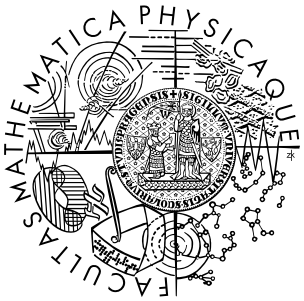
Univerzita Karlova v Praze
Matematicko-fyzikální fakulta

BAKALÁŘSKÁ PRÁCE



Michal Kesely

Slavné neřešitelné problémy

Katedra matematické analýzy

Vedoucí bakalářské práce: RNDr. Dalibor Pražák, Ph.D.
Studijní program: Obecná matematika

2008

Týmto by som chcel poďakovať vedúcemu práce RNDr. Daliborovi Pražákovi, Ph.D. za obetavé a poučné vedenie tejto práce a za jeho čas. Taktiež by som chcel poďakovať Jimovi Loyovi za poskytnutie niektorých zaujímavých materiálov ku kapitole 3.

Prehlasujem, že som svoju bakalársku prácu napísal samostatne a výhradne s použitím citovaných prameňov. Súhlasím so zapožičiavaním práce a jej zverejňovaním.

V Prahe dňa 6.8.2008 Michal Kesely

Obsah

Názov práce: Slavné neřešitelné problémy
Autor: Michal Kesely
Katedra (ústav): Katedra matematické analýzy
Vedúci bakalárskej práce: RNDr. Dalibor Pražák, Ph.D.
e-mail vedúceho: prazak@karlin.mff.cuni.cz

Abstrakt: V predloženej práci študujeme tri slávne antické problémy (délsky problém, trisekciu uhla a kvadratúru kruhu), ktoré sa oveľa neskôr ukázali byť neriešiteľnými. V prvej kapitole sformalizujeme pojem euklidovskej konštrukcie, dokážeme pár viet o algebraických číslach a ukážeme zaujímavú súvislosť medzi euklidovsky konštruovateľnými číslami a algebraickými číslami. V nasledujúcich dvoch kapitolách potom priamo z vlastností konštruovateľných čísel dokážeme neriešiteľnosť prvých dvoch problémov, v tretej kapitole naviac uvedieme aj niekoľko nesprávnych riešení trisekcie uhla. V poslednej kapitole najprv dokážeme existenciu transcendentných čísel, vybudujeme si potrebný aparát a nakoniec dokážeme transcendenciu dvoch známych konštánt - e a π. Neriešiteľnosť kvadratúry kruhu je priamym dôsledkom transcendencie π.

Kľúčové slová: neriešiteľný problém, konštruovateľný, transcendentný

Title: Famous unsolvable problems
Author: Michal Kesely
Department: Department of Mathematical Analysis
Supervisor: RNDr. Dalibor Pražák, Ph.D.
Supervisor's e-mail address: prazak@karlin.mff.cuni.cz

Abstract: In the present work we study three famous problems of antiquity (the Delian problem, the trisection of an angle and the squaring of a circle), which turned to be unsolvable much later. In the first chapter we will formalize the concept of Euclidean construction, prove few theorems about algebraic numbers and show an interesting connection between constructible numbers and algebraic numbers. In the next two chapters we will prove the insolvability of the Delian problem and the trisection of an angle using the properties of constructible numbers. Furthermore in the third chapter we will mention some incorrect solutions of the trisection problem. In the last chapter we will prove the existence of transcendental numbers, build an appropriate apparatus and finally we will prove the transcendence of two famous constants - e and π. The insolvability of the squaring problem is a direct consequence of the transcendence of π.

Keywords: unsolvable problem, constructible, transcendental

Úvod

Starovekí Gréci boli oddaní geometrii a považovali ju za matku všetkých vied. Všetky svoje matematické znalosti vyjadrovali pomocou geometrických útvarov a konštrukcií - napríklad súčin dvoch čísel vyjadrovali ako obsah obdĺžnika o príslušných stranách. Boli si vedomí aj toho, že existujú aj iné čísla ako racionálne, hoci tento fakt prijímali len veľmi ťažko, pretože to bola rana do ich matematických ideálov.

Gréci boli v geometrických konštrukciách neprekonateľní, avšak ani oni nezvládli splniť všetky úlohy. Medzi tri najznámejšie patrili délsky problém (problém duplicity kocky), problém trisekcie uhla a problém kvadratúry kruhu. Ich podstatou je zostrojenie kocky s objemom 2, rozdelenie daného uhla na tretiny a konštrukcia štvorca s rovnakým obsahom ako má kruh o polomere 1. Už v týchto dobách boli síce predložené riešenia týchto problémov (a treba podotknúť, že správne), lenže žiadne z nich neboli „čisté". Za čisté totiž Gréci považovali iba to, čo dnes nazývame euklidovskou konštrukciou. Pri nej sú jedinými povolenými nástrojmi nekonečne dlhé jednohranné pravítko bez rysky a kružidlo. Prvé riešenia používali napríklad krivky (spomeňme kvadratrix), ktoré euklidovsky skonštruovať nešli. A pomocou euklidovskej konštrukcie zostali tieto problémy nevyriešené ešte dlhé roky.

A tak podozrenie, že tieto problémy nemajú riešenie, nadobúdalo na sile. Avšak prvé dva problémy odolávali, až kým Descartes nezaviedol základy analytickej geometrie. Zrazu namiesto kreslenia čiar stačilo počítať rovnice. A pomocou nich sa (pomerne jednoducho) ukázalo, že délsky problém ani problém trisekcie uhla nie sú euklidovsky riešiteľné. Kvadratúra kruhu však odolávala aj naďalej.

Matematici sa zhodli, že podstata tohto problému spočíva ešte kdesi hlbšie. Začalo sa trochu rozjasňovať, keď sa ukázalo, že existuje akýsi zvláštny druh čísel - transcendentné čísla. Nebolo ťažké dokázať, že žiadne transcendentné číslo nejde euklidovsky skonštruovať. Liouville skonštruoval niektoré čísla, o ktorých aj dokázal, že sú transcendentné. Cantor dokonca dokázal, že ich je nespočítateľne veľa. Otvárala sa cesta, ako sa zbaviť posledného problému. Stačilo ukázať, že π je transcendentné číslo. V roku 1873 sa Hermiteovi podarilo dokázať transcendenciu e a o deväť rokov neskôr Lindemann upravením Hermiteovho dôkazu dospel k záveru, že π je transcendentné.

Tým sa zavŕšila jedna kapitola antickej matematiky - o niekoľko tisíc rokov neskôr. V tejto práci si ukážeme, ako možno neriešiteľnosť týchto troch problémov dokázať.

Kapitola 1

Konštruovateľné čísla

Táto kapitola je akousi prípravou pred samotným dôkazom neriešiteľnosti troch antických problémov. Neriešiteľnosť dvoch z troch problémov bude priamym dôsledkom vlastností konštruovateľných čísel. Pre problém kvadratúry kruhu však budeme potrebovať ešte akúsi nadstavbu o algebraických číslach.

1.1 Aké čísla vlastne možno zostrojiť?

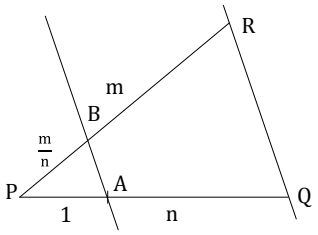
Definícia 1.1.1. Pravítkom bez rysky rozumieme nekonečne dlhé pravítko, na ktorom sa nenachádzajú žiadne značky a má iba jednu hranu. Takéto pravítko možno použiť na spojenie dvoch známych bodov alebo na predĺženie existujúcej úsečky. Kružidlom rozumieme kružidlo nastaviteľné na ľubovoľne veľký, ale už známy, polomer, ktoré na sebe nemá žiadne značky. Kružidlo sa ihneď po konštrukcii sklapne.

Definícia 1.1.2. Číslo a sa nazýva euklidovsky skonštruovateľné, pokiaľ je možné z jednotkovej úsečky pomocou kružidla a pravítka bez rysky v konečnom počte krokov zostrojiť úsečku dĺžky a.

Pri euklidovskej geometrickej konštrukcii máme k dispozícii len kružidlo a pravítko bez rysky. Ak začíname len s úsečkou jednotkovej dĺžky, jednoduchým spôsobom skonštruujeme všetky prvky okruhu celých čísel. Odtiaľ už vieme známym spôsobom skonštruovať všetky úsečky, ktorých dĺžka je racionálne číslo. Z úsečiek racionálnych dĺžok potom budeme môcť konštruovať ďalšie úsečky iných zaujímavých dĺžok.

Lema 1.1.3. *Všetky úsečky racionálnych dĺžok sú euklidovsky skonštruovateľné.*

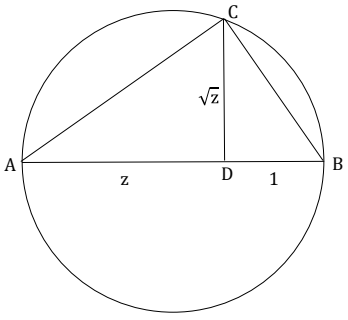
Dôkaz. Nech $\frac{m}{n}$ je racionálne číslo, kde m, $n \in \mathbb{N}$. Vezmeme úsečky zodpovedajúce prirodzeným číslam m a n tak, že ich konce umiestnime do toho istého bodu P. Cez opačné konce úsečiek (Q a R) vedieme priamku. Na úsečku PQ dĺžky n ešte nanesieme jednotkovú úsečku, a tak vznikne bod A. Nakoniec vedieme rovnobežku k priamke QR cez bod A. Priesečník úsečky PR a tejto priamky označme B.



Z podobnosti trojuholníkov vyplýva, že úsečka PB má dĺžku $\frac{m}{n}$. □

Lema 1.1.4. *Pokiaľ je euklidovsky skonštruovateľné číslo $z > 0$, tak je euklidovsky skonštruovateľné aj číslo $\sqrt{z}$.*

Dôkaz. Zostrojíme úsečku AB dĺžky *z+1*, pozostávajúcu z dvoch častí, AD a DB - jedna má dĺžku z a druhá má dĺžku 1. Nad takouto úsečkou zostrojíme Tálesovu kružnicu. Z bodu D vztýčime kolmicu na úsečku AB a jej priesečník s kružnicou označíme C.



Zrejme trojuholník ACB je pravouhlý, podobne aj trojuholníky ADC a BDC. Tieto trojuholníky sú si navzájom podobné a preto platí $\frac{|AD|}{|CD|} = \frac{|CD|}{|DB|}$. Po dosadení teda $\frac{z}{|CD|} = \frac{|CD|}{1}$, z čoho $|CD|^2 = z$ a $|CD| = \sqrt{z}$, čo sme chceli ukázať. □

Ostatné euklidovsky skonštruovateľné čísla potom dostaneme postupnými iteráciami Pytagorovej vety. V prvom kroku zoberieme všetky racionálne čísla a vytvoríme všetky čísla, ktoré sa použitím Pytagorovej vety dajú vytvoriť (nazvime ich napríklad konštruovateľné čísla *prvého rádu*). V n-tom kroku vytvárame ďalšie čísla z konštruovateľných čísel *(n-1)*-vého rádu. Postupné použitie Pytagorovej vety a postupný vznik nových konštruovateľných čísel osvetľuje nasledujúca definícia. Pre podrobný dôkaz ekvivalencie oboch definícií konštruovateľných čísel viď [4], str. 129-133.

Definícia 1.1.5. Zvoľme $K_0 = \mathbb{Q}$ a ďalej pre $n \in \mathbb{N}$ induktívne definujme n-té rozšírenie. Najprv zvolíme prvok w spĺňajúci $w \in K_{n-1}$ a $\sqrt{w} \notin K_{n-1}$. Potom $K_n = \{p + q\sqrt{w} \mid p,\ q \in K_{n-1}\}$. Množinou konštruovateľných čísel nazývame množinu

$$\mathcal{K} = \bigcup_{i=0}^{\infty} K_i$$

Dôkaz korektnosti definície. Potrebujeme ukázať, že príslušné $\sqrt{w}$ možno vždy vybrať tak, aby nepatrilo do K_{n-1}, a tým pádom že žiadne dve rozšírenia nie sú totožné. Bez ujmy na všeobecnosti môžeme predpokladať, že v príslušných prípadoch je $w > 0$, aby $\sqrt{w}$ bola reálne definovaná.
Zrejme $K_0 \subsetneq K_1$ a tiež $K_i \subseteq K_{i+1}$ pre $i \in \mathbb{N}$, potrebujeme však ukázať ostrú inklúziu. Nech teda K_m je najmenšia množina taká, že nejde vybrať $\sqrt{w} \notin K_m$ pre $w \in K_m$. To ale znamená, že pre každé $a \in K_m$ je $\sqrt{a} \in K_m$ a tiež $\sqrt{\sqrt{a}} \in K_m$. Špeciálne dostávame $\sqrt{\sqrt{v}} = p + q\sqrt{v}$ pre nejaké prvky $p,\ q,\ v \in K_{m-1} \subseteq K_m$; $\sqrt{v} \notin K_{m-1}$; $\sqrt{v} \in K_m$. Rovnosť umocníme a máme $\sqrt{v} = p^2 + 2pq\sqrt{v} + q^2v$. Vyjadríme $\sqrt{v} = \frac{p^2+q^2v}{1-2pq} \in K_{m-1}$, čo by bol spor. Preto ostáva možnosť, že menovateľ je nulový, čiže $1 = 2pq$ (špeciálne si všimnime $p \neq 0 \neq q$). Po dosadení do pôvodnej rovnice máme $p^2 + q^2v = 0$. Členy na ľavej strane sú ale nezáporné a ich súčet je 0. Preto oba členy p^2 aj q^2v sú 0. Zároveň ale $p \neq 0$, čo je spor. Definícia má zmysel.

Poznámka 1.1.6. V predchádzajúcej definícii má podmienka $\sqrt{w} \notin K_n$ za dôsledok $K_n \subsetneq K_{n+1}$, teda reťazec týchto množín je ostro rastúci. Preto neexistuje $m \in \mathbb{N}$ také, že $\mathcal{K} = K_m$.

Veta 1.1.7. *Množina konštruovateľných čísel $\mathcal{K}$ je teleso.*

Dôkaz. Potrebujeme ukázať uzavretosť vzhľadom na sčítanie, opačný prvok, násobenie a inverzný prvok. 0 a 1 patria do $\mathcal{K}$ triviálne.
Uzavretosť vzhľadom na súčet a opačný prvok. Nech $i \leq j$ sú minimálne prirodzené indexy také, že $a = p + q\sqrt{w} \in K_i$ a $b = r + s\sqrt{v} \in K_j$. Potom prvok $a+b = p+r+q\sqrt{w}+s\sqrt{v}$ patrí do množiny K_j, a teda aj do množiny $\mathcal{K}$. Časť o opačnom prvku vyplýva okamžite.
Uzavretosť vzhľadom na násobenie. Bez ujmy na všeobecnosti budeme uvažovať prípad, keď oba prvky patria do tej istej množiny K_n. Toto môžeme spraviť vďaka tomu, že tieto množiny tvoria ostro rastúcu postupnosť (inými slovami, ak $a \in K_i$, tak tiež $a \in K_j$ pre každé $j \geq i$). Dokážeme matematickou indukciou. Množina $K_0 = \mathbb{Q}$ je uzavretá na násobenie. Ďalej nech prvky a a b patria do tej istej množiny K_i. Teda $a = p+q\sqrt{w}$ a $b = r+s\sqrt{w}$ pre nejaké $p, q, r, s, w \in K_{i-1}$. Potom $ab = (p+q\sqrt{w})(r+s\sqrt{w}) = pr+(ps+rq)\sqrt{w}+sqw$. Lenže z indukčného predpokladu prvky $pr, ps, rq, sqw \in K_{i-1}$, a teda ab nutne patrí do K_i. Potom aj $\mathcal{K}$ je uzavretá na násobenie.
Uzavretosť vzhľadom na inverzné prvky. Nech prvok $0 \neq a = p + q\sqrt{w} \in K_i$. Potom prvok $\frac{1}{a} = \frac{1}{p+q\sqrt{w}} = \frac{p-q\sqrt{w}}{p^2-q^2w}$ nutne patrí do K_i (zrejme $p^2 - q^2w \neq 0$), pretože menovateľ zlomku $\frac{p-q\sqrt{w}}{p^2-q^2w}$ patrí do K_{i-1}, a teda môžeme opäť uplatniť indukciu. □

Poznámka 1.1.8. Podľa lemy 1.1.4 je $\mathcal{K}$ dokonca uzavretá na tvorbu druhých odmocnín.

1.2 Algebraické čísla

Definícia 1.2.1. Číslo α sa nazýva *algebraické* (nad $\mathbb{Q}$), pokiaľ existuje polynóm $f = \sum_{i=0}^{k} a_i x^i, a_0, ..., a_k \in \mathbb{Q}, a_k \neq 0$ taký, že α je koreňom polynómu f. Množina všetkých čísel algebraických nad $\mathbb{Q}$ sa označuje $\bar{\mathbb{Q}}$. Číslo, ktoré nie je algebraické (nad $\mathbb{Q}$), sa nazýva *transcendentné*.

Poznámka 1.2.2. Je úplne jedno, či pri overovaní algebraickosti čísla berieme polynómy nad $\mathbb{Q}$ alebo polynómy nad $\mathbb{Z}$. Vždy totiž možno polynóm vynásobiť najmenším spoločným násobkom menovateľov jednotlivých koeficientov, čím vytvoríme polynóm nad $\mathbb{Z}$ s rovnakými koreňmi.

Poznámka 1.2.3. Koreňmi polynomiálnych rovníc môžu byť tak reálne ako aj komplexné čísla. Preto budeme používať termín *algebraické číslo* podľa potreby v oboch kontextoch.

Uvážme teraz fixované reálne číslo r a okruh polynómov $\mathbb{Q}[x]$. Potom nasledujúce zobrazenie

$$\begin{aligned} \phi_r : \mathbb{Q}[x] &\longrightarrow \mathbb{R} \\ f(x) &\longmapsto f(r) \end{aligned}$$

sa nazýva *dosadzovací homomorfizmus*. To, že skutočne ide o homomorfizmus, vyplýva z faktu, že $(f+g)(r) = f(r) + g(r)$.

Pozrime sa teraz bližšie na jadro tohoto homomorfizmu. Pokiaľ je číslo r transcendetné, tak do jadra tohto homomorfizmu nespadnú žiadne netriviálne polynómy (pretože žiadny polynóm sa neanuluje v r). V tom prípade je ϕ_r prosté zobrazenie, keďže má nulové jadro.

Na druhej strane, pokiaľ je r algebraické, tak určite existujú polynómy, ktoré sa v r anulujú, a tým pádom sa nachádzajú v jadre ϕ_r. Potom už ϕ_r nemôže byť prosté zobrazenie. Zaujímavý je najmä faktorokruh $\mathbb{Q}[x]/\operatorname{Ker}\phi_r$. Podľa prvej vety o izomorfizme okruhov máme:

$$\mathbb{Q}[x]/\operatorname{Ker}\phi_r \simeq \operatorname{Im}\phi_r$$

Keďže $\mathbb{Q}[x]$ je obor integrity hlavných ideálov a $\operatorname{Ker}\phi_r$ je ideálom tohto oboru, tak $\operatorname{Ker}\phi_r$ musí mať nejaký ireducibilný generátor. Nech je to polynóm g. Zrejme vieme zabezpečiť, aby bol tento polynóm monický.

Definícia 1.2.4. Polynóm g z predchádzajúceho odstavca sa nazýva *minimálny polynóm* prvku r, značíme ho m_r. Pokiaľ minimálny polynóm prvku r má stupeň n, tak o prvku r hovoríme, že je *algebraický stupňa n*.

Príklad 1.2.5. Každé racionálne číslo q je algebraickým číslom stupňa 1, keďže je koreňom polynómu $x - q$. Platí aj opačná implikácia, takže algebraické čísla stupňa 1 sú práve všetky racionálne čísla. Číslo $\sqrt{2}$ je algebraickým číslom stupňa 2, keďže je koreňom polynómu $x^2 - 2$, ale nie je koreňom žiadneho polynómu stupňa 1 (tj. nejde o racionálne číslo).

Veta 1.2.6. *Množina algebraických čísel tvorí teleso.*

Dôkaz. Opäť potrebujeme ukázať uzavretosť vzhľadom na sčítanie, opačný prvok, násobenie a inverzný prvok. 0 a 1 do $\bar{\mathbb{Q}}$ patria triviálne.
Uzavretosť vzhľadom na opačný prvok. Nech $\alpha \in \bar{\mathbb{Q}}$. Takže existuje polynóm f_1 taký, že $0 = f_1(\alpha) = \sum_{i=0}^{k} a_i \alpha^i, a_0, ..., a_k \in \mathbb{Q}, a_k \neq 0$. Potom polynóm

$\tilde{f}_1 = \sum_{i=0}^{k}(-1)^i a_i x^i$ musí mať koreň $-\alpha$, lebo $\tilde{f}_1(-\alpha) = \sum_{i=0}^{k}(-1)^i a_i(-\alpha)^i = \sum_{i=0}^{k} a_i \alpha^i = 0$.
Uzavretosť vzhľadom na súčet. Nech $\alpha \neq 0 \neq \beta$, $\alpha, \beta \in \bar{\mathbb{Q}}$. Nech ich minimálne polynómy sú postupne $m_\alpha = x^m + a_{m-1}x^{m-1} + \ldots + a_1 x + a_0$ a $m_\beta = x^n + b_{n-1}x^{n-1} + \ldots + b_1 x + b_0$, kde $a_i, b_j \in \mathbb{Q}$ (zrejme $a_0 \neq 0 \neq b_0$). Podľa všetkého $0 = m_\alpha(\alpha) = \alpha^m + a_{m-1}\alpha^{m-1} + \ldots + a_1\alpha + a_0$, podobne pre $m_\beta(\beta)$. Prerovnaním dostaneme

$$\begin{aligned} \alpha^m &= -a_{m-1}\alpha^{m-1} - \ldots - a_1\alpha - a_0 \\ \beta^n &= -b_{n-1}\beta^{n-1} - \ldots - b_1\beta - b_0 \end{aligned} \tag{1.1}$$

Zoberme si teraz všetky kombinácie $\{\alpha^p\beta^q\}$ také, že $p = 0, 1, \ldots, m-1$ a $q = 0, 1, \ldots, n-1$. Pre jednoduchosť ich označme $\{\lambda_j\}_{j=1}^{mn}$. Zrejme $\lambda_k \neq 0$. Pre ľubovoľné λ_k je $(\alpha+\beta)\lambda_k$ lineárnou kombináciou prvkov $\{\lambda_j\}$ nad $\mathbb{Q}$. Ak je totiž $\lambda_k = \alpha^p\beta^q$ také, že $p < m-1$ a zároveň $q < n-1$, tak ide o lineárnu kombináciu triviálne. Pokiaľ však $p = m-1$ alebo $q = n-1$, stačí nám použiť 1.1 a opäť dostávame lineárnu kombináciu $\{\lambda_j\}$.
Takže pre každé λ_k existujú racionálne konštanty $c_{k,1}, c_{k,2}, \ldots, c_{k,mn}$ také, že platí $(\alpha+\beta)\lambda_k = c_{k,1}\lambda_1 + c_{k,2}\lambda_2 + \ldots + c_{k,mn}\lambda_{mn}$. Odčítaním ľavej strany rovností dostávame sústavu

$$\begin{aligned} 0 &= (c_{1,1} - (\alpha+\beta))\,\lambda_1 + c_{1,2}\lambda_2 + \ldots + c_{1,mn}\lambda_{mn} \\ 0 &= c_{2,1}\lambda_1 + (c_{2,2} - (\alpha+\beta))\,\lambda_2 + \ldots + c_{2,mn}\lambda_{mn} \\ &\vdots \\ 0 &= c_{mn,1}\lambda_1 + c_{mn,2}\lambda_2 + \ldots + (c_{mn,mn} - (\alpha+\beta))\,\lambda_{mn} \end{aligned}$$

To ale znamená, že nasledujúca homogénna sústava rovníc

$$\begin{aligned} 0 &= (c_{1,1} - (\alpha+\beta))\,y_1 + c_{1,2}y_2 + \ldots + c_{1,mn}y_{mn} \\ 0 &= c_{2,1}y_1 + (c_{2,2} - (\alpha+\beta))\,y_2 + \ldots + c_{2,mn}y_{mn} \\ &\vdots \\ 0 &= c_{mn,1}y_1 + c_{mn,2}y_2 + \ldots + (c_{mn,mn} - (\alpha+\beta))\,y_{mn} \end{aligned}$$

má netriviálne riešenie, a síce vektor $(\lambda_1, \lambda_2, \ldots, \lambda_{mn}) \neq 0$. Preto matica zložená z koeficientov tejto sústavy je singulárna (má netriviálne riešenie), a teda determinant

$$\begin{vmatrix} c_{1,1}-(\alpha+\beta) & c_{1,2} & \dots & c_{1,mn} \\ c_{2,1} & c_{2,2}-(\alpha+\beta) & \dots & c_{2,mn} \\ \vdots & \vdots & \ddots & \vdots \\ c_{mn,1} & c_{mn,2} & \dots & c_{mn,mn}-(\alpha+\beta) \end{vmatrix} = 0$$

Lenže tento determinant má po vyčíslení tvar $\sum_{i=0}^{mn} d_i (\alpha+\beta)^i$, kde $d_i \in \mathbb{Q}$. Takže $\alpha+\beta$ je koreňom polynómu $\sum_{i=0}^{mn} d_i x^i$, čo sme potrebovali.
Uzavretosť vzhľadom na násobenie. Dôkaz je analogický s predchádzajúcim prípadom.
Uzavretosť vzhľadom na inverzné prvky. Nech $\alpha \in \bar{\mathbb{Q}} \setminus \{0\}$. V tom prípade existuje polynóm f_4 taký, že $0 = f_4(\alpha) = \sum_{i=0}^{k} a_i \alpha^i, a_0, ..., a_k \in \mathbb{Q}, a_k \neq 0$. Potom pre polynóm $\tilde{f}_4 = \sum_{i=0}^{k} a_i x^{k-i}$ platí $\alpha^k \tilde{f}_4(\frac{1}{\alpha}) = \alpha^k \sum_{i=0}^{k} a_i \left(\frac{1}{\alpha}\right)^{k-i} = \alpha^k \sum_{i=0}^{k} a_i \alpha^{i-k} = \sum_{i=0}^{k} a_i \alpha^i = f_4(\alpha) = 0$. Keďže $\alpha^k \neq 0$, tak $\frac{1}{\alpha}$ je algebraické číslo. □

Dôsledok 1.2.7. *Predpokladajme, že* $\deg m_\alpha = m$ *a* $\deg m_\beta = n$. *Potom platí:* $\deg m_{-\alpha} = m$, $\deg m_{\alpha+\beta} \leq mn$, $\deg m_{\alpha\beta} \leq mn$ *a* $\deg m_{\frac{1}{\alpha}} = m$.

Definícia 1.2.8. Je daná rovnica tvaru $a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0 = 0$, $n \geq 1, a_i \in \mathbb{Z}, a_n \neq 0$. *Výškou* takejto rovnice nazývame číslo

$$h = n + |a_n| + |a_{n-1}| + \dots + |a_0| \tag{1.2}$$

Veta 1.2.9. *Teleso algebraických čísel je spočítateľné.*

Dôkaz (Cantor). Pre *fixované* h existuje len konečne mnoho rovníc s výškou h (vzhľadom na to, že v rovnosti 1.2 sú všetky členy nezáporné). Každá z týchto rovníc má najviac h rôznych koreňov. Takže existuje *konečný* počet algebraických čísel, ktorých rovnice majú výšku h. Preto môžeme algebraické čísla zoradiť do postupnosti tak, že najprv vezmeme tie, ktorých rovnice majú výšku 1, potom tie, ktorých rovnice majú výšku 2, atď. V tejto postupnosti sa budú niektoré čísla určite opakovať, takže dostávame nerovnosť $|\bar{\mathbb{Q}}| \leq |\mathbb{N}|$. Keďže ale všetky prirodzené čísla sú algebraické, tak tiež $|\bar{\mathbb{Q}}| \geq |\mathbb{N}|$, a teda $|\bar{\mathbb{Q}}| = |\mathbb{N}| = \aleph_0$. □

Veta 1.2.10. *Množinu algebraických čísel nemožno prirodzene rozšíriť. To znamená, že korene polynómov* $\sum_{i=0}^{k} a_i x^i, a_0, ..., a_k \in \bar{\mathbb{Q}}, a_k \neq 0$ *sú opäť len algebraické čísla. (Inými slovami teleso algebraických čísel je algebraickým uzáverom telesa racionálnych čísel.)*

Dôkaz. Majme teda polynóm $f = \sum_{i=0}^{k} a_i x^i, a_0, ..., a_k \in \bar{\mathbb{Q}}, a_k \neq 0, k \geq 2$ (prípad $k = 1$ je triviálny) a označme nejaký jeho nenulový koreň η. Bez ujmy na všeobecnosti môžeme predpokladať, že f je minimálnym polynómom η nad $\bar{\mathbb{Q}}$, špeciálne z toho plynie $a_0 \neq 0$ a $a_k = 1$. Dokážeme, že η je algebraické číslo nad $\bar{\mathbb{Q}}$ stupňa $k \geq 2$.
Predpokladajme, že čísla a_i sú algebraické stupňa s_i. Potom existujú racionálne koeficienty také, že

$$\begin{aligned} a_0^{s_0} &= -u_{0,s_0-1}a_0^{s_0-1} - \ldots - u_{0,1}a_0 - u_{0,0} \\ a_1^{s_1} &= -u_{1,s_1-1}a_1^{s_1-1} - \ldots - u_{1,1}a_1 - u_{1,0} \\ &\vdots \\ a_{k-1}^{s_{k-1}} &= -u_{k-1,s_{k-1}-1}a_{k-1}^{s_{k-1}-1} - \ldots - u_{k-1,1}a_{k-1} - u_{k-1,0} \end{aligned} \tag{1.3}$$

Keďže $f(\eta) = \sum_{i=0}^{k} a_i\eta^i = 0$, môžeme vyjadriť $\eta^k = -\sum_{i=0}^{k-1} a_i\eta^i$ a máme

$$\begin{aligned} \eta^k \prod_{i=0}^{k-1} a_i^{t_i} &= \left(-\sum_{i=0}^{k-1} a_i\eta^i\right) \prod_{i=0}^{k-1} a_i^{t_i} \\ &= -a_0^{t_0+1}a_1^{t_1} \ldots a_{k-1}^{t_{k-1}} - \eta a_0^{t_0}a_1^{t_1+1} \ldots a_{k-1}^{t_{k-1}} - \ldots \\ &\quad - \eta^{k-1}a_0^{t_0}a_1^{t_1} \ldots a_{k-1}^{t_{k-1}+1} \end{aligned} \tag{1.4}$$

Podobne ako vo vete 1.2.6 si zvoľme množinu všetkých možných kombinácií $\bigcup_{j=0}^{k-1}\{\eta^j a_0^{t_0} \ldots a_{k-1}^{t_{k-1}};\ t_l = 0, 1, \ldots, s_l - 1\}$ a opäť ju označme $\{\lambda_r\}_{r=1}^{N}$, kde $N = ks_0s_1 \ldots s_{k-1}$. Kombináciou 1.3 a 1.4 dostávame, že $\eta\lambda_n$ je lineárnou kombináciou $\{\lambda_r\}$ s koeficientmi už v $\mathbb{Q}$, pretože túto kombináciu možno vyjadriť pomocou racionálnych koeficientov $u_{i,j}$. Dôkaz dokončíme presne tak isto, ako vo vete 1.2.6.
Pre každé λ_n existujú konštanty $C_{n,1}, C_{n,2}, \ldots, C_{n,N} \in \mathbb{Q}$ také, že už platí $\eta\lambda_n = C_{n,1}\lambda_1 + C_{n,2}\lambda_2 + \ldots + C_{n,N}\lambda_N$. Odčítaním ľavej strany rovností máme

$$\begin{aligned} 0 &= (C_{1,1} - \eta)\,\lambda_1 + C_{1,2}\lambda_2 + \ldots + C_{1,N}\lambda_N \\ 0 &= C_{2,1}\lambda_1 + (C_{2,2} - \eta)\,\lambda_2 + \ldots + C_{2,N}\lambda_N \\ &\vdots \\ 0 &= C_{N,1}\lambda_1 + C_{N,2}\lambda_2 + \ldots + (C_{N,N} - \eta)\,\lambda_N \end{aligned}$$

Keďže $\lambda_n \neq 0$ pre každé n, je vektor $(\lambda_1, \ldots, \lambda_N)$ netriviálnym riešením príslušnej sústavy a determinant

$$\begin{vmatrix} C_{1,1}-\eta & C_{1,2} & \dots & C_{1,N} \\ C_{2,1} & C_{2,2}-\eta & \dots & C_{2,N} \\ \vdots & \vdots & \ddots & \vdots \\ C_{N,1} & C_{N,2} & \dots & C_{N,N}-\eta \end{vmatrix} = 0$$

Ale $C_{i,j}$ sú racionálne čísla, takže η je koreňom polynómu s racionálnymi koeficientmi a tým pádom ide o algebraické číslo. □

1.3 Vzťah konštruovateľných a algebraických čísel

Lema 1.3.1. *Nech α je kladné algebraické číslo. Potom aj číslo $\sqrt{\alpha}$ je algebraické.*

Dôkaz. Nech minimálny polynóm prvku α je $m_\alpha = \sum_{i=0}^{n} a_i x^i$. Potom $\sqrt{\alpha}$ je koreňom polynómu $f = \sum_{i=0}^{k} a_i x^{2i}$, pretože $f\left(\sqrt{\alpha}\right) = \sum_{i=0}^{k} a_i \left(\sqrt{\alpha}\right)^{2i} = \sum_{i=0}^{k} a_i \alpha^i = m_\alpha\left(\alpha\right) = 0$. □

Veta 1.3.2. *Každé konštruovateľné číslo je algebraické.*

Dôkaz. Spomeňme si na definíciu konštruovateľných čísel. $\mathcal{K}$ je zjednotením akýchsi rozšírení K_i. Pri dôkaze použijeme práve tieto rozšírenia a vetu dokážeme matematickou indukciou.
Nech $r \in K_0 = \mathbb{Q}$. Potom r je algebraické, pretože je koreňom polynómu $x - r$, a teda K_0 obsahuje len algebraické čísla.
Predpokladajme teda, že všetky množiny $K_0, K_1, \dots, K_n$ sa skladajú len z algebraických čísel. Nech ďalej $s \in K_{n+1}$. Potom vyjadríme $s = p + q\sqrt{w}$, kde $p, q, w \in K_n, \sqrt{w} \notin K_n$. Podľa indukčného predpokladu sú čísla p, q, w algebraické a podľa predchádzajúcej lemy je aj číslo $\sqrt{w}$ algebraické. Keďže množina algebraických čísel tvorí teleso, tak aj s je algebraické, a tým pádom aj všetky prvky K_{n+1} sú algebraické.
Potom však nutne každý prvok množiny $\mathcal{K} = \bigcup_{i=0}^{\infty} K_i$ je algebraický, čo sme chceli ukázať. □

Dôsledok 1.3.3. *Teleso konštruovateľných čísel je podtelesom telesa algebraických čísel. Keďže teleso algebraických čísel je spočítateľné, tak aj teleso konštruovateľných čísel je spočítateľné.*

Dôsledok 1.3.4. *Žiadne transcendentné číslo nie je euklidovsky konštruovateľné.*

Kapitola 2

Délsky problém

Majme danú kocku s hranou jednotkovej dĺžky. Je možné euklidovsky zostrojiť hranu kocky, ktorá by mala dvojnásobný objem? Táto úloha sa nazýva Délsky problém, niekedy sa však tiež nazýva problém duplicity, resp. zdvojenia, kocky.

Jednotková kocka ma zrejme objem 1, dvojnásobok je teda samozrejme 2. Preto by sme radi zostrojili úsečku dĺžky $\sqrt[3]{2}$, z ktorej by sme už kocku jednoducho zostrojili.

Veta 2.0.5. *$\sqrt[3]{2}$ nie je konštruovateľné číslo.*

Dôkaz. Dokážme sporom.
Najprv vylúčme možnosť $\sqrt[3]{2} \in K_0$, tj. že ide o racionálne číslo. Nech $\sqrt[3]{2} = \frac{p}{q}, p, q \in \mathbb{Z}$ a navyše $\mathrm{D}(p,q) = 1$. Potom $2q^3 = p^3$, teda $2 \mid p^3$, z čoho $2 \mid p$. Po dosadení $p = 2k$ máme $2q^3 = 8k^3$, teda $q^3 = 4k^3$, z čoho $4 \mid q^3$, takže $2 \mid q$. Potom $\mathrm{D}(p,q) > 1$, čo je spor.
Ďalej nech teda $\sqrt[3]{2} \in \mathcal{K} \setminus K_0$. Vzhľadom na to, že $K_n \subsetneq K_{n+1}$, tak existuje minimálne prirodzené m také, že $\sqrt[3]{2} \in K_m$ (inými slovami $\sqrt[3]{2} \in K_i;\ \forall i \geq m$ a zároveň $\sqrt[3]{2} \notin K_j;\ \forall\, j < m$). V tom prípade sa $\sqrt[3]{2}$ dá vyjadriť ako prvok množiny K_m, a teda pre $p, q, w \in K_{m-1}; \sqrt{w} \notin K_{m-1}$ môžeme písať:

$$\begin{aligned}
\sqrt[3]{2} &= p + q\sqrt{w} \\
0 &= (p + q\sqrt{w})^3 - 2 \\
0 &= p^3 + 3p^2q\sqrt{w} + 3pq^2w + q^3(\sqrt{w})^3 - 2 \\
0 &= (p^3 + 3pq^2w - 2) + (3p^2q + q^3w)\sqrt{w}
\end{aligned}$$

Všetky prvky rovnosti okrem $\sqrt{w}$ náležia do množiny K_{m-1}, a teda ak sa na K_m pozrieme ako na rozšírenie K_{m-1}, musia súčasne platiť tieto dve rovnosti:

$$0 = p^3 + 3pq^2w - 2$$
$$0 = 3p^2q + q^3w$$

Vynásobme druhú rovnosť členom $\sqrt{w}$ (na ktorý sa už teraz pozeráme ako na prvok K_m) a odčítajme ju od prvej rovnosti. Dostávame:

$$2 = p^3 - 3p^2q\sqrt{w} + 3pq^2w - q^3(\sqrt{w})^3 = (p - q\sqrt{w})^3$$

To ale znamená, že $p - q\sqrt{w}$ je koreňom rovnice $x^3 - 2 = 0$. Lenže koreňom tejto rovnosti je podľa predpokladu aj číslo $p + q\sqrt{w}$, pričom obe tieto čísla sú reálne. Lenže rovnica $x^3 - 2 = 0$ má práve jeden reálny koreň, preto medzi číslami musí nastávať rovnosť. Zrejme $q \neq 0$ (ak by to tak bolo, tak $\sqrt[3]{2} = p \in K_{m-1}$, čo je spor s minimalitou m), teda po odčítaní p a vydelení q dostávame $-\sqrt{w} = \sqrt{w}$, čiže $w = 0 \in K_0$, čo je spor. □

Dôsledok 2.0.6. *Délsky problém nie je euklidovsky riešiteľný.*

Kapitola 3

Trisekcia uhla

3.1 Neriešiteľnosť problému

V tejto sekcii sa pokúsime dokázať neriešiteľnosť ďalšieho z antických problémov: trisekcie uhla. Takže sa pokúsime ukázať, že pomocou pravítka bez rysky a kružidla sa nedá roztretiť uhol. Samozrejme, v niektorých špeciálnych prípadoch je trisekcia možná, pretože napríklad tretinu pravého uhla (čo je $\frac{\pi}{6}$) skonštruovať vieme. My však ukážeme, že trisekcia uhla *vo všeobecnosti* možná nie je, tzn. že existuje taký uhol, ktorý sa pomocou pravítka a kružidla roztretiť nedá.

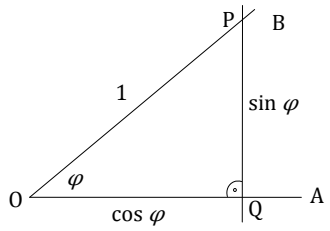
Definícia 3.1.1. Uhol α sa nazýva euklidovsky skonštruovateľný, pokiaľ ho je možné v konečnom počte krokov zostrojiť len pomocou kružidla a pravítka bez rysky.

Opäť sa pokúsime použiť charakteristiku konštruovateľnch čísel. Lenže je rozdiel medzi *konštrukciou uhla* a *konštrukciou čísla*. Preto potrebujeme nájsť nejakú číselnú charakteristiku uhla, ktorej konštruovateľnosť zodpovedá konštruovateľnosti uhla. Pokiaľ sa obmedzíme na interval $(0, \frac{\pi}{2})$, najprirodzenejšou voľbou sú goniometrické funkcie, ktoré ponúkajú prosté zobrazenie intervalu $(0, \frac{\pi}{2})$ do reálnych čísel.

Lema 3.1.2. *Nech $\varphi \in (0, \frac{\pi}{2})$. Uhol φ je euklidovsky skonštruovateľný práve vtedy keď je $\cos\varphi$ konštruovateľné číslo.*

Dôkaz. Pokiaľ je uhol φ euklidovsky skonštruovateľný, zoberme nejaký trojuholník AOB s uhlom φ. Na polpriamku OB nanesme jednotkovú vzdialenosť a príslušný bod označme P. Zostrojme kolmicu na OA prechádzajúcu

bodom P a priesečník označme Q. Potom dĺžka úsečky OQ je $\cos\,\varphi$. Naopak, ak máme danú úsečku OQ dĺžky $\cos\,\varphi$, zostrojíme kolmicu na OQ v bode Q. Priesečník tejto kolmice a jednotkovej kružnice so stredom v bode O označme P. Potom $|\measuredangle QOP| = \varphi$.



□

Lema 3.1.3. *Nech* $\varphi \in (0, \frac{\pi}{2})$. *Potom platí* $\cos\varphi = 4\,\cos^3\frac{\varphi}{3} - 3\,\cos\frac{\varphi}{3}$.

Dôkaz.

$$\begin{aligned}
\cos\varphi &= \cos\left(\frac{2\varphi}{3} + \frac{\varphi}{3}\right) \\
&= \cos\frac{2\varphi}{3}\,\cos\frac{\varphi}{3} - \sin\frac{2\varphi}{3}\,\sin\frac{\varphi}{3} \\
&= \left(\cos^2\frac{\varphi}{3} - \sin^2\frac{\varphi}{3}\right)\,\cos\frac{\varphi}{3} - 2\,\sin^2\frac{\varphi}{3}\,\cos\frac{\varphi}{3} \\
&= \left(2\cos^2\frac{\varphi}{3} - 1\right)\,\cos\frac{\varphi}{3} - 2\left(1 - \cos^2\frac{\varphi}{3}\right)\,\cos\frac{\varphi}{3} \\
&= 4\,\cos^3\frac{\varphi}{3} - 3\,\cos\frac{\varphi}{3}
\end{aligned}$$

□

Lema 3.1.4 (Viètove vzťahy)**.** *Nech* α, β, γ *sú koreňmi kubickej rovnice* $x^3 + ax^2 + bx + c = 0,\ a, b, c \in \mathbb{R}$. *Potom platí*

$$\begin{aligned}
a &= -(\alpha + \beta + \gamma) \\
b &= \alpha\beta + \alpha\gamma + \beta\gamma \\
c &= -\alpha\beta\gamma
\end{aligned}$$

Dôkaz. $x^3 + ax^2 + bx + c = (x - \alpha)(x - \beta)(x - \gamma) = x^3 - (\alpha + \beta + \gamma)x^2 + (\alpha\beta + \alpha\gamma + \beta\gamma)x - \alpha\beta\gamma$ a porovnáme koeficienty. □

Veta 3.1.5. *Trisekcia uhla veľkosti $\frac{\pi}{3}$ nie je euklidovsky možná.*

Dôkaz. Dosaďme do lemy 3.1.3 veľkosť uhla $\frac{\pi}{3}$. Potom dostávame rovnosť $4\cos^3\frac{\pi}{9} - 3\cos\frac{\pi}{9} = \cos\frac{\pi}{3} = \frac{1}{2}$. To ale znamená, že $\cos\frac{\pi}{9}$ je koreňom rovnice $4x^3 - 3x - \frac{1}{2} = 0$. Po vynásobení rovnice číslom 2 a substitúcii $y = 2x$ (táto substitúcia síce zmení korene, ale nezmení vlastnosť konštruovateľnosti) dostávame rovnosť

$$y^3 - 3y = 1 \tag{3.1}$$

Podobne ako vo vete 2.0.5 budeme dokazovať, že táto rovnosť nemá konštruovateľné riešenie, opäť sporom.
Nech koreň rovnosti 3.1 je racionálne číslo tvaru $\frac{p}{q}$, kde $p, q \in \mathbb{Z}$ a $\mathrm{D}(p,q) = 1$. Po úprave dostávame rovnosť $p\ (p^2 - 3q^2) = q^3$, teda $p \mid q^3$. Aby mohlo byť zároveň $\mathrm{D}(p,q) = 1$, musí nutne byť $p = \pm 1$. Po dosadení do rovnice dostávame $\pm(1 - 3q^2) = q^3$, takže $\pm 1 = q^3 \pm 3q^2$. To ale znamená, že $q^2 \mid \pm 1$, teda opätovne $q = \pm 1$. Potom ale $\frac{p}{q} = \pm 1$, čo ale nie je koreň rovnice 3.1. Riešenie rovnice teda nemôže byť racionálnym číslom.
Z lemy 3.1.4 pre rovnosť 3.1 plynie $\alpha + \beta + \gamma = 0$. Nech teda aspoň jedno z čísel α, β, γ je konštruovateľné riešenie rovnice v $\mathcal{K} \setminus K_0$. Podobne ako pri dôkaze neriešiteľnosti Délskeho problému vezmeme najmenšie rozšírenie K_n také, že daný koreň je prvkom tohoto rozšírenia (pokiaľ by bolo konštruovateľných koreňov viac, vezmeme také minimálne rozšírenie, ktoré obsahuje aspoň jedno konštruovateľné riešenie). Bez ujmy na všeobecnosti nech α je ten koreň, a teda $\alpha = p + q\sqrt{w} \in K_n$. Dosaďme do rovnice a máme

$$\begin{aligned} 0 &= (p + q\sqrt{w})^3 - 3(p + q\sqrt{w}) - 1 \\ &= (p^3 + 3pq^2w - 3p - 1) + (3p^2q + q^3w - 3q)\sqrt{w} \end{aligned}$$

Opäť teda zároveň musia platiť rovnosti

$$\begin{aligned} 0 &= p^3 + 3pq^2w - 3p - 1 \\ 0 &= 3p^2q + q^3w - 3q \end{aligned}$$

Vynásobením druhej rovnosti prvkom $\sqrt{w}$ a odčítaním od prvej rovnosti dostávame

$$\begin{aligned} 0 &= (p^3 + 3pq^2w - 3p - 1) - (3p^2q + q^3w - 3q)\sqrt{w} \\ &= [p^3 - 3p^2q\sqrt{w} + 3pq^2w - q^3(\sqrt{w})^3] - 3[p - q\sqrt{w}] - 1 \\ &= (p - q\sqrt{w})^3 - 3(p - q\sqrt{w}) - 1 \end{aligned}$$

To ale znamená, že $p-q\sqrt{w}$ je ďalšie riešenie rovnosti 3.1, dokonca koštruovateľné. Bez ujmy na všeobecnosti nech toto riešenie je β. Zrejme $\alpha \neq \beta$, takže ide o dve rôzne riešenia. Potom pre riešenie γ ($\alpha \neq \gamma \neq \beta$) tejto rovnosti platí

$$\gamma = -\alpha - \beta = -(p + q\sqrt{w}) - (p - q\sqrt{w}) = -2p$$

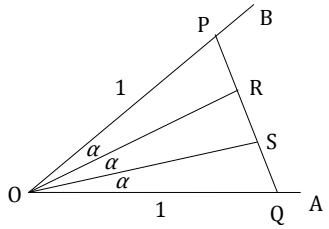
Lenže $p \in K_{n-1}$, a teda aj $\gamma \in K_{n-1}$, čo je spor s minimalitou vybraného rozšírenia. □

Dôsledok 3.1.6. *Existuje uhol, ktorého trisekcia pomocou pravítka bez rysky a kružidla nie je možná, a teda problém trisekcie uhla nie je vo všeobecnosti euklidovsky riešiteľný.*

3.2 Zdanlivé riešenia trisekcie uhla

V tejto sekcii si predstavíme niektoré časté zdanlivé riešenia trisekcie uhla a vysvetlíme si, v čom sú chybné. Väčšina chybných riešení buď v skutočnosti nedelí uhol na tretiny alebo používa nepovolené nástroje a operácie.

Príklad 3.2.1. Majme (pre jednoduchosť ostrý) uhol AOB, ktorý chceme rozdeliť na tretiny. Vezmime kružidlo a nanesme na ramená tohto uhla jednotkovú vzdialenosť a dostaneme body P a Q. Spojíme tieto body priamkou a úsečku PQ (euklidovsky) rozdelíme na tretiny a dostaneme body R a S. Potom tvrdíme, že $|\measuredangle AOS| = |\measuredangle SOR| = |\measuredangle ROB| = \frac{1}{3}|\measuredangle AOB|$.



Evidentne sme sa nedopustili žiadnej nepovolenej operácie, takže očakávame, že výsledný postup *nedelí* uhol na tretiny. Ukážeme dokonca, že uvedený postup nefunguje *pre žiadny* ostrý uhol.

Pre spor predpokladajme, že tento postup skutočne funguje a $|\measuredangle AOS| = |\measuredangle SOR| = |\measuredangle ROB| = \alpha$. Trojuholník QOP je rovnoramenný a preto sú uhly OQP a OPQ zhodné, čiže majú veľkosť $\frac{\pi-3\alpha}{2} = \frac{\pi}{2} - \frac{3\alpha}{2}$. Dopočítaním uhlov zistíme, že $|\measuredangle ORP| = |\measuredangle OSQ| = \frac{\pi}{2} + \frac{\alpha}{2}$ a $|\measuredangle ORS| = |\measuredangle OSR| = \frac{\pi}{2} - \frac{\alpha}{2}$. Trojuholník SOR je teda rovnoramenný a označme $|PR| = |RS| = |SQ| = a$ a $|OS| = |OR| = b$.
Zo sínusovej vety pre trojuholník SOR dostávame

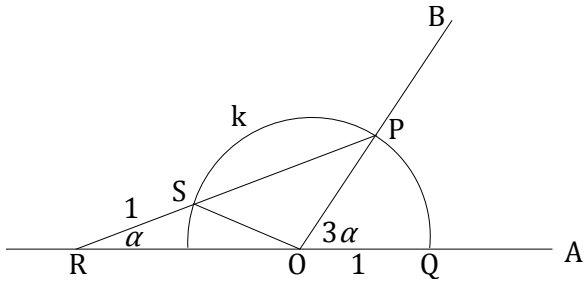
$$\frac{a}{\sin\alpha} = \frac{b}{\sin\left(\frac{\pi}{2} - \frac{\alpha}{2}\right)} = \frac{b}{\cos\frac{\alpha}{2}}$$

Pre trojuholník ROP však sínusová veta dáva

$$\frac{a}{\sin\alpha} = \frac{1}{\sin\left(\frac{\pi}{2} + \frac{\alpha}{2}\right)} = \frac{1}{\cos\frac{\alpha}{2}}$$

Spojením rovností dostávame $\frac{b}{\cos\frac{\alpha}{2}} = \frac{1}{\cos\frac{\alpha}{2}}$. Keďže $\cos\frac{\alpha}{2}$ je na intervale $(0, \pi)$ nenulový, tak plynie $b = 1$. Potom však body P, Q, R a S ležia na kružnici so stredom v O a polomerom 1, ale zároveň ležia na jednej úsečke. Spor.

Príklad 3.2.2 (Archimedes)**.** Majme opäť ostrý uhol AOB. Spravme kružnicu k o polomere 1 so stredom v O. Priesečníky ramien uhla a kružnice označme znovu P a Q. Ďalej zostrojme úsečku PR tak, aby R ležalo na priamke OA a zároveň dĺžka úsečky RS (kde S je priesečníkom úsečky PR a kružnice k) bola 1. Potom $|\measuredangle ARP| = \frac{1}{3}|\measuredangle AOB|$.



Označme $|\measuredangle ARP| = \alpha$. Trojuholník OSR je rovnoramenný a $|\measuredangle ROS| = \alpha$ a $|\measuredangle OSR| = \pi - 2\alpha$. Ďalej uhol OSP má veľkosť 2α. Trojuholník SOP je

takisto rovnoramenný a $|\measuredangle SPO| = 2\alpha$ a $|\measuredangle SOP| = \pi - 4\alpha$. Veľkosť uhla AOB je teda 3α.

V tomto prípade sa nám podarilo uhol roztretiť, takže sme sa niekde museli dopustiť nepovolenej operácie. A skutočne, pozrime sa na konštrukciu úsečky PR. Vyžadujeme, aby jedna konkrétna časť úsečky mala dĺžku 1. Keby šlo o to nakresliť úsečku dĺžky 1, nemáme problém, lenže táto úsečka je súčasťou inej úsečky, a preto potrebujeme dĺžku 1 preniesť. Na to však nemôžeme použiť kružidlo a príslušnú dĺžku si nemôžeme ani zaznačiť na pravítko (viď definícia 1.1.1). Požadovanú úsečku PR teda nevieme euklidovsky skonštruovať.

Príklad 3.2.3. Pomerne jednoduchým nápadom je použiť geometrickú postupnosť. Uhol euklidovsky rozpoliť vieme, takže vieme vytvoriť aj jeho štvrtinu, osminu, atď. Tiež máme $\sum_{i=1}^{\infty} \left(\frac{1}{4}\right)^i = \frac{1}{3}$, teda sčítaním štvrtiny uhla, $\frac{1}{16}$ uhla, $\frac{1}{64}$ uhla, atď. dostaneme tretinu uhla.

Tento postup vôbec nevyznieva hlúpo, najmä keď si uvedomíme, že množina konštruovateľných čísel je zjednotením *nekonečného* počtu iných množín. Môže teda nekonečný počet iterácií viesť ku konštruovateľnému číslu? V určitých špeciálnych prípadoch určite áno, ale vo všeobecnosti nie. Ak je totiž číslo a konštruovateľné, tj. $a \in \mathcal{K} = \bigcup_{n=0}^{\infty} K_n$, kde K_n sú popísané v prvej kapitole, tak existuje minimálne m také, že $a \in K_m$, a na takúto konštrukciu potrebujeme len m, teda konečne veľa, krokov.

Kapitola 4

Kvadratúra kruhu

V tejto kapitole ukážeme, že kvadratúra kruhu vo všeobecnosti nie je možná. Zoberme si kruh o polomere 1, ten má obsah π. Takže by sme radi vytvorili štvorec, ktorý má stranu dlhú $\sqrt{\pi}$.

Pri dôkaze neriešiteľnosti tohto problému sa potrebujeme odvolať na charakteristiky algebraických čísel. Keďže každé konštruovateľné číslo je aj algbraické, stačí, ak dokážeme, že $\sqrt{\pi}$ je transcendentné. Na to nám však postačuje ukázať, že π je transcendentné, pretože algebraické čísla sú uzavreté na tvorbu druhých odmocnín.

4.1 Transcendentné čísla

Keďže množina reálnych čísel je nespočítateľná, na základe vety 1.2.9 transcendentné čísla existujú, a dokonca je ich nespočítateľne veľa. Dôkaz tejto vety je však nekonštruktívny. Preto uvedieme aj iný dôkaz, ktorý niektoré transcendentné čísla priamo konštruuje.

Veta 4.1.1 (Liouville)**.** *Nech α je algebraické číslo stupňa $n > 1$. Potom existuje $Q \in \mathbb{Z}$ také, že $\forall\, q \geq Q$ a $\forall\, p \in \mathbb{Z}$ platí*

$$\left|\alpha - \frac{p}{q}\right| > \frac{1}{q^{n+1}}$$

Dôkaz. Uvažujme postupnosť zlomkov $\alpha_m = \frac{p_m}{q_m}$ takú, že $q_m \to \infty$ pre $m \to \infty$ a p_m nech je také, že $\left|\alpha - \frac{p_m}{q_m}\right|$ je minimálne možné (tj. $\frac{p_m}{q_m}$ je

zlomok najlepšie aproximujúci α pri danom menovateli q_m). Potom zrejme platí $\alpha_m \to \alpha$.
Na základe poznámky 1.2.5 je α iracionálne číslo, teda $\alpha_m \neq \alpha \ \forall\, m \in \mathbb{N}$, lebo α_m je racionálne a α je iracionálne.
Nech $f(x) = \sum_{i=0}^{n} a_i x^i$ je ten polynóm stupňa n, ktorý zabezpečuje algebraickosť α, tj. $f(\alpha) = 0$. Potom máme

$$\begin{aligned} f(\alpha_m) = f(\alpha_m) - f(\alpha) &= \sum_{i=0}^{n} a_i \alpha_m^i - \sum_{i=0}^{n} a_i \alpha^i \\ &= a_1(\alpha_m - \alpha) + a_2(\alpha_m^2 - \alpha^2) + \ldots + a_n(\alpha_m^n - \alpha^n) \\ &= (\alpha_m - \alpha)[a_1 + a_2(\alpha_m + \alpha) + a_3(\alpha_m^2 + \alpha_m\alpha + \alpha^2) + \ldots \\ &\quad \ldots + a_n(\alpha_m^{n-1} + \alpha_m^{n-2}\alpha + \ldots + \alpha^{n-1})] \end{aligned}$$

Keďže $\alpha_m \to \alpha$, tak pre dostatočne veľké m bude $|\alpha_m - \alpha| < \varepsilon$ (pre ľubovoľné pevné $\varepsilon > 0$). Potom môžeme odhadnúť

$$\begin{aligned} \left|\frac{f(\alpha_m)}{\alpha_m - \alpha}\right| &= \left|a_1 + a_2(\alpha_m + \alpha) + \ldots + a_n(\alpha_m^{n-1} + \alpha_m^{n-2}\alpha + \ldots + \alpha^{n-1})\right| \\ &\leq |a_1| + |a_2|\,|(\alpha_m + \alpha)| + \ldots + |a_n|\left|(\alpha_m^{n-1} + \ldots + \alpha^{n-1})\right| \\ &< |a_1| + 2\,|a_2|\,(|\alpha| + \varepsilon) + \ldots + n\,|a_n|\,(|\alpha| + \varepsilon)^{n-1} = H \end{aligned}$$

Keďže pravá strana nerovnosti je závislá len na α a ε, tak H je pevné číslo. Uvažujme m dokonca také veľké, že $q_m > H$. Potom

$$|\alpha - \alpha_m| > \frac{|f(\alpha_m)|}{H} > \frac{|f(\alpha_m)|}{q_m}$$

Ukážeme, že q_m je hľadané Q. Označme teda $P = p_m$ a $Q = q_m$. Počítajme

$$|f(\alpha_m)| = \left|\sum_{i=0}^{n} a_i \left(\frac{P}{Q}\right)^i\right| = \left|\frac{1}{Q^n}\right| \left|\sum_{i=0}^{n} a_i P^i Q^{n-i}\right|$$

Všimnime si, že suma na pravej strane je celé číslo. Zrejme však $f(\alpha_m) \neq 0$. Keby tomu tak bolo, potom $f(x) = (x - \alpha_m)g(x)$. Potom by ale α muselo byť koreňom polynómu g, ktorého stupeň je $n - 1$. To je ale v spore s tým, že ide o algebraické číslo stupňa n.

Potom ale aj $|\sum_{i=0}^{n} a_i P^i Q^{n-i}| \neq 0$, takže $|\sum_{i=0}^{n} a_i P^i Q^{n-i}| \geq 1$. Z toho máme $|f(\alpha_m)| \geq \frac{1}{Q^n}$ a kombináciou nerovností dostávame

$$|\alpha - \alpha_m| > \frac{|f(\alpha_m)|}{Q} \geq \frac{1}{Q^n}\frac{1}{Q} = \frac{1}{Q^{n+1}},$$

čo sme chceli dokázať. □

Veta 4.1.2. *Čísla tvaru*

$$\begin{aligned}\beta &= \sum_{i=1}^{\infty} b_i 10^{-i!}, \quad b_i \in \{1, 2, \ldots, 9\} \\ &= 0, b_1 b_2 000 b_3 0000000000000000 b_4 0 \ldots\end{aligned}$$

sú transcendentné pre ľubovoľnú voľbu koeficientov b_i

Dôkaz. Čísla tohto tvaru nie sú racionálne, keďže zrejme nemajú ukončený ani periodický desatinný rozvoj. Preto sa pokúsime nejako použiť Liouvilleovu vetu.
Označme β_m číslo

$$\sum_{i=1}^{m} b_i 10^{-i!} = 0, b_1 b_2 000 b_3 0 \ldots 0 b_m$$

Potom číslo $|\beta - \beta_m|$ má prvú nenulovú cifru na $(m+1)!$-tom mieste desatinného rozvoja, a preto $|\beta - \beta_m| < 10.10^{-(m+1)!}$.
Ďalej pre spor predpokladajme, že β je algebraické číslo. Nech jeho stupeň je n. Potom z Liouvilleovej vety plynie, že $\left|\beta - \frac{p}{q}\right| > \frac{1}{q^{n+1}}$ pre dostatočne veľké menovatele q. Zapíšme β_m ako $\frac{p}{q} = \frac{p}{10^{m!}}$, čo môžeme spraviť vďaka tomu, že β_m má za desatinnou čiarkou $m!$ desatinných miest. Dostávame $|\beta - \beta_m| > \frac{1}{10^{m!(n+1)}}$ pre dostatočne veľké m.
Takže spolu máme

$$\begin{aligned}\frac{1}{10^{m!(n+1)}} < |\beta - \beta_m| < 10.10^{-(m+1)!} &= \frac{1}{10^{(m+1)!-1}} \\ 10^{m!(n+1)} &> 10^{(m+1)!-1} \\ m!(n+1) &> (m+1)! - 1\end{aligned}$$

Lenže $n+1$ je pevné číslo, takže posledná nerovnosť pre dostatočne veľké m (stačí napríklad vziať $m \geq n+1$) platiť nemôže. To je spor s predpokladom, že β je algebraické, a teda β je transcendentné. □

Dôsledok 4.1.3. *Množiny konštruovateľných ani algebraických čísel nie sú uzavreté v* $\mathbb{R}$ *(resp.* $\mathbb{C}$*).*

Dôkaz. Vezmime si čísla β_m z predchádzajúceho dôkazu. Tieto čísla sú racionálne, a teda konštruovateľné a algebraické. Zrejme tiež $\beta_m \to \beta$ pre $m \to \infty$. β je ale transcendentné číslo. □

4.2 Niekoľko prípravných tvrdení

Definícia 4.2.1. Nech $f(x) = \sum_{i=0}^{n} a_i x^i, a_i \in \mathbb{R}$ je polynóm stupňa n. Potom pre $t \in \mathbb{C}$ definujeme krivkový integrál

$$I_f(t) = \int_\varphi e^{t-u} f(u)\,\mathrm{d}u$$

pozdĺž úsečky $[0, t]$. Ďalej definujeme polynóm

$$\bar{f}(x) = \sum_{i=0}^{n} |a_i|\, x^i$$

Lema 4.2.2. *Platí*

$$I_f(t) = e^t \sum_{i=0}^{n} f^{(i)}(0) - \sum_{i=0}^{n} f^{(i)}(t)$$

kde $f^{(i)}$ *označuje i-tú deriváciu polynómu* f*.*

Dôkaz. Integrujme per partes:

$$\begin{aligned}
I_f(t) &= \int_\varphi e^{t-u} f(u)\,\mathrm{d}u = \left[-e^{t-u} f(u)\right]_0^t - \int_\varphi \left(-e^{t-u}\right) f'(u)\,\mathrm{d}u \\
&= -f(t) + e^t f(0) + \int_\varphi e^{t-u} f'(u)\,\mathrm{d}u \\
&= -f(t) + e^t f(0) - f'(t) + e^t f'(0) + \int_\varphi e^{t-u} f''(u)\,\mathrm{d}u \\
&\vdots \\
&= \sum_{i=0}^{n} e^t f^{(i)}(0) - \sum_{i=0}^{n} f^{(i)}(t) + \int_\varphi e^{t-u} f^{(n+1)}(u)\,\mathrm{d}u \\
&= e^t \sum_{i=0}^{n} f^{(i)}(0) - \sum_{i=0}^{n} f^{(i)}(t),
\end{aligned}$$

pretože $f^{(n+1)}(x) = 0$ (stupeň polynómu f je n). □

Lema 4.2.3. *Platí*

$$|I_f(t)| \leq |t|\, e^{|t|}\, \bar{f}(|t|)$$

Dôkaz. Nech u je bod náležiaci úsečke $[0, t]$. Potom zrejme $|u| \leq |t|$ a tiež $|t - u| \leq |t|$. Potom

$$\left|e^{t-u}\right| = e^{\mathrm{Re}(t-u)} \leq e^{|t|}$$
$$|f(u)| \leq \bar{f}(|u|) \leq \bar{f}(|t|)$$

a môžeme odhadnúť

$$\begin{aligned}|I_f(t)| &\leq L(\varphi) \cdot \sup_{u\in\langle\varphi\rangle} \left|e^{t-u} f(u)\right| \leq L(\varphi) \cdot \sup_{u\in\langle\varphi\rangle} \left|e^{t-u}\right| \cdot \sup_{u\in\langle\varphi\rangle} |f(u)| \\ &\leq |t|\, e^{|t|}\, \bar{f}(|t|)\end{aligned}$$

□

Ešte budeme potrebovať tzv. fundamentálnu vetu o symetrických polynómoch, ktorú však ponecháme bez dôkazu. Dôkaz tohto tvrdenia možno nájsť napríklad v [6], str. 99-102.

Definícia 4.2.4. Nech S_n označuje symetrickú grupu na n prvkoch (tj. grupu všetkých permutácií n-prvkovej množiny) a K nejaký okruh. Potom polynóm $f \in K[x_1, x_2, \ldots, x_n]$ sa nazýva *symetrický v premenných* $x_1, \ldots, x_n$, pokiaľ

$$f(x_1, x_2, \ldots, x_n) = f\left(x_{\sigma(1)}, x_{\sigma(2)}, \ldots, x_{\sigma(n)}\right) \qquad \forall\, \sigma \in S_n$$

Definícia 4.2.5. Nech K je okruh a $K[x_1, x_2, \ldots, x_n]$ označuje okruh polynómov n premenných. Potom polynómy

$$\begin{aligned}e_1 &= \sum_{j=1}^{n} x_j \\ e_2 &= \sum_{j_1<j_2\leq n} x_{j_1} x_{j_2} \\ e_3 &= \sum_{j_1<j_2<j_3\leq n} x_{j_1} x_{j_2} x_{j_3} \\ &\vdots \\ e_n &= x_1 x_2 \ldots x_n\end{aligned}$$

sa nazývajú *elementárne symetrické polynómy nad* $x_1, x_2, \ldots, x_n$.

Veta 4.2.6 (Fundamentálna veta o symetrických polynómoch)**.** *K nech je okruh a ďalej nech $f \in K[x_1, \ldots, x_n]$ je symetrický polynóm v $x_1, \ldots, x_n$. Potom $f \in K[e_1, e_2, \ldots, e_n]$.*

Veta 4.2.7 (Leibnizova formula)**.** *Nech $f_1, f_2, \ldots, f_k$ sú dostatočne hladké funkcie. Potom pre $n \in \mathbb{N} \cup \{0\}$ platí*

$$(f_1 f_2 \ldots f_k)^{(n)} = \sum_{n_1+n_2+\ldots+n_k=n} \frac{n!}{n_1! \ldots n_k!} f_1^{(n_1)} \ldots f_k^{(n_k)}$$

Dôkaz. Formulu dokážeme indukciou najprv len pre dve funkcie a potom opätovne použijeme indukciu, aby sme dostali všeobecné tvrdenie pre k funkcií.

Potrebujeme teda ukázať platnosť

$$(fg)^{(n)} = \sum_{i=0}^{n} \binom{n}{i} f^{(i)} g^{(n-i)}$$

Pre $n = 0$ zjavne $(fg)^{(0)} = fg = \binom{0}{0} f^{(0)} g^{(0)}$. Pre indukciu teda predpokladajme, že $(fg)^{(n)} = \sum_{i=0}^{n} \binom{n}{i} f^{(i)} g^{(n-i)}$ a pokúsme sa vyjadriť $(fg)^{(n+1)}$. Použijeme pritom kombinatorickú identitu $\binom{n}{i} + \binom{n}{i+1} = \binom{n+1}{i+1}$.

$$\begin{aligned}
(fg)^{(n+1)} &= \left((fg)^{(n)}\right)' = \left(\sum_{i=0}^{n} \binom{n}{i} f^{(i)} g^{(n-i)}\right)' \\
&= \sum_{i=0}^{n} \binom{n}{i} f^{(i+1)} g^{(n-i)} + \sum_{i=0}^{n} \binom{n}{i} f^{(i)} g^{(n+1-i)} \\
&= \sum_{i=0}^{n-1} \binom{n}{i} f^{(i+1)} g^{(n-i)} + f^{(n+1)} g + f g^{(n+1)} + \sum_{i=1}^{n} \binom{n}{i} f^{(i)} g^{(n+1-i)} \\
&= f g^{(n+1)} + \sum_{i=1}^{n} \binom{n}{i-1} f^{(i)} g^{(n+1-i)} + \sum_{i=1}^{n} \binom{n}{i} f^{(i)} g^{(n+1-i)} + f^{(n+1)} g \\
&= f g^{(n+1)} + \sum_{i=1}^{n} \binom{n+1}{i} f^{(i)} g^{(n+1-i)} + f^{(n+1)} g \\
&= \sum_{i=0}^{n+1} \binom{n+1}{i} f^{(i)} g^{(n+1-i)}
\end{aligned}$$

Rozšírme vzorec na k funkcií. Pre jednu funkciu vzorec platí triviálne, vzorec pre dve funkcie sme odvodili vyššie. Predpokladajme teda, že vzorec platí pre všetky počty funkcií až po k a odvodíme platnosť pre $k+1$ funkcií.

$$\begin{aligned}
(f_1 \dots f_k f_{k+1})^{(n)} &= \sum_{i=0}^{n} \binom{n}{i} (f_1 \dots f_k)^{(i)} f_{k+1}^{(n-i)} \\
&= \sum_{i=0}^{n} \frac{n!}{i!\,(n-i)!} \left(\sum_{i_1+\dots+i_k=i} \frac{i!}{i_1! \dots i_k!} f_1^{(i_1)} \dots f_k^{(i_k)} \right) f_{k+1}^{(n-i)} \\
&= \sum_{i=0}^{n} \sum_{i_1+\dots+i_k=i} \frac{n!}{i_1! \dots i_k! (n-i)!} f_1^{(i_1)} \dots f_k^{(i_k)} f_{k+1}^{(n-i)} \\
&= \sum_{n_1+\dots+n_k+n_{k+1}=n} \frac{n!}{n_1! \dots n_k! n_{k+1}!} f_1^{(n_1)} \dots f_k^{(n_k)} f_{k+1}^{(n_{k+1})},
\end{aligned}$$

čo sme chceli dokázať. □

Pracujme teraz s polynómom $g(x) = x^{p-1}(x-\lambda_1)^p(x-\lambda_2)^p \dots (x-\lambda_r)^p$, kde $p \in \mathbb{N}$. Podľa Leibnizovej formuly

$$\begin{aligned}
g^{(k)}(x) &= \sum_{k_0+\dots+k_r=k} \frac{k!}{k_0! \dots k_r!} \left(x^{p-1}\right)^{(k_0)} \left((x-\lambda_1)^p\right)^{(k_1)} \dots \left((x-\lambda_r)^p\right)^{(k_r)} \\
&= k! \sum_{\substack{k_0+\dots+k_r=k \\ k_0 \le p-1 \\ k_1,\dots,k_r \le p}} \left(\frac{1}{k_0! \dots k_r!} \frac{(p-1)!}{(p-1-k_0)!} x^{p-1-k_0} \prod_{j=1}^{r} \frac{p!}{(p-k_j)!} (x-\lambda_j)^{p-k_j} \right) \\
&= k! \sum_{\substack{k_0+\dots+k_r=k \\ k_0 \le p-1 \\ k_1,\dots,k_r \le p}} \left(\binom{p-1}{k_0} x^{p-1-k_0} \prod_{j=1}^{r} \binom{p}{k_j} (x-\lambda_j)^{p-k_j} \right)
\end{aligned}$$

Budú nás zaujímať niektoré konkrétne hodnoty tejto derivácie, hlavne v bodoch $0, \lambda_1, \dots, \lambda_r$. Predpokladajme na chvíľu, že $\lambda_1, \dots, \lambda_r \in \mathbb{Z}$. Všimnime si, že hodnota $g^{(k)}(x)$ je po dosadení celého čísla tiež celé číslo, dokonca suma na pravej strane je celé číslo. Preto má význam hovoriť o deliteľnosti. Prvá a štvrtá rovnosť z 4.1 platia, pretože v každom sčítanci sa bude vyskytovať člen 0^D, kde $D > 0$. Jediný nenulový člen v druhej rovnosti je len

$(p-1)!\binom{p-1}{p-1}0^0\prod_{j=1}^{r}\binom{p-1}{0}(-\lambda_j)^{p-0}$. Špeciálne si kvôli tretej a piatej rovnosti ešte uvedomme, že $p! \mid k!$ pre $k \geq p$.

$$\begin{aligned} g^{(k)}(0) &= 0 \quad \forall\, k = 0, \dots p-2, \\ g^{(p-1)}(0) &= (p-1)! \prod_{j=1}^{r} (-\lambda_j)^p, \\ g^{(k)}(0) &= k!A \equiv 0 \pmod{p!} \quad \forall\, k \geq p, \text{ kde } A \in \mathbb{Z}, \\ g^{(k)}(\lambda_j) &= 0 \quad \forall\, k = 0, \dots p-1, \\ g^{(k)}(\lambda_j) &= k!B_j \equiv 0 \pmod{p!} \quad \forall\, k \geq p, \text{ kde } B_j \in \mathbb{Z}. \end{aligned} \tag{4.1}$$

Teraz už nebudeme predpokladať $\lambda_j \in \mathbb{Z}$, ale budeme predpokladať, že $h(x) = (x-\lambda_1)\dots(x-\lambda_r) \in \mathbb{Z}[x]$ (napríklad $h(x) = (x-\sqrt{2})(x+\sqrt{2}) = x^2 - 2$ je celočíselný polynóm, ale $\pm\sqrt{2}$ nie sú celé čísla). Všimnime si, že po roznásobení sa koeficienty tohto polynómu až na znamienko tvoria elementárne symetrické polynómy nad $\lambda_1, \dots, \lambda_r$. Chvíľu teda budeme λ_j považovať za premenné. Zrejme $g^{(k)}(0)$ aj $\sum_{j=1}^{r} g^{(k)}(\lambda_j)$ sú celočíselné symetrické polynómy v $\lambda_1, \dots, \lambda_r$. Potom podľa fundamentálnej vety o symetrických polynómoch ide o celočíselné polynómy v $e_{\lambda_1}, \dots, e_{\lambda_r}$, kde e_{λ_j} sú elementárne symetrické polynómy nad $\lambda_1, \dots, \lambda_r$. To sú však koeficienty polynómu $h(x)$, ktoré sú podľa predpokladu celé čísla. Teda aj $g^{(k)}(0)$ a $\sum_{j=1}^{r} g^{(k)}(\lambda_j)$ sú celé čísla. V tomto prípade môžeme teda písať

$$\begin{aligned} g^{(p-1)}(0) &= (p-1)! \prod_{j=1}^{r} (-\lambda_j)^p, \\ g^{(k)}(0) &\equiv 0 \pmod{p!} \quad \forall\, k \neq p-1, \\ \sum_{j=1}^{r} g^{(k)}(\lambda_j) &\equiv 0 \pmod{p!} \quad \forall\, k \in \mathbb{N}. \end{aligned} \tag{4.2}$$

Prvú rovnosť možno odôvodniť rovnako ako v 4.1. Druhá rovnosť vyplýva z faktu, že suma na pravej strane derivácie $g^{(k)}(0)$ je symetrická v $\lambda_1, \dots, \lambda_r$, a teda celé číslo. Tretia rovnosť platí z podobného dôvodu.

4.3 Transcendencia e

Čisto zo záujmových dôvodov uvedieme aj dôkaz transcendencie e. Z predchádzajúcej sekcie už totiž máme k dispozícii príslušný matematický aparát a samotný dôkaz je jednoduchšou verziou dôkazu transcendencie π, takže slúži aj k lepšiemu pochopeniu tohto dôkazu.

Veta 4.3.1. *e je transcendentné číslo.*

Dôkaz. Predpokladajme, že e je algebraické číslo. Potom existujú celé čísla $a_k \neq 0, a_{k-1}, \ldots, a_0$ také, že

$$a_k e^k + a_{k-1} e^{k-1} + \ldots + a_0 = 0 \tag{4.3}$$

Definujme

$$\begin{aligned} f(x) &= x^{p-1}(x-1)^p \ldots (x-k)^p \\ m &= \deg f = p - 1 + kp \\ J &= \sum_{j=0}^{k} a_j \, I_f(j) = \sum_{j=0}^{k} a_j \int_{\varphi_j} e^{j-u} f(u) \, \mathrm{d}u, \end{aligned}$$

kde krivka φ_j je úsečka $[0, j]$. Naviac podľa definície 4.2.1 máme

$$\bar{f}(x) = x^{p-1}(x+1)^p \ldots (x+n)^p$$

Použime teraz lemu 4.2.2 a rovnosť 4.3 a dostávame

$$\begin{aligned} J &= \sum_{j=0}^{k} a_j \left(e^j \sum_{i=0}^{m} f^{(i)}(0) - \sum_{i=0}^{m} f^{(i)}(j) \right) \\ &= \left(\sum_{i=0}^{m} f^{(i)}(0) \right) \left(\sum_{j=0}^{k} a_j e^j \right) - \sum_{j=0}^{k} \sum_{i=0}^{m} a_j f^{(i)}(j) \\ &= -\sum_{j=0}^{k} \sum_{i=0}^{m} a_j f^{(i)}(j) \end{aligned} \tag{4.4}$$

Podľa 4.1 je však

$$\begin{aligned} f^{(p-1)}(0) &= (p-1)!(-1)^p \ldots (-k)^p = (p-1)!(-1)^{kp}(k!)^p \\ f^{(i)}(j) &\equiv 0 \pmod{p!} \quad \text{ak } i \neq p-1 \text{ alebo } j \neq 0 \end{aligned} \tag{4.5}$$

Voľme teda p ako prvočíslo tak, aby $p > \max_{0\leq j\leq k}\{|a_j|, k\}$. Dosadením 4.5 do 4.4 dostaneme, že $(p-1)! \mid J$. Na druhej strane však platí $p \nmid f^{(p-1)}(0)$, teda aj $p \nmid J$, čiže $J \neq 0$. Z toho nám vyplýva

$$|J| \geq (p-1)!$$

Podľa lemy 4.2.3 ale máme

$$\begin{aligned}
|J| &\leq \sum_{j=0}^{k} |a_j|\,|I_f(j)| \leq \sum_{j=0}^{k} |a_j|\, je^j \bar{f}(j) \\
&\leq \left(\sum_{j=0}^{k} |a_j|\, je^j\right)(2k)^{p-1+kp} \\
&\leq \max_{0\leq j\leq k}\left\{|a_j|\, je^j\right\}\left((2k)^{k+1}\right)^p = BC^p,
\end{aligned}$$

kde B a C sú prirodzené čísla. Dolné a horné ohraničenia si však pre veľké p odporujú, čím sme dospeli k sporu. e je teda transcendentné číslo. □

4.4 Transcendencia π

Veta 4.4.1. *π je transcendentné číslo.*

Dôkaz. Pre spor predpokladajme, že π je algebraické. Keďže algebraické čísla tvoria teleso a i je algebraické, tak aj $i\pi$ je algebraické číslo. Označme teda $m_{i\pi} \in \mathbb{Q}[x]$ minimálny polynóm $i\pi$. Ak treba, vynásobme tento polynóm najmenším spoločným násobkom menovateľov jednotlivých koeficientov z $\mathbb{Q}$. Výsledný polynóm je už nad $\mathbb{Z}$ a označme ho $M_{i\pi}$. Korene sa nezmenili. Nech $M_{i\pi}$ je stupňa n. Potom má n komplexných koreňov $\alpha_1, \ldots, \alpha_n$, pričom $\alpha_1 = i\pi$. Takže $M_{i\pi} = a(x-\alpha_1)\ldots(x-\alpha_n)$, kde $a \in \mathbb{N}$. Definujme

$$\begin{aligned}
A &= \{\delta_1\alpha_1 + \ldots + \delta_n\alpha_n \mid \delta_j \in \{0,1\}\}, \\
B &= \{\beta \mid \beta \in A, \beta \neq 0\} = \{\beta_1, \ldots, \beta_k\},
\end{aligned}$$

pričom množinu A považujeme za množinu formálnych súčtov (teda ak aj $\alpha_1 = \alpha_2$, budeme tieto dva prvky považovať za rôzne). Zrejme $|A| = 2^n$ a

$1 \leq k \leq 2^n - 1$. Podľa Eulerovej formuly $e^{\alpha_1} = e^{i\pi} = -1$, takže

$$\begin{aligned} 0 &= (e^{\alpha_1} + 1)(e^{\alpha_2} + 1) \dots (e^{\alpha_n} + 1) \\ 0 &= \sum_{\gamma \in A} e^{\gamma} = \sum_{\gamma \in B} e^{\gamma} + \sum_{\gamma \in A \setminus B} e^{0} \\ 0 &= \sum_{j=1}^{k} e^{\beta_j} + 2^n - k \end{aligned} \tag{4.6}$$

Ešte definujme

$$\begin{aligned} f(x) &= a^{kp} x^{p-1} (x - \beta_1)^p \dots (x - \beta_k)^p \\ m &= \deg f = p - 1 + kp \\ J &= \sum_{j=1}^{k} I_f(\beta_j) = \sum_{j=1}^{k} \int_{\varphi_j} e^{\beta_j - u} f(u) \, \mathrm{d}u, \end{aligned}$$

kde krivka φ_j je úsečka $[0, \beta_j]$. Podľa definície 4.2.1 navyše

$$\bar{f}(x) = a^{kp} x^{p-1} (x + |\beta_1|)^p \dots (x + |\beta_k|)^p$$

Podľa lemy 4.2.2 a rovnosti 4.6 máme

$$\begin{aligned} J &= \sum_{j=1}^{k} \left(e^{\beta_j} \sum_{i=0}^{m} f^{(i)}(0) - \sum_{i=0}^{m} f^{(i)}(\beta_j) \right) \\ &= -(2^n - k) \sum_{i=0}^{m} f^{(i)}(0) - \sum_{i=0}^{m} \sum_{j=1}^{k} f^{(i)}(\beta_j) \end{aligned} \tag{4.7}$$

Nech $\{e_1, \dots, e_n\}$ tvorí množinu n elementárnych symetrických polynómov nad $\{\alpha_1, \dots, \alpha_n\}$. Potom, keďže $M_{i\pi} \in \mathbb{Z}[x]$, tak $ae_1, \dots, ae_n \in \mathbb{Z}$ - stačí polynóm $M_{i\pi}$ roznásobiť a $ae_1, \dots, ae_n \in \mathbb{Z}$ budú jeho koeficienty, tým pádom celé čísla.
Ďalej $h(x) = a^k(x - \beta_1) \dots (x - \beta_k) = (ax - a\beta_1) \dots (ax - a\beta_k) \in \mathbb{Z}[ax]$, pretože k elementárnych symetrických polynómov nad $\{a\beta_1, \dots, a\beta_k\}$ je symetrických nad $\{a\alpha_1, \dots, a\alpha_n\}$, a teda ide o polynómy nad $\{ae_1, \dots, ae_n\}$. Zrejme $f(x) = x^{p-1}(h(x))^p$.

Teda stačí použiť 4.2 a máme

$$f^{(p-1)}(0) = (p-1)! \prod_{j=1}^{k} (-a\beta_j)^p = (p-1)!\, a^{pk} \prod_{j=1}^{k} (-\beta_j)^p$$

$$f^{(i)}(0) \equiv 0 \pmod{p!} \qquad \forall i \neq p-1 \tag{4.8}$$

$$\sum_{j=1}^{k} f^{(i)}(\beta_j) \equiv 0 \pmod{p!}$$

Zvoľme teda p ako prvočíslo tak, aby $p > \max\left\{\left|a^k \beta_1 \dots \beta_k\right|, 2^n - k\right\}$. Dosaďme 4.8 do 4.7 a dostaneme $(p-1)! \mid J$. Zároveň však $p \nmid J$, lebo $p \nmid f^{(p-1)}(0)$. To znamená, že $J \neq 0$, a teda

$$|J| \geq (p-1)!$$

Na druhej strane ale podľa lemy 4.2.3

$$\begin{aligned}
|J| &\leq \sum_{j=1}^{k} |I_f(\beta_j)| \leq \sum_{j=1}^{k} |\beta_j|\, e^{|\beta_j|} \bar{f}(|\beta_j|) \\
&\leq k \max_{1\leq j\leq k} \left\{|\beta_j|\, e^{|\beta_j|}\right\} |a|^{kp} \left(2 \max_{1\leq j\leq k} \{|\beta_j|\}\right)^{p-1+kp} \\
&\leq k \max_{1\leq j\leq k} \left\{|\beta_j|\, e^{|\beta_j|}\right\} \left(\left(2\,|a| \max_{1\leq j\leq k} \{|\beta_j|\}\right)^{k+1}\right)^{p} \\
&= BC^p
\end{aligned}$$

kde B a C sú prirodzené čísla. Pre dostatočne veľké p si však tieto ohraničenia odporujú, čím sme dospeli ku sporu. □

Dôsledok 4.4.2. *Kvadratúra kruhu nie je pomocou euklidovskej konštrukcie vo všeobecnosti možná.*

Dôkaz. Predpokladajme, že $\sqrt{\pi}$ je konštruovateľné. Potom je aj algebraické. Keďže množina algebraických čísel tvorí teleso, tak aj číslo π by bolo algebraické. Avšak číslo π je v skutočnosti transcendentné. Teda $\sqrt{\pi}$ je transcendentné a podľa dôsledku 1.3.4 a nemôže ísť o konštruovateľné číslo, čo je spor. Takže $\sqrt{\pi}$ nie je konštruovateľné. □

Zoznam použitého značenia

$\lvert a\rvert$	absolútna hodnota čísla a
$\mathrm{Re}(a)$	reálna časť komplexného čísla a
$\lvert AB\rvert$	dĺžka úsečky AB
$\lvert\measuredangle AOB\rvert$	veľkosť uhla AOB
$\mathbb{N}$	množina prirodzených čísel
$\mathbb{Z}$	množina celých čísel
$\mathbb{Q}$	množina racionálnych čísel
$\bar{\mathbb{Q}}$	množina algebraických čísel
$\mathbb{R}$	množina reálnych čísel
$\mathbb{C}$	množina komplexných čísel
$\lvert A\rvert$	počet prvkov množiny A, mohutnosť množiny A
$a \in A$	prvok a patrí do množiny A
$a \notin A$	prvok a nepatrí do množiny A
$A \subseteq B$	A je podmnožinou B
$A \subsetneq B$	A je ostrou podmnožinou B
$A \cup B$	zjednotenie množín A a B
$A \setminus B$	množinový rozdiel množín A a B
$\sup_{a\in A} f(a)$	suprémum funkčných hodnôt cez množinu A
$a \mid b$	a delí b
$a \nmid b$	a nedelí b
$\mathrm{D}(a, b)$	najväčší spoločný deliteľ a a b
$a \equiv b \pmod p$	p delí $a - b$

$\operatorname{Ker}\phi$	jadro homomorfizmu ϕ
$\operatorname{Im}\phi$	obraz homomorfizmu ϕ
A/B	množina rozkladových tried A podľa B
$K[x_1, \ldots, x_n]$	množina polynómov n premenných nad telesom/okruhom K
$\operatorname{lc}(f)$	vedúci koeficient polynómu f
$\deg f$	stupeň polynómu f
$\int_\varphi f(z)\,\mathrm{d}z$	krivkový integrál funkcie f pozdĺž krivky φ
$\langle\varphi\rangle$	obraz krivky φ v $\mathbb{C}$
$L(\varphi)$	dĺžka krivky φ
f', $f^{(k)}$	prvá derivácia f, k-ta derivácia f

Literatúra

[1] Stewart, I.: *Odsud až do nekonečna*. Argo a Dokořán, Praha, 2006.

[2] Beckmann, P.: *Historie čísla* π. Academia, Praha, 1998.

[3] Allen, G. D.: *Lectures on the History of Mathematics*. Lecture notes. Cit. 16. 6. 2008. Dostupné na internete: <http://www.math.tamu.edu/∼don.allen/masters/>

[4] Courant, R. & Robbins, H.: *What is mathematics? An elementary approach to ideas and methods*. Oxford University Press, New York, 1958.

[5] Loy, J.: *Trisection of an Angle*. Cit. 16. 6. 2008. Dostupné na internete: <http://www.jimloy.com/geometry/trisect.htm>

[6] Fine, B. & Rosenberger, G.: *The Fundamental Theorem of Algebra*. Springer-Verlag, New York, 1997.

[7] Smith, D. E.: *The History and Transcendence of* π. In: Young, J. W. A.: *Monographs on Topics of Modern Mathematics Relevant to the Elementary Field*. Longmans Green and Co., New York, 1927.

[8] Hardy, G. H. & Wright, E. M.: *An Introduction to the Theory of Numbers: Fifth Edition*. Oxford University Press, New York, 1979.

[9] Filaseta, M.: *Transcendental Number Theory*. Lecture notes.

[10] *e and pi are transcendental*. Cit. 16. 6. 2008. Dostupné na internete: <http://homepage2.nifty.com/PAF00305/math_e/transcendental/transcendental.html>