Eötvös Loránd Tudományegyetem
Matematika Intézet

Schőn Tímea

Miért nem kör alakú a tó?

Magasabb fokú polinomok az elemi geometriában

BSc szakdolgozat

Témavezető: Szabó Csaba

ELTE Algebra és Számelmélet Tanszék

2016. Budapest

Köszönetnyilvánítás

Szeretném megköszönni Cserti József és Kaufmann Zoltán segítségét, akik a probléma fizikai megközelítéséhez adtak hasznos tanácsokat. Ötleteiknek, szemléletüknek köszönhetően lényegesen leegyszerűsödött a középiskolai példa megtalálásának folyamata.

Köszönettel tartozom általános- és középiskolai tanáraimnak, akik elindítottak a matematika felé vezető úton, továbbá egyetemi oktatóimnak, akik beavattak a rejtelmeibe. Mindannyian hozzájárultak ahhoz, hogy szilárdan kitartsak tanári ambícióim mellett.

Köszönöm a családomnak, akik a kezdetektől fogva támogattak. Köszönöm a barátaimnak, akiknek mindig volt hozzám néhány bíztató szava. Végül, de nem utolsó sorban szeretném megköszönni páromnak, hogy mindig szívesen gondolkozott velem a feladat megoldásán, és hogy tanácsaival segítette dolgozatom elkészülését.

Tartalomjegyzék

Bevezetés

Szakdolgozatom alapja egy elemi geometriai példa. A feladat, amelyből kiindultunk, a legtöbb diák számára ismert. Jancsi meg akarja látogatni Juliskát, de a lova szomjas, ezért le kell mennie a folyó partjára. Hol kell megitatnia Jancsinak a lovát, hogy a lehető legrövidebb úton érjen oda Juliskához?

A példa megoldása a tengelyes tükrözésben rejlik: Jancsi pontját tükrözzük a folyó egyenesére, ezt a tükrözött pontot össszekötjük Juliska pontjával, és ahol ez a szakasz metszi az egyenest, ott kell megitatni a lovat. Ez a tengelyes tükrözés tulajdonságaiból és a háromszög-egyenlőtlenségből egyszerűen következik.

A mi példánkban Jancsi egy tónál itatja meg a lovát. A tó kör alakú, Jancsi is és Juliska is rajta kívül helyezkedik el. A kérdés változatlan: hol kellene megitatni a lovat, hogy Jancsi a legrövidebb úton érjen oda Juliskához?

A dolgozat első felében a feladat megoldását keressük háromféle módszerrel. Az első módszer alapötletét évfolyamtársam, Kecskeméti Judit szakdolgozatából [2] merítettem. Ő végül az analízis segítségével oldotta meg a problémát, de abból kiindulva, hogy érintő ellipszist kell keresni, a koordinátageometriai meggondolás is hasznosnak bizonyult. Bár a kapott polinom meglehetősen bonyolult lett, nekem ez a kedvenc megoldási módszerem, mert nagyon hasonlít a középiskolában megoldott példákhoz, és mert a rezultáns-módszer megismerésével új utak nyíltak meg előttem a többváltozós egyenletrendszerek megoldása terén. Lévén, hogy fizika a minor szakom, akarva-akaratlanul is belegondoltam, mit jelent ez a probléma a fizika nyelvére lefordítva. A második és harmadik módszer egyik fő feltevése (melyet a 2.3 részben bizonyítunk) ezen a fizikai meggondoláson alapszik, a fény viselkedése ugyanis nagyon hasonlít matematikailag az itt felvázolt problémára.

A dolgozat második felében a megoldás geometriai szerkeszthetőségét vizsgáljuk. A szerkeszthetőség kérdésével és a Galois-elmélet alapjaival minden tanárszakos hallgató találkozik az algebra kurzus keretében. Azt azonban kevesen tudják, hogy a Galois-csoportokról tanultak hogyan segíthetnek a szerkeszthetőség kérdésének eldöntésében. Ennek bemutatása mellett célunk az is, hogy egy szép példát találjunk, melyről egy tehetséges középiskolás diák már meg tudja mutatni, hogy a megoldás nem szerkeszthető.

Manapság már az oktatásban is egyre gyakrabban nyúlnak tanárok a számítástechnika eszközeihez, sőt sok esetben meg is tanítják a diákoknak bizonyos matematikai programcsomagok használatát. Úgy gondolom, ez mindenképpen hasznos, hiszen, ha a hosszas számításokat elvégzi helyettünk a számítógép, több időnk van gondolkozni fontosabb példákon, illetve az eredmények értelmezésén. Ebben a szellemben a legtöbb bonyolultabb számolást a *Maple* program segítségével végeztem el. Minden alkalommal jeleztem, hogy épp milyen függvényeket használtam.

Személyes motváció

Általános- és középiskolában a geometria nem tartozott az erősségeim közé, általában nehezen vettem észre a szükséges összefüggéseket. Ezzel szemben algebrából mindig is a jobbak közé tartoztam, soha sem okozott gondot az ismeretlenekkel való számolás, sőt ezt kifejezetten élveztem. A koordinátageometria megismerésével kezdtem nyitni a geometria felé, végül az egyetemen értettem meg, mennyire közel áll egymáshoz a két terület. Témaválasztás előtt sokat gondolkoztam, hogy melyiket válasszam a kettő közül, ezért is örültem annyira, amikor Szabó Csaba ezt a feladatot ajánlotta. Hogy a szerkeszthetőség és a Galois-elmélet kapcsolatának elvi hátterét maradéktalanul megértsem, elvégeztem Hermann Péter absztrakt algebra kurzusát. Ez nem csak azért volt hasznos, mert nem teljesen egyedül kellett feldolgoznom a témakört, hanem erős absztrakt algebrai alapokat is adott, melyek addig sajnos hiányoztak. A téma kiválasztásakor és kidolgozásakor két fontos célom volt: fejlődni, és élvezni a munkát. Azt hiszem az eddig leírtak tükrében nyilvánvaló, hogy mindkettő megvalósult.

1. fejezet

Polinomok keresése

A szerkeszthetőség vizsgálatához először is egy polinomra van szükségünk. Célunk, hogy ez minél egyszerűbben kezelhető legyen, ezért megpróbáljuk több oldalról is megközelíteni a problémát. A továbbiakban különböző módszerekkel és paraméterezéssel keressük a megoldást. A szerkeszthetőség kérdését csak a következő fejezetben vizsgáljuk.

A feladatot – a rezultáns-módszert leszámítva – középiskolai eszközökkel és ötletekkel oldjuk meg. Magasabb fokú paraméteres egyenletrendszereket nehéz jól kezelni hagyományos módszerekkel. Erre jelent megoldást a rezultáns, mely két polinom közös gyökeinek meghatározására alkalmas. Hogy hogyan, arra a dolgozatban számos példát mutatunk majd.

1.0.1. Definíció. Tekintsük az $f = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_0$ és $g = b_m x^m + \ldots + b_0$ T test fölötti polinomokat. Legyen $\bar{T}$ egy alkalmas test, melyben f-nek n db gyöke van: $\alpha_1, \ldots, \alpha_n$, g-nek pedig m db gyöke: $\beta_1, \ldots, \beta_m$. Ekkor az f és g polinomok *rezultánsát* a következő kifejezés adja meg:

$$R(f,g) = a_n^m b_m^n \prod_{i=1}^{n}\prod_{j=1}^{m}(\alpha_i - \beta_j)$$

1.0.2. Állítás. *Legyen T test, valamint $f = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_0$ és $g = b_m x^m + \ldots + b_0$ úgy, hogy $f, g \in T[x]$. Legyen D egy $(m+n)\times(m+n)$-es mátrix determinánsa, amit következőképpen készítünk el: Az első sorba az $a_n, \ldots a_0$ együtthatókat írjuk, majd a sor végéig csupa nullát. A második sor első eleme nulla, majd jönnek az $a_n, \ldots a_0$ együtthatók, és megint csupa nulla. Ezt addig folytatjuk az f együtthatóival, amíg a_0 az utolsó oszlopba kerül. Ezután g együtthatóival megismételjük az eljárást. Ekkor $a_n \neq b_n \neq 0$ esetén, $D = R(f,g)$.*

Bizonyos jegyzetekben [1] az 1.0.2 állításban szereplő mátrix determinánsa szerepel definíciójaként, majd tétel mondja ki, hogy a rezultáns a polinomok gyökeivel kifejezhető. Ez természetesen csak módszertanilag tér el a mi bevezetésünktől, hiszen a két megfogalmazás ekvivalens. Mi

Kuros jegyzetét [3] vettük alapul, az ő definícióját használva ugyanis azonnal látszik a rezultáns legfontosabb tulajdonsága:

1.0.3. Állítás. *A T test fölötti $a_n x^n + \ldots + a_0$ és $b_n x^n + \ldots + b_0$ polinomok rezultánsa akkor és csak akkor nulla, ha a két polinomnak van közös gyöke $\bar{T}$-ben.*

Az 1.0.3 állítás segítségével tehát feltételt találhatunk arra, hogy a két polinomnak közös gyöke legyen, az 1.0.2 segítségével pedig ki is tudjuk számítani a rezultáns értékét. Bár láttuk, hogy az 1.0.2 állításban szereplő determináns csak akkor egyezik meg a rezultánssal, ha $a_n \neq b_n \neq 0$, a dolgozatban az így kiszámított kifejezéseket is $R(f, g)$-vel fogjuk jelölni, és mindig megvizsgáljuk, hogy mikor nem nullák a főegyütthatók.

Vegyük észre, hogy ha egy polinomról azt akarjuk eldönteni, hogy van-e többszörös gyöke, akkor ennek a polinomnak és formális deriváltjának érdemes a rezultánsát venni. A rezultánshoz szorosan kapcsolódó fogalom a diszkrimináns, melynek segítségével eldönthetővé válik, hogy egy polinomnak van-e többszörös gyöke.

1.0.4. Definíció. Legyen T test, az $f \in T[x]$ főegyütthatója c, ekkor az f polinom diszkriminánsának a következő kifejezést nevezzük:

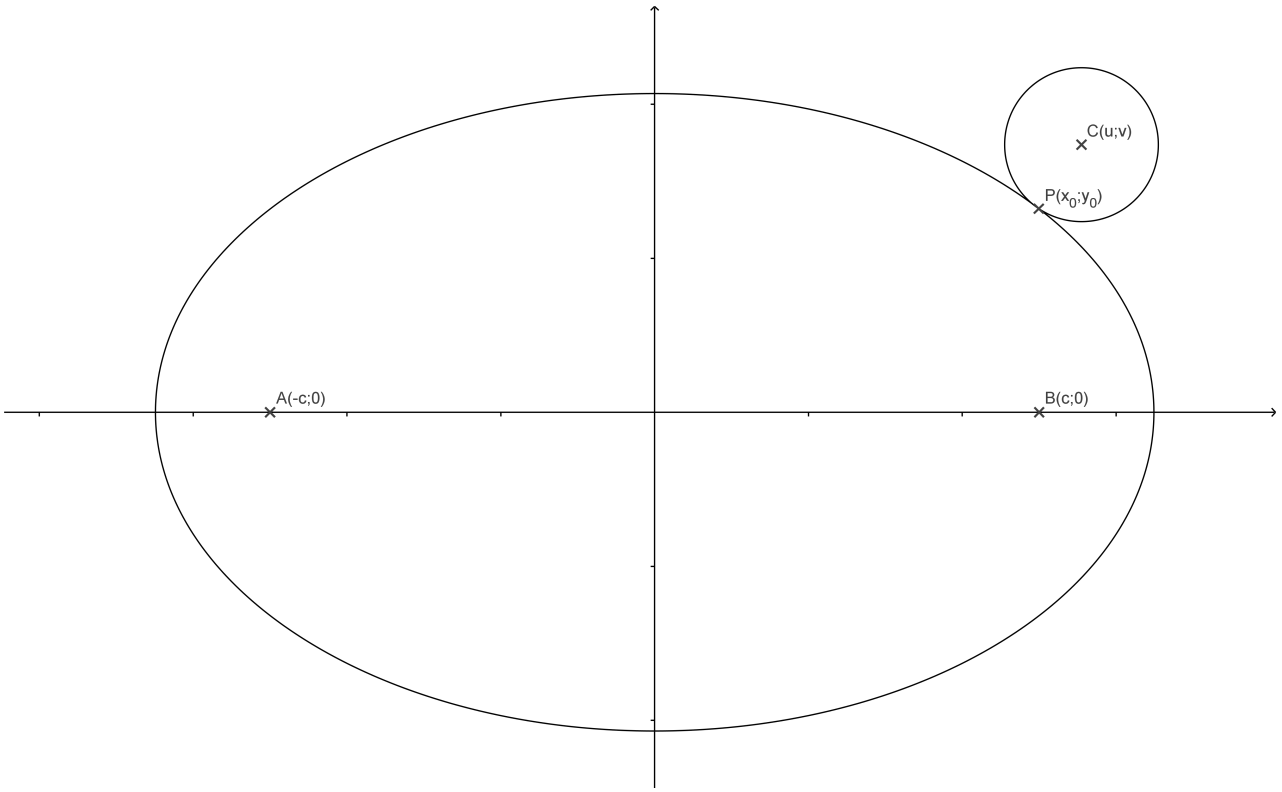
$$\frac{(-1)^{\frac{n(n-1)}{2}} R(f, f')}{c}$$

1.0.5. Állítás. *Egy T test fölötti polinomnak akkor és csak akkor 0 a diszkriminánsa, ha van többszörös gyöke egy alkalmas $T-$nél bővebb testben.*

A dolgozatban a diszkriminánst csak arra használjuk, hogy a többszörös gyökök létezésének feltételét vizsgáljuk. Erre természetesen a rezultáns is elegendő lenne. A diszkrimináns azonban többletinformációt nyújt akkor is, ha minden gyök egyszeres, ezért érdemes tisztában lenni ezzel a fogalommal is.

1.1. Megoldás ellipszis segítségével

Az ellipszis azon pontok halmaza a síkon, melyeknek a két adott fókuszponttól mért távolságösszegük állandó. Az ellipszisről emellett azt is tudjuk, hogy minden belső pontban a távolságösszeg kisebb ennél az állandónál, és minden külső pontban a távolságösszeg nagyobb nála. Ha tehát a két fókuszpontnak az A és B pontot választjuk, és az állandó értékét elkezdjük növelni, az ellipszisnek és a körnek eleinte nem lesz közös pontja, de aztán egy bizonyos érték esetén érinteni fogják egymást. Ebben az érintési pontban fogjuk a legrövidebb út során érinteni a kört.



1.1. ábra. Megoldás ellipszis segítségével

A fent leírtakat érdemes átfogalmazni a koordinátageometria nyelvére: adott egy $(u; v)$ középpontú kör és a rá nem illeszkedő A és B pontok. Keressük azt az ellipszist, mely kívülről érinti a kört, fókuszpontjai pedig $A(-c; 0)$ és $B(c; 0)$. Az ellipszis kanonikus helyzetű. Az állandó távolságösszeg jelölésére bevezetjük az a változót. A távolságösszeg ekkor $2a$ és természetesen $2a > 2c > 0$. A szokásos jelölésekkel $a^2 - b^2 = c^2$.

A kör sugara az általánosság megszorítása nélkül egynek vehető. A dolgozatban szögekről és távolságokról állapítjuk meg, hogy szerkeszthetőek-e. Ha tehát az elrendezésre most egy R-szeres nagyítást alkalmaznánk, akkor az 1-sugarú kör esetén megszerkeszthető hosszúságok és szögek R-sugarú kör esetén is megszerkeszthetőek lennének. Ennek oka, hogy a nagyítás hasonlósági transzformáció, tehát szögtartó, és aránytartó (vagyis bármelyik két szakasz hosszának aránya megegyezik képeik hosszának arányával).

Alakzatok egyenletei

Az $(u; v)$ középpontú egységnyi sugarú kör egyenlete:

$$(x - u)^2 + (y - v)^2 = 1 \tag{1.1}$$

Az ellipszis egyenlete:

$$\frac{x^2}{a^2} + \frac{y^2}{a^2 - c^2} = 1 \tag{1.2}$$

1.1.1. Az egyenletrendszer megoldása

Az érintési pont a körön és az ellipszisen is rajta van. A pont koordinátái így mindkét alakzat egyenletének gyökei. Rendezzük 0-ra mindkét egyenletet, végezzük el a négyzetre emeléseket, és szorozzunk a nevezőkkel:

$$0 = x^2 - 2ux + u^2 + y^2 - 2vy + v^2 - 1$$
$$0 = a^2x^2 - c^2x^2 + a^2y^2 - a^4 + a^2c^2$$

Ahhoz, hogy a rezultáns-módszert használni tudjuk, x hatványai szerint kell rendezni az egyenletet:

$$0 = x^2 - 2ux + u^2 + y^2 - 2vy + v^2 - 1$$
$$0 = (a^2 - c^2)x^2 + a^2(y^2 - a^2 + c^2)$$

Az ismeretlenek x, y, és a. Vezessük be az $f(x, y, a)$ és $g(x, y, a)$ polinomokat:

$$f(x, y, a) = x^2 - 2ux + u^2 + y^2 - 2vy + v^2 - 1$$
$$g(x, y, a) = (a^2 - c^2)x^2 + a^2(y^2 - a^2 + c^2)$$

Természetesen az első polinom nem függ a-tól, hiszen ez az ellipszis egy paramétere, a kör tőle független. Az egyenletrendszer megoldható a két polinom rezultánsának segítségével. Figyeljük meg, hogy a rezultáns definíciójában valamilyen T test fölötti polinomok szerepelnek, most viszont az együtthatók az y és az a polinomjai, az $f(x)$ és a $g(x)$ tehát gyűrű feletti polinomok. Tegyük fel, hogy $x = \alpha$, $y = \beta$ és $a = \gamma$, melyek egy alkalmas T-nél bővebb test elemei, az egyenletrendszer megoldásai. Ekkor $f(x, \beta, \gamma)$ és $g(x, \beta, \gamma)$ már $\bar{T}$ együtthatós egyváltozós polinomok, melyeknek α közös gyökük, így az $R(f(x), g(x))$ rezultáns, amely β és γ polinomiális kifejezése, nulla, tehát β és γ gyöke $R(f(x), g(x))$-nek. Ugyanakkor ha $R(f(x), g(x))(y, a)$-nak létezik β és γ megoldása, akkor a rezultáns nulla, azaz a két polinomnak vagy van közös gyöke, vagy mindkettő főegyütthatója nulla. Tekintsük tehát az $f(x)$ és $g(x)$ polinomokat. Ha most felírjuk a két polinom rezultánsát az x változóra, akkor feltételt kaphatunk arra, hogy a polinomoknak legyen közös gyökük:

$$R(f(x), g(x)) = \begin{vmatrix} 1 & -2u & u^2 + y^2 - 2vy + v^2 - 1 & 0 \\ 0 & 1 & -2u & u^2 + y^2 - 2vy + v^2 - 1 \\ (a^2 - c^2) & 0 & a^2(y^2 - a^2 + c^2) & 0 \\ 0 & (a^2 - c^2) & 0 & a^2(y^2 - a^2 + c^2) \end{vmatrix}$$

A *resultant* függvény a következő eredményt adta:

$$\begin{gathered}R(f(x),g(x)) = c^4y^4 + (4a^2c^2v - 4c^4v)y^3 + \\ +(-2a^4c^2 + 4a^4u^2 + 4a^4v^2 + 2a^2c^4 - 6a^2c^2u^2 - 10a^2c^2v^2 + 2c^4u^2 + 6c^4v^2 + 2a^2c^2 - 2c^4)y^2 + \\ +(-4a^6v + 8a^4c^2v - 4a^4u^2v - 4a^4v^3 - 4a^2c^4v + 8a^2c^2u^2v + 8a^2c^2v^3 - 4c^4u^2v - 4c^4v^3 + 4a^4v - 8a^2c^2v + 4c^4v)y + \\ +a^8 - 2a^6c^2 - 2a^6u^2 + 2a^6v^2 + a^4c^4 + 4a^4c^2u^2 - 4a^4c^2v^2 + a^4u^4 + 2a^4u^2v^2 + a^4v^4 - 2a^2c^4u^2 + \\ +2a^2c^4v^2 - 2a^2c^2u^4 - 4a^2c^2u^2v^2 - 2a^2c^2v^4 + c^4u^4 + 2c^4u^2v^2 + c^4v^4 - 2a^6 + 4a^4c^2 - 2a^4u^2 - 2a^4v^2 - 2a^2c^4 + \\ +4a^2c^2u^2 + 4a^2c^2v^2 - 2c^4u^2 - 2c^4v^2 + a^4 - 2a^2c^2 + c^4\end{gathered} \tag{1.3}$$

Látszik, hogy az $R(f(x), g(x))$ rezultáns már csak két változótól függ: y-tól és a-tól. Az így kapott kétváltozós polinom gyökeit meghatározva feltételt találhatunk arra, hogy az egyenletrendszernek legyen megoldása. Az $f(x)$ főegyütthatója 1, így ha a rezultáns 0, akkor az $f(x)$-nek és $g(x)$-nek van közös gyöke.

Ahhoz, hogy a két alakzatnak közös pontja legyen, nem elegendő, hogy f-nek és g-nek van közös gyöke x függvényében, az is kell, hogy az y változó függvényében legyen közös gyökük. Ha azt is szeretnénk, hogy ez a pont érintési pont legyen, akkor az kell, hogy pontosan egy valós gyöke legyen az $R(f,g)(y)$-nak. Ez akkor teljesül, ha a valós gyök négyszeres gyök, vagy akkor, ha kétszeres, és ezen kívül csak nem valós komplex gyökök vannak. Ha többszörös gyököket keresünk, az $R(f,g)$ diszkriminánsát érdemes meghatározni:

$$4096c^4(a-c)^6(a+c)^6a^4u^4g(a)$$

Itt $g(a)$ egy a^2-ben negyedfokú polinom, melynek együtthatói u, v és c többváltozós polinomjai. Azt fogom vizsgálni, hogy milyen esetekben lehet 0 a diszkrimináns.

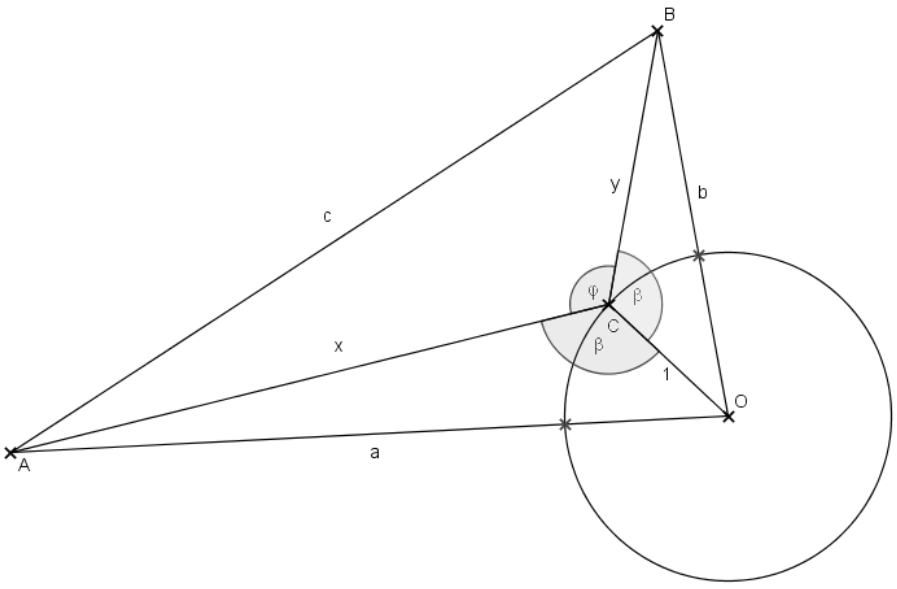
- Ha c^4 nulla lenne, az azt jelentené, hogy a fókusztávolság nulla, azaz Jancsi és Juliska ugyanott lennének. Ez egy elfajuló eset, ami kevésbé érdekes.
- Ha a^4 lenne nulla, akkor Jancsi vagy Juliska a kör egy pontja lenne, azaz már eleve a tó partján állna, ez is túlságosan leegyszerűsítené a problémát.
- Ha u^4 nulla, akkor a kör középpontja az y tengelyen van, mely az A és B pontok felezőmerőlegese. Ekkor a legrövidebb út mindig szerkeszthető: Jancsi a felező merőleges és a kör metszéspontjánál itatja meg a lovát.
- Ha $(a-c)^6(a+c)^6$ nulla volna, az azt jelentené, hogy $(a+c)(a-c) = 0$. Mivel feltettük azt, hogy a, $c > 0$, így $(a+c)$ nem lehet nulla. De $2a > 2c$-nek is teljesülnie kell, ezért $a \neq c$, tehát $a^2 - c^2$ mindig pozitív.

Ez azt jelenti, hogy a $g(a)$ polinom gyökeit kellene vizsgálni, ami túl bonyolultnak tűnik, így megpróbálunk egy ennél jobban kezelhető polinomot keresni.

1.2. Megoldás keresése a koszinusz-tétel segítségével

A fény adott közegben mindig úgy terjed, hogy a terjedési időnek szélsőértéke (általában minimuma) legyen. Ha feltételezzük, hogy közben végig azonos sebességgel (azaz változatlan közegben) halad, akkor ez a legrövidebb vagy leghosszabb utat jelenti. Fizikailag tehát a fenti probléma megfogalmazása a következő: adott egy pontszerű fényforrás (A), egy tőle különböző B pont, és egy gömbtükör. Hol verődik vissza a fény a gömbtükrön, hogy az A pontból érkező fénysugár átmenjen a B ponton? Szemléletesen azt gondoljuk, hogy az 1.2 ábra jelöléseinek megfelelően történnek a dolgok, vagyis az ott egyenlőnek jelölt β szögek valóban egyenlőek. Megtanultuk ugyanis a síktükör visszaverésénél, hogy a beesési szög és a felület normálisa által bezárt szög mindig megegyezik a normális és a visszaverődési szög által bezárt szöggel. Geometriai és fizikai szemléletünk alapján úgy érezzük, ez gömbtükör esetén is igaz. Szerencsére a fény terjedése ebben az esetben jól kezelhető matematikailag, deriválással egyszerűen beláthatjuk a szögek egyenlőségét, ezt a 2.3 részben meg is tesszük.

A megoldás során adottnak tekintjük az a, b és c értékeket; a kör sugarát az általánosság megszorítása nélkül 1-nek vehetjük. Az ismeretlenek x, y és $\cos\beta$.



1.2. ábra. Koszinusz-tételes megoldás

Koszinusz-tétel a háromszögekre.

$$a^2 = 1^2 + x^2 - 2x\cos\beta \tag{1.4}$$

$$b^2 = 1^2 + y^2 - 2y\cos\beta \tag{1.5}$$

$$c^2 = x^2 + y^2 - 2xy\cos\varphi \tag{1.6}$$

A $\cos\varphi$ értéke kifejezhető $\cos\beta$ segítségével, ugyanis $\cos\varphi = \cos(-2\beta)$. Mivel a koszinusz-függvény páros, $\cos(-2\beta) = \cos(2\beta)$. Az addíciós tétel miatt: $\cos(2\beta) = \cos^2\beta - \sin^2\beta$. A Pithagoraszi-azonosság alapján $\cos^2\beta + \sin^2\beta = 1$, tehát $\cos^2\beta - \sin^2\beta = 2\cos^2\beta - 1$, vagyis $\cos\varphi = 2\cos^2\beta - 1$. Eszerint az (1.6) összefüggés az alábbiak szerint módosul:

$$c^2 = x^2 + y^2 - 2xy(2\cos^2\beta - 1) \tag{1.7}$$

1.2.1. Megoldás x-re

A (1.4) egyenletből kifejezzük $\cos\beta$-t:

$$\cos\beta = \frac{x^2 + 1 - a^2}{2x}$$

A kapott értéket behelyettesítjük a (1.5) és (1.7) egyenletekbe:

$$b^2 = 1 + y^2 - 2y\frac{x^2 + 1 - a^2}{2x}$$
$$c^2 = x^2 + y^2 - 2xy\left(2\frac{(x^2 + 1 - a^2)^2}{4x^2} - 1\right)$$

Szorzunk a nevezőkkel, majd 0-ra rendezzük az egyenleteket:

$$0 = x + xy^2 - (x^2 + 1 - a^2)y - xb^2$$
$$0 = x^3 + xy^2 - y(x^2 + 1 - a^2)^2 + 2xy - xc^2$$

Hogy a rezultáns módszert használni tujdjuk, rendezzük y hatványai szerint a tagokat, és nevezzük el az így kapott polinomokat $f(x, y)$-nak és $g(x, y)$-nak:

$$f(x, y) = xy^2 - (x^2 + 1 - a^2)y + x - xb^2 \tag{1.8}$$

$$g(x, y) = xy^2 + (2a^2x^2 - x^4 - a^4 + 2a^2 - 1)y + x^3 - c^2x \tag{1.9}$$

Tekintsük most úgy, hogy az f és a g az y polinomjai, továbbá az $x = \alpha$ és $y = \beta$ ezek $\bar{T}$-beli közös gyökei. Ekkor ha felírjuk a két polinom $R(f(y), g(y))$ rezultánsát, úgy, hogy $x = \alpha$, akkor természetesen a $\bar{T}$-beli együtthatós $R(f(y), g(y)) = 0$, hiszen $f(y)$-nak és $g(y)$-nak közös gyöke β. Ez azt jelenti, hogy α gyöke az $R(f(y), g(y))(x)$ polinomnak. Ha most azt tesszük fel, hogy

az $R(f(y),g(y))(x)$ polinomnak létezik egy α gyöke, azaz $R(f(y),g(y))(\alpha)=0$, akkor $x=\alpha$ esetén vagy van közös gyöke a két polinomnak az y változóra, vagy $a_n=b_n=0$. Jelen esetben $a_n=b_n=x$, azaz $x=0$ esetén is nulla lesz a rezultáns. Ekkor azonban Jancsi a tó partján állna, és a feladat túl egyszerű volna.

Mindez azt jelenti, hogy az $R(f(y),g(y))(x)$ gyökeit meghatározva feltételt adhatunk az (1.8) és (1.9) egyenletből álló egyenletrendszer megoldhatóságára. A két polinom rezultánsa:

$$R(f,g)=\begin{vmatrix} x & -(x^2+1-a^2) & x-ab^2 & 0 \\ 0 & x & -(x^2+1-a^2) & x-ab^2 \\ x & (2a^2x^2-x^4-a^4+2a^2-1) & x^3-c^2x & 0 \\ 0 & x & (2a^2x^2-x^4-a^4+2a^2-1) & x^3-c^2x \end{vmatrix}$$

$R(f,g)$ értékére a *resultant* függvény a következőt adta:

$$\begin{gathered} R(f,g)=b^2x^{10}-(4a^2b^2-a^2+b^2+c^2)x^8- \\ -(-6a^4b^2+3a^4+a^2b^2-3a^2c^2+a^2+b^2-2c^2)x^6- \\ -(4a^6b^2-3a^6-5a^4b^2+3a^4c^2+3a^4-2a^2c^2+a^2+b^4-2b^2c^2-b^2+c^4+c^2)x^4- \\ -(-a^8b^2+a^8+3a^6b^2-6^6c^2-3a^6-3a^4b^2+2a^4c^2+3a^4+a^2b^2-a^2c^2-a^2)x^2 \end{gathered}$$

Látható, hogy a rezultáns értéke már csak x-től függ. Az x^2 minden tagból kiemelhető, ha leosztunk vele, egy új $h(x)$ polinomot kapunk:

$$\begin{gathered} h(x)=b^2x^8-(4a^2b^2-a^2+b^2+c^2)x^6- \\ -(-6a^4b^2+3a^4+a^2b^2-3a^2c^2+a^2+b^2-2c^2)x^4- \\ -(4a^6b^2-3a^6-5a^4b^2+3a^4c^2+3a^4-2a^2c^2+a^2+b^4-2b^2c^2-b^2+c^4+c^2)x^2+ \\ +a^8b^2-a^8-3a^6b^2+6^6c^2+3a^6+3a^4b^2-2a^4c^2-3a^4-a^2b^2+a^2c^2+a^2 \end{gathered}$$

A jobb áttekinthetőség érdekében vezessük be a $z=x^2$ változót:

$$\begin{gathered} h(z)=b^2z^4-(4a^2b^2-a^2+b^2+c^2)z^3- \\ -(-6a^4b^2+3a^4+a^2b^2-3a^2c^2+a^2+b^2-2c^2)z^2- \\ -(4a^6b^2-3a^6-5a^4b^2+3a^4c^2+3a^4-2a^2c^2+a^2+b^4-2b^2c^2-b^2+c^4+c^2)z+ \\ +a^8b^2-a^8-3a^6b^2+6^6c^2+3a^6+3a^4b^2-2a^4c^2-3a^4-a^2b^2+a^2c^2+a^2 \end{gathered} \tag{1.10}$$

Ez a polinom az előzőnél sokkal jobban kezelhető. Három paramétertől függ. Mivel ezek hosszúságok, a, b és c is pozitív valós számok.

1.2.1. Állítás. *Az x szám szerkeszthetősége ekvivalens a legrövidebb út szerkeszthetőségével.*

Bizonyítás. Természetesen, ha a legrövidebb út szerkeszthető, akkor x is szerkeszthető. Most tegyük fel, hogy x szerkeszthető. Bebizonyítjuk, hogy ekkor a legrövidebb út is szerkeszthető. Az A pontból x sugárral kört szerkesztünk. Ez két helyen fogja metszeni az eredetileg megadott kört. A legrövidebb út a kettő közül abban a pontban érinti a tavat, melyet összekötve a B ponttal, nem metszük el újra a kört. Ha megvan, hol kell Jancsinak érintenie a tavat, akkor a legrövidebb utat is megszerkeszthetjük. □

Ez azt jelenti, hogy (tekintettel arra, hogy z szerkeszthetősége ekvivalens x szerkeszthetőségével) z szerkeszthetőségét vizsgálva eldönthetjük, hogy a feladat megoldása szerkeszthető-e.

1.2.2. Megoldás $\cos\beta$-ra

Az előző megoldás után észrevettük, hogy máshogy megoldva az egyenletrendszert, az a-ban és a b-ben szimmetrikus egyenlethez jutnánk, melyek egyetemi tanulmányaink során gyakran bizonyultak hasznosnak. Ezért újra megoldjuk az (1.4), (1.5) és (1.7) egyenletekből álló egyenletrendszert. A megoldás során ismét polinomok rezultánsával dolgozunk. Rendezzük 0-ra az egyenleteket:

$$0 = 1^2 + x^2 - 2x - a^2\cos\beta \tag{1.11}$$

$$0 = 1^2 + y^2 - 2y - b^2\cos\beta \tag{1.12}$$

$$0 = x^2 + y^2 - 2xy - c^2(2\cos^2\beta - 1) \tag{1.13}$$

Három egyenletünk, és három változónk van. Az első egyenlet az y-tól nem függ, a második pedig az x-től. Láttuk, hogy a rezultáns-módszer két egyenletre működik jól. Csoportosítsuk az x hatványai szerint a 1.11 és 1.13 egyenleteket:

$$0 = x^2 - 2\cos(\beta)x + 1 - a^2$$
$$0 = x^2 - 2y(\cos^2(\beta) - 1)x + y^2 - c^2$$

Vezessük be az $f(x, y, \cos\beta)$ és a $h(x, y, \cos\beta)$ polinomokat:

$$f(x, y, \cos\beta) = x^2 - 2\cos(\beta)x + 1 - a^2$$
$$h(x, y, \cos\beta) = x^2 - 2y(\cos^2(\beta) - 1)x + y^2 - c^2$$

Ha x függvényében írjuk fel a két polinom rezultánsát, akkor, mint láttuk, az x változó kiküszöbölhető az egyenletekből.

$$R(f,h) = \begin{vmatrix} 1 & -2\cos(\beta) & 1-a^2 & 0 \\ 0 & 1 & -2\cos(\beta) & 1-a^2 \\ 1 & -2y(\cos^2(\beta)-1) & y^2-c^2 & 0 \\ 0 & 1 & -2y(\cos^2(\beta)-1) & y^2-c^2 \end{vmatrix}$$

A *resultant* függvénnyel kiszámítva a az eredmény:

$$R(f,h) = q(y,\cos\beta) = y^4 + (-8\cos^3\beta + 4\cos\beta)y^3 +$$
$$+(-16a^2\cos^4\beta - 16\cos^4\beta + 16a^2\cos^2\beta - 12\cos^2\beta - 2a^2 - 2c^2 + 2)y^2 +$$
$$+(8a^2cos^3\beta + 8c^2\cos^3\beta - 8\cos^3\beta - 4a^2\cos\beta - 4c^2\cos\beta + 4\cos\beta)y -$$
$$-4c^2\cos^2\beta + a^4 - 2a^2c^2 + c^4 + 1$$

A kapott $R(f,h)$ polinom már csak az y és $\cos\beta$ értékektől függ, ugyanúgy, ahogy a 1.9 kifejezés. Tekintsük a következő polinomokat:

$$g(y,\cos\beta) = y^2 - 2\cos(\beta)y + 1 - b^2 \tag{1.14}$$

$$\begin{aligned} R(f,h)(y,\cos\beta) &= y^4 + (-8\cos^3\beta + 4\cos\beta)y^3 + \\ &+(-16a^2\cos^4\beta - 16\cos^4\beta + 16a^2\cos^2\beta - 12\cos^2\beta - 2a^2 - 2c^2 + 2)y^2 + \\ &+(8a^2cos^3\beta + 8c^2\cos^3\beta - 8\cos^3\beta - 4a^2\cos\beta - 4c^2\cos\beta + 4\cos\beta)y - \\ &-4c^2\cos^2\beta + a^4 - 2a^2c^2 + c^4 + 1 \end{aligned} \tag{1.15}$$

Az eddigiekhez hasonlóan kiküszöböljük az y változót az $R(g,R(f,h))$ rezultánssal, melynek értékét *resultant* függvény adta:

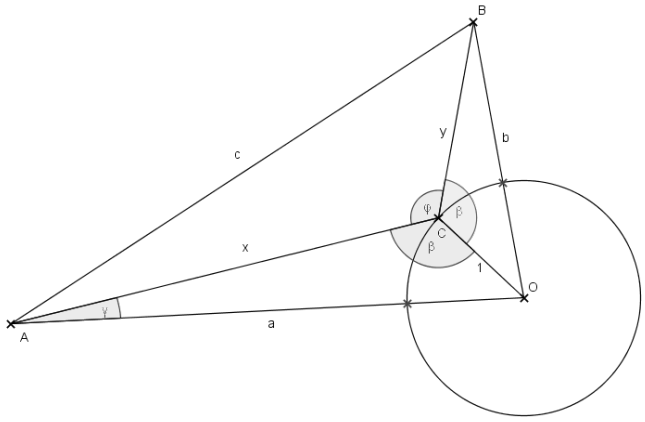
$$R(g,q) = \cos^8\beta(256a^4b^4 - 256a^4b^2 - 256a^2b^4 + 256a^2b^2c^2 + 256a^2b^2) +$$
$$+\cos^6\beta[(-64a^6 - 512a^4b^4 + 576a^4b^2 + 128a^4c^2 + 64a^4 + 576a^2b^4 + 384a^2b^2c^2) +$$
$$+(-64a^2c^2 - 640a^2b^2 - 64a^2c^4 - 64b^6 + 128b^4c^2 + 64b^4 - 64b^2c^4 - 64b^2c^2)] +$$
$$+\cos^4\beta[(32a^6b^2 + 112a^6 + 320a^4b^4 + 64a^4b^2c^2 - 368a^4b^2 - 208a^4c^2 - 128a^45) +$$
$$+(-32a^2b^6 + 64a^2b^4c^2 - 368a^2b^4 - 32a^2b^2c^4 + 32a^2b^2c^2 + 512a^2b^2 + 80a^2c^4 + 128a^2c^2) +$$
$$+(112b^6 - 208b^4c^2 - 128b^4 + 80b^2c^4 + 128b^2c^2 + 16c^6 + 16c^4)] +$$
$$+\cos^2\beta[(36a^6b^2 - 48a^6 - 64a^4b^4 - 64a^4b^2c^2 + 48a^4b^2 + 72a^4c^2) +$$
$$+(32a^2b^6 - 64a^2b^4c^2 + 48a^2b^4 + 32a^2b^2c^4 + 112a^2b^2c^2 - 48b^6 + 72b^4c^2 + 64b^4 - 24c^6 - 32c^4)] +$$
$$+a^8 - 4a^6b^2 - 4a^6c^2 + 6a^4b^4 + 4a^4b^2c^2 + 6a^4c^4 + 8a^4c^2 -$$
$$-a^2b^6 + a^2b^4c^2 + 4a^2b^2c^4 - 16a^2b^2c^2 - 4a^2c^6 - 16a^2c^4 +$$
$$+b^8 - 4b^6c^4 + 6b^4c^4 - 8b^4c^2 - 4b^2c^6 - 16b^2c^4 + c^8 + 16c^4$$

Hogy áttekinthetőbb legyen a polinom, bevezetjük a $\cos^2\beta = t$ helyettesítést:

$$\begin{aligned}
p(t) = t^4(256a^4b^4 - 256a^4b^2 - 256a^2b^4 + 256a^2b^2c^2 + 256a^2b^2)+\\
+t^3[(-64a^6 - 512a^4b^4 + 576a^4b^2 + 128a^4c^2 + 64a^4 + 576a^2b^4 + 384a^2b^2c^2)+\\
+(-64a^2c^2 - 640a^2b^2 - 64a^2c^4 - 64b^6 + 128b^4c^2 + 64b^4 - 64b^2c^4 - 64b^2c^2)]+\\
+t^2[(32a^6b^2 + 112a^6 + 320a^4b^4 + 64a^4b^2c^2 - 368a^4b^2 - 208a^4c^2 - 128a^4)+\\
+(-32a^2b^6 + 64a^2b^4c^2 - 368a^2b^4 - 32a^2b^2c^4 + 32a^2b^2c^2 + 512a^2b^2 + 80a^2c^4 + 128a^2c^2)+\\
+(112b^6 - 208b^4c^2 - 128b^4 + 80b^2c^4 + 128b^2c^2 + 16c^6 + 16c^4)]+\\
+t[(36a^6b^2 - 48a^6 - 64a^4b^4 - 64a^4b^2c^2 + 48a^4b^2 + 72a^4c^2 + 32a^2b^6 - 64a^2b^4c^2)+\\
+(48a^2b^4 + 32a^2b^2c^4 + 112a^2b^2c^2 - 48b^6 + 72b^4c^2 + 64b^4 - 24c^6 - 32c^4)]+\\
+a^8 - 4a^6b^2 - 4a^6c^2 + 6a^4b^4 + 4a^4b^2c^2 + 6a^4c^4 + 8a^4c^2 -\\
-a^2b^6 + a^2b^4c^2 + 4a^2b^2c^4 - 16a^2b^2c^2 - 4a^2c^6 - 16a^2c^4 +\\
+b^8 - 4b^6c^4 + 6b^4c^4 - 8b^4c^2 - 4b^2c^6 - 16b^2c^4 + c^8 + 16c^4
\end{aligned} \tag{1.16}$$

1.2.2. Állítás. *Az β szög szerkeszthetősége ekvivalens a legrövidebb út szerkeszthetőségével.*

Bizonyítás. Az nyilvánvaló, hogy ha a legrövideb út szerkeszthető, akkor β is. Érdekesebb kérdés, hogy ennek a megfordítása is igaz-e. Tegyük fel, hogy β szerkeszthető. Ekkor $\sin\beta$ is szerkeszthető, ugyanúgy, ahogy $\frac{\sin\beta}{a}$. A szinusz-tétel miatt $\frac{\sin\beta}{a} = \frac{\sin\gamma}{1}$. Ez azt jelenti, hogy $\sin\gamma$ is szerkeszthető. Ha $\sin\gamma$ szerkeszthető, akkor γ is szerkeszthető, ekkor pedig a legrövidebb út is. Ugyanis, ha az AO szakaszra az A csúcsnál felmérjük a γ szöget, akkor az így kapott szögszárral a kört elmetszve, megkapjuk azt a pontot, ahol Jancsinak érintenie kell a tavat. □

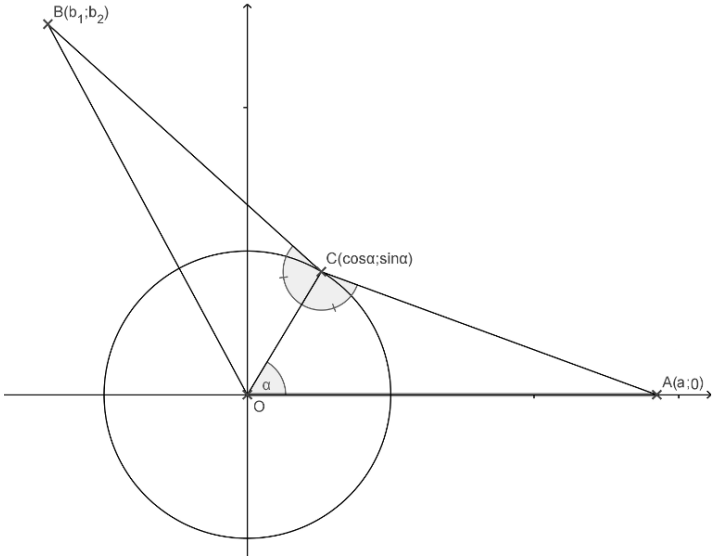


1.3. ábra. Ha β szerkeszthető, akkor a legrövidebb út is

Az így kapott polinom valóban szimmetrikus a-ban és b-ben, ezért kifejezhetnénk a szimmetrikus polinomok alaptételének segítségével az együtthatókat. Bár ez szép feladat lenne, megpróbálunk még egy ennél is egyszerűbb vagy jobban kezelhető polinomot keresni.

1.3. Megoldás keresése komplex számok segítségével

Az 1.4 ábrán láthatóak a használt jelölések. Ezek közül adottnak tekintjük az a, b_1, b_2 értékeket, a $\cos\alpha$ és a $\sin\alpha$ ismeretlenek, továbbá feltehetjük, hogy a kör origó középpontú egységkör. Az A, B és C a megfelelő komplex számokat jelölik.



1.4. ábra. Megoldás komplex számokkal

Egyenlő szögeket keresünk. Bár eddig a pontig még nem bizonyítottuk, $\frac{C-A}{C}$ szöge megegyezik $\frac{C}{C-B}$ szögével. Tudjuk, hogy a komplex számokat trigonometrikus alakjukkal felírva, két komplex szám hányadosának a szöge az osztandó és az osztó szögének különbsége. Ez azt is jelenti, hogy a $\frac{C-A}{C}$ komplex számot osztva a $\frac{C}{C-B}$ komplex számmal, a kapott $\frac{(A-C)(B-C)}{C^2}$ komplex szám szöge $0°$. Ekkor igaz a következő:

$$\frac{(A-C)(B-C)}{C^2} \in \mathbb{R}^+ \tag{1.17}$$

Sajnos az, hogy a két komplex szám hányadosának szöge $0°$, nem ekvivalens az előbbi állításunkkal. Ehelyett vegyük a $\frac{(A-C)(B-C)}{C^2} \in \mathbb{R}$ feltételt, mely viszont már az. Ekkor igaz a következő:

$$\operatorname{Im}\left(\frac{(A-C)(B-C)}{C^2}\right) = 0 \tag{1.18}$$

Felhasználva az adott paramétereinket, a következő egyenletet kell megoldanunk:

$$\operatorname{Im}\left(\frac{(a-\cos\alpha-i\sin\alpha)(b_1+b_2i-\cos\alpha-i\sin\alpha)}{(\cos\alpha+i\sin\alpha)^2}\right) = 0 \tag{1.19}$$

Az 1.19 egyenletet szorozva $1 = \frac{(\cos\alpha-i\sin\alpha)^2}{(\cos\alpha-i\sin\alpha)^2}$-nel, a nevezőből eltűnik i, így elegendő csak a számláló képzetes részével foglalkozni:

$$z = (a-\cos\alpha-i\sin\alpha)(b_1+b_2i-\cos\alpha-i\sin\alpha)(\cos\alpha-i\sin\alpha)^2$$

A fenti szorzatot az *expand* függvénnyel bontottuk fel, majd z képzetes részét vettük:

$$\begin{aligned}\mathrm{Im}(z) = a\sin^3\alpha - b_2\cos\alpha\sin^2\alpha - ab_2\sin^2\alpha + b_1\sin^3\alpha + \\ + ab_2\cos^2\alpha + a\sin\alpha\cos^2\alpha + b_1\sin\alpha\cos^2\alpha + 2ab_1\sin\alpha\cos\alpha - b_2\cos^3\alpha\end{aligned}$$

Ezen a *simplify(z,trig)* függvény segítségével további trigonometrikus átalakításokat hajtottunk végre:

$$\mathrm{Im}(z) = a\sin\alpha + b_1\sin\alpha + 2ab_1\cos\alpha\sin\alpha - ab_2 + 2ab_2\cos^2\alpha - b_2\cos\alpha = 0 \tag{1.20}$$

Az (1.20) egyenletben $\sin\alpha$ mindenütt maximum első hatványon szerepel, ezért kiemelhetjük:

$$ab_2 + b_2\cos\alpha - 2ab_2\cos^2\alpha = \sin\alpha(a + b_1 + 2ab_1\cos\alpha)$$

Négyzetre emelve az egyenletet, $\sin\alpha$ immár a második hatványon lesz:

$$b_2^2(a + \cos\alpha - 2a\cos^2\alpha)^2 = \sin^2\alpha(a + b_1 + 2ab_1\cos\alpha)^2$$

Ne feledjük, hogy a négyzetre emelés nem ekvivalens átalakítás, itt hamis gyökök keletkezhetnek! Az ismert összefüggés alapján $\sin^2\alpha = 1 - \cos^2\alpha$, ezt helyettesítve az előző egyenletbe:

$$b_2^2(a + \cos\alpha - 2a\cos^2\alpha)^2 = (1 - \cos^2\alpha)(a + b_1 + 2ab_1\cos\alpha)^2$$

A jobb áttekinthetőség érdekében vezessük be az $x = \cos\alpha$ helyettesítést. Az *expand* és *simplify* függvények segítségével 0-ra rendezzük az egyenletet, így megkapjuk a keresett polinomot:

$$\begin{aligned}f(x) = (4a^2b_1^2 + 4a^2b_2^2)x^4 + (4ab_1^2 + 4a^2b_1 + 4b_2^2a)x^3 - \\ -(4a^2b_1^2 + 4a^2b_2^2 - a^2 - 2ab_1 - b_1^2 - b_2^2)x^2 - \\ -(4a^2b_1 - 2b_2^2a + 4ab_1^2)x - a^2 - 2ab_1 - b_1^2 + b_2^2a^2\end{aligned} \tag{1.21}$$

Nyilvánvaló, hogy $\cos\alpha$ szerkeszthetősége ekvivalens a legrövidebb út szerkeszhetőségével, ezért elegendő az $f(x)$ polinom gyökeinek szerkeszthetőségét vizsgálni.

2. fejezet

Geometriai szerkeszthetőség

A geometria egy nagy kérdése, hogy milyen problémák szerkeszthetők körzővel és vonalzóval. Azt például a legtöbb középiskolás tudja, hogy 20°-os szöget nem tudunk szerkeszteni, azaz tetszőleges szöget nem tudunk harmadolni. Ennek bizonyítása azonban túl mutat a geometrián, és erősen támaszkodik absztrakt algebrai fogalmakra, állításokra, melyekkel minden tanárszakos hallgató megismerkedett harmadik félévben. Éppen ezért a legalapvetőbb fogalmakat nem részletezzük, csak azokat a definíciókat, állításokat mondjuk ki, melyek túlmutatnak az Algebra 3 tárgy tanagyagán. A fejezet elméleti háttere Hermann Péter kurzusa és jegyzete [4] nyomán íródott.

2.0.1. Definíció. Legyen $K \leq L$ test, és tegyük fel, hogy L tartalmazza egy nem nulla K[x]-beli $f \neq 0$ polinom összes gyökét (legyenek ezek $\alpha_1, \ldots, \alpha_n \in L$), ekkor a $K(\alpha_1, \ldots, \alpha_n)$ test az f polinom *felbontási teste K fölött.*

2.0.2. Állítás. *Minden $f \in K[x]$ polinomnak egyértelműen létezik felbontási teste K fölött.*

Egyetemi tanulmányaink során megtanultuk, hogy egy r szám akkor és csak akkor szerkeszthető, ha az alapadatok által generált testből másodfokú bővítések sorozatával eljuthatunk egy olyan testhez, mely tartalmazza r-t. Ennél azonban többet is mondhatunk. A következő állítás sokkal hasznosabb lesz munkánk során.

2.0.3. Állítás. *Legyen K_0 egy szerkesztési feladat alapadatai által generált test. Ekkor egy $r \in \mathbb{R}$ szám akkor és csak akkor szerkeszthető, ha az r szám K_0 fölötti minimálpolinomjának felbontási teste K_0-nak 2-hatványfokú bővítése.*

2.1. Polinomok Galois-csoportja

A Galois-csoport meghatározása segítségünkre lehet szerkesztési kérdések eldöntésében. A következőkben bemutatjuk a Galois-csoport néhány fontos tulajdonságát, majd ezeket a tu-

lajdonságokat felhasználva meghatározzuk bizonyos polinomok Galois-csoportját. Látni fogjuk, hogy ez már elegendő a szerkeszthetőség kérdésének megválaszolására.

A továbbiakban legyen f egy irreducibilis n-edfokú $K(\subseteq \mathbb{C})$ fölötti polinom, melynek K fölötti felbontási teste L. Ekkor:

1. A $K \leq L$ testbővítés foka megegyezik f Galois-csoportjának elemszámával.
2. Az f polinom Galois-csoportja az S_n permutációcsoport valamely részcsoportja.
3. Ha $K \leq L$ véges, akkor a polinom Galois-csoportját egy f fokával megegyező hosszúságú ciklus generálja.

2.1.1. Állítás. *Tegyük fel, hogy $f \in \mathbb{Z}[x]$, és p egy alkalmas prím, úgy, hogy f_{modp} polinomnak – melyet az f polinomból úgy tudunk előállítani, hogy együtthatóit modulo p vesszük – nincs többszörös gyöke a felbontási testében. Ekkor f_{modp} Galois-csoportja izomorf f Galois-csoportjának egy részcsoportjával.*

Az előző állításban feltétel, hogy a modulo p vizsgált polinomnak nem lehet többszörös gyöke. Ez azt jelenti, hogy a polinom rezultánsa modulo p nem lehet nulla, azaz f rezultánsa nem lehet osztható p-vel.

A fenti állítások segítségével következtetéseket vonhatunk le polinomok Galois-csoportjáról. A Galois-csoport elemszáma megegyezik a felbontási test bővítésének fokával, így el tudjuk dönteni, hogy a szerkesztés elvégezhető-e.

Példa. Elegendő ismeretet szereztünk ahhoz, hogy a negyedfokú polinomunk gyökeiről megállapíthassuk, hogy szerkeszthetőek-e. Mivel a komplex megoldás során kapott polinom tűnik a legyegyszerűbbnek, kezdjük ezzel a vizsgálódást. Az (1.21) polinomba konkrét értékeket helyettesítek. Legyen $a = 2$, $b_1 = 0$ és $b_2 = 3$. A vizsgált polinomunk ekkor:

$$f_1(z) = 144z^4 - 72z^3 - 131z^2 + 36z + 32$$

Ez irreducibilis, hiszen modulo 7 vizsgálva a $4z^4 + 5z^3 + 2z^2 + z + 4$ polinom irreducibilis. Ha $f_1(z)$ reducibilis volna, akkor modulo 7 is az volna.

A polinom diszkriminánsát a Maple program segítségével számítottuk ki. Értéke: $81977831424 = 2^{12} \cdot 3^2 \cdot 71 \cdot 31321$, ennek prímosztóival nem fogunk számolni.

Mivel modulo 7 vizsgálva $4z^4+5z^3+2z^2+z+4$ irreducibilis, a polinom felbontási testének foka osztható a polinom fokával, azaz néggyel. Ez azt jelenti, hogy a $\mathbb{Z}_7$ fölötti $f_{1_{\mathrm{mod}\,7}}$ polinom Galois-csoportjának elemszáma is osztható néggyel, így – tudván, hogy a Galois-csoport részcsoportja az eredeti polinom Galois-csoportjának – f_1 Galois-csoportjának elemszáma is osztható lesz néggyel.

Ha modulo 11 vizsgáljuk, f_1 két irreducibilis polinom szorzatára bomlik:

$$f_{1_{\mathrm{mod}11}}(z) = 10(z^3 + 2z^2 + 6z + 7)(z + 3)$$

Mivel z^3+2z^2+6z+7 irreducubilis $\mathbb{Z}_{11}$ fölött, $f_{1_{\mathrm{mod}11}}$ felbontási testének foka osztható hárommal, ily módon $f_{1_{\mathrm{mod}11}}$ Galois-csoportjának elemszáma is osztható hárommal. Azt is tudjuk, hogy $f_{1_{\mathrm{mod}11}}$ Galois-csoportja részcsoportja f Galois-csoportjának, f Galois-csoportjának elemszáma tehát szintén osztható hárommal.

Tudjuk, hogy f_1 Galois csoportja részcsoportja S_4-nek. Azt is beláttuk, hogy a Galois-csoport elemszáma osztható 3-mal és 4-gyel, osztható lesz tehát 12-vel is. S_4-nek csak két ilyen részcsoportja van, A_4 és önmaga. Ez már persze elegendő a szerkeszthetőség kérdésének megválaszolásához, hiszen így a felbontási test foka nem lehet 2-hatvány, de most már határozzuk meg a polinom Galois-csoportját! Tekintve, hogy $f_{1_{\mathrm{mod}7}}$ irreducubilis negyedfokú, a Galois-csoportot egy négyhosszú ciklus generálja. Erről tudjuk, hogy páratlan permutáció, így a Galois-csoport nem lehet A_4, ami a páros permutációk csoportja. Tehát az f_1 polinom Galois-csoportja az S_4.

2.2. Hamis gyök keresése

A polinomok Galois-csoportjának megállapítása igen elegáns, ám középsikolában aligha tárgyalható. Megpróbálunk tehát egy könnyebben emészthető módot találni a nem-szerkeszthetőség belátására. Sajnos ez nem túl egyszerű feladat, konsruktív módszerekel nem jutottunk eredményre, ezért úgy döntöttünk, olyan polinomokat keresünk, melyeknek van egy „szép” gyöke, hátha ezek után észreveszünk valamit. Ehhez megnézzük, hogyan lehet a polinomnak $1/2$ gyöke, majd igyekszünk olyan eseteket keresni, amikor ez egy hamis gyök. Ilyenkor a polinomunk $f(z) = (2z - 1)g(z)$ alakú ahol $g(z)$ harmadfokú és többnyire irreducibilis.

Helyettesítsünk be $z = \frac{1}{2}$-et a (1.21) polinomba:

$$f\left(\frac{1}{2}\right) = 0 = 3a^2b_1^2 - b_2^2a^2 + 6a^2b_1 + 6ab_1^2 - 2b_2^2a + 3a^2 + 6ab_1 - b_2^2 + 3b_1^2$$

Érdekes kérdés lehet, hogy hogyan viselkedik a polinom a függvényében, de helyettesítsünk be inkább konkrét értéket, legyen $a = 2$. Ez a polinom már csak b_1-től és b_2-től függ:

$$0 = \frac{27}{4}b_1^2 - \frac{9}{4}b_2^2 + 9b_1 + 3$$

Szorozzunk fel a nevezővel, hogy eltűnjenek a törtes együtthatók:

$$0 = 27b_1^2 - 9b_2^2 + 36b_1 + 12$$

Fejezzük ki b_2^2-et (szerencsére az eredeti polinom is mindig négyzetesen függ b_2-től, így minden a-ra hasonlóan járhatunk el):

$$b_2^2 = \frac{1}{9}(27b_1^2 + 36b_1 + 12)$$

Most „elfelejtjük", hogy $z = \frac{1}{2}$ megoldás, és visszahelyettesítjük f-be az előbb kiszámított b_2^2 értéket az $a = 2$ feltétellel:

$$\left(-16b_1^2 + \frac{16}{3}(2+3b_1)^2\right) z^4 + \left(16b_1 + 8b_1^2 - \frac{8}{3}(2+3b_1)^2\right) z^3 +$$
$$+ \left(4 + 4b_1 - 15b_1^2 - 5(2+3b_1)^2\right) z^2 +$$
$$+ \left(-16b_1 + \frac{4}{3}(2+3b_1)^2 - 8b_1^2\right) z - 4 - 4b_1 - b_1^2 + \frac{4}{3}(2+3b_1)^2$$

Ezután különböző b_1 értékekre faktorizáltuk a polinomot, bízva benne, hogy valamiféle hasonlóságot fedezünk fel bennük. Pl. $b_1 = 0 \Leftrightarrow b_2 = \frac{2}{3}\sqrt{3}$ esetén:

$$\frac{4}{3}(2z-1)(8z^3 - 6z - 1) \tag{2.1}$$

Ha $b_1 = \frac{1}{2} \Leftrightarrow b_2 = \frac{7}{6}\sqrt{3}$:

$$\frac{1}{12}(2z-1)(416z^3 + 72z^2 - 318z - 121)$$

Ha $b_1 = \frac{1}{3} \Leftrightarrow b_2 = \sqrt{3}$:

$$\frac{1}{9}(2z-1)(224z^3 + 32z^2 - 170z - 59)$$

Ha $b_1 = 1 \Leftrightarrow b_2 = \frac{5}{3}\sqrt{3}$:

$$\frac{1}{3}(2z-1)(224z^3 + 48z^2 - 174z - 73)$$

Ha $b_1 = 2 \Leftrightarrow b_2 = \frac{8}{3}\sqrt{3}$:

$$\frac{16}{3}(2z-1)(38z^3 + 9z^2 - 30z - 13)$$

Ha $b_1 = 500 \Leftrightarrow b_2 = \frac{1502}{3}\sqrt{3}$:

$$\frac{4}{3}(2z-1)(6012008z^3 + 1503000z^2 - 4884006z - 2067001)$$

Ha $b_1 = 599$ (prím) $\Leftrightarrow b_2 = \frac{1799}{3}\sqrt{3}$:

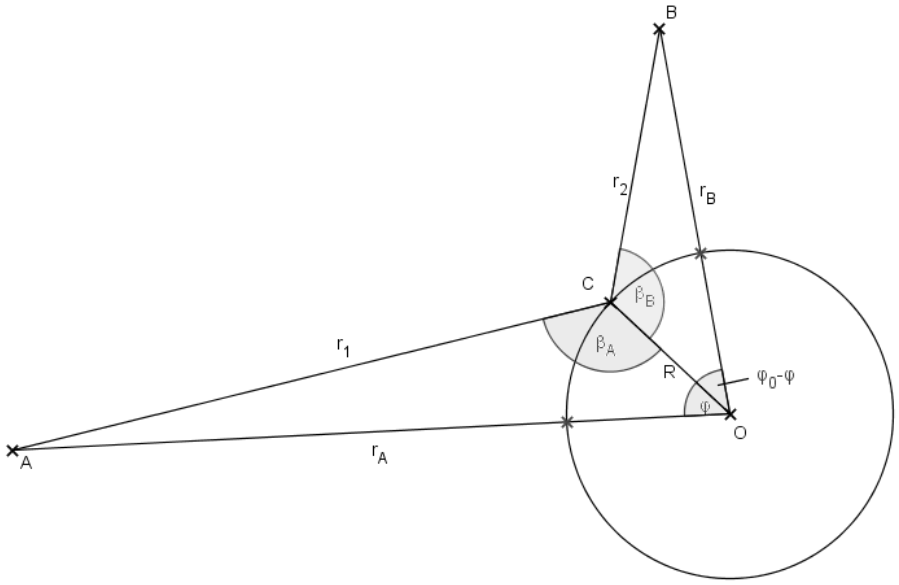
$$\frac{1}{3}(2z-1)(34502432z^3 + 8625600z^2 - 28029630z - 11862001)$$

Úgy tűnik, minden racionális a-ra és b_1-re egy elsőfokú és harmadfokú irreducibilis szorzatára bomlik a polinom, ha $z = \frac{1}{2}$ megoldás. Érdekes lenne megvizsgálni, hogy így van-e, de mi inkább gyakorlatban szeretnénk alkalmazni az eredményeinket. Ehhez vegyük alaposabban szemügyre a

$b_1 = 0$ esetet. Ekkor a harmadfokú tag $\cos 20$ minimálpolinomja. A használt paraméterezésben egyértelmű, hogy $z = \frac{1}{2}$ lesz a valós gyök. De vajon létezhet-e olyan paraméterezése, vagy megfogalmazása a feladatnak, ahol $\cos 20$ lesz a megoldás? Ha találnánk ilyet, akkor a példát már egy erősebb középsikolában is feladhatnánk, és könnyen be tudnánk látni, hogy a probléma nem megszerkeszthető.

2.3. Kísérlet középiskolai feladat gyártására

A dolgozat elején szerepelt egy állítás, melynek bizonyítását itt célszerű bemutatni.



2.1. ábra. A 2.3.1 állításhoz tartozó ábra

2.3.1. Állítás. *A fenti ábra jelöléseivel* $r_1 + r_2$ *akkor minimális, ha* $\sin \beta_A = \sin \beta_B$.

Bizonyítás. Írjuk fel a koszinusz-tételt a két háromszögre:

$$r_1 = \sqrt{R^2 + r_A^2 - 2Rr_A \cos \varphi}$$
$$r_2 = \sqrt{R^2 + r_B^2 - 2Rr_B \cos(\varphi_0 - \varphi)}$$

Az $r_1 + r_2$ távolságösszegnek akkor van szélsőértéke, ha $\frac{\partial}{\partial \varphi}(r_1 + r_2) = 0$. Azaz a következő egyenletet kell megoldanunk:

$$\frac{-2Rr_A \sin \varphi}{2\sqrt{R^2 + r_A^2 - 2Rr_A \cos \varphi}} + \frac{2Rr_B \sin(\varphi_0 - \varphi)}{2\sqrt{R^2 + r_B^2 - 2Rr_B \cos \varphi_0 - \varphi}} = 0$$

Vegyük észre, hogy a nevezőkben r_1 és r_2 szerepel!

$$\frac{r_B \sin(\varphi_0 - \varphi)}{r_2} = \frac{r_A \sin\varphi}{r_1}$$

Most használjuk a szinusz-tételt:

$$\begin{aligned} \frac{r_A}{r_1} &= \frac{\sin\beta_A}{\sin\varphi} \quad \rightarrow \quad \frac{r_A \sin\varphi}{r_1} = \sin\beta_A \\ \frac{r_B}{r_2} &= \frac{\sin\beta_B}{\sin(\varphi_0 - \varphi)} \quad \rightarrow \quad \frac{r_B \sin(\varphi_0 - \varphi)}{r_2} = \sin\beta_B \end{aligned}$$

Ez azt jelenti, hogy a derivált akkor és csak akkor lesz nulla, ha $\sin\beta_A = \sin\beta_B$ $\square$

Nézzük, mit jelent ez a feltétel! A $\sin\beta_A = \sin\beta_B$ egyenlőség akkor és csak akkor áll fenn, ha $\beta_A = \beta_B$ vagy ha $\beta_B = 180° - \beta_A$. Vegyük észre, hogy az 1.3 részben tárgyalt megoldásban is éppen ilyen gyököket keresünk. 1.17 ugyanis nem csak akkor teljesül, ha a $\frac{(A-C)(B-C)}{C^2}$ komplex szám szöge 0°, hanem akkor is, ha 180°. Ez azt jeleni hogy az $\frac{(A-C)}{C}$ és a $\frac{C}{(B-C)}$ komplex szám szögének különbsége 180°. Figyeljük meg, a komplex számok segítségével való megoldás és az előző levezetés során a szögek irányítását! Az α_A szög megegyezik $\frac{C}{(B-C)}$ szögével, α_B szögének irányítása azonban ellentétes $\frac{(A-C)}{C}$ szögével. Ez azt jelenti, hogy ha a komplex számok segítségével való megoldás során ugyanúgy irányítanánk a szögeket, mint az előző levezetésben, akkor itt is az $\arg\left[\frac{(A-C)}{C}\right] + \arg\left[\frac{C}{(B-C)}\right] = 180°$ feltételt kapnánk. Tehát a negyedfokú polinom lehetséges gyökei között kell keresnünk a legrövidebb és leghosszabb utak során érintett pontokhoz tartozó szögeket.

Ezek után nézzük meg megint a 2.1 polinomot! Arra vagyunk kíváncsiak, hogy milyen szögek esetén teljesül a $8\cos^3\alpha - 6\cos\alpha - 1 = 0$ összefüggés. Ehhez gondoljunk bele, hogy annak idején a $\cos 3\alpha = \frac{1}{2}$ egyenletből kiindulva, ekvivalens átalakításokat végezve kaptuk $\cos 20$ minimálpolinomját. Ez azt jelenti, hogy $8\cos^3\alpha - 6\cos\alpha - 1 = 0$ azon szögek esetén lesz igaz, melyek megoldásai a $\cos 3\alpha = \frac{1}{2}$ trigonometrikus egyenletnek:

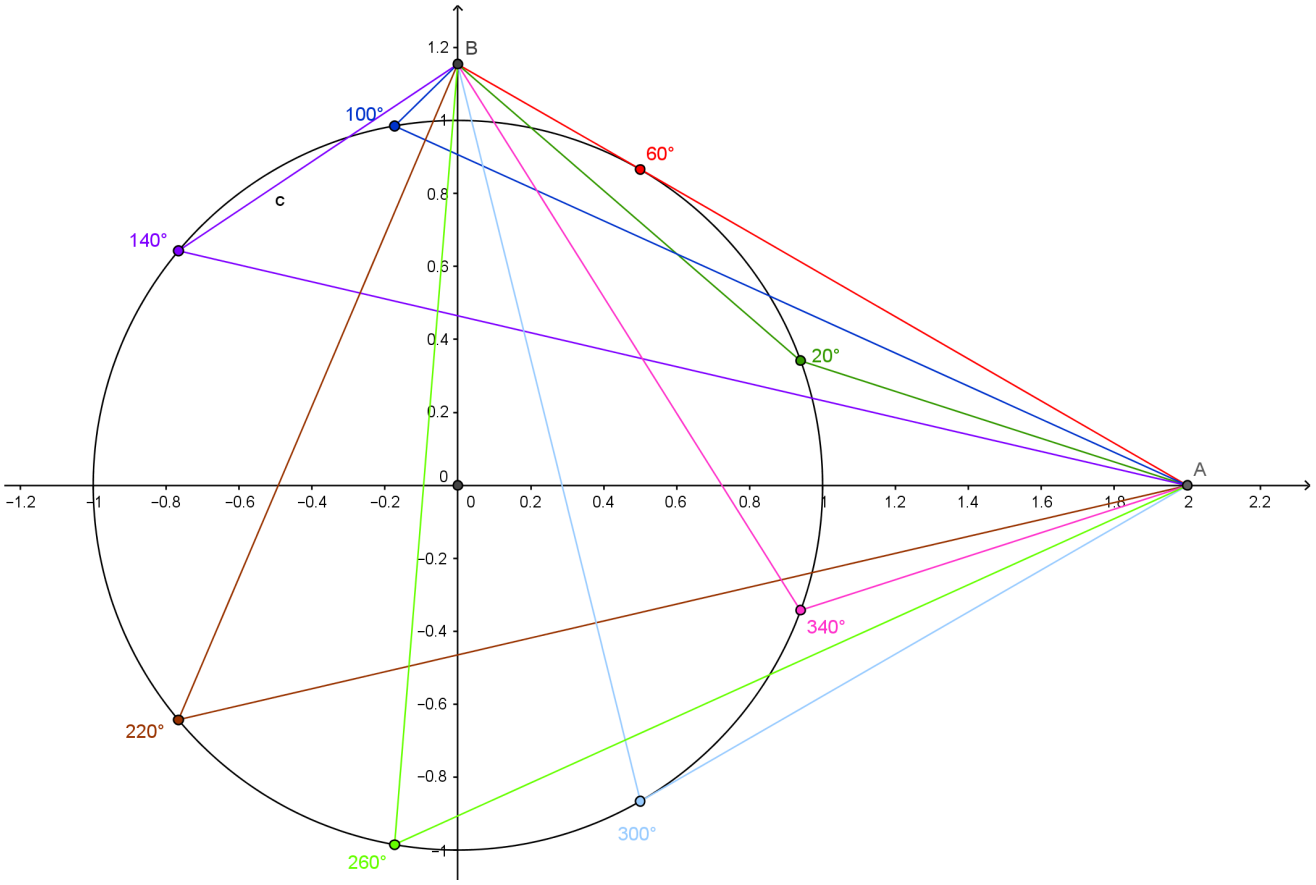
$$\begin{aligned} 3\alpha &= 60° + k \cdot 180°, \text{ ahol } k \in \mathbb{Z} \\ \alpha &= 20° + k \cdot 120°, \end{aligned}$$

vagy

$$\begin{aligned} 3\alpha &= 300° + l \cdot 180° \text{ ahol } l \in \mathbb{Z} \\ \alpha &= 100° + l \cdot 120° \end{aligned}$$

A koszinusz függvény periodicitása miatt elegendő a $[0°, 360°]$ intervallumon keresni a megoldásokat: $\alpha_1 = 20°$, $\alpha_2 = 100°$, $\alpha_3 = 140°$, $\alpha_4 = 220°$, $\alpha_5 = 260°$, $\alpha_6 = 340°$. Ne feledjük el, hogy

a 2.1 polinom akkor is nulla, ha $z = \cos\alpha = \frac{1}{2}$, így tehát az $\alpha_7 = 60°$ és $\alpha_8 = 300°$ eseteket is meg kell vizsgálni a szélsőértékek keresésekor. A 2.2 ábrán ezeket a szögek és a tavat ezeknél a szögeknél érintő utak láthatók.



2.2. ábra. A lehetséges legrövidebb és leghosszabb utak

Az ábrán látszik, de könnyen be is látható, hogy amikor $\alpha = 60°$, akkor az A-ból B-be vezető út a kör érintője. Ez egyben azt is jelenti, hogy nincs más olyan útvonal, amin Jancsi szárazföldön el tud jutni a tavat érintve Juliskához. Nyilvánvaló, hogy ha $\alpha \in [60°, 300°]$, akkor Jancsi már azelőtt érinti a tópartot, hogy a α-hoz tartozó kerületi pontot elérné. Ha $\alpha \in [300°, 60°]$, akkor nem tud úgy eljutni Juliskához, hogy ne kelljen átgázolnia a tavon, ugyanis ekkor $\alpha \in [60°, 120°]$. Ráadásul a háromszög-egyenlőtlenség miatt az érintő lesz a legrövidebb út, ami azt jelenti, hogy a kérdést módosítani kell, ha azt szeretnénk, hogy az $\alpha_1, \ldots \alpha_6$ valamelyike legyen a keresett megoldás. Számoljuk ki tehát, hogy melyik útvonal a leghosszabb, ezután majd ehhez igazítjuk a feladat szövegét.

Az nyilvánvaló, hogy nem a 20°-hoz és a 340°-hoz tartozó útvonalak a leghosszabbak, mert náluk hosszabb a 300°-on átmenő út. Az is világos, hogy nem a 100°-hoz tartozó út a leghosszabb, mert a 140°-nál érintő út ennél hosszabb. Ennél ugyanakkor hosszabb a 220°-os

szöget érintő út. Ez azt jelenti, hogy csak a 220°, 260° és a 300∘ szögeket érintő utak hosszát kell kiszámítani.

A 300°-hoz tartozó út hossza:

$$r_{300} = \sqrt{(2-\cos 60°)^2 + \sin^2 60°} + \sqrt{\cos^2 60° + \left(\frac{2}{3}\sqrt{3} + \sin 60°\right)^2}$$

$$r_{300} = \sqrt{\left(2-\frac{1}{2}\right)^2 + \frac{3}{4}} + \sqrt{\frac{1}{4} + \left(\frac{2}{3}\sqrt{3} + \frac{\sqrt{3}}{2}\right)^2}$$

$$r_{300} = \sqrt{3} + \sqrt{\frac{1}{4} + \left(\frac{2}{3}\sqrt{3} + \frac{\sqrt{3}}{2}\right)^2}$$

$$r_{300} = \sqrt{3} + \sqrt{\frac{13}{3}} = \sqrt{3}\left(1 + \frac{\sqrt{13}}{3}\right) \approx 3,81$$

A 260°-nál érintő út hossza:

$$r_{260} = \sqrt{(2+\cos 10°)^2 + \sin^2 10°} + \sqrt{\cos^2 10° + \left(\frac{2}{3}\sqrt{3} + \sin 10°\right)^2}$$

$$r_{260} = \sqrt{4 + 4\cos 10° + \cos^2 10° + 1 - \cos^2 10°} + \sqrt{1 - \sin^2 10° + \frac{4}{3} + \frac{4}{3}\sqrt{3}\sin 10° + \sin^2 10°}$$

$$r_{260} = \sqrt{5 + 4\cos 10°} + \sqrt{\frac{7}{3} + \frac{4}{3}\sqrt{3}\sin 10°} \approx 4,54$$

A 220°-os szöghöz tartozó út hossza:

$$r_{220} = \sqrt{(2+\cos 40°)^2 + \sin^2 40°} + \sqrt{\cos^2 40° + \left(\frac{2}{3}\sqrt{3} + \sin 40°\right)^2}$$

$$r_{220} = \sqrt{4 + 4\cos 40° + \cos^2 40° + 1 - \cos^2 40°} + \sqrt{1 - \sin^2 40° + \frac{4}{3} + \frac{4}{3}\sqrt{3}\sin 40° + \sin^2 40°}$$

$$r_{220} = \sqrt{5 + 4\cos 40°} + \sqrt{\frac{7}{3} + \frac{4}{3}\sqrt{3}\sin 40°} \approx 4,79$$

A fentiek azt jelentik, hogy r_{220} a leghosszabb út, amelyről azonnal látszik, hogy a probléma ekvivalens a 40° szerkeszthetőségével. Sőt, mivel tudunk szöget felezni, ekvivalens a 20° szerkeszthetőségével is. Erről pedig a legtöbb iskolában bizonyítás nélkül megtanítják, hogy nem szerkeszthető.

Most megszerzett tudásunk birtokában, adjunk fel az eredeti példánk helyett egy másikat: Piripócson triatlon versenyt rendeznek speciális szabályokkal: A sorrend itt biciklizés, futás, úszás. A kör alakú tó partján valahol elhelyeznek egy jelölő bóját. A starttól a bójáig és a bójától a célig kijelölnek egy-egy egyenes szakaszt, ezeken a szakaszon folyik a verseny. A versenyzőknek az első szárazföldi szakaszon biciklivel kell megtenni a távot, a tóban úszni kell,

a második szárazföldi távon pedig futniuk kell. A triatlonosok híresek erőnlétükről, ezért minél hosszabb szakaszt szeretnénk kijelölni. Hol helyezzük el a bóját a tó partján, hogy a lehető leghosszabb versenytávot kelljen teljesíteniük?

Mint láttuk, az így kapott feladat elemi úton még nem megoldható, szükség van hozzá $\cos 20$ minimálpolinomjára, ily módon a minimálpolinom fogalmára és rengeteg alapozó ismeretre. Előfordulhat, hogy van egy olyan szép paraméterezés, amin középiskolások számára is azonnal látszik a megoldás, sajnos ezt mi most nem találtuk meg.

Irodalomjegyzék

[1] Kiss Emil, *Bevezetés az algebrába*, Typotex, (2007) 3

[2] Kecskeméti Judit, *Többváltozós szélsőérték keresés korlátos halmazokon*, Szakdolgozat, (2015) 1

[3] A. G. Kuros, *Felsőbb algebra*, Tankönyvkiadó, (1967) 4

[4] Hermann Péter, *Field Extensions*, Egyetemi előadásjegyzet 16