LATIN NÉGYZETEK ÉS ALKALMAZÁSAIK

Kis Ágnes

Témavezető: Szőnyi Tamás

Szamitógéptudományi Tanszék

Eötvös Loránd Tudományegyetem

Budapest

2016

Tartalomjegyzék

Ronald A. Fisher emlékére festett
latin négyzetet ábrázoló ablak Cambridge-ben

Bevezetés

> ”For what is useful above all is technique, and mathematical technique is taught mainly through pure mathematics.”
>
> *A mathematician's apology*
> G. H. Hardy

Algebrai szemmel a latin négyzetek kvázicsoportok műveletttáblái (Cayley-táblái), de a Sudokunak bármely megoldása is latin négyzetet ad.

Elnevezése Leonhard Eulertől származik, aki írásaiban latin karaktereket használt a latin négyzet szimbólumaiként.

A nagyon egyszerű konstrukció széleskörben alkalmazhatónak bizonyult.

Sok érdeme van ebben Ronald A. Fishernek, Dénes Józsefnek és A. D. Keedwellnek, akik könyvének gazdag problémafelvetéseit Erdős Pál dícséri újabb kiadásuk előszavában. Elmondása szerint ugyanis 73 megoldatlan problémát vet fel *Latin Squares and their Applications* c. első könyve a szerzőpárosnak – mely 1974-ben került kiadásra –, és ebből 1991-ben megjelent *Latin Squares* c. könyvig 20-at teljesen megoldottak, feleennyit pedig részben.

Több formája is ismeretes a latin négyzet alapú táblajátékoknak, tudományos kísérletek tervezésében – így gyógyszerészetben, pszichológiai kutatásokban – is nagy szerepet tölt be. A II. Világháború ideje alatt hírközlésre használták, kódelméleti alkalmazásai elterjedtek.

Jelen dolgozat célja elméleti alkalmazások szemléltetése mellett, hogy bepillantást nyerjünk a latin négyzetek sok téren megvalósuló hasznáról.

1. fejezet

Latin négyzetek

1.1. Néhány definíció

1.1.1. Definíció. (Latin négyzet) Egy $n \times n$-es L mátrixot, melynek elemei egy n szimbólumot tartalmazó S halmazból kerülnek ki, *n-edrendű latin négyzet*nek nevezünk, ha S minden szimbóluma pontosan egyszer fordul elő minden sorban és oszlopban.

1	2	3
2	3	1
3	1	2

1.1. ábra.

1.1.2. Megjegyzés. Többnyire az n szimbólumnak az $\{1, 2, \ldots n\} \subseteq \mathbb{N}$ számokat választjuk az egyszerűség kedvéért.

1.1.3. Definíció. (Redukált/standard forma) Egy latin négyzet, melynek elemei a természetes számok halmazából kerülnek ki *redukált* vagy *standard formá*ban van, ha az első oszlop és az első sor elemei rendezettek. (Esetünkben $1, 2, 3, \ldots n$.)

1.1.4. Definíció. (Görög-latin négyzet) Két n-edrendű latin négyzetet egymásra téve a cellákban szimbólumok helyett szimbólum párokat kapunk. Ha ezek a párok minden cellában egyediek, akkor *görög-latin négyzetet* kaptunk.

1.1.5. Megjegyzés. Mivel n-edrendű latin négyzetekről beszélünk, a lehetséges szimbólum párok száma n^2. Így a görög-latin négyzetnek elő kell állítania n^2 különböző pár mindegyikét pontosan egyszer.

1.1.6. Definíció. (Transzverzális) Egy n-ed rendű latin négyzet *transzverzálisa* celláinak egy olyan n számosságú halmaza, melynek elemei úgy kerülnek ki a latin négyzetből, hogy minden sorából és minden oszlopából pontosan egyet választunk ki, olyan módon, hogy minden cella más szimbólumot tartalmazzon. (1.2. ábra)

1	2	3
2	3	1
3	1	2

1.2. ábra. latin négyzet transzverzálisa

1.2. A 36 tiszt problémája

Az eredeti feladatot Euler 1782-ben publikálta, mely a következőképpen hangzott:

1.2.1. Feladat. Egy díszszemlére érkezett 6 ezredből 6-6 különböző féle rendfokozatú tiszt által vezényelt alegységeket úgy kell elrendezni egy 6×6-os négyzetben, hogy minden sorban és minden oszlopban pontosan egyszer forduljon elő a tiszt rendfokozata és ezrede.

Ez a feladat 200 éven át tartó vitát indított meg a görög-latin négyzetek létezésének feltételeiről, ugyanis ennek átfogalmazása azt a kérdést teszi fel, van-e 6×6-os görög-latin négyzet?

Látni fogjuk, hogy $n = 2$-re nem létezik görög-latin négyzet és $n = 6$-ra se talált Euler, ezért azt sejtette, hogy $4n + 2$ (ahol $n \in \mathbb{N}$) alakú számokra nincs.

Ezt az állítását a hatvanas években sikerült megcáfolni, ám az $n = 6$ esetben igaza volt. Ennek a feladatnak lett a neve a *36 tiszt problémája*, melynek bizonyítását Gaston Terry adta majd 120 évvel később, szimmetriai meggondolásokkal az összes eset áttekintésével ([8]).

1960-ban, miután E. C. Parkernek sikerült találnia $n = 10$ esetre megfelelő latin négyzetpárt (ld. 1.3. ábra), az eredetileg statisztikus R.C. Bose és S.S. Shrikhande segítségével általánosságban is megcáfolták Euler sejtését. Sőt, az is kiderült, hogy az ilyen alakú számok közül csak $n = 2$ és $n = 6$ esetben nincs megoldás.

0	4	1	7	2	9	8	3	6	5
8	1	5	2	7	3	9	4	0	6
9	8	2	6	3	7	4	5	1	0
5	9	8	3	0	4	7	6	2	1
7	6	9	8	4	1	5	0	3	2
6	7	0	9	8	5	2	1	4	3
3	0	7	1	9	8	6	2	5	4
1	2	3	4	5	6	0	7	8	9
2	3	4	5	6	0	1	8	9	7
4	5	6	0	1	2	3	9	7	8

0	7	8	6	9	3	5	4	1	2
6	1	7	8	0	9	4	5	2	3
5	0	2	7	8	1	9	6	3	4
9	6	1	3	7	8	2	0	4	5
3	9	0	2	4	7	8	1	5	6
8	4	9	1	3	5	7	2	6	0
7	8	5	9	2	4	6	3	0	1
4	5	6	0	1	2	3	7	8	9
1	2	3	4	5	6	0	9	7	8
2	3	4	5	6	0	1	8	9	7

1.3. ábra. Görög-latin négyzet $n = 10$-re E. T. Parkertől([9])

1.2.2. Megjegyzés. A fenti két latin négyzetből készült görög-latin négyzetet szokták $6, 2$ indexű Euler négyzetnek is hívni, ahol az első tag a rendet, a második az egymásra helyezett ortogonális négyzetek számát jelenti (ld. például [7]). Eszerint a fent látható két négyzet két darab $6, 1$ indexű Euler négyzet.

1.3. Ortogonalitás

Az előző részben tárgyalt görög-latin négyzetpárokat *ortogonálisaknak* mondjuk. Erre a definícióra építkezve juthatunk el igen lényeges és hasznos fogalmakhoz, alkalmazásokhoz.

1.3.1. Definíció. (Ortogonalitás)

1. Jelölje az L latin négyzet i. sorának j. elemét $L_{i,j}$. Az L^1, L^2 n-edrendű latin négyzetek *ortogonálisak*, ha az $(L^1_{i,j}, L^2_{i,j})$ párok $1 \leq i, j \leq n$ esetén a $1, 2, \ldots, n$ számokból képezhető összes rendezett párt pontosan egyszer állítják elő, azaz ha egymásra helyezve őket görög-latin négyzetet kapunk.

2. Az n-edrendű latin négyzetek egy $\left\{L^1, L^2, \ldots, L^k\right\}$ halmaza ortogonális rendszert alkot, ha közülük bármely kettő ortogonális.

   Ezek elemszámát több irodalomban jelölik $N(n)$-nel ([3],[1]), mi is innentől így hivatkozunk rá.

1.3.2. Megjegyzés. Egy másik kapcsolódó függvény, n_r, melyet azon legkisebb pozitív egész szám jelölésére használjuk, amelyre: $\forall v \geq n_r\ \exists\ r$ elemű ortogonális rendszere v rendű latin négyzeteknek.

Euler sejtésének cáfolata vezetett az $N(n)$ és n_r függvények értékeinek vizsgálatáról szóló tanulmányokhoz.

A következő tétellel egy felső korlátot adunk $N(n)$-re.

1.3.3. Tétel. $N(n) \leq n - 1$.

Bizonyítás

1. A rendszerben lévő összes latin négyzet szimbólumait nevezzük át úgy, hogy az első soruk rendezett legyen. Az egyszerűség kedvéért legyenek a szimbólumok az $1, 2, \ldots, n$ számok.

   Így ha az első sorban a 2 szimbólumot az 1-re cseréljük egy négyzetben, azt ugyanúgy meg kell tennünk a négyzet többi 2 szimbólumával, mely eredetileg is az volt. Hogy melyik szimbólumot melyikkel helyettesítjük, szükségszerűen négyzetenként változik.

2. Majd sorok cseréjével (természetesen az 1. sor kivételével, hiszen azt már rendeztük) érjük el, hogy a rendszerből egy tetszőleges négyzet standard legyen, mégpedig úgy, hogy közben minden latin négyzeten ugyanezeket a sorcseréket hajtjuk végre.

Vegyük észre, hogy ezzel nem veszítettük el az ortogonalitást, hiszen a szimbólumok nem befolyásolják, csupán azok helye, másrészt a sorok szimultán cseréivel nem veszítünk el egyetlen rendezett párt sem a későbbi egymásra helyezett négyzetekből.

Egyértelmű, hogy az azonos szimbólumokból álló párok az első sorban fognak létrejönni.

Minden latin négyzet első oszlopának 2. sorában különböző szimbólumoknak kell szerepelniük, ugyanis, ha lehetne két latin négyzetnek ugyanaz az s szimbóluma a 2. sor 1. helyén, akkor előállna belőlük egy olyan négyzet, melynek az $(1, s)$ és a $(2, 1)$ pozícióiban ugyanaz a rendezett pár szerepelne, így nem lehetnének ortogonálisak a négyzetek. □

A fenti bizonyítás 1., 2. pontjában le is írtuk, hogyan jön létre ún. *latin négyzetek standardizált ortogonális rendszere*:

1.3.4. Definíció. (Standardizált ortogonális rendszer) Latin négyzetek ortogonális rendszerét standardizáltnak mondjuk, ha minden latin négyzetének első sora és egynek első oszlopa rendezett.

1.3.5. Definíció. (Teljes ortogonális rendszer) Ha adott n-re létezik ilyen $n-1$ elemű ortogonális rendszer, akkor azt *teljes ortogonális rendszer*nek nevezzük.

1.3.6. Megjegyzés. Az ortogonális rendszer tetszőleges elemét lehet standard alakra hozni szimultán rendezésekkel.

Nyilvánvaló, hogy az első eset, amikor értelmezhető a latin négyzetek ortogonális rendszere az $n = 3$, ugyanis $n = 2$-re az alábbi két latin négyzet létezik:

1	2
2	1

és

2	1
1	2

,

melyek nyilván nem ortogonálisak egymással.

$n = 3$-ra létezik ortogonális rendszer:

1	2	3
2	3	1
3	1	2

1	2	3
3	1	2
2	3	1

melyről már tudjuk, hogy teljes ortogonális rendszer is.

Érdekes kérdés lehet ezek konstrukciója. Ebben segíthet nekünk a következő tétel:

1.3.7. Tétel. *Egy latin négyzetnek akkor és csakis akkor létezik ortogonálisa*[1]*, ha létezik n diszjunkt transzverzálisa.*

Bizonyítás Legyen L^1 n-edrendű latin négyzet redukált formában az egyszerűség kedvéért.

Vegyük L^1-nek n celláját, melyek ugyanazt a rögzített s szimbólumot tartalmazzák. Ekkor L^1 ortogonálisának megfelelő celláiban egyet kivéve – melyről feltehetjük, hogy az első sorban van, hiszen bármely ortogonális rendszer átalakítható standardizálttá – minden helyen más szimbólumnak kell szerepelnie, különben nem lehetnének ortogonálisak.

Mivel az s szimbólum L^1 minden sorában és oszlopában pontosan egyszer szerepel, ugyanezeknek a celláknak az értékei ennek ortogonálisának – ami legyen L^2 – egy transzverzálisát adják.

Megfordítva: ha létezik n diszjunk transzverzális, akkor az L^2-ben ezekre a helyekre sorra $1, 2, \ldots, n$-et beírva megkaptuk az ortogonális párt. $\square$

1.3.8. Megjegyzés. A tétel szemléletesen $n = 3$-ra:

$$L^1 = \begin{array}{|c|c|c|}\hline 1 & 2 & 3 \\ \hline 2 & 3 & 1 \\ \hline 3 & 1 & 2 \\ \hline \end{array} \qquad L^2 = \begin{array}{|c|c|c|}\hline 1 & 2 & 3 \\ \hline 3 & 1 & 2 \\ \hline 2 & 3 & 1 \\ \hline \end{array}$$

[1]Eredetileg *orthogonal mate* (ortogonális társ), jelentése: létezik hozzá egy ugyanolyan dimenziós latin négyzet, mellyel ortogonális párt alkotnak.

2. fejezet

Matematikai alkalmazások

2.1. Véges Geometria

2.1.1. Véges projektív síkok

Ennek a résznek a tárgyalásához szükségünk lehet az absztrakt projektív sík axiómáira és azok eredetének megértésére. Kihasználva az alkalmat, példákat, jelöléseket is bevezetünk.

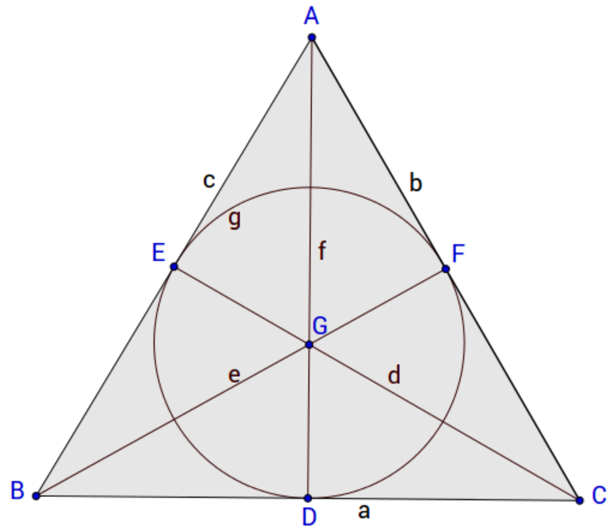
2.1.1. Definíció. Azt a projektív síkot, amit az euklidészi sík ideális pontokkal és egyenesekkel való kibővítéseként kapunk, *klasszikus projektív síknak* nevezzük. Ezen a síkon a pont és egyenes illeszkedési viszonyairól tudottakat mondjuk alaptényeknek, és axiómaként tekintünk rájuk innentől.

K1. Bármely két ponthoz pontosan egy mindkettőre illeszkedő egyenes van.

K2. Bármely két egyeneshez pontosan egy mindkettőre illeszkedő pont van.

K3. Van olyan négy pont, hogy azok közül bármely kettőre egyaránt illeszkedő egyenes már a maradék két pont egyikéhez sem illeszkedik.

2.1.2. Megjegyzés. Ezeket az axiómákat tekinthetjük a projektív síkok modellejeként is, hiszen vannak más rendszerek is, melyekben definiálhatunk pontokat, egyeneseket és illeszkedést, melyekkel az axiómák teljesülni fognak. Ilyen például a *Fano sík*, ld. 2.1. Az ábra jelöléseit használva a Fano sík ponthalmaza: $\mathcal{P} = \{A, B, C, D, E, F, G\}$,



2.1. ábra. Fano sík

egyenesei: $a = \{B, D, C\}$, $b = \{A, F, C\}$, $c = \{A, E, B\}$, $d = \{E, G, C\}$, $e = \{B, G, F\}$, $f = \{A, G, D\}$.

Ebből definiáljuk az absztrakt projektív síkot, más axiómákkal helyettesítve a 3. axiómát, melyet úgy is nevezünk, hogy létezik *valódi négyszög*.

2.1.3. Definíció. A $\Pi = (\mathcal{P}, \mathcal{E}, \mathcal{I})$ hármast, ahol $\mathcal{P}$ és $\mathcal{E}$ két diszjunkt halmaz, $\mathcal{I} \subset \mathcal{P} \times \mathcal{E}$ pedig egy illeszkedésnek nevezett reláció, *projektív síknak* nevezünk, ha kielégíti a következő axiómákat:

P1. $\mathcal{P}$ bármely két különböző eleméhez pontosan egy olyan eleme van $\mathcal{E}$-nek, amely mindkettővel relációban áll.

P2. $\mathcal{E}$ bármely két különböző eleméhez pontosan egy olyan eleme van $\mathcal{P}$-nek, amely mindkettővel relációban áll.

P3. $\mathcal{E}$ minden eleme legalább három különböző $\mathcal{P}$-beli elemmel áll relációban.

P4. $\mathcal{P}$ minden eleme legalább három különböző $\mathcal{E}$-beli elemmel áll relációban.

2.1.4. Megjegyzés. 1. $\mathbb{F}$ test feletti projektív sík jelölése: $PG(2, \mathbb{F})$.

2. **P1**, **P2** és **P3**, **P4** egymás duálisai, ezért ha egy tétel igaz, akkor annak duálisa is nyilván igaz lesz.

3. A **P3** és **P4** axiómák az elfajuló esetek kizárására szolgálnak, és ekvivalensek **K3**-mal. Ennek bizonyítása megtalálható a [4] könyv 1. fejezetében.

4. A klasszikus projektív sík, $PG(2,\mathbb{R})$) nyilván absztrakt is.

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

1. *Minden egyenesén* $n+1$ *pont van.*

2. *Minden pontján* $n+1$ *egyenes megy át.*

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

Ellenőrizhetjük is ezeket a Fano-síkon, mely egy 2-rendű projektív sík, és valóban mind a 7 pontja (egyenese) 3 egyenessel (ponttal) áll relációban.

Ennek a tételnek köszönhetően értelmes a következő definíciónk.

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

2.1.7. Állítás. *Tetszőleges* q*-ra* $\mathbb{F}_q = GF(q)$ *véges test feletti vektortérből mindig származtatható projektív sík, melynek rendje* q*.*

Bizonyítás Legyen V egy $\mathbb{F}_q$ feletti három dimenziós vektortér. Legyen $\mathcal{P}$ V egydimenziós, $\mathcal{E}$ pedig V kétdimenziós altereinek halmaza, az illeszkedés pedig legyen a halmazelméleti tartalmazás.

A háromdimenziós vektortérben két különböző egydimenziós alteret pontosan egy kétdimenziós altér tartalmaz, és bármely két különböző kétdimenziós altér metszete pontosan egy egydimenziós altér lehet, ezért **P1** és **P2** teljesül.

Legyenek $e_1, e_2, e_3 \in V$ a vektortér bázisvektorai. Ekkor az e_1, e_2 vektorok által generált kétdimenziós altér biztosan tartalmazza az e_1, e_2 és $e_1 + e_2$ vektorok által generált három egydimenziós alteret, amivel **P3** axiómát láttuk be.

Tekintsük az e_1 által generált V_1 egydimenziós alteret. A V_1-et tartalmazó kétdimenziós alterek: $< e_1, e_2 >$, $< e_1, e_3 >$, $< e_1, e_2 + e_3 >$. Így a **P4** axióma is teljesül.

Ebből kapjuk a projektív sík algebrai modelljét: a V-ben az egydimenziós altereket – azaz a pontokat – generáló vektorukkal, a kétdimenziós altereket – azaz az egyeneseket – pedig az ortogonális kiegészítőjük egyik generáló vektorával adjuk meg.

Ekkor egy x pontot a $(x_1, x_2, x_3) \neq (0, 0, 0)$ hármasok jelentenek, és mivel vektorokról van szó: $\forall\lambda(\neq 0) \in \mathbb{F}_q$-ra $x = (x_1, x_2, x_3) = (\lambda x_1, \lambda x_2, \lambda x_3) = \lambda x$ ugyanaz a pont. Hasonlóan az egyenesek olyan $[u_1, u_2, u_3] \neq [0, 0, 0]$ ponthármasok, ahol $[u_1, u_2, u_3]$ és $[\lambda u_1, \lambda u_2, \lambda u_3]$ ugyanazt az u egyenest jelentik $\lambda \neq 0$ és $\lambda \in \mathbb{F}_q$ esetén.

Nyilván a pontok és egyenesek száma megegyezik. q elemű test esetén q^3 féle ponthármas létezik, de ebből az egyik a csupa 0, λ-t pedig $q - 1$ félét választhatunk. Így kapjuk, hogy a pontok és egyenesek száma

$$\frac{q^3 - 1}{q - 1} = \frac{(q^2 + q + 1)(q - 1)}{q - 1} = q^2 + q + 1,$$

tehát a véges projektív sík rendje valóban q. $\square$

2.1.8. Következmény. *Algebrai tanulmányainkból tudjuk, hogy $GF(q)$ létezésének szükséges és elégséges feltétele, hogy $q = p^n$, ahol p egy prím és $n \geq 1$, $n \in \mathbb{N}$.*

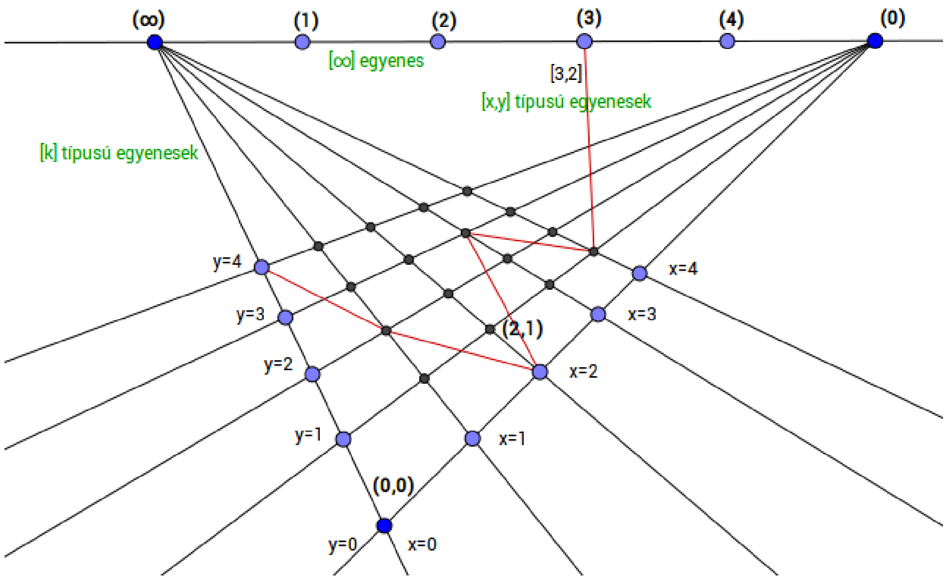
Az előző tételnek és ennek a következménye, hogy mindig létezik prímhatványrendű projektív sík, nevezetesen $PG(2, \mathbb{F}_q)$.

2.1.9. Állítás. *$\{L^1, L^2, \ldots, L^{n-1}\}$ latin négyzetek teljes ortogonális rendszeréből mindig konstruálható projektív sík.*

Bizonyítás Először felépítjuk a síkot, majd belátjuk, hogy érvényesek az axiómák.

Feleljenek meg a latin négyzetek az ideális egyenes $n-1$ ideális pontjának és jelöljük őket a 2.2 ábrához igazodva (i)-vel $\forall i = 1, 2, \ldots, n-1$. Definiáljunk két másik ideális pontot az ideális egyenesen, (∞)-t, és (0)-t, melyek a sorok és az oszlopok szerepét töltik be. Egy ideális ponthoz tartozó egyenespár ne metssze egymást, viszont minden (∞)-re illeszkedő egyenes metsszen minden (0)-ra illeszkedőt. A négyzetekben az egyes szimbólumok által alkotott mező n-esek legyenek az ideális pontjaikra illeszkedő egyenesek, tehát minden (i) négyzet minden j szimbólumához rendeljünk egy $[i, j]$ egyenest, mely pontosan akkor illeszkedik egy (x, y) típusú pontra, ha az i. négyzet x. sorában és y. oszlopában a j szimbólum szerepel.

Megadtuk az illeszkedést, és a pontok és egyenesek halmazát: $\mathcal{P} = \{(x, y), (x), (\infty)\}$, $\mathcal{E} = \{[m, k], [k], [\infty]\}$, ahol $x, y, m, k \in \{0, 1, \ldots, n-1\}$.



2.2. ábra.

Ezekre lássuk be az axiómák teljesülését!

P1 ideális pontokra nyilván igaz: az ideális egyenes összeköti őket, minden nem ideális egyenes pedig egy-egy latin négyzet szimbólumainak illeszkedését vagy a sorokat, oszlopokat jelentő egyenesek, tehát hozzá vannak rendelve egyértelműen egy ideális ponthoz. A nem ideális pontokra is teljesül ugyanezért: az egyenesek, mint diszjunkt azonos szimbólumot tartalmazó mező n-esek, lefedik az összes cellát négyzetenként. Ha több ilyen egyenes kötne össze két pontot, az azt jelentené, hogy két latin négyzetben van olyan szimbólumhoz tartozó egyenes, amely több mint 2 helyen megegyezik, ez pedig ellentmond az ortogonalitásnak. A nem ideális és ideális pontok közötti többszörös egyenes pedig azt jelentené, egy cellába több szimbólumot akarunk beírni, amit nyilván nem lehet.

P2, amikor nem ideális egyenesekről beszélünk: bármely két oszlopot/sort jelképező egyenes nyilván pontosan egyszer metsz egy sort/oszlopot jelentő egyenest, míg ugyanazon osztályba tartozó egyenesek közös pontja csak az ideális pontjuk lehet. Vegyük a szimbólum n-eseket jelentő egyeneseket: ezek minden sort és minden oszlopot egyetlen helyen metszenek négyzetenként. Egymást is pontosan egyszer metszhetik, vagy mert ugyanazon négyzethez tartoznak (ekkor az ideális pontban), vagy azért, mert a hozzájuk tartozó négyzetek előállítanak egy párt, ami szimbólumpáronként (bármely 2 ilyen egyenesre) pontosan egyszer történik meg. Ideális és nem ideális egyenes esetében megint egyértelmű, hogy nem lehet egynél több közös pontjuk (egy sor nem lehet oszlop is, stb...).

P3 és **P4** pedig nyilván teljesülnek $n \geq 2$ miatt. □

2.1.10. Megjegyzés. A bizonyítás első részével (rendtől és latin négyzetektől függően) egy 2.2 ábrán láthatóhoz hasonló véges projektív síkot kapunk. Erről leolvasható, hogy a latin négyzetek rendje $n = 5$, és a harmadik négyzetben a 2-es szimbólum elhelyezkedése a következő ($L_{x,y}$ jelentése: L négyzet x. oszlopa és y. sora):

$$L^3 = \begin{array}{|c|c|c|c|c|} \hline & & 2 & & \\ \hline & & & & 2 \\ \hline & 2 & & & \\ \hline & & & 2 & \\ \hline 2 & & & & \\ \hline \end{array}$$

2.1.11. Megjegyzés. Az $[x, y]$ típusú egyenesek illeszkedési szabályainál felcserélhető a pár szerepe. Például a [5] könyvben minden (i) négyzet minden j szimbólumához $[i, j]$ egyenes helyett $[j, i]$ egyenest rendel (amikor az i. négyzet x. sorában és y. oszlopában a j szimbólum szerepel).

Az állítás visszafele is teljesül, lássuk most ennek bizonyítását.

2.1.12. Állítás. *n-edrendű projektív síkból mindig konstruálható $\{L^1, L^2, \ldots, L^{n-1}\}$ latin négyzetek teljes ortogonális rendszere.*

Bizonyítás Az egyszerűség kedvéért számozás helyett jelöljük most az $(1), (2), \ldots, (n-1)$ ideális pontokat $I_1, I_2, \ldots, I_{n-1}$-nek. Jelentsék ezek a latin négyzeteket, a rajtuk átmenő nem ideális $m_{i,j}$ ($i = 1, 2, \ldots, n-1$ és $j = 1, 2, \ldots, n$) egyenesek jelöljék az i. négyzethez tartozó j. szimbólumot.

Mivel n-edrendú projektív síkról beszélünk, $n^2 + n + 1$ pontja van, és minden egyenesén $n + 1$. Tehát az ideális egyenes pontjain kívül még van n^2 pont, amiket a a latin négyzetek n^2 mezőiként értelmezünk.

Így a négyzetek oszlopait jelenthetik a (∞), sorait a (0) ideális pontokra illeszkedő egyenesek. Az is egyértelmű, hogy a latin négyzeteket jelentő ideális pontokra illeszkedő (szimbólumokhoz tartozó) egyenesek még n darab pontra illeszkednek.

Megkaptuk a latin négyzetek konstrukcióját, már csak azt kell belátnunk, hogy

1. valóban latin négyzeteket kaptunk;
2. a latin négyzetek páronként ortogonálisak.

Tegyük fel indirekt, hogy I_k négyzetnek van oszlopa vagy sora, ahol a j. szimbólum kétszer szerepel. Ez azt jelentené, hogy van olyan $m_{k,j}$ egyenes kétszer metszi ugyanahhoz a sorhoz/oszlophoz tartozó egyenest. Ez nyilván ellentmond **P1**-nek. ↯

Szintén indirekt módon lássuk be, hogy a latin négyzetek páronként ortogonálisak. Tegyük fel, hogy $\exists\ I_j, I_k$ négyzetpár, melyek nem azok, tehát valamely (x', y'), (x, y) helyekre $((I_k)_{(x,y)}, (I_j)_{(x,y)}) = ((I_k)_{(x',y')}, (I_j)_{(x',y')})$. Ez azt jelentené, hogy a szimbólumpároshoz tartozó 2 egyenes két helyen is metszi egymást – az (x, y) és az (x', y') pontokban –, ami ellentmond **P2**-nek. ↯ □

2.1.13. Megjegyzés. Tehát testből is. (Ld. 2.1.7 tétel.)

A következő konstrukció szintén test feletti projektív síkot ad:

$$\mathcal{P} = \{(x, y), (m), (\infty) : x, y, m \in GF(q)\}$$

$$\mathcal{E} = \{[m, b], [c], [\infty] : m, b, c \in GF(q)\}$$

Az egyenesekre való illeszkedés pedig: $[\infty] = \{(m), (\infty) : m \in GF(q)\}$; $[c] = \{(\infty), (x, y) : x = c \text{ és } y \in GF(q)\}$; $[m, b] = \{(m), (x, mx + b) : x \in GF(q)\}$.

Itt a latin négyzeteket az (m) típusú pontok jelentik (ahol $m \neq 0$), az m. négyzet b szimbóluma pedig az x. sorban és $mx + b$. oszlopban lesz.

2.1.2. Affin síkok

Ha egy $\Pi = (\mathcal{P}, \mathcal{E}, \mathcal{I})$ projektív síknak egy egyenesét és annak összes pontját elhagyjuk, akkor Π' a megmaradt $\mathcal{P}'$ pontokkal, $\mathcal{E}'$ egyenesekkel és az $\mathcal{I}' = \mathcal{I} \cap \mathcal{P}' \times \mathcal{E}'$ relációval egy affin síkot ad.

2.1.14. Definíció. A $\Pi' = (\mathcal{P}', \mathcal{E}', \mathcal{I}')$ hármast, ahol $\mathcal{P}'$ és $\mathcal{E}'$ két diszjunkt halmaz, $\mathcal{I}' \subset \mathcal{P}' \times \mathcal{E}'$ pedig egy illeszkedésnek nevezett reláció, *affin síknak* nevezünk, ha kielégíti a következő axiómákat:

A1. $\mathcal{P}'$ bármely két különböző eleméhez pontosan egy olyan eleme van $\mathcal{E}'$-nek, amely mindkettővel relációban áll.

A2. Ha $P \in \mathcal{P}$ 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.

A3. $\mathcal{E}'$ minden eleme legalább két különböző $\mathcal{P}'$-beli elemmel áll relációban.

A4. $\mathcal{P}'$ minden eleme legalább három különböző $\mathcal{E}'$-beli elemmel áll relációban.

2.1.15. Definíció. (Affin sík projektív lezártja) A $\Pi' = (\mathcal{P}', \mathcal{E}', \mathcal{I}')$ hármas legyen az affin sík továbbra is. $e, f \in \mathcal{E}'$ legyenek *párhuzamosak*, ha nincs közös pontjuk. Ekkor a párhuzamosság ekvivalenciarelációt ad, mert reflexív, szimmetrikus és **A2** miatt tranzitív is. Legyen $\mathcal{P}_\infty$ az ideális pontok halmaza, elemei pedig ekvivalencia osztályonként egy ideális pont, l_∞ pedig legyen az ideális egyenes.

A $\Pi' = (\mathcal{P}', \mathcal{E}', \mathcal{I}')$ affin sík *projektív lezártja* legyen $\Pi = (\mathcal{P}, \mathcal{E}, \mathcal{I})$, ahol $\mathcal{P} = \mathcal{P}' \cup \mathcal{P}_\infty$, $\mathcal{E} = \mathcal{E}' \cup \{l_\infty\}$ és az ideális elemek illeszkedése: az ideális pontok a hozzájuk tartozó ekvivalencia osztály egyeneseire illeszkednek, az ideális egyenesek pedig csakis az ideális pontokra.

2.1.16. Állítás. *Affin sík projektív lezártja mindig projektív sík.*

Bizonyítás Lássuk be **P1**-et esetszétválasztással.

Affin pontokra: mivel **A1** és **P1** ugyanazt mondja ki affin és projektív síkok pontjaira, és mert ideális egyenes nem illeszkedik soha affin pontokra, **P1** teljesülni fog ezekre továbbra is. Ideális és affin pontokra: ideális pontokra csak akkor illeszkednek affin egyenesek, ha benne vannak a megfelelő ekvivalencia osztályban. **A2** axióma szerint pedig, ha egy e egyenesre nem illeszkedik egy P affin pont, akkor $!\exists$ e-vel párhuzamos egyenes, amelyre már illeszkedik. Ideális pontokra: illeszkedik rájuk az ideális egyenes, és bármely affin egyenes csak akkor illeszkedik egy ideális pontra, ha a neki megfelelő párhuzamossági osztályba tartozik. Ilyen pedig minden affin egyeneshez csak 1 létezhet.

Most pedig **P2**-t ugyanígy.

Affin egyenesek vagy metszik egymást, vagy párhuzamosak. Ha metszik egymást, nyilván nem egy osztályba tartoznak, így nincs közös ideális pontjuk. Ha párhuzamosak, akkor pedig nyilván épp fordítva. Affin egyenes a hozzá tartozó párhuzamossági osztályának ideális pontjában metszi az ideális egyenest csak, ahova vele csak párhuzamos affin egyenesek futnak be.

P3 és**P4** pedig egyértelmű. □

A következő tétel egyértelműen következik az eddigiekből.

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

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

2.1.18. Definíció. (Affin sík rendje) Ha az $\mathcal{A}$ affin sík minden egyenesére n pont illeszkedik, akkor az affin sík rendje n.

2.1.19. Tétel. *$\exists$ n-edrendű affin sík $\Leftrightarrow$ $\exists$ n-edrendű latin négyzetek teljes ortogonális rendszere.*

Bizonyítás Ez következik abból, hogy n-edrendű affin sík létezése ekvivalens n-edrendű projektív sík létezésével. □

2.1.3. Egzisztencia tételek

A következő tétel egy szükséges feltételt ad n-edrendű projektív síkok létezésére.

2.1.20. Tétel. (Bruck-Ryser) *Legyen $n \equiv 1, 2$ (mod 4). Ekkor csak akkor létezik n-edrendű projektív sík, ha n felírható 2 négyzetszám összegeként.*

(A bizonyítás megtalálható [4] könyv 1. fejezetében.)

2.1.21. Következmény. *A Bruck-Ryser csak szükséges feltételt ad. Ellenpéldaként említhetjük az 1898-ban bizonyított $n = 10$ esetet ([11]), amire: $10 \equiv 2$ (mod 4) és $10 = 1^2 + 3^2$, mégsem létezik 10-ed rendű projektív sík. Fontos megemlíteni, hogy a mai napig csak ezt az egy kivételt ismerjük.*

Viszont elmondhatjuk, hogy $n = 14$*-re vagy* $n = 21$*-re biztosan nem létezik ilyen rendű projektív sík, míg* 17*-ről például nem tudunk semmit a Bruck-Ryser alapján, mert* $17 = 4^2 + 1^2$.

A következő számelméleti lemma segítségével könnyű ellenőriznünk nagyobb számokra, hogy mely esetekben nem létezik a fenti felbontás.

2.1.22. Lemma. *Egy pozitív egész szám felírható legfeljebb két négyzetszám összegeként* $\Leftrightarrow$ *minden* $4k + 3$ *alakú prímosztója páros kitevőn szerepel.*

Szemléltetésképp lássuk be a fenti példáinkra, hogy nem írhatók fel két négyzetszám összegeként. Nyilván a 14 és a 21 nem négyzetszámok, ezért a lemma pont azt a feltételt vizsgálja, amire szükségünk van. Prímtényezős felbontásaikban páratlan kitevőn szerepel a 7: valóban nem létezhet ilyen rendű projektív sík.

A Bruck-Ryser tétel 1949-ben lett bebizonyítva, 1950-ben Bruck, Ryser és Chowla kiterjesztette blokkrendszerekre, melyeket a véges geometriák általánosításának tekintünk.

Szintén a blokkrendszerek elméletéből ismert Wilson tétel megfelelője latin négyzetekre a Chowla-Erdős-Straus tétel, melynek kulcsszerepe van Wilson tételének bizonyításában is.

2.1.23. Tétel. (Chowla-Erdős-Straus) $N(n) \to \infty$*, ha* $n \to \infty$.

2.2. Algebra

Említettük a bevezető részben, hogy a latin négyzetek nem mások, mint kvázicsoportok művelettáblái. Most ezt fogjuk vizsgálni, míg eljutunk algebrai úton az $N(n)$ egy becsléséhez.

2.2.1. Definíció. (Algebra) Egy $\mathcal{A}$ *algebra* alatt egy nem üres A halmazt értünk, és egy ezen értelmezett $\Omega = \omega_1, \omega_2, \ldots, \omega_k$ műveletcsaládot, melynek ω_i elemei $A^{n_i} \to A$ függvények ($n_i \geq 0$). Ekkor ω_i n_i változós függvényre $n_i = 0$ esetén azt mondjuk, konstans, $n_i = 1$ esetén egyváltozós (például csoportoknál az invertálás művelete), $n_i = 2$ esetén bináris, stb.

Jelölése: (A, Ω).

2.2.2. Definíció. (Kvázicsoport) *Kvázicsoportnak* nevezünk egy $\mathcal{A} = (A, .)$ algebrát, melyre:

$$\forall a, b \in A$$

mindkét egyenletnek

$$a.x = b, \quad y.a = b$$

pontosan egy megoldása létezik $x, y \in A$-ban.

Ekkor a megoldást a bal- és jobboldali inverzekkel írjuk fel: $x = a \backslash b$ és $y = b/a$.

2.2.3. Megjegyzés. Ez pedig egyértelműen azt jelenti, hogy a művelettábla egy latin négyzetet ad.

Próbáljuk meg ezeket a feltételeket átfogalmazni algebrai azonosságokra egy könnyebben kezelhező definíció érdekében.

2.2.4. Definíció. (Kvázicsoport axiomatikus felírása) Az $\mathcal{A} = (A, ., \backslash, /)$ algebrai stuktúra kvázicsoport, ha

1. A egy nem üres halmaz;
2. a három ezen értelmezett bináris műveletekre (szorzás: '.', baloldali osztás: '\' és a jobboldali osztás: '/') teljesül:
   (a) $\forall x, y \in A$:
   $$x.(x \backslash y) = y, \quad (y/x).x = y$$
   (b) $\forall x, y \in A$:
   $$x \backslash (x.y) = y, \quad (y.x)/x = y.$$

Az első pár azt jelenti, hogy $\exists\ u, v$ megoldása $x.u = y$ és $v.x = y$ egyenleteknek, mégpedig $u = (x \backslash y)$, $v = (y/x)$. A második pár pedig az egyértelműséget jelenti.

2.2.1. Páronként ortogonális latin négyzetek

Logikus feltenni a kérdést, hogy annak mi lehet a feltétele, hogy két kvázicsoport műveletttáblája ortogonális latin négyzetpárt adjon?

Először definiáljuk az ortogonális kvázicsoportokat, melyek művelettáblája ortogonális latin négyzeteket ad, majd megpróbáljuk átalakítani a feltételeket a kvázicsoportokéhoz hasonlóan csupán bináris műveletek és azonosságok segítségével.

2.2.5. Definíció. (Ortogonális kvázicsoportok) Legyen a két kvázicsoport $\mathcal{A}_1 = (A, .)$ és $\mathcal{A}_2 = (A, \circ)$. Azt mondjuk, hogy ezek *ortogonálisak*, ha

$$x.y = z.t \quad \wedge \quad x \circ y = z \circ t$$

$$(x, y, z, t \in A)$$

teljesül, akkor

$$x = z \quad \wedge \quad y = t.$$

Még egyszerűbben minden $a, b \in A$-ra egyértelműen létezzen megoldása a következő egyenletrendszernek:

$$x.y = a, \qquad x \circ y = b$$

ahol $x, y \in A$.

2.2.6. Megjegyzés. Fontos, hogy a két kvázicsoport alaphalmaza, így rendje is megegyezzen.

Nyilván a $x.y$ és $x \circ y$ műveletek meghatározzák latin négyzeteikben az x. sorban és y. oszlopban szereplő szimbólumot.

Legyen $\triangle$: $(a, b) \to x$ és $\triangledown : (a, b) \to y$, ahol $x.y = a$ és $x \circ y = b$ $(x, y, a, b \in A)$, tehát ezek a latin négyzetek egymásra helyezése után a szimbólumpárokhoz rendeli a négyzetbeli koordinátáikat ($\triangle$ az első koordinátát, $\triangledown$ a másodikat). Ezen műveletek leírására és egyértelműségére törekszünk.

Próbáljuk meg ezt is leírni bináris műveletek és azonosságok segítségével.

2.2.7. Definíció. Jelöljük a két – azonos A alaphalmazú – kvázicsoporthoz tartozó bináris műveletek a $(., /, \backslash)$ és $(\circ, \varnothing, \otimes)$ hármasokkal és hozzunk létre egy új $\mathcal{Q}^{(2)} = (A, /, \backslash, \circ, \varnothing, \otimes, \triangle, \triangledown)$ algebrai struktúrát a következő műveletekkel és azonosságokkal:

1. a 6 bináris művelet az $\mathcal{A}_1$ és $\mathcal{A}_2$ algebrákból;

2. a $4 - 4$ – előző részben található – kvázicsoport azonosság;

3. a fent leírt két bináris művelet: $x \vartriangle y$ és $x \triangledown y$;

4. 4 újabb azonosság a két új műveletre: $\forall x, y \in A$-ra:

$$(x.y) \vartriangle (x \circ y) = x, \quad (x.y) \triangledown (x \circ y) = y;$$

$$(x \vartriangle y).(x \triangledown y) = x, \quad (x \vartriangle y) \circ (x \triangledown y) = y.$$

Az első sor az új azonosságok definícióját adja meg, a másik ezek egyértelműségével ekvivalens.

Ekkor $\mathcal{Q}^{(2)}$ meghatároz 2 – A alaphalmazon értelmezett – ortogonális latin négyzetet. Fordítva is működik: adott két ortogonális latin négyzetből tudunk konstruálni ilyen struktúrát.

Azért is volt fontos a definíciók átírása azonosságokra és bináris műveletekre, hogy beláthassuk a következő tételeket.

2.2.8. Állítás. *Kvázicsoportok zártak a direkt szorzatra.*

Bizonyítás Legyen $\mathcal{A} = (A, ., /, \backslash)$ és $\mathcal{B} = (B, \circ, \varnothing, \oslash)$ két kvázicsoport. Ezek direkt szorzata:

$$\mathcal{A} \times \mathcal{B} = (A \times B, \cdot, /, \backslash),$$

ahol ha $|A| = a$ és $|B| = b$, akkor $|A \times B| = a \cdot B$, $A \times B$ elemei (a, b) alakú párok, ahol $a \in A$ és $b \in B$ és a műveleteket úgy definiáljuk, hogy: $(a, b) \cdot (c, d) = (a.c, b \circ d)$.

Így nyilván értelmesek a bináris műveletek és teljesülnek az azonosságok. $\square$

2.2.9. Állítás. *Két $\mathcal{Q}^{(2)}$ típusú algebrai struktúra direkt szorzata is $\mathcal{Q}^{(2)}$ típusú algebrai struktúra.*

Bizonyítás Legyen

$$\mathcal{Q}_1^{(2)} = (A, ._1, \circ_1, /_1, \backslash_1, \varnothing_1, \oslash_1, \vartriangle_1, \triangledown_1)$$

és

$$\mathcal{Q}_2^{(2)} = (B, ._2, \circ_2, /_2, \backslash_2, \varnothing_2, \oslash_2, \vartriangle_2, \triangledown_2)$$

a két struktúránk. Ezek direkt szorzata legyen:

$$\mathcal{Q}_1^{(2)} \times \mathcal{Q}_2^{(2)} = (A \times B, ., \circ, /, \backslash, \varnothing, \otimes, \triangle, \triangledown),$$

ahol a $*$ helyére beírva a bináris műveleteket jelentsék a következőt: $(a, b) * (a', b') = (a *_1 a', b *_2 b')$. Például a két szorzásra: $(a, b).(a', b') := (a._1 a', b._2 b')$ és $(a, b) \circ (a', b') := (a \circ_1 a', b \circ_2 b')$.

Egyrészről tudjuk, hogy kvázicsoportok direkt szorzata is kvázicsoport, másrészt pedig a fent látott módon definiált bináris műveletek továbbra is teljesíteni fogják az azonosságokat.

Így ha $\mathcal{A} = (A, ._1, /_1, \backslash_1), \mathcal{B} = (A, \circ_1, \varnothing_1, \otimes_1) \in \mathcal{Q}_1^{(2)}$ és $\mathcal{A}' = (B, ._2, /_2, \backslash_2), \mathcal{B}' = (B, \circ_2, \varnothing_2, \otimes_2) \in \mathcal{Q}_2^{(2)}$ az eredeti ortogonális kvázicsoportok, akkor az újak $(\mathcal{A} \times \mathcal{A}')$ és $(\mathcal{B} \times \mathcal{B}')$. $\square$

2.2.10. Tétel. *Van olyan $\mathcal{Q}^{(2)}$ típusú algebrai struktúra, amely tartalmaz olyan kvázicsoportot, melynek rendje prímhatványok szorzataként áll elő úgy, hogy $n = 2^{i_1} p_2^{i_2} \dots p_t^{i_t}$ (ahol p_i-k különböző prímek), esetén a kitevőkre teljesüljön: $i_1 \geq 2$ és $j > 1$-re $i_j \geq 1$.*

Bizonyítás $\forall p_j^{i_j}$-re létezik projektív sík, amiből tudunk konstruálni két $p_j^{i_j}$ rendű ortogonális latin négyzetet (ld. 2.1.12). (Többet is: mivel prímhatványok, létezik $p_j^{i_j} - 1$, de ehhez szükséges, hogy ha $p_j = 2$, akkor a kitevő nagyobb legyen 1-nél.)

Az ortogonális latin négyzetekből ortogonális kvázicsoportokat tudunk konstruálni. Ilyen prímhatványrendű ortogonális kvázicsoportból létrehozott $\mathcal{Q}^{(2)}$ típusú algebrai struktúrák direkt szorzataként könnyen kapunk a tételben említett rendű struktúrát. $\square$

2.2.2. MacNeish tétele

Az előző fejezetben leírt $\mathcal{Q}^{(k)}$ struktúrát konstruáltuk meg $k = 2$-re, most lássuk az általános definícióját:

2.2.11. Definíció. A $\mathcal{Q}^{(k)}$ algebra műveleteinek tekintsük k kvázicsoport művelethármasait, és vegyünk hozzá meg $2k(k-1)$ bináris műveletet.

Az egyenletek legyenek a kvázicsoportokhoz tartozó definícióból származó egyenletek. A maradék $2k(k-1)$ műveletet a ∇, $\triangle$ műveletek szerepére tartjuk fent, így latin négyzetpáronként lesz még 4 egyenletünk.

Így kapunk $2k(k-1)+3k$ bináris műveletet és $4k+4\cdot k(k-1)$ azonosságot.

2.2.12. Állítás. *A fent megadott $\mathcal{Q}^{(k)}$ struktúra zárt a direkt szorzatra.*

Bizonyítás 2.2.9 tétel általánosítása. □

2.2.13. Tétel. *Ha létezik k darab n-edrendű páronként ortogonális latin négyzet, akkor létezik n elemű alaphalmazon értelmezett $\mathcal{Q}^{(k)}$ típusú struktúra.*

Megfordítva, ha létezik n elemű alaphalmazon értelmezett $\mathcal{Q}^{(k)}$ típusú struktúra, akkor létezik k darab n-edrendű páronként ortogonális latin négyzet.

Bizonyítás Ha létezik k darab n-edrendű páronként ortogonális latin négyzet, akkor létezik ugyanennyi n-edrendű ortogonális kvázicsoport. Ezekhez hozzá véve a $\mathcal{Q}^{(k)}$ definíciójában felírt műveleteket és azonosságokat készen vagyunk.

A másik irány bizonyítása: ha van egy n elemű alaphalmazon értelmezett $\mathcal{Q}^{(k)}$ típusú struktúránk, akkor ezek szorzásainak művelettábláiból meg is kapjuk a latin négyzeteket. □

Ezek segítségével bizonyítsuk be a következő tételt.

2.2.14. Tétel. *Ha $n=p_1^{i_1}\dots p_t^{i_t}$ és $k+1\le \min p_j^{i_j}$, akkor létezik $\mathcal{Q}^{(k)}$ típusú struktúra n elemű alaphalmazon.*

Bizonyítás Legyen $n_1=p_1^{i_1}\ge k+1$, amire nyilván $k+1\ge 3$, hiszen ennél kisebb k-ra nem definiáltuk $\mathcal{Q}^{(k)}$-t.

Mivel n_1 prímhatvány, létezik ilyen rendű projektív sík, tehát $n_1-1\ge k$ darab páronként ortogonális latin négyzet is. Ekkor 2.2.13 tétel miatt létezik $\mathcal{Q}^{(k)}$ típusú struktúra.

Legyen általánosabban $n_j := p_j^{i_j}$ minden előforduló j-re. Ezek n_1 mintájára előállítanak egy-egy k darab páronként ortogonális latin négyzet-rendszert, melyekből építhető $\mathcal{Q}^{(k)}$ struktúra.

Korábbi ismereteink alapján ezek direkt szorzata is $\mathcal{Q}^{(k)}$ típusú struktúra, mégpedig n elemű. □

2.2.15. Következmény. *Ebből az is következik a 2.2.13 tétellel, hogy létezik k darab $n \times n$-es páronként ortogonális latin négyzet.*

Ezzel bebizonyítottuk MacNeish tételét is.

2.2.16. Tétel. (MacNeish) *Ha $n = p_1^{i_1} p_2^{i_2} \dots p_t^{i_t}$ akkor létezik k-elemű páronként ortogonális rendszere n-edrendű latin négyzeteknek (ahol $k + 1 \leq \min p_j^{i_j}$).*

2.2.17. Következmény. 1. *Tudjuk, hogy ha n prímhatvány, akkor: $N(n) = n - 1$.*

2. *MacNeish tétele bármilyen $n \geq 3$-ra azt jelenti, hogy $N(n) \geq p(n)$, ahol $n = p_1^{i_1} p_2^{i_2} \dots p_t^{i_t}$ és $p(n) = \min(p_1^{i_1}, p_2^{i_2}, \dots p_t^{i_t}) - 1$.*

3. *MacNeish azt sejtette, hogy $N(n) = p(n)$ is teljesül, ami az Euler-sejtést bebizonyította volna, ugyanis $p(n) = 1$ minden $n = 4k + 2$ alakú számra.*

   Nézzük $n = 10$ esetben. Ekkor $p(n) = \min(2^1, 5^1) - 1 = 1$, tehát a MacNeish tétel szerint $N(10) = 1$. Ennek is cáfolata ezért az E. T. Parker által mutatott 10-edrendű latin négyzetpár.

3. fejezet

Praktikus alkalmazások

3.1. Kísérletek tervezése

A latin négyzetek fontosságát a statisztikában és a kísérlettervezésben, mint már említettük, Ronald Fisher ismerte fel. 1935-ben megírt *Design of experiments* című könyve úttörőnek számít a témában.

Mi az ún. összehasonlító kísérletekkel foglalkozunk. Az *összehasonlító kísérletek* célja:

1. különböző kezelések/kezelés-kombinációk összehasonlítása;

2. ezek mérhető hatásainak összehasonlítása.

Egy összehasonlító kísérlet *faktoriális*, ha lehetővé teszi különböző kezelési módszerek egyidejű vizsgálatát.

Minden ilyen kísérletnek tartalmaznia kell *kísérleti egységeket*, melyeket hívnak *parcelláknak*, mezőgazdasági okokból[1], vagy *futamoknak* amiatt, ahogyan bizonyos kísérleteket végrehajtanak. Mi az általánosság megőrzése érdekében mintaként is hivatkozunk ezekre az egységekre.

A fejezet címe angolul *design of experiments (DOE)*, amit lehet kísérletek tervezésének, de kísérletek modelljének is fordítani. Amikor ezt definiáljuk, akkor inkább

[1]Sok esetben fizikailag is felosztják a földeket, hogy az így kapott parcellákra alkalmazhassák az adott módszerek egyikét.

kísérletek modelljét szeretnénk meghatározni.

Az alábbi definíció D. J. Finney-től származik.

3.1.1. Definíció. (Kísérletek modellje) *Kísérletek modellje* alatt egy olyan struktúrát értünk, mely tartalmazza

1. az összehasonlításra szánt kezelések halmazát;
2. a mintákra vonatkozó specifikációkat;
3. egy szabályt a kezelések mintákra való alkalmazására;
4. az elvégzendő megfigyelések, mérések specifikációit.

3.1.1. Fisher-féle kísérlettervezés

Egy jól megtervezett kísérletnek igazodnia kell a *Fisher-féle alapelvekhez*, amit úgy is szoktak hívni, hogy a *Három R (Three R's)*.

1. **Replikáció** (replication): a kezelések több kísérleti egységen is ki legyenek próbálva. Ez segít a hiba becslésében.
2. **Randomizáció** (randomization): a kezelések elosztásának véletlenszerűségére utal. Egy randomizációra akkor mondhatjuk, hogy megfelelő, ha minden parcella egyenlő eséllyel kapja a kezelések bármelyikét.

   Nagyon egyszerű módszer erre például, ha a kezeléseket vesszük a latin négyzetek szimbólumainak. Ekkor t féle kezelés esetén t-edrendű latin négyzetet veszünk, és annak sorainak permutációiból választunk egyet, majd egy ettől független permutációját vesszük ugyanezen négyzet oszlopainak.
3. **Zaj-faktorok kiszűrése** (reduce noise/blocking): a kísérleti egységek blokkokba rendezésének módszere. A csoportosításnak meg kell történnie még mielőtt a kezeléseket alkalmaznánk. Gyakran a blokkokkal törekszünk arra, hogy ugyanannyi kísérleti egységet tartalmazzanak.

3.1.2. Megjegyzés. A randomizációra egy híres példa a *Lady tasting tea* néven elterjedt randomizált kísérlet, mely Fisher már említett könyvéből származik.

A kísérletben szereplő hölgy 8 véletlen sorrendben adott csésze teáról próbálta meg eldönteni, hogy melyik készült először a tea, melyik a tej hozzáadásával. A 8 csészéből 4 az előbbi módszerrel, másik 4 az utóbbival készült. A kísérlet fontos eleme, hogy a döntést elég volt összehasonlításos alapon meghozni.

Most lássunk két egyszerű példát a hatékonyság szemléltetésére.

3.1.3. Példa. Szőtt késztermék mintázatát kell minőségileg összehasonlítani, ahol a különböző tényezők befolyásolhatják a minőséget:

1. 5 féle kikészítésű szál van,
2. 5 féle gép,
3. és 5 féle gépkezelő.

Ezekre tekintünk zaj-faktorokként.

Egyértelmű és egyszerű megoldás lenne minden lehetőséget megvizsgálni, de ez 125 kísérletet jelentene. A latin négyzetek segítségével rendezhetjük viszont a kísérleteket (ld. 3.1. ábra) úgy, hogy 25 kísérletet kelljen végrehajtani. Az ábrán S_i a szövőgépeket jelenti, K_i a munkásokat, Y_i pedig a szálak fajtáit ($i \in 1, 2, 3, 4, 5$).

	K_1	K_2	K_3	K_4	K_5
S_1	Y_1	Y_4	Y_5	Y_2	Y_3
S_2	Y_3	Y_1	Y_2	Y_4	Y_5
S_3	Y_2	Y_5	Y_1	Y_3	Y_4
S_4	Y_5	Y_3	Y_4	Y_1	Y_2
S_5	Y_4	Y_2	Y_3	Y_5	Y_1

3.1. ábra.

Így minden munkással az 5 munkanapon úgy kell végrehajtani a kísérleteket, hogy egy munkás a héten pontosan egyszer használjon minden fonalat és minden gépet.

Tekintsük a szálak által alkotott latin négyzetet, aminek szimbólumait számokra cserélve a 3.2 ábrán látható négyzetet kapjuk.

Vegyük még befolyásoló tényezőnek az 5 napot, amikor dolgoznak a munkások. Keressünk egy a fentire ortogonális négyzetet, mely a napokat fogja jelenteni. Új táblázatunk a kísérlet megtervezéséhez látható a 3.3 ábrán.

1	4	5	2	3
3	1	2	4	5
2	5	1	3	4
5	3	4	1	2
4	2	3	5	1

3.2. ábra.

	K_1	K_2	K_3	K_4	K_5
S_1	$1,1$	$4,2$	$5,4$	$2,3$	$3,5$
S_2	$3,3$	$1,4$	$2,1$	$4,5$	$5,2$
S_3	$2,2$	$5,3$	$1,5$	$3,4$	$4,1$
S_4	$5,5$	$3,1$	$4,3$	$1,2$	$2,4$
S_5	$4,4$	$2,5$	$3,2$	$5,1$	$1,3$

3.3. ábra.

Egy másik kísérlet a [10] könyvéből:

3.1.4. Példa. A kísérlet célja: a légszennyezettséget próbálták csökkenteni azáltal, hogy különböző, nagyon kis mennyiségű vegyszerekkel módósítottak egy benzin keveréket. Legyenek ezek a vegyianyagok A, B, C és D.

A 4 különböző eljárást 4 különböző autóval, 4 különböző sofőrrel tesztelték.

Felteszi a szerző a kérdést, miért nem inkább egy sofőrrel és egy autóval hajtjuk végre a kísérleteket? Ilyen módon bár standardizálnánk a feltételeket, a latin négyzet design-nak megvan az az előnye, hogy az általa végzett kísérletek nem csupán egy sofőrre és egy autóra vonatkoznak.

Tehát a különböző autók és sofőrök szerepe a beazonosítható zaj-faktorok kiszűrése a blokkosítás által, így biztosítva a kiegyensúlyozottságot.

A sofőrök jelölése: D_1, D_2, D_3, D_4, az autók jelölése pedig: C_1, C_2, C_3, C_4 szimbólumokkal történik.

A 3.4 ábra első táblázatában a vegyianyagok mellett a gépjárművek által kibocsátott légszennyező anyagok mértéke látható, melyeket két megfigyelést átlagolva kapunk. A második táblázat utolsó sora a legalacsonyabb érték és a legmagasabb közötti különbséget jelenti. Látszik, hogy a legnagyobb ingadozás a sofőrök esetében történik, míg különböző vegyianyagok esetében alacsonynak mondható.

	C_1	C_2	C_3	C_4
D_1	$A, 19$	$B, 24$	$C, 23$	$D, 26$
D_2	$D, 23$	$C, 24$	$A, 19$	$B, 30$
D_3	$B, 15$	$D, 14$	$C, 15$	$A, 16$
D_4	$C, 19$	$A, 18$	$B, 19$	$D, 16$

Gépjárművek	Sofőrök	Vegyianyagok
$C_1 : 19$	$D_1 : 23$	$A : 18$
$C_2 : 20$	$D_2 : 24$	$B : 22$
$C_3 : 19$	$D_3 : 15$	$C : 21$
$C_4 : 22$	$D_4 : 18$	$D : 19$
3	9	4

3.4. ábra. Kibocsátott légszennyező anyagok kísérletekre és átlagaik blokkokra

A nullhipotézis, hogy nincs különbség a 4 vegyianyag használata között, mely ellen az *ANOVA* (Analyis Of Variance) nevű eljárással (melynek leírása [10] könyvének 4. fejezetében található) nem találtak meggyőző bizonyítékot, ugyanakkor megmutatta, hogy a latin négyzet design hatékonysága nagy a sofőrök által keltett zajok kiszűrésében.

3.1.2. Néhány fontosabb modell

A legismertebb kísérleti módszer összehasonlító kísérletek elvégzésére az ún.

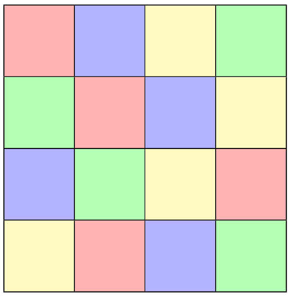
1. **Randomizált blokk design** (Randomized complete block design). Ez az elrendezés a standard módszer a mezőgazdaságban.

   Blokkokra osztva a parcellákat (ezeket egy táblázat soraiként képzelhetjük el) minden blokk pontosan egy parcellát rendel minden kezeléshez.

   Ennek egy ábrázolását ld. 3.5 ábrán: a sorokban a különböző színek jelölik a blokkokat, így ezt *sor-latin négyzetnek* is szokták nevezni.[2] Ezekre lehet alkalmazni a 4 féle kezelést/kezelés kombinációt.

2. **Sor és oszlop design** (Row and column design). Nagyon hasonlít az előző módszerre, de még egy csoportosítást el kell végeznünk, így nem csak a sorok, hanem az oszlopok is blokkokat alkotnak. A sorokból készült blokkok és az oszlopokból készültek fedik tehát egymást. Ezt az elrendezést mezőgazdasági kísérletek során alkalmazzák leggyakrabban. (A 3.6 ábrához hasonlóan a sorok és oszlopok metszetében a kísérleti egységek állnak ilyenkor.)

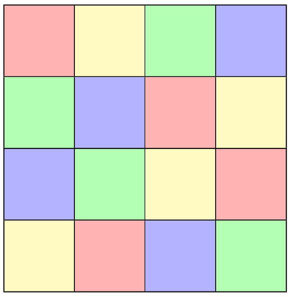
[2]Ebből már jön, hogy ha az oszlopokban fordul elő minden szimbólum pontosan egyszer, akkor *oszlop-latin*, és ha hagyományos latin négyzetről beszélünk, azt egyes irodalmak *sor-oszlop-latin négyzetnek* is nevezik.



3.5. ábra. Sor-latin négyzetes elrendezés

(a) A **latin négyzet design**. Ekkor a sor és oszlop design elrendezésének latin négyzetet veszünk. A legegyszerűbb sor és oszlop designként tartják számon. (Ld. 3.6 ábrát.)

(b) Vannak esetek, amikor két latin négyzetet egymás mellé téve készítünk sor és oszlop design-t (így a kapott elrendezés egy n sor és $2n$ oszlopból álló csoportosítás).



3.6. ábra. Latin négyzetes elrendezés

3.1.5. Megjegyzés. A latin négyzet design hátránya, hogy n oszlop, n sor és n féle kezelés kell egy ilyen kísérlet elvégzéséhez.

Mégis jó néhány eset van, ahol úgy adódnak a körülmények, hogy jól használható ez az elrendezés. Lássunk most néhányat, melyek precízebb leírása megtalálható [1] könyv 10. fejezetében.

1. Gyümölcsösökben, fák különböző kezelések melletti terméseinek összehasonlítására.

2. Üvegházakban az asztalok elhelyezkedése, a bent uralkodó hő és fényviszonyok miatt könnyen adódik a sor-oszlop design használata, habár ezek a tényezők nem feltétlenül segítik az ezen belüli latin négyzetes elrendezést.

3. Erdészeti kísérletek. Több forrás utal faiskolákban tett kísérletekre az 1920-as években, J. F. Box Fisher által végzett kísérletekről beszél, míg H. M. Steven angol erdők faiskoláiban $4, 5$ és 6-odrendű latin négyzet elrendezésekről ír.

4. Állatokkal végzett kísérletekről is olvashatunk.

   (a) Mézelő méhek különböző koncentrációjú lime-sulfur oldatra való reakciójának vizsgálatáról számol be C. G. Butler, D. J. Finney és P. Schiele 1943-ban.

   (b) 49 patkányon végeztek diétákat összemérő kísérleteket. Egy 7-edrendű latin négyzet sorai jelentették, hogy a lehetséges 7 alom közül melyikből származtak a patkányok, az oszlopok pedig a súlyaik szerint csoportosították őket, így csökkentve a zaj-faktorokat.

3.1.6. Megjegyzés. Előfordul, hogy változtatják a kezelések elrendezését, ugyanis még ha ki is hat az első kezelés valamennyire a mintára, megesik, hogy ennek jelentősége elég kicsi, így megéri váltani. Ilyet legfőképpen mezőgazdaságban láthatunk.

3.1.7. Megjegyzés. Vannak még a kísérleti modellek között olyanok, melyeknek közük van a latin négyzetekhez. Ilyen design-ok például a korábban látott (3.1.3 példa 2. része) görög-latin négyzetek, a fél-latin négyzetek vagy a latin kockák. Ezeknek részletezése szintén a [1] könyvben található.

A felfedezés jelentősége mind anyagilag, időben és etikai szempontból is óriási, gondoljunk például az állatkísérletekre, mezőgazdasági optimalizálási kísérletekre (haszonnövény termőképessége), oktatásfejlesztésre, kombinált gyógyszerterápiák hatékonyságának vizsgálatára vagy különböző pszichológiai kezelések kipróbálására.

3.2. Egy játék

3.2.1. Kamisado

Latin négyzeteknél leggyakrabban említett játék a *Kamisado*. Egy 8×8 részre osztott, színezett táblán játsszák, mely minden oszlopában és sorában minden szín pontosan egyszer szerepel.

3.7. ábra. A Kamisado táblája

A játék tervezőjének elmondása alapján a Kamisado alapötlete, hogy: *'[..] whatever colour you land on, your opponent must move a piece that matches this'*, azaz hogy bármilyen színre lépünk, a másik játékosnak is muszáj azonos színre tennie egy bábuját.

Érdekes kérdés lehet, hogy hány féle ilyen táblát lehetne konstruálni, hogy a játék igazságosságán ne változtasson?

A feladat átfogalmazva tehát, hogy keressünk olyan 8×8-as latin négyzetet, amely $180°$-os elforgatottra szimmetrikus. Ennek részletes átgondolását találhatjuk a [13] cikkben.

Köszönetnyilvánítás

Ezúton szeretném megköszönni témavezetőmnek, Szőnyi Tamásnak, hogy tartalmas előadásai során érdeklődést keltett bennem. Köszönöm türelmét, útmutatásra szánt idejét és energiáját. Köszönöm továbbá Zempléni Andrásnak a statisztikai részek átnézését, segítő tanácsait.

Hálával tartozom családomnak és barátaimnak a támogatásért, folyamatos bíztatásért.

Irodalomjegyzék

[1] J. Dénes, A.D. Keedwell, *Latin Squares*, *New developments in the theory and applications. Annals of Discrete Mathematics*, **46** (1991)

[2] J. Dénes, A.D. Keedwell, *Latin Squares and their Applications*

[3] Szőnyi Tamás, *Szimmetrikus Struktúrák*

[4] Kiss György, Szőnyi Tamás, *Véges geometriák* (2001)

[5] Kárteszi Ferenc, *Bevezetés a véges geometriákba*

[6] Dénes Tamás, *Latin négyzetek I.-II., Kömal* (2005 április,május), 194-199. és 262-269.

[7] Harris F. MacNeish, *Euler Squares*, *Annals of Mathematics (Second Series)* **Vol. 23** (1922), 221–227

[8] *Le problème des 36 officiers*, C. R. Assoc. Franc. Av. Sci. **29** (1900), 170–203.

[9] E. T. Parker, *Orthogonal Latin Squares*, *Proc. Nat. Acad. Sci. U.S.A.*, **45** (1959) 859–862.

[10] Box-Hunter-Hunter, *Statistics for experimenters*

[11] Clement W. H. Lam, Larry Thiel, S. Swiercz, *The Nonexistence of Finite Projective Planes of Order 10*, *Canad. J. Math.*,**41** (1989) 1117–1123.

[12] *http://hu.wikipedia.org*

[13] *http://math.stackexchange.com/questions/534531/how-many-latin-squares-are-there-with-the-following-restrictions*