

Opponensi Vélemény

Sziklai Péter: Applications of Polynomials over Finite Fields című MTA-doktori értekezéséről

A *Galois geometriák*, azaz a véges testek feletti projektív síkok és terek geometriája, a matematika igen fontos és napjainkban is erőteljesen vizsgált ága annak köszönhetően, hogy ilyen terekbe beágyazható alakzatok és konfigurációk gyakran jelentős kombinatorikai, számelméleti, csoportelméleti és algebrai geometriai fogalmakkal és tételekkel állnak szoros kapcsolatban. Ez egyrészt jelentősen hozzájárul a mondott szakterületek bizonyos témaköreinek kidolgozásához, másrészt lehetőséget nyújt szélesebb eszköztár és mély eredmények alkalmazására a Galois-geometriák tanulmányozásában. Ennek megfelelően, a Galois-geometriák (általánosabban a véges geometriák) kutatása több irányban folyik, és jellege folytán fontos gyakorlati, elsősorban kódelméleti és kriptográfiai alkalmazásai is vannak.

A magyar kombinatorikai iskola szellemében, Sziklai Péter tudományos munkája a Galois-geometriák olyan érdekes alakzataira irányul, melyek bizonyos tulajdonságra nézve extrémálisak. Ilyenek például a legkisebb méretű k -lefogó ponthalmazok (k -blocking sets), melyek minden k -kodimenziós alteret metszenek, a minden egyenest legfeljebb n pontban metsző síkbeli ponthalmazok (ívek), vagy olyanok amelyeknél az egyenesekkel való metszésszám csak néhány előírt értéket vehet fel, továbbá a kevés irányt lefogó affin ponthalmazok, valamint a Galois-sík legtöbb pontot tartalmazó adott fokú irreducibilis síkgörbéi. Jól ismert, hogy a Galois geometriák mélyebbnek bizonyult tételei majdnem mindig érvényüket veszítik általános (nem test feletti) véges projektív síkokon és magasabb dimenziós projektív tereknél alig gyengébb véges geometriákban. Módszertani szempontból ez azzal a következménnyel jár, hogy a Galois geometriák kutatásában a leszámlálási eljárások önmagukban nem elégségesek, hiszen az ilyen tisztán kombinatorikus bizonyítások minden további nélkül átvihetők lennének az általánosabb esetekre, de ott az eredmények már nem érvényesek. Erre világít rá Beniamino Segre 1955-ben publikált híres tétele és annak bizonyítása. Galois síkon, nagyfokú szabályosággal rendelkező ponthalmazok létezése véges testek speciális tulajdonságainak a függvénye, és a Segre módszer ilyen, gyakran a test karakterisztikájától erősen függő, tulajdonságok felkutatására lehet alkalmazni.

Több mint húsz évvel ezelőtt, a véges geometriák két kiváló tudósa, Aart Blokhuis és Szőnyi Tamás észrevették, hogy a leszámlálási módszer Galois-geometriákbeli “fogyatékoságát” ki lehet küszöbölni a Galois sík lefogó pontthalmazainak a vizsgálatában egy alapvetően új algebrai módszer alkalmazásával. A módszer lényege abban áll, hogy Galois síkon, adott pontthalmaz egyenesekkel való metszési viselkedése egy alkalmas véges test feletti kétváltozós polinommal jól leírható. Ezt a kétváltozós polinomot Rédei polinomnak szokás hívni, mert több lefogó pontthalmazra és irányokra vonatkozó idevágó eredményt Rédei László hézagos polinomokról szóló könyve inspirálta. Ez a ún. polinomos módszer Galois terekben is nagyon hasznosnak bizonyul, amikor többváltozós Rédei polinomok segítségével az egyenesekre vonatkozó eredményeket hipersíkokra általánosítjuk.

A Rédei polinomok elméletét Szőnyi Tamás és tanítványai dolgozták ki az elmúlt két évtizedben a tárgykör más jelentős nemzetközi kutatóival (Simeon Ball, Aart Blokhuis, Leo Storme) szorosan együttműködve. Ebben a közös kutatómunkában, Sziklai Péter alapvető eredményeivel főszerepet játszott. Disszertációja e témakörrel készülő monográfiájának részletes összefoglalója.

A szokott módon, a disszertáció első fejezeteiben a szerző a témakörre vonatkozó alapismereteket összegzi és idézi, főképpen a véges testek felett definiált polinomok és algebrai síkgörbék elméletéből. Sajátos egyéni stílusában bevezeti a Rédei polinomokat, tárgyalja ezek elemi tulajdonságait. Kiemeli, hogy $p > 0$ karakterisztikájú test felett, egy nem-konstans polinom p -edik (parciális) deriváltja eltűnhet, ami miatt fontos információk elveszhetnek. Helyesen rámutat arra, hogy ez a veszély a Hasse-féle derivált használatával megszüntethető, és ezt a véges testek feletti algebrai görbék egyik alapvető eredményén, a Stöhr-Voloch tételen illusztrálja. Már a disszertáció e részében is találunk a szerzőtől származó érdekesebb eredményeket, melyek a későbbi fejezetekben további eredményekkel kombinálva jelentős szerephez jutnak. Ez különösen a 9. fejezet eredményeire igaz, ahol tulajdonképpen egy a későbbiekben gyakran előforduló bizonyítási ötletet bocsát előre a szerző.

Sziklai Péter tudományos munkájának sokoldalúságát jól bizonyítja a 8. fejezetben szereplő becslése és az ebből adódó Sziklai-sejtés néven ismert probléma tudományos viszhangja. Szellemes leszámolási módszerrel a q -adrendű véges test felett definiált algebrai sík görbék pont-

jainak számát felülről megbecsülte. Ha a görbe n -ed fokú és nem tartalmaz a test felett lineáris komponenseket, ez a korlát $(n-1)q+n = (n-1)q+1+(n-2)/2$. Sziklai sejtése ennél valamivel többet állít, mégpedig azt, hogy $(n-2)/2$ elhagyható. E sejtést nemrég Homma és Kim bebizonyították, és az idevágó extrémális görbéket is megadták. Sziklai kétségtelen érdeme annak megmutatása, hogy kombinatorikus okoskodással érdemes próbálkozni még olyan témakörben is, melyben mélyebb eredményeket eddigieken csak az algebrai számelmélet (zéta függvény), a függvénytestek elmélete, és a pozitív karakterisztikájú test feletti algebrai geometria legsúlyosabb eszközeivel értek el. Ezek az eszközök jól láthatók a disszertációban is idézett híres Hasse-Weil tétel (ami a véges test feletti Riemann sejtés) André Weil-től és Enrico Bombieri-től származó bizonyításában.

A 10. fejezet Vandermonde- és szuper-Vandermonde-halmazokkal foglalkozik (ld. 10.4 definíció). Szemléletesen ezek véges test olyan T részhalmazai, melyeknek összege, négyzetösszege, ... k -adik hatványösszege 0. Vandermonde-halmazokra ez a k ($|T|-2$)-ig, szuper-Vandermonde-halmazokra ($|T|-1$)-ig mehet. A dolgozatban ilyen halmazokra nevezetes példákat találunk, melyek additív és multiplikatív részcsoporthokból, oválisokból és hiperoválisokból kaphatók. Meglepő és szép eredmény, hogy mind a kicsi ($< p$ elemű), mind a nagy ($> q/p$ elemű) szuper-Vandermonde-halmazok pontosan leírhatók: ezek multiplikatív részcsoporthok transzformáltjai. Ugyancsak kiemelem, hogy a 10.4 szakasz $PG(2, q)$ olyan részhalmazainak méretére ad alsó becslést, amelyeket minden egyenes 0 modulo r pontban metsz. A szerzők megmutatják, hogy egy ilyen hamaznak legalább $(r-1)q + (p-1)r$ pontja van, ahol p az alaptest karakterisztikája. Fontos megjegyezni, hogy Barlotti klasszikus eredménye szerint egy ún. (k, r) -ívnek legfeljebb $k \leq (r-1)q + r$ pontja van, és egyenlőség esetén a halmazt minden egyenes 0 vagy r pontban metszi (ezeket szokták maximális ívnek nevezni). Így a fenti alsó becslésből páratlan rendű Galois-síkokra azonnal következik Ball-Blokhuis-Mazzocca híres eredménye maximális ívek nemlétezéséről. A fejezet mindkét részében véges testek feletti polinomok mesteri alkalmazása kellett a tételek belátásához.

A 11. fejezet lefogó ponthalmazokról szól, tulajdonképpen az itt tárgyalt eredmények motiválják a szerzőtől származó *linearitási sejtést*, mely szerint minden minimális, kis lefogó ponthalmaz lineáris $GF(q)$ alkalmas részteste felett. A sejtés igazolásában a szerző jutott legmesszebb-

bre, a fejezetben részletesen láthatunk a megoldásra tett több kísérletet is. Ezekkel vagy korábbi eredményeket lehet rövidebben belátni, vagy még teljesen fel nem tárt új tulajdonságait mutatják a kis lefogó pontthalmazoknak és a hozzájuk rendelt görbéknek. A Rédei-polinom homogén koordinátákkal felírt változatának vizsgálatával három olyan görbét lehet hozzárendelni a pontthalmazhoz, amelyeknek nagyjából azonosak a $\text{GF}(q)$ -racionális pontjaik, pedig nincs közös komponensük (sőt, triviális eseteket leszámítva, semelyik kettőnek sincs, ld. 11.19 Lemma). Ezen görbéket vizsgálva Sziklai Péter lényegesen továbbfejleszti Szőnyi 1 modulo p -s tételét. Megmutatja, hogy minden egyenes 1 modulo p^e pontban metszi a minimális lefogó pontthalmazt, méghozzá olyan e -re, amelyre e osztja h -t, ahol $q = p^h$. Ráadásul az is adódik a szellemes bizonyításból, hogy ha egy egyenes pontosan $p^e + 1$ pontban metszi a minimális lefogó pontthalmazt, akkor ezek a pontok egy $\text{PG}(1, p^e)$ részegyenest alkotnak. Ez a fontos eredmény valós esélyt ad arra, hogy a linearitási sejtést be lehessen látni.

A 12. fejezet magasabb dimenziós terek lineáris pontthalmazaival és az $(n - k)$ -dimenziós altereket lefogó Rédei típusú lefogó pontthalmazokkal foglalkozik. Ebben a fejezetben az algebrai módszer helyett a geometriai, kombinatorikai érvelések kifinomult alkalmazásán van a hangsúly. Szemléletesen a fejezet fő kérdése az, hogy egy kevés irányt meghatározó pontthalmaz mikor áll elő alacsonyabb dimenziós hasonló tulajdonságú halmazra emelt kúpként. (A fordított irány a kevés irányt meghatározó halmazok "triviális" konstrukciója.) A 12.15 Tétel erre a kérdésre ad lényegében éles választ, az élességet a 12.16. Állítás mutatja. Ha a dimenzió elég nagy (itt a nagy k -tól és a $q = p^h$ -beli h -tól függő értéket jelent), akkor minden kevés irányt meghatározó q^k pontú pontthalmaz kúp. Azt is kiemelhetjük, hogy a pontthalmaz méretére adott korlát jobb, mint a kis k -lefogó pontthalmazok vizsgálatánál általában szokásos korlát.

A 13. fejezetben stabilitási jellegű eredményeket találunk. Ízelítőül a három dimenziós tér másodrendű kúpjának diszjunkt kúpszeletekkel való befedését (az angol nyelvű szakirodalomban ezeket flock néven szokták említeni). Egy ilyen kúp (csúcspontját kivéve) nagyon egyszerűen lefedhető diszjunkt kúpszeletekkel, elég az egy a kúphoz kitérő egyenesen átmenő síkokra által kimetszett kúpszeletekre gondoljunk (ezt a nagyon egyszerű példát lineárisnak szokás nevezni). Léteznek nem lineáris flock-ok is, ezekből nem-desarguesiani tranzlációs síkokat lehet

szerkeszteni. Tanulmányozásuk ma is a véges geometriák fontos és sokat vizsgált témaköre. Segre ívekre vonatkozó beágyazási kérdésének megfelelője flock-okra az, hogy ha q -nál kicsivel kevesebb diszjunkt kúpszelet van adva (ezt partial flock-nak szokták hívni), akkor vajon ki tudjuk-e egészíteni ezt befedéssé (flock-ká) további kúpszeletek hozzávételével. A 13.4 Tétel ezt igazolja, ha a "hiányzó" kúpszeletek száma kisebb, mint kb. $\sqrt{q}/4$. Különösen szép az eredményben (ill. a bizonyításban) az, hogy Segre eredeti (ívek beágyazhatóságáról szóló) bizonyításához hasonlóan itt is az algebrai görbék jelentik a fő feagyvert. Ugyanakkor az a mód, ahogy a görbéket hozzárendeli a szerző a részleges befedéshez, lényegesen különbözik Segre módszerétől. Korábban Storme és Thas a q páros esetben síkbeli íveket tudott a partial flock-okhoz hozzárendelni, így közvetlenül tudták Segre beágyazási tételét alkalmazni. A fejezet későbbi részeiben az eredményt másodrendű kúpokról bizonyos magasabb rendű síkgörbékre emelt kúpokra is sikerrel kiterjeszti Sziklai Péter, számos technikai nehézséget leküzdve.

A 14. fejezet irányok számáról szóló stabilitási kérdéseket vizsgál. Többek között a 12. fejezet, valamint Ball és Lavrauw munkái alapján viszonylag sokat tudunk n dimenziós tér q^{n-1} elemű pontthalmaza által meghatározott irányokról. A fejezet fő kérdése az, hogy ha (az egyszerűség kedvéért a három dimenziós esetre fogalmazva meg) $q^2 - \varepsilon$ pont nem határoz meg majdnem minden irányt, akkor vajon kiegészíthető-e ugyanezen irányokat meghatározó q^2 pontú halmazzá. Sziklai Péter Rédei-polinomok és algebrai geometriai módszerek eredeti és mély alkalmazásával belátja az alábbi 14.13. Tételt: Ha $\varepsilon < p$, $q = p^h$, és az U halmaz, melyre $|U| = q^2 - \varepsilon$, nem egészíthető ki q^2 pontú, ugyanezen irányokat meghatározó pontthalmazzá, akkor a nem-meghatározott irányok egy $(\varepsilon^4 - \varepsilon^3 + \varepsilon)$ -rendű síkgörbében vannak. Ha tehát ε tényleg kicsi (mondjuk $< \log q$), akkor a nem-meghatározott irányok száma legfeljebb $q(\log q)^4$, azaz sokkal kevesebb, mint az összes irányok száma (ami kb. q^2). Természetesen, magasabb dimenzióban kevésbé lehet az U méretét csökkenteni, mindazonáltal a konklúzió erősebb: ha U nem bővíthető ugyanezen irányokat meghatározó halmazzá, akkor a nem-meghatározott irányokat egy egyenes vagy egy kúpszelet tartalmazza (a részletekért ld. a 14.12 Tételt). Ezek az eredmények bizonyos $T_2^*(K)$ típusú parciális geometriák ovoidjaira vonatkozó beágyazási eredményeket is adnak, amikor K hiperovális vagy maximális ív.

A 15. fejezet az irányprobléma egy jól ismert, Ball - Gács - Sziklai szerzőhármastól származó általánosításával foglalkozik. A korábbi technikákat jelentősen továbbfejlesztve, az idevágó ismert eredményeket a szerzőnek sikerül megjavítania.

Összefoglalva: A 10-14. fejezet a szerző számos, nemzetközileg is elismert és kiválónak tartott, alapvetően új tudományos eredményeit tartalmazza: Ezek az eredmények a következők:

- nagy szuper-Vandermonde halmazok osztályozása,
- minimális kis lefogó halmazok linearitási tulajdonságok útján való jellemzése,
- kevés irányt meghatározó affin ponthalmazok stabilitása,
- hipersíknál kisebb méretű affin ponthalmazoktól független irányok geometriájának a leírása.

A következő kérdést fogalmazom meg:

A disszertációban bevezett és sikerrel használt algebrai eszközöket, majdnem teljes egészében, a véges geometriák dolgozták ki, Rédei László vizsgálatait folytatva. Vajon mi annak az oka, hogy a disszertáció több témakörében a véges test feletti algebrai görbékre vonatkozó mélyebb eredmények, a Hasse-Weil tétel, a Stöhr-Voloch korlát és a zéta függvény, csak kevés szerephez jutottak?

Sziklai Péter akadémiai doktori disszertációja a véges geometriák kombinatorikájának legfontosabb és legmélyebb kérdéseiben, a polinomos módszerrel elért eredményeit foglalja össze. Ezek az eredmények igen jelentősek, a nemzetközi szakmai tudományos közvélemény által jól ismertek és igen magasra értékelték. Ennek alapján megállapítható, hogy Sziklai Péter a véges geometriák nemzetközi szinten is kiemelkedő szakembere. Javasolom az akadémiai doktori fokozat megszerzésére vonatkozó nyilvános vita kitűzését és Sziklai Péter számára az MTA doktora fokozat megadását.

Potenza 2014. február 12.

Korchmáros Gábor
MTA doktor