AZ AXIOMATIKUS MÓDSZER KORLÁTAI.[1]

1. Axiómarendszerek felállítására a következő meggondolás vezet: A matematikában minden bizonyítás úgy történik, hogy az állítást más tételekre vezetjük vissza és minden definíció más fogalmakra vezeti vissza a definiálandó fogalmat. E visszavezetések során valahol meg kell állnunk: bizonyos fogalmakat tovább nem elemezendő alapfogalmakul, bizonyos tételeket tovább nem bizonyítandó alaptételekül, axiómákul kell elfogadnunk. Az alapfogalmakról nem használhatunk fel semmi mást, mint amit az axiómák kimondanak róluk, mintegy implicite definiáljuk ezeket az axiómákkal.

---

[1] A Kir. Magyar Pázmány Péter Tudományegyetem Elméleti Fizikai Intézetének kollokviumán 1940. márc. 8-án tartott előadás. Ismertnek teszem fel a halmazelmélet elemeit és KALMÁR LÁSZLÓ «A HILBERT-féle bizonyításelmélet célkitűzései, módszerei és eredményei» című ugyanitt 1939. november 3-án tartott előadását (részletes kidolgozását l. a Matematikai és Fizikai Lapok jelen füzetében, 65—119 old.) Erre a cikkre (K) jelzéssel fogok hivatkozni, jelöléseit további magyarázat nélkül használom. Az egyetlen eltérés a negáció jele: $\bar{A}$ helyett $\neg A$-t fogok írni. Összefoglalom a felhasznált logikai jeleket jelentésük szerint:

$\uparrow$	«igaz»
$A \,\&\, B$	«és»
$A \rightarrow B$	«következik»
$\neg A$	«nem»
$(x)\,F(x)$	«minden x-re igaz $F(x)$»
$(Ex)F(x)$	«van olyan x, melyre igaz $F(x)$»
$(x)\,(Ey)F(x, y)$	«minden x-hez van olyan y, melyre igaz $F(x, y)$».

Konkrét formulákat gót betűkkel szokás jelölni.

Az axiomatikus módszer, az elemi logika és logikai függvénykalkulus alapfogalmai (K)-ban megtalálhatók, ezért előadásomnak ezekre vonatkozó bevezető részét elhagyom. Viszont CHURCH abszolút eldönthetetlen problémáját, melyre az előadáson csak kevés idő jutott, kissé részletesebben tárgyalom.

Arra emlékeztet ez, ahogyan egy egyenletrendszer implicit definíciót ad a benne szereplő ismeretlenekre. Például arról az x, y, z-ről akarunk beszélni, melyekre

$$\begin{cases} x + y + z = 100 \\ x - y + z = 60; \end{cases}$$

ilyenek: 80, 20, 0, de 79, 20, 1 is, 78, 20, 2 is,... tehát az egyenletrendszer ezeket a számhármasokat definiálja implicite. Szándékosan választottam határozatlan egyenletrendszert, mert egy axiómarendszertől, melyhez hasonlítani akarom, semmiképpen sem várható, hogy az illető tudományág alapfogalmait egyértelműen adja meg, hiszen ezek az alapfogalmak általában nem is foghatók meg precízen (például a geometria szemléletből nyert határozatlan fogalmakra épít, a naiv halmazfogalom pedig még ellentmondásosnak is bizonyult). Egy-egy axiómarendszernek tehát több modell is eleget tesz. Például PEANO axiómái[2], melyeket a természetes számok megalapozására vezetett be, kitűnően teljesülnek bármely számtani haladványra is, ha a 0-nak nevezett definiálatlan alapfogalom helyébe az illető számtani haladvány első tagját, az «eggyel továbbszámlálás» helyébe a differencia hozzáadását képzeljük.

Ennek ellenére megkívánjuk egy axiómarendszertől, hogy lehetőleg teljesen képviselje azt és csakis azt a tudományágat, melynek felépítésére bevezettük. A *teljesség*nek ezt a követelését több különböző módon szokás precizírozni. Én a két legfontosabb módot tárgyalom, és meg fogom mutatni, hogy axiomatikus módszereink mindkettővel szemben csődöt mondanak.

2. Az eddigi gondolatmenethez természetesen csatlakozó követelés a következő volna: ha nem is várható, hogy egy axiómarendszernek egyetlen modell tesz eleget, de legalább egyenlő strukturájúak legyenek a neki eleget tevő modellek, mint ahogy az 1, 2, 3,... természetes számok sorozatát és a 2, 4, 6,... számtani haladványt egyenlő strukturájunak érezzük. Precízebben:

[2] (*K*) 73. old.

ha adva van két modell, amely az axiómarendszernek eleget tesz, lehessen ezeknek elemeit és a köztük fennálló relációkat úgy rendelni kölcsönösen és egyértelműen egymáshoz, hogy ha az egyik modell bizonyos $a, b, c, \ldots$ elemeinek a másikban $a', b', c', \ldots$ a párja és az egyik modellben definiált R relációnak a másik modellben R' a párja, továbbá az R reláció fennáll az $a, b, c, \ldots$ elemek között, akkor az R' reláció is fennálljon az $a', b', c', \ldots$ elemek között. Ezt fejezik ki úgy, hogy a két modell izomorf legyen, és az olyan axiómarendszert, melynek eleget tevő bármely két modell izomorf, *monomorf*nak nevezzük. Ehhez mindenesetre szükséges — korántsem elegendő —, hogy egyáltalán lehessen egymáshoz rendelni kölcsönösen és egyértelműen bármely két modell elemeit, azaz, hogy a modellek egyenlő számosságúak legyenek.

Hosszú ideig hitték a matematikusok, hogy a matematika különböző ágai számára felállított axiómarendszerek monomorfok. A geometriára HILBERT[3] ezt be is bizonyította úgy, hogy a geometria axiomatizált fogalmai segítségével definiált egy távolságok közötti összeadás- és szorzás-fogalmat és megmutatta, hogy ezekre érvényesek a valós számok műveleti szabályai (egyértelmű megfordíthatóság, kommutatív, asszociatív, disztributív törvények s. i. t.), így nyert egy halmazt, mely izomorf a valós számok halmazával. Két nem izomorf geometriai modell ilymódon két nem izomorf modellt adna a valós számok rendszerében is; márpedig az aritmetika rendszereinek monomorfizmusában rendületlenül hittek.

Ezt a hitet két irányban is megdöntötte SKOLEM. Főeredményeit úgy lehet összefoglalni, hogy *az axiomatikus módszer sokat markol és keveset fog.* E kettő közt nincs okozati összefüggés: külön-külön igazak. Előbb bizonyította be SKOLEM[4] a megszámlálhatón túlmenő fogalmakat axiomatizáló rendszerekről

---

[3] D. HILBERT: Grundlagen der Geometrie. (7. kiadás: Leipzig és Berlin, 1930).

[4] TH. SKOLEM: Einige Bemerkungen zur axiomatischen Begründung der Mengenlehre, Math.-kongressen in Helsingfors 1922, 217—232. old.

(tehát például a valós számokéról), hogy keveset fognak, és jóval később[5] a természetes számok lehetséges axiómarendszereiről, hogy sokat markolnak.

3. Hogy például a halmazelmélet axiómarendszerei *keveset fognak*, azon ezt értem: bármi módon adnak meg egy axiómarendszert a halmazelmélet számára, melynek tehát a megszámlálhatón túlmenő bármily nagy számosságok implicit definícióját is tartalmaznia kellene, hacsak nem ellentmondásos az axiómarendszer, mindig található hozzá egy megszámlálható modell is, amely kielégíti. Mivel pedig a halmazelmélet fogalmai önmagukban nem voltak precízek és éppen az axiómák által akartuk őket precízen bevezetni, úgy, hogy nem szabad rajtuk mást érteni, mint amit az axiómák róluk kimondanak: semmi sem jogosít fel arra, hogy mást értsünk rajtuk, mint azt a megszámlálható modellt, mely kielégíti az axiómarendszert, tehát, arra sem, hogy egyáltalán beszéljünk megszámlálhatón túlmenő számosságokról.

Ugyanez érvényes a valós számokat bevezető axiómarendszerekre is: ott kontinuum számosságot akarunk markolni és az axiómarendszer megint megszámlálható modellt fog. Persze, ha az axiómarendszertől függetlenül hiszünk a valós számokban, ezeknek a kontinuum számosságú halmaza szintén jó modell a kérdéses axiómarendszer számára, tehát az mindenesetre fennáll, hogy ez az axiómarendszer nem monomorf.

Skolem bizonyítása Löwenheim következő tételén alapul: ha a logikai függvénykalkulus egy zárt (azaz szabad változót nem tartalmazó) formulája kielégíthető egy individuumtartományban, akkor e halmaznak van oly megszámlálható része, hogy ezen belül is kielégíthető. Alapgondolata ez: legyen például a kérdéses zárt formula:

$$(x)\,(Ey)\,\mathfrak{A}\,(x, y),$$

(ahol $\mathfrak{A}(x, y)$-ban már nincsenek kötött változók, például ilyen

[5] Th. Skolem: Über die Unmöglichkeit einer vollständigen Charakterisierung der Zahlenreihe mittels eines endlichen Axiomensystems, Norsk matematisk forenings skrifter, Series II. No. 10. (1933), 73—74. old.

alakú: $F(x, y) \rightarrow G(y, x)$); hogy ez kielégíthető $\mathfrak{J}$-ben, az azt jelenti, hogy az $\mathfrak{A}(x, y)$-ban szereplő függvényváltozók (például F és G) választhatók úgy, hogy ha x az $\mathfrak{J}$ halmaz teszésszerinti eleme, van olyan y elem $\mathfrak{J}$-ben, hogy $\mathfrak{A}(x, y) = \uparrow$. Ez a «minden x-hez tartozik ily y» tulajdonképpen y-t mint x függvényét adja meg[6], tehát van egy olyan $\mathfrak{J}$-ben definiált $y = f(x)$ függvény $\mathfrak{J}$-beli értékekkel, hogy a fenti formula ezzel egyértelmű:

$$(x)\,\mathfrak{A}(x, f(x)),$$

szavakban: minden $\mathfrak{J}$-beli x-re $\mathfrak{A}(x, f(x)) = \uparrow$. Legyen most a az $\mathfrak{J}$-nek egy tetszésszerint választott eleme, akkor erre is

$$\mathfrak{A}(a, f(a)) = \uparrow.$$

$f(a)$ maga is $\mathfrak{J}$-beli érték, tehát őrá is

$$\mathfrak{A}(f(a), f(f(a))) = \uparrow.$$

Ugyanezt megismételhetjük $f(f(a))$-val s. i. t. ad inf. Világos, hogy a $(x)(Ey)\,\mathfrak{A}(x, y)$ formula már az

$$a, f(a), f(f(a)), \ldots$$

$\mathfrak{J}$-beli megszámlálható sorozaton kielégíthető: ha e sorozat bármely x tagjához a következő tagot választjuk y-nak, akkor teljesül $\mathfrak{A}(x, y) = \uparrow$. Ezzel Löwenheim tétele e példán igazolva van; az általános esetben ehhez lényegében hasonló, csak megfelelően komplikáltabb gondolatmenettel bizonyítható.

Mármost Skolem vette észre e tétel nagy jelentőségét. Minden axiómarendszer véges, vagy megszámlálható sok zárt formulából

---

[6] Az intuicionista felfogás szerint $(x)\,(Ey)\,\mathfrak{A}(x, y)$ azt jelenti, hogy ismeretes egy eljárás, mellyel az individuumtartomány minden x eleméhez megkonstruálható egy olyan y, hogy $\mathfrak{A}(x, y) = \uparrow$ legyen. Ez az eljárás y-t mint x függvényét adja meg. A klasszikus felfogás szerint $(x)\,(Ey)\,\mathfrak{A}(x, y)$ csak annyit jelent, hogy az individuumtartomány minden x eleméhez vannak olyan y-ok, melyekre $\mathfrak{A}(x, y) = \uparrow$; ha a kiválasztási axiómát alkalmazzuk, az ily y-ok halmazának kiválasztott eleme ismét x-nek jól definiált függvénye lesz. Skolem ad olyan bizonyítást is, mely nem használja fel a kiválasztási axiómát, l. Th. Skolem: Über einige Grundlagenfragen der Mathematik, Skrifter utgitt av det Norske Videnskaps-Akademi i Oslo I. Mat.-naturv. klasse, No 4 (1929), 1—49. old.

áll; SKOLEM egyetlen zárt formuláról ilyen rendszerekre általánosította a LÖWENHEIM-tételt és így adódik, hogy minden axiómarendszer, ha egyáltalán kielégíthető, már megszámlálható individuumtartományban is kielégíthető. Persze nem volna értelme azt kívánni, hogy akkor vegyünk több mint megszámlálható sok axiómát alapul, hiszen éppen az axiómák segítségével akarjuk magalapozni a «több mint megszámlálható» fogalmát.

Speciálisan a geometria axiómarendszerére ez a következőt jelenti: már HILBERT[3] taglalta, hogy az ő II. folytonossági axiómája nélküli geometriai rendszer kielégíthető egy megszámlálható individumtartományban is. A kérdéses axióma vezeti be a folytonosságot: a kontinuum számosságú valós koordinátájú pontokat. Mármost SKOLEM tétele szerint akkor is van oly megszámlálható modell, mely eleget tesz a rendszernek, ha a II. folytonossági axiómát hozzávesszük; ebben a modellben nem lehet bevezetni tetszésszerinti valós koordinátákat, csak bizonyos speciális eljárással képzetteket, — mint ahogy példánkban nem írhatjuk x helyébe az $\mathfrak{Z}$ halmaz tetszőleges elemét, csak azokat, melyek egy a-ból f szukcesszív alkalmazásával: $f(a), f(f(a)), \ldots$ állnak elő — ilyen pedig csak megszámlálható sok van. S már ezek is elegendők ahhoz, hogy az axiómarendszert kielégítsék; csak azon az alapfogalmon, amin eddig tetszésszerinti valós számot értettünk, most egy bizonyos eljárással konstruálható valós számok közül egy tetszőlegest kell érteni.

Éppen így a halmazelméletben a megszámlálható modell tartalmi interpretációja más lesz, mint amit eredetileg értettünk a halmazelmélet alapfogalmain; ami ott például kontinuumszámosságú halmaz volt, az e lefordítás után valami egészen más lesz, s így nincs ellentmondásban azzal, hogy elemei megszámlálhatók.

4. SKOLEM másik nagy eredményén, hogy *az axiomatikus módszer sokat markol*, precízen a következőt értem: bármennyire is szeretnénk a legszűkebben a nagyság szerint rendezett természetes számok testére szabni egy axiómarendszert, feltétlenül lesznek ω-nál magasabb rendszámú halmazok is, melyek

azt kielégítik. (A PEANO-axiómák[2] ugyan tökéletesen jellemzik az ω rendszámot, de az 5. PEANO-axiómában egy axiomatizálatlan «halmaz» fogalom is szerepel. Ha — kellően megszorítva — ezt is axiomatizáljuk, SKOLEM eredménye az így nyert axiómarendszerre is kiterjeszthető lesz.) Tehát még a természetes számok rendszere sem monomorf és tiszta axiomatikus módon nem tudjuk az ω rendszámú halmazt elválasztani a magasabb rendszámú halmazoktól.

A bizonyítás rendkívül szellemes; itt csak egy példán mutatom meg, hogy körülbelül miről van szó.

Válasszunk ki néhány tételt, melyek a nagyság szerint rendezett természetes számokra vonatkoznak, például a következőket: minden számnak van közvetlen rákövetkezője; definiálható rájuk egy összeadásnak és egy szorzásnak nevezett művelet, melyek természetes számokra alkalmazva ismét természetes számot adnak, teljesítik a kommutatív, asszociatív, disztributív törvényeket és olyanok, hogy van két 0-nak és 1-nek nevezett természetes szám, melyekre tetszésszerinti n esetén $n+0=n$ és $n\cdot 1=n$. Válasszuk ezeket a tételeket axiómáknak. Akkor meg lehet adni — a nagyság szerint rendezett természetes számoktól rendszámban is különböző — más halmazokat, amelyek ugyancsak kielégítik ezeket. Ilyen például a nemnegatív egész együtthatós polinomok halmaza a következő rendezésben: Egy $a_n x^n + \dots + a_1 x + a_0$ polinom később következik egy $b_m x^m + \dots + b_1 x + b_0$ polinomnál, ha magasabbfokú nála, vagy, ha egyenlőfokúak és balról jobbra haladva az első eltérő együttható az első polinomban nagyobb, mint a másodikban.

Ily polinomok összege, szorzata ismét ily polinom; az összeadás és szorzás törvényei itt is teljesülnek; 0-nak és 1-nek itt a konstans 0 illetve konstans 1 vehető (ahol tehát a_0 kivételével minden együttható 0, 0-adfokú polinom). Minden ily polinomnak van közvetlen rákövetkezője, például $2x^3+3x^2$ rákövetkezője $2x^3+3x^2+1$, ennek rákövetkezője $2x^3+3x^2+2$. De, hogy a polinomok megadott rendezése jóval bonyolultabb az ω rend-

számúnál, az világos: például mindjárt az x polinomot végtelen sok polinom előzi meg: mindazok, melyek alacsonyabb fokúak, tehát az összes konstansok: a konstans 0, 1, 2,... (Az így rendezett polinomhalmaz rendszáma egyébként ω^{ω}). Ha a természetes számsor más tulajdonságait is axiómákul vesszük, akkor ez a modell esetleg nem lesz jó, de más még bonyolultabb modell lesz jó helyette. Például a következő tulajdonsághoz: 0-on kívül minden számnak van közvetlen megelőzője, nem jó a modell, mert x-nek például nincs közvetlen megelőzője. De ha a legmagasabb tag együtthatóján kívül negatív együtthatókat is megengedünk, jó modellt kapunk; ekkor például x megelőzője $x-1$. (Az így kibővített polinomhalmaz még csak nem is jólrendezett).

Skolem megmutatja, hogy akárhány (véges, vagy megszámlálható sok) tulajdonságot veszünk hozzá a természetes számok felsorolt tulajdonságaihoz, mindig lesz oly még bonyolultabban rendezett függvényhalmaz, amely azoknak is eleget tesz.

5. A monomorfizmus követelésével szemben tehát siralmasan áll az axiomatikus módszer. Van azonban a teljességnek más fogalmazása is: ilyen a *kategoricitás*. E szerint akkor mondunk egy axiómarendszert teljesnek, ha bármilyen $\mathfrak{A}$ állítást fogalmazunk meg az általa definiált alapfogalmak segítségével, vagy $\mathfrak{A}$ vagy $\neg\mathfrak{A}$ bizonyítható benne. Tényleg jogosnak látszik akkor mondani teljesnek egy rendszert, ha elég erős ahhoz, hogy a körébe vágó felvethető problémákat eldöntse. De ez igen erős követelés.

Igen egyszerű rendszerekre teljesülhet. Például Presburger[7] bebizonyította arra a rendszerre, mely a logika axiómáiból, a Peano-féle axiómákból és az összeg rekurzív definíciójából áll.[8] Mit lehet ebben a rendszerben felírni? Változók közti össze-

[7] M. Presburger: Über die Vollständigkeit eines gewissen Systems der Arithmetik ganzer Zahlen, in welchem die Addition als einzige Operation hervortritt, Comptes-rendus du I. Congrès des Mathématiciens des Pays Slaves 1929 (1930), 92—101. old.

[8] (*K*) 93. old., 73. old. és 47. lábjegyzet, 96. old.

adások ilyesmit adnak például: $x+x+x+y+y$, ezt szokás így is írni $3x+2y$; tehát pozitív egész együtthatójú elsőfokú polinomok írhatók fel, ilyenek közti egyenlőségeket, egyenlőtlenségeket és ezek közti logikai relációkat lehet felírni a rendszerben. Az elsőfokú határozott vagy határozatlan egyenletek és egyenlőtlenségek körében mozgó problémák pedig tudvalevően eldönthetők.

Mindez egycsapásra megváltozik, ha a szorzást is bevezetjük, hiszen a szorzás a számelmélet minden bonyodalmát behozza a rendszerbe; például a GOLDBACH-sejtést és a nagy FERMAT-problémát is.[9]

Pedig úgy érezzük, hogy az még mindig elég egyszerű rendszer, melyben csak összeadás és szorzás szerepel. Már ebben ilyen mindmáig eldöntetlen problémák vannak, tehát már itt sem várható, hogy meg lehet adni egy általános eldöntési eljárást, ami a rendszer kategoricitásának precíz bizonyításához szükséges lenne; hát még bonyolultabb rendszerekben. De a hit azért megvolt a matematikusokban, hogy el lehet dönteni a GOLDBACH-sejtést, a nagy FERMAT-problémát is, bízhattak benne, hogy valaki majd csak eldönti ezeket is egyszer; *hinni* lehetett axiómarendszereink kategoricitásában. Egyik legfrappánsabb eseménye volt a bizonyításelméletnek, mikor GÖDEL[10] 1931-ben megadott — ténylegesen, konstruktíve megadott — egy számelméleti problémát, melyről kifogástalan módon bebizonyította, hogy egy, a számelméletet kifogástalanul megalapozó, axiómarendszerben eldönthetetlen. Szeretném GÖDEL gondolatmenetét legalább vázolni. Egy módosítással mondom el, ami már későbbi és ROSSERTŐL[11] származik.

6. A kérdéses axiómarendszerben néhány alapjel szerepel:

---

[9] (*K*) 102—103. old.

[10] K. GÖDEL: Über formal unentscheidbare Sätze der Principia Mathematica und verwandter Systeme I, Monatshefte für Math. und Phys. 38 (1931), 173—198. old.

[11] J. B. ROSSER: Extensions of some theorems of Gödel and Church. J. Symbol. Logic, 1 (1936), 87—91. old.

a zárójelek, a logikai jelek, 0, a «rákövetkezés» jele, ezenkívül előre megmondja GÖDEL, hogy hogyan fogja jelölni a változókat: egy megszámlálható $x_1, x_2, x_3, \ldots$ sorozatból fogja venni a jeleket számukra.[12] Ezt megteheti, hiszen minden konkrét formulában csak véges sok változó szerepelhet. E megszámlálható sok jelből csak megszámlálható sok formulát lehet képezni. Végre egy bizonyítás úgy fogható fel, mint véges sok formula sorozata, melyek közül néhány formula axióma, a többi ezekből a megengedett következtetési szabályok szukcesszív alkalmazásával következik; az utolsó közülük a bebizonyított formula.

Mármost GÖDEL gondolatmenetét követve, lefordítjuk ezt a rendszert a számelméletre: egy szótárt szerkesztünk, melyben az axiómarendszer jeleinek, formuláinak, bizonyításainak természetes számokat feleltetünk meg. A konstans jeleknek, amilyen például a $\rightarrow$ jel, az első néhány törzsszámot, a változóknak a többi törzsszámot. Így egy adott formula jeleihez egy véges számsorozat tartozik; magának a formulának azt a számot feleltetjük meg, melynek törzstényezős felbontásában a kitevők rendre az illető véges számsorozat tagjai.[13] Megmutatom egy példán, hogy ezt hogyan kell érteni. Vegyük például ezt a formulát: $(x_1)(x_1 = x_1)$. Ha a kétféle zárójel megfelelői 2, illetve 3, az $=$-é[14] 5 és a változóknak megfelelő törzsszámok például 19-nél kezdődnek, akkor e formula a következő jelsorozatot adja: 2, 19, 3, 2, 19, 5, 19, 3 és az a szám, melynek felbontásában ezek a kitevők:

$$n = 2^2 . 3^{19} . 5^3 . 7^2 . 11^{19} . 13^5 . 17^{19} . 19^3,$$

---

[12] Valójában GÖDEL különböző típusú változókat is megkülönböztet.

[13] A számelmélet alaptételét, hogy minden természetes szám egyértelműen írható fel törzsszámok szorzataként, ebben az alakban használom fel: Ha n legnagyobb törzsszámosztója p, akkor n felírható, egy és csakis egy módon mint a törzsszámok

$$2, 3, 5, 7, 11, 13, 17, 19, 23, \ldots$$

sorozatának p-ig terjedő valamennyi tagja bizonyos nemnegatív egész kitevős hatványainak szorzata. Például: $28 = 2^2 . 3^0 . 5^0 . 7$.

[14] Az $=$ jelet GÖDEL a logikai jelekkel fejezi ki.

amit — bár kissé soká tartana — ki is lehetne számítani és így a fenti formulának egyetlen szám felel meg. Fordítva, a törzstényezős felbontás egyértelműsége miatt, ha egy szám egyáltalán szerepelt e hozzárendelések közt, rá lehet ismerni, hogy melyik formulához rendeltük; például ha egy szám törzstényezős felbontása $2^{19}.3^5.5^{23}$, akkor ennek a következő formula felelt meg:

$$x_1 = x_2.$$

Formulák közti kapcsolatoknak így számelméleti függvények fognak megfelelni. Például, hogy az n-hez rendelt A formula negációjának milyen szám felel meg, az csak n-től függ, és így kapható meg: n törzstényezős felbontásából konstatáljuk, hogy milyen formulát rendeltünk hozzá, ha A-t, akkor felírjuk a $\neg A$ formulát és megkonstruáljuk a hozzátartozó számot. n-nek ezt a függvényét $\tau(n)$-nel fogom jelölni; tehát, ha A-hoz n, akkor $\neg A$-hoz $\tau(n)$ tartozik. Hasonlóan, az ahhoz a formulához rendelt szám, mely a k-hoz tartozó egyváltozós $F(x_1)$ formulából keletkezik, ha x_1 helyébe egy l természetes számhoz rendelt számjelet[15] helyettesítünk, k-nak és l-nek könnyen megkonstruálható függvénye. Ezt $\sigma(k, l)$-lel fogom jelölni. A k-hoz rendelt $F(x_1)$ formulát jelölhetjük így: $F_k(x_1)$, tehát $\sigma(k, l)$ az $F_k(\mathfrak{z}_l)$-hez rendelt számot jelenti. Ha speciálisan l-et helyettesítünk k helyébe is, $\sigma(l, l)$ az $F_l(\mathfrak{z}_l)$ formulához[15] rendelt szám lesz.[16] (Ha eltekintünk attól, hogy nem minden számhoz rendeltünk egyváltozós formulát, az egyváltozós formulák így volnának egysorba rendezhetők: $F_1(x_1)$, $F_2(x_1)$,... és akkor $\sigma(l, l)$, hol $l = 1, 2, \ldots$, a következő formulához rendelt számokat adná: $F_1(\mathfrak{z}_1)$, $F_2(\mathfrak{z}_2)$,.... Látható, hogy e mögött

---

[15] Például ha az a természetes szám rákövetkezőjének jele a formalizmusban fa, akkor 3 számjele: $fff0$ és a szótár ennek is megfeleltet egy természetes számot [ami 3-tól különböző, t. i., ha f-nek 11 és 0-nak 7 felel meg, $(2.3.5)^{11}.7^7$]. Az $fff0$ jel helyett rövidítésül $\mathfrak{z}_3$-at fogok írni.

[16] A könnyebb áttekinthetőség kedvéért összefoglalom a felhasznált megfeleltetéseket:

Szótár:

(,	),	=,	0,	f,...,	x_1,	x_2,...,	$F_k(x_1)$,	$F_k(\mathfrak{z}_l)$,	$F_l(\mathfrak{z}_l)$
2,	3,	5,	7,	11,...,	19,	23,...,	k ,	$\sigma(k, l)$,	$\sigma(l, l)$

és ha $\mathfrak{A}$-nak n felel meg, akkor $\neg\mathfrak{A}$-nak $\tau(n)$.

a halmazelmélet átlós módszerének gondolata van). GÖDEL bebizonyította, hogy $\tau(n)$ is, $\sigma(m, n)$-is rekurzív függvények.[17]

Végre egy bizonyításhoz — mely nem egyéb, mint egy véges formulasorozat — ismét véges számsorozat tartozik; rendeljük a bizonyításhoz azt a számot, melynek törzstényezős felbontásában e számsorozat tagjai a kitevők. Fel lehet ismerni, hogy egy számhoz milyen bizonyítást rendeltünk (ha egyáltalán szerepelt e szám a hozzárendelésben), például ha 0-nak 7 felel meg,

$$2^{2430\,000\,000\,000\,000\,000\,000} \cdot 3^{2430\,000\,000\,000} = 2^{2^{19} \cdot 3^5 \cdot 5^{19}} \cdot 3^{2^7 \cdot 3^5 \cdot 5^7},$$

---

[17] Rekurzív függvények azok, amelyek felépíthetők úgy, hogy kiindulunk a legegyszerűbb konstansból, 0-ból és a legegyszerűbb egyváltozós számelméleti függvényből, mely a továbbszámlálásnak felel meg (n-hez a rákövetkező számot rendeli), $n+1$-ből, azután szukcesszív helyettesítésekkel és rekurziókkal képezünk új függvényeket a már definiáltakból. Helyettesítés például: ha már definiáltuk $f(n) = n!$-t és $g(n) = n^2$-et, akkor $f(g(n)) = (n^2)!$ A rekurzió olyan definíció, mely megadja a függvény értékét a 0 helyen és azt, hogy ha már ismerjük az értékét egy tetszésszerinti n helyen, hogyan lehet ebből az $n+1$ helyen felvett értékét kiszámítani. Kiszámítás közben már előzőleg definiált függvényeket szabad felhasználni. Ha például már az 1 konstans és a szorzat, mint tényezőinek függvénye definiálva van, akkor egy $g(n)$ függvény definiálható így:

$$g(0) = 1, \qquad (a)$$

$$g(n+1) = (n+1) \cdot g(n). \qquad (b)$$

E definíció módot ad arra, hogy $g(n)$ értékét bármely adott n helyen kiszámítsuk: szukcesszíve mehetünk vissza, például (b) szerint

$$g(3) = 3 \cdot g(2),$$
$$g(2) = 2 \cdot g(1), \text{ tehát } g(3) = 3.2 \cdot g(1),$$
$$g(1) = 1 \cdot g(0), \text{ tehát } g(3) = 3.2.1 \cdot g(0),$$

de (a) szerint $g(0) = 1$, tehát $g(3) = 3.2.1 = 3!$

Éppen ez a döntő tulajdonság; hogy bármely rekurzív függvény értéke bármely adott helyen véges számú lépésben kiszámítható.

Rekurzív reláción oly összefüggést értünk számelméleti változók között, mely akkor és csak akkor áll fenn, ha egy rekurzív függvény 0 értéket vesz fel. Például bebizonyítható, hogy $|m-n|$ rekurzív függvény, tehát két tetszésszerinti rekurzív függvény közti egyenlőség rekurzív reláció, mert például $\varphi(n) = \psi(m)$ akkor és csak akkor igaz, ha $|\varphi(n) - \psi(m)| = 0$. Az előbbiek szerint bármely rekurzív relációról bármely adott helyen véges számú lépésben eldönthető, hogy teljesül-e vagy sem.

Az elemi számelméletben szerepet játszó valamennyi függvényről és relációról be lehet bizonyítani, hogy rekurzívok.

tehát e szám annak a bizonyításnak (és nem formulának, mert a kitevők összetett számok) felel meg, mely két formulából áll, az egyik a 19, 5, 19-hez, a másik a 7, 5, 7-hez rendelt jelekből áll; azaz e bizonyítás:

$$\frac{x_1 = x_1}{0 = 0}$$

($x_1 = x_1$ axióma, ebből $0 = 0$ helyettesítéssel adódik). Látjuk, hogy már e — triviálisan egyszerű — bizonyításhoz is milyen nagy szám tartozik; már egy valamire való bizonyításnak áttekinthetetlen nagy szám felelne meg. Egy bizonyítást *bonyolultabbnak* vagy *egyszerűbbnek* fogok mondani egy másiknál, a szerint, hogy nagyobb vagy kisebb számot rendeltünk-e hozzá.

E fordításban az axiómarendszer formuláira, bizonyításaira vonatkozó állítások természetes számokra vonatkozó számelméleti állításoknak felelnek meg. Például ennek az állításnak az igazsága: «*az l-hez rendelt formula a k-hoz rendelt bizonyításnak végformulája*» csak k-tól és l-től függ és ezek kitevőit megnézve, könnyen meggyőződhetünk arról, hogy teljesül-e; jelöljük az idézőjelek közti állítást $\beta(l, k)$-val. GÖDEL bebizonyította, hogy $\beta(l, k)$ rekurzív reláció.

GÖDEL bizonyításának egyik legfontosabb lépése, hogy megmutatja, hogy minden rekurzív relációhoz konstruálható a rendszerben egy formula, mely — változóinak helyére $\mathfrak{z}_m$, $\mathfrak{z}_n$,...-et helyettesítve — bizonyítható, ha a kérdéses reláció az m, n... helyen teljesül, és megcáfolható, azaz tagadása bizonyítható, ha a reláció nem teljesül e helyen. Nevezzük ezt a formulát a szóbanforgó reláció képének. A formulákat eddig egyszerűen jelsorozatoknak tekintettük; ez a tétel mintegy jelentést rendel némelyikükhöz. Például ha egy kétváltozós formula a $\mathfrak{z}_m$, $\mathfrak{z}_n$ helyen bizonyítható, ha m és n oly számok, hogy az $m < n$ rekurzív reláció teljesül, és cáfolható ha $m < n$ nem teljesül, akkor azt mondhatjuk, hogy az illető formula azt jelenti, azt mondja ki, hogy $m < n$.

Mármost legyen a $\beta(\sigma(l, l), k)$ rekurzív reláció képe egy $\mathfrak{B}_1(x_1, x_2)$ formula. Mit mond ki a reláció? Azt, hogy a $\sigma(l, l)$-

hez rendelt formula, azaz $F_l(\mathfrak{z}_l)$ a k-hoz rendelt bizonyításnak végformulája. Ha itt $\sigma(l, l)$ helyett $\tau(\sigma(l, l))$-t írunk, akkor $F_l(\mathfrak{z}_l)$ helyébe $\neg F_l(\mathfrak{z}_l)$ lép, tehát $\beta\big(\tau(\sigma(l, l)), k\big)$ azt jelenti, hogy $\neg F_l(\mathfrak{z}_l)$ a k-hoz rendelt bizonyítás végformulája; legyen ennek képe egy $\mathfrak{B}_2(x_1, x_2)$ formula. Ezek segítségével könnyen felírható a rendszerben annak az állításnak a képe, hogy az $F_l(\mathfrak{z}_l)$ formula nem bizonyítható egyszerűbben, mint a saját tagadása:

$$(x_2)\{\mathfrak{B}_1(x_1, x_2) \rightarrow (Ex_3)[x_3 \leqq x_2 \,\&\, \mathfrak{B}_2(x_1, x_3)]\};$$

ezt a formulát $\mathfrak{B}(x_1)$-gyel fogom rövidíteni. (Csak egy szabad változója van: x_1).

(Az itt formalizált állítás nem abszurdum: ha $F_l(\mathfrak{z}_l)$ nem bizonyítható, akkor semminél sem bizonyítható egyszerűbben, még a saját tagadásánál sem). Feleljen meg a $\mathfrak{B}(x_1)$ formulának az r szám, azaz legyen $\mathfrak{B}(x_1)$ az $F_r(x_1)$ formula. Mi az értelme $\mathfrak{B}(\mathfrak{z}_r)$-nek? Ez egyrészt $F_r(\mathfrak{z}_r)$-rel azonos, másrészt $\mathfrak{B}$ jelentése következtében azt mondja ki, hogy $F_r(\mathfrak{z}_r)$ nem bizonyítható egyszerűbben, mint $\neg F_r(\mathfrak{z}_r)$. Tehát $F_r(\mathfrak{z}_r)$ maga mondja ki ezt: «Én nem vagyok egyszerűbben bizonyítható, mint a saját tagadásom».

Ha előre akartunk volna egy ilyen furcsa értelmű formulát felírni, mindenki azt mondta volna, hogy lehetetlen. Itt azonban kifogástalan, konstruktív úton, rekurziókkal definiáltuk a τ, σ függvényeket és a β relációt, ezután egy rekurzív reláció képét, mint egyváltozós formulát, ugyanígy megkonstruáltunk egy $\mathfrak{z}_r$ helyet, amit a változó helyébe írva, olyan formulához jutottunk, amelynek meglepetésünkre a fenti furcsa értelme van. Mi tehát nem *állítottuk* egy ilyen formula létezését, hanem *megkonstruáltunk* egy ilyet. Pontosan megmondhatjuk, hogy melyik ez a formula: ami a jól megkonstruált r számhoz tartozó $F_r(x_1)$ formulából lesz, ha változója helyébe $\mathfrak{z}_r$-et helyettesítünk.

Ezekután könnyen bebizonyítható, hogy ez az $F_r(\mathfrak{z}_r)$ formula eldönthetetlen. Mert ha valaki megadna rá egy konkrét bizonyítást, akkor konstatálhatnók, hogy milyen bonyolult ez a

bizonyítás, vagyis milyen számot rendeltünk hozzá; csak véges számú kisebb szám van, tehát az összes egyszerűbb bizonyítások száma véges, nézzük végig ezeket. Ha köztük van $\neg F_r(\mathfrak{z}_r)$ bizonyítása is, ellentmondásra jutottunk, hiszen ekkor $F_r(\mathfrak{z}_r)$ is, $\neg F_r(\mathfrak{z}_r)$ is bizonyítható. Ha nincs köztük $\neg F_r(\mathfrak{z}_r)$ bizonyítása, akkor $F_r(\mathfrak{z}_r)$ mindenesetre egyszerűbben bizonyítható be, mint $\neg F_r(\mathfrak{z}_r)$, pedig $F_r(\mathfrak{z}_r)$ éppen azt mondja ki, hogy ő nem bizonyítható egyszerűbben, mint a tagadása, tehát ezzel bebizonyítottuk, hogy $F_r(\mathfrak{z}_r)$ hamis dolgot állít; azonban az, amit most elmondtam, precíz fogalmazásban kifogástalan bizonyítása $\neg F_r(\mathfrak{z}_r)$-nek. Ismét bizonyítható volna $F_r(\mathfrak{z}_r)$ is, $\neg F_r(\mathfrak{z}_r)$ is, ami ellentmondás.

Ugyanígy lehet kimutatni, hogy $\neg F_r(\mathfrak{z}_r)$ sem lehet bizonyítható. Mert ha valaki megadna rá egy konkrét bizonyítást, akkor ismét csak véges sok ennél egyszerűbb bizonyítás volna; nézzük végig ezeket. Ha $F_r(\mathfrak{z}_r)$ bizonyítása köztük van, $\neg F_r(\mathfrak{z}_r)$ is, $F_r(\mathfrak{z}_r)$ is bizonyítható, és ez ellentmondás. Ha $F_r(\mathfrak{z}_r)$ bizonyítása nincs köztük, akkor $F_r(\mathfrak{z}_r)$ nem bizonyítható egyszerűbben, mint $\neg F_r(\mathfrak{z}_r)$, de éppen ez az az állítás, amit $F_r(\mathfrak{z}_r)$ kimond. Ez, amit most elmondtam, precíz fogalmazásban kifogástalan bizonyítása $F_r(\mathfrak{z}_r)$-nek. Tehát ismét bizonyítható volna $\neg F_r(\mathfrak{z}_r)$ is, $F_r(\mathfrak{z}_r)$ is, ez pedig ellentmondás.

Tehát $F_r(\mathfrak{z}_r)$ tényleg eldönthetetlen.

Megjegyzem még, hogy ez az eldönthetetlen probléma átalakítható úgy, hogy a logikai jeleken kívül csak az összeadás és a szorzás jele szerepeljen benne; tehát a számelméletben kaptunk ilyen aránylag egyszerű eldönthetetlen problémát.

7. Az így megadott eldönthetetlen probléma önmagában nem érdekes, mesterséges konstrukció, egyenesen erre a célra készült. De rögtön következik belőle egy igen érdekes probléma eldönthetetlensége is. $F_r(\mathfrak{z}_r)$ ugyanis azt mondta ki, hogy ő maga nem bizonyítható be egyszerűbben mint a saját tagadása, ami igazzá válik, ha $F_r(\mathfrak{z}_r)$ egyáltalán nem bizonyítható; ez utóbbit azonban bebizonyítottuk, tehát tulajdonképpen bebizonyítottuk, hogy $F_r(\mathfrak{z}_r)$ igazat mond. De csak úgy bizonyítottuk be, hogy az ellenkező

feltevésből ellentmondást hoztunk ki, tehát felhasználtuk azt a feltevést, hogy a rendszerben nincs ellentmondás. Jelöljük azt az állítást, hogy az axiómarendszer ellentmondásmentes (ezt könnyen fel lehet írni a rendszer jeleivel), $\mathfrak{W}$-vel, akkor nem magát $F_r(\mathfrak{z}_r)$-et, hanem ezt bizonyítottuk:

$$\mathfrak{W} \rightarrow F_r(\mathfrak{z}_r).$$

Ha tehát $\mathfrak{W}$ bizonyítható volna a rendszerben, akkor következménye $F_r(\mathfrak{z}_r)$ is bizonyítható volna. Ez azonban — mint láttuk — ellentmondásra vezetne. Így tehát, ha egy axiómarendszer valójában ellentmondásmentes, akkor ez az ellentmondásmentesség nem bizonyítható be oly módszerekkel, melyek a rendszeren belül formalizálhatók. Tehát maga a rendszer ellentmondásmentessege is a rendszer eldönthetetlen problémái közé tartozik.

Éppen ezért kellett GENTZENnek az aritmetika ellentmondásnélküliségének bebizonyításához az ε-típusú transzfinit indukció mint kibuvó, mert ez nem formalizálható a rendszeren belül.[18]

8. GÖDEL bizonyítását, mint már említettem, egy speciális axiómarendszerre írta le részletesen, azonban bizonyítás közben csak azt használta fel, hogy az axiómarendszer elég «szabályos» (ebből adódik, hogy a rávonatkozó állításoknak megfeleltethető számelméleti relációk rekurzívok), és elég «kifejezőképes» (t. i. ahhoz, hogy bármely rekurzív relációnak legyen képe a formulák közt). Ezeknek a feltételeknek minden eddig felállított axiómarendszer eleget tesz, mely az aritmetikát tartalmazza. Más és más axiómarendszerhez más és más eldönthetetlen GÖDEL-probléma tartozik, hiszen, ha a kérdéses eldönthetetlen tételt axiómaként hozzávesszük a rendszerhez, ezzel ő eldönthetővé válik, s az új rendszernek más lesz az eldönthetetlen problémája. CHURCH[19] azonban példát adott oly problémára, mely független az alapul vett axiómarendszertől és semmilyen — a logikát

[18] (*K*) 105—109. old.

[19] A. CHURCH: A note on the Entscheidungsproblem, J. of symb. logic 1. (1936), 40—41. old. és helyesbbítés 1. (1936), 101—102. old.

tartalmazó — axiómarendszerben nem dönthető el, tehát jogosan nevezhető «abszolút eldönthetetlen» problémának. Persze, ez nem lehet olyan típusú, mint a GÖDEL-féle, mely egy egyszerű számelméleti tétel eldöntését kívánja, hiszen, ha volna bizonyítás arra, hogy egy ilyen számelméleti tétel abszolúte nem bizonyítható, ez éppen a kérdéses tétel tagadását bizonyítaná. Ha például egy diofantikus egyenlet megoldhatósága volna a probléma, tudjuk, hogy ha megoldható egy ilyen egyenlet, akkor elég messzire menve a természetes számok sorában, meg is kapjuk egy megoldását; ha tehát valaki bebizonyítaná, hogy a megoldhatóság abszolúte nem bizonyítható, akkor ebben az is benne volna, hogy bármily messze menve a természetes számok sorában, sohasem nyerhető megoldás a diofantikus egyenlet számára, ezzel azonban éppen az egyenlet megoldhatatlansága volna bizonyítva. A CHURCH-féle példa tehát nem egy tétel bebizonyítását vagy cáfolását kívánja, hanem annak eldöntését, hogy egy tételsorozat mely tagjai igazak, melyek nem. (Ilyen típusú probléma a FERMAT-féle, ahogyan a híres WOLFSKEHL-féle végrendeletet megfogalmazza: a 100.000 márkás díj annak adandó ki, aki a FERMAT-tételt bebizonyítja mindazokra a kitevőkre, amelyekre igaz, és megcáfolja azokra, amelyekre nem igaz).

CHURCH egyenesen e célra konstruált egy problémát. Szebb volna, ha egy konkrét számelméleti problémára, például a FERMAT-tételre is alkalmazható lenne a módszer, vagy a következő általánosabb problémára: eldöntendő, hogy mely diofantikus egyenletek oldhatók meg. Bár egyelőre még nem vihető át a módszer ilyen problémákra, mégis egyszerűbb ezeken szemléltetni CHURCH gondolatmenetét, mint az ő sokkal bonyolultabb, mesterséges problémáján. Én tehát a

$$P(x_1, x_2, \ldots, x_n) = 0 \qquad (P \text{ polinom})$$

diofantikus egyenletek megoldhatóságának problémáján mutatom be CHURCH módszerét, kiemelve, hogy mi hiányzik ahhoz, hogy erre is alkalmazható legyen, a folytatást azonban úgy mondva el, mintha megvolna az, ami hiányzik.

A szóbanforgó probléma egy megoldása abban áll, hogy megadunk egy utasítást, mely minden P polinomhoz 1-et vagy 0-t rendel a szerint, hogy a megfelelő diofantikus egyenlet (t. i. $P = 0$) megoldható-e vagy nem oldható meg; persze véges számú lépésben eldönthetőnek kell lenni, hogy az utasítás mit rendel egy-egy adott polinomhoz. Minthogy megszámlálható sok polinom van és véges számú lepésben meg lehet határozni egy adott polinomhoz a sorszámát a polinomok szokásos

$$P_1, P_2, \ldots, P_n, \ldots \qquad (P)$$

megszámlálásában és fordítva is, egy sorszámhoz a hozzátartozó polinomot, ezért egy ilyen utasítás egy olyan függvény megadásában áll, melynek minden adott helyen véges számú lépésben kiszámítható az értéke és amely az n helyen az 1 vagy 0 értéket veszi fel, a szerint, amint a polinomok megszámlálásánál a P_n-hez tartozó $P_n = 0$ diofantikus egyenlet megoldható vagy sem. (A minden egyes helyen véges számú lépésben kiszámítható függvény fogalmát sikerült precizírozni; mint minden precizírozásnál, itt sem tökéletesen biztos, hogy a precíz fogalom pontosan fedi az érzésszerinti legáltalánosabb ilyen függvényfogalmat, de ezt nagyon valószínűvé teszi, hogy az utóbbi időben többen, egymástól függetlenül, különböző utakon akartak megadni ily legáltalánosabb függvénydefiníciókat,[20] és utólag minde fogalmakról be lehetett bizonyítani, hogy ekvivalensek. Itt nyilván a rekurzív függvények általánosításáról van szó, ezért e precizírozott függvényfogalmat általános rekurzív függvénynek nevezzük).

A csak 0 és 1 értékeket felvevő általános rekurzív függvényeket karakterisztikus függvényeknek fogom nevezni. Bármely karakterisztikus függvény rendelhető számelméleti problémánk

---

[20] Lásd S. C. Kleene: General recursive functions of natural numbers, Math. Ann. 112 (1936), 727—742. old; S. C. Kleene: λ-definibility and recursiveness, Duke mathematical journal 2 (1936), 340—353. old.; A. M. Turing: Computability and λ-definibility, J. of symb. logic, 2 (1937), 153—163. old; D. Hilbert und P. Bernays. Grundlagen der Mathematik, II. kötet, Berlin (1939), Supplement II.

egy-egy állítólagos megoldásához, amely azt állítja, hogy a $P_n = 0$ diofantikus egyenlet akkor és csak akkor oldható meg, ha a kérdéses karakterisztikus függvény értéke az n helyen 1. Bebizonyítandó, hogy egyikük sem *helyes* megoldás, azaz minden karakterisztikus függvényhez meg lehet adni egy diofantikus egyenletet, amelyről el tudjuk dönteni, hogy megoldható-e, vagy nem, de ha megoldható, akkor éppen 0-t, s ha nem, akkor éppen 1-et rendel hozzá, illetve sorszámához az illető karakterisztikus függvény.

Ennek megvalósításához két gondolat vezet. Az első — és ez az, amit a most tárgyalt problémára ezideig nem sikerült átvinni — abban áll, hogy azt, hogy egy általános rekurzív függvény értéke egy adott helyen 0, fogalmazzuk át a mi problémánkra. A tárgyalt esetben ez pontosabban a következőt jelenti: az kellene, hogy minden $g(n)$ általános rekurzív függvényhez és minden n számhoz hozzá lehessen rendelni egy polinomot úgy, hogy $g(n) = 0$ akkor és csak akkor álljon, ha a polinomnak megfelelő diofantikus egyenlet megoldható; amellett az is kell, hogy a polinom n-től is (ne csak változóitól, amelyekre nézve meg kell oldani a diofantikus egyenletet) polinomiálisan függjön. Tehát: minden $g(n)$ általános rekurzív függvényhez legyen egy olyan $P^{(g)} = P^{(g)}(t; x_1, x_2, \ldots, x_r)$ polinom, hogy $g(n) = 0$ ekvivalens legyen azzal, hogy van oly $x_1, x_2, \ldots x_r$, amelyekre $P^{(g)}(n; x_1, x_2, \ldots, x_r) = 0$. A továbbiakban felteszem, hogy ez a követelés teljesül. Ha van olyan n argumentum, melyre ez a $P^{(g)}$ polinom a (P) sorozat n-edik tagjával, P_n-nel azonos, akkor $g(n)$ nem lehet a problémánk megoldása, mert ha az volna, erre az n argumentumra is azzal volna ekvivalens $g(n) = 0$, hogy *nincs* olyan $x_1, x_2, \ldots, x_r$, amelyekre $P_n(x_1 x_2, \ldots, x_r) = 0$. A továbbiakban azt fogom megmutatni, hogy minden karakterisztikus $g(n)$ függvényhez található ilyen n argumentum. Ehhez kell a másik gondolat, mely a halmazelmélet átlós módszerére emlékeztet.

A fenti (P) megszámlálásban szerepeljenek a konstansok (mint 0-változós függvények) is; viszont legyen

$$Q_1, Q_2, \ldots, Q_n, \ldots \qquad (Q)$$

a legalább egyváltozós polinomok egy megszámlálása; s ha Q_n első változója helyébe a konstans m számot tesszük, a keletkező eggyel kevesebb változós polinom sorszáma a P-k között legyen $h(m, n)$; azaz minden m-re és n-re $P_{h(m,n)}$ eggyel kevesebb változós mint Q_n, és a változók (t. i. $x_1, x_2, \ldots, x_r$) bármely értékére

$$Q_n(m, x_1, x_2, \ldots, x_r) = P_{h(m,n)}(x_1, x_2, \ldots, x_r).$$

Ha a Q-k megszámlálása is a szokásos (a P-ből a konstansok kihagyásával adódó), akkor könnyen belátható, hogy h rekurzív függvény.

Mármost legyen adva számelméleti problémánk egy állítólagos megoldása, amiről be akarjuk bizonyítani, hogy nem helyes megoldás; a megfelelő karakterisztikus függvény legyen $g(n)$ úgy, hogy tehát az állítólagos megoldás úgy szól, hogy $P_n = 0$ akkor és csak akkor oldható meg, ha $g(n) = 1$ (különben pedig $g(n) = 0$). Tekintsük a $g\big(h(n, n)\big)$ függvényt. (Ha a $g\big(h(m, n)\big)$ függvény értékeit kétdimenziósan rendezzük:

$$\begin{array}{llll} \boldsymbol{g\big(h(1,1)\big)}, & g\big(h(2,1)\big), & g\big(h(3,1)\big), & \ldots \\ g\big(h(1,2)\big), & \boldsymbol{g\big(h(2,2)\big)}, & g\big(h(3,2)\big), & \ldots \\ g\big(h(1,3)\big), & g\big(h(2,3)\big), & \boldsymbol{g\big(h(3,3)\big)}, & \ldots \\ \ldots & \ldots & \ldots & \end{array}$$

akkor $g\big(h(n, n)\big)$ éppen a főátló szolgáltatta függvény). Nyilván g-vel és h-val együtt $g\big(h(n, n)\big)$ is általános rekurzív függvénye n-nek. Ehhez is tartozna tehát egy $P^{(g(h))}(t; x_1, x_2, \ldots, x_r)$ polinom úgy, hogy $g\big(h(n, n)\big) = 0$ ekvivalens azzal, hogy

$$P^{(g(h))}(n; x_1, x_2, \ldots, x_r) = 0$$

megoldható az x-ekre. Ha n helyébe is változót írunk, legyen $P^{(g(h))}(x_1; x_2, \ldots, x_{r+1})$ a (Q) sorozat polinomjai közül az s-edik, azaz $P^{(g(h))}(x_1; x_2, \ldots, x_{r+1}) = Q_s(x_1, x_2, \ldots, x_{r+1})$; akkor a h függvény definíciója szerint bármely n-re $P^{(g(h))}(n; x_1, x_2, \ldots, x_r) = Q_s(n, x_1, \ldots, x_r) = P_{h(n,s)}(x_1, x_2, \ldots, x_r)$. E szerint $g\big(h(n, n)\big) = 0$ ekvivalens azzal, hogy $P_{h(n,s)} = 0$ megoldható; speciálisan $n = s$-re $g\big(h(s, s)\big) = 0$ azzal, hogy $P_{h(s,s)} = 0$ megoldható. Azonban $g\big(h(s, s)\big)$

egy konkrét általános rekurzív függvény értéke egy konkrét helyen, tehát kiszámítható és így véges számú lépésben kideríthető, hogy 0-e vagy 1 (más értéket a feltevés szerint g nem vesz fel); ha 0, akkor tehát bebizonyult, hogy $P_{h(s,\,s)} = 0$ megoldható, ha 1, akkor meg nem oldható meg, pedig ha $g(n)$ számelméleti problémánknak helyes megoldásához tartozna, akkor fordítva lenne: $g(n)$ oly és csak oly n argumentumokra volna 1, melyekre $P_n = 0$ megoldható.

Amint említettem, a vázolt gondolatot nem a diofantikus egyenletek megoldhatósági problémáján, hanem egy egyenesen e célra készült önmagában nem érdekes problémán sikerült Churchnek keresztülvinnie, de megmutatta, hogy következik belőle egy önmagában is rendkívül érdekes probléma eldönthetetlensége: az u. n. «Entscheidungsproblem»-é.[21] Ennek általános megoldhatóságában alig is hitt valaki, mégis frappáns eredmény, hogy megoldhatatlanságát matematikai módszerekkel be lehetett bizonyítani.[22]

9. Dolgozatom tárgya az axiomatikus módszer gyarlóságainak kimutatása volt. Kiderült, hogy az axiomatikus módszer sohasem fogja meg szorosan azt, amit megfogni akar és hogy minden axiómarendszernek vannak eldönthetetlen problémái. Ez elég pesszimista képet ad Hilbert biztonságérzésével szemben, aki szerint minden matematikust ez a hit vezet: «Itt a probléma, keresd a megoldását, tisztán gondolkodás útján megtalálhatod, mert a matematikában nincs ignorabimus!» Én mégis azt hiszem,

---

[21] (*K*) 84—85. old.

[22] Kalmár László vette észre a hasonlóságot a Church-féle megoldhatatlan probléma és a diofantikus egyenletek megoldhatóságának problémája között; e hasonlóság alapján igyekszik bebizonyítani az utóbbi, konkrét számelméleti, probléma megoldhatatlanságát is. Erre vonatkozó, még befejezetlen, vizsgálatait szives volt rendelkezésemre bocsátani és ezzel megkönnyítette számomra a Church-féle gondolatmenet vázolását. Ugyancsak Kalmár mutatta meg egy eddig még nem publikált dolgozatában, hogy a Church-féle gondolatmenet közvetlenül alkalmazható az eldöntésprobléma megoldhatatlanságának bebizonyítására, míg Church ezt közvetve, az ő komplikáltabb problémája eldönthetetlenségének felhasználásával mutatta meg.

hogy a vázolt bizonyítások oly szépek, hogy nem kelthetnek pesszimisztikus hangulatot. A helyzet tisztázása nem szegényebbé válást, hanem gazdagodást jelent. És, hogy ezt a helyzetet a legtisztább matematikai eszközökkel sikerült megvilágítani, az mégiscsak a matematika és speciálisan a HILBERT-féle bizonyításelmélet diadala és legszebb teljesítményei közé tartozik. Hogy az «ignorabimus»-t precízen be lehet bizonyítani, az talán nem kevésbbé szép, mintha a matematikában tényleg nem volna «ignorabimus». Hadd fejezzem be CANTOR szavaival, melyek a halmazelmélet támadóinak szóltak: «Könnyen megeshetik velük, hogy éppen ott, ahol halálos sebet akarnak ejteni a tudományon, ennek egy új ága virágzik ki hirtelen a szemük előtt, ha lehet még szebb, és gazdagabb jövőt ígérő minden régebbinél».

Péter Rózsa.

DIE SCHRANKEN DER AXIOMATISCHEN METHODE.*

In der Mathematik bedarf man zur Definition eines Begriffes andere Begriffe, zum Beweis eines Satzes andere Sätze. In jedem Zweig der Mathematik müssen dabei gewisse Sätze als Grundsätze, Axiome, gewisse Begriffe als Grundbegriffe angenommen werden; letztere werden durch die Axiome sozusagen implizite definiert. Es ist nicht zu erwarten, dass diese Definition die Grundbegriffe eindeutig bestimmt, diese haben ja meist gar nicht einen exakt-eindeutigen Sinn; doch es ist eine naturgemässe Forderung, dass das Axiomensystem die betrachtete Wissenschaft möglichst *vollständig* vertreten soll.

---

* Vortrag, gehalten am 8. März 1940. im Kolloqium des Instituts für Theoretische Physik der Universität zu Budapest, als Fortsetzung eines ebenda gehaltenen Vortrags von LÁSZLÓ KALMÁR über Zielsetzungen und Ergebnisse der HILBERTschen Beweistheorie; s. die vorangehende Arbeit in dieser Zeitschrift. In der Arbeit von KALMÁR wird die axiomatische Methode, der Aussagenkalkul und der logische Funktionenkalkul eingehend besprochen, darum lasse ich die auf diese bezügliche Einleitung meines Vortrags weg, dafür behandle ich eingehender das absolut unentscheidbare Problem von CHURCH.

Die Forderung der Vollständigkeit lässt sich auf verschiedene Weisen präzisieren. Z. B. als die Forderung, das dass Axiomensystem *monomorph* sein soll, d. h., dass sich die Elemente und Beziehungen zweier Modelle, welche beide dem Axiomensystem genügen, so einander zuordnen lassen sollen, dass falls dabei die Elemente $a, b, c, \ldots$ in $a', b', c', \ldots$ die Beziehung R in R' übergehen und zwischen den Elementen $a, b, c, \ldots$ die Beziehung R besteht, so zwischen $a', b', c', \ldots$ die Beziehung R' bestehen soll. Seit langem hatten die Mathematiker an dem Monomorphismus der verschiedenen mathematischen Axiomensysteme geglaubt. Diese Glaube wurde durch SKOLEM in zwei Richtungen widerlegt. SKOLEMS Ergebnis lässt sich so zusammenfassen, dass *die axiomatische Methode einerseits zu wenig, andererseits zu viel ergreift.* Zu wenig, in folgendem Sinne: mit Benutzung eines LÖWENHEIMschen Satzes hat SKOLEM in 1922. bewiesen, dass es zu einem jeden widerspruchsfreien Axiomensystem ein abzählbares Mcde gibt, welche diesem genügt; dies gilt also z. B. auch für ein beliebiges Axiomensystem der Mengenlehre. Da unter den Grundbegriffen nichts inhaltliches zu verstehen ist, ist kein Grund da, unter der Gesamtheit der Mengen etwas anderes zu verstehen, als SKOLEMS abzählbares Modell und so kann es nicht gelingen, das Überabzählbare exaktaxiomatisch zu ergreifen. Der inhaltliche Mengenbegriff liefert freilich auch ein gutes, und zwar überabzählbares Modell für das Axiomensystem; wird er zugelassen, so gibt es für das System sogar betreffs der Mächtigkeit verschiedene Modelle, also ist dieses gewiss nicht monomorph. Dasselbe gilt auch für die möglichen Axiomensysteme der reellen Zahlen, und für die der Geometrie.

Andererseits hat SKOLEM in 1933. bewiesen, dass einem beliebigen Axiomensystem für die natürliche Zahlenreihe, so eng man es auch fassen will, immer auch Modelle genügen, welche einen höheren Ordnungstyp als ω besitzen. Hier ergreift also die axiomatische Methode zu viel.

Eine andere Fassung der Forderung der Vollständigkeit ist die der *Kategorizität.* Ein Axiomensystem heisst kategorisch, wenn jeder Satz, der sich mittels seiner Grundbegriffe formulieren lässt, in ihm entweder beweisbar, oder widerlegbar ist. Das ist eine sehr starke Forderung; für das Bruchstück der Arithmetik, welche als einzige Operation die Addition enthält, wurde ihr Bestehen von PRESBURGER bewiesen; wird jedoch auch die Multiplikation zugelassen, so lassen sich auch bis heute nicht entschiedene Sätze im System formulieren, wie z. B. der grosse FERMATsche Satz, und bereits diese Tatsache machte die Beweisbarkeit der Kategorizität sehr zweifelhaft. Dennoch

hat die Mehrheit der Mathematiker zu jeder Zeit in der Entscheidbarkeit der verschiedenen mathematischen Probleme geglaubt. Diese Glaube wurde durch GÖDEL und CHURCH widerlegt. GÖDEL gab in 1931. ein arithmetisches Problem an, von dem er mit tadellosen Mitteln bewiesen hat, dass es im üblichen Axiomensystem der Arithmetik, ja sogar auch in einem viel weiteren System *unentscheidbar* ist. Er bewies auch, dass sich die Widerspruchsfreiheit des Systems im selben System formulieren, doch nicht entscheiden lässt. Von seinem speziellen Axiomensystem nützte er dabei nur solche Eigenschaften aus, die sämtlichen, für die Arithmetik aufgestellten Axiomensystemen zukommen, also gibt es in jedem solchen System unentscheidbare Probleme, freilich in jedem System andere.

Nun gab CHURCH in 1936. ein Bespiel für ein Problem an, welches unabhängig von einem zugrunde gelegten Axiomensystem unentscheidbar ist, also mit recht *absolut-unentscheidbar* genannt werden kann. Es folgt daraus auch die Unentscheidbarkeit des logischen Entscheidungsproblems.

Es hat sich also herausgestellt, dass die Axiomensysteme nie genau das ergreifen können, was sie ergreifen wollen, und dass es in allen Sytemen unentscheidbare Probleme gibt. Diese Ergebnisse widerlegen zwar HILBERTS Glauben: «In der Mathematik gibt es kein Ignorabimus»; dass sich aber diese Tatsachen mit den HILBERTschen rein mathematischen Methoden klarlegen liessen, dass man das «Ignorabimus» in der Mathematik mit mathematischen Mitteln streng beweisen kann, ist vielleicht nicht weniger schön, als wenn es in der Mathematik kein «Ignorabimus» gäbe.

Rózsa Péter.