AZ ÚN. MEGOLDHATATLAN MATEMATIKAI PROBLÉMÁKRA VONATKOZÓ KUTATÁSOK ALAPJÁUL SZOLGÁLÓ CHURCH-FÉLE HIPOTÉZISRŐL

KALMÁR LÁSZLÓ lev. tag

(A Magyar Tudományos Akadémia 1956. évi Nagygyűléséhez kapcsolódó osztályülésen, május 31-én, elhangzott előadás*)

1. GÖDEL [1] és CHURCH [1] ma már klasszikusnak tekinthető publikációja óta számos matematikai logikai dolgozat foglalkozik ún. megoldhatatlan matematikai problémák szerkesztésével. Minthogy a szakirodalomban egyesek olyan filozófiai következtetéseket vontak le az ilyen problémák létezéséből, amelyek legalább is súrolják az agnoszticizmus határát (lásd pl. POST [1], WEDBERG [1]), ezért szükségesnek látszik megvizsgálni, milyen értelemben megoldhatatlanok a szóban forgó problémák és mennyiben érinti ilyen problémák létezése a világ és törvényszerűségei megismerhetőségének kérdését.

2. GÖDEL említett dolgozatában, valamint a hozzá kapcsolódó kutatásokban a következőről van szó. Adva van egy A axiómarendszer, amely azoknak a módszereknek rögzítésére szolgál, amelyeket bizonyos típusú problémák megoldására felhasználunk. Maguk a szóban forgó problémák a következő alakúak. Adva van egy T ítélet, amely az A axiómarendszer alapfogalmai, továbbá a logikai fogalmak segítségével megfogalmazható; és azt kérdezzük, igaz-e a T ítélet, vagy nem. (Logikai fogalmakon itt a logikai ítéletkalkulusnak az „és", „vagy", „ha ... akkor ...", „... akkor és csak akkor, ha ...", „nem" szavaknak megfelelő műveleteit, a „van oly ..., amelyre ..." „minden ...-re ..." szavaknak megfelelő ún. kvantorokat, valamint az egyenlőségrelációt értjük.) Az A axiómarendszer helyességében olyan értelemben megbízunk, hogy a szóban forgó problémát megoldottnak tekintjük, ha akár a T ítéletet, akár kontradiktórius tagadását, a $\bar{T}$ ítéletet, sikerül bebizonyítani az A axiómarendszer axiómáiból kiindulva, az A axiómarendszerben megengedett következtetésmódok véges számú alkalmazásával; az első esetben azt mondjuk, hogy a probléma megoldása az, hogy a T ítélet igaz, a második esetben az, hogy a T ítélet hamis. (Az A axiómarendszer helyességében való bizalom azt a feltételezést is magában foglalja, hogy e két eset egyidejűleg semmiféle T ítélet esetén nem következhetik be, vagyis, hogy az A axiómarendszer ellentmondástalan.) Ha egy ilyen természetű probléma ebben az értelemben nem

* A Magyar Tudományos Akadémia illetékes szervei az előadást téves intézkedés folytán a következő címen hirdették meg: „Matematikai problémák eldönthetőségének fogalmáról"; ez a cím azonban nem felel meg az előadás tárgyának.

oldható meg, vagyis ha sem a T, sem a $\overline{T}$ ítélet nem bizonyítható be az A axiómarendszerben, az semmiféle agnoszticista következtetésre nem jogosít, hiszen nem azt mutatja, hogy egyáltalában nem tudjuk eldönteni, igaz-e a T ítélet, hanem csak azt, hogy ennek eldöntésére nem alkalmas az A axiómarendszer; ez pedig nem „tudásunk határának" létezését, hanem csak az A axiómarendszer egy bizonyos fogyatékosságát, ti. nem teljes, pontosabban: nem kategorikus voltát mutatja.

Abból a tényből, hogy valamely A axiómarendszer nem kategorikus, vagyis, hogy van olyan, A alapfogalmai és a logikai fogalmak segítségével megfogalmazható T ítélet, hogy sem T, sem $\overline{T}$ nem bizonyítható be az A axiómarendszerben, csak az vonhat le agnoszticista következtetéseket, aki ragaszkodik az *abszolút axiómarendszer* koncepciójához, mégpedig A-t ilyen axiómarendszernek tartja. Ez a koncepció abban a véleményben áll, hogy van olyan axiómarendszer, amelyen belül minden helyes matematikai meggondolás elvégezhető. Ez a vélemény közel áll a mechanisztikus materializmus azon feltételezéséhez, hogy van olyan differenciálegyenlet, amelynek alapján, megfelelő kezdeti feltételek ismerete esetén minden, a valóságra vonatkozó kérdésre választ lehet adni, tehát a világ kimerítő megismerése rögzíthető módszerek keretein belül lehetséges. Másrészt, a matematikai megismerésre korlátozva, RUSSELL és WHITEHEAD logicista iskolája hirdetett ilyen véleményt. A logicisták szerint a halmazelmélet antinómiái a circulus vitiosushoz hasonló logikai hibák következményei. Hogy ilyen hibák elkövetését meggátolják, a matematikai logika eszközei segítségével igyekeztek pontosan megfogalmazni a megengedett logikai lépéseket. Véleményük szerint az így előálló, matematikai logikai jellegű axiómarendszerben, amely azonban tartalmaz néhány nem-logikai axiómát is, minden helyes matematikai meggondolás elvégezhető; ami nem végezhető el, azt eleve hibásnak ítélik. E vélemény alátámasztására *Principia Mathematica* című háromkötetes könyvükben (WHITEHEAD—RUSSELL [1]) a matematika addig ismert fejezetei legfontosabb tételeit felírják a matematikai logika jeleivel és bizonyításukat is megadják, vagy legalábbis vázolják, az említett axiómarendszerből kiindulva.

GÖDEL [1] azonban éppen a *Principia Mathematica* axiómarendszeréről mutatta meg, hogy van olyan, ráadásul elemi aritmetikai, T ítélet, hogy sem T, sem $\overline{T}$ nem bizonyítható be a kérdéses axiómarendszerben. Aki elfogadja azt a hipotézist, hogy a *Principia Mathematica* axiómarendszere a fenti értelemben abszolút matematikai axiómarendszer, az ebből azt a következtetést vonja le, hogy az a probléma, igaz-e a T ítélet, vagy nem, semmiféle helyes matematikai módszerrel nem dönthető el.

GÖDEL azonban ugyanakkor megadott olyan axiómarendszert, amelyben ez a probléma mégis csak eldönthető, ráadásul olyat, amelynek minden axió-

máját el kell, hogy fogadják azok, akik megbíznak a *Principia Mathematica* axiómarendszerében. Ez az axiómarendszer ugyanis egyetlen egy axióma hozzávételében különbözik a *Principia Mathematica* axiómarendszerétől, s ez az egy axióma azt mondja ki, hogy a *Principia Mathematica* eredeti axiómarendszere ellentmondástalan; márpedig ezt az axiómát el kell, hogy fogadják azok, akik megbíztak a *Principia Mathematica* axiómarendszerében. Így GÖDEL eredménye azt mutatja, hogy a *Principia Mathematica* axiómarendszere sem kategorikus, egyben azonban azt is, hogy az a hipotézis, hogy ez az axiómarendszer a matematika abszolút axiómarendszere, tarthatatlan. Ezzel azonban elesett az az alap, amelyen agnoszticista következtetéseket lehetne levonni GÖDEL eredményéből.

Az abszolút matematikai axiómarendszer „babéraira" GÖDEL eredményei előtt a halmazelmélet ZERMELO—FRAENKEL-féle axiómarendszere (lásd pl. FRAENKEL [1]) is pályázhatott azon az alapon, hogy a matematika jelenleg ismeretes fejezetei felépíthetők a halmazelmélet speciális ágaiként. GÖDEL említett dolgozatában épp ezért megjegyzi, hogy eredményei szószerint átvihetők a ZERMELO—FRAENKEL-féle axiómarendszerre is; ezért ez sem tekinthető a matematika abszolút axiómarendszerének.

Azonban GÖDEL eredményeinek jelentősége még ennél is nagyobb. Ugyanis meggondolásai bármely olyan A axiómarendszerrel kapcsolatban elvégezhetők, amely bizonyos, nagyon általános, feltételeknek eleget tesz. E feltételek háromféle követelményt állítanak az A axiómarendszer elé. Röviden így lehet nevezni ezeket a követelményeket: az axiómarendszer 1. eléggé kifejező, 2. eléggé szabályos, 3. eléggé ellentmondástalan legyen. GÖDEL tétele — általános alakjában — azt mondja ki, hogy minden, e követelményeknek eleget tevő A axiómarendszerhez van olyan, ezen axiómarendszer alapfogalmai és a logikai fogalmak segítségével megfogalmazható $T = T(A)$ ítélet, hogy sem T, sem $\overline{T}$ nem bizonyítható be az A axiómarendszerben. Maguknak az 1—3. követelményeknek pontos alakja attól függ, hogyan bizonyítjuk be a GÖDEL-tételt. Az 1. követelmény azt kívánja, hogy bizonyos alakú aritmetikai ítéletek megfogalmazhatók legyenek az A axiómarendszer alapfogalmai és a logikai fogalmak segítségével, továbbá bizonyos alakú aritmetikai és logikai jellegű következtetésmódokat el lehessen végezni az A axiómarendszer axiómái és következtetési szabályai segítségével. A 3. követelmény nemcsak azt kívánja, hogy ne legyen két olyan ítélet, amelyek mindketten bebizonyíthatók az A axiómarendszer axiómái és következtetési szabályai segítségével, és amelyek egymásnak ellentmondanak, amennyiben ugyanis az egyik a másiknak tagadása, hanem ezenfelül azt is, hogy bizonyos alakú végtelen sok ítélet se legyen egyidejűleg bebizonyítható az A axiómarendszerben, amelyek közül kettőkettő, vagy általában véges számú ugyan nem mond egymásnak ellent, de

összességükben ellentmondanak egymásnak: ti. olyan ítéletek, amelyek közül az egyik azt állítja, hogy van olyan nemnegatív egész szám, amelynek megvan egy bizonyos tulajdonsága, a második azt, hogy a 0-nak nincs meg ez a tulajdonsága, a harmadik azt, hogy az 1-nek nincs meg, a következő azt, hogy a 2-nek nincs meg, és így tovább. (Ezt a követelményt az A axiómarendszer ω-ellentmondástalanságának szokás nevezni.) A 2. követelménynek még a hozzávetőleges megfogalmazása is messze vezetne; elég talán annyit mondani róla, hogy triviálisan kielégíti minden olyan axiómarendszer, amelynek véges számú axiómája és következtetési szabálya van, de kielégítik bizonyos „végtelen" axiómarendszerek is. Mindenesetre igaz, hogy minden olyan axiómarendszer kielégíti az 1—3. követelményeket, amelyet eddig a matematikának valamely, legalábbis az aritmetikát magában foglaló fejezetének axiomatizálására használtak vagy javasoltak. Az 1. követelmény olyan keveset kíván, hogy olyan axiómarendszer, amely ezt nem teljesíti, nem tekinthető aritmetikai (vagy a matematika valamely, az aritmetikát is magában foglaló fejezetére vonatkozó) axiómarendszernek; az olyan axiómarendszer, amely a 3. követelményt nem teljesíti, nyilván nem tekinthető helyesnek; az olyan axiómarendszer pedig, amely a 2. követelményt nem teljesíti, teljesen használhatatlan, minthogy vagy azt lehetetlen áttekinteni, mely axiómák tartoznak hozzá, vagy azt, mely következtetésmódok vannak benne megengedve, így semmi sem biztosíthatja, hogy axiómái és következtetési szabályai tartalmilag elfogadhatók.

GÖDEL tétele tehát nemcsak egyes axiómarendszerekről mondja ki, hogy nem kategorikusak, hanem úgyszólván minden használható aritmetikai (vagy a matematika valamely, az aritmetikát is magában foglaló fejezetére vonatkozó) axiómarendszerről; tehát nemcsak egyes axiómarendszerek egy bizonyos fogyatékosságát fedi fel, hanem magának az axiómatikus módszernek egy sajátosságát: azt, hogy egy axiómarendszer felállítása magában rejti ezen axiómarendszer állandó bővítésének kötelezettségét, legalábbis, amennyiben a kérdéses axiómarendszert arra akarjuk használni, hogy sorra valamennyi aritmetikai problémát megoldjunk a segítségével. Sőt, ez a kötelezettség már akkor is fennáll, ha csak bizonyos típusú aritmetikai problémák közül akarjuk valamennyit megoldani az axiómarendszer segítségével. Ugyanis a GÖDEL-tétel bizonyítása, függetlenül az A axiómarendszertől, mindig olyan alakú, az A axiómarendszerben sem be nem bizonyítható, sem meg nem cáfolható T ítélet létezését mutatja, amely azt mondja ki, hogy minden nemnegatív egész számnak megvan egy bizonyos (az A axiómarendszertől függő) tulajdonsága; mégpedig olyan tulajdonsága, hogy bármely numerikusan adott természetes számról az A axiómarendszerben (és általában bármely, az 1. követelménynek eleget tevő axiómarendszerben)

el lehet dönteni, megvan-e a kérdéses tulajdonsága (ha megvan, ezt, ha pedig nincs meg, akkor azt be lehet a kérdéses axiómarendszerben bizonyítani). Ennélfogva már ahhoz is, hogy sorra valamennyi ilyen típusú aritmetikai problémát meg tudjunk oldani axiómatikusan, szükség van az alapul vett axiómarendszer szakadatlan bővítésére.

Hogy az axiómarendszer alkalmas szakadatlan bővítési folyamata valóban segít a GÖDEL-tétel által feltárt nehézségen, azt a következő tény mutatja. A GÖDEL-tétel bizonyítása az általános esetben is ugyanakkor, amikor minden, az 1—3. követelményeknek eleget tevő A axiómarendszerhez megad egy, az A axiómarendszer alapfogalmai és a logikai fogalmak segítségével megfogalmazható, de az A axiómarendszerben sem be nem bizonyítható, sem meg nem cáfolható T — $T(A)$ ítéletet, egyúttal megadja az A axiómarendszer olyan A' bővítését, amelyben ez a T ítélet bebizonyítható. Magában véve ilyen bővítés létezése triviális: elegendő volna magát a T ítéletet új axiómaként hozzávenni az axiómarendszerhez. Azonban a GÖDEL-tétel bizonyítása az A axiómarendszer olyan A' bővítését adja meg, amely tartalmilag elfogadható, amennyiben az A axiómarendszer helyességében megbízunk; ugyanis A' egyetlen egy új axióma hozzávételével keletkezik A-ból és ez az új axióma azt mondja ki, hogy az eredeti A axiómarendszer ellentmondástalan. (Természetesen ehhez a bővített A' axiómarendszerhez a GÖDEL-tétel szerint ismét van olyan $T(A')$ ítélet, amely A'-ben sem bizonyítható be, sem pedig nem cáfolható meg; de viszont létezik olyan még bővebb A'' axiómarendszer is, amelyben ez a $T(A')$ itélet is bebizonyítható, és így tovább.)

Az a meggondolás, amelyet fentebb a *Principia Mathematica* axiómarendszerének speciális esetében alkalmaztunk, mutatja, hogy ennélfogva nemcsak ez az axiómarendszer, de semmiféle más axiómarendszer sem tekinthető a matematika abszolút axiómarendszerének, úgy, hogy épp a GÖDEL-tétel következtében kell elejteni az abszolút axiómarendszer koncepcióját, vagyis azt az alapot, amelyből kiindulva agnoszticista következtetést lehetne levonni a GÖDEL-tételből.

3. Azt, hogy a GÖDEL-tétel még legáltalánosabb alakjában sem jogosít agnoszticitista következtetésekre, ma már a legtöbb matematikai logikus elismeri, hiszen a GÖDEL-tétel csak relatíve (ti. valamely A axiómarendszerre nézve) megoldhatatlan aritmetikai probléma létezését mondja ki. Egészen más a helyzet azonban a CHURCH-tétel esetében, amely, szokásos megfogalmazásában, abszolút-megoldhatatlan aritmetikai probléma létezése bebizonyításának és így a GÖDEL-tétel élesítésének igényével lép fel.

Félreértések elkerülése végett jó lesz eleve leszögezni, hogy a CHURCH-tétel *nem* olyan T aritmetikai ítélet létezését mondja ki, amelyről be lehetne bizonyítani, hogy semmiféle helyes eljárással nem lehet eldönteni, igaz-e vagy

nem. Olyan típusú T ítélet esetén, mint amilyet a GÖDEL-tétel bizonyítása szolgáltat, ez nem is volna lehetséges. Ha ugyanis a T ítélet azt mondja ki, hogy minden nemnegatív egész számnak megvan valamely olyan tulajdonsága, hogy bármely adott nemnegatív egész számról el tudjuk dönteni, megvan-e a kérdéses tulajdonsága, és be lehetne bizonyítani, hogy semmiféle helyes eljárással nem lehet eldönteni, igaz-e a T ítélet, vagy nem, akkor maga ez a bizonyítás azt is bebizonyítaná, hogy minden nemnegatív egész számnak megvan a kérdéses tulajdonsága. Ha ugyanis valamely n nemnegatív egész számnak nem volna meg a kérdéses tulajdonsága, akkor annak (a feltevés szerint lehetséges) eldöntése során, megvan-e az n számnak a kérdéses tulajdonsága, az derülne ki, hogy nincs meg, tehát nem minden nemnegatív egész számnak van meg; vagyis mégis csak eldőlne, hogy igaz-e a T ítélet, vagy nem, ti. az, hogy nem igaz. De akkor meg éppen annak bizonyítása, hogy semmiféle helyes eljárással nem lehet eldönteni, igaz-e a T ítélet, vagy nem, döntené el, hogy igaz-e a T ítélet, vagy nem, ti. bebizonyítaná, hogy T igaz, hiszen minden nemnegatív egész számnak megvan a kérdéses tulajdonsága.

A CHURCH-tételben azonban nem egy T ítéletről van szó, hanem végtelen sokról, mégpedig az ítéletek egy olyan egyparaméteres seregéről, ahol a paraméter megszámlálhatóan végtelen sok $p_0, p_1, p_2, \ldots$ értéket vesz fel; ez a megszámlálás effektív, vagyis bármely p paraméterértékéhez véges számú lépésben meg tudunk határozni olyan nemnegatív egész számot, hogy $p = p_n$, és viszont, bármely adott nemnegatív egész n esetén véges számú lépésben meg lehet határozni a p_n paraméterértéket. A CHURCH-tételben szereplő probléma az, hogy a p paraméter mely értékeire igaz a megfelelő $T = T(p)$ ítélet. Ilyen típusú „egyparaméteres problémasereg" pl. az, hogy a racionális egész együtthatójú egyváltozós polinomok közül melyek reducibilisek a racionális számok testében; vagy hogy melyeknek van pozitív egész zérushelyük; vagy hogy melyeknek lehet meghatározni valamennyi zérushelyét a négy alapművelet és a gyökvonás véges számú alkalmazása segítségével. A felsorolt három problémasereg esetén a paraméter a kérdéses egész együtthatójú egyváltozós polinom; és mindhárom esetben ismeretes olyan eljárás, amelynek segítségével a paraméterként szereplő polinom bármely választása esetén véges számú lépésben meg tudjuk állapítani, igaz-e a megfelelő (a polinom reducibilitását, pozitív egész zérushelyének létezését ill. zérushelyeinek algebrai kiszámíthatóságát kimondó) ítélet: ilyen eljárást az első problémasereg esetén KRONECKER adott meg, a második problémasereg esetén klasszikus eljárásról van szó, a harmadik problémasereg esetén pedig a GALOIS-elmélet szolgáltat ilyen eljárást. A KRONECKER-féle eljárás többváltozós polinomokra is alkalmazható; ezzel szemben többváltozós (racionális egész együtthatós) diofantikus egyenletek esetén ezidőszerint nem ismeretes olyan eljárás, amelynek

segítségével, mihelyt meg van adva a (zérusra redukált) egyenlet baloldala, véges számú lépésben el lehetne dönteni, van-e az egyenletnek pozitív egész számokból álló megoldásrendszere. Nem ismeretes megoldó eljárás e probléma azon speciális esetére sem, hogy a p primszám mely értékeire van olyan pozitív egész x, y és z szám, amelyekre $x^p + y^p = z^p$ (FERMAT-féle probléma); e problémasereg paramétere a p primszám.

Mármost CHURCH tétele szokásos, de mint látni fogjuk, nem egészen helyes fogalmazásában azt mondja ki, hogy van olyan egyparaméteres problémasereg, amely abszolút-megoldhatatlan abban az értelemben, hogy nincs olyan eljárás, amelynek segítségével a paraméter bármely adott értéke esetén véges számú lépésben el lehetne dönteni, mi a válasz a problémaseregnek a kérdéses paraméterértékhez tartozó problémájára. Itt, mint már mondtuk, olyan problémaseregről van szó, amelynek a paramétere megszámlálhatóan végtelen sok, mégpedig effektív $p_0, p_1, p_2, \ldots$ megszámlálással megadott, értéket vesz fel; s a p_n paraméterértékhez tartozó probléma olyan alakú, hogy igaz-e valamely, a GÖDEL-tételben szereplő ítélethez hasonló típusú $T(p_n)$ aritmetikai ítélet, vagy sem.

A CHURCH-tétel e fogalmazásában szerepel valamely problémasereg megoldására alkalmas, bármely adott paraméterértékhez tartozó probléma megoldását véges számú lépésben szolgáltató eljárás fogalma. E fogalomról minden matematikus definíció nélkül is tudja, mit jelent. Pl. amikor fentebb azt mondtuk, hogy van olyan eljárás, amelynek segítségével bármely adott racionális egész együtthatójú egyváltozós polinomról véges számú lépésben el tudjuk dönteni, van-e pozitív egész zérushelye, viszont többváltozós polinomok esetén nem ismeretes ilyen eljárás, mindenki tudta, mit jelent ez.

Könnyen látható, hogy valamely fent vázolt alakú egyparaméteres problémasereghez akkor és csak akkor van olyan eljárás, amelynek segítségével bármely adott p paraméterértékről véges számú lépésben el lehet dönteni, igaz-e a $T(p)$ ítélet, ha van olyan eljárás, amelynek segítségével a problémasereg ún. karakterisztikus függvényének, vagyis a következőképpen definiált χ aritmetikai függvénynek értékét bármely adott helyen véges számú lépésben ki lehet számítani:

$$\chi(n) = \begin{cases} 1, \text{ ha a } T(p_n) \text{ ítélet igaz,} \\ 0, \text{ ha a } T(p_n) \text{ ítélet nem igaz.} \end{cases}$$

Valóban, ha van ilyen „problémamegoldó" eljárás, akkor adott n-hez véges számú lépésben meg tudjuk határozni a p_n paraméterértéket, tehát további véges számú lépésben el tudjuk dönteni, igaz-e a $T(p_n)$ ítélet, vagyis véges számú lépésben ki tudjuk számítani a $\chi(n)$ függvényértéket. Fordítva, ha van ilyen „függvényérték-kiszámító" eljárás, akkor a paraméter adott p értékéhez

véges számú lépésben meg tudunk határozni olyan n nemnegatív egész számot, hogy $p = p_n$, további véges számú lépésben ki tudjuk számítani a $\chi(n)$ függvényértéket, tehát el tudjuk dönteni, igaz-e a $T(p) = T(p_n)$ ítélet. Ennélfogva CHURCH tétele úgy is fogalmazható, hogy van olyan, fent említett alakú, egyparaméteres problémasereg, amelynek karakterisztikus függvényéhez nincs olyan eljárás, amelynek segítségével bármely adott helyen véges számú lépésben ki lehetne számítani a megfelelő függvényértéket.

Az is világos minden matematikus számára, mit értünk ilyen „függvényérték-kiszámító" eljáráson, ill. olyan (egy- vagy többváltozós) aritmetikai függvényen, amelyhez van ilyen eljárás, röviden: „effektíve kiszámítható" függvényen. Pl. a számtan elemeiből ismeretes, hogyan számíthatjuk ki bármely két adott nemnegatív egész szám összegét és szorzatát véges számú lépésben; ennélfogva $x+y$ és xy az x és y változók effektíve kiszámítható függvényei. Vagy a faktoriális-függvény

$$\begin{cases} 0! = 1, \\ (x+1)! = x!\,(x+1) \end{cases}$$

rekurzív definíciója alapján világos, hogy bármely adott n nemnegatív egész számhoz véges számú lépésben ki tudjuk számítani $n!$ értékét. Valóban, ez áll $n = 0$ esetén, hiszen az első egyenlet közvetlenül megadja $0!$ értékét; és ha valamely n-re áll, akkor áll $n+1$-re is, hiszen $(n+1)!$ kiszámításához nem kell mást tenni, mint a második egyenletben x helyébe n-et helyettesíteni, majd a jobboldalon $n!$-t a feltevés szerint véges számú lépésben kiszámítható értékével pótolni, végül az $n!\,(n+1)$ szorzást elvégezni. Hasonlóan látható, hogy bármely olyan aritmetikai függvény effektíve kiszámítható, amely az $y = 0$ konstansból és az $y = x+1$ (vagy akár a $z = x+y$ és a $z = xy$) függvényből kiindulva véges számú helyettesítés (vagyis függvény vagy függvények függvényének képzése) és

$$\begin{cases} \varphi(0, y, z, \ldots) = \alpha(y, z, \ldots), \\ \varphi(x+1, y, z, \ldots) = \beta(x, \varphi(x, y, z, \ldots), y, z, \ldots) \end{cases}$$

alakú, ún. primitív rekurzív definíció segítségével definiálható (az utóbbi definíció a φ függvényt definiálja az előzőleg definiálandó α és β függvények segítségével). Az ilyen függvényeket primitív rekurzív függvényeknek nevezzük. Hasonló igaz e függvények osztályának számos általánosítására, mint pl. az ún. többszörösen rekurzív függvényekre (lásd PÉTER [1]). Azt is könnyű látni, hogy a kiszámító eljárás véges számú lépésének mindegyike ebben az általánosabb esetben is, úgy, mint az $y = x!$ függvény esetén, a következő két típusú lépés egyike: 1. valamely egyenletben (a szóban forgó függvény definíciós egyenleteinek egyikében) változók helyébe adott nemnegatív egész számok

helyettesítése; 2. valamely már megkapott egyenletben egy másik már megkapott egyenlet egyik oldalának másik oldalával való pótlása (ilyen lépés volt fentebb az, amikor $n!(n+1)$ szorzást elvégeztük, ekkor ugyanis az $n!(n+1)=m$ egyenletnek, ahol m az $n!(n+1)$ szorzat numerikus értéke, baloldalát pótoltuk jobboldalával). Ez a felismerés indította KLEENE-t a rekurzív függvény fogalmának következő általánosítására: általános rekurzív függvénynek nevezzük az olyan aritmetikai függvényt, amelyet olyan, a kérdéses függvényt és további segédfüggvényeket tartalmazó egyenletrendszerrel lehet definiálni, amelyből a kérdéses függvény értékét bármely adott helyen véges számú 1. és 2. típusú lépés segítségével egyértelműen ki lehet számítani (lásd KLEENE [1]). Az általános rekurzív függvények tehát, definíciójuk folytán, effektíve kiszámítható függvények.

Mármost CHURCH tételének bizonyítása azon a hipotézisen alapul, hogy fordítva is, minden kiszámítható függvény általános rekurzív függvény. CHURCH ezt a hipotézist definíció alakjába öltözteti: a kiszámítható függvény fogalmát úgy definiálja, hogy az általános rekurzív, vagy ami ezzel egyenértékű, a λ-definiálható, vagyis az ő ún. λ-konverziós kalkulusában jólképzett formulával előállítható függvényeket nevezi kiszámítható függvényeknek (lásd CHURCH [1], 356. oldal). Látszólag joga van ahhoz, hogy a kiszámítható függvény fogalmát tetszése szerint definiálja, mert előtte senki sem definiálta szabatosan ezt a szakkifejezést. Azonban egy ilyen definíció, mint általában minden olyan fogalom szabatos definíciója, amelyet definíció nélkül is használ az ember, egy bizonyos veszélyt rejt megában. Megeshetik ugyanis, hogy valamely függvényről be lehet bizonyítani, hogy nem effektíve kiszámítható e definíció értelmében, s utólag mégis kiderül, hogy megadható olyan eljárás, amelynek segítségével szemmelláthatólag bármely adott helyen véges számú lépésben ki lehet számítani a függvény értékét. Hasonló a helyzet az effektíve megoldható problémasereg fogalmával, ha azt CHURCH nyomán úgy definiáljuk, hogy olyan problémasereget értünk rajta, amelynek karakterisztikus függvénye általános rekurzív függvény: megeshetik, hogy valamely problémaseregről be lehet bizonyítani, hogy e definíció értelmében megoldhatatlan s utólag valaki mégis megoldja.

Maga CHURCH is nyilván érzi, hogy nem pusztán definícióról van szó, hiszen több mint két oldalnyi érvet sorol fel annak plauzibilissé tételére, hogy „definíciója" valóban fedi a kiszámítható függvény addig definíció nélkül használt fogalmát. Egy másik dolgozatában pedig (CHURCH [2]) a második számosztály konstruktíve megadható rendszámának addig szintén definíció nélkül használt fogalmát definiálja azáltal, hogy ugyancsak visszavezeti a kiszámítható (aritmetikai) függvény fogalmára s ez utóbbit ismét azonosítja az általános rekurzív függvény fogalmával, majd a következőket mondja. Azok

számára, akik nem tartják meggyőzőnek azt, hogy a konstruktív rendszám e definíciója fedi ezt a fogalmat, álljon ez a definíció kihívásként (challenge): adjanak meg olyan bővebb definíciót, amely alá eső rendszámok szintén megérdemlik a konstruktív rendszám nevet, vagy pedig olyan szűkebb definíciót, amely szintén kimeríti azoknak a rendszámoknak fogalmát, amelyek ezt a nevet megérdemlik.

Egyébként már POST [1] is rámutatott arra, hogy az effektíve kiszámítható függvény fogalmának az általános rekurzív függvény fogalmával való azonosításának definíció alakjába öltöztetése elhomályosítja ezen azonosítás szakadatlan verifikálásának szükségességét. (Ebben igazat adok Postnak, a hozzáfűzött agnoszticista megjegyzésében azonban, amely szerint a CHURCH-tétel a Homo Sapiens matematizáló képességének határaira vonatkozó alapvető felfedezés volna, nem, hiszen nem lehet abszolút határról beszélni.)

Az ún. abszolút megoldhatatlan problémákra (helyesen: problémaseregekre) vonatkozó további kutatások ugyancsak ezen a CHURCH-féle hipotézisen, vagy más hasonló, azzal ekvivalens hipotézisen alapulnak. Így pl. TURING [1] az effektíve kiszámítható függvény fogalmát az olyan aritmetikai függvény fogalmával azonosítja, amelyhez szerkeszthető olyan (pontosan definiált értelemben vett) számológép, amellyel a kérdéses függvény értékét bármely adott helyen véges számú lépésben ki lehet számítani. Az ebben az azonosításban rejlő hipotézis plauzibilitása mellett szintén számos érvet sorol fel; egyik érve éppen annak bizonyítása, hogy e hipotézis ekvivalens a CHURCH-félével (lásd TURING [2]). MARKOV ([1] és [2]; lásd még ott idézett többi munkáját is) a problémamegoldó eljárás (algoritmus) fogalmát a karakterisztikus függvényen át vezető kerülőút megtakarításával, közvetlenül definiálja; e definíció felhasználásával számos problémaseregnek algoritmussal való megoldhatatlanságát bizonyította be, köztük olyanokét is, amelyekre előzőleg valóban kerestek megoldó algoritmust az algebristák. Vizsgálatai azonban szintén egy hipotézisen alapulnak, amely szerint minden algoritmus egy bizonyos normálalakra hozható. E hipotézis plauzibilitását ismét egy sereg érvvel igyekszik alátámasztani. NOVIKOV [1] ugyancsak e MARKOV-féle hipotézis alapján bizonyította be a csoportelmélet szóproblémájának megoldhatatlanságát. Egyébként GYETLOVSZ [1] megmutatta, hogy a MARKOV-féle hipotézis szintén ekvivalens a CHURCH-félével.

4. A megoldhatatlan problémaseregek létezésére vonatkozó CHURCH-tétel még akkor sem jogosít agnoszticista következtetésekre, ha elfogadjuk a CHURCH-féle hipotézist. Valóban, a világ kimerítő megismerésére irányuló törekvésünk során, e megismerés fejlődésének minden stádiumában csak véges számú matematikai probléma megoldását kívánja a világ megismerésére irányuló következő lépés; végtelen sok matematikai probléma megoldását csak a meg-

ismerés egész végtelen folyamata kívánja. Igaz, hogy a világ megismerése folyamatát elősegíti, ha valamely végtelen problémasereg valamennyi problémáját egyidejűleg, közös eljárással meg tudjuk oldani, mert akkor, valahányszor a világ megismerésére irányuló törekvésünk során olyan problémára bukkanunk, amely e problémasereghez tartozik, alkalmazhatjuk e probléma megoldására azt az általános módszert, amit a problémasereg megoldására találtunk; azonban, ha valamely problémasereghez nincs is olyan általános eljárás, amellyel a problémasereg bármely adott problémáját véges számú lépésben meg tudjuk oldani, ez nem zárja ki azt, hogy amint valamely, e problémasereghez tartozó probléma a világ megismerésére irányuló törekvésünk során felmerül, e speciális problémát meg tudjuk oldani.

Egyébként PÉTER RÓZSA bebizonyította, hogy a CHURCH-tétel az általános alakban fogalmazott GÖDEL-tétel *következménye*; majd, PÉTER RÓZSA bizonyítását elemezve, bebizonyítottam, hogy a GÖDEL-tételt olyan általánosan is meg lehet fogalmazni, hogy a CHURCH-tétel egyenesen *speciális esete* legyen, annak ellenére, hogy a GÖDEL-tétel ebben az általános fogalmazásban is csak relatíve (valamely axiómarendszerre nézve) megoldhatatlan aritmetikai probléma létezését állítja (lásd KALMÁR [1]). Ebből is világos, hogy a CHURCH-tételből sem lehet agnoszticista következtetést levonni, hiszen az a fenti meggondolás, amely azt mutatta, hogy a GÖDEL-tételnek nincs ilyen következménye, a GÖDEL-tétel ezen általános megfogalmazására is alkalmazható. Ezenkívül azt is mutatja PÉTER Rózsával közös eredményünk, hogy helytelen a CHURCH-tételt a GÖDEL-tétel élesítésének tekinteni azon az alapon, hogy a CHURCH-tételben nincs szó olyan axiómarendszerről, amelynek segítségével leszögeznők, milyen módszereket szabad a tételben szereplő problémák megoldására alkalmazni, tehát a CHURCH-tétel ilyen értelemben abszolút-megoldhatatlan probléma létezését állítja. (Ebben a beállításban ott a hiba, hogy a CHURCH-tétel nem megoldhatatlan *probléma*, hanem megoldhatatlan *problémasereg* létezését állítja; a tévedésre az ad alkalmat, hogy problémasereg helyett szokás problémát is mondani.)

5. A CHURCH-tétel szokásos bizonyítása ún. konstruktív bizonyítás, azaz módot ad egyrészt a kérdéses problémasereg effektív megadására, másrészt minden olyan effektíve megadott megoldás-kísérlethez, amely a problémasereg karakterisztikus függvényét általános rekurzív függvényként állítaná elő, olyan ellenpélda effektív megadására, amely megcáfolja, hogy a kérdéses megoldás-kísérlet a problémasereg helyes megoldása volna. Ez az ellenpélda abban áll, hogy effektíve ki tudunk jelölni egy speciális, a problémasereghez tartozó problémát (hogy melyiket, az éppen a kérdéses megoldás-kísérlettől függ), azt effektíve meg tudjuk oldani, azonban a megoldás épp az ellenkező lesz, mint amit a kérdéses megoldás-kísérlet szolgáltatna. Ily módon a kér-

déses problémasereg megoldhatatlanságát — a CHURCH-féle hipotézis felhasználásával — nem úgy mutatjuk meg, hogy megadjuk egy megoldhatatlan speciális esetét, hanem éppen effektíve megoldható speciális esetein keresztül.

Meg fogom azonban mutatni, hogy ha nem ragaszkodunk a konstruktív bizonyításmódhoz, így többek között megengedjük a harmadik kizárása elvének korlátlan alkalmazását (mint ahogy azt matematikai bizonyításokban általában meg szokás engedni), akkor abszolút-megoldhatatlan aritmetikai probléma (nem problémasereg!) létezése is következik a CHURCH-féle hipotézisből, mégpedig olyan körülmények között, hogy ez a következmény erős érvet ad magának a CHURCH-féle hipotézisnek plauzibilitása *ellen*. (Mint már CHURCH [1] megjegyezte, a CHURCH-féle hipotézis, vagyis az effektíve kiszámítható függvény fogalmának az általános rekurzív függvény fogalmával való azonosítása mellett csak plauzibilitási érveket lehet felhozni, mint ahogy általában azt, hogy valamely szabatos definíció nélkül is használatos fogalomnak egy bizonyos szabatos definíciója fedi a kérdéses fogalmat, nem lehet szabatosan bebizonyítani, csak plauzibilitási érvekkel lehet alátámasztani. Ez azonban nem zárja ki azt, hogy a CHURCH-féle hipotézis plauzibilitása ellen is lehessen érveket felhozni.)

Valóban, ismeretes, hogy van olyan kétváltozós φ általános rekurzív függvény, hogy a következőképpen definiált egyváltozós ψ aritmetikai függvény nem általános rekurzív függvény:

$$\psi(x) = \begin{cases} \text{a legkisebb olyan } y \text{ nemnegatív egész szám, amelyre} \\ \quad \varphi(x, y) = 0, \text{ ha van ilyen szám,} \\ 0, \text{ ha nincs olyan } y \text{ nemnegatív egész szám, amelyre} \\ \quad \varphi(x, y) = 0 \end{cases}$$

(lásd KLEENE [1], 741. oldal, XIV. tétel). A φ függvényt akár primitív rekurzív függvénynek is választhatjuk; sőt, meg lehet mutatni, hogy van ilyen tulajdonságú φ elemi függvény is, vagyis olyan függvény, amely az 1 konstansból, továbbá az x, y és egyéb (szumma- és produktum-index gyanánt használandó) változókból véges számú aritmetikai összeadás, aritmetikai kivonás, aritmetikai szorzás és aritmetikai osztás segítségével felépített kifejezéssel definiálható. Itt aritmetikai összeadáson két tag összeadását vagy szummaképzést, aritmetikai kivonáson két tag különbsége abszolút értékének képezését, aritmetikai szorzáson két tényező összeszorzását vagy produktumképzést, aritmetikai osztáson pedig két nemnegatív egész szám hányadosa egész részének képezését értjük; ha a nevezőben 0 áll, akkor értsünk ez utóbbi művelet eredményén pl. 0-t.

Minthogy a ψ függvény nem általános rekurzív függvény, a CHURCH-féle hipotézis szerint nem is effektíve kiszámítható függvény, vagyis nincs

olyan eljárás, amelynek segítségével bármely adott n helyen véges számú lépésben ki lehetne számítani a $\psi(n)$ függvényértéket. Másrészt világos, hogy ha n olyan nemnegatív egész szám, amelyhez van olyan y nemnegatív egész szám, hogy $\varphi(n, y) = 0$, akkor véges számú lépésben meg tudjuk találni a legkisebb ilyen y számot, vagyis véges számú lépésben ki tudjuk számítani a $\psi(n)$ függvényértéket. Ehhez nem kell mást tennünk, mint sorra kiszámítani a $\varphi(n, 0), \varphi(n, 1), \varphi(n, 2), \ldots$ függvényértéket (mindegyiket véges számú lépésben ki tudjuk számítani, hiszen φ általános rekurzív, tehát biztosan effektíve kiszámítható függvény), míg az első olyat meg nem találjuk közöttük, amely 0, és leolvasni, mi volt ebben a φ függvény második argumentuma. Az is világos, hogy ha n olyan nemnegatív egész szám, amelyről be lehet bizonyítani, hogy nincs olyan y nemnegatív egész szám, hogy $\varphi(n, y) = 0$, akkor szintén véges számú lépésben meg tudjuk határozni a $\psi(n)$ függvényértéket. Annak bizonyítása ugyanis, hogy nincs ilyen y, szükségképpen véges számú lépésből áll, és arra az eredményre vezet, hogy $\psi(n) = 0$.

A most leírt két eljárást egyesítve olyan eljárást kapunk, amelynek segítségével legalábbis bizonyos n nemnegatív egész számok esetén véges számú lépésben ki tudjuk számítani a $\psi(n)$ függvényértéket, ti. azon n-ek esetén, amelyekhez vagy van olyan y nemnegatív egész szám, hogy $\varphi(n, y) = 0$, vagy pedig be lehet bizonyítani, hogy nincs ilyen y. Ehhez nem kell mást tennünk, mint egyidejűleg elkezdeni kiszámítani sorra $\varphi(n, 0), \varphi(n, 1), \varphi(n, 2), \ldots$ értékét és ugyanakkor megpróbálni bebizonyítani, hogy nincs olyan y nemnegatív egész szám, amelyre $\varphi(n, y) = 0$, egészen addig, amíg vagy olyan értékre nem bukkanunk a $\varphi(n, 0), \varphi(n, 1), \varphi(n, 2), \ldots$ sorozatban, amely 0, vagy annak bizonyítása nem sikerül, hogy nincs a sorozatnak ilyen tagja; az első esetben $\psi(n)$ a $\varphi(n, 0), \varphi(n, 1), \varphi(n, 2), \ldots$ sorozat első olyan tagjában, amelynek 0 az értéke, a φ függvény második argumentuma, a második esetben $\psi(n) = 0$.

Mármost a CHURCH-féle hipotézis szerint többek között ez az eljárás sem lehet olyan, amelynek segítségével bármely n helyen ki lehet számítani a $\psi(n)$ függvényértéket (ha ugyanis valamely n helyen ki lehet számítani, akkor véges számú lépésben ki lehet számítani); tehát, a harmadik kizárása elvének alkalmazásával, adódik, hogy van olyan n nemnegatív egész szám, amelyre a fenti eljárás nem alkalmazható; vagyis amelyre egyrészt nincs olyan y nemnegatív egész szám, hogy $\varphi(n, y) = 0$, másrészt az, hogy nincs ilyen y, nem bizonyítható be.

Hangsúlyozom, hogy ebben a meggondolásban azon, hogy „bebizonyítható", nem azt értettük, hogy valamely adott axiómarendszer keretein belül bebizonyítható, hanem azt, hogy valamilyen helyes (és természetesen véges számú lépésből álló) módszerrel bebizonyítható. Valóban, akármilyen helyes módszerrel sikerül bebizonyítanunk azt, hogy nincs olyan y nemnegatív egész

szám, amelyre $\varphi(n, y) = 0$, ezzel kiszámítottuk a $\psi(n)$ függvényértéket, mégpedig a $\psi(n) = 0$ eredménnyel.

Ennélfogva *a Church-féle hipotézisből*, a fenti meggondolás szerint, *olyan aritmetikai tartalmú T ítélet létezése következik*, ti. azé, hogy nincs olyan y nemnegatív egész szám, amelyre $\varphi(n, y) = 0$, *amely egyrészt igaz, másrészt azonban semmiféle helyes meggondolással nem bizonyítható be.*

Az ilyen T ítéletnek természetesen a tagadása (azaz esetünkben az az ítélet, hogy van olyan y nemnegatív egész szám, amelyre $\varphi(n, y) = 0$) sem bizonyítható be semmiféle helyes meggondolással, mert helyes meggondoláson természetesen csak olyan meggondolást értünk, amelynek segítségével csak igaz ítélet bizonyítható be, márpedig a T ítélet igaz, tehát tagadása nem igaz. Eszerint, ha a CHURCH-féle hipotézis igaz, akkor sem maga a T ítélet, sem tagadása nem bizonyítható be semmilyen helyes módszerrel, vagyis az a probléma, hogy igaz-e a T ítélet, abszolút-megoldhatatlan probléma. Hangsúlyozom, hogy határozott, paramétert nem tartalmazó problémáról, nem pedig problémaseregről van szó, hiszen φ határozott (KLEENE által effektíve megadott) általános rekurzív függvény, és n is határozott nemnegatív egész szám (amelynek a létezése a CHURCH-féle hipotézisből következik), tehát T határozott, semmiféle paramétert nem tartalmazó ítélet.

A CHURCH-féle hipotézisnek ez a következménye meglepő ugyan, de magában véve még elfogadható volna, ha ugyanakkor nem derült volna ki, hogy ez a T ítélet, amelyről abszolút-eldönthetetlen, hogy igaz-e, — igaz. Márpedig az, hogy egy igaz ítélet semmiféle helyes módszerrel nem bizonyítható be, annyira nem valószínű, hogy az a körülmény, hogy a CHURCH-féle hipotézisből olyan igaz ítélet létezése következik, amely semmiféle helyes módszerrel nem bizonyítható be, plauzibilissé teszi azt, hogy maga a CHURCH-féle hipotézis sem igaz.

Megjegyzem, hogy a T ítélet ismét olyan alakú, mint amilyenről a GÖDEL-tétellel kapcsolatban szó volt, ti. azt mondja ki, hogy minden y nemnegatív egész számnak megvan egy bizonyos tulajdonsága (az, hogy $\varphi(n, y) \neq 0$), mégpedig olyan, hogy bármely adott y nemnegatív egész számról (véges számú lépésben) el tudjuk dönteni, megvan-e a kérdéses tulajdonsága (hiszen φ általános rekurzív, tehát mindenesetre effektíve kiszámítható függvény). Az ilyen alakú ítéletek esetén fentebb megmutattuk, hogy nem lehet bebizonyítani, hogy semmiféle helyes eljárással nem lehet eldönteni, igaz-e a kérdéses ítélet. Mi ezt nem is bizonyítottuk be, hanem csak azt mutattuk meg, hogy a CHURCH-féle hipotézisből következik, hogy semmiféle helyes eljárással nem lehet eldönteni, igaz-e a kérdéses ítélet. Más szóval bebizonyítottuk, hogy a CHURCH-féle hipotézisnek olyan következménye van, amelynek igazságát nem lehet bebizonyítani. Ez is a CHURCH-féle hipetézis plauzibilitása elleni érvnek tekinthető.

6. A fenti meggondolást úgy is lehet fogalmazni, mint választ CHURCH fentemlített kihívására (nem a második számosztály konstruktíve megadható rendszámaira, hanem a CHURCH-féle hipotézis eredeti alakjára vonatkoztatva). Azt állítom, hogy a fenti ψ függvény ellenpélda a CHURCH-féle hipotézisre, azaz példa olyan függvényre, amely (mint KLEENE bebizonyította) nem általános rekurzív függvény, mégis effektíve kiszámítható; mégpedig a fentemlített eljárás: $\varphi(n, 0), \varphi(n, 1), \varphi(n, 2), \ldots$ értékének kiszámítása és ugyanakkor annak, hogy nincs olyan y nemnegatív egész szám, amelyre $\varphi(n, y) = 0$, minden lehető helyes módon való bizonyításának megpróbálása, mindaddig, míg vagy az utóbbi sikerül, vagy a $\varphi(n, 0), \varphi(n, 1), \varphi(n, 2), \ldots$ függvényértékek sorozatában olyanra nem bukkanunk, amely 0, olyan, amelynek segítségével bármely adott n helyen véges számú lépésben ki lehet számítani a ψ függvény értékét. Ezt az állításomat nem bizonyítom be, éppoly kevéssé, mint CHURCH a maga hipotézisét. De ugyanolyan joggal, mint CHURCH, én is mondhatom, álljon ez az állítás kihívásként: aki kételkedik benne, adjon meg olyan n nemnegatív egész számot, amelyre be tudja bizonyítani, hogy ez az eljárás nem vezet véges számú lépésben a $\psi(n)$ függvényérték kiszámításához. Világos, hogy ezt senki sem tudja semelyik n nemnegatív egész szám esetén sem bebizonyítani. Mert ahhoz többek között be kellene bizonyítania, hogy a $\varphi(n, 0), \varphi(n, 1), \varphi(n, 2), \ldots$ függvényértékek kiszámítása során sohasem bukkanunk olyanra, amely 0, vagyis, hogy nincs olyan y nemnegatív egész szám, amelyre $\varphi(n, y) = 0$. Ezzel azonban megadná annak, hogy nincs ilyen y, egy bizonyítását, tehát megmutatná, hogy a fentemlített eljárás mégis csak a $\psi(n)$ függvényérték kiszámításához vezet véges számú lépésben a $(\psi(n) = 0$ eredménnyel).

7. Ha valamely H hipotézisből következik egy I ítélet, akkor jogos azt mondani, hogy az I ítélet bennerejlik a H hipotézisben (akkor is, ha annak, aki a H hipotézist kimondta, esetleg szubjektíve nem volt szándékában belerejteni). Ilyen értelemben a CHURCH-féle hipotézisben bennerejlik az az állítás, hogy van olyan T ítélet, amely egyrészt igaz, másrészt semmiféle helyes meggondolással nem bizonyítható be (sem meg nem cáfolható); mégpedig olyan alakú T ítélet, hogy nincs olyan y nemnegatív egész szám, amelyre $\varphi(n, y) = 0$, ahol φ valamely általános rekurzív, vagy akár elemi függvény, n pedig valamely nemnegatív egész szám.

Ez a CHURCH-féle hipotézisben bennerejlő állítás erősen agnoszticista, mégpedig kantiánus jellegű állítás, hiszen azt mondja, hogy az objektív valóságban magában (an sich) igaz a T ítélet, de számunkra sohasem derülhet ki, hogy így van, hiszen mi ezt csak valamely bizonyítás útján tudhatnók meg.

Az az ellenérv sem áll meg, hogy a T ítélet nem az objektív valóságra vonatkozik. Világosan látszik, hogy nem így van, ha a φ függvényt elemi

függvénynek választjuk. Ugyanis minden olyan ítélet, amelyben csak nemnegatív egész számokról és a négy aritmetikai alapműveletről van szó, az objektív valóságban meglevő mennyiségi viszonyokra vonatkozik. Valóban, az ítéletben szereplő nemnegatív egész számokat bizonyos tárgyak, pl. golyók, elektronok (vagy akár azoknak csak a jövő században felfedezendő részei) számaként interpretálhatjuk; az összeadásnak a kérdéses tárgyak megfelelő halmazainak egyesítése felel meg, az aritmetikai kivonásnak elvevés (abból a halmazból veszünk el, amelyből lehet, annyi tárgyat, amennyiből a másik halmaz áll), a szorzásnak egyenlő számú tárgyból álló sorok egyesítése egy halmazba, az aritmetikai osztásnak a tárgyak egy halmazának egyenlő számú tárgyból álló sorokba, továbbá esetleg egy kevesebb tárgyból álló sorba való elrendezése (a szumma- és produktumképzés pedig ismételt összeadás ill. szorzás). Így pl. a GOLDBACH-féle sejtés az objektív valóságnak azt a feltételezett tulajdonságát fejezi ki, hogy ha bizonyos tárgyakat ki lehet rakni két sorba úgy, hogy mindegyikben ugyanannyi tárgy legyen, akkor e tárgyakat szét lehet választani két olyan csoportba, hogy egyik csoportban levő tárgyakat sem lehet egynél több sorban elrendezni úgy, hogy minden sorban ugyanannyi, de egynél több tárgy legyen. Hasonlóan látható, hogy ha φ elemi függvény és n nemnegatív egész szám, akkor az az ítélet, hogy nincs olyan y nemnegatív egész szám, hogy $\varphi(n, y) = 0$, az objektív valóságban meglevő valamely (esetleg nagyon bonyolult) mennyiségi törvényszerűséget fejez ki. Eszerint a CHURCH-féle hipotézisben bennerejlik az az állítás, hogy van olyan törvényszerűség, amely az objektív valóságban megvan, de az, hogy megvan, semmiféle helyes meggondolással nem látható be. Ezt az állítást nem fogadhatja el senki, aki meg van arról győződve, hogy az objektív valóságban meglevő törvényszerűségek megismerhetők; ennélfogva a CHURCH-féle hipotézist sem fogadhatja el.

8. A fenti meggondolásban szerepel a tetszőleges helyes módszerrel való matematikai bizonyítás fogalma. Ez a fogalom szintén olyan, amit szabatos definíció nélkül használnak a matematikában.* A fenti meggondolást, e fogalom szabatos definíciója hiján, csak heurisztikus meggondolásnak tekinthetjük;

* A moszkvai Harmadik Össz-szövetségi Matematikai Kongresszuson, ahol szintén előadtam a jelen dolgozat tartalmát, arról értesültem, hogy NOVIKOV sejtése szerint egyszer majd a tetszőleges, tartalmilag helyes matematikai bizonyítás fogalmát is sikerül olyanféle szabatos definícióval elhatárolni, mint az effektíve kiszámítható függvény fogalmát sikerült (a CHURCH-féle hipotézis értelmében) az általános rekurzív függvény fogalma (vagy a normalizálható algoritmus MARKOV-féle fogalma) segítségével. A Szovjetunióban ez a sejtés NOVIKOV-féle prognózis néven ismeretes. A magam részéről a NOVIKOV-féle prognózist éppoly kevéssé tartom plauzibilisnek, mint azt, hogy az effektíve kiszámítható függvény fogalma szabatos definícióval elhatárolható. (Utólagos megjegyzés, 1956. szeptember 5-én.)

azonban plauzibilitási érvként (a CHURCH-féle hipotézis plauzibilitása ellen) ilyen meggondolás is megengedhető.

A fenti meggondolás azonban szó szerint elismételhető úgy, hogy tetszőleges helyes módszerrel való bizonyítás helyett valamely olyan A axiómarendszer keretei között végzett bizonyítást mondunk, amely eleget tesz a következő feltételeknek.

1. Az A axiómarendszer formulái (vagyis az A axiómarendszerben megfogalmazható ítéleteket formalizáló formulák) a 0 és 1 konstansból, továbbá nemnegatív egész számokon átfutó változókból úgy épülnek fel, hogy ezekből először az aritmetikai műveletek jelének ($+, \Sigma, |\ -\ |, \cdot, \Pi, [\ /\ ]$) (ismételt) alkalmazásával (elemi függvényeket előállító) kifejezéseket készítünk, majd ilyen kifejezéseket az egyenlőség jelével ($=$) összekapcsolunk, végül az így keletkező „elemi egyenletekre" (ismételten) alkalmazzuk a logikai ítéletkalkulus műveleteinek jelét ($\neg, \wedge, \vee, \rightarrow, \leftrightarrow$) és a kvantorok jelét ($\exists, \forall$).

2. Valahányszor valamely φ (kétváltozós) elemi függvény valamely numerikusan adott m, n helyen valamely k értéket vesz fel, az ezt a tényt formalizáló formula bebizonyítható az A axiómarendszerben. (Ez a formula úgy keletkezik a φ elemi függvényt előállító kifejezésből, hogy változói helyébe az m és n nemnegatív egész számokat formalizáló kifejezéseket helyettesítjük, majd az így keletkező kifejezést az egyenlőség jelével összekötjük a k nemnegatív egész számot formalizáló kifejezéssel. Itt pl. a k számot formalizáló kifejezésen $k = 0$ esetében 0-t, különben $(\ldots((1 + 1) + 1) + \ldots) + 1$-et értünk, k számú 1-gyel.)

3. Valahányszor az A axiómarendszer valamely x szabad (azaz kvantorral le nem kötött) változót tartalmazó $\mathbf{F}(x)$ formulájához található olyan, valamely nemnegatív egész számot formalizáló $\mathbf{k}$ kifejezés, hogy az $\mathbf{F}(\mathbf{k})$ formula, amely $\mathbf{F}(x)$-ből x helyébe $\mathbf{k}$ helyettesítésével keletkezik, bebizonyítható az A axiómarendszerben, akkor az az $\exists x \mathbf{F}(x)$ formula is bebizonyítható az A axiómarendszerben, amely azt formalizálja, hogy van olyan x nemnegatív egész szám, amelyre $\mathbf{F}(x)$ áll.

4. Az A axiómarendszer ellentmondástalan (azaz nincs olyan $\mathbf{F}$ formulája, hogy $\mathbf{F}$ is, tagadása: $\overline{\mathbf{F}}$ is, bebizonyítható az A axiómarendszerben).

Valóban, fentebb abból, hogy helyes módszerrel való bizonyításról van szó, csak azt használtuk fel, hogy ha valamely φ elemi függvény és n nemnegatív egész szám esetén be lehet bizonyítani, hogy nincs olyan y nemnegatív egész szám, hogy $\varphi(n, y) = 0$ (amit így formalizálunk: $\neg \exists y \mathbf{f}(\mathbf{n}, y) = 0$, ahol $\mathbf{f}(x, y)$ a $\varphi(x, y)$ elemi függvényt formalizáló kifejezés, $\mathbf{n}$ az n nemnegatív egész számot formalizáló kifejezés és az $\mathbf{f}(\mathbf{n}, y)$ kifejezés úgy jön létre $\mathbf{f}(x, y)$-ből, hogy az x változó helyébe az $\mathbf{n}$ kifejezést helyettesítjük), akkor ez

igaz is, tehát akkor $\psi(n) = 0$. Ez fennáll akkor is, ha ilyen A axiómarendszerben való bizonyításra szorítkozunk. Valóban, ha nem volna igaz, hogy nincs olyan y nemnegatív egész szám, hogy $\varphi(n, y) = 0$, vagyis, ha volna olyan m nemnegatív egész szám, hogy $\varphi(n, m) = 0$, akkor 2. miatt az ezt formalizáló $\mathbf{f}(\mathbf{n}, \mathbf{m}) = 0$ formula, tehát 3. folytán az $\exists y \mathbf{f}(\mathbf{n}, y) = 0$ formula is bebizonyítható volna az A axiómarendszerben (az x változó szerepét most y vette át, az $\mathbf{F}(x)$ formuláét ill. a $\mathbf{k}$ kifejezését pedig $\exists y \mathbf{f}(\mathbf{n}, y)$ ill. $\mathbf{m}$). Ez azonban 4. miatt nem lehetséges, hiszen a $\neg \exists y \mathbf{f}(\mathbf{n}, y) = 0$ formula a feltevés szerint bebizonyítható A-ban.

Mármost a fenti meggondolás azt adja, hogy a CHURCH-féle hipotézisből következik olyan φ kétváltozós elemi függvény és olyan n nemnegatív egész szám létezése, hogy egyrészt nincs olyan y nemnegatív egész szám, hogy $\varphi(n, y) = 0$, másrészt az ezt a tényt formalizáló $\neg \exists y \mathbf{f}(\mathbf{n}, y) = 0$ formula semmiféle, az 1—4. feltételeknek eleget tevő A axiómarendszerben nem bizonyítható be.

A CHURCH-féle hipotézisnek ez a következménye azonban megcáfolható. Valóban, könnyű olyan A_0 axiómarendszert megadni, amely teljesíti az 1—3. feltételeket és amelynek axiómái részben a logikai függvénykalkulus axiómáiból (lásd pl. HILBERT—BERNAYS [1], 105. oldal) logikai változók és függvényváltozók helyébe az axiómarendszer formuláinak helyettesítésével keletkező formulák, részben verifikálható formulák (lásd ugyanott, 238. oldal), következtetési szabályai pedig a logikai függvénykalkulus következtetési szabályai (lásd ugyanott, 105—106. oldal.) Vegyük hozzá A_0-hoz új, az y szabad változóit tartalmazó axiómaként a $\neg \mathbf{f}(\mathbf{n}, y) = 0$ formulát. A keletkező A axiómarendszerben a $\neg \exists y \mathbf{f}(\mathbf{n}, y) = 0$ formula, mint a logikai függvénykalkulus axiómáinak és következtetési szabályainak felhasználásával könnyen adódik, bebizonyítható. Az A axiómarendszer nyilván szintén teljesíti az 1—3. feltételeket. Felhasználva azt a tényt, hogy az új $\neg \mathbf{f}(\mathbf{n}, y) = 0$ axióma a feltevés folytán (ti. hogy bármely y nemnegatív egész számra $\varphi(n, y) \neq 0$) verifikálható, az aritmetika axiómarendszere ellentmondástalanságának GENTZEN-féle bizonyításából (lásd GENTZEN [1], [2]) adódik, hogy az A axiómarendszer ellentmondástalan, vagyis a 4. feltételt is teljesíti.

A CHURCH-féle hipotézis e *cáfolata* már szabatosan definiált fogalmakkal dolgozik; mégsem értékelem többnek, mint plauzibilitási meggondolásnak. Valóban, ahhoz, hogy a ψ függvény értékét az olyan n helyeken is kiszámítsuk e meggondolás felhasználásával, amelyhez nincs olyan y nemnegatív egész szám, hogy $\varphi(n, y) = 0$, minden n-hez egy-egy az 1—4. feltételeknek eleget tevő olyan A axiómarendszert kell megkeresnünk, amelyben a $\neg \exists y \mathbf{f}(\mathbf{n}, y) = 0$ formula bebizonyítható. Ilyen axiómarendszert *megadni* könnyű a fentiek alapján, de annak megmutatásához, hogy valóban eleget tesz a 4. feltételnek,

valamilyen helyes módszerrel meg kell mutatnunk, hogy a $\neg \mathfrak{f}(n, y) = 0$ formula verifikálható, vagyis, hogy nincs olyan y nemnegatív egész szám, hogy $\varphi(n, y) = 0$; tehát végeredményben így sem kerülhetjük el a tetszőleges helyes módszerrel való bizonyítás fogalmát.

9. Még egy lehetséges ellenvetést kell kivédenem. Azt lehetne mondani, hogy a CHURCH-féle hipotézis úgy értendő, hogy csak azokra az aritmetikai függvényekre állítja, hogy általános rekurzív függvények, amelyeknek értéke bármely adott helyen valamely *egységes eljárással* véges számú lépésben kiszámítható; ezzel szemben a ψ függvény értékeinek kiszámítására adott eljárás nem egységes, hiszen más-más olyan n helyeken, amelyekhez nincs olyan y nemnegatív egész szám, hogy $\varphi(n, y) = 0$, más-más lesz az a „valamilyen helyes módszer", amellyel ez bebizonyítható. Véleményem szerint azonban az „egységes eljárás" fogalma relatív. Az általános iskolai tanuló minden egyes számtanpélda megoldására szolgáló eljárást másnak vél; és csak akkor jön rá, hogy egységes eljárásról van szó, amikor megtanul elsőfokú egyenleteket felállítani és megoldani. De nemcsak az egyes ember, hanem az emberiség fejlődésében is észlelhetünk hasonlót; pl. a csoportelmélet felfedezése óta számos olyan eljárást egységesnek tekintünk, amelyek azelőtt külön-külön algebrai, számelméleti vagy geometriai eljárásoknak számítottak. Így a kiszámítható függvény fogalmának és vele együtt a CHURCH-féle hipotézisnek csak akkor van objektív értelme, ha nem keverjük bele az „egységes eljárás" fogalmát.

10. Meggondolásaim, amelyek úgy vélem, újabb érvet adnak a CHURCH-tételnek agnoszticista következtetések levonására való felhasználása ellen, természetesen nem érintik a CHURCH-tételnek magának, vagy az ún. megoldhatatlan problémaseregekre vonatkozó többi tételnek érvényét, vagy jelentőségét. Csak azt mutatják, hogy ezeket a tételeket szabatosabban úgy kellene kimondani, hogy a kérdéses problémaseregek *általános rekurzív eljárással* (vagy normális algoritmussal) nem oldhatók meg, ahelyett, hogy röviden megoldhatatlanságukról beszélünk. Ilyen fogalmazásuk esetén nyilvánvalóbbá válnék az is, hogy agnoszticista következtetéseket nem lehet belőlük levonni.

IRODALOM

CHURCH, A. [1], An unsolvable problem of elementary number theory, *American J. of Math.*, **58** (1936), 345—363.

[2], The constructive second number class, *Bulletin of the American Math. Soc.*, **44** (1938), 224—232.

Детловс, В. К. [1], Нормальные алгорифмы и рекурсивные функции, Доклады Акад. Наук СССР, **90** (1953), 249—252.

FRAENKEL, A. [1], *Zehn Vorlesungen über die Grundlegung der Mengenlehre* (Leipzig—Berlin, 1927).

GENTZEN, G. [1], Die Widerspruchsfreiheit der reinen Zahlentheorie, *Math. Annalen*, **112** (1936), 493—565.

[2], Neue Fassung des Widerspruchsfreiheitsbeweises für die reine Zahlentheorie, *Forschungen zur Logik und zur Grundlegung der exakten Wissenschaften*, Neue Folge, **4** (1938), 19—44.

GÖDEL, K. [1], Über formal unentscheidbare Sätze der Principia Mathematica und verwandter Systeme I, *Monatshefte f. Math. und Phys.*, **38** (1931), 349—360.

HILBERT, D.—BERNAYS, P. [1], *Grundlagen der Mathematik*, **1** (Berlin, 1934).

KALMÁR L. [1], On unsolvable mathematical problems, *Library of the* X^{th} *Int. Congress of Philos.* (Amsterdam, 1948), I, 756—758.

KLEENE, S. C. [1], General recursive functions of natural numbers, *Math. Annalen*, **112** (1936), 727—742.

Марков, А. А. [1], Теория алгорифмов, *Az Első Magyar Mat. Kongresszus Közl.* (Budapest, 1950), 191—203.

[2], Теория алгорифмов, Труды Мат. Инст. им. В. А. Стеклова, **42** (1954), 1—375.

Новиков, П. С. [1], Об алгоритмической неразрешимость проблемы тождества слов в теории групп, Труды Мат. Инст. им. В. А. Стеклова, **44** (1955), 1 - 143.

PÉTER R. [1], *Rekursive Funktionen* (Budapest, 1951).*

POST, E. L. [1], Finite combinatory processes — formulation 1, *Journal of Symb. Log.*, 1 (1936), 103—105.

TURING, A. M. [1], On computable numbers, with an application to the Entscheidungsproblem, *Proc. of the London Math. Soc.*, (2) **42** (1937), 230—265, **43** (1937), 544—546.

[2], Computability and λ-definability, *Journal of Symb. Log.*, **2** (1937), 153—163.

WEDBERG, A. [1], L. NELSON, Critical philosophy and mathematical axiomatics ismertetése, *Journal of Symb. Log.*, **14** (1949), 244—246.

WHITEHEAD, A. N.—RUSSELL, B. [1], *Principia Mathematica* 1—3, (Cambridge, England, 1910—1913).

* Időközben megjelent a 2. kiadása is: Budapest, 1957. (Utólagos megjegyzés, 1957. március 5-én.)