Általánosított diagonális egyenletek megoldhatósága véges testek felett

Felszeghy Bálint

TDK dolgozat

Konzulens: Dr. Rónyai Lajos

Kivonat

Dolgozatom témája az algebra – különösen az algebrai geometria – egy központi kérdése: véges test feletti többváltozós polinomok gyökének létezésére szeretnék jó elégséges feltételt bizonyítani. A bevezetésben összekötöm e kérdést egyenletek megoldhatóságával, és bemutatom a feladat számelméleti megfogalmazását.

A 2. fejezetben ismertetem egy polinom rangjának fogalmát, majd erre adok egy – a rang kiszámítását lényegesen megkönnyítő – ekvivalens jellemzést. A fejezet további részében Rédei sejtésével foglalkozom, amely a rang segítségével ad elégséges feltételt polinom nullhelyének létezésére, bár teljes általánosságban sajnos nem igaz. A sejtés kimondása után e fejezetben tárgyalt állítások és a cáfolat nem saját eredményeim, a hivatkozott irodalomban fellelhetőek.

Egy speciális polinomosztályra, az úgynevezett általánosított diagonális polinomokra vizsgálom a Rédei sejtést a 3. részben. A rang előbb említett ekvivalens állítása felhasználásával bizonyítom, hogy egy általánosított diagonális polinom rangja a változószámával egyezik meg. A véges test elemszámára vonatkozó feltétel mellett igazolom Rédei sejtését. Általános prímtestre a sejtés feltételén kicsit módosítva tudom bebizonyítani azt.

Végül felvetem a korábban szereplő polinomosztályok két lehetséges általánosítását. Vázolom egy elképzelésemet, amely segítségével úgy gondolom, hogy igazolható lesz a gyök létezésére vonatkozó kritérium ezen osztályokra is.

1. Bevezetés

Az egyenletek megoldhatósága a matematika egyik legrégebben felmerült kérdése, mind elméleti, mind gyakorlati szempontból központi jelentőségű. Egyebek mellett a hagyományos számfogalom kiterjesztéséhez is elvezetett. Az ember az őt körülvevő világ megfigyeléséből magától értetődő módon absztrahálta a pozitív egész számok fogalmát. A sorban ezután következett a 0 és a negatív egészek, a racionális számok, majd a geometria fejlődésével az irracionális számok. Utóbbiak közül elsőként az az ismert kérdés vetődött fel, hogy milyen hosszú egy egységoldalú négyzet átlója, azaz mi lehet az $x^2 - 2 = 0$ egyenlet gyöke. A komplex számok bevezetése szintén természetes módon kötődik egyenletek megoldásához. Igaz az, hogy ez utóbbi számkörben tetszőleges polinomiális egyenlet megoldható.

A modern algebra általánosságban vizsgálja a fenti típusú kérdéseket. A számfogalom általánosításaként bevezethető a test fogalma. Dolgozatomban véges testek felett értelmezett egyenletekkel fogunk foglalkozni, azaz az ismeretlenek mellé egy véges halmazból választjuk a számokat, és megoldást is ezek közül keresünk. Ismert, hogy tetszőleges q prímhatványhoz létezik q elemszámú test, sőt ez izomorfia erejéig egyértelmű. Interpolációval könnyű igazolni, hogy egy véges testet önmagába képező (akárhány változós) függvény polinommal reprezentálható. Nem jelenti tehát az általánosság megszorítását, hogy a továbbiakban egyenlet megoldása alatt polinom gyökét fogjuk érteni. Egyéb véges testekkel kapcsolatos alapvető tételeket ezentúl hivatkozás nélkül fogunk használni, ezek többek között [1]-ben megtalálhatóak.

Legyen p egy prím és a p elemű test $\mathbb{F}_p$. Ekkor $\mathbb{F}_p$ elemeinek tekinthetjük a modulo p maradékosztályokat, és így az egyenlet megoldása a klasszikus számelmélet nyelvén megfogalmazható probléma. Adott egy egészegyütthatós (többváltozós) $F(x_1, \ldots, x_n)$ polinom, kérdés, hogy vannak-e olyan $a_1, \ldots, a_n$ egész számok, amelyekre $F(a_1, \ldots, a_n)$ osztható p-vel.

Természetes módon merül fel polinomok nullhelyeinek problémája az algebrai geometriában is, ahol görbék, felületek, hiperfelületek megadására valamilyen F polinommal az $F(x_1, \ldots, x_n) = 0$ egyenletet használják. Ezek vizsgálatához elengedhetetlen tudni, hogy létezik-e egyáltalán pontja a szóban forgó hiperfelületnek ${\mathbb{F}_p}^n$-ben.

2. Rédei sejtése

1946-ban megjelent [2] cikkében Rédei László megfogalmazott egy sejtést prímrendű testek feletti többváltozós polinomok gyökeinek létezéséről. Noha nemrégiben kiderült, hogy a sejtés teljes általánosságban nem igaz, sok fontos

polinomosztályra bizonyítottan megállja a helyét. A következőkben a rang definíciója és jellemzése után bemutatom a sejtést és rövid áttekintést adok a téma már ismert eredményeiről, az ellenpéldáról és egy szép polinomosztályról, amelyre a sejtés igazolható.

Dolgozatomban p végig egy prímszámot fog jelölni, $\mathbb{F}_p$ a p elemű testet, $\mathbb{F}_p[x_1, \ldots, x_n]$ az $\mathbb{F}_p$-ből vett együtthatókkal képzett n változós polinomok gyűrűjét, $F(x_1, \ldots, x_n) \in \mathbb{F}_p[x_1, \ldots, x_n]$ esetén pedig $\deg F$ az F polinom fokát. Az F-et *redukált*nak hívjuk, ha tetszőleges x_i változójában a foka legfeljebb $p-1$. Felhasználva a Kis Fermat tételt – amely szerint $x_i^p \equiv x_i \pmod{p}$ – minden polinom helyettesíthető egy redukált polinommal anékül, hogy helyettesítési értéke bárhol megváltozna. Rédei sejtésének megfogalmazásához szükségünk van egy redukált polinom *rang*jának fogalmára.

Legyen $F(x_1, \ldots, x_n) \in \mathbb{F}_p[x_1, \ldots, x_n]$. Ekkor $\operatorname{rang} F$ az a legkisebb r egész szám, amelyre igaz, hogy F invertálható homogén lineáris változócserével r változóssá tehető.

Rédei eredeti definíciója szemléletes, azt ragadja meg, hogy „lényegében" hány változós F. A következő tétel viszont általános módszert ad a rang meghatározására.

Egy F redukált polinom x_i változója szerinti $\frac{\partial F}{\partial x_i}$ deriváltja topológia bevezetése nélkül is értelmezhető: legyen egyenlő a polinomok jól ismert deriválási szabálya alapján kapott polinommal. Az $\mathbb{F}_p[x_1, \ldots, x_n]$ additív struktúrája tekinthető $\mathbb{F}_p$ feletti vektortérnek. Értelmes ezért $\frac{\partial F}{\partial x_i}$ $(1 \leq i \leq n)$ vektorsorozat rangjáról, azaz közülük az $\mathbb{F}_p$ felett lineárisan függetlenek maximális számáról beszélni.

2.1. tétel. *Ha* $F(x_1, \ldots, x_n) \in \mathbb{F}_p[x_1, \ldots, x_n]$, *akkor*

$$\operatorname{rang} F = \operatorname{rang} \left\{ \frac{\partial F}{\partial x_i} \ : \ 1 \leq i \leq n \right\}.$$

A rang ezen ekvivalens jellemzését egymástól függetlenül Rónyai Lajos és én is megtaláltuk, itt saját bizonyításomat közlöm.

Bizonyítás: Az $F(x_1, \ldots, x_n)$ polinomot, mint $F(\boldsymbol{x})$ skalár-vektor függvényt fogjuk tekinteni. Jelölje $\nabla G(\boldsymbol{x})$ a G $\boldsymbol{x}$ helyen vett parciális deriváltjaiból álló sorvektort.

Legyen A egy $n \times n$-es $\mathbb{F}_p$ elemű invertálható mátrix és vezessük be a következő jelölést: $F_A(\boldsymbol{x}) := F(A\boldsymbol{x})$. A rang definíciója szerint, ha $r = \operatorname{rang} F$, akkor van olyan invertálható A mátrix, amelyre F_A csak r változójától függ. Tegyük fel ezért, hogy A ez a mátrix és F_A nem függ x_{r+1}, x_{r+2}, $\ldots$, x_n változóitól. Egy redukált polinom x_i szerinti deriválja pontosan akkor azonosan 0, ha a polinom konstans x_i-ben, tehát most $\frac{\partial F_A}{\partial x_{r+1}} = \cdots = \frac{\partial F_A}{\partial x_n} = 0$.

A láncszabály értelmében $\nabla F_A(\boldsymbol{x}) = \nabla F(A\boldsymbol{x}) \cdot A$, avagy $\boldsymbol{x}$ helyébe $A^{-1}\boldsymbol{x}$-et téve: $\nabla F_A(A^{-1}\boldsymbol{x}) = \nabla F(\boldsymbol{x}) \cdot A$.

Ha $V = \left\{ \boldsymbol{a} \in {\mathbb{F}_p}^n \mid \nabla F(\boldsymbol{x}) \cdot \boldsymbol{a} = 0 \right\}$, akkor $n - r = \dim V$, mert A utolsó $n - r$ oszlopa eleme V-nek és ezek lineárisan függetlenek; ugyanakkor, ha $n - r$-nél több (legyen s) lineárisan független $\boldsymbol{a}$ eleme volna V-nek, akkor ez az s oszlop kiegészíthető volna egy olyan invertálható A' mátrixszá, amelyre $F_{A'}$-nak (legalább) s parciálisa 0, tehát $F_{A'}$ kevesebb, mint r változójától függne csak.

Másrészt jelölje $\operatorname{rang} \nabla F$ a tételben szereplő $\operatorname{rang} \left\{ \frac{\partial F}{\partial x_i} \ : \ 1 \leq i \leq n \right\}$ számot. Így $\dim V = n - \operatorname{rang} \nabla F$, ugyanis, ha például $\frac{\partial F}{\partial x_i}$ $(1 \leq i \leq \operatorname{rang} \nabla F)$ lineárisan függetlenek, akkor $\boldsymbol{a} \in V$-nek a $\operatorname{rang} \nabla F + 1 \leq i \leq n$ komponensei tetszőlegesen választhatóak, hozzájuk az első $\operatorname{rang} \nabla F$ koordináta egyértelműen adódik.

Azt kaptuk tehát, hogy $n - r = \dim V = n - \operatorname{rang} \nabla F$, amiből adódik az állítás.

□

Rédei sejtése ezek után a következő:

2.2. sejtés. [RÉDEI] *Legyen* $F(x_1, \ldots, x_n) \in \mathbb{F}_p[x_1, \ldots, x_n]$, *nem konstans redukált polinom. Ha* $\deg F \leq \operatorname{rang} F$, *akkor* F*-nek van gyöke* ${\mathbb{F}_p}^n$*-ben.*

A már idézett [3] cikkében Rónyai ellenpéldát adott a sejtésre. Ezt a részletek pontos igazolása nélkül mutatom be.

Legyen $p \geq 5$ és $c \in \mathbb{F}_p$ kvadratikus nem-maradék, azaz olyan szám, amelyik nem áll elő, mint $\mathbb{F}_p$ valamely elemének négyzete. Ismert, hogy $p \geq 3$ esetén $\frac{p-1}{2}$ ilyen elem van $\mathbb{F}_p$-ben. Az

$$F(x_1, \ldots, x_n) = \left(\sum_{i=1}^{n} x_i^2 \right)^2 - c$$

definícióval láthatóan F olyan polinom, amelynek nincs gyöke ${\mathbb{F}_p}^n$-ben és $\deg F = 4$. Mivel $p \geq 5$, így F redukált is, és a 2.1. tétel használatával könnyedén igazolható $\operatorname{rang} F = n$. Tehát $n \geq 4$ esetén ez ellenpélda Rédei sejtésére. Amennyiben $p = 3$, egy hasonló jellegű redukált polinom konstruálható, amely szintén cáfolja a sejtést.

Triviálisan igaz viszont Rédei állítása a $p = 2$ esetre, hiszen egy $\mathbb{F}_2$ feletti redukált polinom minden változójában lineáris, az ilyen nem konstans polinomok pedig nyilván felveszik a 0-t.

A fenti F-et kicsit módosítva tetszőleges $d \geq 6$ fokú ellenpéldát kaphatunk. A $d = 3$ és 5 esetek még nyitottak. Ha $d = 2$, akkor a sejtés megint

igaz. Megfelelő változócsere után ugyanis feltehető, hogy F majdnem diagonális, azaz

$$\sum_{i=1}^{n} a_i x_i^2 + \sum_{i=1}^{n} b_i x_i + c$$

alakú, ahol $a_i, b_i, c \in \mathbb{F}_p$. Az ilyen típusú polinomokról a későbbiekben – jóval általánosabban – belátjuk, hogy létezik nullhelyük, ha $n \geq 2$.

A sejtés helyzete általános polinomokra tehát az alábbi táblázatban foglalható össze:

$\deg F$	$p = 2$	$3 \leq p$
1, 2	igaz	igaz
3, 5	igaz	nyitott
4, 6 $\leq$	igaz	nem igaz

Mostantól speciális polinomosztályokat fogunk tekinteni. *Diagonális*nak nevezzük az

$$F(x_1, \ldots, x_n) = \sum_{i=1}^{n} a_i x_i^{k_i}$$

alakú polinomokat, ahol k_i pozitív egész, $a_i \in \mathbb{F}_p$ és $a_1 a_2 \ldots a_n \neq 0$. Az érdekes kérdés ezekre természetesen $F(x_1, \ldots, x_n) + c = 0$ megoldhatósága, ahol $c \in \mathbb{F}_p$. E polinomosztály viszonylag könnyen kezelhető, a gyök létezéséhez jó kritériumok ismertek, sőt a szakirodalomban több cikk található, amely a megoldások számával foglalkozik, ilyen például [6].

Rónyai eredménye a következő:

2.3. tétel. *Legyen*

$$F(x_1, \ldots, x_n) = \sum_{i=1}^{n} f_i(x_i) \ ,$$

ahol $f_i \in \mathbb{F}_p[x_i]$ *és* $1 \leq \deg f_i \leq p-1$. *Ekkor a* $\deg F \leq \operatorname{rang} F$ *elégséges feltétel* $F(x_1, \ldots, x_n) = 0$ *egyenlet megoldhatóságához.*

A fenti alakú F polinomokkal definiált $F(x_1, \ldots, x_n) = 0$ egyenletek a *majdnem diagonális egyenlet*ek. Nyilvánvaló a 2.1. tételből, hogy ha semelyik f_i nem lineáris, akkor $\operatorname{rang} F = n$. A tétel szerint tehát Rédei sejtése igaz majdnem diagonális egyenletekre ([3]-ban ezek megtalálhatóak).

3. Általánosított diagonális egyenletek

A 2.3. tétel általánosítása felé teszünk lépéseket ebben a szakaszban. Egy $F(x_1,\dots,x_n) \in \mathbb{F}_p[x_1,\dots,x_n]$ polinomot *általánosított diagonális polinomnak* nevezünk, ha

$$F(x_1,\dots,x_n) = \sum_{i=1}^{n} x_i^k + g(x_1,\dots,x_n) \ ,$$

ahol $1 \le k \le p-1$ és $g(x_1,\dots,x_n) \in \mathbb{F}_p[x_1,\dots,x_n]$ tetszőleges k-nál kisebb fokú polinom.

Vizsgáljuk meg, hogy mit állít Rédei sejtése általánosított diagonális polinomokról!

3.1. tétel. *Ha* $k=1$, *akkor* $\operatorname{rang} F = 1$. *Egyébként* $\operatorname{rang} F = n$.

Bizonyítás: A $k=1$ eset nyilvánvaló. Legyen ezért $k \ge 2$ és

$$F_i(x_1,\dots,x_n) := \frac{\partial F}{\partial x_i}(x_1,\dots,x_n) = kx_i^{k-1} + \frac{\partial g}{\partial x_i}(x_1,\dots,x_n)$$

Tegyük fel, hogy vannak olyan $\alpha_i \in \mathbb{F}_p$ számok, hogy

$$G(x_1,\dots,x_n) := \sum_{i=1}^{n} \alpha_i F_i(x_1,\dots,x_n) = 0$$

fennáll minden $(x_1,\dots,x_n) \in {\mathbb{F}_p}^n$ esetén. Egy rögzített j-re G tekinthető x_j egyváltozós $G_j(x_j)$ polinomjának ($\mathbb{F}_p(x_1,\dots,x_{j-1},x_{j+1},\dots,x_n)$ felett). Miután $\deg G_j \le p-1$, ezért azonosan 0 csak úgy lehet, ha x_j^l minden együtthatója 0. Tudjuk, hogy $\deg \frac{\partial g}{\partial x_i} < k-1$, ezért x_j^{k-1} együtthatója $\alpha_j k$. Igazoltuk tehát, hogy minden j-re $\alpha_j = 0$, ami azt jelenti, hogy az F_i-k lineárisan függetlenek, így a 2.1. tétel szerint $\operatorname{rang} F = n$.

□

A $k=1$ esettel a továbbiakban nem foglalkozunk. Figyelembe véve az előző tételt, a 2.2. sejtés most azt állítja, hogy amennyiben $n \ge k$, úgy az általánosított diagonális polinomnak van gyöke ${\mathbb{F}_p}^n$-ben. A 3.2. tételben kimondandó alsó korlátot tudom bizonyítani n-re a sejtés szerinti k helyett. Előbb azonban megmutatjuk, hogy a Rédei-sejtés másik iránya éles, azaz definiálunk polinomokat, amelyekre $n < k$ és nincsen gyökük.

Legyen $k = p-1$ és $g(x_1,\dots,x_n) = 1$, azaz

$$F(x_1,\dots,x_n) = \sum_{i=1}^{n} x_i^{p-1} + 1 \ .$$

Miután $x_i^{p-1} = 0$, vagy 1 minden x_i-re, ezért összegük legfeljebb n, F értékkészlete pedig $\{1, 2, \ldots, n+1\}$, ami $n+1 < k+1 = p$ miatt nem tartalmazza a 0-t.

Hasonló ötletű ellenpélda adható $k = \frac{p-1}{2}$-vel:

$$F(x_1, \ldots, x_n) = \sum_{i=1}^{n} x_i^{\frac{p-1}{2}} + \frac{p-1}{2} .$$

Most $x_i^{\frac{p-1}{2}}$ 0, 1 vagy -1 lehet, ezért $\left| \sum_{i=1}^{n} x_i^{\frac{p-1}{2}} \right| < \frac{p-1}{2}$, tehát F-nek valóban nem lehet nullhelye $\mathbb{F}_p{}^n$-ben.

A $k = 2$ esetben is világos, hogy $n < k$, azaz $n = 1$ változószám mellett nem lesz mindig megoldás, tetszőleges másodfokú irreducíbilis polinom mutatja ezt.

A felsorolt példákat Rédei is bemutatta 1946-os [2] cikkében.

A pozitív irányú fő eredmény a következő tétel:

3.2. tétel. *Tegyük fel, hogy* $n \geq \left\lceil \frac{p-1}{\lfloor \frac{p-1}{k} \rfloor} \right\rceil$. *Ekkor* $F(x_1, \ldots, x_n) = \sum_{i=1}^{n} x_i^k + g(x_1, \ldots, x_n) = 0$ *megoldható* $\mathbb{F}_p{}^n$*-ben.*

Vegyük észre, hogy $k \mid p-1$ esetén a fenti korlát éppen k-t adja, azaz e speciális esetben bebizonyítottuk a 2.2. sejtést. Minden szóba jövő k-ra igaz viszont, hogy $p-1 \geq \left\lceil \frac{p-1}{\lfloor \frac{p-1}{k} \rfloor} \right\rceil$, azaz $n = p-1$ változó biztosan elég a megoldhatósághoz.

A bizonyítás előkészítéséhez felidézzük Alon úgynevezett nem-eltűnési tételét, amely bizonyításával együtt megtalálható [4]-ben.

3.3. tétel. [Alon] *Legyen* $G(x_1, \ldots, x_k) \in \mathbb{F}_p[x_1, \ldots, x_k]$ k *változós polinom, és tegyük fel, hogy valamely* $0 \leq t_i \leq p-1$ $(1 \leq i \leq k)$ *egész számokra* $\deg G = \sum_{i=1}^{k} t_i \geq 1$, *továbbá* $\prod_{i=1}^{k} x_i^{t_i}$ *együtthatója nem 0. Válasszunk minden* i*-hez tetszőleges* $S_i \subseteq \mathbb{F}_p$ *halmazokat, amelyekre* $|S_i| = t_i + 1$. *Ekkor* G *nem konstans az* $S_1 \times S_2 \times \cdots \times S_k$ *halmazon.*

A tételt kimondhattuk volna úgy is, hogy G nem azonosan 0 az $S_1 \times S_2 \times \cdots \times S_k$ halmazon. Könnyű belátni, hogy ez ekvivalens alak, innen származik a nem-eltűnési tétel elnevezés.

A 3.2. tétel speciális esetét igazoljuk először, amikor $k \mid p-1$.

3.4. tétel. *Ha* $k \mid p-1$, $n \geq k$ *és* $F(x_1, \ldots, x_n) = \sum_{i=1}^{n} x_i^k + g(x_1, \ldots, x_n)$, *akkor az* $F(x_1, \ldots, x_n) = 0$ *egyenlet megoldható* $\mathbb{F}_p^n$*-ben.*

Bizonyítás: Amennyiben $n > k$, úgy helyettesítsünk be 0-t x_k, x_{k+1}, $\ldots$, x_n változókba. Így olyan – továbbra is általánosított diagonális – egyenletet kaptunk, amelyben $n = k$. Feltesszük ezért a bizonyítás hátralevő részében, hogy polinomunk eleve $F(x_1, \ldots, x_k) = \sum_{i=1}^{k} x_i^k + g(x_1, \ldots, x_k)$ alakú.

Legyen $G(x_1, \ldots, x_k) = F(x_1, \ldots, x_k)^{p-1}$. Így G csak 0 vagy 1 értékeket vehet fel. Ha $G(x_1, \ldots, x_k) = 0$, akkor – az $\mathbb{F}_p$ nullosztómentessége miatt – $F(x_1, \ldots, x_k) = 0$. Elegendő tehát belátnunk, hogy G nem konstans $\mathbb{F}_p{}^k$-ban, amit a 3.3. tétel segítségével fogunk igazolni.

Legyen ezért $t_i = p-1$ $(1 \leq i \leq k)$ és $S_i = \mathbb{F}_p$. Világos, hogy $\deg G = k(p-1) = \sum_{i=1}^{k} t_i$. A multinomiális tétel alkalmazásával végezzük el a $\left(\sum_{i=1}^{k} x_i^k\right)^{p-1}$ hatványozást. Eszerint $\prod_{i=1}^{k} x_i^{p-1}$ együtthatója $\frac{(p-1)!}{((p-1)/k)!^k} \neq 0$. Alon tételének feltételei tehát teljesülnek, azaz G nem konstans, amivel tételünket beláttuk.

□

3.5. megjegyzés. Az analóg állítás igaz, ha p helyett $q = p^r$-et írunk, valamely r pozitív egész számra, fenntartva $k \mid p-1$-et. Alon tétele igaz marad és fenti bizonyításunkat is csak $\frac{(q-1)!}{((q-1)/k)!^k} \neq 0$ igazolásával kell kiegészítenünk. Ennek érdekében azt kell kiszámolnunk, hogy a tört számlálójában és nevezőjében p azonos hatványon szerepel-e.

Bizonyítás: A $(p^r-1)!$-ban p kitevője

$$\sum_{i=1}^{\infty} \left\lfloor \frac{p^r-1}{p^i} \right\rfloor = \sum_{i=1}^{r-1} \left\lfloor p^{r-i} - \frac{1}{p^i} \right\rfloor = \sum_{i=1}^{r-1} \left(p^{r-i} - 1\right) \ .$$

A nevezőben

$$k \sum_{i=1}^{\infty} \left\lfloor \frac{\frac{p^r-1}{k}}{p^i} \right\rfloor = k \sum_{i=1}^{r-1} \left\lfloor \frac{p^{r-i}-1}{k} + \frac{p^i-1}{p^i k} \right\rfloor =$$

$$k \sum_{i=1}^{r-1} \frac{p^{r-i}-1}{k} = \sum_{i=1}^{r-1} \left(p^{r-i} - 1\right)$$

Az utolsó előtti egyenlőséget az indokolja, hogy a $k \mid p-1$ feltétel és $p-1 \mid p^l - 1$ $(l \geq 1)$ miatt $\frac{p^{r-i}-1}{k}$ egész szám és $0 < \frac{p^i-1}{p^i k} < 1$.

□

Sajnos e bizonyítás nem általánosítható $k \nmid p-1$ esetre, ezért a továbbiakban csak prím elemszámú testekkel foglalkozunk.

A 3.4. tétel más módszerrel való igazolása megtalálható [5]-ben, arra a technikára még e dolgozatban visszatérek.

Készen állunk a 3.2. tétel bizonyítására.

Bizonyítás: Akárcsak a 3.4. tétel igazolásakor $n = k$, most feltehető $n = \left\lceil \frac{p-1}{\lfloor \frac{p-1}{k} \rfloor} \right\rceil$ és ismét legyen $G(x_1, \ldots, x_n) = F(x_1, \ldots, x_n)^{p-1}$. A cél hasonló, megadjuk $\mathbb{F}_p{}^n$ egy részhalmazát, amelyen G nem konstans.

A nem-eltűnési tételben szereplő paraméterek legyenek az alábbiak:

$$t_i = \left\lfloor \frac{p-1}{k} \right\rfloor k \quad \text{, ha } 1 \le i \le n-1 \text{ és}$$
$$t_n = \left(p - 1 - (n-1) \left\lfloor \frac{p-1}{k} \right\rfloor \right) k \ .$$

Az $1 \le i \le n-1$ esetekben nyilvánvaló $0 \le t_i \le p-1$, jól látszik továbbá, hogy $\sum_{i=1}^{n} t_i = (p-1)k = \deg G$.

Miután

$$t_n = \left(p - 1 - (n-1) \left\lfloor \frac{p-1}{k} \right\rfloor \right) k = \left(p - 1 - \left(\left\lceil \frac{p-1}{\lfloor \frac{p-1}{k} \rfloor} \right\rceil - 1 \right) \left\lfloor \frac{p-1}{k} \right\rfloor \right) k$$
$$\le \left(p - 1 - \left(\frac{p-1}{\lfloor \frac{p-1}{k} \rfloor} - 1 \right) \left\lfloor \frac{p-1}{k} \right\rfloor \right) k = \left\lfloor \frac{p-1}{k} \right\rfloor k \le p-1 \quad \text{és}$$
$$t_n > \left(p - 1 - \frac{p-1}{\lfloor \frac{p-1}{k} \rfloor} \left\lfloor \frac{p-1}{k} \right\rfloor \right) k = 0,$$

tehát t_n is megfelelő.

Szerepel G-ben a $\prod_{i=1}^{n} x_i^{t_i}$ monom, amely a $\left(\sum_{i=1}^{k} x_i^k \right)^{p-1}$ kifejtéséből jön, hiszen $x_i^{t_i} = \left(x_i^k\right)^{\lfloor \frac{p-1}{k} \rfloor}$, illetve $x_n^{t_n} = \left(x_n^k\right)^{p-1-(n-1)\lfloor \frac{p-1}{k} \rfloor}$. Együtthatója pedig $\frac{(p-1)!}{\prod_{i=1}^{n}(t_i/k)!} \neq 0$, ami azt jelenti, hogy Alon tétele alkalmazható, S_i halmazokat tetszőlegesen választhatjuk $|S_i| = t_i + 1$ betartása mellett. Állításunkat ezzel beláttuk.

□

Hasonlóan igaz a 3.2. tétel alábbi általánosítása:

3.6. megjegyzés. Legyen $n \ge \left\lceil \frac{p-1}{\lfloor \frac{p-1}{k} \rfloor} \right\rceil$ és vizsgáljuk az $F(x_1, \ldots, x_n) =$

$\sum_{i=1}^{n} a_i x_i^k + g(x_1, \ldots, x_n)$ polinomot, ahol $a_i \in \mathbb{F}_p$ és $a_1 \ldots a_n \neq 0$. Ekkor létezik F-nek gyöke ${\mathbb{F}_p}^n$-ben.

A bizonyítás szó szerint ugyanúgy megy, a különbség mindössze annyi, hogy a $\prod_{i=1}^{n} x_i^{t_i}$ együtthatója most $\frac{(p-1)!}{\prod_{i=1}^{n}(t_i/k)!} \prod_{i=1}^{n} a_i^{(t_i/k)!}$, ami természetesen ismét nem 0.

4. További problémák

Természetes módon merül fel a 2.3. tétel és az általam tekintett általánosított diagonális egyenletek egy lehetséges közös általánosítása.

Legyen

$$F(x_1, \ldots, x_n) = \sum_{i=1}^{n} h_i(x_i) + g(x_1, \ldots, x_n) \ ,$$

ahol $\deg h_i = k_i$, $\deg g = d$ és teljesül $d < k_n \leq k_{n-1} \leq \cdots \leq k_1 = k$.

Egy speciálisabb eset, ami az általánosított diagonális egyenleteket még magába foglalja

$$F(x_1, \ldots, x_n) = \sum_{i=1}^{n} x_i^{k_i} + g(x_1, \ldots, x_n) \ , \tag{1}$$

ahol a fokszámokra vonatkozó előbbi összefüggések továbbra is fennállnak. A fenti esetekhez hasonlóan a triviális $k_n = k_{n-1} = 1$ esettől eltekintve $\operatorname{rang} F = n$, ezért Rédei sejtése szerint a $k \leq n$ esetben kell létezzen F-nek gyöke.

Carlitz [5] cikkében olvasható módszert esetleg fel lehetne használni a bizonyításhoz, amennyiben $k \mid p-1$. Az elképzelést az alábbiakban vázolom.

Tegyük fel, hogy $n = k$. Carlitz technikája – amelyet a 3.4. tétel igazolásához is használ –, hogy az $F(x_1, \ldots, x_k)^{p-1}$ polinomot összegzi $x_i = 0 \ldots p-1$-re $(1 \leq i \leq k)$. Ha nem lenne gyöke F-nek ${\mathbb{F}_p}^k$-ban, úgy ezen összeg 0 lenne, ami azonban igazolható, hogy nem fordulhat elő.

Az (1) polinom gyöke létezésének bizonyításához összegezzük F-et *néhány* – jól megválasztott – x_i-re. Ezáltal kapunk egy $h(y_1, \ldots, y_l)$ polinomot, ahol $0 < l < k$, $y_1, \ldots, y_l$ az $x_1, \ldots, x_k$ közül néhány, h egy főtagja $a y_1^{m_1} y_2^{m_2} \ldots y_l^{m_l}$, $a \neq 0$ és minden i-re $0 \leq m_i \leq p-1$. Ha ilyen h polinomot tudnánk mutatni, akkor alkalmazva a 3.4. és a 3.2. tételek bizonyításához is használt nem-eltűnési tételt, könnyen bizonyíthatjuk a nullhely létezését:

Alon tétele szerint van olyan $y_1, \ldots, y_l$, hogy

$$1 = h(y_1, \ldots, y_l) = \sum_{x_{i_1} \in \mathbb{F}_p} \cdots \sum_{x_{i_{k-l}} \in \mathbb{F}_p} F(x_1, \ldots, x_k)^{p-1}$$

Ám, abban az esetben, ha nem volna gyöke F-nek, akkor minden $x_1, \ldots, x_k$-ra $F(x_1, \ldots, x_k)^{p-1} = 1$ lenne, ezt összegezve $p^{k-l} = 0$ volna.

A megfelelő $h(y_1, \ldots, y_l)$ polinom készítéséhez jól használható lehet az alábbi ismert összefüggés:

$$\sum_{x \in \mathbb{F}_p} x^m = \begin{cases} -1 & \text{, ha } p-1 \mid m \text{ és} \\ 0 & \text{egyébként.} \end{cases}$$

Alkalmazva a multinomiális tételt:

$$\sum_{x_{i_1} \in \mathbb{F}_p} \cdots \sum_{x_{i_{k-l}} \in \mathbb{F}_p} F(x_1, \ldots, x_k)^{p-1} =$$

$$\sum_{(*)} \frac{(p-1)!}{\prod_{i=1}^{k+1} n_i!} \sum_{x_{i_1} \in \mathbb{F}_p} \cdots \sum_{x_{i_{k-l}} \in \mathbb{F}_p} g(x_1, \ldots, x_k)^{n_{k+1}} \prod_{i=1}^{k} x_i^{k_i n_i} ,$$

ahol a (*) összegzés az $n_1, \ldots, n_{k+1}$ nemnegatív egész számokra megy, az $n_1 + \cdots + n_{k+1} = p-1$ feltétel mellett. Rögzített $n_1, \ldots, n_{k+1}$ esetén jelölje az előbbi kifejezésben szereplő $g(x_1, \ldots, x_k)^{n_{k+1}} \prod_{i=1}^{k} x_i^{k_i n_i}$-ben valamely x_i együtthatóját m. A fenti összefüggést alkalmazva, amennyiben $p-1 \nmid m$ és összegzünk x_i-re, akkor ez a tag 0. Nem reménytelen tehát a fent megfogalmazott h polinom előállítása ilyen módon.

Hivatkozások

[1] R. Lidl, H. Niederreiter, *Finite Fields;* Addison-Wesley Publishing Co. 1983.

[2] L. Rédei, Zur Theorie der Gleichungen in endlichen Körpern, *Acta Univ. Szeged Sect. Sci. Math. 11 (1946), 63–70.*

[3] L. Rónyai, On a conjecture of László Rédei, *manuscript (2002)*

[4] N. Alon, Combinatorial Nullstellensatz, *Combinatorics, Probability and Computing 8 no. 1-2, 7-29 (1999)*

[5] L. Carlitz, Solvability of certain equations in a finite field, *Quart. J. Math. (2) 7, 3-4 (1956)*

[6] L. Carlitz, H. H. Corson, Some special equations in a finite field, *Monatsh. Math. 60, 114-122 (1956)*