Transzcendens számok

Szakdolgozat

Írta: **Pálfy Máté**
Matematika BSc, matematikus szakirány

Témavezető: **Kós Géza**
egyetemi adjunktus
Analízis Tanszék

Eötvös Loránd Tudományegyetem
Természettudományi Kar
Budapest 2019.

Köszönetnyílvánítás

Szeretnék kronologikus sorrendben haladni a köszönetnyílvánításban mindazok felé, akiknek köszönhetem, hogy ez a dolgozat elkészült.

Középiskolai Tanáromnak, Holló Gábornak, aki megkedveltette velem a matematikát, és lenyűgöző óráival mondhatni a matekhoz bilincselt.

Családomnak és Zsófinak, akik támogattak a tanulmányaim alatt, még hogy ha ez a közös idő rovására is ment. Zsófinak külön hála a lelki támogatásért és amiért egy-egy finom étellel újra erőt adott a tanuláshoz.

Frenkel Péter és Pelikán József kiváló algebra órái miatt, amik egy-egy ponton igen hasznosak voltak a szakdolgozatom megírásához.

Elekes Márton és Keleti Tamásnak a nagyszerű "Valós függvénytan szeminárium" című órái miatt, tulajdonképpen egy ott elhangzott feladatból alakult ki a 3-ik fejezet, és egy-egy ponton a szakdolgozatomba beválogatott írások az ott kialakított ízlésemet tükrözik.

Laczkovich Miklósnak, aki rendelkezésemre bocsátotta Tóth Dávid írását, amit az Átdarabolások című órája alapján gépelt le.

Végül, de nem utolsó sorban Kós Gézának, aki gondosan átnézte a szakdolgozatomat, és az utolsó félév során sok más, nem feltétlenül a szakdolgozatomhoz kapcsolódó témában is a segítségemre tudott lenni.

Tartalomjegyzék

1. Bevezetés

Transzcendens számokkal sokan foglalkoztak igen neves matematikusok, többek között Weierstrass, Gelfond, Schneider, Lang, Baker és még lehetne sorolni. Az első kérdés, ami felmerült velük kapcsolatban, hogy egyáltalán léteznek-e? Liouville konstruált legelőször transzcendens számot, majd rövidesen belátták egy-egy neves állandóról - π és e - hogy transzcendensek. Később Cantor megmutatta, hogy bizonyos értelemben hemzsegnek a transzcendens számok. Mára a transzcendens számok elmélete egy külön kutatási területté nőtte ki magát a matematikának.

A dolgozat 2. fejezetében a Liouville számokkal foglalkozom, mérték és kategória szempontjából legfőképpen, majd kategorikus tulajdonságukból egy-egy szép tulajdonságukat bemutatjuk. A 3. fejezet paradox halmazokkal foglalkozik, ami egy Valós függvénytan szemináriumon elhangzott kérdésből nőtte ki magát, hogy vajon létezik-e nemüres $A \subset \mathbb{R}^2$, ami felbontható $A = B \sqcup C$ alakban, ahol A, B, C mindegyike egybevágó. A megdöbbentő válasz az, hogy igen, és a konstrukció maga nem is igazán nehéz, de használ transzcendens számokat, a fejezet végére eljutunk a Banach-Tarski paradoxonhoz.

A 4 és 5-ik fejezet klasszikus transzcendens eredményekkel foglalkozik, ehhez írodott a 6-ik fejezet, a Függelék, amiben egy-egy állítást bizonyítunk, ami a 4 és 5-ik fejezetben hangzik el bizonyítás nélkül.

Lényegében a fejezetek függetlenek egymástól, így olvashatóak különkülön, az 5-ös fejezetben használok egy-egy fogalmat, amit már a 4-es fejezetben bevezettem. Persze egy-egy alapvető fogalom csak egy helyen lett definiálva, amit a későbbiekben használunk minden ismétlés nélkül.

2. Liouville számok

A fejezet elején szereplő tételek és állítások nagyrésze [6]-ból származik.

2.1. definíció. *Egy α komplex számot algebrainak hívunk $\mathbb{Q}$ felett, ha gyöke egy nemzérus racionális együtthatós polinomnak.*

Nyílvánvalóan a racionális helyett egész együtthatós polinomot is mondhattunk volna, a kettő ekvivalens. Innentől kezdve ha egy számra csak annyit mondunk, hogy algebrai, akkor azt úgy értjük, hogy, algebrai $\mathbb{Q}$ felett.

Könnyen látható, hogy ha egy szám algebrai, akkor azok a polinomok, amiknek gyöke α, azok egy ideált alkotnak, de tetszőleges test feletti polinomgyűrű főideálgyűrű, azaz egy elemmel generált, mi esetünkben csak annyi lesz fontos, hogy minden polinom, aminek gyöke az α előáll $f(x)p(x)$, ahol $p(x)$ az ideál generátoreleme, továbbá p-t választhatjuk úgy, hogy főegyütthatója 1 legyen. Ekkor ezt az egyértelműen meghatározott polinomot hívják α minimálpolinomjának $\mathbb{Q}$ felett, és ha $p(x)$ foka n, akkor az α-t n-edfokú algebrai számnak nevezzük. A minimálpolinom irreducibilis, mivel ha felbomlana alacsonyabb fokú polinomok szorzatára, akkor azok közül az egyiknek gyöke volna α, így p nem lehetne az ideál egy generátor eleme.

Gyakran fogjuk használni az α egész minimálpolinomja kifejezést, ami az α minimálpolinomjának egy olyan pozitív egész számszorosa, hogy az egész együtthatós, de primitív polinom, természetesen ez a polinom is egyértelműen meghatározott. Transzcendens számok a nem algebrai számok. Az α szám konjugáltjai alatt a minimálpolinomjának összes gyökét értjük.

Sokáig megoldatlan kérdés volt, hogy egyáltalán létezik-e transzcendens szám. Sokan vélték úgy a 18 században, hogy mind az e és a π is transzcendensek, ezek a 19 századra váltak csak tételekké, amelyek Hermite és Lindemann nevéhez fűződnek. Az első lépéseket a transzcendens számok ismerete felé vezető úton Liouville tette meg a következő tétellel:

2.2. tétel. *Legyen α egy $n > 1$ n-edfokú algebrai szám, ekkor létezik egy c konstans α-tól függően, hogy $\forall \frac{p}{q} \in \mathbb{Q}$-ra:*

$$\left|\alpha - \frac{p}{q}\right| \geq \frac{c}{q^n}$$

Bizonyítás. Jelölje α konjugáltjait $\alpha = \alpha_1, \alpha_2 ..... \alpha_n$ valamint legyen $f(x) = a_n x^n + ... + a_1 x + a_0$ az α egész minimálpolinomja. A tétel minden nemvalós komplex számra triviális, így feletehető, hogy α valós.

Az $f(\frac{p}{q}) \neq 0$ tetszőleges $\frac{p}{q} \in \mathbb{Q}$-ra (különben f reducibilis lenne), a következő becsléseket tehetjük meg:

$$(*) \quad \left| f(\alpha) - f(\frac{p}{q}) \right| = \left| f(\frac{p}{q}) \right| = \left| \frac{a_n p^n + a_{n-1} p^{n-1} q + ...a_1 p q^{n-1} + a_0 q^n}{q^n} \right| \geq \frac{1}{q^n}$$

felhasználva, hogy a számláló egy nemnulla egész szám. Jelölje továbbá $M = max\{ \mid \alpha_1 \mid, ... \mid \alpha_n \mid \}$ a legnagyobb aszolút értékű konjugáltat.

I. eset: $\mid \frac{p}{q} \mid > 2M \Rightarrow \mid \alpha - \frac{p}{q} \mid \geq M \geq \frac{M}{q^n}$.

II. eset: $\mid \frac{p}{q} \mid \leq 2M$, ekkor $\left| \alpha_i - \frac{p}{q} \right| \leq 3M$ és (*)-ot használva:

$$\mid \alpha - \frac{p}{q} \mid \geq \frac{1}{\mid a_n \mid \prod_{j=2}^{n} \mid \alpha_j - \frac{p}{q} \mid q^n} \geq \frac{1}{|a_n| \, (3M)^{n-1}}$$

A két esetet összevetve kapjuk, hogy $c := min\{M, \frac{1}{|a_n|(3M)^{n-1}}\}$ jó választás. □

Ezzel kézhez kaptunk egy tételt, amivel könnyedén konstruálhatunk transzcendens számokat, legyen $\alpha = \sum_{n=0}^{\infty} \frac{1}{10^{n!}}$, meggmutatjuk ugyanis, hogy α-t túl jól közelítik a részletösszegei, így nem lehet algebrai szám.

Indirekt okoskodunk, tegyük fel, hogy α egy m-edfokú algebrai szám, és tekintsük a $\frac{p_k}{q_k} = \sum_{j=0}^{k} \frac{1}{10^{k!}}$ közelítő törteket, ahol $q_k = 10^{k!}$. Ekkor azt kapjuk, hogy:

$$\frac{c_\alpha}{10^{k!m}} \leq \mid \alpha - \frac{p_k}{q_k} \mid = \sum_{n=k+1}^{\infty} \frac{1}{10^{(k+1)!}} < \frac{10}{9} \frac{1}{10^{(k+1)!}}$$

ami nagy k-ra ellentmondás. Többek között ez a bizonyítás is vezetett el a valós számok egy igen fontos és érdekes részhalmazához, a Liouville számokhoz.

2.3. definíció. *$\alpha \in \mathbb{R}$ számot n-ed rendben jól közelíthetőnek nevezzük, ha létezik végtelen sok $\frac{p_k}{q_k}$, hogy $\mid \alpha - \frac{p_k}{q_k} \mid < \frac{1}{q_k^n}$.*

2.4. definíció. *Azon irracionális számokat, amelyek minden n-re jólközelíthetőek, Liouville számoknak hívjuk. Jelük:* $\mathbb{L}$

Könnyen látható, hogy minden Liouville szám transzcendens, mivel ha létezne egy α algebrai Liouville szám, legyen mondjuk n-edfokú, akkor n+1-re létezne végtelen sok $\frac{p_k}{q_k}$, hogy

$$\frac{c_\alpha}{q_k^n} \leq \mid \alpha - \frac{p_k}{q_k} \mid < \frac{1}{q_k^{n+1}}$$

mivel $k \longrightarrow \infty$ esetén $q_k \longrightarrow \infty$ is teljesül, így megint elég nagy k-ra ellentmondást kapunk. Most szükségünk lesz a 2.2.tétel egy "több dimenziós" változatára:

2.5. lemma. *Legyen* $f \in \mathbb{Z}[x_1, ..., x_n]$ *egy nemzérus n-változós polinom, i-edik változójában nézve* d_i*-fokú. Legyen* $\underline{\alpha} \in \mathbb{R}^n$ *olyan, hogy* $f(\underline{\alpha}) = 0$*. Ekkor bármely* $\underline{\beta} \in \mathbb{Q}^n, \quad \underline{\beta} = (\frac{a_1}{b_1}, ..., \frac{a_n}{b_n})$*-re a következő két eshetőség áll fenn:*

$$f(\underline{\beta}) = 0$$

vagy

$$\mid \underline{\alpha} - \underline{\beta} \mid > \frac{c}{b_1^{d_1}.....b_n^{d_n}}$$

ahol c egy $\underline{\alpha}$*-tól és az f polinomtól függő konstans.*

Bizonyítás. Ha $f(\underline{\beta}) = 0$ esetben vagyunk, nincsen mit bizonyítani, feltehetjük tehát, hogy $f(\underline{\beta}) \neq 0$. Legyen $B = \{\underline{x} \in \mathbb{R}^n :\mid \underline{\alpha} - \underline{x} \mid \leq 1\}$, az $\underline{\alpha}$ 1 sugarú zárt környezete. Ha $\underline{\beta} \notin B$, akkor $\mid \underline{\alpha} - \underline{\beta} \mid > 1 \geq \frac{1}{b_1^{d_1}.....b_n^{d_n}}$.

Ha $\underline{\beta} \in B$, akkor a Lagrange-középértéktételt használva kapjuk valamely $c \in [\underline{\alpha}, \underline{\beta}]$ szakaszon lévő pontra, hogy fennáll a következő egyenlőség:

$$(*) \quad \Big|f(\underline{\alpha}) - f(\underline{\beta})\Big| = \Big|f(\underline{\beta})\Big| = \Big|\langle f'(c), \underline{\beta} - \underline{\alpha}\rangle\Big|$$

a Cauchy-Schwarz egyenlőtlenséggel tovább becsülve (*)-ot:

$$\Big|f(\underline{\alpha}) - f(\underline{\beta})\Big| \leq \big|f'(c)\big|\Big|\underline{\beta} - \underline{\alpha}\Big| \leq$$

$$\leq \max_{x\in B}\left|f'(x)\right|\left|\underline{\beta}-\underline{\alpha}\right| < K\left|\underline{\beta}-\underline{\alpha}\right|$$

ahol K egy konstans, ami az f' B-n vett maximumánál nagyobb. Na de

$$\left|f(\underline{\alpha})-f(\underline{\beta})\right| = \left|f(\underline{\beta})\right| \geq \frac{1}{b_1^{d_1}....b_n^{d_n}}$$

mivel $f(\underline{\beta}) \neq 0$, így közös nevezőre való hozás után a számlálóban egy nemnulla egész szám áll. Innét a $min\{1, \frac{1}{K}\}$ c-nek jó választás. □

2.6. definíció. *Legyen adott egy $\mathbb{F} \leq \mathbb{K}$ testbővítés, valamint legyen legyen $V \subset \mathbb{K}$. Ekkor V-t algebrailag függetlennek nevezzük $\mathbb{F}$ felett, ha bármely véges sok eleme V-nek nem gyöke egyetlen egy nemzérus $\mathbb{F}$-beli együtthatós polinomnak sem.*

Ezzel a terminológiával élve tehát egy darab transzcendens szám mindig algebrailag független $\mathbb{Q}$ felett, sőt, $\mathbb{A}$ felett is.

2.7. tétel. *(Adams tétele) Legyen p és q két relatív prím pozitív egész, nagyobbak, mint egy. Ekkor az $\alpha = \sum_{n=1}^{\infty} \frac{1}{p^{n!}}$ és a $\beta = \sum_{n=1}^{\infty} \frac{1}{q^{n!}}$ Liouville számok algebrailag függetlnek $\mathbb{Q}$ felett.*

Bizonyítás. Indirekt tegyük fel, hogy létezik egy $f(x, y)$ nemzérus egész együtthatós polinom (definíció szerint racionális együtthatós, de felszorozhatunk a nevezőkkel), amelyre $f(\alpha, \beta) = 0$. Vezessük be a következő jelöléseket: $R_N = \sum_{n=1}^{N} \frac{1}{p^{n!}}$ és $S_N = \sum_{n=1}^{N} \frac{1}{p^{n!}}$. Azt állítjuk, hogy végtelen sok N-re $f(R_N, S_N) \neq 0$.

Ha ez nem így volna, akkor egy indextől kezdődve minden N-re $f(R_N, S_N) = 0$ állna. Valamint R_N és S_N definíciójából fakadóan fennállnak:

$$(*) \quad \frac{1}{p^{(N+1)!}} < \sum_{n=(N+1)!}^{\infty} \frac{1}{p^{n!}} = \mid \alpha - R_N \mid < \frac{2}{p^{(N+1)!}}$$

és

$$(**) \quad \frac{1}{q^{(N+1)!}} < \sum_{n=(N+1)!}^{\infty} \frac{1}{q^{n!}} = \mid \beta - S_N \mid < \frac{2}{q^{(N+1)!}}$$

Írjuk fel f-et a következő alakban: $f(x, y) = \sum_{I} C_I (x-\alpha)^i (y-\beta)^j$, ahol I végigfut a nemnegatív egész index párokon és csak véges sok C_I nemnulla.

Habár jelenleg most elvesztettük azt, hogy az együtthatók egészek, kihasználhatjuk a tétel feltételei közül azt, hogy p és q relatív prímek, méghozzá úgy, hogy legyenek $d_{i,j} := p^i q^j$ pozitív egészek. Ezek különböző (i,j) párok esetén különbözőek! Jelölje most $I_0 = (i_0, j_0) \in I$ azt az indexet, amelyre d_{I_0} minimális a $C_{I_0} \neq 0$ feltétel mellett, ilyen van, mivel különbözőek a $d_{i,j}$-k. Most pedig megbecsüljük C_{I_0}-t:

$$0 <\mid C_{I_0} \mid \leq \sum_{I\setminus\{I_0\}} \frac{|C_I||R_N-\alpha|^i|S_N-\beta|^j}{|R_N-\alpha|^{i_0}|S_N-\beta|^{j_0}} \leq \sum_{I\setminus\{I_0\}} \frac{|C_I| \mid \frac{2}{p^{(N+1)!}} \mid^i \mid \frac{2}{q^{(N+1)!}} \mid^j}{\mid \frac{1}{p^{(N+1)!}} \mid^{i_0} \mid \frac{1}{q^{(N+1)!}} \mid^{j_0}}$$

$$\leq \sum_{I\setminus\{I_0\}} 2^D (\frac{d_{I_0}}{d_I})^{(N+1)!}$$

ahol az első egyenlőtlenség definíció szerint igaz, a második az $f(R_N, S_N) = 0$ feltételből és sok háromszög egyenlőtlenségből adódik. A harmadikban használtuk (*) és (**)-t, másrészről az utolsó egyenlőtlenségben D-vel jelöltük a polinom legmagasabb fokú tagját. Emlékeztetve megint arra, hogy d_{I_0} szigorúan a legkisebb szám volt, elég nagy N-re ellentmondást kapunk a $\mathbb{C}_{I_0} \neq 0$ feltétellel, így valóban végtelen sok N esetén $f(R_N, S_N) \neq 0$ teljesül.

Így viszont feltéve mondjuk, hogy p $>$ q, akkor az előző 2.5-ös lemma állítása szerint kapjuk, hogy

$$\mid (\alpha,\beta) - (R_N, S_N) \mid \geq \frac{c}{p^{N!D}}$$

ahol c nem függ R_N és S_N-től. Másrészről ismét (*) és (**)-ot használva azt kapjuk, hogy

$$\big|(\alpha,\beta) - (R_N, S_N)\big| \leq \frac{\widetilde{c}}{q^{(N+1)!}}$$

N-re ismét ellentmondásra jutottunk, így α és β valóban algebrailag függetlenek. □

Megjegyzés: Tulajdonképpen a $d_{i,j}$ számok páronként különbözősége elegendő volt a tételünk bizonyításához, így könnyedén általánosítható a tétel végtelen sok páronként relatív prím egészekre, amelyek nagyobbak, mint 1 (mivel végtelen sok elem algebrai függetlensége a véges részhalmazainak füg-

getlenségével van definiálva).

Most pedig megvizsgáljuk a Liouville számok szerkezetét Lebesgue mérték és kategória szempontjából.

Állítás: A Liouville számok Lebesgue-nullmértékű halmazt alkotnak.

Bizonyítás. Vegyük észre, hogy a Liouville számok egész számra való eltolás esetén invariánsak, ismét Liouville számot kapnánk, így elegendő megmutatni, hogy a $[0;1]$-beli Liouville számok nullmértékűek. Itt pedig egy erősebb állítás is igaz lesz, még pedig az, hogy már a harmadrendben jól közelíthető számok is nullmértékűek.

Vezessük be $q \geq 1$-re a $V_q = \cup_{p=0}^{q}(\frac{p}{q} - \frac{1}{q^3}, \frac{p}{q} + \frac{1}{q^3})$ halmazt. Világos, hogy $V = \cap_{q\geq 1} V_q$ megegyezik a [0;1]-beli 3-ad rendben jól közelíthető valós számokkal (részletesebben: azok lennének a 3-ad rendben jól közelíthető számok, amik végtelen sok V_q-ban szerepelnek, de ezek monoton csökkenő halmaz sorozatot adnak, így valóban a metszet adja ki a 3-ad rendben jól közelíthető $[0;1]$-beli számokat). Nézzük meg a V_q halmaz Lebesgue-mértékét:

$$\lambda(V_q) \leq \sum_{p=0}^{q} \lambda(\frac{p}{q} - \frac{1}{q^3}, \frac{p}{q} + \frac{1}{q^3}) = (q+1)\frac{2}{q^3} \leq \frac{4}{q^2}$$

Speciálisan azt kaptuk, hogy $\sum_{q=1}^{\infty} \lambda(V_q) < \infty$, így a Borel-Cantelli lemma szerint azok a számok, amelyek végtelen sok V_q-ban fordulnak elő, azaz V-ben, nullmértékűek. □

Következmény: Van olyan transzcendens szám, ami nem Liouville szám.

Most kategória szempontjából fogjuk megvizsgálni a Liouville számokat, ki fog derülni, hogy ők egy reziduális halmazt alkotnak (azaz egy első kategóriájú halmaz komplementerét), és emiatt rengeteg érdekes tulajdonságukra fog fény derülni a Liouville számoknak, mint például hogy kontinuum sok Liouville szám van és bármely valós szám előáll kettő Liouville szám összegeként.

Ezen tulajdonság nem annyira a Liouville számok speciális definíciójából fakad, hanem inkább mert ők kategória szempontjából igen nagy, reziduális halmazt alkotnak (azon belül is sűrű nyíltak metszete lesz, mint látni fogjuk),

mielőtt ezt belátnánk, könnyen meggondolható, hogy az alábbi jellemzése a Liouville számoknak ekvivalens a fentebbi definícióval:

$$\mathbb{L} = \{\alpha \in \mathbb{R} \setminus \mathbb{Q} \mid \quad \exists \quad \frac{p_1}{q_1}, \frac{p_2}{q_2}, ..., \frac{p_n}{q_n}, ... \in \mathbb{Q}, q_j > 1 \quad \left|\alpha - \frac{p_n}{q_n}\right| < \frac{1}{q_n^n}\}$$

Ebben a megfogalmazásban a következő féleképpen írhatjuk fel a Liouville számokat, legyen: $V_n = \bigcup_{q\geq 2} \bigcup_{p\in\mathbb{Z}} (\frac{p}{q} - \frac{1}{q^n}, \frac{p}{q} + \frac{1}{q^n}) \setminus \{\frac{p}{q}\}$, ekkor $\mathbb{L}$ pontosan azokból az elemekből áll, amelyik végtelen sok V_n-ben van benne, de pont mint előbb, V_n-nek monoton fogyóak, így: $\mathbb{L} = \bigcap_{n\geq 1} V_n$.

Minden n-re V_n nyílt, mivel nyílt intervallumok uniójaként áll elő, sűrű, mert lezárása tartalmazza a racionális számokat. A Baire-kategória tétel miatt $\mathbb{L}$ sűrű, mi több, reziduális, mivel egy első kategóriájú halmaz komplementere.

Most néhány topológiai állítást nézünk meg, amik reziduális halmazokról szólnak, így ezek eredményét egyszerűen csak alkalmazzuk a Liouville számokra, mint speciális esetként felhasználva, hogy ők reziduális halmazt alkotnak (mivel sűrű nyíltak metszete). Mint ígértük, megmutatjuk, hogy sok Liouville szám van:

2.8. tétel. *Minden reziduális halmaz számossága kontinuum számossgágú*

Bizonyítás. Egy Cantor-típusú halmaz létezését fogjuk megmutatni, ami alatt egymásba skatulyázott korlátos zárt intervallumok rendszerét értjük, melyek egy-egy végtelen hosszú 0-1 sorozattal kódolhatóak el, amelyek ismerten kontinuum számosságúak.
Legyen tehát G egy reziduális halmaz, valamint $F = \mathbb{R} \setminus G = \bigcup_{i=1}^{\infty} F_i$, ahol mindegyes F_i egy sehol sem sűrű halmaz. Ekkor tekintsünk egy tetszőleges nemelfajuló korlátos zárt intervallumot, I-t. Mivel F_1 sehol sem sűrű, ezért 1. lépésként tudunk nyomban választani kettő darab F_1-től diszjunkt zárt, nemelfajuló részintervallumát I-nek, legyenek ezek I_0 és I_1.

2. lépésként F_2 sehol sem sűrűségét kihasználva kapjuk, hogy mind I_0 és I_1-ben tudunk találni ismét kettő darab nem elfajuló, diszjunkt zárt részintervallumot, jelölje ezeket: $I_{0,0}, I_{0,1}, I_{1,0}, I_{1,1}$. Teljesen hasonlóan tudunk n-ik lépésben nemelfajuló, F_n-től diszjunkt zárt részintervallumait választani

az n-1-ik lépésben megalkotott intervallumoknak felhasználva F_n sehol sem sűrűségét, az indexelése ezen 2^n-en darab intervallumnak pedig az összes n hosszú 0-1 sorozattal történik, még hozzá ha egy n hosszú 0-1 sorozat kiterjeszt egy n-1 hosszú 0-1 sorozatot, akkor az n hosszú címkét kapó intervallum részintervalluma az n-1 hosszú címkét kapó $(n-1)$-ik lépésben keletkezett intervallumnak.

Így minden egyes végtelen hosszú 0-1 sorozat egy-egy fogyó kompakt halmazcsaládot kódol el, melyeknek bármely véges metszete nemüres, így az összes metszete nemüres. Különböző 0-1 sorozatokhoz különböző metszetek tartoznak, mivel az első hely, legyen ez az n-ik, ahol két darab különböző 0-1 sorozat eltér egymástól, tekintve a n-ik lépésben megfelelő intervallumokat, azok diszjunktak. Az egész F diszjunkt ezen összes 0-1 sorozattal kódolt metszetek uniójától, mivel az n-ik lépésben tárolt intervallumok unióitól már F_n diszjunkt, az n-ik lépésben lévő intervallumok uniói, pedig lefedik az összes 0-1 sorozattal kódolt metszetek elemit. □

Következmény: A Liouville számok számossága kontinuum.

A most következendő állítások/tételek/definíciók mindegyik [1]-ból származik.

2.9. definíció. *Legyen X egy topologikus tér és $f : X \longrightarrow \mathbb{R}$ folytonos függvény, azt mondjuk, hogy f sehol sem lokálisan konstans,ha minden nemüres nyílt halmazán az X-nek a függvény nem konstans.*

2.10. definíció. *Egy X topologikus tér egy $x \in X$ pontjában lokálisan összefüggő, ha minden x-et tartalmazó V nyílt környezetre létezik egy U környezete x-nek, hogy U összefüggő és $U \subset V$. Az X tér lokálisan összefüggő, ha minden $x \in X$ pontjában lokálisan összefüggő.*

2.11. definíció. *X egy Baire-tér, ha teljesül benne a Baire-kategória tétel, azaz sűrű nyíltak metszete sűrű.*

Példák Baire terekre: Teljes metrikus terek, a számegyenes nemelfajuló intervallumai, kompakt T_2-terek. (Azt, hogy ezek valóban Baire-terek, a függelékben részletezzük).

2.12. lemma. *Legyen X egy lokálisan összefüggő Baire-tér, $I \subset \mathbb{R}$ egy nemüres és nem egy pontból álló intervallum, valamint legyen Γ egy megszámlálható halmaz. $\forall \gamma \in \Gamma$ adva van egy G_γ halmaz, ami sűrű nyílt halmazok metszete I-ben.*

Ezeken kívül $\forall \gamma \in \Gamma$-ra adottak nekünk egy $f_\gamma : X \longrightarrow I$ folytonos, sehol sem lokálisan konstans függvények.

Ekkor $\bigcap_{\gamma \in \Gamma} f_\gamma^{-1}(G_\gamma)$ egy sűrű nyílt halmazok metszetéből álló halmaz X-ben (speciálisan reziduális).

Bizonyítás. Elég belátni, hogy $f_\gamma^{-1}(G_\gamma)$ az sűrű nyílt halmazok metszete X-ben $\forall\gamma$-ra, mivel megszámlálhatóan sok megszámlálható sok sűrű nyílt halmaz metszete szimplán csak megszámlálhatóan sok sűrű nyílt metszete. Legyen $G_\gamma = \bigcap_{j \in \mathbb{N}} V_j$, ahol V_j sűrű nyílt halmaz I-ben. Mivel f folytonos, ezért $f_\gamma^{-1}(V_j)$ nyílt X-ben, illetve $f_\gamma^{-1}(G_\gamma) = \bigcap_{j \in \mathbb{N}} f_\gamma^{-1}(V_j)$, így elegendő belátni, hogy $f_\gamma^{-1}(V_j)$ sűrű X-ben.

Ehhez meg kell mutatnunk, hogy tetszőleges $B \subset X$ nem üres nyílt halmazába belemetsz a $B_j = f_\gamma^{-1}(V_j)$. Itt feltehetjük, hogy B egy összefüggő halmaz, mivel ha nem az lenne, akkor B nemüressége miatt tartalmazna pontot,nevezzük ezt x-nek, és a tér lokális összefüggősége miatt lenne egy B-beli, nyílt összefüggő nemüres környezete x-nek, és ha abba belemetsz B_j, akkor B-be is.

Tegyük fel tehát, hogy B összefüggő, ekkor mivel f sehol sem lokálisan konstans, de folytonos, így f(B) egy összefüggő részhalmaza I-nek, ami nem egy pontú, így egy részintervalluma I-nek, azaz létezik $(a, b) \subset I$, hogy $(a, b) \subset f_\gamma(B)$. V_j sűrű I-ben, így $\emptyset \neq V_j \cap (a, b) \subset f_\gamma(B) \cap (a, b)$, tehát $B_j = f_\gamma^{-1}(V_j)$ valóban belemetsz B-be. □

Most egy állítás keretében összefoglaljuk, hogy mit nyertünk az előző lemmával, kifejezetten a Liouville számokra koncentrálva:

Állítás: Legyen $I \subset \mathbb{R}$ egy nemüres belsejű intervallum, $0 \notin \Gamma$ egy megszámlálható halmaz, $\forall \gamma \in \Gamma$ adva van egy $f_\gamma : I \longrightarrow \mathbb{R}$ folytonos, sehol sem lokálisan konstans függvény. Ekkor létezik kontinuum sok $x \in I$ Liouville szám, amelyre $f_\gamma(x)$ Liouville szám $\forall \gamma \in \Gamma$ esetén.

Bizonyítás. Legyen $\Gamma' = \Gamma \cup \{0\}$ és $f_0(x) = x$, $\forall x \in I$. Mivel I egy intervallum, ezért ő egy lokálisan összefüggő Baire-tér, Γ' megszámlálható és válasszuk $G_\gamma = \mathbb{L}$-et $\forall \gamma \in \Gamma'$ esetén. Ekkor az előző lemma éppen azt mondja, hogy $H = \bigcap_{\gamma \in \Gamma'} f_\gamma^{-1}(\mathbb{L})$ sűrű nyílt halmazok metszete I-ben. Ekkor $H \subset \mathbb{L}$ az f_0 választása miatt, de H számossága kontinuum, mivel H egy reziduális halmaz. □

Ezek után ajándékba kapjuk Erdős Pál két híres tételét Liouville számokról, mégpedig:

2.13. tétel. *Minden valós szám előáll két darab Liouville szám összegeként és minden nemnulla valós szám előáll két darab Liouville szám szorzataként.*

Bizonyítás. Legyen $t \in \mathbb{R}$ tetszőleges, $I = \mathbb{R}$ és $f_t(x) = t - x$ választással kapjuk az előbbi állításból, hogy van $x \in \mathbb{L}$, hogy $f_t(x)$ is Liouville. A másodikat tetszőles $t > 0$ mellett $I = (0, \infty)$ és $f_t(x) = \frac{t}{x}$ választással nyerjük. □

Megjegyzés: ennél erősebb állítást nyertünk, minden x valós számra kontinuum sok Liouville számpárt tudunk mondani, melyek összegeként előáll x, analóg állítás igaz a szorzatra.

Megjegyzés: A fenti tételt rengeteg féle függvényre bevethetjük, például $t > 0$-ra $I = (0, \sqrt{t})$ és $f(x) = \sqrt{t^2 - x^2}$ választással nyerjük, hogy minden pozitív valós szám előáll, mint két Liouville szám négyzetösszege (persze ismét kontinuum sok féleképpen).

3. Váratlan halmazok a síkon és a térben

A most következő fejezetben a bizonyításokat [8] és [9] alapján dolgoztam fel.

Az előző fejezetben kiderült, hogy kontinuum sok transzcendens szám van (Liouville számból is már kontinuum sok volt), ennek ellenére nem a fenti bizonyítás a legismeretesebb erre, hanem ami George Cantor-tól származik, ami egyszerű eleganciával mutat rá, hogy pontosan mennyi transzcendens szám van.

Jelöljük $H_{k,n}$-el azokat komplex számokat, amelyek egy legfeljebb n-edfokú nemnulla egész együtthatós polinom gyökei, azaz:

$$H_{k,n} = \{z \in \mathbb{C} : \exists p(x) \in \mathbb{Z}[x], 0 \leq \deg p \leq n, p(x) = a_0 + ... + a_n x^n, \sum_{j=0}^{n} \left|a_j\right| < k\}$$

Világos, hogy $H_{k,n}$ véges minden k és n esetén, valamint hogy: $\mathbb{A} = \bigcup_{k>0,n>0} H_{k,n}$. Azaz az algebrai számok halmaza megszámlálható! Így szükségképpen kontinuum sok transzcendens szám létezik.

3.1. tétel. *Létezik a síkon egy $\emptyset \neq A = B \cup C$ halmaz, ahol B és C diszjunkt felbontása A-nak úgy, hogy mind A, B és C egybevágó egymással.*

Bizonyítás. Legyen

$$H := \{a_0 + ... + a_n x^n : a_0 \leq 0, ..., a_n \leq 0, \quad a_0, ...a_n \in \mathbb{Z}\}$$

a nempozitív egész együtthatós polinomok halmaza, amely a fenti Cantor-féle bizonyítás alapján ugyanazzal a gondolatmenettel igazolható, hogy megszámlálható. Vegyünk egy tetszőleges $\omega \in \mathbb{C}, |\omega| = 1$ transzcendens számot, amit szintén meg tudunk tenni, mivel egységhosszú komplex számok kontinuum sokan vannak. Legyen

$$A := \{p(\omega) = a_0 + ...a_n \omega^n : p(x) \in H\}$$

Mivel ω transzcendens, így különböző H-beli polinomok esetén különböző

$p(\omega)$ értékeket kapunk. Ekkor azt kell észrevenni, hogy a

$$B := \omega A = \{\omega a \mid a \in A\}$$

és a

$$C := -1 + A = \{-1 + a \mid a \in A\}$$

halmazok az A-val mind egybevágó halmazok, mivel forgatással és eltolással keletkeztek A-ból. Most belátjuk, hogy $A = B \cup C$.

Ehhez tulajdonképpen csak azt kell észrevenni, hogy így B nem más, mint az összes olyan H-beli polinom kiértékelve ω helyen, ahol a polinom konstans tagja 0, míg C azon komplex számokból áll, amelyek olyan H-beli polinom ω helyen vett kiértékeléseként keletkeztek, ahol a konstans tag szigorúan negatív. Ebből már világos, hogy $A = B \cup C$. □

A következőben a gömbfelszínen fogunk mutatni egy halmazt igazán váratlan tulajdonságokkal, aminek a létezését egy szintén váratlan részcsoport felbukkanása okozza a tér egybevágóságai között (speciálisan SO(3)-ban találjuk majd), ezen csoport felfedezéséhez fogunk használni transzcendens számokat, és majd megmutatjuk, hogyan lehet egy ilyen eredményt paradox halmaz elkészítésére alkalmazni.

3.2. tétel. *Az SO(3) csoport tartalmaz egy 2 rangú szabadcsoportot.*

Bizonyítás. Legyen

$$A = \begin{bmatrix} \cos\varphi & -\sin\varphi & 0 \\ \sin\varphi & \cos\varphi & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

és

$$B = \begin{bmatrix} 1 & 0 & 0 \\ 0 & \cos\varphi & -\sin\varphi \\ 0 & \sin\varphi & \cos\varphi \end{bmatrix}$$

azaz az x- és y-tengelyek körüli φ szögű elforgatás, ha φ-t úgy választjuk, hogy $\cos\varphi$ transzcendens, akkor A és B egy kettő rangú szabadcsoportot fognak alkotni. Ilyen választás persze van, mivel a cos értékkészlete kontinuum

számosságú. Ahhoz, hogy belássuk, hogy ez igaz, ahhoz a következő tipusú "szavakra" kell belátnunk, hogy nem adják vissza az identitást:
(a_1) A^n, (a_2) B^m
(b_1) $A^{n_1}B^{m_1}.....A^{n_k}$, (b_2) $B^{n_1}A^{m_1}.....B^{n_k}$
(c_1) $A^{n_1}B^{m_1}.....A^{n_k}B^{m_k}$, (c_2) $B^{n_1}A^{m_1}.....B^{n_k}A^{m_k}$

ahol $n, m \in \mathbb{Z}^* = \mathbb{Z} \setminus \{0\}$, $k > 0$, $n_i, m_i \in \mathbb{Z}^*$ $i = 1, ...k$.
A fenti esetekből a szimmetria miatt nyílván elegendő igazolni $(a_1), (b_1), (c_1)$ eseteket. Ezekhez igénybe vesszük az úgy nevezett első és másodfajú Csebisev polinomkat, amelyek a következőképpen értelmezendőek:

Az elsőfajú Csebisev polinom:

$$\begin{aligned} T_0(x) &:= 1 \\ T_1(x) &:= x \\ T_n(x) &:= 2xT_n(x) - T_{n-1}(x), \quad \text{ha } n \geq 2. \end{aligned}$$

Teljesen világos, hogy T_n egész együtthatós, $n \geq 1$ esetén a főegyütthatója 2^{n-1}. $T_n(\cos x) = \cos(nx)$, is teljesül, ami már nem teljesen nyílvánvaló, de könnyen belátható indukcióval:
$n = 0$-ra és $n = 1$-re triviálisan teljesül, ha feltesszük, hogy $n \geq 2$ és az állítás igaz $\forall k < n$-re, akkor:

$$T_n(\cos(x)) = 2\cos(x)T_{n-1}(\cos(x)) - T_{n-2}(\cos(x)) \overset{\text{ind. felt}}{=}$$

$$2\cos(x)\cos((n-1)x) - \cos((n-2)x) = \cos(nx)$$

felhasználva, hogy $2\cos(\alpha)\cos(\beta) = \cos(\alpha+\beta) + \cos(\alpha-\beta)$.

A másodfajú Csebisev polinomokat az alábbi módon definiáljuk:

$$\begin{aligned} U_0(x) &:= 1 \\ U_1(x) &:= 2x \\ U_n(x) &:= 2xU_{n-1}(x) - U_{n-2}(x), \text{ha } n \geq 2. \end{aligned}$$

A következő állítások mind igazak a másodfajú Csebisev polinomokra, és úgy

igazolható, mint a fenti esetben: U_n főegyüttható ja 2^n és $U_n(\cos(x))\sin(x) = \sin((n+1)x)$.

Ekkor $n \in \mathbb{Z}^*$-ra az A mátrix geometriai jelentéséből (vagy teljes indukcióval) igaz:

$$A^n = \begin{bmatrix} \cos(n\varphi) & -\sin(n\varphi) & 0 \\ \sin(n\varphi) & \cos(n\varphi) & 0 \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} \cos(|n|\,\varphi) & -\sin(n\varphi) & 0 \\ \sin(n\varphi) & \cos(n\varphi) & 0 \\ 0 & 0 & 1 \end{bmatrix} =$$

$$= \begin{bmatrix} T_{|n|}(cos\varphi) & -\sin(n\varphi) & 0 \\ sin(n\varphi) & \cos(n\varphi) & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$

hasonló állítás teljesül B-re is. Vegyük észre, hogy a mátrix bal felső eleme nem lehet egyenlő eggyel, mivel akkor $\cos\varphi$ gyöke lenne egy egész együtthatós polinomnak, ellentmondva annak transzcendens választásának! Ezzel az (a_1) esetet le is tudtuk.

A (b_1) esetnek úgy látunk neki, hogy feltesszük indirekt: $A^{n_1}B^{m_1}.....A^{n_k} = id = id_{\mathbb{R}^3}$. Ekkor a fenti (a_1) eset miatt $k > 1$. Szorozzuk balról A^{n_k}-val, jobbról pedig A^{-n_k}-val, ekkor a következő típusú egyenlőséghez jutunk:

$$A^m B^{l_1} A^{t_2} .....B^{l_{k-1}} = 0$$

ahol m egész szám, $l_1, t_2, ...l_{k-1} \in \mathbb{Z}^*$. Ha $m \neq 0$, akkor egy (c_2) típusú egyenlőséghez jutunk, amit hamarosan megtárgyalunk, hogy nem lehet, míg ha m=0, akkor egy (b_2) típusú egyenlőséghez jutunk, így azt kapjuk, hogy folyamatosan alkalmazva egy (b_1) vagy egy (b_2) típusú egyenlőségre a fenti redukciós lépéseket, hogy balról és jobbról beszorzunk egy elemmel és annak inverzével, előbb vagy utóbb $(a_1), (a_2), (c_1), (c_2)$ tipusú egyenlőséghez jutunk, így elegendő már csak igazolni az előzőek fényében, hogy egy (c_1) típusú egyenlőség sem állhat fennt!

Ahhoz, hogy (c_1) típusú egyenlőség sem állhat fennt, előrevetítjük, hogy

milyen alakú lesz $A^{n_1}B^{m_1}.....A^{n_k}B^{m_k}$:

$$(*)A^{n_1}B^{m_1}.....A^{n_k}B^{m_k} = 2^{t-2k}\begin{bmatrix} v(\cos\varphi) & c_1 \cdot g(\cos\varphi)\sin\varphi & c_2 \cdot h(\cos\varphi) \\ f(\cos\varphi)\sin\varphi & l(\cos\varphi) & c_3 \cdot w(\cos\varphi) \\ q(\cos\varphi) & s(\cos\varphi)\sin\varphi & z(\cos\varphi) \end{bmatrix}$$

ahol $c_1 = -\operatorname{sgn}(n_1)$, $c_2 = \operatorname{sgn}(n_1 m_s)$, $c_3 = -\operatorname{sgn}(m_s)$ valamint v, g, h, f, l, w, q, s, z racionális együtthatós polinomok, $t = |n_1| + ... + |m_s|$, valamint $\deg(h) = t$, $\deg(g) = \deg(w) = t-1$ és $\deg(v), \deg(z) \leq t-1$ és az összes többi polinom foka is legfeljebb akkora, mint h foka. Mindezek mellett még g, h és w polinomok főegyütthatója pedig 1. Mostantól kezdve a jobb felső sarokban lévő tagra fogunk koncentrálni, ehhez persze egy ideig nyomon kell követnünk a mátrix szorzásban keletkezett összes elemet. Emlékeztetünk, hogy :

$$A^n = \begin{bmatrix} \cos(n\varphi) & -\sin(n\varphi) & 0 \\ \sin(n\varphi) & \cos(n\varphi) & 0 \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} \cos(\mid n \mid \varphi) & -\operatorname{sgn}(n)\sin(\mid n \mid \varphi) & 0 \\ \operatorname{sgn}(n)\sin(\mid n \mid \varphi) & \cos(\mid n \mid \varphi) & 0 \\ 0 & 0 & 1 \end{bmatrix} =$$

$$= \begin{bmatrix} T_{|n|}(\cos\varphi) & -\operatorname{sgn}(n)U_{|n|-1}(\cos\varphi)\sin(\varphi) & 0 \\ \operatorname{sgn}(n)U_{|n|-1}(\cos\varphi)\sin\varphi & T_{|n|}(\cos\varphi) & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

$$B^m = \begin{bmatrix} 1 & 0 & 0 \\ 0 & \cos(m\varphi) & -\sin(m\varphi) \\ 0 & \sin(m\varphi) & \cos(m\varphi) \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & \cos(\mid m \mid \varphi) & -\operatorname{sgn}(m)\sin(\mid m \mid \varphi) \\ 0 & \operatorname{sgn}(m)\sin(\mid m \mid \varphi) & \cos(\mid m \mid \varphi) \end{bmatrix} =$$

$$= \begin{bmatrix} 1 & 0 & 0 \\ 0 & T_{|m|}(\cos\varphi) & -\operatorname{sgn}(m)U_{|m|-1}(\cos\varphi)\sin\varphi \\ 0 & \operatorname{sgn}(m)U_{|m|-1}(\cos\varphi)\sin\varphi & T_{|m|}\cos\varphi \end{bmatrix}$$

Most pedig megnézzük az A^nB^m mátrixok szorzatát, majd végül megál-

lapítjuk $A^{n_1}B^{m_1}.....A^{n_k}B^{m_k}$ értékét k-ra való indukcióval.

$$A^nB^m = \begin{bmatrix} T_{|n|}(\cos\varphi) & \begin{bmatrix} -\operatorname{sgn}(n)T_{|m|}(\cos\varphi)\cdot \\ \cdot U_{|n|-1}(\cos\varphi)\sin\varphi \end{bmatrix} & \begin{bmatrix} \operatorname{sgn}(nm)U_{|n|-1}(\cos\varphi)\cdot \\ \cdot U_{|m|-1}(\cos\varphi)\sin^2\varphi \end{bmatrix} \\ \operatorname{sgn}(n)U_{|n|-1}(\cos\varphi)\sin\varphi & T_{|n|}(\cos\varphi)T_{|m|}(\cos\varphi) & \begin{bmatrix} -\operatorname{sgn}(m)T_{|n|}(\cos\varphi)\cdot \\ \cdot U_{|m|-1}(\cos\varphi)\sin\varphi \end{bmatrix} \\ 0 & \operatorname{sgn}(m)U_{|m|-1}(\cos\varphi)\sin\varphi & T_{|m|}(\cos\varphi) \end{bmatrix}$$

Ami tulajdonképpen egy mechanikus mátrix szorzásból adódik. Itt $\sin^2\varphi = 1-\cos^2\varphi$ felhasználásával, illetve a Csebisev-polinomok főegyütthatóira tett megállapítással már meg is kaptuk k=1 esetén (*)-ot. Innentől indukcióval bizonyítunk, feltesszük, hogy (k-1)-re igaz az állítás, és felhasználjuk fentti számolásainkat, ahol t jelöli most a $|n_1|+...+|m_{k-1}|$ összeget:

$$A^{n_1}B^{m_1}.....A^{n_k}B^{m_k} = (A^{n_1}B^{m_1}...A^{n_{k-1}}B^{n_{k-1}})A^{n_k}B^{m_k} =$$

$$= 2^{t-2(k-1)} \begin{bmatrix} v(\cos\varphi) & c_1\cdot g(\cos\varphi)\sin\varphi & c_2\cdot h(\cos\varphi) \\ f(\cos\varphi)\sin\varphi & l(\cos\varphi) & c_3\cdot w(\cos\varphi) \\ q(\cos\varphi) & s(\cos\varphi)\sin\varphi & z(\cos\varphi) \end{bmatrix} \cdot$$

$$\cdot \begin{bmatrix} \left[T_{|n_k|}(cos\varphi)\right] & \begin{bmatrix} -\operatorname{sgn}(n_k)T_{|m_k|}(\cos\varphi)\cdot \\ \cdot U_{|n_k|-1}(\cos\varphi)\sin\varphi \end{bmatrix} & \begin{bmatrix} \operatorname{sgn}(n_km_k)U_{|n_k|-1}(\cos\varphi)\cdot \\ \cdot U_{|m_k|-1}(\cos\varphi)\sin^2\varphi \end{bmatrix} \\ \operatorname{sgn}(n_k)U_{|n_k|-1}(\cos\varphi)\sin\varphi & T_{|n_k|}(\cos\varphi)T_{|m_k|}(\cos\varphi) & \begin{bmatrix} -\operatorname{sgn}(m_k)T_{|n_k|}(\cos\varphi)\cdot \\ \cdot U_{|m_k|-1}(\cos\varphi)\sin\varphi \end{bmatrix} \\ 0 & \operatorname{sgn}(m_k)U_{|m_k|-1}(\cos\varphi)\sin\varphi & \left[T_{|m_k|}(\cos\varphi)\right] \end{bmatrix}$$

Amiből számolással adódik az állítás, kiszámoljuk most a jobb felső elemét a mátrixnak, mivel úgyis arra fogunk koncentrálni az ellentmondás érdekében, lássuk a számolást (l_{1_3}-al jelölve a kérdéses elemet):

$$l_{1_3} = v(\cos\varphi)\cdot\operatorname{sgn}(n_km_k)U_{|n_k-1|}(\cos\varphi)U_{|m_k-1|}(\cos\varphi)(1-\cos^2\varphi)+c_1\cdot g(\cos\varphi)\sin\varphi\cdot$$

$$\cdot(-\operatorname{sgn}(m_k))T_{|n_k|}(\cos\varphi)\cdot U_{|m_k|-1}(cos\varphi)\sin\varphi + c_2\cdot h(\cos\varphi)\cdot T_{|m_k|}(\cos\varphi).$$

Innét már csak azt kell észrevenni, hogy a második tag fogja adni a szigorúan

legnagyobb tagot abban az értelemben, hogy az $t' = t + |n_k| + |m_k|$ fokú polinomot fog adni, $\cos\varphi$ helyettesítéssel, míg az összeg többi tagja legfeljebb $t'-1$-edfokú polinomokba $cos\varphi$-nek való behelyettesítésével keletkezik. A sgn függvény multiplikativitása miatt úgyszíntén az előreígért $\mathrm{sgn}(n_1 m_k)$ szorzat is kiemelhető, valamint a csebsiev polinomok főegyüttthatója, hogy a végén 1 főegyüttthatós polinom álljon a mátrix jobb felső sarkában, ahogyan azt ígértük.
A végső ellentmondást tehát az adja a (c_1) típusú egyenlőség lehetetlenségére, hogy az abban az esetben felírt $A^{n_1}B^{m_1}.....A^{n_k}B^{m_k}$ kifejezés mátrixának jobb felső sarkában álló elem nem lehet 0 a $\cos\varphi$ transzcendens választása miatt, azaz biztosan nem kapjuk vissza az egységmátrixot. □

1.Megjegyzés: Ismert, hogy SO(3) elemei geometriailag úgy képzelhetőek, hogy a térben egy origón átmenő egyenes körül forgatunk valamilyen szöggel, ezek után gyakran SO(3) elemeire mint forgatások fogunk hivatkozni.

2.Megjegyzés: A p=3 a legkisebb dimenzió, amikor $\mathbb{R}^p$ egybevágóságai tartalmaznak egy szabadcsoportot, ugyanis p=1 esetén ha a és b egy-egy egybevágóságai $\mathbb{R}$-nek, akkor a^2 és ^{2} is egy-egy eltolás, így speciálisan kommutálnak is: $a^2b^2 = b^2a^2$.
A p=2 esetben úgy járhatunk el, hogy egy a egybevágóság előáll, mint $x \longmapsto Ax + c$, ahol A egy ortogonális 2x2-es mátrix, c pedig 2-dimenziós vektor. Ekkor az a^2 egy olyan egybevágóságot ad, amely most úgy szintén $Ax + c$ alakú, de most már A egy egy olyan ortogonális mátrix, aminek determinánsa 1, azaz egy forgatást reprezentál az origó körül. Hasonlóan egy másik b egybevágóságra $b^2 = Bx + d$ alakú, ahol B egy forgatás az origó körül, d pedig egy eltolás. Kiszámolva az $a^2b^2a^{-2}b^{-2}$ és $a^{-2}b^{-2}a^2b^2$ egybevágóságokat mindkettő egy-egy eltolást eredményez, speciálisan az előbbi két kifejezés kommutál egymással, így nem létezhet szabadcsoport $\mathbb{R}^2$ egybevágóságai között sem.

3. Megjegyzés: Ismert, hogy ha a és b két darab "elem", amelyek egy szabadcsoportot generálnak $F_{a,b}$-t, akkor $G_n = \{b^{-i}ab^i \mid i = 0, 1, , , , n-1\}$ csoportok egy-egy n-edrendű szabadcsoportot alkotnak $F_{a,b}$-n belül, mi több, $G_\infty = \{b^{-i}ab^i \mid i \in \mathbb{N}\}$ egy $\aleph_0$ rangú szabadcsoportot ad $F_{a,b}$-ben, így a fenti

tétellel igen sokféle rangú szabadcsoport létezését garantáltuk, hamarosan ezt a rangot még tovább fogjuk növelni, a maximálisig, azaz kontinuum rangú szabadcsoportot fogunk mutatni!

Most pedig az előző igen hosszú tétel segítségével megmutatjuk, milyen típusú váratlan halmaz konstruálható meg, majd a konstrukción keresztül eljutunk a híres Banach-Tarski féle paradoxonhoz is. S a következőkben az egységgömb felszínét fogja jelölni, azaz $S = \{x \in \mathbb{R}^3 \mid |x| = 1\}$. Egy gyors lemmát még megfontolunk, hogy az utána következő tétel bizonyítása gondtalanul mehessen végbe:

3.3. lemma. *Legyen $C \subset S$ egy megszámlálható részhalmaza a gömbfelületnek, ekkor $\exists \varrho \in SO(3)$, hogy $\varrho(C) \cap C = \emptyset$.*

Bizonyítás. Soroljuk fel C elemeit: $C = \{c_1, c_2, ...\}$, ekkor az $\{(x, -x) \mid x \in S\}$ párok halmaza kontinuum sokan vannak, így létezik egy origón átmenő f egyenes, amely átmegy egy (x,-x), $x \in S$ pontpáron és diszjunk C elemitől. Ekkor kontinuum sok lehetőségünk van megválasztani egy forgatást f körül, mivel a forgatás szöge α szabadon választahtó a $[0, 2\pi)$ intervallumból.

Egy ϱ f körüli forgatást nevezzünk rossznak, ha $\exists(i, j)$, hogy $\varrho(c_i) = c_j$, de minden (i, j) párra pontosan egy f körüli forgatás létezik, ami c_i-t c_j-be viszi, így a rossz f körüli forgatások száma legfeljebb az (i,j) párok számosságával egyezik meg, azaz megszámlálható sok rossz forgatásunk van. Ekkor bármilyen NEM rossz forgatás f körül JÓ, abban az értelemben, hogy $\varrho(C) \cap C = \emptyset$.

□

3.4. tétel. *Létezik egy $A \subset S$, a következő tulajdonságokkal:*
(a) S tartalmaz végtelen sok A-val egybevágó, páronként diszjunkt példányt.
(b) S lefedhető A 4 egybevágó példányával!

Bizonyítás. Jegyezzük meg gyorsan, hogy ez a halmaz igazán paradox tulajdonságokkal rendelkezik, és szinte mint minden olyan halmaz, amely valamilyen az intuíciónkkal szembemenő tulajdonsággal rendelkezik, ennek a megkonstruálása is használni fogja a kiválasztási axiómát.

Mivel SO(3) éppen a gömb (irányítástartó) izometriái, bármilyen $\varphi \in SO(3)$ bármilyen $A \subset S$-et önmagával egybevágó példányba viszi át ($\varphi(A)$-ba). Legyenek most $\varphi, \psi \in SO(3)$ olyanok, hogy szabadcsoportot alkossanak, jelöljük ezt G-vel. Ilyen választás a 3.2-es tétel miatt létezik. Ekkor G elemei a következőféleképpen néznek ki, amit használni is fogunk:

$$(*) \quad G = \{\varphi^{a_1}\psi^{a_2}....\psi^{a_2 n} \mid n \geq 2, \quad a_2, ...a_{2n-1} \in \mathbb{Z} \setminus \{0\}\}$$

Emlékeztetjük az olvasót, hogy a fenti alakú (redukált szavak) formális kifejezések midegyike különböző forgatást definiál.

Nevezzük $x, y \in S$ pontokat ekvivalensnek, ha:

$$x, y \in S\text{-re} \quad x \sim y \iff \exists g \in G, g(x) = y$$

Nyílvánvalóan egy ekvivalenciarelációt kaptunk ezzel, így S előáll páronként diszjunk osztályok uniójaként áll elő. Bármely az identitástól különböző G-beli elemnek két darab fixpontja van, a forgatástengely döféspontjai a gömbfelszínen. Jelölje továbbá e a G csoport egységelemét (azaz az üres kifejezést).

Tekintsük a következő a halmazt:

$$C = \{x \in S \mid \exists g \in G \setminus \{e\}, g(x) = x\}$$

Világos, hogy C megszámlálható, mivel már maga G is az volt, és minden nemüres kifejezéshez kettő darab fixpont tartozott.

Ha $x \in C$, $x \sim y \implies y \in C$, mivel legyen $g, h \in G$ olyanok, hogy $g(x) = x, g \neq e$ és $h(x) = y$, ekkor egyrészről $hgh^{-1} \neq e$, mert akkor $g = h^{-1}h = e$ lenne, másrészről pedig: $hgh^{-1}(y) = hg(x) = h(x) = y$, azaz $y \in C$ valóban teljesül. Így kaptuk tehát azt, hogy mind C és $S \setminus C$ ekvivalencia osztályok uniójaként áll elő. U jelölje (*) azon forgatásait, ahol $a_1 \neq 0$, Illetve $H \subset S \setminus C$ olyan, hogy minden egyes $S \setminus C$-beli ekvivalencia osztályból pontosan egy elemet tartalmaznak. Ekkor

$$A := \{\chi(x) \mid \chi \in U, x \in H\}$$

halmaz teljesíteni fogja a tétel kritériumait.

Először az (a) részt vizsgáljuk, azaz hogy végtelen sok páronként diszjunkt egybevágó példánya megtalálható A-nak S-en. Állítjuk, hogy a $\psi^n(A)$, $n = 1, 2, 3...$ halmazok páronként diszjunktak. Ha nem így lenne, akkor létezik n és m különböző pozitív egészek, $x_1 \in H$ és $x_2 \in H$, $\chi_1 \in U$ és $\chi_2 \in U$ úgy, hogy:

$$(1) \quad \psi^n \chi_1(x_1) = \psi^m \chi_2(x_2)$$

Ez utóbbi abból fakad, ha $y \in \psi^n(A) \cap \psi^m(A)$, akkor $y = \psi^n(y_1) = \psi^m(y_2)$ valamely $y_1, y_2 \in A$-ra, de A választása miatt $y_1 = \chi_1(x_1)$, $\chi_1 \in U, x_1 \in H$ alakú és hasonlóan ez elmondható y_2-re. (1)-et átrendezve kapjuk, hogy $x_1 = \chi_1^{-1}\psi^{n-m}\chi_2(x_2)$, de most jön a lényeg! Előbbi azt jelenti, hogy $x_1 \sim x_2$, de H minden ekvivalencia osztályból legfeljebb egy elemet tartalmazott (egészen konrétan az $S \setminus C$ ekvivalencia osztályaiból tartalmazott pontosan egy elemet), így a $\chi_1^{-1}\psi^{n-m}\chi_2$ transzformációnak az identitásnak kell lennie, ami nem lehet amiatt, hogy χ_1^{-1} utolsó helyén φ-nek egy nemnulla kitevős hatványa áll (mert U-ban csak olyan transzformációk voltak, amikben az első helyen φ kitevője nemnulla), hasonlóan χ_2 első helyén ismét φ-nek egy nemnulla kitevős hatványa áll, de őket elválasztja ψ^{n-m}, ahol $n \neq m$, így ez a transzformáció nem reprezentálhatja az identitást.
Most rátérünk a (b) részre, miszerint lefedjük S-t A négy egybevágó példányával. Először lefedjük $S \setminus C$-t, mégpedig a következőféleképpen:

$$S \setminus C \subset A \cup \varphi(A)$$

Ez utóbbit bizonyítja következő gondolatmenet: ha $x \in S \setminus C$ tetszőleges, akkor $\exists g \in G$ és $y \in H$, hogy $x = g(y)$, ha g olyan, hogy az első helyen φ kitevője nemnulla, akkor $g \in U$, és így $x \in A$. Ha $g \notin U$, akkor $\varphi^{-1}g \in U$, és így $\varphi^{-1}g(y) = \varphi^{-1}(x) \in A$, azaz $x \in \varphi(A)$. Ha $x \in C$, akkor az előző 3.3-as lemma alapján $\exists \varrho \in SO(3)$, hogy $\varrho(C) \cap C = \emptyset$. Ekkor $\varrho(C) \subset S \setminus C \subset A \cup \varphi(A)$, amiből nyílvánvaló, hogy $C \subset \varrho^{-1}(A) \cup \varrho^{-1}\varphi(A)$.
Mindent egybevetve kaptuk, hogy:

$$S = (S \setminus C) \cup C \subset A \cup \varphi(A) \cup \varrho^{-1}(A) \cup \varrho^{-1}\varphi(A)$$

amivel a tétel bizonyítása kész.

□

Egyik következménye az előző tételnek, hogy bizonyos típusú mérték nem létezését lehet levezetni belőle, ami persze nem meglepő annak, aki ismeri a Vitali-halmazt és társait.

3.5. tétel. *Nincsen olyan mérték S-en, amely az S összes részhalmazán van értelmezve, invariáns az egybevágóságokra nézve és S mértéke* 4π.

Bizonyítás. Ha volna ilyen, nevezzük ezt m-nek, akkor az előző részben látott A választásával kapjuk, hogy mivel van A-ból végtelen sok páronként diszjunkt, vele egybevágó példány, nevezzük őket: $A_1, A_2, ...$, akkor kapjuk az egybevágóság invarianciával felhasználva, hogy:

$$\bigcup_{i=1}^{\infty} A_i \subset S \Longrightarrow \sum_{i=1}^{\infty} m(A_i) = m(\bigcup_{i=1}^{\infty} A_i) \leq m(S) = 4\pi \Longrightarrow m(A) = 0$$

Viszont A négy egybevágó példánya lefedi S-et, amiből $\frac{1}{4}m(S) \leq m(A) \Longrightarrow \pi \leq m(A)$, ami ellentmondás.

□

Most a beígért Banach-Tarski paradoxon fog következni, ami mára tulajdonképpen tétel, régen ez a konstrukció azon célból született, hogy a kiválasztási axióma helytelenségét mutassa meg, mára ez úgy él a fejekben, mint a kiválasztási axióma egy különös következménye. Mivel gömbök átdarabolhatóságáról szól a tétel, így előtte meg kellene mondanunk, hogy mit értünk átdarabolhatóság alatt, és néhány alapvető állítást megnézünk, amikre szükségünk lesz a tétel bizonyítása során.

3.6. definíció. *$A, B \subset \mathbb{R}^n$ halmazokat egymásba átdarabolhatónak nevezzük, ha $\exists n > 0$, hogy $A = \bigsqcup_{i=1}^{n} A_i$ és $B = \bigsqcup_{i=1}^{n} B_i$ és A_i egybevágó B_i-vel. Ezt így jelöljük: $A \equiv B$, ha hangsúlyozni szeretnénk, hogy hány darabra osztottuk szét a halmazainkat, akkor $A \equiv_n B$-t írunk, ahol az n index utal a darabok számára*

Könnyen megmutatható, hogy $\equiv$ ekvivalenciareláció, tranzitivitás az egyetlen picit meggondolandóbb, de könnyen igazolható, hogy ha $A \equiv_n B$ és $B \equiv_k C \Longrightarrow A \equiv_{n+k} C$.Ez utóbbi megfontolást nem részletezzük, hanem egy hasonló jellegű állítást látunk be. Ehhez előtte emlékeztetjük az olvasót a Cantor-Schröder-Bersntein tételre, mely szerint ha adott két halmaz A és B, valamint f egy $f : A \longrightarrow B$ injekció és g egy $g : B \longrightarrow A$ injekció, akkor létezik egy h bijekció A és B között, még hozzá a következő speciális alakban: $A = A_1 \cup A_2$ és $B = B_1 \cup B_2$ két-két diszjunkt halmazra való felbontása A-nak és B-nek, ahol $f(A_1) = B_1$ és $g(B_2) = A_2$, azaz f bijekció A_1 és B_1 között, míg g egy bijekció B_2 és A_2 között. Íme az állítás:

$$\text{Ha } A \equiv_n X \subset B \text{ és } B \equiv_k Y \subset A, \text{ akkor} A \equiv_{n+k} B.$$

Bizonyítás. Legyen tehát $A = \bigsqcup_{i=1}^{n} A_i$ és $X = \bigsqcup_{i=1}^{n} X_i$ felbontások az átdarabolhatóság deinícióri szerint, valamint jelöljük φ_i-vel azt az egybevágóságot, amely A_i-t B_i-be viszi. Hasonlóan legyen $B = \bigsqcup_{j=1}^{k} B_j$ és $Y = \bigsqcup_{j=1}^{n} Y_j$ és az itt megefelelő egybevágóságot pedig ψ_j fogja jelölni. Ekkor az $f(a) = \varphi_i(a)$, $a \in A_i$ egyenlőséggel értelmezett függvény egy injenkciója A-nak B-be (mivel minden egybevágóság injektív), és $g(b) = \psi_j(b), b \in B_j$ pedig B egy injekciója A-ba. Ekkor $A = C_1 \cup C_2$ és $B = D_1 \cup D_2$ legyenek olyan két-két részre való partícionálása A-nak és B-nek, amit a Cantor-Schröder-Bersntein tétel garantál, ekkor kapjuk a következőket:

$$A = C_1 \cup C_2 = C_1 \cup g(D_2) = \bigcup_{i=1}^{n} (A_i \cap C_1) \cup \bigcup_{j=1}^{k} \psi_j(B_j \cap D_2)$$

és

$$B = D_1 \cup D_2 = f(C_1) \cup D_2 = \bigcup_{i=1}^{n} \varphi_i(A_i \cap C_1) \cup \bigcup_{j=1}^{k} (B_j \cap D_2)$$

Amiből világos, hogy a φ_i és ψ_j^{-1} egybevágóság a megfelelő halmazok között biztosítják a kívánt egybevágóságokat. □

3.7. tétel. *Legyen B_1 és B_2 két azonos sugarú diszjunkt gömb a térben, ekkor $B_1 \equiv_{10} (B_1 \cup B_2)$.*

Bizonyítás. O fogja jelölni a B_1 gömb középpontját, és S a felszínét. Bevezetjük továbbá az r_x jelölést $x \in S$ esetére, ami azt a szakaszt fogja jelölni, ami összeköti O-t x-el, kihagyva belőle O-t. Ezzel az új jelöléssel pedig $C \subset S$ esetén a C^* halmazt a következőképpen deiniáljuk: $C^* = \bigcup_{x \in C} r_x$. Használni fogjuk a 3.4-es tételben nyert speciális $A \subset S$-et, méghozzá legyen $A_i, i = 1, 2, 3, 4$, A-val egybevágó halmaz, amelyek uniója lefedi S-et. Diszjunktizáljuk őket! Azaz legyen $C_1 = A_1$ és $i \geq 2$ esetén legyen $C_i = A_i \setminus \bigcup_{j<i} A_j$. Ekkor C_i-k továbbra is fedik S-et.

$B_1 \equiv_1 B_1 \subset (B_1 \cup B_2)$ nyílvánvaló, most megmutatjuk, hogy $(B_1 \cup B_2) \equiv_9 V \subset B_1$, amely az előző állítás fényében már igazolja az tételt. Ha γ-val jelöljük azt az eltolást, amely B_1-et B_2-be viszi, akkor 9 diszjunkt részre osztását kaphatjuk a két gömb uniójának a következő előállítás során:

$$B_1 \cup B_2 = [C_1^* \cup \{O\}] \cup C_2^* \cup .. \cup C_4^* \cup \gamma(C_1)^* \cup ... \cup \gamma(C_4)^* \cup \{\gamma(O)\}$$

Ekkor ha $D_i : i = 1, 2, 3, ...$ végtelen sok A-val egybevágó példány S-en, akkor $[C_1^* \cup \{O\}]$ egybevágó D_1^*-al, C_i^* egybevágó D_i^* egy részhalmazával (mivel a C_i-ket megcsonkoltuk) i=2,3,4 esetén, hasonlóan kapjuk, hogy $\gamma(C_i^*)$ pedig egybevágó D_{i+4}^* egy-egy részhalmazával i=1,2,3,4 esetén, míg $\{\gamma(O)\}$ egybevágó D_9 bármilyen egyelemű részhalmazával. EZzel megmutattuk, hogy $B_1 \cup B_2$ beledarabolható (méghozzá 9 darabban!) B_1 egy bizonyos részhalmazába, amivel a tétel bizonyítása készen van.

□

Ezen fejezet lezáró tételéhez érkezünk, amikor is kontinuum rangú szabad csoportot fogunk mutatni $SO(3)$-ban. Ez semmilyen féleképpen sem egy váratlan halmaz a síkon vagy a térben (legfőképpen, mert egy csoport), de a 3.4-es tételt tovább lehetne erősíteni apró módosításokkal úgy, hogy kontinuum sok egybevágó diszjunkt példánya található meg egy bizonyos $A \subset S$-nek a gömbfelszínen, míg továbbra is 4 egybevágó példányával lefedhető a gömbfelszín.

3.8. lemma. *Létezik $A \subset \mathbb{R}$, amely kontinuum számosságú és algebrailag független $\mathbb{Q}$ felett.*

Bizonyítás. Zorn-lemmát fogjuk használni, nyílván azokra a halmazokra, amelyek algebrailag függetlenek $\mathbb{Q}$ felett, hogy mutassunk egy maximális algebrailag független halmazt (azaz ő nem valódi része egyetlen egy olyan halmaznak sem, amely algebrailag független). Ezek után belátjuk, hogy bármilyen maximális algebrailag független halmaz számossága szükségképpen kontinuum.

Ha adott tehát algebrailag független halmazok egy lánca, azaz $\{V_i : i \in I\}$ algebrailag független halmazok $\forall i$-re úgy, hogy $\forall l, k \in I$: $V_l \subset V_k$ vagy $V_k \subset V_l$, akkor könnyen láthatóan felső korlátja lesz ennek a láncnak a $\bigcup_{i\in I} V_i$ halmaz. Világos, hogy ha $\bigcup_{i\in I} V_i$ nem lenne algebrailag független, az azért van, mert tudok mutatni $\alpha_1, ..., \alpha_n \in \bigcup_{i\in I} V_i$, hogy ők már nem algebrailal függetlenek. Ezen felül $\forall j, (j \in \{1, , , n\})$ $\exists i_j \in I$, hogy $\alpha_j \in V_{i_j}$, Ekkor ezen véges sok halmaz közül a legbővebb tartalmazza az összes α_j-t, ellentmondva ezen legbővebb halmaz algebrai függetlenségének.

Legyen most $H \subset \mathbb{R}$ maximális az algebrai függetlenségre nézve, valamint jelöljük H számosságát κ-val. H maximalitását ott tudjuk kihasználni, hogy egyetlen egy valós szám sem vehető hozzá H-hoz, hogy az algebrailag független maradjon, azaz $\forall r \in \mathbb{R}$ $\exists h_1, ..., h_k \in H$, (k függ az r-től), hogy $r, h_1, .., h_k$ algebrailag függő $\mathbb{Q}$ felett, azaz létezik egy $\mathbb{Q}$ feletti nem azonosan nulla (k+1) változós polinom, aminek gyöke $r, h_1, .., h_k$. Nézzük meg, hogy hányféleképpen tudok kivenni véges sok H-beli elemet, és hozzájuk egy $\mathbb{Q}$ feletti akárhány változós polinomot. Nyílván legfeljebb $\kappa \cdot \aleph_0$-szor, mivel H összes véges részhalmazai κ sokan vannak, ha H végtelen elemszámú és $\aleph_0$ sok akárhány változós $\mathbb{Q}$ feletti polinom van, mert minden n-re csak megszámlálható sok $\mathbb{Q}$-beli együtthatós n-változós polinom létezik. Ha véges elemszámú, akkor $\kappa \cdot \aleph_0 = \aleph_0$, de nyílván ebben az esetben is pontosan ennyiféleképpen tudunk választani véges sok H-beli elemet és egy többváltozós racionális együtthatós polinomot. Fordítva, ha kiválasztok véges sok $h_1, ..., h_k \in H$ számot, és egy (k+1) változós nemazonosan nulla polinomot $\mathbb{Q}$ felett, $q(x_1, ..., x_{k+1})$-t, akkor $q(h_1, ...h_k, x_{k+1})$-nek csak véges sok gyöke van. Így azon valós számok, amelyek az előbbi alakban állnak elő, mint $q(h_1, ...h_k, x_{k+1})$-nak a gyökei, azok is $\kappa \cdot \aleph_0$ sokan vannak, de így minden valós szám előáll H maximalitása miatt! Így $c = \kappa \cdot \aleph_0$, amiből világos, hogy

$\kappa = c$ szükségképpen igaz.

□

Forgatás alatt a továbbiakban mindig $SO(3)$-beli csoportelem által reprezentált forgatást fogunk érteni. Két origón átmenő síkra való tükrözés kompozíciója világos, hogy a két sík metszeteként előálló egyenes körüli forgatás, méghozzá kétszer akkora szöggel, amelyet a síkok bezártak. Ez a gondolatmenet könnyen eljátszható visszafele is, bármely forgatás előáll, mint két origón átmenő síkra való tükrözés kompozíciójaként, persze ezen síkok választása már nem egyértelmű. Egy origón átmenő síkot annak valamelyik normálvektorával jellemezhetjük. Sőt, ha tehát adott egy $\underline{v}$ vektor, akkor nem csak azt a síkot jellemezhetjük $\underline{v}$-vel, aminek a $\underline{v}$ a normálvektora, hanem az erre a síkra vett tükrözést. Az előbbiek miatt tehát bevezetjük a $T_{\underline{v}}$ jelölést, amely arra síkra való tükrözést fogja jelölni, aminek a normálvektora a $\underline{v}$. Ekkor a $T_{\underline{v}} \circ T_{\underline{w}}$ egy forgatást reprezentál, és ezt a forgatást jellemezhetjük egy valós szám-hatossal: $(v_1, v_2, v_3, w_1, w_2, w_3) = (\underline{v}, \underline{w}) \in \mathbb{R}^6$. Az előbbiek alapján tetszőleges forgatás is reprezentálható legalább egy valós szám-hatossal.

Most megvizsgáljuk egy $T_{\underline{v}}$ transzformáció mátrixát (a természetes bázisban felírva), majd annak speciális alakjából egy ügyes gondolatmenettel adni fogja magát a kontinuum rangú szabadcsoport.

3.9. tétel. *Minden $\underline{0} \neq \underline{v} \in \mathbb{R}^3$ által meghatározott $T_{\underline{v}}$ tükrözés mátrixa a természetes bázisban a következő alakban áll elő:*

$$\begin{bmatrix} 1 - \frac{2v_1^2}{v_1^2+v_2^2+v_3^2} & -\frac{2v_1v_2}{v_1^2+v_2^2+v_3^2} & \frac{-2v_1v_3}{v_1^2+v_2^2+v_3^2} \\ -\frac{2v_1v_2}{v_1^2+v_2^2+v_3^2} & 1 - \frac{2v_2^2}{v_1^2+v_2^2+v_3^2} & -\frac{2v_2v_3}{v_1^2+v_2^2+v_3^2} \\ -\frac{2v_1v_3}{v_1^2+v_2^2+v_3^2} & -\frac{2v_2v_3}{v_1^2+v_2^2+v_3^2} & 1 - \frac{2v_3^2}{v_1^2+v_2^2+v_3^2} \end{bmatrix}$$

Bizonyítás. Ha S jelöli a $\underline{v}$ normálvektorú origón átmenő síkot, akkor egy tetszőleges $(x_1, x_2, x_3) = \underline{x} \in \mathbb{R}^3$ vektor S-re vett merőleges vetületére (amit mostantól $\underline{x}_S$-el jelölünk) igaz, hogy $\underline{x}_S = \underline{x} - \frac{\langle \underline{x}, \underline{v} \rangle}{|\underline{v}|^2} \underline{v}$. Ezt mutatja a $\langle \underline{x} - \frac{\langle \underline{x}, \underline{v} \rangle}{|\underline{v}|^2} \underline{v}, \underline{v} \rangle = \langle \underline{x}, \underline{v} \rangle - \langle \frac{\langle \underline{x}, \underline{v} \rangle}{|\underline{v}|^2} \underline{v} \rangle = 0$ számolás.

Így $\underline{x}'$-vel jelölve a kapott képpontot a tükrözés után fennál, hogy:

$\underline{x'} = 2\underline{x}_S - \underline{x} = \underline{x} - 2\frac{\langle \underline{x},\underline{v}\rangle}{|\underline{v}|^2}$, koordinátákkal:

$$T_{\underline{v}}(\underline{x}) = \begin{bmatrix} x_1 - \frac{2v_1}{v_1^2+v_2^2+v_3^2}(v_1x_1+v_2x_2+v_3x_3) \\ x_2 - \frac{2v_2}{v_1^2+v_2^2+v_3^2}(v_1x_1+v_2x_2+v_3x_3) \\ x_3 - \frac{2v_3}{v_1^2+v_2^2+v_3^2}(v_1x_1+v_2x_2+v_3x_3) \end{bmatrix}$$

Ebből a tétel állítása már nyílvánvaló. □

Az előző állításból tulajdonképpen csak annyit fogunk használni, hogy a $T_{\underline{v}} \circ T_{\underline{w}}$ mátrix bármelyik eleme a következő formában áll elő:

$$\frac{p(v_1, v_2, v_3, w_1, w_2, w_3)}{v_1^2 + v_2^2 + v_3^2 + w_1^2 + w_2^2 + w_3^2}$$

ahol p egy 6 változós egész együtthatós polinom, ez a két mátrix összeszorzásából világos, persze a szorzatmátrix különböző elemeinél a p polinomok különbözhetnek.

Ha egy forgatást 6 számmal paramétereztünk, akkor azt a fenti értelemben értjük, azaz ha adva van a forgatás egy tetszőleges $T_{\underline{v}} \circ T_{\underline{w}}$ alakban vett előállítása, akkor az ebből nyert $(v_1, ..., w_3)$ valós szám-hatos biztosítja a paraméterezést.

3.10. tétel. *Tegyük fel, hogy $A_1, ..., A_n \in SO(3)$ paraméterezhető 6n darab $\mathbb{Q}$ felett algebrailag független számokkal. Ekkor ezek a forgatások függetlenek is (azaz egy szabadcsoportot alkotnak).*

Bizonyítás. Legyen ez a 6n paraméter $v_1, ...v_{6n}$. Indirekt okoskodunk, tegyük fel, hogy van egy nemüres redukált szó, amely az identikus forgatást adja, legyen ez B. Ekkor B a következő alakot ölti: $B = A_{i_1}^{m_1}....A_{i_s}^{m_s} = id$, ahol $m_1, ...m_s$ nemnulla egész számok, és $i_k \neq i_{k+1}$, $k = 1, .., s-1$ esetén. Mivel bármely $C \in SO(3)$-ra $C^{-1} = C^T$, ezért $A_{i_1}^{m_1}....A_{i_s}^{m_s}$ mátrix minden eleme $\frac{p(v_1,...v_{6n})}{q(v_1,...,v_{6n})}$ alakú, $p(x_1, ...x_{6n})$ és $q(x_1, ..., x_{6n})$ racionális együtthatós polinomokkal. Ez utóbbi hányados értéke 0 vagy 1, aszerint, hogy a szorzatmátrix melyik eleme, mivel az eredmény az egységmátrix. Mivel a paraméter számaink algebrailag függetlenek voltak, ezért azok a helyek, ahol az egységmátrixban nulla áll, ott a p polinom nulla, míg ahol 1-es áll, ott $p \equiv q$.

Most jön a bizonyítás kulcsgondolatmenete, ugyanis vegyük észre, hogy ha adva lennének tetszőleges $A_1, ...A_n$ forgatások tetszőleges 6n darab számmal paraméterezve (azaz semmilyen féle algebrai függetlenséget sem teszünk fel rólunk), akkor az $A_{i_1}^{m_1}....A_{i_s}^{m_s}$ mátrix kiszámításánál szó szerint ugyanezek a p és q polinomok jelennének meg, mint fent, de ez azt jelentené, hogy az $A_1, ..., A_n$ mátrixok tetszőleges választása mellett $A_{i_1}^{m_1}....A_{i_s}^{m_s}$ szorzatmátrix az identitást adná. Ha F és G független forgatások, (ilyen biztosan létezik a 3.2-es tétel értelmében), akkor $F^{-1}GF, ..., F^{-n}GF^n$ is független forgatások, de az előző okoskodások alapján egy nemtriviális szó az identikus forgatást eredményezné, ellentmondva $F^{-1}GF, ..., F^{-n}GF^n$ függetlenségének. Így maga $A_1, ..., A_n$ forgatások is függetlenek. □

3.11. tétel. *$SO(3)$ csoport tartalmaz kontinuum rangú szabadcsoportot.*

Bizonyítás. Vegyünk egy $H \subset \mathbb{R}$ algebrailag független halmazt $\mathbb{Q}$ felett (ilyen van a 3.8-as lemma értelmében). Osszuk ezt széjjel 6-os csomagokba (ekkor kontinuum sok csomagot kapunk), és tekintsük ezen 6-osok által reprezentált forgatásokat. Ahhoz, hogy ezek kontinuum rangú szabadcsoportot alkossanak, az kell, hogy kontinuum sokan legyenek (ez teljesül is), valamint hogy bármely véges része független legyen, ezt pedig éppen az előző 3.10-es tétel garantálja. □

4. A Lindemann-Weierstrass tétel

Ebben a fejezetben "bizonyos kinézetű" számokról igazoljuk azok transzcendens voltát. Természetes lenne most az e és a π transzcendenciájával kezdeni, azonban ehelyett egy sokkal erősebb tétellel indítunk, a Lindemann-Weierstrass tétellel, amiből kipotyog az e és a π mellett rengeteg másik szám transzcendenciája. Ahhoz, hogy eljussunk e tétel bizonyításához és hogy ne kelljen rengeteg technikai részletet a bizonyítás közben elemezni, ezzel megtörve a tétel bizonyításának megértését, néhány állítás/lemma/tétel-t fogunk most megnézni, amelyek első ránézésre nem is feltétlen fognak kapcsolódni egymáshoz, azonban mindegyiknek szerepe lesz a Lindemann-Weierstrass tétel bizonyításában. Testbővítések témakörből eredményeket fogunk használni, amelyeknek egy részét ismertnek tételezzük fel, míg másik részük a függelékben bizonyításra kerül (ezt valamilyen formátumban majd jelezzük az állítás után), illetve egy-egy állítás bizonyítása ezen fejezet keretén belül történik. A bizonyításokat [6] és [2]-ből dolgoztuk fel.

4.1. lemma. *Legyen $t \in \mathbb{C}$ tetszőleges és f egy m-edfokú polinom, emellett jelölje $I(t,f)$ a következő komplex vonalintegrált $I(t,f) := \int_0^t e^{t-u} f(u)du$, ahol az integrálási utat a $[0,t]$ szakasznak választjuk. Ekkor $I(t,f) = e^t \sum_{j=0}^{m} f^{(j)}(0) - \sum_{j=0}^{m} f^{(j)}(t)$.*

Bizonyítás. Teljes indukcóval bizonyítjuk a lemmát. m=0-ra triviális, hiszen ekkor f valamilyen konstans c, és így $I(t,f) := \int_0^t e^{t-u}cdu = [-ce^{t-u}]_{u=0}^{u=t} = e^t c - e^0 c$. Tegyük fel, hogy minden legfeljebb m-edfokú polinomra már tudjuk az állítást, és legyen f egy tetszőleges (m+1)-edfokú polinom. Ekkor parciális integrálással és indukcióval kapjuk:

$$I(t,f) := \int_0^t e^{t-u} f(u)du = [-e^{t-u}f(u)]_{u=0}^{u=t} + \int_0^t e^{t-u} f'(u)du =$$

$$= e^t f(0) - f(t) + e^t \sum_{j=0}^{m} f'^{(j)}(0) - \sum_{j=0}^{m} f'^{(j)}(t) = e^t \sum_{j=0}^{m+1} f^{(j)}(0) - \sum_{j=0}^{m+1} f^{(j)}(t).$$

□

4.2. lemma. *Legyen $\alpha_1, ..., \alpha_n \in \mathbb{C}$ páronként különböző számok. Ekkor $e^{\alpha_1 t}, ..., e^{\alpha_n t}$ függvények lineárisan függetlenek $\mathbb{C}$ felett.*

Bizonyítás. Ha nem így volna, akkor léteznének $\lambda_1, ..., \lambda_n$ nem mind nulla komplex számok, amelyekre $\lambda_1 e^{\alpha_1 t} + ... + \lambda_n e^{\alpha_n t} \equiv 0$. Ez utóbbi egyenletet deriváljuk (n-1)-szer, majd helyettesítsünk mindenhol $t = 0$-t, akkor az eredeti és az (n-1) deriváltegyenlettel kapjuk, hogy:

$$\lambda_1 + ... + \lambda_n = 0$$
$$\lambda_1 \alpha_1 + ... + \lambda_n \alpha_n = 0$$
$$\lambda_1 \alpha_1^2 + ... + \lambda_n \alpha_n^2 = 0$$
$$...$$
$$\lambda_1 \alpha_n^{n-1} + ... + \lambda_n \alpha_n^{n-1} = 0$$

Ez utóbbi lehetetlen, hiszen mint $\lambda_1, ..., \lambda_n$-ben n ismeretlenes n egyenletből álló homogén lineáris egyenletrendszernek tekintve a fenti egyenleteket, az együttható mátrix egy Vandermonde mátrix $\alpha_1, ..., \alpha_n$-ben, ezek determinánsa nemnulla jól ismerten (persze $\alpha_1, ...\alpha_n$ különbözősége kell hozzá), így csakis azonosan nulla megoldása lehetne az egyenletrendszernek, de abból indultunk ki, hogy $\lambda_1, ..., \lambda_n$ nem mindegyike nulla. □

Megjegyzés: Ez utóbbi lemmát ott fogjuk kihasználni majd a későbbiekben, hogy több $\lambda_1 e^{\alpha_1} + ... + \lambda_n e^{\alpha_n}$ ($\alpha_1, ..., \alpha_n$ különbözők, $\lambda_1, ..., \lambda_n$ nem mindegyike nulla) típusú kifejezéseket szorzunk össze, amelyek eredménye szintén valami $b_1 e^{\gamma_1} + ...b_k e^{\gamma_k}$ alakú kifejezés, és itt nem lehet minden $b_1, ..., b_k$ együttható nulla (persze a kapott szorzatkifejezés $b_1 e^{\gamma_1} + ... + b_k e^{\gamma_k}$ értéke lehet nulla), mivel $\lambda_1 e^{\alpha_1 t} + ... + \lambda_n e^{\alpha_n t}$ alakú függvények szorzata $b_1 e^{\gamma_1 t} + ... + b_k e^{\gamma_k t}$ alakú, ez utóbbi pedig nem azonosan nulla komplex analatikus függvények szorzata, így ő maga sem nulla. Tehát $b_1, ..., b_k$ nem mindegyike nulla.

Most pedig néhány testelméletből való alapvető definíció és eredmény átismétlése következik, ezek egy részét általánosabban is ki lehetne mondani, de nekünk lényegében csak arra lesz szükségünk, amikor $\mathbb{Q}$ valamilyen vé-

ges bővítése lesz adott, egy-egy állítás viszont általánosabban is kimondásra kerül.

4.3. definíció. $\mathbb{K} \leq \mathbb{L}$ *testbővítést végesnek nevezzük, ha* $\mathbb{L}$*, mint* $\mathbb{K}$ *feletti vektortér véges dimenziós.*

4.4. definíció. $\mathbb{K} \leq \mathbb{L}$ *testbővítést algebrainak nevezzük, ha* $\forall \alpha \in \mathbb{L}$ *algebrai* $\mathbb{K}$ *felett.*

4.5. definíció. $\mathbb{K} \leq \mathbb{L}$ *bővítés szeparábilis, ha minden* $\alpha \in \mathbb{L}$*-re a* $\mathbb{K}$ *feletti minimálpolinomja szeparábilis, azaz a minimálpolinom összes gyöke különböző (*$\mathbb{K}$ *valamelyik algebrai lezártjában).*

Ismert, hogy $\mathbb{Q}$-nak minden algebrai bővítése szeparábilis, sőt, ez minden nullkarakterisztikájú test esetén is elmondható. Ha adott $\mathbb{K} \leq \mathbb{L}$ testbővítések, akkor tetszőleges $\vartheta \in \mathbb{L}$ esetén $\mathbb{K}(\vartheta)$ jelöli azt a legszűkebb $\mathbb{L}$-beli résztestet, amely tartalmazza $\mathbb{K}$-t és ϑ-t. Mivel könnyen ellenőrizhetően egy adott testben akárhány résztest metszete is test, így az előbbi definíció értelmes. Ekkor azt mondjunk, hogy ϑ-t adjungáltuk $\mathbb{K}$-hoz.

4.6. definíció. $\mathbb{K} \leq \mathbb{L}$ *testbővítést egyszerűnek hívunk, ha egy elemmel generálható, azaz létezik* $\vartheta \in \mathbb{L}$*, hogy* $\mathbb{L} = \mathbb{K}(\vartheta)$

Ez utóbbi generáló elemet szokás "primitív" elemnek is hívni. Úgy szintén ismert a következő tétel:

4.7. tétel. *Minden véges szeparábilis bővítés egyszerű.*

Mostantól kezdve ha azt mondjuk, hogy adott $\mathbb{Q}$-nak egy $\mathbb{K}$ véges bővítése, akkor mindig hozzáértjük, hogy $\mathbb{K} \leq \mathbb{C}$. Néha azt is mondjuk majd, hogy "adott egy $\mathbb{K}$ n-edfokú algebrai számtest", ekkor $\mathbb{K}$ mindig $\mathbb{Q}$-nak egy n-edfokú (tehát egyben véges is) bővítését fogja jelenteni. Ha adott csak úgy egy "algebrai számtest", az mindig valamilyen n-re $\mathbb{Q}$ véges bővítését jelenti. Mivel egy algebrai számtest $\mathbb{Q}$-nak véges bővítése, ezért $\mathbb{K}$ mindig előáll $\mathbb{K} = \mathbb{Q}(\vartheta)$ alakban. Úgy szintén ismert, hogy ekkor az $n = [\mathbb{K} : \mathbb{Q}]$ testbővítés foka éppen a ϑ konjugáltjainak száma. Ez utóbbi közös n számra az $1, \vartheta, ..., \vartheta^{n-1}$ bázis $\mathbb{K}$-ban (mint vektortérben $\mathbb{Q}$ felett).

Eddig $\alpha \in \mathbb{C}$ algebrai szám konjugáltjai alatt a minimálpolinomjának az összes gyökét értettük, most egy másik típusú konjugált fogalmat vezetünk be. Mindkettő fogalmat használni fogjuk, de ezek megkülönbeztetése nem fog gondot okozni, szükség esetén hangsúlyozzuk is majd, hogy a "régi" vagy az "új" konjugáltság fogalomra gondolunk, persze e "régi" és "új" fogalom kapcsolódni fog egymáshoz, amelyet igyekszünk részletezni, de egy-egy állítás bizonyítása a függelékbe fog szorulni. Egy gyors jelölést még bevezetünk az új konjugáltság fogalom bevezetése előtt: egy n-edfokú ϑ algebrai szám esetén a konjugáltjait (ez még a régi értelemben vett konjugáltság) jelöljük $\vartheta = \vartheta^{(1)}, \vartheta^{(2)}, ..., \vartheta^{(n)}$-el.

4.8. definíció. *Legyen $\mathbb{K}$ n-edfokú algebrai számtest, valamint legyen $\vartheta \in \mathbb{K}$ olyan, hogy $\mathbb{K} = \mathbb{Q}(\vartheta)$. Ekkor a fentiek alapján tetszőleges $\alpha \in \mathbb{K}$ előáll $\alpha = c_0 + c_1\vartheta + ... + c_{n-1}\vartheta^{n-1}$ alakban, ekkor az "α szám konjugáltjai $\underline{\underline{\mathbb{K}}}$-ban" alatt a következő számokat értjük:*

$$c_0 + c_1\vartheta^{(i)} + ... + c_{n-1}(\vartheta^{(i)})^{n-1}, \quad i = 1, 2, ..., n$$

Gyűjtsük össze, hogy mit tud ez az új konjugáltság fogalom! Most minden $\alpha \in \mathbb{K}$ számnak n darab konjugáltja van, ebben az új értelemben, függetlenül attól, hogy ő maga n-ed fokú vagy kisebb fokú-e. Bár a definícióban az "α konjugáltjai $\mathbb{K}$-ban" kifejezéssel éltünk, egyáltalán semmi sem garantálja, hogy ezek a konjugáltak mind $\mathbb{K}$-ba fognak esni. Ezen n db konjugált között előfordulhat, hogy néhány ugyanaz, például: $\mathbb{Q}(\sqrt{2})$-ben az 1 és a $\sqrt{2}$ bázis, továbbá a primitív elem maga választható $\sqrt{2}$-nek, az ő konjugáltjai: $\sqrt{2}, -\sqrt{2}$. Az "1" felírása $\mathbb{Q}(\sqrt{2})$-ben: $1 = 1\cdot 1 + 0\cdot\sqrt{2}$, így az "1" konjugáltjai $\mathbb{Q}(\sqrt{2})$: $1 \cdot 1 + 0 \cdot \sqrt{2} = 1$ és $1 \cdot 1 + 0 \cdot (-\sqrt{2}) = 1$.

4.9. tétel. *Legyen $\mathbb{K}$ n-edfokú algebrai számtest, valamint $\alpha \in \mathbb{K}$ tetszőleges, m-edfokú algebrai szám. Ekkor α konjugáltjai $\mathbb{K}$-ban nem más, mint $\frac{n}{m}$ alkalommal felsorolva mindegyik konjugáltja α-nak.*

A bizonyítás a függelékbe kerül. Az utóbbi tétel egyik következménye, hogy α konjugáltjai $\mathbb{K}$-ban nem függenek a primitív elem választásától. A $\vartheta \mapsto \vartheta^{(i)}$ megfeleltetés egy $\sigma_i : \mathbb{Q}(\vartheta) \longmapsto \mathbb{Q}(\vartheta^{(i)})$ izomorfizmust ad, ismert

(és könnyű látni is), hogy így áll elő a $\mathbb{Q}(\vartheta)$ test összes homomorfizmusa a komplex számok testébe. Evégett gyakran fogjuk egy α szám $\mathbb{K}$-beli konjugáltjait $\sigma_i(\alpha)$-val jelölni, ami mellesleg valóban az α i-edik konjugáltját adja vissza, mint a σ_i izomorfizmus kiszámítása az α helyen.

Emlékeztetünk arra, hogy algebrai egészeknek hívjuk azon komplex számokat, amelyek gyökei egy egész együtthatós normált polinomnak (ekvivalensen vele az, hogy az egész minimálpolinomjuk főegyütthatója 1). Ismert, hogy az algebrai számok testet alkotnak és az algebrai egészek gyűrűt alkotnak, szintúgy az algebrai egészek egy gyűrűt alkotnak egy $\mathbb{K}$ algebrai számtestben. Ha adott egy α n-edfokú algebrai szám az ő egész minimálponimjával: $a_n\alpha^n+...+a_0 = 0$, akkor $a_n\alpha$ egy algebrai egész, hogy ezt lássuk, az előbbi egyenletet a_n^{n-1}-el beszorozva kapjuk: $(a_n\alpha)^n+a_{n-1}(a_n\alpha)^{n-1}+...+a_n^{n-1}a_0 = 0$. Hasonlóan $a_n\alpha^{(i)}$ is algebrai egész. Speciálisan véges sok algebrai számra létezik egy közös egész szám, amelyekkel beszorozva mindegyik algebrai számot algebrai egészet kapunk (az egész minimálpolinomok főegyütthatóinak legkisebb közös többszöröse). A későbbiek során egy egész szám alatt csak "simán" egy egész számra gondolunk a racionális számok között.

Felhasználjuk még a következő két elemi megfigyelést, amelyek az elemi szimmetrikus polinomok tételének gyakorlatilag közvetlen következménye: Ha $f(x_1,...x_n) \in \mathbb{Q}[x_1,...x_n]$ szimmetrikus $x_1,...,x_n$-ben, és $\beta_1,...,\beta_n$ éppen az össze gyöke egy racionális együtthatós polinomnak (lehetnek köztük egyformák is), akkor $f(\beta_1,...,\beta_n) \in \mathbb{Q}$, sőt, ha f egész együtthatós, és maga a polinom, aminek a gyökei $\beta_1,...,\beta_n$ is egész együtthatós plusz normált, akkor $f(\beta_1,...,\beta_n) \in \mathbb{Z}$. Ez utóbbi megfigyeléseket gyakran egy szám és konjugáltjaira (mind a régi és mind az új értelemben), vagy annak olyan konstansszorosára alkalmazzuk, amely már algebrai egészek, vagy esetleg egy olyan polinomra, amelynek együtthatói mind szimmetrikusak valamely $\beta_1,...,\beta_n$-ben, és ekkor magáról a polinomról fogjuk tudni eldönteni, hogy racionális/egész együtthatós.

Ezek után készen állunk a fejezet főtételére:

4.10. tétel. *(Lindemann-Weierstrass, 1885) Ha $\alpha_1,....,\alpha_n$ különböző algebrai egészek, akkor $e^{\alpha_1},...,e^{\alpha_n}$ lineárisan független $\mathbb{A}$ felett.*

Mielőtt a tételt belátnánk, nézzük meg annak néhány következményét!

4.11. tétel. $\forall \alpha \in \mathbb{A} \setminus \{0\}$ e^α *transzcendens.*

Bizonyítás. Tegyük fel, hogy mégsem, ekkor $e^\alpha = \beta = \beta e^0 \longrightarrow 1 \cdot e^\alpha - \beta \cdot e^0 = 0$, ellentmondva a 4.10-es tételnek. □

Következmény 1: az e transzcendens.

Következmény 2: a π transzcendens. (Ha ugyanis nem így volna, akkor π és $\alpha = i\pi$ is algebrai volna, de $e^{i\pi} = -1$.

4.12. tétel. *Ha* α *nemnulla algebrai szám, akkor* $\sin\alpha$, $\cos\alpha$, $\tan\alpha$ *is transzcendens.*

Bizonyítás. Mivel $\sin\alpha = \frac{e^{i\alpha}-e^{-i\alpha}}{2i}$ és $\cos\alpha = \frac{e^{i\alpha}+e^{-i\alpha}}{2}$, valamint $\tan\alpha$ ez utóbbiak hányadosa, hogy ha ezek valamelyike algebrai volna, akkor az egyenletet 0-ra rendezve ellentmondásra jutnánk a 4.10-es tétellel, a $\tan\alpha$ esetet kiírjuk részletesebben, tegyük fel, hogy $\tan\alpha = \beta$ algebrai:

$$e^{i\alpha} - e^{-i\alpha} = i(e^{i\alpha} + e^{-i\alpha})\beta \Rightarrow (1 - i\beta)e^{i\alpha} + (-1 - i\beta)e^{-i\alpha} = 0$$

Itt mindkét együtthatónak nullának kellene lennie, de legalább az egyik nemnulla. □

4.13. tétel. $\alpha \neq 0$ *algebrai, ekkor* $\log\alpha$ *transzcendens (*α *akármlyik logaritmusát is tekintve).*

Bizonyítás. Ha algebrai lenne, akkor $e^{\log\alpha} = \alpha$ transzcendens lenne 4.11-es tétel szerint. □

Bizonyítás. (4.10-es tételé) Indirekt bizonyítunk, legyenek $d_1, ..., d_s \in \mathbb{A}$ nem mindegyik nulla úgy, hogy:

$$(*) \quad d_1 e^{\alpha_1} + ... + d_s e^{\alpha_s} = 0$$

a d_i-k közül a 0-k el is hagyhatóak, feltehető tehát, hogy a d_i-k mindegyike nemnulla. A következő lépések célja az lesz, hogy az egyenletről minél

"szebb" dolgokat mondhassunk el. Szorozzuk be (*)-ot $\sum_{j=1}^{s} \sigma_k(d_j)e^{\alpha_j}$ alakú kifejezésekkel, ahol σ_k végigfut a $\mathbb{Q}(d_1, ..., d_s)$ test összes $\mathbb{C}$-be való homomorfizmusain, mint ahogy azt fentebb leírtuk, ezek számát jelöljük l-el. Ekkor az állítjuk, hogy egy következő típusú egyenletbe lyukadunk ki:

$$(**) \quad a_1e^{\gamma_1} + ... + a_ne^{\gamma_n} = 0$$

Ahol $a_1, ..., a_n$ racionális számok, nem mindegyike nulla és $\gamma_1, ..., \gamma_n$ különböző algebrai számok. Természetesen (**) egyenletet be fogjuk majd szorozni egy nagy egész számmal, hogy feltehessük, hogy $a_1, ..., a_n$ egészek is, így ha beláttuk, hogy valóban ilyen alakú lesz (**), ahogy írtuk, akkor $a_1, ..., a_n$-ekről fel fogjuk tenni, hogy még egészek is. Lássuk be először azt, hogy egyáltalán nem fog mindegyik e^{γ_1} tag kiesni, ehhez tekintsük azt a teljes rendezést a komplex számokon, hogy $\alpha \neq \beta$ esetén: $\alpha < \beta \iff Re(\alpha) < Re(\beta)$ vagy $Re(\alpha) = Re(\beta)$ esetben pedig $Im(\alpha) < Im(\beta)$ teljesül. Feltehető az általanosság megszorítása nélkül, hogy α_1 volt a legkisebb a kiinduló α_j-k közül erre rendezésre nézve. Ekkor a $\prod_{k=1}^{l} \sigma_l(d_1)e^{\alpha_1} = \sigma_1(d_1)\sigma_2(d_1)....\sigma_l(d_1)e^{n\alpha_1}$ tagot senki sem fogja kiejteni, továbbá mivel d_1 nemnulla, ezért egy σ homomorfizmus során $\sigma(d_1)$ sem nulla (test homomorfizmusa tulajdonképpen a test beágyazását adja, így nemnulla elem nemnulla elembe megy át).

Most nézzük meg, hogy egy a_j miért lesz racionális, ezt úgy fogjuk belátni, hogy a (*) egyenelet $\sum_{j=1}^{s} \sigma_k(d_j)e^{\alpha_j}$ alakú kifejezésekkel való beszorzása után egy általános tagja az összegnek úgy fog kinézni, hogy (valamilyen szám) $\cdot$ $e^{\sum_{i=1}^{s} \lambda_i\alpha_i}$, ahol $\sum \lambda_i = l$ (mivel l db hosszú kifejezést szoroztunk össze), és erről a (valamilyen számról) mutatjuk meg, hogy racionális. Ezek után, ha összevonjuk a $e^{\sum_{i=1}^{s} \lambda_i\alpha_i}$ alakú tagokat, ahol a kitevők ugyanazt az algebrai számot adják, valamelyik γ_j-t, végül pedig egy ilyen együtthatója racionális számok összege lesz.

Mivel $d_1, ..., d_s$ mindegyike algebrai, ezért $\mathbb{Q}(d_1, ..., d_s)$ $\mathbb{Q}$-nak véges bővítése, ezért ez egy véges szeparábilis bővítés, így a 4.7-es tétel alapján egyszerű is, legyen ϑ olyan, hogy $\mathbb{Q}(d_1, ..., d_s) = \mathbb{Q}(\vartheta)$. Megmutatjuk, hogy $e^{\sum_{i=1}^{s} \lambda_i\alpha_i}$

együtthatója ϑ és konjugáltjaiban egy racionális együtthatós polinom, ami szimmetrikus is lesz még ϑ és konjugáltjaiban, ez pedig a fentebbi szimmetrikus polinomokra tett megjegyzések alapján éppen azt eredményezi, hogy $e^{\sum_{i=1}^{s} \lambda_i \alpha_i}$ együtthatója racionális.

Ha tehát fixáltunk $\lambda_1, ..., \lambda_n$ nemnegatív egészeket, akkor a $\prod_{k=1}^{l} (\sum_{j=1}^{s} \sigma_k(d_j) e^{\alpha_j})$ alakból világos, hogy amindent-mindennel összeszorzás után a $e^{\sum_{i=1}^{s} \lambda_i \alpha_i}$ együtthatója :

$$(1) \qquad \sum_{i_1,...,i_k \in \{1,...,s\}} \prod_{k=1}^{l} \sigma_k(d_{i_k})$$

ahol persze az $i_1, ..., i_k$ indexek közül pontosan λ_1 darab 1-es,..., λ_s darab index értéke s. Mivel l db σ van, ez pontosan azt jelenti, hogy a $\mathbb{Q}$-nak $\mathbb{Q}(\vartheta)$ éppen l-edfokú bővítése, amit használni fogunk, hogy $\mathbb{Q}(\vartheta)$, mint $\mathbb{Q}$ feletti vektortérben midegyik d_j-t fel tudjuk írni a $1, \vartheta, ..., \vartheta^{l-1}$ bázisban:

$$d_j = \sum_{z=0}^{l-1} q_{j_z} \vartheta^z$$

Ha ezek mellett még ϑ konjugáltjait $\vartheta = \vartheta_{(1)}, ..., \vartheta_{(l)}$-el jelöljük, akkor $\sigma_k(d_j) = \sum_{z=0}^{l-1} q_{j_z} \vartheta_{(k)}^z$, éppen a k-ik konjugáltja d_j-nek $\mathbb{Q}(\vartheta)$-ban (ezen "újabb" 4.8-as definíció értelmében vett konjugált). Ezeket visszaírva (1)-be kapjuk a következő kifejezést:

$$(2) \qquad \sum_{i_1,...,i_k \in \{1,...,s\}} \prod_{k=1}^{l} (\sum_{z=0}^{l-1} q_{i_{k_z}} \vartheta_{(k)}^z)$$

ami viszont tényleg szimmetrikus $\vartheta_{(j)}$-kben, ezt ellenőrizendő elég látni, hogy egy $\vartheta_{(a)}$ és $\vartheta_{(b)}$ $(1 \leq a < b \leq l)$ cseréje a (2) kifejezést önmagába viszi át. Ez utóbbi viszont már nyílvánvaló a (2)-es alakból, mivel egy ilyen csere a külső szumma egy tetszőleges tagját a külső szumma másik tagjába viszi át, így gyakorlatilag a külső szumma összeadandói megpermutálódtak, de újra ugyanazokat a számokat adjuk össze. Megkaptuk tehát, hogy $e^{\sum_{i=1}^{s} \lambda_i \alpha_i}$ együtt-

hatója valóban szimmetrikus polinomja racionális együtthatókkal (az, hogy polinom, nem néztük, de nyílvánvaló) ϑ_j-knek, így racionális maga $e^{\sum_{i=1}^{s} \lambda_i \alpha_i}$ együtthatója. (Így a (**) alakot valóban igazoltuk, és emlékeztetünk, hogy $a_1, ..., a_n$-ről feltehető az is, hogy egészek is).

Ezek után feltehetjük, hogy a (**) egyenletben a γ_i számok összes konjugáltjai is szerepel (amelyik nem, az nulla együtthatóval), így persze nem vesztettünk az eddigi adatainkból, továbbra is γ_i-k algebrai egészek, és páronként különbözők, valamint e^{γ_i}-ik egész együtthatós lineáris kombinációja szerepel (**)-ban. Ezek után $\mathbb{K}$ jelölje azt az algebrai számtestet, amit γ_i-k $\mathbb{Q}$-hoz adjungálásával kapunk. Erről a $\mathbb{K}$ testről már előljáróban jegyezzük meg, hogy egyrészt szeparábilis bővítése $\mathbb{Q}$-nak, véges bővítése $\mathbb{Q}$-nak, illetve hogy éppen a γ_i-k minimálpolinomjainak szorzatának felbontási teste, amit a véges bővítéssel együtt kombinálva kapjuk, hogy ez egy normális bővítése $\mathbb{Q}$-nak, a normalitást pedig a szeparábilitással ötvözve, hogy $\mathbb{K}$ egy Galois bővítése $\mathbb{Q}$-nak. Mindezek azt is mutatják, hogy ezen $\mathbb{K}$ test homomorfizmusai $\mathbb{C}$-be nem mások, mint a $Gal(\mathbb{K}/\mathbb{Q})$ elemei, amelyeket most el is nevezünk $\tau_1, ..., \tau_d$-nek.

Bevezetjük $i = 1, ..., d$ esetén a következő függvényeket:

$$A_i(t) := a_1 e^{\tau_i(\gamma_1)t} + ... + a_n e^{\tau_i(\gamma_n)t} = \tau_i(a_1) e^{\tau_i(\gamma_1)t} + ... + \tau_i(a_n) e^{\tau_i(\gamma_n)t}$$

ahol a második egyenlőség abból fakad, hogy az a_j számok egészek, így azokat bármelyi τ fixen hagyja. Vegyük észre, hogy egyik sem azonosan nulla. Előbbi állítást igazolja az, hogy mivel γ_j-k különbözőek voltak, így rögzített i esetén $\tau_i(\gamma_j)$-k is különbözőek lesznek, a 4.2-es lemma ekkor garantálja, hogy $A_i(t)$ függvények egyike sem nulla. Ezek után vegyük észre, hogy a most definiálandó függvényünk sem lehet nulla a 4.2-es lemma utáni megjegyzésből adódóan:

$$B(t) = \prod_{i=1}^{d} A_i(t) = b_1 e^{\beta_1 t} + ... + b_M e^{\beta_M t}$$

ahol $\beta_1, ..., \beta_M$ páronként különböző algebrai számok, míg $b_1, ..., b_m$ egész számok, amelyek nem mindegyike 0, valamint B(1)=0. Ez utóbbi $B(1) = 0$

egyenletet írjuk is ki, mert használni fogjuk még:

$$(i) \quad B(1) = b_1 e^{\beta_1} + ... + b_M e^{\beta_M} = 0$$

Megmutatjuk, hogy tetszőleges τ Galois csoportbeli elem a $(b_k, \beta_k), k = 1, ..., M$ párokat permutálja. Ehhez lépjünk vissza egy pillanatra a $B(1)$ definíciójához, ami nem más, mint:

$$B(1) = \prod_{i=1}^{d} (\tau_i(a_1) e^{\tau_i(\gamma_1)} + ... + \tau_i(a_n) e^{\tau_i(\gamma_n)})$$

Jelölje L_j, $j = 1, ..., M$ esetén azon $(i_1, ..., i_d)$, $\quad i_1, ..., i_d \in \{1, ..., n\}$ indexek halmazát, amelyekre a $\tau_1(\gamma_{i_1}) + ... + \tau_d(\gamma_{i_d})$ összegek megegyeznek (ezek szolgáltatják az e^{β_j} tagot), ekkor $b_j = \sum_{(i_1,...,i_d) \in L_j} \tau_1(a_{i_1}) \cdot ... \cdot \tau_d(a_{i_d})$. Mivel tetszőleges τ Galois csoportbeli elem esetén $\tau\tau_1, ..., \tau\tau_d$ a $\tau_1, ..., \tau_d$ egy permutációja, így a kitevő β_j-k és együttható b_j-k egyszerre permutálódnak, méghozzá ugyanabba a (β_k,b_k) párba. Egyik fontos következménye annak, hogy tetszőleges τ permutálja a (β_k,b_k) párokat, hogy "csak simán" permutálja a β_k-kat is a τ. Ebből fakadóan ha felírnánk a β_k-knak egy szimmetrikus polinomját, akkor az egy racionális szám lenne, mivel tetszőleges automorfizmus fixen hagyja. Később még azt is felhasználjuk, hogy ha N egész számot úgy választjuk, hogy $N\beta_1, ..., N\beta_M$ mindegyike algebrai egész legyen (mondjuk ilyen N a β_j-k egész minimál polinomjainak főegyütthatóinak szorzata), akkor $N\beta_1, ..., N\beta_M$ tetszőleges egész együtthatós szimmetrikus polinomja EGÉSZ szám.

Most pedig a 4.1-es lemmában szereplő $I(t, f)$-et fogjuk használni, alkalmas t és f-ek választása mellett. Először is $r = 1, ..., M$ esetén bevezetjük a következő f_r polinomot:

$$f_r(x) = N^{Mp} \frac{(x - \beta_1)^p \cdot ... \cdot (x - \beta_M)^p}{x - \beta_r}$$

ahol p a későbbiekben tisztázandó jó nagy prímszámot fog jelölni és N olyan, hogy $N\beta_1, ..., N\beta_M$ mind algebrai egészek, továbbá ez a N^{Mp} szorzótényező

fogja garantálni, hogy a későbbiekben megjelenő szimmetrikus kifejezések $\beta_1, ..., \beta_M$-ben szimmetrikusak lesznek $N\beta_1, ..., N\beta_M$-ben is. Az f_r polinom fokát m-el fogjuk jelölni a későbbiekben (így $m = Mp - 1$). Ekkor tekintsük megint csak $r = 1, ..., M$ esetén a következő kifejezést:

$$J_r := \sum_{k=1}^{M} b_k I(\beta_k, f_r)$$

Innentől a következő a célunk:

- nagy p-re $J_1 \cdot ... \cdot J_M$ egy egész szám, ami osztható $(p-1)!$-al, de p-vel nem (így speciálisan nemnulla), ami alapján $J_1 \cdot ... \cdot J_M$ abszolút értéke leaglább $(p-1)!$ lesz.
- $I(t, f)$ definícióját használva egy triviális becsléssel $|J_1 \cdot ... \cdot J_M|$-re valamilyen p-től független c-re c^p alakú felső becslést adni

Ez utóbbi két tulajdonság fogja szolgáltatni az ellentmondást, mivel $(p-1)!$ gyorsabban tart a végtelenbe, mint c^p. Először is J_r a 4.1-es lemmát használva és (i)-t:

$$(ii) \quad J_r = \sum_{k=1}^{M} b_k (e^{\beta_k} \sum_{j=0}^{m} f_r^{(j)}(0) - \sum_{j=0}^{m} f_r^{(j)}(\beta_k)) = -\sum_{k=1}^{M} b_k \sum_{j=0}^{m} f_r^{(j)}(\beta_k) =$$

$$= -\sum_{j=p-1}^{m} \sum_{k=1}^{M} b_k f_r^{(j)}(\beta_k)$$

ahol az utolsó egyenlőségnél a szummát megcseréltük és $j = (p-1)$-től kezdtük a szummát, mivel az előtte álló $(p-1)$-nél kisebb deriváltak esetén azokba β_k-t helyettesítve 0-t kapunk. Vegyük észre azt is, hogy rögzített r esetén és $j = (p-1)$-re a

$$\sum_{k=1}^{M} b_k f_r^{(p-1)}(\beta_k) = b_r f_r^{(p-1)}(\beta_r) = N^{Mp}(p-1)! \prod_{i \neq r} (\beta_r - \beta_i)^p$$

Ahhoz, hogy megértsük $J_1 \cdot ... \cdot J_M$ valóban egész, még hozzá a fentebb leírt tulajdonságokkal, írjuk ki részletesen $J_1, .., J_M$-et:

$$J_1 = (N^{Mp}(p-1)! \prod_{i\neq 1}(\beta_1 - \beta_i)^p) + ... + (b_1 f_1^{(m)}(\beta_1) + ... + b_M f_1^{(m)}(\beta_M))$$

$$...$$

$$J_M = (N^{Mp}(p-1)! \prod_{i\neq M}(\beta_M - \beta_i)^p) + ... + (b_1 f_M^{(m)}(\beta_1) + ... + b_M f_M^{(m)}(\beta_M))$$

Amikor a szorzást elvégezzük és mindent-mindennel szorzunk, úgy képzeljük el, hogy $J_1, ..., J_M$-en belül direkt elhelyeztünk zárójeleket, és a belső zárójeleket mint egy egésznek tekintve szorzunk mindent mindennel, így például az első tagja a szorzatnak: $N^{M^2p} \cdot (p-1)!^M \prod_{j=1}^{M} \prod_{i\neq j} (\beta_j - \beta_i)^p$, míg az utolsó: $\prod_{l=1}^{M}(b_1 f_l^{(m)}(\beta_1) + ... + b_M f_l^{(m)}(\beta_M))$. Amikor a szorzásnál J_k-ból kiveszünk egy zárójelet , azt "jellemzi" az, hogy az f_k polinom hányadik deriváltját is nézzük abban a zárójelben. Végezzünk tehát úgy egy csoportosítást a kapott összeadandokból, hogy külön előbb összeadjuk azokat az M-tényezős szorzatokat: $\prod_{l=1}^{M}(b_1 f_l^{(t_l)}(\beta_1) + ... + b_M f_l^{(t_l)}(\beta_M))$, ahol $t_1 + ... + t_M$ állandó. Minden egyes ilyen csoportról azt állítjuk, hogy az összeg egy egész. A legelső csoport, amikor is $t_1 + ... + t_M = M(p-1)$, azaz az egytagú $N^{M^2p} \cdot (p-1)!^M \prod_{j=1}^{M} \prod_{i\neq j} (\beta_j - \beta_i)^p$ összeg szimmetrikus $N\beta_1, ..., N\beta_M$-ben így egy egész, sőt, ha p olyan prím, hogy nagyobb mint N és $\left|\prod_{i\neq j}(N\beta_i - N\beta_j)\right|$ (ami fix, p-től független), akkor az első szám p-vel nem osztható. A többi esetben, amikor is $t_1 + ... + t_M > M(p-1)$ úgy érvelünk, hogy $N\beta_1, ..., N\beta_M$ olyan egész együtthatós polinomját kapjuk, amiből kiemelhető a p!, valamint minden Galois csoportbeli elem fixen hagyja az összeadandót, ami alapján ez egy algebrai egész szám, miközben racionális, tehát egy egész szám, ami p! kiemelése miatt p!-al osztható is. A p! azért emelhető ki minden összeadandóból, mivel egy $\prod_{l=1}^{M}(b_1 f_l^{(t_l)}(\beta_1) + ... + b_M f_l^{(t_l)}(\beta_M))$ szorzótényezők közül legalább az egyikben p! alkalommal deriváltunk, továbbá a végeredmény nyílván $N\beta_1, ..., N\beta_M$ egészegyüttható polinomja lesz, lássuk, hogy miért hagyja

fixen ezt minden eleme a Galois csoportnak: egy τ permutálja (β_k, b_k) párokat, valamint ennek következtében τ permutálja az $f_1, ..., f_M$ polinomokat is, így egy $\prod_{l=1}^{M}(b_1 f_l^{(t_l)}(\beta_1) + ... + b_M f_l^{(t_l)}(\beta_M))$ tag szó szerint egy olyan típusú M-tényezős szorzatba megy át, amilyen ő maga, tehát egy τ csak megpermutálja az összeadandókat. Tehát $t_1 + ... + t_M = M(p-1)$ esetén az összeg egy $(p-1)$!-al osztható szám, míg $t_1 + ...t_M > M(p-1)$ esetén p!-al is osztható, tehát végül kaptuk, hogy $J_1 \cdot ... \cdot J_M$ osztható $(p-1)$!-al, de nem p-vel, így $|J_1 \cdot ... \cdot J_M| \geq (p-1)!$.

Mivel J_r M darab (ami fix) $I(t, f)$ típusú kifejezés összege (fix b_k együtthatókkal), ezért annak belátásához, hogy $|J_1 \cdot .... \cdot J_M| \leq c^p$ elég csak azt belátni, hogy egy $I(\beta_k, f_r)$ abszolút értéke felülbecsülhető $d^{\deg f_r} = d^{Mp-1} \leq c^p$-el, ahol c független deg f_r-től, ezt egy egyszerű triviális becsléssel érhetjük el:

$$\left|I(\beta_k, f_r)\right| = \left|\int_0^{\beta_k} e^{\beta_k - u} f_r(u) du\right| \leq |\beta_k|\, e^{|\beta_k|} \max_{u \in [0;\beta_k]} \left|f_r(u)\right| \leq$$

$$\leq |\beta_k|\, e^{|\beta_k|} (\prod_{i \neq k} \max_{u \in [0;\beta_i]} |u - \beta_i|)^p \cdot \max_{u \in [0;\beta_k]} (|u - \beta_k|^p, 1)$$

ahol az utolsó kifejezés világos, hogy tényleg felülbecsülhető valamilyen c^p-vel, így ezzel teljessé téve a Lindemann-Weierstrass tétel bizonyítását.

□

Hivatalosan a Lindemann-Weierstrass tétel, amely 1885-ben született, nem így volt kimondva, hanem ez a fajta egyszerűsítése Alan Baker matematikusnak köszönhető, íme a tétel eredeti 1885-ös formája:

4.14. tétel. *Ha $\alpha_1, ..., \alpha_n$ $\mathbb{Q}$ felett lineárisan független algebrai számok, akkor $e^{\alpha_1}, ..., e^{\alpha_n}$ algebrailag függetlenek $\mathbb{Q}$ felett.*

Bizonyítás. Ha $e^{\alpha_1}, ..., e^{\alpha_n}$ algebrailag nem függetlenek, akkor létezik egy egész együtthatós n változós polinom, aminek gyöke a $(e^{\alpha_1}, ..., e^{\alpha_n})$ n-es. Ezt a polinomot kiírva a helyettesítés után ilyen alakú egyenletet kapunk:

$$\sum_{i_1,...,i_n} a_{i_1,...,i_n} e^{i_1\alpha_1 + ... + i_n\alpha_n} = 0$$

ahol az $a_{i_1,...,i_n}$ együtthatók nemnulla egészek. Ekkor az újrafogalmozott Lindemann-Weierstrass tétel szerint (4.10-es tétel) nem lehet, hogy az $i_1\alpha_1 + ... + i_n\alpha_n$ számok közül mindegyik különböző, de akkor az $\alpha_1, ..., \alpha_n$ számok mégis csak lineárisan függők.

□

Bár nyertük, hogy mind π és e transzcendensek, mai napig megoldatlan kérdés, hogy vajon $\pi + e$ vagy πe transzcendensek-e, a sejtés az, hogy mindkettő az. A témakörhöz tartozik egy utóbbi kérdésnél sokkal erősebb megoldatlan sejtés, amihez két gyors definíciót nézzünk meg:

4.15. definíció. *Legyen $\mathbb{F} \leq \mathbb{K}$ testbővítések, ekkor $V \subset \mathbb{K}$ transzcendens bázisa $\mathbb{K}$-nak $\mathbb{F}$ felett, ha $\mathbb{K}$ algebrai bővítése $\mathbb{F}(V)$-nek és V algebrailaig független $\mathbb{F}$ felett.*

Bizonyítás nélkül közlünk néhány állítást a transzcendens bázisról, ezek bizonyítása például [3]-ban megtalálhatóak. Az, hogy létezik transzcendens bázis, az fogja garantálni, hogy egy maximális algebrailag független V halmaz $\mathbb{F}$ felett pont olyan lesz a maximalitás miatt, hogy $\mathbb{K}$ algebrai bővítése $\mathbb{F}(V)$-nek, sőt, pontosan a maximális algebrailag független halmazok lesznek transzcendens bázisok. Persze ilyen maximális algebrailag független halmazt az ember Zorn-lemmával talál (mint ahogyan azt tettük a 3.8-as lemmában). Sőt, mi több, az is igaz, hogy bármely kettő transzcendens bázis számossága megegyezik, ez vezet el a következő definícióhoz:

4.16. definíció. *$\mathbb{F} \leq \mathbb{K}$ testbővítés transzcendens foka egy transzcendens bázisának számossága.*

Ez után kimondhatjuk a sokkal általánosabb sejtést, amelyet S. Schanuel fogalmazott meg:

Sejtés: $\alpha_1, ..., \alpha_n$ lineárisan független komplex számok $\mathbb{Q}$ felett, ekkor a $\mathbb{Q}(\alpha_1, ..., \alpha_n, e^{\alpha_1}, ..., e^{\alpha_n})$ test $\mathbb{Q}$ feletti transzcendens foka legalább n.

Ha tehát Schanuel sejtése igaz lenne, akkor tekintve az 1, $2\pi i$, e, $e^{2\pi i}$ által generált testet a racionálisak felett, kapnánk, hogy ennek transzcendens foka legalább 2, azaz π és e algebrailag függetlenek $\mathbb{Q}$ felett, amiből bőven következik, hogy mind a $\pi + e$ és πe transzcendensek.

5. Siegel lemmája és a Hat exponenciális tétel

Ebben a szakaszban a Siegel lemmát fogjuk belátni, amelynek mára rengeteg variánsa ismert, mi ezek közül 3-at látunk be, amely először egész megoldásai egy egész együtthatós homogén lineáris egyenletrendszernek és annak nagyságára vonatkozik, majd a következő verzió algebrai egész együtthatós homogén lineáris egyenletrendszerről és annak algebrai egészekből álló megoldására mond valamit, ezt lesz a legnehezebb bebizonyítani a 3 változat közül, majd a 3-ik verzó algebrai együtthatós, algebrai egészekből álló megoldás létezéséről szól és annak valamilyen értelemben vett nagyságáról mond valamit. Siegel lemmája utána a Hat exponenciális tétel következik és annak egy alkalmazása. A bizonyítások során [6] és [4]-t követjük.

5.1. tétel. *(Siegel lemma, 1-es verzió) Legyen* $\sum_{i=1}^{N} a_{i_j} x_i = 0$ $j = 1, ..., M$*-re,* $M < N$ *egy* N *változós* M *ismeretlenes egész együtthatós homogén lineáris egyenletrendszer, valamit legyen* $|A| := \max_{1 \le i \le M, 1 \le j \le N} \left|a_{i_j}\right|$*. Ekkor létezik egy nemtriviális egészekből álló* $(x_1, ..., x_N)$ *megoldás, amelyre* $\left|x_j\right| < 2 + (N|A|)^{\frac{M}{N-M}}$*,* $j = 1, .., N$*.*

Bizonyítás. Kissé következetlenül, de jelöljük A-val a homogén lineáris egyenletrendszerhez tartozó mátrixot (ezért jelöltük a fenti mennyiséget $|A|$-val). Vezessük be még a következő jelöléseket:

$$\Lambda := \{\underline{x} \in \mathbb{Z}^N : A\underline{x} = \underline{0}\}$$

valamint $|\underline{x}| := \max_{\underline{x} \text{ koordinátái}} \left|x_j\right|$. Ezek mellett még egy plusz jelölés $H \in \mathbb{Z}_{>0}$ mellett:

$$C_H^N := \{\underline{x} \in R^N : |x| \le H\}$$

Ekkor nyílvánvalóan $\left|C_H^N \cap \mathbb{Z}^N\right| = (2H+1)^N$, valamint vegyük észre, hogy az $A : \mathbb{R}^N \longrightarrow \mathbb{R}^M$ lineáris leképezésre teljesül, hogy ha $\underline{x} \in C_H^N$, akkor $A\underline{x} \in C_{N|A|H}^M$. Szintén világos, hogy:

$$\left|C_{N|A|H}^M \cap \mathbb{Z}^M\right| = (2N|A|\,H + 1)^M$$

Válasszuk H egy olyan pozitív egész, ami tudja:

$$(N|A|)^{\frac{M}{N-M}} \leq 2H < (N|A|)^{\frac{M}{N-M}} + 2$$

Ezzel felírhatjuk a következő becslés sorozatot:

$$\left|C_H^N \cap \mathbb{Z}^N\right| = (2H+1)^N = (2H+1)^M (2H+1)^{N-M} \geq$$
$$\geq (2H+1)^M (N|M|)^M > (2N|A|\, H+1)^M = \left|C_{N|A|H} \cap \mathbb{Z}^M\right|$$

Speciális nem lehet, hogy A injektíven képezi bele a $C_H^N \cap \mathbb{Z}^N$ halmazt a $C_{N|A|H}^M \cap \mathbb{Z}^M$ halmazba. Így $\exists \underline{x}, \underline{y} \in C_H^N \cap \mathbb{Z}^N, \underline{x} \neq \underline{y}$, hogy $A\underline{x} = A\underline{y}$ és így $A(\underline{x} - \underline{y}) = 0$. Ekkor fennáll erre az egész megoldás vektorra, hogy $\left|\underline{x} - \underline{y}\right| \leq 2H < (N|A|)^{\frac{M}{N-M}} + 2$.

□

Ezt felhasználva szeretnénk további algebrai számtestekbeli együtthatós lineáris egyenletrendszerek megoldásainak nagyságáról mondani valamit, ehhez azonban néhány dolgot felidézünk az algebrai számelmélet területéről. Ezekből néhány állítást a függelékben belátunk, hogy melyiket, szokás szerint jelezzük valahogyan az állítás után.

Legyen $\mathbb{K}$ egy algebrai számtest, és legyenek adottak a $\sigma_1, .., \sigma_d$ beágyazásai a komplex számtestbe, definiáljuk egy $\alpha \in \mathbb{K}$ "magasságát":

$$H(\alpha) := \max\{\left|\sigma_l(\alpha)\right| : l = 1, ..., d\}$$

Megjegyezném, hogy ez a sajátos fordítása az angol "height" szónak, amit azért szeretnék kiemelni, mert sok szerző a "height" kifejezést egy α algebrai szám minimálpolinomjának együtthatóinak abszolút értékének minimumaként deiniálja, és e fenti definíció eredményeképp kapott számra pedig a "size" kifejezést használja.

Ha adott egy $\mathbb{K}$ algebrai számtest, akkor a $\mathbb{K}$-ba eső algebrai egészek gyűrűjét mostantól $\mathcal{O}_{\mathbb{K}}$-val fogjuk jelölni. Egy fontos tény, hogy $\mathcal{O}_{\mathbb{K}}$ egy d-rangú szabad $\mathbb{Z}$ modulus, azaz léteznek $\omega_1, .., \omega_d \in \mathcal{O}_{\mathbb{K}}$, hogy bármely $\alpha \in \mathcal{O}_{\mathbb{K}}$

előáll egyértelműen egész együtthatós lineáris kombinációjaként a $\omega_1, ..., \omega_d$ számoknak. Egy ilyen $\omega_1, ..., \omega_d$-est szokás egész bázisnak is nevezni, persze egy egész bázis közel sem egyértelmű. Egy ilyen egész bázisnak a létezését a függelékbe részletezzük.

Még egy tétel, hogy ha adott egy $\omega_1, ..., \omega_d$ egész bázis (valamely most rögzített $\mathbb{K}$ testtel persze), és definiáljuk a következő $d \times d$-es mátrixot: $W := (\sigma_l(\omega_k))_{1 \geq l,k \geq d}$, akkor W invertálható. Ezt úgy szintén a függelékben részletezzük.

5.2. tétel. *(Siegel lemma, 2-es verzió) Ha adott egy d-edfokú algebrai számtest és $A := (\alpha_{i_j})$ $M \times N$-es mátrix, ahol $M < N$ és $\alpha_{i_j} \in \mathcal{O}_{\mathbb{K}}$. Ezek mellett legyen:*

$$H(A) := \max\{H(\alpha_{i_j}) : 1 \leq i \leq M, 1 \leq j \leq N\}$$

Ekkor létezik a $A\underline{x} = \underline{0}$ homogén lineáris egyenletrendszernek egy nemtriviális $\underline{x} \in \mathcal{O}_{\mathbb{K}}^N$ megoldása, amire:

$$\max_{1 \leq j \leq N} H(x_j) \leq B_{\mathbb{K}}(M, N) H(A)^{\frac{M}{N-M}}$$

ahol $B_{\mathbb{K}}(M, N)$ egy $M, N, \mathbb{K}$-tól függő konstans.

Bizonyítás. A bizonyítás tulajdnoképpen az 5.1-es tételre való visszajátszás az előbb felsorolt fogalmak birtokában. Vegyünk tehát egy $\omega_1, ..., \omega_d$ egész bázist, és legyen a W mátrix úgy, mint fentebb. Bármelyik α_{i_j} A-beli elemre létezik $a_{ijk} \in \mathbb{Z}$ $1 \leq k \leq d$, hogy:

$$\alpha_{ij} = \sum_{k=1}^{d} a_{ijk} \omega_k$$

Ha most alkalmazzuk a $\sigma_1, ..., \sigma_d$ beágyazásokat a fenti egyenletre, akkor kapjuk, hogy:

$$\sigma_l(\alpha_{ij}) = \sum_{k=1}^{d} a_{ijk} \sigma_l(\omega_k)$$

minden $1 \leq l \leq d$ esetén. Definájuk a következő vektort.

$$\underline{\alpha_{ij}} := (\sigma_1(\alpha_{ij}, ..., \sigma_d(\alpha_{ij}))^T = W(a_{ij1}, ..., a_{ijd})^T$$

Így W^{-1} átszorzás után kapjuk a következő egyenlőséget (és egy újabb vektor deinícióját is):

$$W^{-1}(\sigma_1(\alpha_{ij}, ..., \sigma_d(\alpha_{ij}))^T = (a_{ij1}, ..., a_{ijd})^T := \underline{a_{ij}}$$

Ha elnevezzük W^{-1} elemeit v_{kl}-el, akkor a fenti egyenlet az $\underline{a_{ij}}$ elemeire a következőket jelenti:

$$a_{ijk} = \sum_{l=1}^{d} v_{kl}\sigma_l(\alpha_{ij})$$

Ekkor igaz az is, hogy:

$$(*) \quad \left|a_{ijk}\right| \leq d \max_{1\leq l\leq d} v_{kl}\sigma_l(\alpha_{ij}) \leq dC_{\mathbb{K}}H(A)$$

ahol a $C_{\mathbb{K}} := \max_{1\leq k,l\leq d}|v_{kl}|$, és vegyük észre, hogy ez a konstans csakis a $\mathbb{K}$ testtől függ.

Keressük most az $\underline{x} \in \mathcal{O}_{\mathbb{K}}^N$, $A\underline{x} = \underline{0}$ megoldást a következő alakban:

$$\underline{x} = (\sum_{l=1}^{d} b_{1l}\omega_l, ..., \sum_{l=1}^{d} b_{Nl}\omega_l)$$

ahol $b_{jl} \in \mathbb{Z}$ és $1 \leq j \leq N, 1 \leq j \leq d$. Ezt lebontva az $A\underline{x} = \underline{0}$ i-ik sorára:

$$(**) \quad \sum_{j=1}^{N} \alpha_{ij}x_j = \sum_{j=1}^{N}(\sum_{k=1}^{d} a_{ijk}\omega_k)(\sum_{l=1}^{d} b_{jl}\omega_l) = \sum_{j=1}^{N}\sum_{l=1}^{d}\sum_{k=1}^{d} a_{ijk}b_{jl}\omega_k\omega_l = 0$$

És itt használjuk ki mégegyszer igen erősen az egész bázis tulajdonságait, ugyanis $\omega_k\omega_l \in \mathcal{O}_{\mathbb{K}}$, így ők is kifejezhetőek az ω_m-ek egész együtthatós lineáris kombinációjaként, ehhez legyenek $c_{klm} \in \mathbb{Z}$ olyan egész számok, amelyre:

$$\omega_k\omega_l = \sum_{m=1}^{d} c_{klm}\omega_m$$

ezt (**)-ba visszaírva:

$$\sum_{m=1}^{d}\sum_{j=1}^{N}\sum_{l=1}^{d}\sum_{k=1}^{d} a_{ijk}b_{jl}c_{klm}\omega_m = 0$$

ami PONTOSAN akkor teljesülhetne, ha ω_m együtthatói mindegyike nulla, azaz: $\sum_{j=1}^{N}\sum_{l=1}^{d}\sum_{k=1}^{d} a_{ijk}b_{jl}c_{klm} = 0$. Ez pedig a b_{jl}-ekben nézve egy Nd ismeretlenes, és az ω_m-ek és minden $i = 1, ..., M$ sor esetén összesen Md darab egyenletet jelent, ahol most már minden egész szám, tökéletesen előkészítve a terepet a Siegel lemma 1-es verziójára. Ha visszanézzük (*)-ban az a_{ijk}-ra tett becslést és belekalkulkálva a c_{klm}-ek abszolút értékét, amelyek szintén csak egy $\mathbb{K}$-tól függő konstansok, akkor kapjuk a b_{jl}-ekre a következő becslést:

$$\max_{j,l}\left|b_{jl}\right| \leq 2 + (Nd \cdot dCH(A))^{\frac{Md}{Nd-Md}}$$

ahol C egy $\mathbb{K}$-tól függő konstans, és ezeket a $b_{j,l}$-eket visszaírva az $\underline{x}$ megoldás vektor koordinátáinak magasságára a következőt jelenti:

$$H(x_j) \leq d(2 + (Nd \cdot dCH(A))^{\frac{M}{N-M}}) \max_{1\leq l\leq d} H(\omega_l)$$

ahol az utolsó maximum úgy szintén csak egy $\mathbb{K}$-tól függő konstans, valamint ez utóbbi egyenlőtlenségből már következik maga a tétel állítása.

□

Még egy gyors fogalomra emlékeztetünk, mégpedig az $\alpha_1, ..., \alpha_n$ számok nevezőjére, ami a következő:

$$D(\alpha_1, ..., \alpha_n) := \min\{c \in \mathbb{Z}_{>0} : c \cdot \alpha_j \in \mathcal{O}_{\mathbb{K}}, 1 \leq j \leq n\}$$

Egy A mátrix esetén $D(A)$ a mátrix elemeinek nevezőjét jelenti.

5.3. tétel. *(Siegel lemma, 3-as verzió) Legyen adott egy $\mathbb{K}$ algebrai számtest és egy $M \times N$, $M < N$ mátrix, $\mathbb{K}$-beli elemekkel. Ekkor az $A\underline{x} = \underline{0}$-nak létezik*

egy nemtriviális $\underline{x} \in \mathcal{O}_{\mathbb{K}}^N$*-beli megoldása, amelyre:*

$$\max_{1\leq j\leq N} H(x_j) \leq B_{\mathbb{K}}(M,N)(D(A)H(A))^{\frac{M}{N-M}}$$

Bizonyítás. A bizonyítás abból áll, hogy, egy $\underline{x}$ megoldása az $A\underline{x} = \underline{0}$-nak akkor és csak akkor ha $\underline{x}$ megoldása az $A'\underline{x} = \underline{0}$, ahol $A' = D(A)A$, ez utóbbira pedig a Siegel lemma 2-es verziójának állítását alkalmazva kapjuk az eredményt. □

Megjegyzés: Itt szükésgesnek érezzük megjegyezni azt, hogy a 3-as verzióban kiszámított $B_{\mathbb{K}}(N,M)$ konstans ugyanaz, mint a 2-es verzióban, illetve azt, és ez a még fontosabb, amit egy ponton később ki fogunk használni, hogy $B_{\mathbb{K}}(N,M) = C'(CN)^{\frac{M}{N-M}}$ alakú, ahol C, C' ettől a $\mathbb{K}$ testtől függő konstans, nem az N, M számoktól függ.

Újabb néhány fogalomra emlékeztetünk. Ha adott egy $\mathbb{K}$ algebrai számtest, és az ő $\sigma_1, ..., \sigma_d$ beágyazásai, akkor $\alpha \in \mathbb{K}$-ra $N_{\mathbb{K}}(\alpha)$ jelöli a következő számot:

$$N_{\mathbb{K}}(\alpha) = \prod_{k=1}^{d} \sigma_k(\alpha)$$

szimplán $N(\alpha)$-t írunk, ha $N_{\mathbb{Q}(\alpha)}(\alpha)$-ra gondolunk. Ekkor igaz az, hogy $N_{\mathbb{K}}(\alpha) = N(\alpha)^{[\mathbb{K}:\mathbb{Q}(\alpha)]}$, ez abból fakad, hogy $N(\alpha)$ személy szerint az α konjugáltjainak szorzata (így speciálisan nemnulla ez a szám, ha α maga nemnulla és algebrai egész α esetén pedig egész ez a szám) és a $\sigma_k(\alpha)$ számok pedig $[\mathbb{K} : \mathbb{Q}(\alpha)]$ alkalommal felsorolva α konjugáltjai, ezt a függelékben bizonyítjuk is.

Mindezek implikálják még azt is, hogy ha $\alpha \in \mathcal{O}_{\mathbb{K}}$, akkor $1 \leq \left|N_{\mathbb{K}}(\alpha)\right| \leq H(\alpha)^{d-1}|\alpha|$, mivel a σ_k közül az egyik az identitás.

Mindezek mellett a Hat exponenciális tétel bizonyítása során fel fogjuk használni a maximum elvet és azt, hogy egy ha adott egy f egészfüggvény, aminek rendje ρ, akkor egy R sugarú körben nem lehet több gyöke f-nek, mint AR^{ρ}, A egy f-től függő konstans. Ez utóbbit a függelékben bizonyítjuk.

5.4. tétel. *(Hat exponenciális tétel) Legyen* $x_1, x_2 \in \mathbb{C}$ *lineárisan függetlenek* $\mathbb{Q}$ *felett, valamint* $y_1, y_2, y_3 \in \mathbb{C}$ *lineárisan függetlenek* $\mathbb{Q}$ *felett. Ekkor az* $e^{x_i y_j}$

számok közül legalább az egyik transzcendens.

Bizonyítás. Tegyük fel, hogy mind a hat szám algebrai, ekkor tekinthetjük az általuk generált algebrai számtestet, amit $\mathbb{K}$-val jelölünk. Definiálni fogunk egy egészfüggvényt, aminek egyelőre elég sok paraméterét nem mondjuk meg:

$$F(z) := \sum_{i=1}^{r} \sum_{j=1}^{r} a_{ij} e^{(ix_1+jx_2)z}$$

ahol $a_{ij} \in \mathcal{O}_{\mathbb{K}}$ lesz majd úgy, hogy ha $F(k_1y_1 + k_2y_2 + k_3y_3 = 0$ teljesüljön, valahányszor $1 \leq k_1, k_2, k_3 \leq n$ és $k_1, k_2, k_3 \in \mathbb{Z}$, ahol n ismét egy újabb paraméter, amit még nem mondtunk meg. Ez utóbbi helyeken felhívjuk a figyelmet, hogy az $e^{(ix_1+jx_2)(k_1y_1+k_2y_2+k_3y_3)}$ $\mathbb{K}$-beli értéke vesz fel.

Ez tulajdonképpen n megmondása után az a_{ij}-kre nézve egy r^2 ismeretlenes, n^3 darab egyenletből álló homogén lineáris egyenletrendszer. Ahhoz, hogy Siegel lemmáját egyáltalána alkalmazhassuk Siegel lemmáját, kell, hogy $r^2 > n^{\frac{3}{2}}$, előre eláruljuk, hogy $r = 8n^{\frac{3}{2}}$-et fogunk választani (még mindig nem mondtuk meg, mi az n!).

Jelöljük D-vel az $e^{x_iy_j}$ számok közös nevezőjét, ekkor ez utóbbi egyenletrendszerben szereplő együtthatók (amik a $e^{(ix_1+jx_2)(k_1y_1+k_2y_2+k_3y_3)}$-k) közös nevezője legfeljebb D^{6rn}, továbbá egy ezen együtthatók magassága felülbecsülhető e^{c_0rn}-el, ahol c_0 független n-től (mert elég, ha az $e^{x_iy_j}$-k magasságát felülbecsülöm e^{c_0}-val. Siegel lemmája ekkor azt mondja nekünk (a 3-as verzió), hogy létezik nemtriviális $a_{ij} \in \mathcal{O}_{\mathbb{K}}$ megoldása az egyenletrendszernek, amelyre:

$$\max_{i,j} H(a_{ij}) \leq B_{\mathbb{K}}(n^3, 8n^{\frac{3}{2}})(D^{68n^{\frac{3}{2}}n} e^{c_0 8n^{\frac{3}{2}}n})^{\frac{n^3}{64n^3-n^3}} \leq e^{c_1 n^{\frac{5}{2}}}$$

valamilyen c_1, n-től nem függő konstanssal (ez pontosan a Siegel lemmák utáni megjegyzésből fakad). Maga az $F(z)$ nem lesz azonosan nulla, mivel az x_1, x_2 lineárisan függetlenek $\mathbb{Q}$ felett, így mindegyik $ix_1 + jx_2$ kitevő különböző, így az előző fejezetbeli egyik állítás miatt egy ilyen függvény nem lehet azonosan nulla. Most jön egy apró, de finom észrevétel, hogy akkor hogyan is válasszuk majd meg az n-et, az biztos, hogy $F(z)$ egy elsőrendű függvény

lesz, így gyökei egy R sugarú körben konstansszor R körül mozoghatnak, míg az

$$\{k_1y_1 + k_2y_2 + k_3y_3 : k_1y_1 + k_2y_2 + k_3y_3 \in D_R(0), k_1, k_2, k_3 \in \mathbb{Z}_{>0}\}$$

halmaz számossága konstansszor R^3 körül mozog, így nem lehet az összes ilyen alakú szám gyöke az F(z)-nek. Legyen tehát s a legkisebb természetes szám, amire tetszőleges $1 \leq k_1, k_2, k_3 \leq s$ esetén $F(\sum_{i=1}^{3} k_i y_i) = 0$, de $F(\sum_{i=1}^{3} k_i y_i) \neq 0$ valamely $k_i = s+1$ és $1 \leq k_1, k_2, k_3 \leq s+1$ mellett. Ekkor definíció szerint $s \geq n$ (n-et még persze továbbra sem mondtuk meg!). Ez utóbbit elnevezzük w-el, legyen tehát $w = \sum_{i=1}^{3} k_i y_i$ (ahol nem tűnik el az F).

Az a_{ij}-k magasságaira tett megfigyeléseink az $F(w)$ magasságára is mond valamit:

$$H(F(w)) \leq \sum_{i=1}^{r}\sum_{j=1}^{r} H(a_{ij})H(e^{(ix_1+jx_2)(k_1y_1+k_2y_2+k_3y_3)}) \leq C_0^{n^{\frac{5}{2}}+(s+1)r} \leq C_1^{s^{\frac{5}{2}}}$$

valamely C_1, n-től független konstansra. Viszont, mivel D volt a közös nevezője az az $e^{x_iy_j}$ számoknak, és a $a_{ij} \in \mathcal{O}_{\mathbb{K}}$, ezért $D^{6r(s+1)}F(w)$ már biztosan egy algebrai egész! Így a tétel megkezdése előtti emlékeztetőkkel:

$$1 \leq N_{\mathbb{K}}(D^{6r(s+1)}F(w)) \leq H(D^{6r(s+1)}F(w))^{[\mathbb{K}:\mathbb{Q}]-1}\left|D^{6r(s+1)}F(w)\right|$$

speciálisan az előbb nyert becsléseket $\left|F(w)\right|$-re:

$$(*) \quad \left|F(w)\right| \geq H(F(w))^{1-[\mathbb{K}:\mathbb{Q}]}D^{-6r(s+1)[\mathbb{K}:\mathbb{Q}]} \geq C_2^{-s^{\frac{5}{2}}}$$

Most megmutatjuk, hogy (*) elég nagy n esetén ellentmondásra vezet. Tekintsük a következő holomorf függvényt:

$$(**) \quad G(z) = F(z)\prod_{1\leq k_1,k_2,k_3\leq s}\frac{w-(k_1y_1+k_2y_2+k_3y_3)}{z-(k_1y_1+k_2y_2+k_3y_3)}$$

A maximum elvet szeretnénk használni, egy alkalmas R sugarú körre,

ezt eláruljuk előre, hogy $R = s^{\frac{3}{2}}$-ed lesz ez az alkalmas kör, bár további kritériumaink a R sugarú körrel az lesz, hogy $|w| < R$ és minden $|z| = R$ esetén álljon fent:

$$\big|z - (k_1y_1 + k_2y_2 + k_3y_3)\big| \geq \frac{R}{2}$$

valahányszor $(k_1y_1 + k_2y_2 + k_3y_3) \in \{k_1y_1 + k_2y_2 + k_3y_3 : 1 \leq k_1, k_2, k_3 \leq s\}$. Ezzel nyertünk az n nagyságára valamilyen feltételt, ugyanis ha s elég nagy, akkor $R = s^{\frac{3}{2}}$ valóban teljesíteni tudja az előbbi feltételt, mivel $n \leq s$, ezért elég n-et elég nagynak választani, hogy ez teljesüljön. Mivel $F(w) = G(w)$, ezért G-re a maximum elvet alkalmazva a R sugarú kör mellett kapjuk:

$$\big|F(w)\big| \leq |F|_R \left(\frac{C_3 s}{R}\right)^{s^3}$$

ahol $|F|_R$ az $|F|$ maximumát jelöli az R sugarú körön. Ezt becsülhetjük háromszög egyenlőtlenségeken keresztül az a_{ij}-k magasságára tett becslésekkel (és így abszolút értékükre is van egy becslésünk) és az $|e^z| \leq e^{|z|}$-val:

$$|F|_R \leq r^2 e^{c_1 n^{\frac{5}{2}}} e^{c_1 r R}$$

mindent egybevetve és beírva, mi volt a R, kapjuk:

$$C_2^{-s^{\frac{5}{2}}} \leq \big|F(w)\big| \leq r^2 e^{c_1 n^{\frac{5}{2}}} e^{c_1 r R} \left(\frac{C_3 s}{s^{\frac{3}{2}}}\right)^{s^3}$$

ami elég nagy s-re ellentmondás, elég nagy s pedig az n elég nagy választásával elérhető. □

Itt mindenképpen érdemes megemlíteni a négy exponenciális sejtést, amely x_1, x_2 és y_1, y_2 párokról szólnak, amelyek lineárisan függetlenek $\mathbb{Q}$ felett. Ekkor legalább az egyik $e^{x_i y_j}$ transzcendens.

1971-es Putnam feladat volt, hogy ha α valós olyan, hogy $1^\alpha, 2^\alpha, 3^\alpha ...$ mindegyike egész, akkor α egy nemnegatív egész szám. A bizonyítás nagyon szellemes és az ötlete az x^α függvény vizsgálata, osztott diferenciák segítségével, az érdeklődő olvasó [5]-ban megtalálhatja az eredti bizonyítást. Mi most egy másik utat mutatunk.

5.5. tétel. *Ha c olyan, hogy $2^c, 3^c, 5^c$ egész, akkor c egy nemnegatív egész.*

Bizonyítás. Ha c-ről kihoznánk, hogy racionális, onnan már könnyen láthatóan c-nek egy nemnagatív egésznek kell lennie. tegyük fel tehát, hogy c irracionális, ekkor az $x_1 = 1, x_2 = c$ és $y_1 = \log 2, y_2 = \log 3, y_3 = \log 5$ választással a hat exponenciális tételt alkalmazva a $2, 3, 5, 2^c, 3^c, 5^c$ számok legalább egyike transzcendens, ellentmondva a kiindulási feltételnek, így a baj ott lehetett, hogy c mégiscsak raionális. □

6. Függelék

Itt ebben a szakaszban bizonyítjuk az előbbi fejezetekben felbukkanó egy-egy állításokat, amiket ott akkor helyben nem részleteztünk. Így is lesz olyan, amit csak kimondunk, mert bizonyítása vagy ismert, vagy tananyaga valamely alaptárgynak. Először belátjuk a 2-es fejezetben Baire-terekre példaként felsorolt topologikus terekről, hogy ők valóban Baire-terek.

6.1. tétel. *Sűrű nyílt halmazok metszete sűrű, ha X:*
a, teljes metrikus tér
b, a számegyenes nemelfajuló intervalluma
c, kompakt T_2 tér

Bizonyítás. a, Legyen $V_1, V_2, ...$ nemüres sűrű nyílt halmazok X-ben, megmutatjuk, hogy metszetük is sűrű. Ehhet legyen $V \subset X$ nemüres nyílt halmaz. Mivel V_1 sűrű, így belemetsz minden nemüres nyíltba, speciálisan V-be is. Legyen ez a pont x_1. Ekkor létezik egy $r_1 > 0$, hogy $\overline{B(x_1, r_1)} \subset V \cap V_1$. A V_2 halmaz sűrűségét kihasználva létezik $x_2 \in X$ és $r_2 > 0$, hogy:

$$B(x_2, r_2) \subset \overline{B(x_2, r_2)} \subset B(x_1, r_1) \quad \text{és} \quad \overline{B(x_2, r_2)} \subset V \cap V_1 \cap V_2$$

Hasonlóan minden n-re létezik $x_n \in X$, hogy:

$$B(x_n, r_n) \subset \overline{B(x_n, r_n)} \subset ... \subset B(x_2, r_2) \subset \overline{B(x_2, r_2)} \subset B(x_1, r_1)$$

$$\overline{B(x_n, r_n)} \subset V \cap V_1 \cap V_2 \cap .... \cap V_n$$

Nyílván választhatjuk úgy az r_n sugarakat, hogy $r_n \longrightarrow 0$, midőn $n \longrightarrow \infty$. Ekkor Cantor tétele szerint (teljes metrikus terekben): $\bigcap\limits_n \overline{B(x_n, r_n)} \neq \emptyset$ és így $V \cap \bigcap\limits_n V_n \neq \emptyset$. Megmutattuk tehát, hogy $\bigcap\limits_n V_n$ tetszőleges nemüres nyíltba belemetsz, tehát sűrű.

A b, részhez vegyük észre, hogy Baire-tér sűrű altere ismét Baire-tér, de egy ilyen nemelfajuló intervallum sűrű a lezártjában, ami pedig egy teljes metrikus tér, így az előbb belátott a, rész szerint egyben Baire-tér is.

A c, résznél felhasználjuk, hogy minden kompakt T_2 tér egyben T_4 tér is. Ez utóbbi azt jelenti, ha adott egy V nyílt és $Z \subset V$, Z zárt halmaz, akkor

létezik U nyílt, hogy:

$$Z \subset U \subset \overline{U} \subset V$$

Legyen $V_1, V_2, ...$ sűrű nyílt halmazok, megmutatjuk, hogy metszetük sűrű. Ehhez adjunk meg egy V nemüres nyílt halmazt. $V \cap V_1$ nemüres, mivel V_1 sűrű volt, így $\exists x \in X$, $x \in V \cap V_1$, ekkor mivel a tér T_4, létezik U_1, hogy:

$$\{x\} \subset U_1 \subset \overline{U_1} \subset V \cap V_1$$

V_2 is sűrű, így belemetsz a nemüres U_1-be, a tér T_4-ségét kihasználva kapunk egy nemüres U_2 nyílt halmazt, amelyre:

$$U_2 \subset \overline{U_2} \subset U_1 \cap V_2 \subset V \cap V_1 \cap V_2$$

hasonlóan kapjuk minden n-re, hogy létezik nemüres U_n nyílt, hogy:

$$U_n \subset \overline{U_n} \subset U_{n-1} \cap V_n \subset V \cap V_1 \cap ... \cap V_n$$

Az $\overline{U_n}$ halmazok fogyó kompakt családhalmazt alkotnak, amelyek minden n-re nemüresek, így metszetük sem üres, de ekkor $V \cap \bigcap_n V_n$ sem üres.

□

A komplex függvénytani eszközök bizonyításával folytatjuk, amiket csak a Siegel lemma és a Hat exponenciális fejezetben bukkantak elő. Az itt található bizonyítások [6]-t követik. A későbbiekben $|f|_R$ egy f függvény abszolút értékének maximumát fogja jelenteni az origó körüli R sugarú körvonalon (mindig olyan függvényről lesz szó, ahol ez létezik is).

6.2. tétel. *(Maximum elv) Ha adott egy f nemkonstans holomorf függvény egy $D \subset \mathbb{C}$ tartományon, akkor $|f|$-nek nem létezik lokális maximuma a tartomány egyetlen egy pontjában sem*

Következmény: Ha f holomorf valamilyen $D \subset \mathbb{C}$ korlátos tartományon és folytonos a $\overline{D}$ halmazon, akkor $|f|$ a maximumát mindeképpen egy határpontjában is eléri (ha f nemkonstans, akkor pedig csak is ott érheti el).

6.3. tétel. *(Jensen egyenlőtlenség) Legyen f analatikus a $\{|z| \leq R\}$ egy környezetében és $f(0) \neq 0$, emellett soroljuk fel a nyílt körlemezbe eső gyökeit az f-nek (annyiszor, amennyi a multiplicitásuk): $z_1, ..., z_N$. Ekkor:*

$$\big|f(0)\big| \leq |f|_R \frac{|z_1 ... z_N|}{R^N}$$

Bizonyítás. Könnyen látható, ha $|z_n| \neq R$, akkor tetszőleges $|z| = R$ esetén $\frac{R^2 - z\overline{z_n}}{R(z-z_n)}$ abszolút értéke 1 (írjuk fel z-t $Re^{i\rho}$ alakban és szorozzuk meg a számot $e^{i\rho}$-val, ami nem változtat az abszolút értékén a kifejezésnek). Ekkor deifináljuk a következő holomorf függvényt:

$$g(z) = f(z) \prod_{i=1}^{N} \frac{R^2 - z\overline{z_n}}{R(z - z_n)}$$

ez úgy szintén analatikus a $\{|z| \leq R\}$ egy környezetében és a maximum elv miatt:

$$\left| f(0) \frac{R^N}{z_1 ... z_n} \right| = \big|g(0)\big| \leq |f|_R$$

amiből átszorzás után adódik a tétel állítása. □

Bevezetjük a $\nu(r)$ jelölést, ami mindig az adott témában egy konkrét f-re vonatkozik, és azt mondja meg, hogy f-nek hány gyöke esik a nyílt r sugarú origó közepű körlapba.

6.4. tétel. *Legyen f olyan függvény, mint az előző tételben, ekkor az előbbi jelöléssel:*

$$\int_0^R \frac{\nu(x)}{x} dx \leq \log|f|_R - \log\big|f(0)\big|$$

Bizonyítás. Élünk a $0 = r_0 < r_1 < .. < r_k < r_{k+1} = R$ jelöléssel, ahol $r_1, ..., r_k$ azok az origó középpontú körvonalaknak a sugarai, ahová f-nek a gyökei esnek és a $\nu(r_0) = 0$ jelölést is bevezetjük. Alakítsuk át az integrált:

$$\int_0^R \frac{\nu(x)}{x} dx = \sum_{j=1}^{k} \nu(r_{j+1}) \int_{r_j}^{r_{j+1}} \frac{1}{x} dx = \sum_{j=1}^{k} \Big(\sum_{t=1}^{j+1} (\nu(r_t) - \nu(r_{t-1})) \int_{r_j}^{r_{j+1}} \frac{1}{x} dx =$$

$$= \sum_{t=1}^{k} (\nu(r_{t+1}) - \nu(r_t))(\sum_{j=t}^{k} \int_{r_j}^{r_{j+1}} \frac{1}{x} dx) = \sum_{t=1}^{k} (\nu(r_{t+1}) - \nu(r_t)) \int_{r_t}^{R} \frac{1}{x} dx =$$

$$= \sum_{n=1}^{N} \int_{|z_n|}^{R} \frac{1}{x} dx = \sum_{n=1}^{N} \log \frac{R}{|z_n|} = \log \frac{R^N}{|z_1 ... z_n|}$$

amit az előbb belátott tétellel együtt összevetve teljessé teszi ennek a tételnek a bizonyítását. □

6.5. definíció. *Legyen adva egy f egészfüggvény. Ha létezik egy $\rho > 0$ és $C > 0$, hogy $\big|f(z)\big| \leq C^{R^\rho}$, ha $|z| \leq R$, akkor az ilyen ρ-k infimumát az f rendjének mondjuk.*

6.6. tétel. *Ha f egy legfeljebb ρ rendű egészfüggvény, akkor a $R \geq 1$ sugarú nyílt körbe legfeljebb AR^ρ gyöke esik f-nek, ahol A csupán egy f-től függő konstans.*

Bizonyítás. Ha f-nek n-szeres gyöke van a 0-ban, akkor tekintsük a $g(z) = \frac{f(z)}{z^n}$ függvényt és írjuk fel az előbbi tételt a 2R sugarú körrel:

$$\nu_g(R) \log 2 \leq \int_{R}^{2R} \frac{\nu_g(R)}{x} dx \leq \int_{0}^{2R} \frac{\nu_g(x)}{x} dx \leq \log|g|_{2R} - \log\big|g(0)\big|$$

felhasználva azt, hogy $\log|g|_{2R} = \log|f|_{2R} - n \log 2R$ és az f rendje legfeljebb ρ, az állítás néhány egyszerűbb becslés és átrendezés után adódik.

□

Most pedig néhány állítás bizonyítása következik algebrai számelméletből, amiket az előző fejezetekben használtunk. A bizonyításokat [7]-ből vettem. Emlékeztetünk a 4.8-as deifinícióra:

6.7. definíció. *Legyen $\mathbb{K}$ n-edfokú algebrai számtest, valamint legyen $\vartheta \in \mathbb{K}$ olyan, hogy $\mathbb{K} = \mathbb{Q}(\vartheta)$. Legyen $\alpha \in \mathbb{K}$ tetszőleges, ő előáll $\alpha = c_0 + c_1\vartheta + ... + c_{n-1}\vartheta^{n-1}$ alakban, ahol persze $c_0, ..c_n \in \mathbb{Q}$. Ekkor az "$\alpha$ szám konjugáltjai $\underline{\underline{\mathbb{K}}}$-ban" alatt a következő számokat értjük:*

$$c_0 + c_1\vartheta_i + ... + c_{n-1}(\vartheta_i)^{n-1}, \quad i = 1, 2, ..., n$$

ahol ϑ_i jelöli a ϑ i-edik (régi értelemben vett) konjugáltját.

6.8. tétel. *Legyen $\mathbb{K} = \mathbb{Q}(\vartheta)$ n-edfokú algebrai számtest, valamint $\alpha \in \mathbb{K}$ tetszőleges, m-edfokú algebrai szám. Ekkor α konjugáltjai $\mathbb{K}$-ban nem más, mint $\frac{n}{m}$ alkalommal felsorolva mindegyik konjugáltja α-nak.*

Bizonyítás. Legyen $r(x) \in \mathbb{Q}[x]$ az a legfeljebb (n-1)-edfokú polinom, amelyre $r(\vartheta) = \alpha$ (azaz a fenti definícióban szereplő betűket használva $r(x) = \sum_{i=0}^{n-1} c_i x^i$). Ha már most az α i-edik konjugáltját $\mathbb{K}$-ban α_i-vel jelöljük, akkor $\alpha_i = r(\vartheta_i)$ definíció szerint. Legyen

$$f(x) = \prod_1^n (x - r(\vartheta_i))$$

vegyük észre, hogy $f(x) \in \mathbb{Q}[x]$, mivel a kifejezés maga szimmetrikus $\vartheta_1., .., \vartheta_n$-ben. Na mármost $f(\alpha) = 0$ is teljesül. Ha elnevezzük g-vel az α minimálpolinomját, akkor $g(x) \mid f(x)$, és emiatt

$$f(x) = [g(x)]^s h(x)$$

alakú, ahol $h(x) \in \mathbb{Q}[x]$ és $g(x)$ és $h(x)$ relatív prímek. Ez abból fakad, hogy ahánszoros gyöke az α f-nek, legyen ez s, annyiszor kiemelhető belőle a $g(x)$ faktor, a maradék polinom pedig szükségképpen relatív prím g-hez, mivel egy minimálpolinom irreducibilis. Megmutatjuk, hogy $h(x) \equiv 1$, ami bizonyítja az állításunkat (ugyanis g foka m, így s = $\frac{n}{m}$).

Ha már most $h(x)$ nem konstans, mindenesetre biztos, hogy normált és valamilyen i-re h-nak gyöke egy $r(\vartheta_i)$ de ekkor a $h(r(x))$ polinomnak gyöke ϑ_i, ami azt jelenti hogy $h(r(x))$-et osztja ϑ_i minimálpolinomja, ami éppen maga g, ellentmondva g és h relatív prímségének. Tehát h mégis csak konstans, és akkor a konstans 1. □

Következmény: Az α konjugáltjai $\mathbb{K} = \mathbb{Q}(\vartheta)$-ban nem függnek a ϑ primitív elem választásától.

Ez utóbbi tétel bizonyítja azt is, hogy α magassága tetszőleges $\mathbb{K}$ algebrai számtestben az ő konjugáltjainak (régi értelemben véve, bár újban definíció

szerint igaz) abszolút értékeinek maximuma.

Legyen most adva egy $\mathbb{K}$ n-edfokú algebrai számtest és annak egy bázisa: $\alpha_1, ..., \alpha_n$. Ha most $\alpha_j^{(i)}$ jelöli az α_j konjugáltjait $\mathbb{K}$-ban $i = 1, ..., n$ esetén, akkor deiniáljuk az $\alpha_1, ..., \alpha_n$ halmaz diszkriminánsát:

$$\Delta[\alpha_1, ..., \alpha_n] =\mid \alpha_j^{(i)} \mid^2$$

ahol $\mid \alpha_j^{(i)} \mid$ jelöli a

$$\begin{bmatrix} \alpha_1^{(1)} & \alpha_2^{(1)} & .... & \alpha_n^{(1)} \\ . & . & . & . \\ . & . & . & . \\ \alpha_1^{(n)} & \alpha_2^{(n)} & .... & \alpha_n^{(n)} \end{bmatrix}$$

mátrix determinánsát.

Vegyük észre, hogy a diszkrimináns jóldeiniált, azaz érzéketlen az $\alpha_1, ..., \alpha_n$ számok permutációjára, sőt a konjugáltak sorrendjétől sem függ. Ha megadunk egy másik bázist, mondjuk $\beta_1, ..., \beta_n$-et, akkor léteznek olyan c_{jk} racionális számok, hogy:

$$(*) \quad \beta_k = \sum_{j=1}^{n} c_{jk}\alpha_j \quad k = 1, .., n$$

tudjuk lineáris algebrából persze, hogy ekkor a (c_{ij}) mátrix determinánsa nemnulla, valamint (*)-ot használva a konjugáltakra kapjuk még hogy:

$$\beta_k^{(i)} = \sum_{j=1}^{n} c_{jk}\alpha_j^{(i)} \quad i = 1, ..., n$$

ekkor a determinánsok szorzás tétele alapján kapjuk, hogy:

$$(**) \quad \Delta[\beta_1, ..., \beta_n] =\mid c_{jk} \mid^2 \Delta[\alpha_1, ..., \alpha_n].$$

Most hogy ha felhasználjuk, hogy $\mathbb{K} = \mathbb{Q}(\vartheta)$ valamely ϑ mellett, és azt a

könnyen látható azonosságot, hogy: $(\vartheta^i)^{(j)} = (\vartheta^{(j)})^i$, akkor:

$$D(\vartheta) := \Delta[1, \vartheta, ..., \vartheta^{n-1}]$$

megegyezik a következő mátrix determinánsának négyzetével:

$$\begin{bmatrix} 1 & \vartheta^{(1)} & ..... & (\vartheta^{(1)})^{n-1} \\ \vdots & & & \\ 1 & \vartheta^{(n)} & ..... & (\vartheta^{(n)})^{n-1} \end{bmatrix}$$

ami egy Vandermonde determináns, így mindent összevetve:

$$D(\vartheta) = \prod_{1 \le i < j \le n} (\vartheta^{(i)} - \vartheta^{(j)})^2.$$

Ez utóbbi biztosan nemnnulla, mivel ϑ konjugáltjai mind különbözőek, és mi több, szimmetrikus is a kifejezés ϑ konjugáltjaiban, így egy nemnulla racionális szám! (**)-ra visszatekintve azt láthatjuk, hogy $\mathbb{K}$ tetszőleges bázisának diszkriminánsa egy nemnulla racionális szám. Ha ϑ és konjugáltjai mind valós pozitívak, akkor ez a szám is pozitív. Sőt, hogy ha ϑ-t algebrai egésznek választom (amit mindig el tudok érni), akkor $D(\vartheta)$ egy nemnulla egész szám (mivel egyszerre racionális és algebrai egész).

6.9. definíció. *Ha adott $\mathbb{K}$ algebrai számtest, akkor egy $\alpha_1, ..., \alpha_s \in \mathcal{O}_\mathbb{K}$ rendszert egész bázisnak nevezünk, ha $\forall \beta \in \mathcal{O}_\mathbb{K}$ előáll egyértelműen $c_1, ..., c_s$ egész számokkal*

$$\beta = \sum_{i=1}^{s} c_i \alpha_i$$

alakban.

Vegyük észre, hogy ha van egész bázis, az szükségképpen egy bázisa $\mathbb{K}$-nak (mivel $\forall \beta \in \mathbb{K} \quad \exists m \in \mathbb{Z}, m\beta \in \mathcal{O}_\mathbb{K}$, így $m\beta$ kifejezhető $\alpha_1, ..., \alpha_s$ egész együtthatós lineáris kombinációjaként, majd osztunk m-el, hasonlóan látható be, hogy lineárisan függetlnek is). Így ez az s szám szükségképpen egyenlő $[\mathbb{K} : \mathbb{Q}]$-val.

6.10. tétel. *Minden algebrai számtest rendelkezik egész bázissal.*

Bizonyítás. Tekintsük a $\mathbb{K}$ összes algebrai egészekből alkotott bázisait (nem egész bázist!, azt most bizonyítjuk, hogy lesz), és jegyzeteljük le az összes ezen bázisokhoz tartozó diszkriminánsok abszolút értékeit. Ahogy azt már fentebb beláttuk, ezek mind nemnulla egész számok, abszolút érték vétel miatt pozitív egész számok. Vegyünk egy algebrai egészekből álló bázist, $\omega_1, ..., \omega_n$-et, amire ez az abszolút érték a minimális. megmutatjuk, hogy $\omega_1, ..., \omega_n$ egy egész bázist alkot. Tegyük fel, hogy nem igaz, ez azt jelenti, hogy $\exists \omega \in \mathcal{O}_{\mathbb{K}}$, hogy nem fejezhető ki az $\omega_1, ..., \omega_n$-ek egész együtthatós lineáris kombinációjaként, mindenesetre utóbbiak egy bázist alkotnak, így az igaz, hogy.

$$\omega = a_1\omega_1 + ... + a_n\omega_n$$

valamely $a_1, ..., a_n$ racionális számok mellett, amelyek nem mindegyike egész. Tegyük fel, hogy a_1 nem egész, ekkor írjuk a_1-et a következő alakban: $a_1 = a + r$, ahol a egész és $0 < r < 1$. Tekintsük ekkor a következő algebrai egészekből álló bázist:

$$\omega_1^{(*)} = \omega - a\omega_1 = (a_1 - a)\omega_1 + a_2\omega_2 + ... + a_n\omega_n$$
$$\omega_i^{(*)} = \omega_i, \quad i = 2, ..., n$$

Ekkor a következő mátrix

$$\begin{bmatrix} a_1 - a & a_2 & a_3..... \\ 0 & 1 & 0..... \\ 0 & 0 & 1..... \\ 0 & .... & .....1 \end{bmatrix}$$

determinánsa $a_1 - a = r$. Ekkor felhasználva (**)-ot látjuk, hogy:

$$\Delta[\omega_1^{(*)}, ..., \omega_n^{(*)}] = r^2\Delta[\omega_1, ..., \omega_n]$$

ahol abszolút értéke véve ellentmondásra jutunk, hiszen $\left|\Delta[\omega_1^{(*)}, ..., \omega_n^{(*)}]\right| < \left|\Delta[\omega_1, ..., \omega_n]\right|$, holott $\left|\Delta[\omega_1, ..., \omega_n]\right|$ értéke minimális volt az algebrai egész

bázisok között. □

6.11. tétel. *Bármely kettő egész bázisnak ugyanaz a diszkriminánsa.*

Bizonyítás. Az előző bizonyítás annyit ad, hogy bármely kettő egész bázisnak ugyanakkora abszolút értékű a diszkriminánsa, ez e tétel annyival több, hogy az előjelek stimmelését is garantálja.

Ehhez legyen adva $\alpha_1, ..., \alpha_n$ és $\beta_1, ..., \beta_n$ egy-egy egész bázis, ekkor c_{ij} egész számokkal kapjuk:

$$\alpha_j = \sum_{i=1}^{n} c_{ij}\beta_j, \quad j = 1, .., n$$

ekkor megint (**)-ot használva:

$$\Delta[\alpha_1, ..., \alpha_n] = \mid c_{ij} \mid^2 \Delta[\beta_1, ..., \beta_n]$$

ami valóban garantálja az előjelek stimmelését is.

Gyakran ez utóbbi számra úgy hivatkoznak, mint a $\mathbb{K}$ algebrai számtest diszkriminánsa. □

Ezzel befejeztük a függeléket, alább a felhasznált irodalmak listája található.

Hivatkozások

[1] K. Sentgil Kumar, R. Thangadurai és M. Waldschmidt: *Liouville numbers and Schanuel's conjecture* https://webusers.imj-prg.fr/~michel.waldschmidt/articles/pdf/LiouvilleSchanuelArchiv.pdf

[2] http://www.math.leidenuniv.nl/~evertse/dio15-4.pdf

[3] Kátay Tamás: *Szakdolgozat* https://web.cs.elte.hu/blobs/diplomamunkak/bsc_mat/2018/katay_tamas.pdf

[4] Lenny Fukshansky: *Transcendental Number Theory* Lecture Notes http://www1.cmc.edu/pages/faculty/lenny/classes/spring_2015/m195/m195_lectures.pdf

[5] Putnam feladat,1971 https://mks.mff.cuni.cz/kalva/putnam/psoln/psol716.html

[6] Murty, M. Ram, Rath, Purusottam: *Transcendental Numbers*, SPRINGER 2014 https://www.springer.com/gp/book/9781493908318

[7] Harry Pollard, Harold G. Diamond: *The theory of algebraic numbers*, DOVER BOOKS, Reprint of the Mathematical Association of America, second, 1975 edition https://store.doverpublications.com/0486404544.html

[8] Laczkovich Miklós *Sejtés és bizonyítás* Typotex kiadó, 2010 https://www.typotex.hu/book/165/laczkovich_miklos_sejtes_es_bizonyitas

[9] Laczkovich Miklós Átdarabolások (kézirat, Laczkovich Miklós előadását legépelte Tóth Dávid)