Eötvös Loránd Tudományegyetem
Természettudományi Kar

Kis teljes ívek

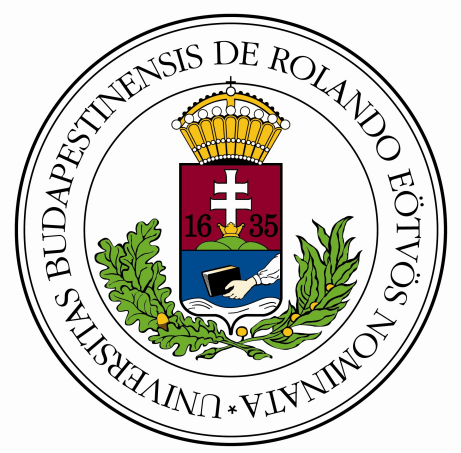
Khayouti Ádám

Témavezető:

Szőnyi Tamás, egyetemi tanár

BSc Szakdolgozat

Számítógéptudományi Tanszék



Budapest, 2023

Köszönetnyilvánítás

Ezt a részt azoknak szánom, akik a dolgozat írása közben mellettem álltak, segítettek. Mindenkinek köszönöm ezúton is!

Nagyon sok ember támogatott a szakdolgozat készítése közben, mind lelkiekben, mind szakmailag. Közülük első helyen a témavezetőm, Szőnyi Tamás áll, ő mindkét halmazban benne volt erősen, és végig segített a haladásban; türelme, segítőkészsége, ösztönző eszközei nélkül nem jöhetett volna létre e dolgozat, és nem találkoztam volna ezzel a témával sem, ami bár elméleti, mégis megfogott egy ilyen alkalmazás irányultságú egyént is. Hálásan köszönöm minden hozzájárulását!

Valamint szeretném még külön megköszönni a családtagjaimnak a biztatást, nővéremnek a dolgozat átolvasását, szaktársaimnak (A-K) a Latexben való segítséget, és barátaimnak, hogy velem együtt szurkoltak az elkészüléséért.

Tartalomjegyzék

Bevezetés, jelölések

A véges geometria olyan része a matematikának, amely véges számú pontból és egyenesből álló geometriákkal foglalkozik. Ez a szakdolgozat is erre a témára fog épülni. Először a projektív és affin síkokról lesz szó, majd egy kis véges testekről tanult ismeretekkel bővülve felépítjük a véges testeken alapuló projektív síkokat is. Ezután átvesszük az ívekről szóló fontosabb definíciókat és tételeket, majd a síkgörbékkel kezdünk foglalkozni, végül konstrukciókat nézünk kis teljes ívekre, valamint kitekintést nyújtunk a témában elért jelentősebb eredményekre a közeli s a távolabbi múltból is.

Jelölések:

AB : A és B pontok összekötő egyenese

$e \cap f$: e és f egyenesek metszéspontja

$\mathbb{K}$: tetszőleges test

$\mathbb{F}_q$: q elemű véges test

PG(2,q) : q-adrendű véges projektív sík

AG(2,q) : q-adrendű véges affin sík

1. Előkészületek

1.1. A projektív sík definíciója

Először definiáljuk a projektív síkot, majd az affin síkot, és ezek elemeinek számáról nézünk tételeket. [2] [6]

1.1.1. Definíció. A projektív síkgeometriában vannak pontok, egyenesek és köztük egy illeszkedési reláció. Ahhoz, hogy valamit projektív síknak nevezzünk, ki kell elégítenie bizonyos illeszkedési axiómákat, amik a következőek:

(a) Tetszőleges két különböző ponthoz pontosan egy egyenes tartozik, amire illeszkedik mindkét pont.

(b) Tetszőleges két különböző egyeneshez pontosan egy pont tartozik, ami illeszkedik mindkét egyenesre.

(c) Minden egyenesre legalább három pont illeszkedik.

(d) Minden ponton legalább három egyenes megy át.

Itt a (b)-ben megfogalmazott "pontosan egy" kifejezés csak az elsőhöz való hasonlóságot hivatott kifejezni(a pont és egyenes szerepének felcserélhetősége), mivel abból már következik, hogy két egyenesre csak legfeljebb 1 közös pont létezik.

Gyakran szerepel a (c) és (d) axióma helyett egy másik, ezekkel ekvivalens: Létezik négy pont, hogy semelyik 3 nincs egy egyenesen.

Tehát a klasszikus projektív geometriában ismert dualitás elve az absztrakt projektív síkokon is érvényes. Egy sík duálisának azt hívjuk, amit úgy kapunk az eredetiből, hogy az eredeti sík egyenesei lesznek a duális síkon a pontok, valamint a pontok lesznek a duális egyenesei. Az illeszkedést pedig úgy definiáljuk, hogy a duális sík egy pontja akkor és csak akkor van rajta a duális sík egy egyenesén, ha az eredeti síkon a pontnak megfelelő egyenesre illeszkedik az egyenesnek megfelelő pont.

Mivel (a) és (b) valamint (c) és (d) axiómák egymás duálisai, ezért minden olyan állítás, ami ezek segítségével bizonyítható, igaz marad akkor is, ha vesszük a duálisát. Ezt sok helyen ki fogjuk használni.

1.1.2. Tétel. Ha a Π projektív síknak van olyan egyenese, amelyre $n+1$ pont illeszkedik, akkor

1. Π minden egyenesén $n+1$ pont van,

2. Π minden pontján át $n+1$ egyenes megy,

3. Π összesen n^2+n+1 pontot és ugyanennyi egyenest tartalmaz.

Bizonyítás. Jelöljük az $n+1$ pontot tartalmazó egyenest e-vel, a rajta lévő pontokat pedig $P_1, P_2, ..., P_{n+1}$-gyel. Ha Q olyan pont, amelyik nincs rajta az e egyenesen, akkor az (a) axióma miatt Q-t valamennyi P_i ponttal ($i = 1, 2, ..., n+1$) össze tudjuk kötni, s a QP_i egyenesek mind különbözők, mert Q nincs rajta e-n. Másrészt minden Q-n átmenő egyenes metszi e-t a (b) axióma miatt, s ez a metszéspont csak a P_i pontok valamelyike lehet, tehát Q-n át pontosan $n+1$ egyenes megy. Gondolatmenetünket dualizálva kapjuk, hogy ha van olyan E pont, amelyen át $n+1$ egyenes megy, akkor minden olyan egyenesen $n+1$ pont van, amelyik nem megy át E-n.

Ha f tetszőleges, e-től különböző egyenes, akkor (d) miatt az $e \cap f$ ponton át megy legalább egy e-től is és f-től is különböző egyenes, aminek (c) miatt van $e \cap f$-től különböző R pontja. Mivel R nincs rajta e-n, ezért rá $n+1$ egyenes illeszkedik. De R az f egyenesen sincs rajta, ezért f-re is $n+1$ pont illeszkedik, amivel állításunk első részét bebizonyítottuk.

Ha P a Π projektív sík tetszőleges pontja, akkor (c) és (d) miatt van a síknak rajta át nem menő egyenese. Ezen az egyenesen az előzőekben bizonyítottak miatt $n+1$ pont van, vagyis P-n át $n+1$ egyenes megy.

Az (a) axióma miatt a sík összes pontjának a számát megkapjuk, ha egy rögzített P ponttal összekötött pontokat megszámoljuk. Tudjuk, hogy P-n át $n+1$ egyenes megy, és ezek mindegyike P-n kívül még n darab pontot tartalmaz. Tehát a projektív sík pontjainak a száma $1+(n+1)n = n^2+n+1$. Ennek az állításnak a duálisa szerint a projektív sík egyeneseinek a száma is n^2+n+1. □

Ebből látszik, hogy ha egy projektív síkbeli egyenesen véges számú pont található, akkor minden egyenesén azonos számú pont van, és minden pontján át ugyanannyi egyenes megy. Innen ered a következő definíció:

1.1.3. Definíció. A Π projektív sík rendje n, ha Π-nek van olyan egyenese, amelyen $n+1$ pont van.

1.1.4. Definíció. Tekintsük a $(\mathcal{P}, \mathcal{E}, I)$ hármast, ahol $\mathcal{P}$ és $\mathcal{E}$ két diszjunkt halmaz, $\mathrm{I} \subset \mathcal{P} \times \mathcal{E}$ pedig egy reláció, ami az illeszkedést adja meg. Ezt *affin síknak* hívjuk akkor, ha megfelel a következő 4 axiómának:

(i) $\mathcal{P}$ bármely két egymástól különböző eleméhez pontosan egy olyan eleme van $\mathcal{E}$-nek, amely mindkettővel relációban áll.

(ii) Ha $\mathrm{H} \in \mathcal{P}$ nem áll relációban az $e \in \mathcal{E}$ elemmel, akkor $\mathcal{E}$-nek pontosan egy olyan eleme van, amely relációban áll P-vel, de nem áll relációban egyetlen olyan $\mathcal{P}$-beli elemmel sem, amely e-vel relációban áll.

(iii) $\mathcal{E}$ minden eleme legalább két különböző $\mathcal{P}$-beli elemmel áll relációban.

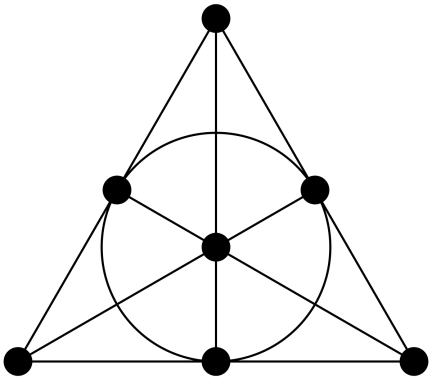
(iv) $\mathcal{P}$ minden eleme legalább három különböző $\mathcal{E}$-beli elemmel áll relációban.

Itt is szintén van hogy, (iii) és (iv) helyett egy másik velük ekvivalens szerepel:

(v) $\exists$ 3 pont, amik nincsenek egy egyenesen.

1.1.5. Definíció. Ha projektív vagy affin sík ponthalmaza véges, akkor véges projektív síknak, illetve véges affin síknak nevezzük.

1.1.6. Példa (Fano-sík)**.** Ezt a síkot csak 7 pont alkotja, amit könnyű egyszerűen elképzelni is: Vegyünk egy szabályos háromszöget, és ennek 7 pontját, amik a következők: a 3 csúcs, a 3 oldalfelező pont, és a háromszög súlypontja. A hét egyenes pedig a 3 oldala a háromszögnek, a 3 súlyvonala, és a beírt köre. Mindegyik egyenes alatt, a 7 pont közül azok halmazát kell érteni, amelyek illeszkednek rá.



1. ábra. : Fano-sík

1.1.7. Példa. Legyen $(\mathcal{P}', \mathcal{E}', I)$ egy affin sík. Nevezzük $\mathcal{E}$ két elemét párhuzamosnak, ha nincs közös pontjuk, vagy ha megegyeznek. A párhuzamosság ekvivalenciareláció, mert triviálisan reflexív és szimmetrikus, a tranzitivitás pedig az (ii) axiómából következik. Hívjuk az egyenesek ekvivalenciaosztályait ideális pontoknak, jelöljük ezek halmazát $\mathcal{P}_\infty$-nel, l_∞ pedig legyen egy $\mathcal{E}$-ben nem lévő új egyenes, amit ideális egyenesnek nevezünk. Ez pontosan az ideális pontokra illeszkedjék. A $(\mathcal{P}', \mathcal{E}', I)$ affin sík projektív lezártja a $(\mathcal{P}, \mathcal{E}, I)$ projektív sík, ahol $\mathcal{P} = \mathcal{P}' \cup \mathcal{P}_\infty$ és $\mathcal{E} = \mathcal{E}' \cup \{l_\infty\}$. Az ideális elemek illeszkedését ugyanúgy definiáljuk, mint amikor az euklidészi síkból a klasszikus projektív síkot elkészítjük: ideális pont egy affin síkbeli egyenesre akkor illeszkedik, ha az egyenes benne van az ideális pontnak megfelelő osztályban; az ideális egyenesre pedig minden ideális pont illeszkedik; affin síkbeli pont az ideális egyenesre sohasem illeszkedik.

Bármely affin sík projektív lezártja projektív sík. Az (a) és (b) axiómák teljesülését esetszétválasztással láthatjuk be. Két különböző affin ponthoz (i) miatt egyértelműen van olyan affin egyenes, ami összeköti őket, az ideális egyenes pedig nem illeszkedik affin pontokra. Egy affin és egy ideális ponthoz (ii) miatt egyértelműen létezik az ideális pont osztályába tartozó, az affin ponton átmenő egyenes, azaz a két pontot összekötő affin egyenes, az ideális egyenes pedig ebben az esetben sem megy át mindkét ponton. Két különböző ideális pontra viszont csak az ideális egyenes illeszkedik, mert egy affin egyenes az ideális pontoknak megfelelő osztályok közül pontosan egyhez tartozik. Tehát (a) axióma teljesül. Két különböző affin egyenes az affin síkon vagy párhuzamos, vagy metszi egymást. Az első esetben nincs közös affin pontjuk, viszont egy osztályba tartoznak, tehát egyértelműen létezik közös ideális pontjuk az ideális egyenesen. A második esetben egyértelműen létezik közös affin pontjuk, viszont különböző osztályokba tartoznak, ezért nincs közös ideális pontjuk. Végül egy affin egyenesnek és az ideális egyenesnek nincs közös affin pontja, viszont pontosan egy közös ideális pontjuk van, az affin egyenesnek megfelelő ideális pont. Ezért a (b) axióma is teljesül. A (c) és (d) axiómák pedig nyilvánvalóan teljesülnek.

Minden affin síknak egyértelműen létezik a projektív lezártja, ha viszont projektív síkból különböző egyeneseket hagyunk el, akkor a kapott affin síkok nem feltétlenül izomorfak.

(Izomorfizmus: Olyan bijekció, amely felcserélhető a műveletekkel. Például: ha φ

felcserélhető a műveletekkel, akkor

$$\forall a_1, a_2 \in A : \varphi(a_1 * a_2) = \varphi(a_1) \oplus \varphi(a_2)$$

Véges projektív vagy affin síkok esetén "művelet" helyett az I illeszkedési relációval való "felcserélhetőséget" kell megkövetelni, azaz P I $l \iff \varphi(P)$ I $\varphi(l)$.)

Ha az affin sík projektív lezártja n-edrendű projektív sík, akkor a 1.1.2 tételből azonnal adódik a következő tétel:

1.1.8. Tétel. Ha az $\mathcal{A}$ affin síknak van olyan egyenese, amelyre n pont illeszkedik, akkor

- $\mathcal{A}$ minden egyenesén n pont van.
- $\mathcal{A}$ minden pontján $n + 1$ egyenes megy át.
- $\mathcal{A}$ összesen n^2 pontot és $n^2 + n$ egyenest tartalmaz.

Az n számot az $\mathcal{A}$ affin sík rendjének nevezzük.

1.2. Véges testek feletti projektív terek

Ebben a fejezetben összefoglaljuk véges testekről tanultakat, valamint a későbbiekben használt állításokat bizonyítás nélkül [2], [4], [3].

1.2.1. Definíció. A test egy olyan $H = (T; +, \cdot)$, $H \neq \emptyset$ kétműveletes algebrai struktúrát jelöl, ahol T kommutatív csoportot alkot az összeadásra nézve, a szorzás kommutatív, asszociatív, minden nem nulla elemnek van inverze a szorzásra nézve, a szorzás disztributív az összeadásra nézve, és H zárt a csoportbeli műveletekre (szorzás, inverzképzés).

1.2.2. Definíció. Ha a szorzás kommutativitását nem tesszük fel, akkor ferdetestről beszélünk.

1.2.3. Definíció. A véges sok elemet tartalmazó testet véges testnek mondjuk.

1.2.4. Tétel (Wedderburn)**.** Minden véges ferdetest test.

1.2.5. Tétel. Véges test elemszáma prímhatvány.

1.2.6. Tétel. Egy G csoport részcsoportja egy olyan $H \subseteq G$ részhalmaz, amelyik zárt a G-beli műveletekre. Világos, hogy H is csoport, ugyanazokkal a műveletekkel. Jelölése: $H \leq G$.

1.2.7. Tétel. Minden $\mathbb{F}_q$ véges test multiplikatív csoportja ciklikus.

1.2.8. Állítás. Ha $\mathbb{F}$ egy q elemszámú test, akkor minden $a \in \mathbb{F}$-re, $a^q = a$ teljesül.

1.2.9. Tétel. Minden p prímre és minden n pozitív egészre létezik p^n elemszámú test. Bármely $q = p^n$ elemszámú test izomorf az $x^q - x$ polinom $\mathbb{F}_p$ feletti felbontási testével.

Tehát beszélhetünk a q elemű testről. Ezeket $\mathbb{F}_q$-val jelöljük és q rendű Galois-testnek nevezzük.

Nézzük most a négyzetelemeket a véges testekben. Jelölje ezek halmazát $\square$. Ha q páros, akkor minden elem négyzetelem, így a következőkben q páratlan. Vegyünk át ezekről néhány egyszerű állítást:

1.2.10. Állítás. Ha $a \in \square$ és $b \in \square \implies ab \in \square$, azaz $\square$ részcsoportot alkot.

1.2.11. Állítás. $|\square| = \frac{q-1}{2}$, mivel az $x^2 = a$-nak 2 megoldása van ($x \neq 0$).

1.2.12. Állítás. Ha $a, b \notin \square$, akkor $ab \in \square$.

1.2.13. Állítás. Legyen $< \omega >= \mathbb{F}_q$, azaz ω generáló elem (számelméletben primitív gyök). Ekkor $\forall a \in \mathbb{F}_q$-ra $a = \omega^i$ $(0 \leq i < q-1)$.

1.2.14. Állítás. a akkor, és csak akkor négyzetelem, ha i páros, azaz $a \in \square \iff i$ páros.

1.2.15. Állítás. $a \in \square \iff a^{\frac{q-1}{2}} = 1$. (Azaz $a \notin \square \iff a^{\frac{q-1}{2}} = -1$.)

1.2.16. Megjegyzés. Speciálisan: $-1 \in \square \iff \frac{q-1}{2}$ páros. (Azaz $-1 \notin \square$, ha $q \equiv 3 \pmod 4$.)

A projektív geometria axiomatikus megalapozására irányuló kutatások új fényt vetettek Papposz és Desargues tételére. Mint kiderült, a Papposz-tétel pontosan a test feletti projektív tereket karakterizálja a projektív terek közt.

Nézzük is meg Papposz tételét:

1.2.17. Tétel (Papposz)**.** Legyen e és f két különböző egyenes a síkon, $A, B, C \in e$ és $A', B', C' \in f$ hat különböző pont, melyek különböznek a $P \in e \cap f$ metszésponttól is. Ekkor az

$$A'' = BC' \cap B'C, B'' = AC' \cap A'C \text{ és } C'' = AB' \cap A'B$$

pontok egy egyenesre illeszkednek.

Ehhez hasonló tétel, amely a ferdetestre épített tereket írja le:

1.2.18. Tétel (Desargues tétele, projektív változat)**.** Legyenek (tetszőleges dimenziójú) projektív térben $S, A_1, B_1, C_1, A_2, B_2, C_2$ olyan különböző pontok, amelyekre az S, A_1, B_1, C_1 , illetve az S, A_2, B_2, C_2 pontok között bármely három független, továbbá amelyekre az S, A_1, A_2, az S, B_1, B_2 és az S, C_1, C_2 ponthármasok kollineárisak. Ekkor az $A = \langle B_1, C_1 \rangle \cap \langle B_2, C_2 \rangle, B = \langle C_1, A_1 \rangle \cap \langle C_2, A_2 \rangle, C = \langle A_1, B_1 \rangle \cap \langle A_2, B_2 \rangle$ ponthármas is kollineáris.

1.3. Síkbeli homogén koordináták

Az ideális pontokkal való bővítést az úgynevezett **homogén koordináták** bevezetésével tudjuk megoldani. A sík pontjainak homogén koordinátás, három összetevős alakját egy háromdimenziós Descartes-féle koordináta-rendszerben szokás szemléltetni. Legyen adott például egy $z = 1$ sík (ez párhuzamos az $x - y$ tengelyek által meghatározott síkkal). Definiáljunk ezen sík pontjai és az origón áthaladó egyenesek között egy kölcsönösen egyértelmű kapcsolatot, úgy hogy az egyenesekhez a síkkal vett metszéspontjukat (döféspontjukat) rendeljük hozzá, a sík tetszőleges pontjához pedig az origóval összekötő egyenest. Az $x-y$ koordinátasíkban fekvő egyeneseknek a $z = 1$ sík végtelen távoli pontjai felelnek meg. Ehhez a fejezethez a [7] és [2] valamint az [1] forrásokat használtam.

1.3.1. Definíció (Homogén koordináta)**.** A sík pontjait olyan rendezett számhármasokkal reprezentáljuk, amelyek arányosság erejéig vannak meghatározva, és mind a három egyszerre nem lehet 0.

Azaz ha (A, B, C) és $\lambda \neq 0 \in \mathbb{R}$, akkor $(\lambda A, \lambda B, \lambda C)$ ugyanazt a pontot jelöli. (0,0,0) homogén koordinátájú pont nem létezik.

Amennyiben az S sík egyeneseit szeretnénk meghatározni, azt legegyszerűbben a térbeli koordináta-rendszer O kezdőpontján átfektetett sík megadásával tehetjük meg. Ezt a síkot az $e \neq 0$ normálvektorával jellemezhetjük. A következőkben az egyenest meghatározó vektorok esetén ilyen normálvektorokra kell gondolnunk.

Vegyük az e egyenes két pontját, $A = (a_1, a_2, 1), B = (b_1, b_2, 1)$, melyek normált homogén koordinátás alakban vannak. Az ezen pontokba mutató helyvektorok vektoriális szorzataként meg tudjuk határozni az e egyenes normálvektorát. Azaz $e = a \times b$. Ennek alapján kiszámíthatók az e vektor koordinátái:

$$e = \begin{vmatrix} i & j & k \\ a_1 & a_2 & 1 \\ b_1 & b_2 & 1 \end{vmatrix} = (a_2 - b_2, b_1 - a_1, a_1 b_2 - b_1 a_2)$$

Mivel az a és b vektorok az S sík e egyenesének és a térbeli koordináta-rendszer O kezdőpontja által meghatározott síkjában vannak, a vektoriális szorzatuk pontosan merőleges lesz az S síkra (és az e egyenesre).

Legyen az e egyenes egyenlete $ax + by + c = 0$ alakú. Szorozzuk meg az egyenlet mindkét oldalát x_3-mal (harmadik koordinátatengely), így a homogén koordináta

definíciójából az $ax_1 + bx_2 + cx_3 = 0$ egyenletet kapjuk. Ennek alapján az e egyenes keresett egyenlete: $(a_2 - b_2)x_1 + (b_1 + a_1)x_2 + (a_1b_2 - b_1a_2)x_3 = 0$

Tehát a sík egyeneseit (hasonlóan a sík pontjaihoz) rendezett számhármasokkal reprezentáljuk, amelyek az arányosság erejéig vannak meghatározva, és mind a három egyszerre nem lehet nulla.

1.3.2. Állítás. Az (x_1, x_2, x_3), (y_1, y_2, y_3) és (z_1, z_2, z_3) pontok akkor és csak akkor vannak egy egyenesen, ha

$$\begin{vmatrix} x_1 & x_2 & x_3 \\ y_1 & y_2 & y_3 \\ z_1 & z_2 & z_3 \end{vmatrix} = 0.$$

1.3.3. Megjegyzés. Megkonstruáljuk a $\mathbb{K}$ testre épített AG(2,$\mathbb{K}$) affin sík egy olyan modelljét, amely a középiskolában tanult kordinátageometriát másolja.

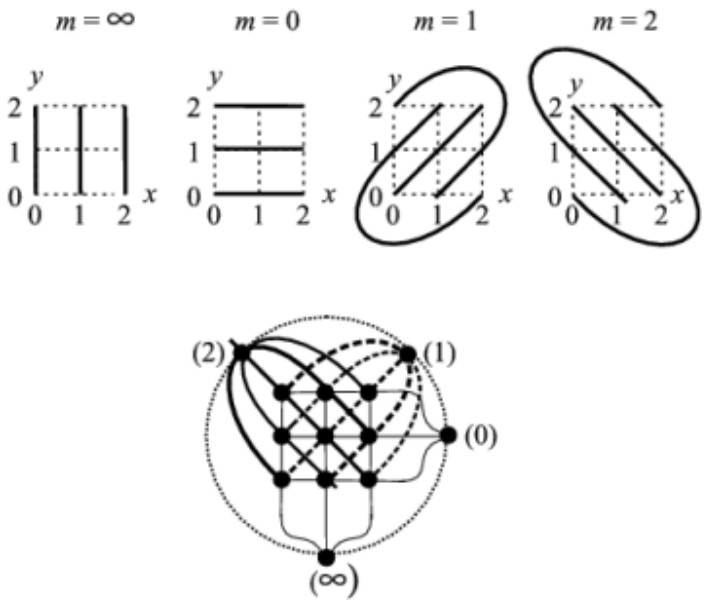
Legyen $\mathcal{P}$ az (x, y) párok halmaza, ahol $x, y \in \mathbb{K}$. Legyen $\mathcal{E}$ az $[m, b]$ párok és a $[c]$ szimbólumok halmaza.

Formálisan $\mathcal{P} = \{(x, y) : x, y \in \mathbb{K}\}$, $\mathcal{E} = \{[m, b] : m, b \in \mathbb{K}\} \cup \{[c] : c \in \mathbb{K}\}$. Végül az illeszkedési reláció (I) az alábbi: (x, y) I $[m, b] \iff y = mx + b, (x, y)$ I $[c] \iff x = c$. Láthatjuk, hogy az illeszkedést lényegében az egyenes egyenleteként tanult képletekkel kapjuk. Mivel $\mathbb{K}$ test, a középiskolában tanult két ponton átmenő egyenes egyenletére, illetve két egyenes metszéspontjára vonatkozó képletek, szó szerint átvihetők a mostani esetre. Speciálisan például két egyenes, $[m, b]$ és $[n, d]$ akkor és csak akkor párhuzamosak, ha $m = n$.

Azt is megfigyelhetjük, hogy minden egynesre $|\mathbb{K}|$ pont illeszkedik (hiszen a pont x koordinátája tetszőleges, illetve a $[c]$ típusú függőleges egyeneseknél az y koordináta tetszőleges). Ennek alapján az AG(2,$\mathbb{K}$) sík rendje $|\mathbb{K}|$. Mivel adott $|\mathbb{K}| = q$ prímhatványra pontosan egy véges test létezik, ezt a síkot AG(2,q)-val fogjuk jelölni.

Nézzük meg az AG(2,q) projektív bővítését. Mivel az egyenesek párhuzamossága meredekségükkel írható le, egy párhuzamossági osztálynak az (m) illetve az (∞) ideális pont felel meg, Eszerint az $[m, b]$ egyenesnek a projektív lezártban megfelelő egyenes pontjai $\{(x, y) : y = mx + b\} \cup \{(m)\}$ és hasonlóan a $[c]$ típusú egyenesekhez a (∞) ideális pontot vesszük hozzá. Az ideális egyenest az $\{(m) : m \in \mathbb{F}_q\} \cup \{(\infty)\}$ pontok alkotják. Ezt a síkot PG(2,q) jelöli.

1.3.4. Példa. Nézzünk egy ábrát [1]-ből harmadrendű affin sík bővítésére.



2. ábra. : Az affin sík az ideális pontokkal

1.3.5. Példa (Fano-sík másképp)**.** A lehető legegyszerűbb/legkisebb példa véges projektív síkra a Fano-sík. A projektív sík homogén koordinátákkal való létrehozása szerint a Fano-sík pontjait hét, nullától különböző számhármassal lehet megadni: $(001), (010),\ (011), (100), (101), (110), (111)$. Bármely egyenesen, amelyik a P és Q pontokat tartalmazza, a harmadik pontot a kettejük koordinátáinak mod 2 összegeként kaphatjuk meg. Másképpen szólva a Fano-sík a 2 elemű véges test feletti véges háromdimenziós vektortér nem nulla elemeiből áll. Ez alapján a Fano-sík egyfajta Desargues-i sík, bár olyan kicsi, hogy kizárólag degenerált konfigurációi vannak. (Nem-degenerált konfigurációhoz ugyanis minimum tíz pont és tíz egyenes szükséges.)

1.3.6. Példa. Ha a PG(2,$\mathbb{K}$) síkból elhagyjuk az $x_3 = 0$ egyenletű egyenest (azaz a [0,0,1] koordinátájú egyenest) és a rajta lévő pontokat, akkor az AG(2,$\mathbb{K}$)-val jelölt affin síkot kapjuk.

A projektív síkbeli koordináták homogenitása miatt feltehetjük, hogy az AG(2,$\mathbb{K}$)-beli pontok harmadik koordinátája 1. Ezért AG(2,$\mathbb{K}$) pontjait kér koordinátával leírhatjuk. Így kapjuk a következő algebrai modellt: A pontok az $(x, y) \in \mathbb{K} \times \mathbb{K}$ rendezett párok; egyenesek azok a rendezett $[A, B, C]$ hármasok, ahol nem nulla

egyszerre A és B is, és $[A, B, C]$ valamint $[\lambda A, \lambda B, \lambda C]$ ugyanazt az egyenest jelenti, ha $0 \neq \lambda \in K$; az (x, y) és az $[A, B, C]$ egyenes pontosan akkor illeszkedik, ha $Ax + By + C = 0$.

A klasszikus euklidészi sík pontjai azonosíthatók a komplex számokkal. Ezt a módszert általánosítva kapjuk AG(2,$\mathbb{K}$) egy másik algebrai modelljét, mely a Gauss-féle számsík általánosítása.

1.3.7. Példa. Legyen f irreducibilis másodfokú polinom a $\mathbb{K}$ test felett, $\mathbb{F}$ pedig a $\mathbb{K}$ másodfokú bővítése az f egy i-vel jelölt gyökével. Ekkor $\mathbb{F}$ elemei $a + bi$ alakba írhatók, ahol $a, b \in \mathbb{K}$. Az AG(2,$\mathbb{K}$) sík (a, b) koordinátájú pontjának feleltessük meg az $a + bi \in \mathbb{F}$ testelemet. Ez a megfeleltetés bijekció AG(2,$\mathbb{K}$) pontjai és $\mathbb{F}$ elemei között. A sík $[A, B, C]$ egyenesének az $\{x + yi \in \mathbb{F} : x, y \in \mathbb{K}, Ax + By + C = 0\}$ részhalmaz felel meg.

Az így felírt modellben könnyen megadhatóak feltételek egyenesek párhuzamosságára, illetve három pont kollinearitására.

1.3.8. Lemma. Legyen $P_j : (a_j, b_j)(j = 1, 2, 3, 4)$ négy pont az AG(2,$\mathbb{K}$) sík 1.3.7 példában szereplő modelljében, ahol $P_1 \neq P_2$ és $P_3 \neq P_4$. A pontok által meghatározott P_1P_2 és P_3P_4 egyenesek akkor és csak akkor párhuzamosak, ha az $a_j + b_j i = z_j \in \mathbb{F}$ testelemekhez létezik olyan $\alpha \in \mathbb{K}$ testelem, melyre $z_4 - z_3 = \alpha(z_2 - z_1)$ teljesül.

Bizonyítás. Az AG(2,$\mathbb{K}$) síkon P_1P_2, illetve a P_3P_4 egyenesek egyenlete

$$(b_2 - b_1)x + (a_1 - a_2)y + (b_1a_2 - b_2a_1) = 0,$$

illetve

$$(b_4 - b_3)x + (a_3 - a_4)y + (b_3a_4 - b_4a_3) = 0.$$

Ez a két egyenes pontosan akkkor párhuzamos, ha

$$\begin{vmatrix} b_2 - b_1 & a_1 - a_2 \\ b_4 - b_3 & a_3 - a_4 \end{vmatrix} = 0.$$

Ez akkor és csak akkor fordulhat elő, ha a mátrixunk sorai lineárisan összefüggenek, azaz, ha létezik olyan $\alpha \in \mathbb{K}$ testelem, melyre

$$a_3 - a_4 = \alpha(a_1 - a_2), \text{ és } b_4 - b_3 = \alpha(b_2 - b_1)$$

is teljesül. Ez viszont pontosan akkor igaz, ha $z_4 - z_3 = \alpha(z_2 - z_1)$ egyenlőség áll fenn. □

1.3.9. Következmény. Az 1.3.7 példában szereplő modell esetén AG(2,q) három különböző $P_j : (a_j, b_j)(j = 1, 2, 3)$ pontja akkor és csak akkor kollineáris, ha a nekik megfelelő $a_j + b_j i = z_j \in F$ testelemekre igaz, hogy $(z_2 - z_3)^{q-1} = (z_2 - z_1)^{q-1}$.

2. Ívekkel kapcsolatos ismeretek

2.1. Alapfogalmak, alaptételek

Ebben a fejezetben először alapfogalmakat, definíciókat veszünk át ívekről, majd ezek, illetve lefogó halmazok méreteiről nézünk becsléseket [2].

2.1.1. Definíció. Projektív sík egy olyan ponthalmazát, amelynek bármely egyenesen legfeljebb 2 pontja van, *ív*eknek nevezzük. Ha ez az ív k pontból áll, akkor k-ívnek mondjuk. Valamint *teljesnek* hívjuk, ha tartalmazásra véve maximális, tehát nem része $(k+1)$-ívnek.

2.1.2. Definíció. Egy sík valamely egyenese *külső egyenes* a k-ívre nézve, ha azzal nincsen egy közös pontja sem.

2.1.3. Definíció. Egy sík valamely egyenese *érintő* a k-ívre nézve, ha azzal 1 közös pontja van.

2.1.4. Definíció. Egy sík valamely egyenese *szelő* a k-ívre nézve, ha azzal 2 közös pontja van.

Számunkra a teljes ívek lesznek a fontos vizsgálandó objektumok, mivel ív része is ív. Ezen belül is azzal a kérdéssel foglalkozunk először, hogy mekkora lehet a legnagyobb ív q-adrendű síkon.

2.1.5. Tétel (Bose)**.** q-adrendű sík tetszőleges k-ívére $k \leq q+2$ teljesül. Ha q páratlan, akkor $k \leq q+1$ is igaz.

Bizonyítás. Vegyük az ív egy tetszőleges P pontját. Egy ponton keresztül $q+1$ egyenes halad át, amik mindegyikén egy pont lehet P-n kívül. Így tehát összesen $q+2$ pontú legfeljebb egy ív. Ha a $k = q+2$ esetet nézzük, akkor akármelyik P-t választva, minden P-n áthaladó egyenesen kell még 1 pontot tartalmaznia az ívünknek. Azaz minden metsző egyenes 2 pontban is metszi az ívet. Ezt kell alkalmazni a páratlan q-ra, és belátni, hogy ott nem létezhetnek $(q+2)$-ívek. Válasszunk egy íven kívüli R pontot. Az ezen áthaladó egyenesek vagy 0 vagy 2 pontban metszik az ívünket, tehát ha R-et összekötjük az ív pontjaival, akkor ily módon párba állítottuk az ívünk pontjait, azaz ívünk mérete is páros kell legyen. De ha $q+2$ páros akkor q is az. □

Azt is meg tudjuk mutatni, hogy nem csak felső korlátot tudunk adni teljes ív méretére, hanem alsót is, tehát nem lehet teljes ív nagyon kicsi sem.

Ehhez szükség van az alábbi lemmára:

2.1.6. Lemma. Projektív sík pontjainak egyenesekkel való lefedéséhez legalább $q+1$ egyenes kell.

Bizonyítás. q egyenes legfeljebb $q(q+1) < q^2+q+1$ pontot fedhet le. □

2.1.7. Megjegyzés. Az is belátható, hogy $q+1$ egyenes csak akkor fedi a sík összes pontját, ha azok egy ponton mennek át.

2.1.8. Megjegyzés. Nézzük meg, hogy éles is lehet-e a Bose tétel becslése.

Az "$y = x^2$" eset: $\mathcal{P} = \{(x, x^2, 1) : x \in \mathbb{F}_q\} \cup Y_\infty(0,1,0)$. Ha q páros, akkor az $x \to x^2$ leképezés automorfizmus (azaz bijektív is), így ilyenkor $\forall$ vízszintes egyenes 1 pontban metszi $\mathcal{P}$-t $\Rightarrow X_\infty(1,0,0)$ is hozzávehető és még akkor is ív marad. "$y = \frac{1}{x}$" hiperbolára is a $\mathcal{H} = \{(x, \frac{1}{x}, 1) : x \in \mathbb{F}_q\} \cup \{X_\infty, Y_\infty\}$ ív marad.

Ezek mutatják, hogy a tételben a becslés **éles** PG(2,q)-ra.

2.1.9. Állítás (Lunelli,Sce)**.** q-adrendű sík k-íve nem lehet teljes, ha $q \geq k(k-1)/2$.

Bizonyítás. Ha a k-ív teljes, akkor az ívre vonatkozva szelő egyenesek a sík minden pontját lefedik. Mivel ehhez a következő (2.1.11) lemma miatt legalább $q+1$ egyenes kell, ezért $k(k+1)/2 \geq q+1$. □

A 2.1.6 Lemma és a 2.1.8 Megjegyzés duálisa a lefogó ponthalmazokkal kapcsolatos legalapvetőbb eredmény. Lefogó ponthalmaznak olyan ponthalmazt nevezünk, amely minden egyenest metsz.

2.1.10. Lemma. A q-adrendű Π_q projektív sík bármely lefogó ponthalmaza legalább $q+1$ pontból áll. Ha a lefogó ponthalmaz elemszáma $q+1$, akkor az egyenes.

Duális módon:

2.1.11. Lemma. Ha egyenesek egy $\mathcal{L}$ halmaza lefedi a q-adrendű sík összes pontját, akkor $|\mathcal{L}| \geq q+1$, és egyenlőség esetén $\mathcal{L}$ egy egy ponton átmenő egyenesek halmaza.

Nézzük ennek a duálisnak a bizonyítását:

Bizonyítás. q darab egyenes legfeljebb $q(q+1)$ pontot fedhet le, így legalább $q+1$ egyenesre van szükség. Ha $q+1$ egyenes, mondjuk $l_1, l_2, ..., l_{q+1}$ lefedik az összes pontot, akkor l_1 $q+1$ pontot, l_2 még q darab pontot, és mindegyik további l_i szintén q darabot. Ha van 3 olyan egyenes, ami nem megy át egy ponton, akkor legyenek ezek l_1, l_2, l_3. Ekkor viszont l_3 csak legfeljebb $q-1$ olyan pontot fed le, ami nincs $l_1 \cup l_2$-n. Ugyanez igaz minden $l_i (i > 3)$-ra is, hisz l_i, az l_1, l_2, l_3 egyenesek közül legalább kettőt különböző pontban metsz. Így összesen legfeljebb $q+1+q+(q-1)(q-1) = q^2+2$ pont lehet fedve. Tehát $l_1, l_2, ..., l_{q+1}$ közül bármely 3 egyenes egy ponton megy át, ami miatt mind egy ponton mennek át.

□

Érdemes megemlíteni, hogy ívet, sőt teljes ívet is, nagyon könnyen konstruálhatunk a mohó algoritmussal: ha már néhány pontot kiválasztottunk úgy, hogy ezek szelői nem fedik le a sík összes pontját, akkor válasszunk egy további pontot a nem fedettek közül, és így tovább. Ez az eljárás akkor ér véget, ha teljes ívet kaptunk.

2.1.12. Definíció. *Oválisnak* olyan ívet nevezünk, amelynek minden pontjában csak egyetlen érintő egyenese van.

2.1.13. Definíció. *Hiperoválisnak* az olyan íveket nevezzük, amelyeknek nincs érintő egyenesük.

Figyelembe véve, hogy k-ív minden pontján pontosan $k-1$ szelő, és így $t = q+2-k$ érintő egyenes megy át, q-adrendű síkok oválisai éppen a $(q+1)$-ívek, a hiperoválisok pedig a $(q+2)$-ívek. Ezekről szólt a 2.1.8 Megjegyzés is, csak ott még nem voltak néven szólítva.

2.1.14. Állítás. Vannak PG(2,q)-ban oválisok, és ha q páros, akkor hiperoválisok is.

2.1.15. Állítás. A $(q+1)$-ívek nem teljesek a páros rendű síkokon.

Bizonyítás. Elég annak bebizonyítására, hogy az $\mathcal{O}$ ovális érintői egy ponton mennek át, azt megmutatnunk, hogy a sík minden pontján megy át érintő, mert a $q+1$ érintő a 2.1.11 Lemma szerint éppen akkor fedi le a sík minden pontját, ha egy közös ponton mennek át. Az ovális pontjait persze lefedik az érintők. Legyen $Y \notin \mathcal{O}$, és kössük össze ezt $\mathcal{O}$ pontjaival. Mivel $\mathcal{O}$-nak páratlan sok pontja van, ezért lesz az YO $(O \in \mathcal{O})$ egyenesek között érintő, vagyis valóban a sík minden pontján megy át érintő. □

Ez azt jelenti, hogy a páros rendű sík oválisának érintői egy ponton mennek át.

2.1.16. Definíció. Legyen $\mathcal{O}$ a q-adrendű Π_q sík egy oválisa, ahol q páros. $\mathcal{O}$ érintőinek metszéspontját az $\mathcal{O}$ *magpont*jának nevezzük.

2.1.17. Lemma. Legyen $\mathcal{O}$ ovális a Π_q q-adrendű síkon, ahol q páratlan. A sík $\mathcal{O}$-hoz nem tartozó bármely pontján vagy 0 vagy 2 érintő megy át.

Bizonyítás. Vegyük $\mathcal{O}$ egyik érintőjét. Jelöljük T-vel a $t \cap \mathcal{O}$ érintési pontot. Belátjuk, hogy $t\backslash\{T\}$ pontjain pontosan egy további érintő megy át. Mivel $\mathcal{O}$ minden pontján pontosan egy érintő megy át, így a t-től különböző érintők száma pontosan q. Ugyanennyi a $t\backslash\{T\}$ pontok száma is, így elég azt megmutatni, hogy $t\backslash\{T\}$ minden pontján megy át t-től különböző érintő. Tekintsünk egy ilyen $R \in t$, $R \neq T$ pontot, és kössük össze $\mathcal{O}\backslash\{T\}$ pontjaival. Mivel $\mathcal{O}\backslash\{T\}$ pontjainak száma páratlan, lesz olyan pont, amelyet R-el összekötve érintőt kapunk. □

2.1.18. Definíció. A páratlan rendű Π_q projektív sík olyan pontját, amelyen az $\mathcal{O}$ oválisnak két érintője megy át, $\mathcal{O}$-ra nézve *külső*, amelyiken 0 érintő megy át, *belső pont*nak nevezzük.

2.1.19. Lemma. A külső pontok száma $q(q+1)/2$, a belsőké $q(q-1)/2$. Tetszőleges, az oválist nem érintő egyenesre igaz a következő: Az egyenesen lévő pontok közül az oválison nem levő pontok fele külső, fele belső pont.

Bizonyítás. Minden érintő kétszer is lefedi a külső pontokat, és érintőből $q+1$ darab van összesen. Azaz a külső pontok száma $(q+1)q/2$, a belsőké pedig $q^2+q+1-(q+1)-q(q+1)/2 = q(q-1)/2$. Ha veszünk egy oválist nem érintő l egyenest, azon k darab külső pont van, és ha ez az egyenes m pontban metszi az oválist, akkor az ezen a pontokon átmenő érintők száma $2k+m = q+1$. És m jelenleg 0 vagy 2, tehát az állítás igaz. □

2.2. Síkgörbék geometriája

Számunkra affin síkgörbe egy olyan ponthalmaz, amelyet $f(x,y) = 0$ definiál, ahol $f(x,y) \in \mathbb{K}[x,y]$ kétváltozós polinom. Ebben a részben Szőnyi Tamás kisdoktorijának [9] egy kisebb részét vázoljuk, példákkal, számolásokkal kiegészítve.

2.2.1. Definíció. Egy $f(x,y)$ affin görbe homogén felbontása legyen a következő:

$$f(x,y) = f_m(x,y) + f_{m+1}(x,y) + ...,$$

ahol $f_i(i = m, m+1, ...)$ i-edfokú homogén polinom. Az m-et az $O = (0,0)$ pont multiplicitásának nevezzük f-en. Legyen továbbá

$$f_m(x,y) = \prod_{i=1}^{m}(a_i \cdot x + b_i \cdot y)$$

Az $a_i \cdot x + b_i \cdot y = 0$ egyenletű egyeneseket az f görbe origóbeli érintőinek nevezzük, az f_m-beli multiplicitást az érintő multiplicitásának.

Tetszőleges pont multiplicitásának meghatározását visszavezethetjük az origóbeli multiplicitás definíciójára affin koordinátatranszformációval. (És ehhez választhatjuk bármely, az adott pontot origóba vivő transzformációt, akár az eltolást is, ez nem fogja a multiplicitást befolyásolni.)

2.2.2. Definíció. Az f görbe P pontja sima (egyszeres, egyszerű), ha m_P multiplicitására $m_P = 1$, szinguláris, ha $m_P > 1$.

2.2.3. Definíció. Az f görbe egy pontja közönséges (szinguláris) pont, ha ott minden érintő multiplicitása 1.

2.2.4. Állítás. Ha P az f affin görbének szinguláris pontja, akkor

$$\left.\frac{\partial f}{\partial x}\right|_P = \left.\frac{\partial f}{\partial y}\right|_P = 0.$$

Szemléletesen az egyszeres (sima) pontokban az érintő egyértelmű, a szinguláris pontokban viszont több érintő is van (illetve az érintő "többszörös").

2.2.5. Példa. Határozzuk meg a szingularitásokat a következő homogén egyenletnél:

$$x^2y^5 - x^5y^2 - 2xy^5z + x^5z^2 + y^5z^2 - x^3yz^3 + 2\alpha x^2y^2z^2 - xy^3z^3 = 0$$

a $(0,0,1)$ és az $(1,0,0)$ pontokban. Először vegyük a $(0,0,1)$ pontbeli szingularitást, ehhez pedig a $z=0$ ideális egyenest, amiből a következő affin egyenlet adódik:

$$x^2y^5 - x^5y^2 - 2xy^5 + x^5 + y^5 - x^3y + 2\alpha x^2y^2 - xy^3 = 0$$

Itt a legkisebb fokú tagok amik megjelennek negyedfokúak, így $P_1(0,0)$ -ban $m_{P_1} = 4$ lesz a multiplicitás. Az itteni érintők meghatározásához vegyük a negyedfokú tagokból álló részt és tegyük egyenlővé 0-val:

$$x^3y - 2\alpha x^2y^2 + xy^3 = 0$$

Ez pedig a következő szorzattá alakítható:

$$xy(x^2 - 2\alpha xy + y^2) = 0$$

Tehát $x=0$ és $y=0$ érintők lesznek. A zárójeles részben így már használhatjuk az $\frac{y}{x} = u$ helyettesítést, amivel a következő másodfokú egyenletet kapjuk:

$$1 - 2\alpha u + u^2$$

Ebből a megoldóképlettel:

$$u_{1,2} = \frac{2\alpha \pm \sqrt{4\alpha^2 - 4}}{2} = \alpha \pm \sqrt{\alpha^2 - 1}$$

Tehát ha u-ra két különböző megoldás jött ki, az érintők mind egyszeresek, és az $x=0, y=0$ mellett az $y = u_1x, y = u_2x$ is érintők lesznek. Ha $u_1 = u_2$, azaz $\alpha^2 = 1$, akkor a két utóbbi érintőből egy $y = \alpha x$ kétszeres érintő lesz.

Ha az $x=0$ az ideális egyenes, akkor a következő egyenletet kapjuk:

$$y^5 - y^2 - 2y^5z + z^2 + y^5x^2 - yz^3 + 2\alpha y^2z^3 - y^3z^3$$

Itt már vannak másodfokú tagok is, ezért $P_2(0,0)$-ban $m_{P_2} = 2$ és az érintők

$$0 = -y^2 + z^2 = (y-z)(y+z)$$

alapján $y=z$ és $y=-z$ (egyszeresek) lesznek, ha a test karakterisztikája nem 2. Ha

a karakterisztika 2, akkor egy érintő van $y = z$, ami kétszeres.

Ha pedig a $(0, 1, 0)$ pontban vizsgálnánk az eredeti egyenletünket, $y = 0$ ideális egyenessel, akkor:

$$x^2 - x^5 - 2xz + x^5z^2 + z^2 - x^3z^3 + 2\alpha x^2z^2 - xz^3$$

adódik, amiből a másodrendűekre:

$$0 = x^2 - 2xz + z^2 = (x - z)^2$$

tehát egy kétszeres $x = z$-t kapunk.

Két görbe metszési multiplicitása precízen definiálva hosszas folyamat lenne, így egy könnyebb tételt használunk definíciónak (azaz az itt bevezetett állítások számunkra axiómák lesznek):

2.2.6. Definíció. Az f és g görbék P pontbeli metszési multiplicitását $I(P; f \cap g)$ jelöli.

2.2.7. Definíció. A $P \in f \cap g$ metszéspontot közönségesnek nevezzük, ha ebben a pontban f és g érintői különbözőek.

Az említett tétel pedig így szól a metszési multiplicitás létezéséről, valamint egyértelműségéről:

2.2.8. Tétel. Pontosan egyféleképpen adható meg olyan metszési multiplicitás, amely rendelkezik az alábbi tulajdonságokkal:

1. $I(P; f \cap g) < \infty$ ha f-nek és g-nek nincs közös komponense,
2. $I(P; f \cap g) = 0$ pontosan akkor, ha $P \notin f \cap g$,
3. $I(P; f \cap g_1g_2) = I(P; f \cap g_1) + I(P; f \cap g_2)$,
4. $I(P; f \cap g) = I(P; f \cap g + hf)$,
5. $I(P; f \cap g) \geq m_P(f) \cdot m_P(g)$ és egyenlőség pontosan akkor áll fenn, ha P közönséges metszéspont.

2.2.9. Megjegyzés (Scherk)**.** Az 5. tulajdonságot lecserélhetjük arra, hogy

$$I(P; f \cap g) = 1, \text{ ha } f \text{ és } g \text{ két különböző } P\text{-n átmenő egyenes.}$$

Így ebből, és az első négyből következik az eredeti 5., és ezt sokkal könnyebb a számolásban használni.

Nézzünk pár példát ennek gyakorlatban való kiszámolására:

2.2.10. Példa. Tekintsük az $f = y - x^2$ és a $g = y - x^3$ egyenesek metszési multiplicitását a $P = (0, 0)$ pontban.

$$I(P; f \cap g) \overset{(4)}{=} I(P; f \cap (g - f)) \overset{(behely.)}{=} I(P; y - x^2 \cap (x^2 - x^3)) \overset{(3)}{=}$$
$$\overset{(3)}{=} I(P; y - x^2 \cap x^2) + I(P; y - x^2 \cap (1 - x)) \overset{(3)}{=} 2 \cdot I(P; y - x^2 \cap x) +$$
$$+ I(P; y - x^2 \cap (1 - x)) \overset{(2)}{=} 2 \cdot I(P; y - x^2 \cap x) + 0 \overset{(Scherk)}{=} 2 \cdot 1 = \underline{\mathbf{2}}$$

Most cseréljük le a második görbénk:

2.2.11. Példa. Tekintsük az $f = y - x^2$ és a $h = y^2 - x^3$ egyenesek metszési multiplicitását a $P = (0, 0)$ pontban.

$$I(P; f \cap h) \overset{(4)}{=} I(P; f \cap (h - y \cdot f)) \overset{(behely.)}{=} I(P; y - x^2 \cap (yx^2 - x^3)) \overset{(3)}{=}$$
$$\overset{(3)}{=} I(P; y - x^2 \cap x^2) + I(P; y - x^2 \cap (y - x)) \overset{(3)}{=} 2 \cdot I(P; y - x^2 \cap x) +$$
$$+ I(P; y - x^2 \cap (1 - x)) \overset{(Scherk)}{=} 2 + I(P; y - x^2 \cap (y - x)) \overset{(4)}{=}$$
$$\overset{(4)}{=} 2 + I(P; y - x^2 \cap (y - x) - f) \overset{(behely.)}{=} 2 + I(P; y - x^2 \cap x^2 - x) \overset{(3)}{=}$$
$$\overset{(3)}{=} 2 + I(P; y - x^2 \cap x) + I(P; y - x^2 \cap x - 1) \overset{(Scherk)}{=} 3 + I(P; y - x^2 \cap x - 1) \overset{(2)}{=}$$
$$\overset{(2)}{=} 3 + 0 = \underline{\mathbf{3}}$$

Most az eddig bevezetett legfontosabb fogalmakat projektív görbékre is definiáljuk.

Projektív görbe pontjának multiplicitása a pont egy környezetében értelmezett affin részének a pontbeli multiplicitása. Ugyanígy definiálhatók a pontbeli érintők és azok multiplicitása is.

Legyen a projektív síkgörbe $f(x_1, x_2, x_3) = 0$,ahol f homogén polinom.

Projektív görbék metszési multiplicitását, mint a P egy környezetében értelmezett affin részük metszési multiplicitását értelmezzük.

Így már ki tudjuk mondani Bézout tételét. Ez a tétel jól szemlélteti azt a jelenséget az algebrai geometriában, hogy egy tétel bizonyítása könnyű lehet általános helyzetű alakzatokra, de komoly nehézségekbe ütközhetünk, ha precízen akarjuk bizonyítani az **általános** esetet.

2.2.12. Tétel. Ha f és g közös komponens nélküli görbék, akkor

$$\sum_P I(P; f \cap g) = \deg(f) \cdot \deg(g).$$

2.2.13. Következmény.

$$\sum_P m_P(f) \cdot m_P(g) \leq \deg(f) \cdot \deg(g),$$

és egyenlőség pontosan akkor áll fenn, ha minden metszéspont közönséges.

Ennek a tételnek a segítségével becslést is tudunk adni egy síkgörbe szinguláris pontjainak számára, hiszen a szinguláris pontok f és f'_x (vagy $\frac{\partial f}{\partial x}$) metszéspontjai.

2.2.14. Tétel. Legyen f egy n-edfokú irreducibilis síkgörbe. Ekkor

$$g + \sum_P m_P(m_P - 1) \leq (n-1)(n-2)$$

és egyenlőség csak abban az esetben teljesül, ha minden szinguláris pont közönséges. Itt g a görbe nemét jelenti (génusz), ami egy nemnegatív egész szám.

2.2.15. Következmény. Legyen f többszörös komponens nélküli algebrai síkgörbe. A komponensek számát jelölje c. Ekkor

$$\sum_P m_P(m_P - 1) \leq (n-1)(n-2) + 2(c-1) \leq n(n-1).$$

Az általunk felhasznált legmélyebb algebrai geometriai segédeszköz, az úgynevezett **Hasse-Weil becslés**. Ehhez az alábbi fogalomra lesz szükségünk:

2.2.16. Definíció. Egy $\mathbb{F}_q$ fölött definiált polinomot abszolút irreducibilisnek nevezünk, ha $\mathbb{F}_q$ algebrai lezártja fölött is irreducibilis (azaz nem bomlik tényezőkre $\mathbb{F}_q$ semelyik algebrai bővítésében).

2.2.17. Tétel (Hasse-Weil)**.** Legyen f egy $\mathbb{F}_q$ felett definiált abszolút irreducibilis projektív görbe. Az f görbe $\mathbb{F}_q$ feletti (PG(2,q)-beli) pontjainak számát jelölje N_q, a sima pontokat egyszer, a szinguláris pontokat alkalmas 0 és m_P közötti multiplicitással számolva. Ekkor

$$\mid N_q - q - 1 \mid \leq 2g\sqrt{q}$$

ahol g a görbe neme. Ha $n = deg(f)$, a görbe fokszáma, akkor

$$\mid N_q - q - 1 \mid \leq (n-1)(n-2)\sqrt{q}$$

2.3. Abszolút irreducibilitási kritériumok

Mivel a Hasse-Weil tétel (2.2.17) csak abszolút irreducibilis projektív görbékre szól, ezért fontos, hogy el tudjuk dönteni egy $\mathbb{F}_q$ felett definiált algebrai görbéről, hogy rendelkezik-e ilyen tulajdonsággal.

Ha a görbének nincs szinguláris pontja, akkor persze abszolút irreducibilis. Ha ugyanis a görbének kettő vagy több komponense lenne, akkor a komponensek metszéspontjaiban nem lenne egyértelmű az érintő, vagyis ezek a pontok szinguláris pontok lennének.

A következőnek említett állítás Segre és Bartocci [8] cikkében található meg. Előnye a szemléletessége, a többi kritériummal szemben.

2.3.1. Tétel. A k-adrendű C görbe legyen definiálható az $\mathbb{K}$ test fölött. Ha

1. létezik olyan $P \in C$ pont, és olyan e érintő P-ben, hogy e egyszeres érintő és $I(P; C \cap e) = \deg(C) = k$, és

2. C-nek nincs P-n átmenő lineáris komponense,

akkor C abszolút irreducibilis, azaz irreducibilis $\mathbb{K}$ algebrai lezártja fölött.

2.3.2. Következmény. Legyen P a C görbe közönséges szinguláris pontja. Ha C-nek van olyan e érintője P-ben, amelyre $e \cap C = P$, és C-nek nincs P-n átmenő lineáris komponense, akkor C abszolút irreducibilis.

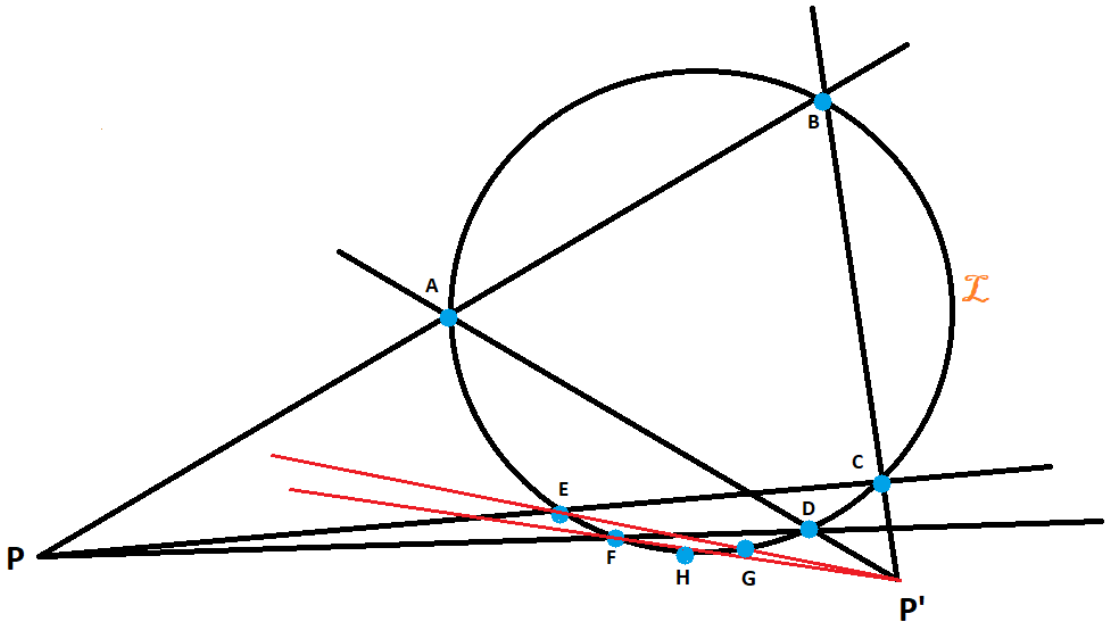
Ennek a kritériumnak nagy előnye, hogy az e érintőre vonatkozó két feltevés teljesülése lényegében ugyanazzal a számítással ellenőrizhető.

3. Kis teljes ívek

3.1. Segre-konstrukció

Vizsgáljuk meg a következőkben, hogy Segre milyen konstrukciót használt teljes ív gyártására, véletlen használatával:
Vegyünk egy $\mathcal{L}$ kúpszeletet, és rajta kívül egy pontot. Vegyünk egy ezen a P ponton átmenő szelőt. Ez a kúpszelettel két metszéspontot ad, legyenek ezek A és B pontok. Minden ilyen szelőre vegyük ezen két (A és B) pont egyikét (1/2-1/2 valószínűséggel). Ha $A = B$, azaz szelő helyett érintő van, akkor ezt a pontot vegyük be az ívbe. A konstrukcióból adódik, hogy minden választásra ívet kapunk, amelyhez $\mathcal{L}$-ről nem vehetők hozzá további pontok. Később felosztjuk a P-n átmenő egyeneseket csoportokra, és azt akarjuk megbecsülni, hogy mennyi annak a valószínűsége, hogy a $P' \notin \mathcal{L}$ hozzávehető ("nincs fedve").

Tekintsük a következő ábrát:



3. ábra. : Segre

P és P' kúpszeleten kívüli pontok. Legyen $C = BP' \cap \mathcal{L}$ és $D = AP' \cap \mathcal{L}$. Ezután kössük össze az új pontjainkat P-vel, és legyen $E = CP \cap \mathcal{L}$ valamint $F = DP \cap \mathcal{L}$. Majd ezeket ismét P'-vel összekötve megkapjuk $G = EP' \cap \mathcal{L}$ és $H = FP' \cap \mathcal{L}$ (lásd: 3.ábra).

Azt szeretnénk vizsgálni, hogyha a P-n átmenő egyeneshármasokon, $\frac{1}{2} - \frac{1}{2}$ eséllyel választjuk a pontokat, akkor milyen eséllyel nem lesz P' hozzávehető az ívhez (lesz P' "fedett"). Ha A-t választottuk az első egyenesről, akkor a harmadikról mindenképp D-t kell, mert csak így lehet fedve, és a második egyenesen mindegy melyik pontot választjuk C és E közül. B-vel való kezdés esetén is 2 módon fedhető le P'. Összesen 8-féleképp választhatjuk a $3 \cdot 2$ pontot ki, és ebből az előbb tárgyalt 4 felállásban ($4/8 = 1/2$ valószínűsége lesz tehát) lesz P' fedett.

Ennek a számolásnak a kiterjesztésével szeretnénk becsülni P' fedettségének valószínűségét, de ehhez az kellene, hogy diszjunkt egyeneshármasokat tudjunk P-n keresztül felvenni. Hogy ilyeneket választhassunk, nem elég a további egyeneseket szimplán az előző háromtól eltérően felvenni, hanem még további egyeneseket is kizár egy-egy ilyen egyeneshármas, azaz ha azokat választanánk másodjára, nem lenne minden új egyenesünk diszjunkt az előzőektől.

Ezeket a kizárt egyeneseket pedig HP és GP alkotják, hiszen ezek korábbi egyenesekhez vezetnének a választás során. Például GP kezdeti egyenessel, a második lépésben E-t visszakapjuk mint metszéspont, és ezáltal $PE = PC$ ismét a választottjaink közé kerülne.
Tehát nem is csak hármasokat, hanem (3+2)-eseket választunk ki ilyen módon.

Így körülbelül ötös (az érintőkkel és hasonló speciális esetekkel nem foglalkozunk, azokat alapból kizárjuk a számolásból, így még erősebb becslést fogunk kapni, hisz azok is fedésbe hozhatják a P' pontot) halmazokra tudtuk osztani az $\mathcal{L}$-en átmenő egyeneseket. Ezekből pedig $q/2$ darab van, valamint P'-t $(q^2 - 1)$ (kúpszelet pontjait illetve P-t leszámítva) módon választhatjuk. Tehát egy tetszőleges $P' \notin \mathcal{L}$ pontra:

$$Pr(P' \text{ nem fedett}) \leq \left(\frac{1}{2}\right)^{q/10}.$$

Annak a valőszínűségét, hogy van olyan P' ami nem fedett, úgy kaphatjuk meg, hogy az összes pontra megköveteljük a nem fedettséget. És mivel az unió valószínűsége kisebb mint az egyes elemeké külön:

$$Pr(\exists\ P' \text{ ami nem fedett}) \leq \sum_{P' \notin \mathcal{L}} Pr(P' \text{ nem fedett}).$$

Ebből pedig:

$$Pr(\exists\ P' \text{ ami nem fedett}) \leq (q^2+q+1-(q+1)-1)\left(\frac{1}{2}\right)^{q/10} = (q^2-1)\left(\frac{1}{2}\right)^{q/10}.$$

Tehát annak a valószínűsége, hogy létezik hozzávehető pont, az az erőszabály miatt 0-hoz fog tartani, azaz az ív majdnem 1 valószínűséggel teljes lesz.

3.2. Tallini Scafati konstrukció

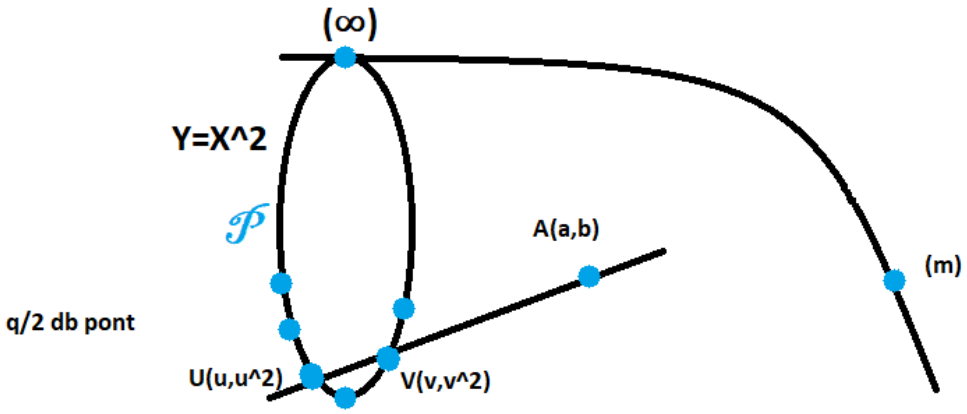
3.2.1. Tétel (Tallini Scafati)**.** Legyen q páros, és legyen $K = \{(x^2+x, (x^2+x)^2) : x \in \mathbb{F}_q\} \cup \{(\infty), (m)\}$, ahol m nem u^2+u alakú. Ekkor K teljes ív lesz PG(2,q)-ban.

Bizonyítás. Belátható, hogy additív részcsoportot alkotnak az x^2+x alakú testelemek, melynek rendje $q/2$. Az $x \to x^2+x$ $\mathbb{F}_q$ felett lineáris leképezés, melynek magja $\{0,1\}$, ami 1-dimenziós altér $\mathbb{F}_q$ fölött. Így a képtér 1 kodimenziós, azaz $q/2$ elemű.

Az (u,u^2) és (v,v^2) pontokat összekötő egyenes meredeksége $u+v$, azaz (m) valóban nincs benne három pontból álló kollineáris halmazban. Tehát K ív.

A továbbiakban ennek teljességének bizonyításával foglalkozunk:

Vegyük a következő ábrát:



4. ábra.

Tehát szeretnénk belátni, hogy K-hoz már nem vehető hozzá egy pont sem, anélkül, hogy keletkezne olyan egyenes, amin 3 pont lenne. Az ideális egyenes pontjait nem kell vizsgálni, hiszen arról már kiválasztottunk 2 pontot $((\infty),(m))$, így a többi nem is jöhet szóba.

Azt kiemelnénk, hogy a $K \setminus \{(m)\}$ ívet sokféleképp tehetjük teljessé, hiszen akármelyik (m) : $m \neq u^2+u$ teljessé teszi.

Vegyünk egy $A(a,b,1)$ pontot a görbén kívül. Tehát erre a pontra $b \neq a^2$. Ezt a későbbiekben mindig feltesszük. Ez akkor lenne az UV-n rajta, ha az 1.3.2 Állításban

szereplő determináns 0 lenne, azaz

$$\begin{vmatrix} u & u^2 & 1 \\ v & v^2 & 1 \\ a & b & 1 \end{vmatrix} = 0.$$

Ezt a determinánst az utolsó sor szerint kifejtve kapjuk a következő egyenletet:

$$a(u^2 - v^2) - b(u - v) + uv^2 - u^2v = a(u + v)(u - v) - b(u - v) + uv(v - u) = 0.$$

Ezt eloszthatjuk $(u - v)$-vel, és helyettesítsük be $u = x^2 + x$ és $v = y^2 + y$-t. Ekkor a következtő egyenlet adódik:

$$C : b + a(x^2 + x + y^2 + y) + (x^2 + x)(y^2 + y) = 0.$$

(Ha ez abszolút irreducibilis, akkor tudnánk a megoldások számát becsülni a Hasse-Weil tétellel, ezért ennek belátása az elsődleges célunk.)
C-t homogenizálva pedig (azaz minden tagot maximális fokúvá teszünk z-k bevezetésével):

$$\hat{C} : bz^4 + ax^2z^2 + axz^3 + ay^2z^2 + ayz^3 + x^2y^2 + xy^2z + x^2yz + xyz^2 = 0.$$

Mik lesznek itt az ideális pontok?

Azokat a legmagasabb fokú x, y-os tagból (x^2y^2) kaphatjuk meg, tehát $x = 0$, vagy $y = 0$ fognak a $z = 0$-hoz tartozni. Azaz $P_1(0, 1, 0)$ és $P_2(1, 0, 0)$ lesznek az ideális pontok. Megvizsgáljuk, hogy ezek szinguláris pontok-e, és teljesülnek-e a Segre-Bartocci tétel feltételei.

Tekintsük $y = 0$ -t ideális egyenesnek, ekkor $P_1 \to (0, 0)$. Tehát, ha most y szerint dehomogenizáljuk:

$$bz^4 + ax^2z^2 + axz^3 + az^2 + az^3 + x^2 + xz + x^2z + xz^2 = 0.$$

Itt nincs elsőfokú tag, de másodfokú igen, tehát $m_{P_1} = 2$. Az érintők meghatározásához vegyük a másodfokúakat: $az^2 + x^2 + xz = 0$. z^2-tel osztva pedig $(\frac{x}{z})^2 + \frac{x}{z} + a = 0$ adódik. Ennek ha egy w gyöke, akkor $w + 1$ is az lesz. (Mert, ha $w^2 + w = a$ és $1^2 + 1 = 0$, akkor $(w+1)^2 + (w+1) = a + 0$, mivel a négyzetreemelés automorfizmus.)

Tehát a két érintő az $x = wz$ és az $x = (w+1)z$. Így az érintők egyszeresek.

Próbáljuk ellenőrizni a Segre kritériumot (2.3.1 Tétel):

1. Lépés: Lehet-e $x = kz$ komponense $\hat{C}$-nek?

Azaz affin koordinátákat használva lehet-e $x = k$ komponense C-nek? (Beírva C egyenletébe, $0 = 0$-t kapunk-e?)

$$b + a(k^2 + k) + ay^2 + ay + (k^2 + k)(y^2 + y) \overset{(?)}{=} 0.$$

Vegyük sorra az együtthatókat:

y^2 együtthatója: $k^2 + k + a = 0 \Rightarrow a = k^2 + k$,

y együtthatója: $k^2 + k + a = 0$ egyezik az előzővel,

az 1 együtthatója: $b + (k^2 + k) = 0 \Rightarrow b = (k^2 + k) = a^2$, azaz A rajta lenne $\mathcal{P}$-n.

2. Lépés: Az e érintő 4 multiplicitással metszi-e C-t P_1-ben?

Legyen $x = wz$, ahol $w^2 + w = a$. A Bézout tételből $|e \cap C| = 4$ multiplicitással számolva. Ezért azt kell ellenőrizni ahhoz, hogy $I(P_1; e \cap C) = 4$ legyen, hogy e csak P_1-ben metszi C-t. Mivel C egyenlete szimmetrikus x-ben és y-ban ugyanez a helyzet P_2-re is, az is 2 multiplicitású szinguláris pont, mint P_1.

Ellenőrizzük, hogy C-nek nincs további szinguláris pontja: Egy ilyen pont csak affin pont lehetne. $f(x, y) = b + a(x^2 + x + y^2 + y) + (x^2 + x)(y^2 + y) = 0$. Számoljuk ki a parciális deriváltakat, ügyelve a 2 karakterisztikára:

$$\frac{\partial f}{\partial x} = a(0 + 1) + 0 + 1(y^2 + y) \to y^2 + y = a,$$

$$\frac{\partial f}{\partial y} = a(0 + 1) + 0 + 1(x^2 + x) \to x^2 + x = a.$$

Ezeket behelyettesítve $f(x, y)$-ba: $b + a(2a)[= 0] + a^2 = 0 \implies b = a^2$. Ezzel ellentmondásra jutottunk, tehát nincs több szinguláris pont.

$I(P_1; e \cap C) = 4 \implies e$ csak P_1-ben metszi C-t. Ez azt jelenti, hogy $\hat{C}$ és $x = wz$ metszéspontja csak P_1. x helyére wz-t helyettesítve:

$$bz^4 + aw^2z^4 + awz^4 + ay^2z^2 + ayz^3 + w^2z^2y^2 + wz^2y^2 + w^2yz^3 + wyz^3 =$$

$$= bz^4 + (aw^2z^4 + awz^4) + (ay^2z^2 + w^2z^2y^2 + wz^2y^2) + (w^2yz^3 + wyz^3 + ayz^3) =$$

[$(w^2 + w = a)$-t használva a zárójelekben, és az azonos tagokat kiejtve]

$$= bz^4 + a^2 z^4 = 0.$$

Ez akkor és csak akkor teljesül, ha $b = a^2$, de akkor $A \in \mathcal{P}$. Vagyis csak $z = 0$ a megoldás, azaz az egyetlen metszéspont P_1.

Azaz $\hat{C}$ abszolút irreducibilis, így lehet használni a Hasse-Weil becslést a megoldások számára: $N \geq q + 1 - 3 \cdot 2 \cdot \sqrt{q} > 0$. Ebből legfeljebb 4 ideális pont kerül levonásra, valamint még lehetne, hogy $U = V$, ekkor $x^2 + x = y^2 + y \implies$ vagy $x + y = 0$ vagy $x + y = 1$. Itt mindkettő 4 megoldást ad, így 12 levonandó pontunk van összesen. Tehát ha q olyan, hogy

$$q + 1 > 6\sqrt{q} + 12,$$

akkor jó lesz. Ez a 2 hatványok közül először $q = 64$-re fog teljesülni.

□

3.3. Lombardo-Radice konstrukciók

Először kimondjuk és belátjuk a tételt $q \equiv 3 \pmod 4$ esetén, majd $q \equiv 1 \pmod 4$ esetben is mutatunk teljes ívet (ami nem kúpszelet).

3.3.1. Tétel (Lombardo-Radice)**.** Legyen $q \equiv 3 \pmod 4$. Legyen $K = \{(x, 1/x) : x = w^2, 0 \neq w \in \mathbb{F}_q\} \cup \{(\infty), (0), (0,0)\}$. Ekkor K teljes ív lesz PG(2,q)-ban.

Bizonyítás. Egy egyenesre csak úgy eshetne 3 pont is, ha azok $(0,0), (u, 1/u), (v, 1/v)$ alakúak, mivel K pontjai 1 kivétellel az $xy = 1$ hiperbolán vannak. Ez viszont azt jelentené, hogy az origóból ezen pontokhoz húzott egyenes meredeksége megegyezik, azaz ha a meredekséghez leosztjuk a második koordinátát az elsővel, $1/u^2 = 1/v^2$ jönne ki. Innen $u^2 = v^2 \implies u = \pm v$. Ha $q \equiv 3 \pmod 4$, akkor -1 nem négyzetelem $\mathbb{F}_q$-ban (1.2.16. Megjegyzés), azaz $u = -v$ nem lehetséges. Ezzel beláttuk, hogy K tényleg egy ívet határoz meg.

Most nézzük meg a teljességet is: Mivel a Tallini Scafati konstrukcióhoz hasonlóan itt sem vehető már ideális pont hozzá az ívhez, elég csak az affin pontokban néznünk. Legyen $A(a, b)$ egy tetszőleges ilyen pont. Ha valamelyik koordinátája A-nak négyzetelem, vagy 0 lenne, akkor könnyen találnánk K-ról 2 vele kollineáris pontot. Például, ha a négyzetelem volna, akkor $(a, 1/a), A$ és (∞) egy egyenesen lennének. Tehát a továbbiakban elég azokkal a pontokkal foglalkoznunk, ahol egyik koordináta sem négyzetelem. Ebben az esetben viszont a/b lesz négyzetelem, mondjuk $a/b = u^2$. Ennek az egyenletnek két megoldása van, u és $-u$, melyek valamelyike, mondjuk u maga is négyzetelem (hiszen -1 nem az). Ez viszont azt jelenti, hogy $(0,0), (u, 1/u)$ és A egy egyenesen van. □

3.3.2. Tétel (Lombardo-Radice)**.** A $q \equiv 1 \pmod 4$ esetben: Legyen most $K = \{(x, 1/x) : x = w^2, 0 \neq w \in \mathbb{F}_q\} \cup \{(\infty), (m)\}$, ahol m nem egy négyzetelem (-1)-szerese. Ekkor K teljes ív.

Bizonyítás. Vegyünk két pontot a hiperboláról: $(x, \frac{1}{x}), (y, \frac{1}{y})$. Ezek egyenesének meredeksége:

$$\frac{\frac{1}{y} - \frac{1}{x}}{y - x} = \frac{-1}{xy}.$$

.

Így, ha $(x, \frac{1}{x})$ és $(y, \frac{1}{y}) \in K$, akkor összekötő egyenesük ideális pontja $(-\frac{1}{xy})$ és itt $-\frac{1}{xy}$ egy négyzetelem (-1)-szerese, azaz nem lehet (m). Ez azt jelenti, hogy K ív.

Teljes ív-e K? Vegyünk egy $A(a, b)$ pontot, ahol $ab \neq 1$. Keresünk olyan $(x, \frac{1}{x}), (y, \frac{1}{y}) \in K$ pontokat, amelyek kollineárisak A-val. Ez mutatja, hogy A nem vehető hozzá K-hoz. Nézzük meg a kollinearitásra vonatkozó determinánst a jelen esetben is:

$$\begin{vmatrix} x & \frac{1}{x} & 1 \\ y & \frac{1}{y} & 1 \\ a & b & 1 \end{vmatrix} = 0.$$

Kifejtve:

$$a(\frac{1}{x} - \frac{1}{y}) - b(x - y) + \frac{x}{y} - \frac{y}{x} = 0.$$

Ezt xy-nal megszorozva, majd $(x - y)$-nal osztva kijön a következő egyenlet: $-a - bxy + x + y = 0$. Vezessük be az $x = u^2$ és $y = v^2$ helyettesítéseket, hiszen K pontjaira $x = w^2$. Azt kapjuk, hogy:

$$C : -a - bu^2v^2 + u^2 + v^2 = 0,$$

és itt az $u, v \neq 0, u \neq v$ megoldásokat keressük. Ezt homogenizálva:

$$-az^4 - bu^2v^2 + u^2z^2 + v^2z^2 = 0.$$

Innentől tegyük fel, hogy $b \neq 0$, erre az esetre a végén visszatérünk.
Ennek az ideális pontjait a $z = 0$ helyettesítéssel kapjuk: ezek $(0, 1, 0)$ és $(1, 0, 0)$.
Második koordináta szerint dehomogenizálva: $(0, 1, 0) \to (0, 0)$ és a $-az^4 - bu^2 + u^2z^2 + z^2 = 0$ affin görbét kell ebben pontban vizsgálni. A legkisebb fokszám 2, tehát 2 multiplicitású szinguláris pont.
Az érintők ebben a pontban: $-bu^2 + z^2 = 0 \to (\frac{z}{u})^2 = b$ egyenletből jönnek.
Alkalmazva a $\beta^2 = b$ helyettesítést(itt $\beta\mathbb{F}_q$ valamely bővítésében van ($\mathbb{F}_{q^2}$-ben)),

$$z = \pm\beta u$$

egyenesek lesznek az érintők a $(0, 1, 0)$ pontban. Az eredeti síkon ezek az $u = \pm\frac{1}{\beta}$ függőleges egyeneseknek felelnek meg. Mivel ez két különböző egyenes, ezért a két érintő egyszeres.

$u = c$ lehet-e komponense a C görbének? (Beírva C egyenletébe, $0 = 0$-t kapunk-e?) Vizsgáljuk meg a behelyettesítés után az együtthatókat:
v^2 együtthatója: $-bc^2 + 1 = 1$,
v együtthatója: 0,
1 együtthatója: $-a + c^2 \implies c^2 = a$ ezt v^2 együtthatójába behelyettesítve $\implies$ $-ab + a = 0$. Tehát A rajta lenne a hiperbolán, ami ellentmondás.
Nézzük meg mi lesz a helyzet $u = \pm\frac{1}{\beta}$-ra. Metszik-e ezek az egyenesek a $(0, 1, 0)$-n kívül máshol is a C görbét? Helyettesítsük be C-be:

$$-a - b\frac{1}{b}v^2 + \frac{1}{b} + v^2 = 0.$$

Ebből a v^2 kiesik, így azt kapjuk, hogy $-a + \frac{1}{b} = 0 \implies ab = 1$, azaz A rajta lenne a hiperbolán. A görbe szimmetrikus u-ra és v-re, így ugyanez a helyzet az $(1, 0, 0)$ ideális pontra.

Lehet-e affin pont szinguláris pont? A parciális deriváltak vizsgálatával az látható, hogy affin szinguláris pont csak $a = 0$ esetén létezhet, amikor még a $(0, 0)$ pont is szinguláris pont.

Így mind az $a = 0$, mind az $a \neq 0$ esetben alkalmazható a Segre-féle kritérium és C és annak projektivizáltja abszolút irreducibilis, így a Tallini Scafati tétel bizonyításának végéhez hasonlóan: $q+1 > 6\sqrt{q}+16$. (A 16 a 3 kizárt egyenes $(u, v \neq 0, u \neq v)$-en a 4-4 pont és a 2 ideális pont 2-2 multiplicitással való esetleges felesleges Hasse-Weil becslésbeli beleszámolása miatt adódik hozzá.) Az $a = 0$ esetben az $u = 0$ illetve a $v = 0$ esetnek megfelelő megoldás csak a $(0, 0)$ pont, vagyis ekkor még kevesebbet kell hozzáadni a reláció jobb oldalához.

Azaz, ha a reláció teljesül, akkor vannak olyan $(u, \frac{1}{u}), (v, \frac{1}{v})$ pontok, amelyek kollineárisak A-val.
Ez 62-nél nagyobb q-kra, azaz a mi esetünkben $q = 67$-re teljesül legkorábban.

Végül vizsgáljuk meg a korábban említett $b = 0$ esetet is. Ekkor a C egyenlet $-a+u^2+v^2 = 0$ lesz. Ez egy másodfokú görbe, melynek ideális pontjai az $u^2+v^2 = 0$ megoldásai. Tehát $u^2 = -v^2$. Ekkor $q \equiv 1(4)$ miatt -1 négyzetelem, vagyis ha $i^2 = -1$, akkor az ideális pontok $(1, i, 0), (1, -i, 0)$. Ezek tehát itt egyszeres (sima) pontok. A C görbe irreducibilis, ha $a \neq 0$, és ekkor $q + 1$ pontja van, amelyből a két ideális pont miatt 2-t, a három kizárt egyenes $(u = 0, v = 0, u = v)$ miatt további 6-ot kell levonni, azaz lesz kollináris ponthármas A-n, ha $q > 7$. Maradt még az az eset, ha $a = b = 0$

Meg kell tehát vizsgálnunk, hogy az origó $O(0,0)$ hozzávehető-e K-hoz.
Nem, hiszen az $E(1,1)$ és a $E'(-1,-1)$ pont is eleme K-nak, mert -1 négyzetelem. De $E, 0, E'$ kollineárisak, azaz O nem vehető hozzá K-hoz.

□

4. További konstrukciók

A Segre-konstrukció (és ennek speciális esetei, a Lombardo-Radice és a Tallini Scafati konstrukciók) mind kúpszeletből, azaz másodfokú görbéből indulnak ki. Természetes ötlet, hogy ne másodfokú, hanem magasabb fokú görbéből próbáljunk kis teljes íveket gyártani.

A harmadfokú görbék esetét részletesebben vizsgálták először Zirilli [10], Szőnyi Tamás [11, 12], Voloch [20, 21], majd újabban Anbar, Bartoli, Giulietti, és Platoni [13, 14, 15, 16]. Ezen a módon az általunk tárgyaltaknál jóval kisebb teljes k-íveket sikerült konstruálniuk, melyekre $k \approx cq^{3/4}$. Emlékeztetőül 2.1.9-ből tudjuk, hogy $k \geq \sqrt{2q}$ teljes k-ívre. A $\sqrt{q}$-s nagyságrend közelébe csak valószínűségi módszerekkel sikerült eljutni. Ezt Kim és Vu [17] tették meg, akik $\leq \sqrt{2q}\log^c q$ méretűteljes ívek létezését mutatták meg. A másik oldalról általában nem ismert, hogy mennyire lehet közel kerülni az oválisok (hiperoválisok) méretéhez. Abban az esetben, ha q négyzet, akkor Fisher, Hirschfeld, Thas [18] és Boros, Szőnyi [19] teljes $(q - \sqrt{q} + 1)$-íveket konstruáltak, PG(2,q)-ban.

A második legnagyobb teljes ív méretére (tehát nem az ovális vagy hiperovális), vonatkozó felső becslések megtalálhatóak [2] 8. fejezetében (8.1.14 és 8.1.15 Tételek).

5. Irodalomjegyzék

[1] Ambrus Gergely és Bérczi Gergely és Csikós Balázs és Frenkel Péter és Gács András és Gyárfás András és Hraskó András és Kiss Emil és Laczkovich Miklós és Lovász László és Montágh Balázs és Moussong Gábor és Pach János és Pelikán József és Recski András és Reiman István és Schmidt Edit és Szőnyi Tamás és Szűcs András és Tóth Géza és Wettl Ferenc : Új matematikai mozaik, Typotex, 2003, ISBN:978-963-9326-41-5, 43.o

[2] Kiss György és Szőnyi Tamás: Véges geometriák, Polygon, 2001, ISSN: 1218-4071

[3] Kiss Emil: Bevezetés az algebrába, Typotex, 2007, ISBN: 978-963-9664-48-7, ISSN:1788-1811

[4] Moussong Gábor : Geometria, Typotex, 2021, ISBN:978-963-279-257-6 Online 8.5 fejezet: Illeszkedési tételek

[5] Csikós Balázs és Kiss György : Projektív geometria, Polygon, 2011, ISSN: 1417-0590

[6] Geometriai halmazrendszerek `https://www.math.u-szeged.hu/~hajnal/courses/MSc_Halmazrendszerek/hrsz98/geo.htm`

[7] Komputergrafika – Matematikai alapok `https://aries.ektf.hu/~hz/pdf-tamop/pdf-01/html/index.html` 4.fejezet

[8] Segre,B.: Ovali e curve o nei piani di Galois di caratteristica due, Atti dell Accad. Naz. Lincei Rend.(8) 32, 1962, 785-790

[9] Szőnyi Tamás: Teljes ívek Galois-geometriákban, Egyetemi doktori értekezés, ELTE, 1984, 2.fejezet

[10] Zirilli, F.: Su una classe di k-archi di un piano di Galois. Atti Accad. Naz. Lincei Rend. 54, 393-397, 1973, MR0358563

[11] Szőnyi, T.: Small complete arcs in Galois planes. Geom. Dedicata. 18(2), 161-172, 1985, MR0792577

[12] Szőnyi, T.: Arcs in cubic curves and 3-independent subsets of abelian groups. In: Combinatorics (Eger, 1987), Colloq. Math. Soc. Jámos Bólyai, vol 52,pp. 499-508, North-Holland, Amsterdam, 1988, MR1221589

[13] Anbar, N., Bartoli, D., Giulietti, M., Platoni, I.: Small complete caps from singular cubics. J. Combin Des., 2013, MR3247026

[14] Anbar, N., Bartoli, D., Giulietti, M., Platoni, I.: Small complete caps from nodal cubics. Arxiv: 1305.3019, MR3247026

[15] Anbar, N., Bartoli, D., Giulietti, M., Platoni, I.: Complete arcs and complete caps from cubics with an isolated double point. Arxiv:1305.3420

[16] Anbar, N., Giulietti, M.: Bicovering arcs and small complete caps from elliptic curves. J. Algebraic Combin. 38, 371-392, 2013, MR3081650

[17] Kim, J.H.(1-MSFT); Vu, V.H. (1-UCSD): Small complete arcs in projective planes., Combinatorica 23 , 2003, no.2, 311-363

[18] J.C. Fisher, J.W.P. Hirschfeld and J.A. Thas: Complete arcs in planes of square order. Annal of Discrete Math, 30, 243-250, 1986, MR0861300

[19] E Boros, T Szőnyi, On the sharpness of a theorem of B. Segre, Combinatorica, 1986, 261-268

[20] Voloch, J.F.: On the completeness of certain plane arcs. European J. Combin. 8, 453-456 , 1987, MR0930181

[21] Voloch, J.F.: On the completeness of certain plane arcs. II. European J. Combin. 11(5), 491-496, 1990, MR1075538

NYILATKOZAT

Név: Khayouti Ádám

ELTE Természettudományi Kar, szak: Matematika BSc

NEPTUN azonosító: S40LAV

Szakdolgozat címe: **Kis teljes ívek**

A szakdolgozat szerzőjeként fegyelmi felelősségem tudatában kijelentem, hogy a dolgozatom önálló szellemi alkotásom, abban a hivatkozások és idézések standard szabályait következetesen alkalmaztam, mások által írt részeket a megfelelő idézés nélkül nem használtam fel.

Budapest, 2023.06.06.

Khayouti Ádám

a hallgató aláírása