f(x)$ minden $x$-re (tehát $x = e$-re is). □

# 12 Rekurzív és rekurzívan felsorolható halmazok

**Definíció.** Az $A \subseteq \mathbf{N}$ halmaz *rekurzív*, ha karakterisztikus függvénye, tehát

$$\chi_A(x) = \begin{cases} 1, & \text{ha } x \in A, \\ 0, & \text{ha } x \notin A \end{cases}$$

rekurzív.

**Definíció.** Az $A \subseteq \mathbf{N}$ halmaz *rekurzíven felsorolható*, ha egy parciálisan rekurzív függvény értékkészlete.

**1. Állítás.** *Minden rekurzív halmaz rekurzíven felsorolható.*

**Bizonyítás.** Legyen tehát $A$ rekurzív, azaz $\chi_A(x)$ rekurzív. Olyan parciálisan rekurzív $f(x)$ függvényt szeretnénk készíteni, amelyre

$$f(x) = \begin{cases} x, & \text{ha } x \in A, \\ \text{nem def.}, & \text{ha } x \notin A, \end{cases}$$

ez nyilván jó lesz. Ehhez vegyük

$$\begin{aligned} f(x) &= \mu y\big[(x = y) \wedge (\chi_A(x) = 1)\big] \\ &= \mu y\big[|x - y| + |\chi_A(x) - 1| = 0\big] \end{aligned}$$

-t.

**2. Állítás.** *Ha $A$, $B$ rekurzív halmazok, akkor $A \cap B$, $A \cup B$ és $\mathbf{N} - A$ is az.*

**Bizonyítás.** $\chi_{A\cap B}(x) = \chi_A(x)\chi_B(x)$. $\chi_{A\cup B}(x) = \mathrm{sg}\big(\chi_A(x) + \chi_B(x)\big)$. $\chi_{\mathbf{N}-A}(x) = 1 \dot{-} \chi_A(x)$.

**3. Állítás.** *Parciálisan rekurzív függvény értelmezési tartománya rekurzíven felsorolható, és megfordítva, minden rekurzíven felsorolható halmaz előáll, mint egy parciálisan rekurzív függvény értelmezési tartománya.*

**Bizonyítás.** Ha $f$ értelmezési tartománya $A$, legyen

$$g(x) = \mu y\big[(y = x) \text{ és } \big(f(x) = f(x)\big)\big].$$

**4. Állítás.** *Ha $A$ és $\mathbf{N} - A$ is rekurzíven felsorolható, akkor akkor $A$ (és persze $\mathbf{N} - A$ is) rekurzív.*

**Bizonyítás.** Az előző Állítás módszerével csinálunk olyan, végtelenségig dolgozó $P$ és $Q$ programokat, hogy $P$ $A$, $Q$ pedig $\mathbf{N} - A$ elemeit adja ki outputként. $x \in A$ eldöntéséhez csak meg kell várni, amíg $x$ megjelenik valamelyik sorozatban.

**5. Állítás.** *Ha $A$ és $B$ rekurzíven felsorolható, akkor $A \cup B$ és $A \cap B$ is.*

**Bizonyítás.**

**6. Állítás.** *Van rekurzíven felsorolható halmaz, amely nem rekurzív.*

**Bizonyítás.** Legyen $K = \{x : \varphi(x,x) \text{ értelmezett}\}$, ahol $\varphi$ az univerzális parciálisan rekurzív függvény. $K$ parciálisan rekurzív függvény értelmezési tartománya, tehát rekurzíven felsorolható. Ha $K$ rekurzív, akkor

$$f(x) = \begin{cases} \varphi(x,x)+1, & \text{ha } x \in K \\ 0, & \text{ha } x \notin K \end{cases}$$

rekurzív függvény. Ezért van $e$, hogy $f(x) = \varphi(e,x)$ teljesül minden $x$-re. Ha $x = e$-t helyettesítünk, akkor nyilván $e \in K$, így $\varphi(e,e) = \varphi(e,e)+1$, ami lehetetlen. □

Mivel $\varphi(x,y)$ definíciója az volt, hogy az $x$-szel kódolt program outputja az $y$ input melett, eredményünk azt mondja, hogy nincs algoritmus, amely minden algoritmusról eldöntené, végetér-e adott input mellett. Az ilyen algoritmus keresése volt a programozás elméletének nevezetes *megállási problémája.*

| Nincs olyan program, amely minden programról eldöntené, hogy befejeződik-e. |
|---|

**7. Állítás.** *Ha $A \neq \emptyset$ rekurzíven felsorolható halmaz, akkor egy rekurzív (tehát totális) függvény értékkészlete.*

**Bizonyítás.** legyen $A$ az $f$ parciálisan rekurzív függvény értékészlete, legyen $a \in A$ tetszőleges elem. $g(x)$-et úgy definiáljuk, hogy $f\big(\alpha(x)\big)$-szel egyenlő, ha ez legfeljebb $\beta(x)$ lépésben kiszámítható, különben legyen $g(x) = a$ (itt $\alpha(x)$ és $\beta(x)$ a Fibonacci sorozat tárgyalásában használt kódolófüggvények).

**8. Állítás.** *Szigorúan monoton növő rekurzív függvény értékkészlete is rekurzív.*

**Bizonyítás.** Készítsük el $f(0), f(1), \ldots$-t. Anak eldöntéséhez, hogy $n$ benne van-e $f$ értékkészletében, elég legfeljebb $f(n)$-et kiszámolni.

**9. Állítás.** *Végtelen rekurzíven felsorolható halmaz tartalmaz végtelen rekurzív részhalmazt.*

**Bizonyítás.** Tegyük fel, hogy $f$ értékkészlete az $A$ végtelen halmaz. Legyen $a_0$ a legkisebb $a$, hogy $f\big(\alpha(a)\big)$ legfeljebb $\beta(a)$ lépésben kiszámítható, $g(0) = f\big(\alpha(a_0)\big) = b_0$. Legyen $a_1 > a_0$ a legkisebb $a > a_0$, amelyre $f\big(\alpha(a)\big) > b_0$ és ez legfeljebb $\beta(a)$ lépésben kiszámítható. Legyen $g(1) = f\big(\alpha(a_1)\big) = b_1$. Az így definiált $g$ szigorúan monoton rekurzív függvény, értékkészlete $B = \{b_0, b_1, \ldots\} \subseteq A$, rekurzív.

**10. Állítás.** *Van olyan $L$ rekurzíven felsorolható halmaz, hogy minden $A$ rekurzíven felsorolható halmazhoz van van $f$ rekurzív függvény, hogy $x \in A$ akkor és csak akkor, ha $f(x) \in L$.*

**Bizonyítás.** Legyen $L = \{x : \varphi(\alpha(x), \beta(x)) \text{ értelmes}\}$. Ha $A$ rekurzíven felsorolható, akkor a 3. Állítás szerint van $g$ parciálisan rekurzív függvény, hogy $g$ értelmezési tartománya $A$. Van olyan $e$ természetes szám, hogy $g(x) = \varphi(e, x)$ minden $x$-re. Ezért $A = \{x : \varphi(e, x) \text{ értelmes}\}$. Így vehetjük $f(x) = 2^e(2x + 1)$-et.

# 13 Kódolás, Gödel-számozás

Ebben a fejezetben *rendkívül vázlatosan* ismertetjük a Gödel-számozást, tehát azt az eljárást, amellyel a logika fogalmai aritmetikai fogalmakká fordíthatók.

**Definíció.** Egy, a természetes számokon értelmezett, $R$ $n$-változós reláció *rekurzív* , ha

$$f(x_1, \ldots, x_n) = \begin{cases} 1, & \text{ha } R(x_1, \ldots, x_n) \text{ fennáll,} \\ 0, & \text{ha nem áll fenn.} \end{cases}$$

karakterisztikus függvénye rekurzív.

Definiáljuk az összes természetes számokból álló számsorozatokon értelmezett $F$ függvényt a következőképpen. $F(x_1, \ldots, x_n) = 2^{x_1}3^{x_2} \cdots p_n^{x_n+1}$, ahol $p_n$ az $n$-edik prímszám. Ez az összes sorozatokat kódolja természetes számokká, mégpedig úgy, hogy a kódból azt is „visszaolvashatjuk", milyen hosszú sorozatból indultunk ki. Itt nem mondhatjuk el, hogy $F$ rekurzív lenne, hiszen nincsen változószáma sem, de azt mondhatjuk, hogy „attól eltekintve" az (nyilván könnyű egyszerű programot írni a kiszámítására és az inverzei kiszámítására).

**Gödel-számozás.** Az adott $L$ első rendű nyelv minden jelének egy természetes számot feleltetünk meg, a következő módon. Tegyük fel, hogy a nyelv (összes) jelei $v_i$, $c_i$, $f_i$, $R_i$, $\neg$, $\vee$, $\exists$, , , ( , ) . Legyen $\alpha(v_i) = 6 + 4i$, $\alpha(c_i) = 7 + 4i$, $\alpha(f_i) = 8 + 4i$, $\alpha(R_i) = 9 + 4i$, $\alpha(\neg) = 0$, $\alpha(\vee) = 1$, $\alpha(\exists) = 2$, $\alpha(,) = 3$, $\alpha(() = 4$, $\alpha()) = 5$. Ezek $L$ jeleinek *Gödel-számai*.

**Definíció.** Ha az $a_1, \ldots, a_t$ jelek Gödel-számai rendre $g_1, \ldots, g_t$, akkor az $a_1a_2 \cdots a_t$ sorozat Gödel-száma legyen $F(g_1, \ldots, g_t)$.

Így a Peano-axiómarendszer nyelvének $0 = 0$ formulája a 984150000000 Gödel-számot kapja, annak $\neg(0 = 0)$ tagadása pedig a következőt:

$$2401963033686297101434476562 5.$$

Ugyanilyen módon jelsorozatok sorozataihoz is Gödel-számokat rendelünk.

Jelölje Vált($x$) azt az (egyváltozós) relációt, hogy $x$ egy változójel Gödel-száma.

**1. Állítás.** Vált($x$) *rekurzív reláció.*

**Bizonyítás.** Vált$(x)$ akkor és csak akkor teljesül, ha $x \geq 6$ és $4|x-6$, ami könnyen láthatóan rekurzív. □

Jelölje Függv$(x)$ azt az (egyváltozós) relációt, hogy $x$ egy változójel Gödel-száma.

**2. Állítás.** Függv$(x)$ *rekurzív reláció.*

**Bizonyítás.** Hasonlóan. □

Hasonlóan látható, hogy rekurzívak a következő relációk: Kif$(x)$: $x$ egy kifejezés Gödel-száma, Form$(x)$: $x$ egy formula Gödel-száma, Szabad$(x,y)$: $x$ egy formula Gödel-száma és $y$ egy benne levő szabad változó Gödel-száma, Logax$(x)$: $x$ egy logikai axióma Gödel-száma, MP$(x,y,z)$ $z$ egy olyan formula Gödel-száma, amely modus ponens-szel keletkezett az $x$ és az $y$ Gödel-számú formulákból, GEN$(x,y)$ ugyanez generalizációra. Ax$(x)$: $x$ a Peano-axiómarendszer egyik axiómájának Gödel-száma, Lev$(x,y)$: $x$ egy levezetés (tehát egy sorozat) Gödel-száma, $y$ a végformulájáé. Utolsó relációnk Tétel$(x)$: $\exists y$Lev$(y,x)$. Ez általában nem lesz rekurzív, csak rekurzívan felsorolható. Érdemes megjegyeznünk, hogy például a Peano-axiómarendszer akkor és csak akkor ellentmondásos, ha a fent említett parciálisan rekurzív függvény felveszi a föntebb kiszámolt óriás számértéket, 2401963033686297101434476562 5-et. Hasonló állítás igaz a halmazelmélet axiómarendszerére.

# 14 A reprezentációs tétel

**A reprezentációs tétel.** *Ha $f(x_1,\ldots,x_n)$ parciálisan rekurzív függvény, akkor van a Peano-axiómarendszer nyelvén olyan $\varphi(x_1,\ldots,x_n,y)$ formula, hogy*

**(1)** *ha $f(a_1,\ldots,a_n)=b$, akkor a természetes számok modelljén $\varphi(a_1,\ldots,a_n,b)$ teljesül;*

**(2)** *PA-ból levezethető, hogy minden $x_1,\ldots,x_n$ esetén legfeljebb egy $y$ van, amelyre $\varphi(x_1,\ldots,x_n,y)$ fennáll.*

Könnyű a tételre példákat mondani: ha $f(x)$ a $\sqrt{x}$ parciális függvény, akkor $\varphi(x,y)$ lehet például $x=y^2$. Általában is, $\varphi$ úgy keletkezik, hogy „kiolvassuk" $f$ konstrukcióját.

**Bizonyítás.** $f$ felépítése szerint haladó indukcióval.
Ha $f(x)=0(x)$, akkor $\varphi(x,y)$-nak vehetjük $y=0$-t.
Ha $f(x)=S(x)$, akkor $\varphi(x,y)$-nak vehetjük $y=S(x)$-et.
Ha $f=I_m^n$, legyen formulánk $y=x_n$.
Ha $f$ kompozícióval áll elő,

$$f(x_1,\ldots,x_n)=g\big(h_1(x_1,\ldots,x_n),\ldots,h_m(x_1,\ldots,x_n)\big)$$

és $g$-t reprezentálja a $\theta$ formula, $h_1, \ldots, h_m$-et pedig rendre a $\psi_1, \ldots, \psi_m$ formula, akkor válasszuk az $f$-et reprezentáló $\varphi$ formulának a következőt:

$$\exists z_1 \cdots \exists z_m \big[\psi_1(x_1, \ldots, x_n, z_1) \wedge \cdots \wedge \psi_m(x_1, \ldots, x_n, z_m) \wedge \theta(z_1, \ldots, z_m, y)\big].$$

Ha most $f(a_1, \ldots, a_n) = b$, akkor van $b_1, \ldots, b_m$, hogy $h_i(a_1, \ldots, a_n) = b_i$ $(1 \leq i \leq m)$ és $g(b_1, \ldots, b_m) = b$ így $\varphi(a_1, \ldots, a_n, b)$ igaz. Másrészt,ha $\varphi(x_1, \ldots, x_n, y_1)$ és $\varphi(x_1, \ldots, x_n, y_2)$ is fennáll, akkor az adódik, hogy $\exists z_1 \cdots \exists z_m \big[\theta(z_1, \ldots, z_m, y_1) \wedge \theta(z_1, \ldots, z_m, y_2)\big]$ és így $y_1 = y_2$.

Végül, ha $f$ minimalizációval adódik:

$$f(x_1, \ldots, x_n) = \mu y[g(x_1, \ldots, x_n, y) = 0]$$

és $g$-t reprezentálja a $\psi$ formula, akkor $\varphi(x_1, \ldots, x_n, y)$ legyen

$$\psi(x_1, \ldots, x_n, y, 0) \wedge (\forall z < y)(\exists t \neq 0)\psi(x_1, \ldots, x_n, z, t).$$

Annak igazolásához hogy ez valóban jó, legyen először $f(a_1, \ldots, a_n) = b$. Ekkor $g(a_1, \ldots, a_n, b) = 0$ így $\psi(a_1, \ldots, a_n, b, 0)$ igaz és a formula másik része is könnyen láthatóan igaz. Ha pedig $\varphi(x_1, \ldots, x_n, y_1)$ és $\varphi(x_1, \ldots, x_n, y_2)$ továbbá $y_1 < y_2$, akkor kiolvasva a formulát $\psi(x_1, \ldots, x_n, y_1, 0)$ teljesül és $\exists t \neq 0 \psi(x_1, \ldots, x_n, y_1, t)$ is, ami lehetetlen. □

**Következmény.** *Ha $R(x_1, \ldots, x_n)$ rekurzív reláció, akkor van olyan Peano-beli $\varphi(x_1, \ldots, x_n)$ formula, hogy tetszőleges $a_1, \ldots, a_n$ természetes számok esetén*
*ha $R(a_1, \ldots, a_n)$ fennáll, akkor $\varphi(a_1, \ldots, a_n)$ igaz;*
*ha $R(a_1, \ldots, a_n)$ nem áll fenn, akkor $\varphi(a_1, \ldots, a_n)$ nem igaz.*

**Bizonyítás.** $R$ rekurzív, így van olyan $f$ rekurzív függvény, hogy $f(x_1, \ldots, x_n) = 1$ akkor és csak akkor ha $R(x_1, \ldots, x_n)$ fennáll. Ha $\psi$ reprezentálja $f$-et, akkor legyen $\varphi$ a következő: $\psi(x_1, \ldots, x_n, \overline{1})$. □

# 15 A nem-teljességi tétel

Kéne egy tolmács, hogy megmondja
neki, kell egy tolmács.
(A végső visszaszámlálás)

**Gödel nem-teljességi tétele.** *Ha a Peano-axiómarendszer ellentmondásmentes, akkor van olyan zárt formula, amely nem levezethető és nem is cáfolható.*

**Bizonyítás.** Legyen $w(u, y)$ a következő reláció: $u$ a legfeljebb egy szabad változót (ezt jelöljük $x$-szel) tartalmazó $\varphi(x)$ formula Gödel-száma és $y$ $\varphi(\overline{u})$ egy levezetésének Gödel-száma. $w(u, y)$ rekurzív reláció, így a reprezentációs tétel következménye segítségével találhatunk olyan $\Psi(u, y)$ formulát, amely azt reprezentálja. Legyen $\theta(u)$ a következő formula: $\forall y \neg \Psi(u, y)$. Ennek egy szabad változója van: $u$. Tegyük fel, hogy Gödel-száma $g$. Nézzük $\theta(\overline{g})$-t! Ha a Peano-axiómarendszer ellentmondásmentes, akkor $\theta(\overline{g})$ és $\neg\theta(\overline{g})$ közül csak az egyik

lehet levezethető, és persze annak kell igaznak lennie a természetes számok modelljén.

Tegyük fel először, hogy $\theta(\overline{g})$ igaz. Ekkor tehát $\forall y \neg \Psi(g, y)$, azaz semmilyen $y$ nem kódolja $\theta(\overline{g})$ egy levezetését, az tehát nem levezethető.

Tegyük fel végül, hogy $\neg\theta(\overline{g})$ igaz. Ekkor van olyan $y$ természetes szám, amire $\Psi(g, y)$ igaz, tehát $w(g, y)$ igaz, tehát $y$ $\theta(\overline{g})$ egy levezetését kódolja, ami ellentmondás. □

Gödel valójában általánosabban mondta ki és bizonyította tételét. Az okoskodás végigvihető a Peano-axiómarendszer helyett bármilyen elsőrendű nyelv bármilyen axiómarendszerével, feltéve, hogy az ellentmondásmentes, az axiómák Gödel-számai rekurzíven felsorolható halmazt alkotnak (azaz, az axiómarendszer „elegendően szabályos"), és a rendszerben felépíthető a számelmélet (azaz a rendszer „eléggé kifejező"). Ilyen rendszer például a Peano-axiómarendszer bármely véges bővítése, a halmazelmélet axiómarendszere, vagy annak bármely véges bővítése. Tehát a nemteljességi tétel azt is kimondja, hogy ha a halmazelmélet axiómarendszeréhez hozzávesszük a kontinuumhipotézist, és akárhány további állítást, mindig marad eldönthetetlen probléma, legalábbis, amíg rendszerünk ellentmondásmentes marad.

Hadd idézzem ide Péter Rózsa szuggesztív leírását Gödel tételéről.

> És amint Gödel az ilyen kétértelmű jelsorozatokkal és a nekik megfelelő számokkal játszadozott, rábukkant egy számra – mondjuk, hogy ez 8 milliárd; valójában pontosan tudjuk, hogyan épül fel törzstényezőkből, de a kiszámításához egy emberélet sem volna elég – és észrevette, hogy ez a következőket tudja: Ha az előbb tárgyalt mondat mintájára a rendszer jeleivel írjuk fel ezt a metamatematikai állítást:
>
> *„A 8 milliárdnak megfelelő formula nem bizonyítható be a rendszerben"*
>
> – és megnézzük, hogy az így nyert formulának a szótár szerint milyen szám felel meg, ámulva fogjuk tapasztalni, hogy éppen 8 milliárd. Tehát a „8 milliárdnak megfelelő formula": maga ez a formula. Így ő kereken ezt mondja ki az egyik értelmével:
>
> *„Én magam nem vagyok bizonyítható."*

# 16 Diofantoszi halmazok

**Definíció.** Az $A \subseteq \mathbf{N}$ halmaz *diofantoszi*, ha van olyan egészegyütthatós $p(x_1, \ldots, x_n, y)$ polinom, hogy

$$A = \{y \in \mathbf{N} : \text{ van } x_1, \ldots, x_n \in \mathbf{N}, \text{ hogy } p(x_1, \ldots, x_n, y) = 0\}.$$

Könnyen látható, hogy például a páros számok halmaza, vagy a négyzetszámoké, diofantoszi. További ilyen példa a 2-hatványok halmazának komplementere, vagy például a Fibonacci-számok halmaza (felhasználva, hogy $x$ Fibonacci-szám akkor és csak akkor, ha $x^2 - xy - y^2 = \pm 1$ megoldható).

Minden diofantoszi halmaz parciálisan rekurzív függvény értékkészlete, tehát rekurzívan felsorolható. A huszadik század matematikájának egyik leglátványosabb eredménye, hogy ez megfordítható.

**Tétel.** (M. Davis, J. Robinson, H. Putnam, J. Matyijaszevics) *Minden rekurzíven felsorolható halmaz diofantoszi.*

**Következmény.** *Nincs olyan algoritmus, amely minden diofantoszi egyenletről eldöntené, hogy megoldható-e.*

**Bizonyítás.** Alkalmazzuk az előző tételt olyan rekurzíven felsorolható halmazra, amely nem rekurzív.

**Következmény.** Minden $A \subseteq \mathbf{N}$ rekurzíven felsorolható halmazhoz létezik olyan egész együtthatós $q(x_1, \ldots, x_n)$ polinom, amelynek az értékkészletének $\mathbf{N}$-be eső része $A$.

**Bizonyítás.** Ha

$$A = \big\{y \in \mathbf{N} : p(x_1, \ldots, x_n, y) = 0 \text{ megoldható}\big\},$$

akkor $A$ a $q$ polinom értékkészletének $\mathbf{N}$-be eső része, ahol $q\big(x_1, \ldots, x_n, y\big) = \big(y+1\big)\big(1 - p^2(x_1, \ldots, x_n, y)\big) - 1$.

Így a fentiek alapján a Fibonacci számok halmaza is megadható, mint egy polinom értékkészletének $\mathbf{N}$-be eső része. Hasonló példa a prímszámok halmazára is adható (prímképlet!): a $(k+2)\{1 - [wz + h + j - q]^2 - [(gk + 2g + k + 1)(h + j) + h - z]^2 - [2n + p + q + z - e]^2 - [16(k+1)^3(k+2)(n+1)^2 + 1 - f^2]^2 - [e^3(e+2)(a+1)^2 + 1 - o^2]^2 - [(a^2-1)y^2 + 1 - x^2]^2 - [16r^2y^2(a^2-1) + 1 - u^2]^2 - [((a + u^2(u^2-a))^2 - 1)(n + 4dy)^2 + 1 - (x + cu)^2]^2 - [u + l + v - y]^2 - [(a^2-1)l^2 + 1 - m^2]^2 - [ai + k + 1 - l - i]^2 - [p + l(a - n - 1) + b(2ap + 2a - p^2 - 2p - 2) - x]^2 - [z + pl(a-p) + t(2ap - p^2 - 1) - pm]^2\}$ polinom nemnegatív értékeinek halmaza éppen a prímszámok.

Egy másik, még érdekesebb következmény, hogy van olyan többváltozós, egész együtthatós polinom (és konkrétan meg is adható), amely akkor és csak akkor veszi fel a 0 értéket, ha ellentmondás van a Peano-axiómarendszerben. Hasonló állítás igaz a halmazelmélet axiómarendszerére (másik polinommal).

**Feladatok. 1.** Lássuk be, hogy a páros számok halmaza diofantoszi !

**2.** Lássuk be, hogy a kettőhatványok halmazának komplementere diofantoszi !

**3.** Lássuk be, hogy a Fibonacci számok halmaza diofantoszi !

**4.** Tegyük fel, hogy $A, B \subseteq \mathbf{N}$ diofantoszi. Lássuk be, hogy $A \cup B$, $A \cap B$ is diofantoszi !

# 17 Matematikusok

**Ackermann, Friedrich Wilhelm** (1896 – 1962 )
**Church, Alonzo** (1903 – 1995 )
**Gödel, Kurt** (1906 – 1978)
**Hilbert, David** (1862 – 1943)
**Kalmár László** (1905 – 1976 )
**Neumann János** (1903 – 1957 )
**Peano, Giuseppe** (1858 – 1932)
**Péter Rózsa** (1905 – 1977)
**Tarski, Alfred** (1901 – 1983)
**Turing, Alan Mathison** (1912 – 1954 )

# 18 Irodalomjegyzék


- Csirmaz László–Hajnal András: *Matematikai logika,* egyetemi jegyzet, ELTE, 1994.
- D. R. Hofstadter: *Gödel, Escher, Bach, Egybefont Gondolatok Birodalma*, TypoTEX, 1998.
- L. A. Lavrov–L. L. Makszimova: *Halmazelméleti, matematikai logikai és algoritmuselméleti feladatok,* Műszaki Könyvkiadó, Budapest, 1987.
- Péter Rózsa: *Játék a végtelennel*, TypoTEX , Budapest, 1999.
- Dennis Shasha: *Dr. Eco talányos kalandjai*, TypoTEX , Budapest, 1999.
- R. Smullyan: *Mi a címe ennek a könyvnek?*, TypoTEX , Budapest, 1996.
- R. Smullyan: *A hölgy vagy a tigris?*, második kiadás, TypoTEX , Budapest, 1996.
- R. Smullyan: *Seherezáde rejtélye*, TypoTEX , Budapest, 1999.
- Szendrei János–Tóth Balázs: Bevezetés a matematikai logikába, Nemzeti Tankönyvkiadó, Budapest, 1996.
- Urbán János: *Matematikai logika (példatár),* Műszaki Könyvkiadó, Budapest, 1983, 1999.

# Tartalomjegyzék