Lajos Mátyás György

# Mintacsoportok

Szakdolgozat
matematika MSc

Témavezető:
Dr. Pálfy Péter Pál
Egyetemi tanár

Eötvös Loránd Tudományegyetem
Természettudományi kar
Algebra és Számelmélet tanszék
Budapest, 2017

# Tartalomjegyzék

**Bevezetés** 1

**Áttekintés** 1

**1. Alapfogalmak, jelölések, alapvető tulajdonságok** 3

**2. 2-nilpotenciaosztályú algebrák** 5

**3. Algebracsoportok generátorai** 7

**4. A Frattini- és a kommutátor-részcsoportok egyezése mintacsoportokban** 9

**5. Mintaalgebrák hatványai** 10

**6. A mintacsoportok alsó- és felső centrális láncai** 11

**7. Prímhatvány-rendű csoportok beágyazása $U_n(\mathbb{F}_p)$-be** 14

**8. A mintacsoportok mint $U_n(\mathbb{F})$ részcsoportjai** 15

**9. Mintacsoportok rész-algebracsoportjainak jellemzése** 18

**10.$(\mathrm{k}, \mathrm{m})$-típusú mintacsoportok** 19

**11.Az $\tilde{f}$ függvények rangja** 22

**12.Minimális rangú $\tilde{f}$ függvények** 24

**13.Mintacsoport-reprezentáció keresése adott generátorokkal** 25

**14.Incidencia-algebrák** 28

**Hivatkozások** 31

# Köszönetnyilvánítás

Meg szeretném köszönni témavezetőmnek, Pálfy Péter Pálnak a dolgozatom megírásához nyújtott segítséget.


# Bevezetés

A mintacsoportok azok a részcsoportjai $U_n(\mathbb{F})$-nek, amelyeknek bármely nemnulla és nem főátlóbeli mezőjét megváltoztatva benne maradunk a csoportban. Ezeket felfoghatjuk úgy is mint részbenrendezett halmazon definiált algebrák, vagy mint $U_n(\mathbb{F})$ diagonális elemmel való konjugálásra invariáns részcsoportjait. Dolgozatom központi kérdése az, hogy mit tudhatunk meg egy mintacsoportól, ha nem mátrixcsoportként, hanem valamilyen más módon van megadva. Vizsgálom nevezetes részcsoportjaikat, centrális láncaikat és generátorrendszereiket. Emellett leírok egy eljárást ami 2-nilpotenciaosztályú csoport esetén közelebb visz a mintacsoport-struktúra megismeréséhez és csak a csoport generátorainak kommutátorait kell ismerni a végrehajtásához. A másik fő probléma az a mintacsoportként való ábrázolhatóság jellemzése. Erre 2-nilpotenciaosztályú csoportok esetén is csak speciális esetben találtam választ.

# Áttekintés

1. fejezet: Bevezetem a dolgozatban használt alapvető fogalmakat és belátok néhány egyszerű állítást. A mintacsoportok felfoghatók speciális mátrixcsoportokként is és úgy is, mint részbenrendezett halmazon definiált algebrák. Ebben a fejezetben mindkét szemléletet ismertetem.

2. fejezet: Leírom a gyűrű- és csoportelméleti kommutátorok egyezését 2-nilpotenciaosztályú algebrákban. A továbbiakban nagy szerepe lesz a 2-nilpotenciaosztályú mintacsoportoknak. Bebizonyítom, hogy az ezekhez tartozó mintaalgebrák is 2-nilpotenciaosztályúak.

3. fejezet: A mintaalgebrai megfelelője alapján szükséges és elégséges feltételt adok arra, hogy egy mintacsoport részhalmaza generálja a csoportot.

4. fejezet: A mintaalgebrabeli szerkezetük alapján megmutatom, hogy egy mintacsoport kommutátor- és Frattini-részcsoportja megegyezik.

5. fejezet: Mintaalgebrák hatványai is mintaalgebrák. Jellemzem az ezekhez tartozó hatványmintákat.

6. fejezet: Mintacsoport alsó centrális láncának elemei megegyeznek a hozzá tartozó mintaalgebra hatványai által generált mintacsoportokkal. Ezért egy adott mintához tartozó mintacsoport és mintaalgebra nilpotenciaosztálya megegyezik és ez éppen a mintabeli leghosszabb lánc hossza. Megmutatom, hogy az alsó és felső

centrális láncok akkor esnek egybe, ha a mintában minden nem-bővíthető lánc ugyanolyan hosszú.

7. fejezet: Megmutatom, hogy minden véges $p$-csoport reprezentálható felsőháromszögmátrixszal. Ez választ ad arra, hogy mely csoportok ábrázolhatók mintacsoport részcsoportjaként.

8. fejezet: Még egy ekvivalens leírását adom a mintacsoportoknak mint $U_n(\mathbb{F})$ részcsoportjainak. Ennek bizonyítása betekintést nyújt a mintacsoportok automorfizmuscsoportjába.

9. fejezet: Ekvivalens jellemzést adok arra, hogy egy mintacsoport részcsoportja a megfelelő mintaalgebra egy részalgebrájához tartozó algebracsoport legyen és mutatok egy példát arra, amikor egy mintacsoport részcsoportja nem izomorf semmilyen algebracsoporttal.

10. fejezet: Definiálom a $(\mathrm{k}, \mathrm{m})$-típusú mintacsoportokat. Ezzel a 2-nilpotenciaosztályú csoportok struktúráját is jellemzem, ugyanis minden 2-nilpotenciaosztályú mintacsoport ábrázolható $(\mathrm{k}, \mathrm{m})$-típusú mintacsoportként.

11. fejezet: Definiálom a 2-nilpotenciaosztályú függvények centrumának értelmezett $f$ lineáris függvényekhez tartozó, az egész csoporton értelmezett $\tilde{f}$ függvényeket. Megmutatom, hogy ezek szimplektikus alakok és formulát adok a rangjukra.

12. fejezet: Vizsgálom azt az eljárást, ami az $r(\tilde{f})$ függvény által definiált súlyozás szerint keres minimális súlyú bázist egy 2-nilpotencia-osztályú mintacsoport centrumának duálisán. Ez az eljárás a mintacsoportként való ábrázolás ismerete nélkül is végrehajtható és információt ad az ábrázolásról.

13. fejezet: Szükséges és elégséges feltételt adok arra, hogy ábrázolható-e egy csoport mintacsoportként úgy hogy egy megadott halmaz elemei mind kanonikus csoportgenerátorba ($I + E(i, j)$-alakú elembe) menjenek.

14. fejezet: Ismertetem az incidencia-algebrák fogalmát és megmutatom, hogy ezek a mintacsoportoknak (és mintaalgebráknak) természetes kiterjesztései. Továbbá definiálom a redukált incidencia-algebra fogalmát és megadok egy feltételt, amiszerint eldönthető, hogy egy incidencia-algebra részalgebrája redukált incidencia-algebra-e.

# 1. Alapfogalmak, jelölések, alapvető tulajdonságok

**1.1. Jelölés.** Legyen $\mathcal{N} = \{1, ..., n\}$.

**1.2. Definíció.** Nevezzük **mintá**nak az $\mathcal{N} \times \mathcal{N}$ olyan $\mathcal{I}$ részhalmazait, ahol ha $(i, j) \in \mathcal{I}$, akkor $i < j$.

**1.3. Definíció.** Egy $\mathcal{I} \subset \mathcal{N} \times \mathcal{N}$ mintát akkor nevezünk **zárt**nak, ha $(i, j) \in \mathcal{I}, (j, k) \in \mathcal{I}$-ből következik $(i, k) \in \mathcal{I}$. Ekkor $\mathcal{I}$ egy részbenrendezést definiál $\mathcal{N}$-en.

**1.4. Jelölés.** Ezt a részbenrendezést jelöljük $<_{\mathcal{I}}$-vel (azaz $i <_{\mathcal{I}} j$ ha $(i, j) \in \mathcal{I}$).

**1.5. Jelölés.** Adott $\mathcal{I}$ mintára jelölje $\mathcal{I}^k$ azon $(i, j) \in \mathcal{I}$ elemeket, amelyek között a leghosszabb lánc $k$ hosszú, azaz létezik $x_1, ..., x_{k-1}$ :

$$i <_{\mathcal{I}} x_1 <_{\mathcal{I}} ... <_{\mathcal{I}} x_{k-1} <_{\mathcal{I}} j,$$

viszont ennél hosszabb lánc nem létezik. Így $\mathcal{I} = \mathcal{I}^1 \dot\cup ... \dot\cup \mathcal{I}^{l(\mathcal{I})}$ ahol $l(\mathcal{I})$ a leghosszabb $\mathcal{I}$-beli láncot jelöli.

**1.6. Jelölés.** Legyen $E(i, j) \in \mathbb{F}^{n \times n}$ az a mátrix, amelynek az $(i, j)$ mezőjében 1-es szerepel és az összes többi mezője 0.

**1.7. Állítás.** Adott $\mathcal{I} \subset \mathcal{N} \times \mathcal{N}$ minta. Az $\{E(i, j) | (i, j) \in I\}$ halmaz által generált lineáris altere $M_n(\mathbb{F}_q)$-nak pontosan akkor gyűrű a mátrixszorzásra nézve, ha $\mathcal{I}$ zárt.

**Bizonyítás:** A mátrixszorzás szabályai szerint

$$E(i, j)E(i', j') = \begin{cases} E(i, j'), \text{ ha } j = i' \\ 0 \text{ különben.} \end{cases}, \tag{1}$$

Ha $(i, j), (i', j') \in \mathcal{I}$ és $j = i'$, akkor a zártsági feltételből következik, hogy $(i, j') \in \mathcal{I}$. Ha pedig létezik $(i, j), (j, k) \in \mathcal{I}$ amire $(i, k) \notin \mathcal{I}$, akkor az $E(i, j)E(j, k)$ szorzás kivezet az altérből. □

**1.8. Definíció.** Ha $\mathcal{I} \subset \mathcal{N} \times \mathcal{N}$ zárt, akkor az $\{E(x) | x \in \mathcal{I}\} \subset \mathcal{A}$ által generált alteret nevezzük az $\mathcal{I}$-hez tartozó **mintaalgebrá**nak, jelöljük ezt $\mathcal{A}(\mathcal{I})$-vel.

**1.9. Definíció.** Az $\{E(i, j) | (i, j) \in \mathcal{I}\}$ halmazt nevezzük $\mathcal{A}(\mathcal{I})$ **kanonikus bázis**ának és jelöljük $\mathcal{B}_{\mathcal{A}}(\mathcal{I})$-vel. Az elemeit pedig nevezzük **kanonikus algebragenerátor**oknak.

**1.10. Definíció.** Egy $\mathcal{A}$ algebra $n$-edik hatványa azon elemekből áll, amelyik $\mathcal{A}$-beli $n$ tényezős szorzatok lineáris kombinációjaként állnak elő, azaz

$$\mathcal{A}^n = \left\{ \sum_i \left( t_i \prod_{j=1}^{n} A_{ij} \right) | t_i \in \mathbb{F}, A_{ij} \in \mathcal{A} \right\}.$$

**1.11. Definíció.** Ha van olyan $n \in \mathbb{N}$, amire $\mathcal{A}^{n+1} = 0$, azaz az algebrában minden $n+1$ tényezős szorzat 0, akkor $\mathcal{A}$ egy **nilpotens** algebra. Ilyenkor a legkisebb olyan $n_{\min}$ szám, amire $\mathcal{A}^{n_{\min}+1} = 0$ az algebra **nilpotencia-osztály**a. Jelöljük ezt nilp($\mathcal{A}$)-val.

**1.12. Tétel.** Legyen $\mathcal{A}$ tetszőleges nilpotens algebra. Legyen $I_{\mathcal{A}} = I$ egy olyan elem, hogy $IA = AI = A$ minden $A \in \mathcal{A}$-ra. Ezt az elemet hozzávéve $\mathcal{A}$-hoz kapunk egy $\bar{\mathcal{A}}$ egységelemes algebrát. Ekkor az $\{I_{\mathcal{A}} + A | A \in \mathcal{A}\} \subset \bar{\mathcal{A}}$ halmaz elemei az $\bar{\mathcal{A}}$-beli szorzás műveletére nézve csoportot alkotnak.

**Bizonyítás:** Ekkor

$$(I + A)(I + B) = I + A + B + AB,$$

tehát a szorzás nem vezet ki halmazból. Az $\mathcal{A}$-beli szorzás asszociativitása átöröklődik a csoport műveletére és az $(I + 0)$ elem egységelem lesz. Az $(I + A)$ elem inverze az

$$(I + A)^{-1} = I - A + A^2 - A^3 + A^4 \pm ... \pm (-A)^{\mathrm{nilp}(\mathcal{A})} = \sum_{i=0}^{\mathrm{nilp}(\mathcal{A})} (-A)^i,$$

elem, mivel $A^{\mathrm{nilp}(\mathcal{A})+1} = 0$. □

**1.13. Definíció.** Ezt a csoportot nevezzük az $\mathcal{A}$-hoz tartozó **algebracsoport**nak.

**1.14. Állítás.** Ha $X \in \mathcal{A}^k$, $Y \in \mathcal{A}^l$ akkor

$$[(I + X), (I + Y)] = (I + X)^{-1}(I + Y)^{-1}(I + X)(I + Y)] \in \{(I + A) | \mathcal{A}^{k+l}\}.$$

**Bizonyítás:** Behelyettesítve az előző bizonyításban felhasznált inverz-formulát és felbontva a zárójelet minden olyan tag amiben nem szerepel $X$ és $Y$ is kiesik (kivéve persze $I$-t). Bármely olyan szorzat amiben $X$ és $Y$ szerepel $\mathcal{A}^{k+l}$-ben van és így ezek összege is abban van. □

**1.15. Jelölés.** Adott $\mathcal{I}$ zárt mintára a

$$\mathcal{B}_{\mathcal{G}}(\mathcal{I}) = \{(I + E(i, j)) | (i, j) \in \mathcal{I}\}$$

halmaz elemeit nevezzük az $\mathcal{I}$-hez tartozó **kanonikus csoportgenerátor**oknak. A 3.1 állításnál látni fogjuk, hogy ha $\mathbb{F} = \mathbb{F}_p$ akkor ezek valóban generálják az $\mathcal{A}$-hoz tartozó algebracsoportot.

**1.16. Definíció.** Az $\mathcal{A}(\mathcal{I})$ mintaalgebra által generált algebracsoportot nevezzük az $\mathcal{I}$-hez tartozó **mintacsoport**nak, jelöljük ezt $\mathcal{G}(\mathcal{I})$-vel. Ezt angolul "pattern group"-nak vagy "partition subgroup"-nak mondják.

**1.17. Megjegyzés.** Mivel $E(i, j)^2 = 0$, ezért $(I + E(i, j))^{-1} = (I - E(i, j))$, viszont pl. $(I + E(i, j) + E(j, k))^{-1} = (I - E(i, j) - E(j, k) + E(i, k))$.

**1.18. Állítás.** Legyen $q = p^k$ a $p$ prímnek egy hatványa. Ha $\mathcal{A}$ egy $\mathbb{F}_q$ feletti algebra amelynek a nilpotencia-osztálya kisebb $p$-nél, akkor az $\mathcal{A}$-hoz tartozó $\mathcal{G}$ algebracsoport exponense $p$, azaz az egységelemen kívül minden elemének a rendje $p$.

**Bizonyítás:** Vegyünk egy tetszőleges $(I+A) \in \mathcal{G}$ elemet. Ekkor

$$(I+A)^p = \left(I + \binom{p}{1}A + \binom{p}{2}A^2 + ... + \binom{p}{1}A^{p-1} + A^p\right).$$

Mivel $\mathbb{F}_q$ egy $p$-karakterisztikájú test, $\binom{p}{k} = 0$ $\mathbb{F}_q$-ban, ha $1 \leq k \leq p-1$. Emellett az $\mathcal{A}$ nilpotencia-osztályáról tett feltevés miatt $A^p = 0$. Így az előző egyenletből azt kapjuk, hogy $(I+A)^p = (I+0)$. □

**1.19. Állítás.** Egy $\mathbb{F}_q$ feletti $n$-nilpotencia-osztályú algebrának legalább $q^n$ eleme van.

**Bizonyítás:** Vegyünk egy $n$ hosszú szorzatot ami nem 0: $\prod_{i=1}^{n} A_i \neq 0$. Legyen $P_k := \prod_{i=1}^{k} A_i$. Indirekten tegyük fel, hogy a $\{P_k | 1 \leq k \leq n\}$ halmaz lineárisan összefüggő $\mathbb{F}_q$ felett. Ez azt jelenti, hogy valamilyen $\{a_i\}$ együtthatókkal $\sum_{i=1}^{n} a_i P_i = 0$ és nem minden együttható nulla. Legyen $a_{i_0}$ a legkisebb nemnulla együttható. Ekkor

$$P_{i_0} = \sum_{i=i_0+1}^{n} \frac{-a_i}{a_{i_0}} P_i.$$

A $\prod_{i=1}^{n} A_i \neq 0$ szorzatba $\prod_{i=1}^{i_0} A_i$ helyére ezt behelyettesítve azt kapjuk, hogy

$$\left(\sum_{i=i_0+1}^{n} \frac{-a_i}{a_{i_0}} P_i\right) \prod_{i=i_0+1}^{n} A_i \neq 0.$$

Viszont ekkor felbontva a zárójelet az összeadandók közül legalább az egyik nem nulla, pedig az legalább $n+1$ $\mathcal{A}$-beli elem szorzata. Ez ellentmondás, ugyanis $\text{nilp}(\mathcal{A}) = n$. Tehát a $\{P_i | 1 \leq i \leq n\}$ halmaz valóban független. Ekkor az általa generált altér $q^n$ elemű.

**1.20. Jelölés.** Legyen $U_n(\mathbb{F})$ azon $M_n(\mathbb{F})$-beli felsőháromszögmátrixok halmaza, melyeknek a főátlójában mindenhol 1-es áll. Ez felfogható úgy is, mint az $n$ elemű teljesen rendezett halmazhoz tartozó mintacsoport.

# 2. 2-nilpotenciaosztályú algebrák

A továbbiakban a 2-nilpotencia osztályú algebrákkal fogunk foglalkozni. A gyűrű- és csoportelméleti kommutátorfogalmak a következők:

**2.1. Definíció.** Tetszőleges gyűrűben két elem **kommutátorá**nak az

$$[x,y]_R = xy - yx$$

elemet nevezzük.

**2.2. Definíció.** Tetszőleges csoportban két elem **kommutátorá**nak az

$$[x,y]_G = x^{-1}y^{-1}xy$$

elemet nevezzük.

A következő tétel szerint a 2-nilpotenciaosztályú algebrákon és a hozzájuk tartozó algebracsoportokon a csoportelméleti és gyűrűelméleti kommutátorfogalmak lényegében megegyeznek.

**2.3. Tétel.** Legyen $\mathcal{A}$ tetszőleges 2-nilpotenciaosztályú algebra, $\mathcal{G}$ a hozzá tartozó algebracsoport. Legyen $X, Y \in \mathcal{A}$. (A hozzájuk tartozó $\mathcal{G}$-beli elemek $(I+X)$ és $(I+Y)$.) Ekkor

$$(I + [X,Y]_R) = [(I+X),(I+Y)]_G.$$

**Bizonyítás:**

$$\begin{aligned}(I+X)^{-1}(I+Y)^{-1}(I+X)(I+Y) &= (I-X+X^2)(I-Y+Y^2)(I+X)(I+Y)\\ &= (I-X-Y+XY+X^2+Y^2)(I+X)(I+Y)\\ &= (I-Y+Y^2-XY+XY)(I+Y)\\ &= (I+XY-YX).\end{aligned}$$

Felhasználtuk, hogy minden $A \in \mathcal{A}$-ra $(1+A+A^2)(1-A) = 0$, illetve hogy a hármasszorzatok mind 0-k. □

A következő állítás mutatja, hogy a mintaalgebra kanonikus generátorai körében az (1)-ben meghatározott szorzás majdnem azonos a megfelelő mintacsoportbeli generátorok kommutálásával:

**2.4. Állítás.** Ha $i < j, i' < j'$:

$$[(I+E(i,j)),(I+E(i',j')] = \begin{cases}(I+E(i,j')), \text{ ha } j = i'\\ (I-E(i',j)), \text{ ha } j' = i\\ (I+0) \text{ különben.}\end{cases} \tag{2}$$

**Bizonyítás:** Az $\{E(i,j), E(i',j')\}$ halmaz egy (legfeljebb) 2-nilpotenciaosztályú algebrát generál, így alkalmazhatjuk erre az algebrára az előző tételt. Eszerint

$$[(I+E(i,j)),(I+E(i',j')] = (I+E(i,j)E(i',j') - E(i',j')E(i,j)),$$

ami (1) alapján épp a bizonyítandó képletet adja. □

**2.5. Tétel.** Adott egy $\mathcal{G}(\mathcal{I})$ mintacsoport. Ha $\mathcal{G}(\mathcal{I})$-nek mint csoportnak a nilpotenciaosztálya 2 (azaz $\forall x,y,z \in G : [[x,y],z] = 1$), akkor a hozzá tartozó $\mathcal{A}(\mathcal{I})$ nilpotenciaosztálya is 2 (azaz $\forall X,Y,Z \in \mathcal{A}(\mathcal{I}) : XYZ = 0$.)

**Bizonyítás:** Ha létezik olyan $X,Y,Z \in \mathcal{A}(\mathcal{I})$ hármas aminek a szorzata nem 0, akkor léteznie kell olyan $(i,j),(i',j'),(i'',j'') \in \mathcal{I}$ hármasnak is, amire

$$E(i,j)E(i',j')E(i'',j'') \neq 0,$$

ugyanis minden $\mathcal{A}(\mathcal{I})^3$-beli elem ilyenek lineáris kombinációjaként áll elő. De ez csak úgy lehet, ha $j = i'$ és $j' = i''$. Ekkor azonban a (2) képlet alapján

$$[[(I+E(i,j)),(I+E(i',j'))],(I+E(i'',j''))] = [(I+E(i,j')),(I+E(i'',j''))] = (I+E(i,j'')) \neq (I+0),$$

ellentmondva a $\mathcal{G}(\mathcal{I})$-ről tett feltevésnek.

# 3. Algebracsoportok generátorai

**3.1. Állítás.** Legyen $\mathcal{A}$ egy nilpotens algebra $\mathbb{F}_p$ felett (ahol $p$ prím) és $\mathcal{B} \subset A$. Ha minden $1 \leq m \leq \text{nilp}(\mathcal{A})$-ra van $\mathcal{B}_m \subset \mathcal{B}$, aminek az $\mathbb{F}_p$ feletti lineáris generátuma épp $\mathcal{A}^m$, akkor az

$$L = \{(I + B)|B \in \mathcal{B})\}$$

halmaz generálja az $\mathcal{A}$-hoz tartozó $\mathcal{G}$ algebracsoportot.

**Bizonyítás:** Indukció $\mathcal{A}$ nilpotencia-osztályára. A kezdőlépés triviális. Vegyük egy tetszőleges $A = \sum_{i=1}^{n} t_i B_i (t_i \in \mathbb{F}_p, B_i \in \mathcal{B})$ elemét $\mathcal{A}$-nak. Nézzük a

$$\prod_{i=1}^{n} (I + B_i)^{t_i} = (I + \mathcal{O}_2 + \sum_{i=1}^{n} t_i B_i)$$

szorzatot, ahol $\mathcal{O}_2 \in \mathcal{A}^2$. Ekkor $(I + \mathcal{O}_2)^{-1} \in (I + \mathcal{A}^2)$ ugyanis $\mathcal{A}^2$ is egy algebra. Szorozzuk meg az előző szorzatot $(I + \mathcal{O}_2)^{-1}$-zel:

$$\prod_{i=1}^{n} (I + B_i)^{t_i} (I + \mathcal{O}_2)^{-1} = ((I + \mathcal{O}_2) + \Sigma)(I + \mathcal{O}_2)^{-1} = (I + \Sigma + \Sigma((I + \mathcal{O}_2)^{-1} - I)),$$

ahol $\Sigma = \sum_{i=1}^{n} t_i B_i$. Mivel $((I + \mathcal{O}_2)^{-1} - I) \in \mathcal{A}^2$, $\mathcal{O}_3 := \Sigma((I + \mathcal{O}_2)^{-1} - I) \in \mathcal{A}^3$. Így az elsőrendű tag után következő tag rendjére vonatkozó indukcióval azt kapjuk, hogy

$$\prod_{i=1}^{n} (I + B_i)^{t_i} \prod_{j=2}^{m} (I + \mathcal{O}_j)^{-1} = (I + \mathcal{O}_{m+1} + \sum_{i=1}^{n} t_i B_i),$$

ahol $\mathcal{O}_{m+1} \in \mathcal{A}^{m+1}$. Legyen $m = \text{nilp}(\mathcal{A})$. Ekkor $\mathcal{O}_{m+1} = 0$, tehát

$$\prod_{i=1}^{n} (I + B_i)^{t_i} \prod_{j=2}^{m} (I + \mathcal{O}_j)^{-1} = (I + \sum_{i=1}^{n} t_i B_i).$$

Az első produktum $L$-beli elemek szorzata. Az $\mathcal{A}^2$ algebrára alkalmazható az eredeti (nilpotencia-osztály szerinti) indukció, ugyanis a nilpotencia-osztálya kisebb $\mathcal{A}$ nilpotencia-osztályánál és az $(\mathcal{A}^2)^k$ algebrát lineárisan generálja a $\mathcal{B}_{2k}$ halmaz. Az indukciós feltevés szerint az $(I + \mathcal{O}_j)^{-1} \in (I + \mathcal{A}^2)$ elemeket generálja az $\{(I + B)|B \in \mathcal{B}_2)\} \subset L$ halmaz, ezért a második produktum elemeit is generálja $L$, azaz $(I + A) \in \langle L \rangle$. Mivel $A$ tetszőleges volt, azt kaptuk, hogy $\mathcal{G} = \langle L \rangle$. □

**3.2. Megjegyzés.** Ha $\mathbb{F} \neq \mathbb{F}_p$, akkor hasonló bizonyítással kapjuk, hogy $L = \{(I + tB)|t \in \mathbb{F}, B \in \mathcal{B}\}$ generálja $\mathcal{G}$-t.

**3.3. Megjegyzés.** Ha $\mathcal{A}$ nilpotencia-osztálya 1, akkor bármely két elemének szorzata 0. Ekkor tehát egy $\mathcal{B} \subset \mathcal{A}$ halmaz által generált lineáris altere $\mathcal{A}$-nak megegyezik az általa generált részalgebrával. Ha $\mathcal{B}$ zárt az algebrabeli szorzásra, akkor is az általa generált algebra megegyezik az általa generált lineáris altérrel. A továbbiakban sokszor az előző esetek valamelyike áll fenn, ilyenkor egyszerűen $\mathcal{B}$ generátumáról beszélünk.

**3.4. Lemma.** Legyen $\mathcal{A}$ egy nilpotens algebra $\mathbb{F}_p$ felett és $\mathcal{B} \subset \mathcal{A}$. Ha $\{B + \mathcal{A}^2 | B \in \mathcal{B}\}$ nem generálja $\mathcal{A}/\mathcal{A}^2$-et, akkor az $\{(I+B)|B \in \mathcal{B}\}$ halmaz nem generálja az $\mathcal{A}$-hoz tartozó $\mathcal{G}$ algebracsoportot.

**Bizonyítás:** Legyen $X \in \mathcal{A}$ olyan, hogy a $\{B+\mathcal{A}^2|B \in \mathcal{B}\}$ halmaz nem generálja $X+\mathcal{A}^2$-et. Ha $\mathcal{G}$ generálná $(I+X)$-et, akkor lenne egy

$$(I+X) = \prod_i (I+B_i)^{\varepsilon_i}$$

alakú előállítása, ahol $(B_i \in \mathcal{B}, \varepsilon_i \in \{-1,+1\})$. Viszont $(I+B)^{-1} = (I-B_i+\mathcal{O}_2^i)$ valamely $\mathcal{O}_2^i \in \mathcal{A}^2$-ra, ezért

$$\prod_i (I+B_i)^{\varepsilon_i} = (I+\mathcal{O}_2' + \sum_i \varepsilon_i B_i)$$

valamely $\mathcal{O}_2' \in \mathcal{A}^2$-re. De ez azt jelentené, hogy $X = \mathcal{O}_2' + \sum_i \varepsilon_i B_i$, amiből következik, hogy $X + \mathcal{A}^2 = \sum_i \varepsilon_i B_i + \mathcal{A}^2$ pedig feltettük, hogy nem. □

**3.5. Lemma.** Legyen $\mathcal{A}$ egy nilpotens algebra $\mathbb{F}_p$ felett, $A \in \mathcal{A}^2$ és legyen $\mathcal{B}$ olyan halmaz, amire $\{B + \mathcal{A}^2 | B \in \mathcal{B}\}$ nem generálja $\mathcal{A}/\mathcal{A}^2$-et. Ekkor $\{(I+B)|B \in \mathcal{B}\} \cup \{(I+A)\}$ sem generálja az $\mathcal{A}$-hoz tartozó $\mathcal{G}$ csoportalgebrát.

**Bizonyítás:** A $\{B+\mathcal{A}^2|B \in (\mathcal{B} \cup \{A\})\}$ halmaz sem generálja $\mathcal{A}/\mathcal{A}^2$-et, tehát a 3.4 lemma szerint $\{(I+B)|B \in \mathcal{B}\} \cup \{(I+A)\}$ nem generálja $\mathcal{G}$-t. □

Az 3.4 lemma megfordítása is igaz:

**3.6. Állítás.** Legyen $\mathcal{A}$ egy nilpotens algebra $\mathbb{F}_p$ felett és legyen $\mathcal{B} \subset \mathcal{A}$ olyan, hogy $\{B+\mathcal{A}^2|B \in \mathcal{B}\}$ generálja $\mathcal{A}/\mathcal{A}^2$-et. Ekkor az $L = \{(I+B)|\mathcal{B}\}$ generálja az $\mathcal{A}$-hoz tartozó $\mathcal{G}$ csoportot.

**Bizonyítás:** Tegyük fel, hogy $L$ nem generálja $\mathcal{G}$-t. Legyen $\mathcal{B}' := \mathcal{B} \cup \mathcal{A}^2$ és $L' = \{(I+B)|B \in \mathcal{B}'\}$. Ekkor a 3.5 állítás szerint $\mathcal{L}'$ sem generálja $\mathcal{G}$-t. De $\mathcal{B}'$-re teljesülnek a 3.1 állítás feltételei, ugyanis abból, hogy $\{B + \mathcal{A}^2|B \in \mathcal{B}'\}$ generálja $\mathcal{A}/\mathcal{A}^2$-et és $\mathcal{A}^2 \subset \mathcal{B}'$ következik, hogy $\mathcal{B}'$ generálja $\mathcal{A}$-t. Viszont így a 3.1 állítás szerint $L'$ generálja $\mathcal{G}$-t és ez ellentmondás. □

**3.7. Állítás.** Legyen $\mathcal{A}$ egy nilpotens algebra $\mathbb{F}_p$ felett és $\mathcal{B} \subset \mathcal{A}$ olyan, hogy $\{(I+B)|B \in \mathcal{B}\}$ generálja $\mathcal{G}$-t. Ekkor $\{B + \mathcal{A}^2|B \in \mathcal{B}\}$ generálja $\mathcal{A}/\mathcal{A}^2$-et.

**Bizonyítás:** Legyen a $\mathcal{B}$ elemei által generált algebra $\bar{\mathcal{B}} \subsetneq \mathcal{A}$. Tegyük fel, hogy $\{B + \mathcal{A}^2|B \in \mathcal{B}\}$ nem generálja $\mathcal{A}/\mathcal{A}^2$-et. Ekkor a $\bar{\mathcal{B}} \cup \mathcal{A}^2$ által generált algebra nem $\mathcal{A}$. Viszont $B_1B_2 \in \bar{\mathcal{B}}, A_1, A_2 \in \mathcal{A}^2$-re

$$(I+B_1+A_1)(I+B_2+A_2) = (I+(B_1+B_2)+(B_1B_2+B_1A_2+B_2A_1+B_2A_2))$$
$$(I+B_1+A_1)^{-1} = (I-(B_1+A_1)+(B_1+A_1)^2 \mp ...) = (I-B_1+(-A_1+B_1^2+...)).$$

A fenti egyenletek mutatják, hogy a csoportműveletek nem vezetnek ki a $\{(I+B+A)|B \in \bar{\mathcal{B}} + \mathcal{A}^2\}$ halmazból. Ez tartalmazza $\{(I+B)|B \in \mathbb{B}\}$-t, ami elvileg generálja $\mathcal{G}$-t, de $\bar{\mathcal{B}} \cup \mathcal{A}^2 \subsetneq A$, és ez ellentmondás. □

**3.8. Tétel.** Legyen $\mathcal{A}$ egy nilpotens algebra és $\mathcal{G}$ a hozzá tartozó algebracsoport. Egy $\mathcal{B} \subset \mathcal{A}$ halmazra ekvivalens a következő két állítás

(i) $\{(I+B)|B \in \mathcal{B}\}$ generálja $\mathcal{G}$-t.

(ii) $\{B+\mathcal{A}^2|B \in \mathcal{B}\}$ generálja $\mathcal{A}/\mathcal{A}^2$-et.

**Bizonyítás:** Ez a 3.6 és 3.7 állítások összegzése. □

**3.9. Állítás.** Az $\{(I+E(x)|x \in \mathcal{I}^1\}$ halmaz generálja az egész $\mathcal{G}(\mathcal{I})$ csoportot ha az alaptest $\mathbb{F}_p$. (Az $\mathcal{I}^1$ jelölést a 1.5 pontban vezettük be.)
**Bizonyítás:** Az $\{E(x)+\mathcal{A}(\mathcal{I})^2|x \in \mathcal{I}^1\} \subset \mathcal{A}(\mathcal{I})$ halmaz generálja $(\mathcal{A}(\mathcal{I}))/(\mathcal{A}(\mathcal{I})^2)$-et, ugyanis $\{E(x)|x \in \mathcal{I}\}$ generálja $\mathcal{A}(\mathcal{I})$-t és $x \in \mathcal{I} \setminus \mathcal{I}^1$-re $E(x) \in \mathcal{A}(\mathcal{I})^2$. □

# 4. A Frattini- és a kommutátor-részcsoportok egyezése mintacsoportokban

**4.1. Lemma.** A $\{E(x)|x \in (\mathcal{I} \setminus \mathcal{I}^1)\}$ halmaz által generált algebra $\mathcal{A}(\mathcal{I})^2$.
**Bizonyítás:** Ez egy speciális esete a 5.1 tételnek.

**4.2. Állítás.** Egy $\mathbb{F}_p$ alaptest feletti $\mathcal{G}(\mathcal{I})$ mintacsoport kommutátora megegyezik az $\mathcal{A}(\mathcal{I})^2$-hez tartozó algebracsoporttal, azaz

$$\mathcal{G}(\mathcal{I})' = \{(I+A|A \in \mathcal{A}(\mathcal{I})^2\}.$$

**Bizonyítás:** Ha $x=(i,j) \notin \mathcal{I}^1$ akkor $\exists k : i <_{\mathcal{I}} k <_{\mathcal{I}} j$, tehát a (2) egyenlet szerint $[(I+E(i,k)),(I+E(k,j))] = (I+E(i,k))$, azaz $(I+E(i,k)) \in \mathcal{G}(\mathcal{I})'$. Az $\{(I+E(i,k))|(i,k) \in (\mathcal{I} \setminus \mathcal{I}^1)\}$ elemek által generált csoport a 3.1 állítás szerint megegyezik az $\{E(i,k)|(i,k) \in (\mathcal{I} \setminus \mathcal{I}^1)\}$ által generált algebrával ami a 4.1 lemma szerint épp $\mathcal{A}(\mathcal{I})^2$, tehát a $\supseteq$ tartalmazás teljesül.
A másik irányhoz vegyünk egy $(I+A) \in \mathcal{G}(\mathcal{I})'$ elemet amire $\exists B_1, B_2 \in \mathcal{A}(\mathcal{I}) : [(I+B_1),(I+B_2)] = (I+A)$. Ez azt jelenti, hogy

$$(I+B_1)(I+B_2) = (I+B_2)(I+B_1)(I+A).$$

Felbontva a zárójelet és átrendezve azt kapjuk, hogy

$$I+B_1+B_2+B_1B_2 = I+B_2+B_1+A+B_2B_1+B_2A+B_1A+B_2B_1A$$
$$A = B_1B_2-B_2B_1-B_2A-B_1A-B_2B_1A.$$

Ebből következik, hogy $A \in \mathcal{A}(\mathcal{I})^2$ tehát a jobb oldal tartalmazza $(I+A)$-t. Az $[(I+B_1),(I+B_2)]$ alakú elemek pedig definíció szerint generálják $\mathcal{G}(\mathcal{I})'$-t. Ezzel beláttuk a $\subseteq$ tartalmazást is. □

**4.3. Megjegyzés.** A bizonyításból kiolvasható, hogy tetszőleges $\mathcal{A}$ algebrára a hozzátartozó algebracsoport kommutátorrészcsoportja benne van az algebra négyzete által generált algebracsoportban. A másik irányú tartalmazáshoz arra volt szükségünk, hogy $\mathcal{A}$-nak van olyan lineáris generátorrendszere, amelyben bármely két báziselem által generált algebra nilpotencia-osztálya legfeljebb 2.

**4.4. Tétel.** Legyen $\mathcal{A}$ egy nilpotens algebra $\mathbb{F}_p$ alaptesttel és $\mathcal{G}$ a hozzá tartozó algebracsoport. Az $\{(I+A)|A \in \mathcal{A}^2\}$ csoport elemei pontosan azok a $\mathcal{G}$-beli elemek, amelyek $\mathcal{G}$ bármely generátorrendszeréből elhagyhatóak.

**Bizonyítás:** Legyen $A \in \mathcal{A}(\mathcal{I})^2$ és vegyünk egy $\mathcal{B}$ halmazt amire $A \in \mathcal{B}$ és $A \in \mathcal{B}$ és$\{(I+B)|B \in \mathcal{B}\}$ generálja $\mathcal{G}(\mathcal{I})$-t. A 3.8 tétel szerint $\{B+\mathcal{A}^2|B \in \mathcal{B}\}$ generálja $\mathcal{A}/\mathcal{A}^2$-et. Ekkor $\mathcal{B} \setminus \{A\}$ is generálja $\mathcal{A}/\mathcal{A}^2$-et tehát a 3.8 tétel másik iránya szerint $\{(I+B)|B \in (\mathcal{B} \setminus \{A\})\}$ generálja $\mathcal{G}(\mathcal{I})$-t. Azt kaptuk tehát, hogy $(I+A)$ egy tetszőlegesen választott generátorrendszerből elhagyható volt.
Legyen $A \notin \mathcal{A}^2$. Ekkor $A+\mathcal{A}^2 \neq \mathcal{A}^2$, így $A+\mathcal{A}^2$ kiegészíthető $\mathcal{A}/\mathcal{A}^2$ bázisává. Legyen ez a bázis $\{B+\mathcal{A}^2|B \in \mathcal{B}\}$ és válasszuk $\mathcal{B}$-t úgy, hogy $A \in \mathcal{B}$ legyen. Ekkor a 3.8 tétel szerint $\{(I+B)|B \in \mathcal{B}\}$ generálja $\mathcal{G}$-t. Viszont $\{B+\mathcal{A}^2|B \in \mathcal{B}'\}$ semmilyen $\mathcal{B}' \subsetneq \mathcal{B}$-re se generálja $\mathcal{A}/\mathcal{A}^2$-et ami a 3.8 tétel szerint ekvivalens azzal, hogy $\{(I+B)|B \in \mathcal{B}'\}$ semmilyen $\mathcal{B}' \subsetneq \mathcal{B}$-re se generálja $\mathcal{G}$-t, azaz $\{(I+B)|B \in \mathcal{B}\}$ egy minimális generátorrendszer. Ezzel bebizonyítottuk az állítást, ugyanis $(I+A) \in \{(I+B)|B \in \mathcal{B}\}$. □

**4.5. Definíció.** Egy $G$ csoport **Frattini-részcsoport**ja a maximális részcsoportjainak a metszete, azaz

$$\Phi(G) = \bigcap_{\substack{M<G \\ \text{maximális}}} M.$$

**4.6. Tétel.** Egy csoport Frattini-részcsoportja pontosan azokból az elemekből áll, amelyek minden generátorrendszerből elhagyhatóak.

**Bizonyítás:** Ez a [1] jegyzet 5. fejezetének 3. tétele. □

**4.7. Tétel.** ([2] 2.1-ben ezt $U_n(\mathbb{F})$-re mondja ki.) Minden $\mathbb{F}_p$ feletti $\mathcal{G}(\mathcal{I})$ mintacsoportban $\Phi(\mathcal{G}(\mathcal{I})) = \mathcal{G}(\mathcal{I})'$, azaz a Frattini-részcsoport megegyezik a kommutátorral.

**Bizonyítás:** A 4.4 és 4.6 tételeket összetéve azt kapjuk, hogy

$$\Phi(\mathcal{G}(\mathcal{I})) = \{(I+A)|A \in \mathcal{A}(\mathcal{I})^2\}.$$

A 4.2 állítás szerint pedig a jobb oldal éppen $\mathcal{G}(\mathcal{I})$ kommutátor-részcsoportja. □

# 5. Mintaalgebrák hatványai

**5.1. Tétel.** Az $\mathcal{A}(\mathcal{I})^k$ algebra megegyezik az

$$H = \left\{ E(x)|x \in \bigcup_{i=k}^{l(\mathcal{I})} \mathcal{I}^i \right\}$$

halmaz által generált algebrával.

**Bizonyítás:** Mindkét algebra egyenlő az általa tartalmazatt kanonikus algebragenerátorok által generált algebrával. Ha $E(a,b) \in \mathcal{A}^k$ akkor

$$E(a,b) = \prod_{i=1}^{k} E(a_i, b_i)$$

ahol $a_1 = a$ és $b_k = b$. Szükségszerűen $b_i = a_{i+1}$-nek kell lennie, különben a szorzat 0 lenne, így $a = a_1 <_{\mathcal{I}} ... <_{\mathcal{I}} a_k <_{\mathcal{I}} b_k = b$ egy $k$ hosszú lánc, így $(a,b) \in \bigcup_{i=k}^{l(\mathcal{I})} \mathcal{I}^i$. Fordítva, ha $(a,b) \in \mathcal{I}^j$ valamely $j \geq k$-ra, akkor van $j$ hosszú lánc $a$ és $b$ között amiből $j$ tagú szorzatként elő tudjuk állítani $E(a,b)$-t. □

**5.2. Megjegyzés.** Mivel $\bigcup_{i=k}^{l(\mathcal{I})}$ egy zárt minta, mondhatjuk azt is, hogy

$$H = \mathcal{A}\left(\bigcup_{i=k}^{l(\mathcal{I})} \mathcal{I}^i\right) = \mathcal{A}(\mathcal{I})^k.$$

# 6. A mintacsoportok alsó- és felső centrális láncai

([2] 2.1. alapján, annak állításait általánosítva)

**6.1. Definíció.** Egy $G$ csoport **alsó centrális lánc**ának a következő $(\gamma_i(G))$ rekurzíven definiált sorozatot nevezzük:

$$\gamma_1(G) := G$$
$$\gamma_i(G) := [\gamma_{i-1}(G), G].$$

**6.2. Lemma.** Minden $(i,j) \in \mathcal{I}^k$-ra $(I + E(i,j)) \in \gamma_k(\mathcal{G}(\mathcal{I}))$.

**Bizonyítás:** Indukcióval. Vegyünk egy $(i,j)$-hez tartozó $i <_{\mathcal{I}} x_1 <_{\mathcal{I}} ... <_{\mathcal{I}} x_{k-1} <_{\mathcal{I}} j$ láncot. Ekkor $(i, x_{k-1}) \in \mathcal{I}^{k-1}$ ugyanis van $i$ és $x_{k-1}$ között $k-1$-hosszú lánc és ha lenne köztük $k$ hosszú akkor ezt behelyettesítve az eredeti lánc $i$ és $x_{k-1}$ közti szakaszaa helyére $k$-nál hosszabb láncot kapnánk $i$ és $j$ között pedig $(i,j) \in \mathcal{I}^k$ miatt ilyen nincs.
Abból, hogy $(i, x_{k-1}) \in \mathcal{I}^{k-1}$ az indukciós feltevés szerint következik, hogy $(I + E(i, x_{k-1}) \in \gamma_{k-1}(\mathcal{G}(\mathcal{I}))$. Ekkor

$$[(I + E(i, x_{k-1})), (I + E(x_{k-1}, j))] = (I + E(i,j))$$

miatt $(I + E(i,j)) \in \gamma_k(\mathcal{G}(\mathcal{I}))$. □

**6.3. Tétel.** Ha $\mathcal{G}(\mathcal{I})$ egy $\mathbb{F}_p$-alaptestű mintacsoport, akkor

$$\gamma_k(\mathcal{G}(\mathcal{I})) = \{(I + A) | A \in \mathcal{A}(\mathcal{I})^k\}$$

.

**Bizonyítás:** A 3.1 állítás szerint az $\{(I + E(x)|x \in \bigcup_{j=k}^{l(\mathcal{I})} \mathcal{I}^j\}$ halmaz generálja az $\{E(x)|x \in \bigcup_{j=k}^{l(\mathcal{I})} \mathcal{I}^j\}$ által generált algebrához tartozó algebracsoportot. A 5.1 tétel szerint ez éppen $\{(I+A)|A \in \mathcal{A}(\mathcal{I})^k\}$. A 6.2 lemma szerint $\{(I+E(x))|x \in \bigcup_{j=k}^{l(\mathcal{I})} \mathcal{I}^j\} \subset \gamma_k(\mathcal{G}(\mathcal{I}))$, így a tétel $\supseteq$ irányát bebizonyítottuk.
Indukció miatt feltehetjük, hogy tetszőleges $(I + A) \in \gamma_{k-1}(\mathcal{G}(\mathcal{I}))$ elemre $A \in \mathcal{A}(\mathcal{I})^{k-1}$. A 1.14 állítás szerint ha $A \in \mathcal{A}(\mathcal{I})^{k-1}, B \in \mathcal{A}(\mathcal{I})$ akkor $[(I + A), (I + B)] = (I + C)$ valamely $C \in \mathcal{A}(\mathcal{I})^k$-re. Ezzel beláttuk a $\subseteq$ irányt. □

**6.4. Definíció.** Egy $G$ csoport **felső centrális lánc**ának a következő $(Z_i(G))$ rekurzíven definiált sorozatot nevezzük:

$$Z_0(G) := 1$$
$$Z_i(G) := \{g \in G : [g, G] \subset Z_{i-1}(G)\}$$

**6.5. Jelölés.** Jelöljük $\rho(x)$-szel a leghosszabb olyan lánc $\mathcal{I}$-beli lánc hosszát, aminek az első eleme $x \in \mathcal{N}$ és jelöljük $\kappa(x)$ a leghosszabb olyan lánc hosszát, aminek a vége $x$.

**6.6. Jelölés.** Legyen

$$\mathcal{I}_k = \{(i, j) \in \mathcal{I}|\kappa(i) + \rho(j) = k\}.$$

**6.7. Lemma.** Ha $x <_{\mathcal{I}} y <_{\mathcal{I}} z$ és $(x, y) \in \mathcal{I}_k$, akkor $(x, z) \in \bigcup_{i=0}^{k-1} \mathcal{I}_i$. Ha $(y, z) \in \mathcal{I}_{k'}$ akkor pedig $(x, z) \in \bigcup_{i=0}^{k'-1} \mathcal{I}_i$.
**Bizonyítás:** A $z$-ből induló leghosszabb lánc elejéhez hozzávéve $y$-t egy eggyel hosszabb láncot kapunk, így $\rho(y) > \rho(z)$. Így $k = \kappa(x) + \rho(y) > \kappa(x) + \rho(z) \Rightarrow (x, z) \in \bigcup_{i=0}^{k-1} \mathcal{I}_i$. A másik állítás bizonyítása hasonlóan megy. □

**6.8. Tétel.**

$$Z_k(\mathcal{G}(\mathcal{I})) = \left\{(I + A)|A \in \mathcal{A}\left(\bigcup_{i=0}^{k-1} \mathcal{I}_i\right)\right\}.$$

**6.9. Megjegyzés.** Ahhoz hogy a jobb oldal értelmes legyen a $\bigcup_{i=0}^{k-1} \mathcal{I}_k$ mintának zártnak kell lennie. Ez viszont igaz, ugyanis $x <_{\mathcal{I}} y <_{\mathcal{I}} z$ esetén a 6.7 lemma szerint $(x, z) \in \bigcup_{i=0}^{k-1} \mathcal{I}_i$.
**Bizonyítás:** Indukcióval bizonyítunk. A kezdőlépés $Z_1(\mathcal{G}(\mathcal{I})) = Z(\mathcal{G}(\mathcal{I})) = \mathcal{A}(\mathcal{I}_0)$. Tegyük fel, hogy $k - 1$-re tudjuk, hogy igaz az állítás. Legyen $(a, b) \in \mathcal{I}_k, (a', b') \in \mathcal{I}$. Ekkor $E(a, b)E(a', b') \in \mathcal{A}\left(\bigcup_{i=0}^{k-1} \mathcal{I}_i\right)$ ugyanis ez vagy 0 vagy $E(a, b')$ és a 6.7 lemmát az $a <_{\mathcal{I}} b = a' <_{\mathcal{I}} b'$ sorozatra alkalmazva kapjuk, hogy $(a, b') \in \bigcup_{i=0}^{k-2} \mathcal{I}_i$. Ehhez hasonlóan megkapjuk, hogy $E(a', b')E(a, b) \in \mathcal{A}\left(\bigcup_{i=0}^{k-2} \mathcal{I}_i\right)$.
Legyen $X \in \mathcal{A}\left(\bigcup_{i=0}^{k-1} \mathcal{I}_i\right)$ és $Y \in \mathcal{I}$. A $[(I + X), (I + Y)]$ kommutátorban felbontva a zárójeleket egy olyan polinomot kapunk, amelyben minden (nem nullaegyüttható) tagban szerepel az $X$ (az $I$ kivételével). Viszont $X$ lineáris kombinációja $E(a, b), (a, b) \in \bigcup_{i=0}^{k-1} \mathcal{I}_i$

elemeknek, amiket az előzőek szerint bármivel megszorozva $\mathcal{A}\left(\bigcup_{i=0}^{k-2}\mathcal{I}_i\right)$-beli elemet kapunk. Ezzel a $\supseteq$ tartalmazást beláttuk.
A másik irányhoz legyen $X$ olyan, hogy valamely $k' \geq k$-ra és $(a,b) \in \mathcal{I}_{k'}$-re $E(a,b)$ nemnulla együtthatóval szerepel $X$ felírásában. Ha $a$ minimális és $b$ maximális lenne, akkor $(I+E(a,b) \in Z(\mathcal{G}(\mathcal{I}))$ lenne. Tegyük fel, hogy $b$ nem maximális (ha $a$ lenne nem minimális akkor hasonlóan menne a bizonyítás). Válasszuk $c >_{\mathcal{I}} b$-t úgy, hogy ő legyen a következő elem a $b$-ből induló maximális hosszúságú sorozatok egyikén. Így $\rho(c) = \rho(b) - 1$, tehát $(a,c) \in \mathcal{I}_{k'-1}$. Ekkor $[(I+X),(I+E(b,c))]$-ben $E(a,c)$ nemnulla együtthatóval szerepel. Viszont ekkor $[(I+X),(I+E(b,c))] \notin \left\{(I+A)|A \in \mathcal{A}\left(\bigcup_{i=0}^{k-2}\mathcal{I}_i\right)\right\}$, ugyanis $(a,c) \in \mathcal{I}_{k'-1}$ és $k'-1 \geq k-1$. □

**6.10. Tétel.** Legyen $l(\mathcal{I})$ a leghosszabb $\mathcal{I}$-beli lánc hossza. Az

$$\mathcal{I}^k = \mathcal{I}_{l(\mathcal{I})-k}$$

egyenlet pontosan akkor teljesül minden $1 \leq k \leq l(\mathcal{I})$-re, ha minden $\mathcal{I}$-beli nem bővíthető lánc $l(\mathcal{I})$ hosszú.

**Bizonyítás:** Ha $(a,b) \in \mathcal{I}^k$, akkor a köztük lévő leghosszabb lánc $k$ hosszú. Vegyünk egy nem bővíthető láncot ami mindkettejüket tartalmazza. A feltételünk szerint ez $l(\mathcal{I})$ hosszú, tehát az $a$ előtti és $b$ utáni részének összesen $l(\mathcal{I})-k$ hosszúnak kell lennie. Emiatt $(a,b) \in \mathcal{I}_{l(\mathcal{I})-k}$. A fordított irányú tartalmazást hasonlóan kapjuk.
A másik irányhoz vegyünk egy nem bővíthető, $l' < l(\mathcal{I})$ hosszú láncot. Ekkor $(a,b) \in \mathcal{I}_0$ és $(a,b) \notin \mathcal{I}^{l(\mathcal{I})}$. □

**6.11. Tétel.** Legyen $l(\mathcal{I})$ a leghosszabb $\mathcal{I}$-beli lánc hossza. Ha minden $\mathcal{I}$-beli nem bővíthető lánc ugyanolyan hosszú, akkor

$$\gamma_k(\mathcal{G}(\mathcal{I})) = Z_{l(\mathcal{I})-k+1}(\mathcal{G}(\mathcal{I})).$$

**Bizonyítás:**

$$\gamma_k(\mathcal{G}(\mathcal{I})) =^1 \mathcal{G}\left(\bigcup_{i=k}^{l(\mathcal{I})}\mathcal{I}^i\right) =^2 \mathcal{G}\left(\bigcup_{i=k}^{l(\mathcal{I})}\mathcal{I}_{l(\mathcal{I})-i}\right) =^3 \mathcal{G}\left(\bigcup_{j=0}^{l(\mathcal{I})-k}\mathcal{I}_j\right) =^4 Z_{l(\mathcal{I})-k+1}(\mathcal{G}(\mathcal{I})).$$

1: ez a 6.3 és a 5.2 megjegyzés összevetéséből következik.
2: ez a 6.10 tétel következménye.
3: átparaméterezés
4: a 6.8 tétel miatt. □

**6.12. Definíció.** Egy $G$ csoport **nilpotencia-osztály**ának az alsó centrális láncának a hosszát nevezzük (azaz a legkisebb $n$ számot, amire $\gamma_{n+1}(G) = 1$).

**6.13. Állítás.** Ez megegyezik a felső centrális lánc hosszával, azaz a legkisebb $n$-nel, amire $Z_n(G) = G$.

**Bizonyítás:** Ez a [1] jegyzetben a 6. fejezet 1. tétele. □

**6.14. Tétel.** Adott $\mathcal{I}$ mintára az $\mathcal{A}(\mathcal{I})$ algebra nilpotencia-osztálya megegyezik a $\mathcal{G}(\mathcal{I})$ csoport nilpotencia-osztályával és mindkettő egyenlő a leghosszabb $\mathcal{I}$-beli lánc hosszával.

**Bizonyítás:** A 6.3 tétel szerint $\gamma_{n+1} = 1 \Leftrightarrow \mathcal{A}(\mathcal{I})^{n+1} = 0$. A legkisebb $n$ amire ez teljesül megadja $\mathcal{A}(\mathcal{I})$ és $\mathcal{G}(\mathcal{I})$ nilpotencia-osztályát is. A 5.1 tétel szerint $\mathcal{A}(\mathcal{I})^{n+1} = 0 \Leftrightarrow \mathcal{I}^{n+1} = \emptyset$, azaz nincs $n+1$-hosszú lánc $\mathcal{I}$-ben. □

**6.15. Állítás.** Az $U_n(\mathbb{F})$ csoport alsó és felső centrális lánca megegyezik (ha valamelyiket fordított sorrendben írjuk).

**Bizonyítás:** Az $U_n(\mathbb{F})$ csoport az $n$-elemű teljesen rendezett halmazhoz tartozó mintacsoport. Itt egyetlen nem bővíthető lánc van, tehát a 6.11 tétel szerint valóban megegyezik a két centrális lánc. □

**6.16. Tétel.** Az $U_n(\mathbb{F}_p)$ csoport centrális láncának $k$-adik eleme megegyezik a $\{E(i,j)|j-i \geq k\}$ halmaz által generált algebrához tartozó mintacsoporttal.

**Bizonyítás:** Az $U_n(\mathbb{F}_p)$ csoport az $\mathcal{I} = \{(i,j)|i < j\}$ mintához tartozó mintacsoport. Ebben a mintában az $i$ és $j$ közti leghosszabb lánc épp $j-i$ hosszú, így $\mathcal{I}^k = \{(i,j)|j-i = k\}$, azaz $\bigcup_{j=k}^{n-1} \mathcal{I}^j = \{(i,j)|j-i \geq k\}$. A 5.1 tétel szerint tehát a $\{E(i,j)|j-i \geq k\}$ halmaz által generált algebra $\mathcal{A}(\mathcal{I})^k$. A 6.3 tétel szerint a hozzá tartozó algebracsoport pedig $\gamma_k(U_n(\mathbb{F}_p))$. □

# 7. Prímhatvány-rendű csoportok beágyazása $U_n(\mathbb{F}_p)$-be

**7.1. Állítás.** Az $\mathbb{F}_q$ feletti $n \times n$-es nemszinguláris mátrixok $\mathrm{GL}(n,q)$ csoportjának az elemszáma

$$|\mathrm{GL}(n,q)| = \prod_{i=0}^{n-1}(q^n - q^i).$$

**Bizonyítás:** A nemszinguláris mátrixok megfeleltethetőek $\mathbb{F}_q^n$ bázisainak. Az első vektor a **0**-n kívül akármi lehet. Ha adott $i$ darab független vektor, ezek egy $q^i$ elemű alteret feszítenek ki. A következő báziselemet a maradék $q^n - q^i$ elem közül kell választanunk. □

**7.2. Állítás.** $|U_n(\mathbb{F}_q)| = q^{\frac{n(n-1)}{2}}$

**Bizonyítás:** Minden $i < j$ pár megfelel $U_n(\mathbb{F}_q)$ egy mezőjének, ahova szabadon választott számot írhatunk $\mathbb{F}_q$-ból. Az ilyen párok száma $\frac{n(n-1)}{2}$. □

**7.3. Állítás.** Minden $p^k = q$ prímhatványra $U_n(\mathbb{F}_q)$ egy $p$-Sylow részcsoportja $\mathrm{GL}(n,q)$-nak.

**Bizonyítás:**

$$\prod_{i=0}^{n-1}(q^n - q^i) = \prod_{i=0}^{n-1} q^i(q^{n-i} - 1) = \prod_{i=0}^{n-1} q^i \prod_{j=1}^{n}(q^j - 1)$$

Az első szorzat értéke $q^{\frac{n(n-1)}{2}}$. A második szorzat minden tagja eggyel kisebb egy $p$-vel osztható számnál, tehát egyik sem osztható $p$-vel. Ezért $q^{\frac{n(n-1)}{2}} = p^{k\frac{n(n-1)}{2}}$ a legnagyobb $p$-hatvány, amivel osztható $|\mathrm{GL}(n,q)|$, tehát a $p$-Sylowjai ennyi eleműek. Viszont ez épp $U_n(\mathbb{F}_q)$ elemszáma. □

**7.4. Megjegyzés.** Felmerülhetne a kérdés, hogy mely csoportok ábrázolhatóak mintacsoport részcsoportjaként. Ez egy gyengítése lenne annak a kérdésnek, hogy mely csoportok ábrázolhatóak mintacsoportként. Viszont az előbbi tétel válaszol erre a kérdése: minden $p$-csoport ábrázolható egy speciális mintacsoport, $U_n(\mathbb{F}_p)$ részcsoporjaként. Minden véges test fölötti mintacsoport $p$-csoport, így azt kaptuk, hogy pontosan a véges $p$-csoportok állnak elő véges mintacsoportként.

**7.5. Tétel.** Ha a $G$ csoportnak az elemszáma a $p$ prímnek valamely hatványa, akkor $G$ izomorf $U_{|G|}(\mathbb{F}_p)$ valamely részcsoportjával.

**Bizonyítás:** Reprezentáljuk $G$-t $\mathrm{GL}(|G|,p)$-ben a permutációmátrixok segítségével. Ez egy $\bar{G}$ részcsoportja $\mathrm{GL}(|G|,p)$-nek. Vegyünk egy $S < \mathrm{GL}(|G|,p)$ $p$-Sylow részcsoportot ami tartalmazza $\bar{G}$-t. Sylow II. tétele szerint $S$ konjugált $\mathrm{GL}(|G|,p)$-ben $U_{|G|}(\mathbb{F}_p)$-vel . Ez a konjugálás $\bar{G}$-t $U_{|G|}(\mathbb{F}_p)$ egy részcsoportjába viszi. □

# 8. A mintacsoportok mint $U_n(\mathbb{F})$ részcsoportjai

**8.1. Jelölés.** Egy $a$ mátrix $(i,j)$ mezőjén álló számot jelöljük $a_{ij}$-vel. Fordítva pedig $(a_{ij})$ jelölje azt a mátrixot, aminek $(i,j)$ mezőjén $a_{ij}$ áll (ahol $a_{ij}$ $i$-nek és $j$-nek a függvénye.

**8.2. Jelölés.** Jelöljük $\mathrm{diag}(t_1,...,t_n)$-nel azt a $(d_{ij})$ diagonális mátrixot, amiben

$$(d_{ij}) = \begin{cases} t_i, \text{ ha } i = j \\ 0 \text{ különben.} \end{cases}$$

.

**8.3. Jelölés.** Legyen $h_i(t) := \mathrm{diag}(\underbrace{1,...,1}_{i-1}, t, 1, ..., 1)$.

**8.4. Megjegyzés.** Ekkor $(\mathrm{diag}(t_1,...,t_n))^{-1} = \mathrm{diag}(t_1^{-1},...,t_n^{-1})$ és $(h_i(t))^{-1} = h_i(t^{-1})$.

**8.5. Megjegyzés.** Legyen $a = (a_{ij})$ egy tetszőleges mátrix, $\tau = \mathrm{diag}(t_1,...,t_n)$. Ekkor $\tau$-val balról szorozva $a$-t az $i$-edik sora $t_i$-szeresére változik, jobbról szorozva pedig a $j$-edik oszlopa $t_j$-szeresére változik. Ebből következik. hogy $a$-t $\tau$-val konjugálva az $(i,j)$ mezője $t_i t_j^{-1}$-szeresére változik, ezt írhatjuk úgy is, hogy

$$\mathrm{diag}(t_1,...,t_n)(a_{ij})\mathrm{diag}(t_1^{-1},...,t_n^{-1}) = (t_i a_{ij} t_j^{-1}). \tag{3}$$

**8.6. Tétel.** Minden $\mathbb{F} \neq \mathbb{F}_2$ testre az $U \leq U_n(\mathbb{F})$ csoport pontosan akkor mintacsoport, ha bármely $\tau$ nemszinguláris diagonális mátrixra $\tau U \tau^{-1} = U$.

**Bizonyítás:** (Bob Guralnick, [2] Proposition 2.1)
A 8.5 megjegyzés miatt minden $(a_{ij})$ mátrixra és $\tau = \mathrm{diag}(t_1, ..., t_n) \in GL_n(\mathbb{F})$ nemszinguláris diagonális mátrixra:

$$(tat^{-1})_{ij} = 0 \Leftrightarrow t_i a_{ij} t_j^{-1} = 0 \Leftrightarrow a_{ij} = 0,$$

azaz a konjugálás nem változtatja meg, hogy melyek a nemnulla mezők. Emiatt a nemszinguláris diagonális mátrixszal konjugálás nem vezethet ki a mintacsoportból.
A másik irányhoz szükségünk lesz a következő állításra:

**8.7. Állítás.** Ha minden $u \in U$-ra és $t \in \mathbb{F}$-re

$$u_{ij} \neq 0 \Rightarrow (I + tE(i,j)) \in U,$$

akkor $U$ egy mintacsoport.

**Bizonyítás:** Legyen

$$\mathcal{I} := \{(i,j) | \exists u \in U : u_{ij} \neq 0\}.$$

Ekkor a feltevés szerint ha $(i,j), (j,k) \in \mathcal{I}$, akkor $(I + E(i,j)), (I + E(j,k)) \in U$, tehát $[(I + E(i,j))(I + E(j,k))] = (I + E(i,k)) \in U$ azaz $(i,k) \in \mathcal{I}$, tehát $\mathcal{I}$ egy zárt minta. A 3.2 megjegyzés szerint $\mathcal{G}(\mathcal{I})$-t generálja az $\{(I + tE(i,j)) | t \in \mathbb{F}, (i,j) \in \mathcal{I}\}$ halmaz, ami a feltétel szerint $U$-ban van. Tehát $U \supseteq \mathcal{G}(\mathcal{I})$, de $\mathcal{I}$ definíciója szerint $U \subseteq \mathcal{G}(\mathcal{I})$, tehát $G = \mathcal{G}(\mathcal{I})$. □
Tehát elég azt igazolnunk, hogy a 8.7 állítás feltételei teljesülnek.
Vegyünk egy $u = (u_{ij}) \in U$ mátrixot. Válasszunk most egy $u_{i_0 j_0}$-t úgy, hogy $i' < i_0$-ra $u_{i'j'} = 0$ legyen minden $j' \neq i'$-re. Legyen $t \neq 0$ és $t \neq 1$ (itt használjuk ki, hogy $\mathbb{F} \neq \mathbb{F}_2$).

**8.8. Lemma.** Ekkor

$$(h_{i_0}(t) u h_{i_0}(t^{-1}))_{ij} = \begin{cases} u_{ij}, \text{ ha } i \neq i_0 \\ t u_{ij}, \text{ ha } i = i_0 \text{ és } j \neq i_0 \\ 1, \text{ ha } i = i_0 = j. \end{cases} \tag{4}$$

**Bizonyítás:** A 8.5 megjegyzés szerint ha $h_{i_0}(t)$-vel konjugáljuk $u$-t, az $t$-vel megszorozza az $i_0$-adik sorát és $t^{-1}$-gyel megszorozza az $i_0$-adik oszlopát. Viszont $u$-nak az $i_0$-adik oszlopa a főátlóbeli 1-estől eltekintve csupa 0 (mert ha $u_{ki} \neq 0$ és $k \neq i$, akkor $k < i$, ellentmondva $i$ minimalitásának). Így a $h_{i_0}(t)$-vel való konjugálás csak megszorozza $t$-vel $u$ $i_0$-adik sorának minden főátlón kívüli elemét. □

**8.9. Lemma.** Az $u' := h_{i_0}(t) u h_{i_0}(t^{-1}) u^{-1}$ szorzatban minden $i$-re $u'_{ii} = 1$ és $j \neq i$, $i \neq i_0$-ra $u'_{ij} = 0$.

**Bizonyítás:** A szorzat mezői $h_{i_0}(t) u h_{i_0}(t^{-1})$ sorainak $u^{-1}$ oszlopainak a skalárszorzatai. A 8.8 lemma szerint az $i_0$-adik sortól eltekintve $h_{i_0}(t) u h_{i_0}(t^{-1})$ sorai megegyeznek $u$ soraival, tehát a $(h_{i_0}(t) u h_{i_0}(t^{-1})) u^{-1}$ szorzat is csak az $i_0$-adik sorban különbözhet az $uu^{-1}$ szorzattól. Viszont $uu^{-1} = I$, tehát $u'$ csak az $i_0$-adik sorában különbözik $I$-től, ami éppen az, amit állítunk. □

**8.10. Lemma.** Az $u'$ mátrix $i_0$-adik sorában a főátlón kívül is van nemnulla mező.

**Bizonyítás:** Ha $u'_{i_0j} = 0$ lenne minden $j \neq i_0$-ra, akkor $(u'u)_{i_0j_0}$ egyenlő lenne $u_{i_0j_0}$-lal, ugyanis $(uu')_{ij}$ definíció szerint $u'$ $i_0$-adik sorának és $u$ $j_0$-adik oszlopának a skalárszorzata. Viszont

$$u'u = (h_{i_0}(t)uh_{i_0}(t^{-1})u^{-1})u = h_{i_0}(t)uh_{i_0}(t^{-1})$$

aminek a 8.8 lemma szerint az $i_0j_0$ mezőjén $tu_{i_0j_0}$ áll és $tu_{i_0j_0} \neq u_{i_0j_0}$ mert $u_{i_0j_0} \neq 0$ és $t \neq 1$. □

Az előző lemma szerint van olyan $j \neq i_0$, amire $u'_{i_0j} \neq 0$. Legyen $j_1$ az egyik ilyen.

**8.11. Lemma.** Ekkor

$$(h_{j_1}(t)u'h_{j_1}(t^{-1}))_{ij} = \begin{cases} u'_{ij}, \text{ ha } i \neq i_0 \text{ vagy } j \neq j_1 \\ tu'_{ij}, \text{ ha } i = i_0 \text{ és } j = j_1 \end{cases} \tag{5}$$

**Bizonyítás:** A 8.5 megjegyzés szerint ez a konjugálás megszorozza $t$-vel a $j_1$-edik sor elemeit és $t^{-1}$-gyel a $j_1$-edik oszlop elemeit. A 8.9 lemma szerint $u'$ $j_0$-adik sorának csak a főátlóban van nemnulla eleme és a $j_1$-edik oszlopának a főátlóbeli elemén kívül csak az $i_0$-adik eleme nem nulla. □

**8.12. Lemma.** Az $u'' := (h_{j_1}(t)u'h_{j_1}(t^{-1}))u'^{-1}$ szorzatnak a főátlón kívül csak az $(i_0, j_1)$ mezője nemnulla.

**Bizonyítás:** A 8.11 lemma szerint ha $u'$-t $h_{j_1}(t)$-vel konjugáljuk azzal a sorok közül csak az $i_0$-adikon változtatunk, tehát ez a szorzat csak az $i_0$-adik sorában különbözhet az identitástól (ez a 8.9 lemma bizonyításának gondolatmenete röviden).

A 8.9 lemma szerint $u'$-nek a főátlón és az $i_0$-adik soron kívül minden mezője 0. Ezért $u'^{-1}$ $j$-edik oszlopa merőleges a $(\underbrace{0, ..., 0}_{l-1}, 1, 0, ..., 0)$ vektorra ha $l \neq j$ és $l \neq i_0$. Azaz a $j$-edik oszlopnak csak a $j$-edik és az $i_0$-adik eleme lehet nemnulla. Ha $j \neq i_0$ akkor $u'$ $j$-edik oszlopának skalárszorzata $u'$ $i_0$-adik sorával 0, azaz

$$0 = u'_{i_0j}(u'^{-1})_{jj} + u'_{i_0i_0}u'^{-1})_{i_0j} = (u'_{i_0j} + (u'^{-1})_{i_0j} \Rightarrow (u'^{-1})_{i_0j} = -u'_{i_0j}$$

Ugyanezzel a gondolatmenetet $u'$ helyett $h_{j_1}(t)u'h_{j_1}(t^{-1})$-vel elmondva azt kapjuk, hogy $j \neq i_0$-ra

$$h_{j_1}(t)u'^{-1}h_{j_1}(t^{-1}) = (h_{j_1}u'h_{j_1}(t^{-1}))^{-1} = -h_{j_1}(t)u'h_{j_1}(t^{-1}).$$

Így $(u'^{-1})_{i_0j} \neq (h_{j_1}(t)u'^{-1}h_{j_1}(t^{-1}))_{i_0j}$ csak $j = j_1$-re teljesül, ezért $(h_{j_1}(t)u'h_{j_1}(t^{-1}))u'^{-1}$ csak a $j_1$-edik oszlopban különbözhet $h_{j_1}(t)u'h_{j_1}(t^{-1})h_{j_1}(t)u'^{-1}h_{j_1}(t^{-1}) = I$-től.

Tehát azt kaptuk, hogy $u''$ az $i_0$-adik során kívül és $j_1$-edik oszlopán kívül nem különbözhet $I$-től, tehát csak az $(i_0, j_1)$ mezőjén különbözhet $I$-től. Itt viszont különbözik is, ugyanis a 8.11 lemma szerint $(h_{j_1}(t)u'h_{j_1}(t^{-1}))_{i_0j_1} = tu'_{i_0j_1}$ és feltevésünk szerint $u'_{i_0j_1} \neq 0$ (és $t \neq 1$), tehát $h_{j_1}(t)u'h_{j_1}(t^{-1}) \neq u'$, tehát azt $u'^{-1}$-gyel megszorozva nem kaphatunk $I$-t. □

Azt kaptuk tehát, hogy $u'' = (I + t \cdot E(i_0, j_1)$ valamely $t \in \mathbb{F}_q$-ra. Két diagonális mátrixszal való konjugálással kaptuk $u$-ból $u''$-t, így $u'' \in U$.

**8.13. Lemma.** Minden $t' \in \mathbb{F}_q$-ra $(I + t'E(i_0, j_1)) \in U$.

**Bizonyítás:** Konjugáljuk $u''$-t $h_{i_0}(t't^{-1})$-zel, így a 8.8 lemma szerint $(I + t' \cdot E(i_0, j_1))$-t kapjuk ($u''$-re is $i_0$ az első (és egyetlen) sor ahol nem csak a főátlóban van nemnulla elem). □

**8.14. Lemma.** Legyen $u^* := u(I + u_{i_0 j_1}^{-1} E(i_0, j_1))$. Ekkor $u^* \in U$ és

$$u_{ij}^* = \begin{cases} 0, \text{ ha } i = i_0, j = j_1 \\ u_{ij}, \text{ különben.} \end{cases}$$

**Bizonyítás:** Mivel $u(I + u_{i_0 j_1}^{-1} E(i_0, j_1)) = u - u_{i_0 j_1} u E(i_0, j_1)$, azt kell csak megnéznünk, hogy mi $uE(i_0, j_1)$. Ez a szorzat azt csinálja, hogy $u$-nak veszi az $i_0$-adik oszlopát és átrakja a $j_1$-edik oszlopba (és minden más oszlopot nulláz). Ha $i \neq i_0$, akkor $u_{i' i_0} = 0$ (ha $i < i_0$ akkor azért mert $i_0$-t úgy választottuk, hogy ilyen ne legyen, ha $i > i_0$ akkor azért mert $u$ egy felső-háromszög mátrix). Ezért $u$ $i_0$-adik oszlopa a főátlón kívül mindenhol nulla, a főátlóban pedig 1. Ezért $uE(i_0, j_1) = E(i_0, j_1)$, így tényleg $u^* = u - u_{i_0 j_1} E(u_0, j_1)$. □

Az $u$ mátrix nemnulla mezőinek számára vonatkozó indukcióval (ami legalább $n$, tehát onnan kezdjük) azt kapjuk, hogy minden $(i, j)$-re, amire $u_{ij}^* \neq 0$ (és minden $t' \in \mathbb{F}$-re), $(I + t'E(i, j)) \in U$. Tehát a 8.7 állítás feltétele teljesül, azaz a 8.7 állítás szerint $U$ mintacsoport. □

**8.15. Megjegyzés.** Ha $\mathbb{F} = \mathbb{F}_2$, akkor a 8.6 tétel konjugálásos feltétele semmitmondó, ugyanis $U_n(\mathbb{F}_2)$-ben az egyetlen nemszinguláris diagonális mátrix az identitás. A következő tétel azt mutatja, hogy $U_n(\mathbb{F}_2)$-nek nem minden részcsoportja mintacsoport.

**8.16. Példa.** A

$$H = \left\{ \begin{bmatrix} 1 & s & t \\ 0 & 1 & s \\ 0 & 0 & 1 \end{bmatrix} | s, t \in \mathbb{F}_2 \right\} \subset U_3(\mathbb{F}_2)$$

halmaz részcsoportja $U_3(\mathbb{F}_2)$-nek, ugyanis szorzásra és invertálásra zárt. Viszont $H$ nem mintacsoport, ugyanis $(I + E(1, 2)) \notin H$ pedig van olyan $h \in H$-nak, amiben $h_{12} \neq 0$. Más testek felett a $\mathrm{diag}(t, 1, 1)$-gyel való konjugálás $t \neq 1$-re az első sor nem főátlóbeli elemeit megszorozza $t$-vel és így kivezet a csoportból, viszont ilyen $\mathbb{F}_2$ felett nincs.

# 9. Mintacsoportok rész-algebracsoportjainak jellemzése

**9.1. Tétel.** ([2] Proposition 2.2.) Adott egy $\mathcal{I}$ zárt minta és a hozzá tartozó $\mathbb{F}$ feletti $\mathcal{G}(\mathcal{I})$ mintacsoportnak egy $H \leq \mathcal{G}(\mathcal{I})$ részcsoportja. Ez a részcsoport pontosan akkor egyezik meg $\mathcal{A}(\mathcal{I})$ egy részalgebrájához tartozó algebracsoporttal, ha a

$$V_H := \{A \in \mathcal{A}(\mathcal{I}) | (I + A) \in H)\} \subseteq \mathcal{A}(\mathcal{I})$$

halmaz zárt az ($\mathcal{A}(\mathcal{I})$ szerinti) összeadásra és skalárral szorzásra (azaz $V_H$ egy vektortér).

**Bizonyítás:** Először tegyük fel, hogy $V_H$ egy vektortér.

**9.2. Lemma.** Ekkor $A, B \in V_H \Rightarrow AB \in V_H$ (ahol a szorzás az $\mathcal{A}(\mathcal{I})$-beli szorzás.

**Bizonyítás:** Mivel $H$ egy csoport, ezért $(I + A)(I + B) = (I + (A + B + AB)) \in H$, azaz $A + B + AB \in V_H$. Felhasználva, hogy $V_H$ vektortér és $A, B, (A + B + AB) \in V_H$ megkapjuk, hogy $AB \in V_H$. □
Emiatt $V_H$ részalgebrája $\mathcal{A}(\mathcal{I})$-nek. Az általa generált csoportalgebra pedig éppen $H$.
A másik irány csak annyit mond, hogy ha $V_H$ algebra, akkor vektortér is, ami definíció szerint igaz. □

**9.3. Példa.** A 1.18 állítás szerint az $\mathbb{F}_p$ feletti, $p$-nél kisebb nilpotencia-osztályú csoportokban minden elem $p$-edik hatványa 1. A 1.19 állítás szerint egy $p$-nél nem kisebb nilpotencia-osztályú algebrának legalább $p^p$ eleme van. Így minden $p^p$-nél kisebb rendű algebracsoport $p$ exponensű. Viszont $U_{p^2}(\mathbb{F}_p)$-nek van $p^2$-rendű eleme (pl. egy $p^2$ hosszú ciklus permutációmátrixa). Ez az elem egy $p^2$-elemű részcsoportja $U_{p^2}(\mathbb{F}_p)$-nek és van $p^2$ rendű eleme, így ($p > 2$ esetén) nem lehet izomorf egy algebracsoporttal.

# 10. $(\mathrm{k}, \mathrm{m})$-típusú mintacsoportok

**10.1. Definíció.** ([5] Definition 4.1.) Legyen $\mathrm{k} \geq 1, \mathrm{m} \geq 1, l \geq 0, n = \mathrm{k} + l + \mathrm{m}$ és minden $\nu \in \{1, ..., l\}$-re legyen adott egy $K_\nu \subset \{1, ..., \mathrm{k}\}$ és egy $M_\nu \subset \{1, ..., \mathrm{m}\}$. A $\{(K_\nu, M_\nu) | \nu \in \{1, ..., l\}\}$ halmazrendszerhez tartozó **$(\mathbf{k}, \mathbf{m})$-típusú minta** a következő számpárokból áll:

$$\begin{aligned} \nu \in \{1, ..., l\}, i \in K_\nu\text{-re} &: (i, \mathrm{k} + \nu) \\ \nu \in \{1, ..., l\}, j \in M_\nu\text{-re} &: (\mathrm{k} + \nu, \mathrm{k} + l + j\}, \text{ és} \\ i \in \{1, ..., \mathrm{k}\}, j \in \{1, ..., \mathrm{m}\}\text{-re} &: (i, \mathrm{k} + l + j). \end{aligned} \tag{6}$$

Az ilyen mintához tartozó mintaalgebrákat **$(\mathbf{k}, \mathbf{m})$-típusú mintaalgebrá**nak nevezzük, az ezeknek megfelelő mintacsoportokat pedig **$(\mathbf{k}, \mathbf{m})$-típusú mintacsoport**nak.
A $(\mathrm{k}, \mathrm{m})$-típusú mintáknak egy ekvivalens jellemzése a következő:

**10.2. Tétel.** Az $\mathcal{I} \subset \mathcal{N} \times \mathcal{N}$ egy $(\mathrm{k}, \mathrm{m})$-típusú minta pontosan akkor, ha

$$\{(i, j) | 1 \leq i \leq \mathrm{k}, n - \mathrm{m} + 1 \leq j \leq n\} \subset \mathcal{I}$$

és minden $(i, j) \in \mathcal{I}$-re teljesül a következő:

$$\begin{aligned} (i, j) \in \mathcal{I}, i \leq \mathrm{k} &\Rightarrow j \geq k + 1 \\ (i, j) \in \mathcal{I}, i \geq \mathrm{k} + 1 &\Rightarrow j \geq n - \mathrm{m} + 1. \end{aligned}$$

**Bizonyítás:** Ezek nyilvánvalóan teljesülnek a $(\mathrm{k},\mathrm{m})$-típusú mintákra. Ha adott egy minta amire ezek teljesülnek, akkor legyen

$$K_\nu = \{i : (i, \mathrm{k}+\nu) \in \mathcal{I}\}$$
$$M_\nu = \{j : (\mathrm{k}+\nu, n-\mathrm{m}+j) \in \mathcal{I}\}.$$

Ezek a halmazok éppen az $\mathcal{I}$ mintát definiálják. □

**10.3. Megjegyzés.** Az ekvivalens meghatározásból kiolvasható a $(\mathrm{k},\mathrm{m})$-típusúság egy szemléletes jelentése: a mátrix jobb felső $\mathrm{k}\times\mathrm{m}$ sarkában tetszőlegesen határozhatjuk meg a mezőket. Ezen kívül még néhány ettől balra vagy lejjebb lévő mezőben is szabad kezet kapunk.

**10.4. Elnevezés.** Az (6) egyenlet első sorában meghatározott mintaelemeket nevezzük $A$-típusúnak, a második sorában meghatározottakat $B$-típusúnak és a harmadik sorában meghatározott elemeket pedig nevezzük $C$-típusúnak. Ennek megfelelően egy $(\mathrm{k},\mathrm{m})$-típusú mintaalgebrában az $E(i,j)$ elemeket is $A$, $B$ vagy $C$-típusúnak nevezhetjük annak függvényében, hogy $(i,j)$ melyik sorban lett meghatározva. Ugyanígy a mintacsoportban az $(I+E(i,j))$ elemek is klasszifikálhatóak.

**10.5. Jelölés.** Az $A$-típusú mintaelemek halmazát jelöljük $A$-val, az $A$ típusú mintaalgebra elemek halmazát $A_{\mathcal{A}}$-val és az $A$ típusú mintacsoport elemek halmazát pedig $A_{\mathcal{G}}$-vel. Ehhez hasonlóan definiálhatjuk $B, B_{\mathcal{A}}, B_{\mathcal{G}}, C, C_{\mathcal{A}}, C_{\mathcal{G}}$-t.

**10.6. Megjegyzés.** Legyen $a \in A, b \in B$. Ekkor $E(a)E(b) = ([(I+E(a)),(I+E(b))]-I)$ pontosan akkor nem nulla, ha ugyanamiatt a $\nu$ miatt került be a mintába $a$ és $b$, azaz $a = (i, \mathrm{k}+\nu), b = (\mathrm{k}+\nu, \mathrm{k}+l+j)$ és $i \in K_\nu, j \in M_\nu$. (Egy mintaelemről egyértelműen megállapítható, hogy melyik $\nu$ miatt került be a mintába.)

**10.7. Lemma.** A $C_{\mathcal{G}}$ halmaz által generált $\mathcal{C}_{\mathcal{G}}$ részcsoport benne van a mintacsoport centrumában és tartalmazza a mintacsoport kommutátorát, azaz

$$Z(\mathcal{G}(\mathcal{I})) \geq \mathcal{C}_{\mathcal{G}} \geq (\mathcal{G}(\mathcal{I}))'$$

**Bizonyítás:** Mindkét tartalmazás kézenfekvő. □

**10.8. Megjegyzés.** Adott $(\mathrm{k},\mathrm{m})$-re $l$ akármilyen nagy lehet, tehát a mintát megvalósító mátrix is akármilyen nagy lehet. Adott $(\mathrm{k},\mathrm{m})$-re az ilyen típusú mintacsoportok rendje akármilyen nagy lehet, viszont az előző lemma szerint $|C_{\mathcal{G}}| = |C| = \mathrm{k}\cdot\mathrm{m}$ és $C_{\mathcal{G}}$ generátuma tartalmazza a csoport kommutátor-részcsoportját, így egy $\mathbb{F}_q$ feletti $(\mathrm{k},\mathrm{m})$-típusú mintacsoport kommutátor-részcsoportjának a rendje legfeljebb $q^{\mathrm{k}\cdot\mathrm{m}}$ lehet.

**10.9. Definíció.** A legszűkebb zárt mintát, ami egy $(\mathrm{k},\mathrm{l})$-típusú minta $A$ és $B$ típusú elemeit tartalmazza **szűkített $(\mathrm{k},\mathrm{l})$-típusú mintá**nak nevezzük. Expliciten megadva ez az olyan minta, melynek elemei

$$\begin{aligned} \nu \in \{1,\ldots,l\}, i \in K_\nu\text{-re} &: (i, \mathrm{k}+\nu) \\ \nu \in \{1,\ldots,l\}, j \in M_\nu\text{-re} &: (\mathrm{k}+\nu, \mathrm{k}+l+j\}, \text{ és} \\ \text{ha } \exists\nu : i \in K_\nu, j \in M_\nu, \text{ akkor} &: (i, \mathrm{k}+l+j). \end{aligned} \tag{7}$$

Az ezekhez tartozó mintaalgebrák és mintacsoportok értelemszerűen a **szűkített $(\mathbf{k},\mathbf{l})$-típusú mintaalgebrá**k és **szűkített $(\mathbf{k},\mathbf{l})$-típusú mintacsoport**ok.

**10.10. Jelölés.** Szűkített (k, l)-típusú minta esetén a (7) egyenlet harmadik sorában definiált elemeket nevezzük $\widehat{C}$ típusúnak, és ennek megfelelően definfiáljuk $\widehat{C}, \widehat{C}_{\mathcal{A}}$ és $\widehat{C}_{\mathcal{G}}$-t.

**10.11. Tétel.** Egy $\mathcal{I}$ zárt minta pontosan akkor szűkített (k, m)-típusú, ha

$$(i,j) \in \mathcal{I}, i \leq \mathrm{k} \Rightarrow j \geq k+1$$
$$(i,j) \in \mathcal{I}, i \geq \mathrm{k}+1 \Rightarrow j \geq n-\mathrm{m}+1.$$

és ha $i \leq \mathrm{k}$ és $j \geq n-\mathrm{m}+1$, akkor $\exists x : i <_{\mathcal{I}} x <_{\mathcal{I}} j$.

**Bizonyítás:** Az első két feltétel a 10.2 tételből következik (ugyanis minden szűkített (k, m)-típusú minta részhalmaza egy (k, m)-típusú mintának). A szűkített (k, m)-típusú minták definíciója szerint ha $(i, \mathrm{k}+l+j) \in \mathcal{I}$, akkor $\exists \nu : i \in K_\nu, j \in M_\nu$. Ekkor $i <_{\mathcal{I}} \mathrm{k}+\nu <_{\mathcal{I}} \mathrm{k}+l+j$, ami igazolja a tétel harmadik feltételét tetszőleges $(i, \mathrm{k}+l+j) \in \mathcal{I}$ párra.
Ha a három feltétel teljesül, akkor a 10.2 tétel bizonyításában definiált $K_\nu, M_\nu$ halmazok által meghatározott szűkített (k, m)-típusú minta éppen $\mathcal{I}$. □

**10.12. Tétel.** Legyen $G$ egy olyan 2-nilpotencia-osztályú csoport, amire $G' = Z(G)$. Ekkor $G$ minden mintacsoportként való ábrázolása egy szűkített (k, m)-típusú mintacsoport valamilyen k, m párra.

**Bizonyítás:** Ha $G$ nem ábrázolható mintacsoportként akkor igaz az állítás. Ha igen, akkor vegyük egy $\mathcal{G}(\mathcal{I})$ ábrázolását. Ebben a 6.14 tétel szerint nincs 2-nél hosszabb lánc. Ha lenne egy $i <_{\mathcal{I}} j$ 1-hosszú nembővíthető lánca, akkor $(I + E(i,j))$ felcserélhető lenne minden másik elemmel de nem lenne benne a kommutátorban. Tehát azt kaptuk, hogy minden nembővíthető lánc hossza 2. Eszerint $\mathcal{I}$ elemeit felbontható három diszjunkt halmazra aszerint, hogy az elemei az őket tartalmazó maximális láncok alján, közepén vagy tetején vannak. Legyen ez a három halmaz rendre $X, Y, Z$. Számozzuk meg a halmazok elemeit ($X := \{x_1, x_2, ..., x_{|}X|\}$ stb.). Legyen $|X| = \mathrm{k}, |Y| = l$ és $|Z| = \mathrm{m}$. Definiáljuk $\phi$-t a következő módon

$$\phi(I + E(x_i, y_\nu)) = (I + E(i, \mathrm{k}+\nu))$$
$$\phi(I + E(x_i, z_j)) = (I + E(i, \mathrm{k}+l+j))$$
$$\phi(I + E(y_\nu, z_j)) = (I + E(\mathrm{k}+\nu, \mathrm{k}+l+j))$$

ahol $x_i \in X, y_\nu \in Y$ és $z_j \in Z$. Könnyen látható, hogy ez homomorfizmust definiál és a képtere mintacsoport. □

**10.13. Megjegyzés.** Ha $G' < Z(G)$, akkor $(G \setminus (Z(G)) \cup G'$ részcsoportja $G$-nek és $Z(G) \setminus G' \cup \{1\}$ is az, és $G$ előáll mint ezek direkt szorzata. Ráadásul ha $G$ mintacsoport volt, akkor $Z(G) \setminus G' \cup \{1\}$ egy elemi abel $p$-csoport. Tehát $G = G_1 \times G_2$ ahol $G_1' = Z(G_1)$ és $G_2$ Abel-csoport. Így a $G' = Z(G)$ feltétel nem lényegesebben erősebb a 2-nilpotenciaosztályúságnál.

# 11. Az $\tilde{f}$ függvények rangja

**11.1. Jelölés.** Vegyünk egy $\mathcal{I}$ szűkített $(\mathrm{k},\mathrm{m})$-típusú mintát. Legyen a hozzá tartozó $\widehat{C}_{\mathcal{A}}$ halmaz által lineárisan generált altere a mintaalgebrának $\mathcal{C}$. Az $A_{\mathcal{A}}$ és $B_{\mathcal{A}}$ által együtt generált lineáris altér legyen $\mathcal{D}$.

**11.2. Definíció.** Egy adott $f \in \mathcal{C}^* = \mathrm{Hom}(\mathcal{C}, \mathbb{F}_q)$ lineáris leképezésre legyen $\tilde{f}$ az az $\mathcal{A}(\mathcal{I}) \times \mathcal{A}(\mathcal{I}) \to \mathbb{F}_q$ függvény amit a következő egyenlet definiál:

$$\tilde{f}(x,y) = f([x,y]_{\mathcal{A}}) = f(xy - yx).$$

Ez a függvény jóldefiniált, ugyanis $\mathcal{C}$ tartalmazza $\mathcal{A}(\mathcal{I})$ kommutátorát (ugyanis $\mathcal{A}(\mathcal{I})^2$-t tartalmazza és altér.)

**11.3. Megjegyzés.** Úgy is felfoghatjuk, hogy $\tilde{f}$ egy $\mathcal{D}\times\mathcal{D} \to \mathbb{F}_q$ függvény, ugyanis $\mathcal{A}(\mathcal{I}) = \mathcal{D} \oplus \mathcal{C}$ és ha $x \in \mathcal{C}$ vagy $y \in \mathcal{C}$, akkor $[x,y]_{\mathcal{A}} = 0$, tehát ha $x = d + c$ ahol $d \in \mathcal{D}, c \in \mathcal{C}$, akkor $[x,y] = [d+c,y] = (d+c)y - y(d+c) = (dy - yd) + (cy - yc) = [d,y] + [c,y] = [d,y]$.

**11.4. Definíció.** Adott egy $\mathbb{F}$ test feletti $V$ vektortér. **Szimplektikus alak**nak azokat a $V \times V \to \mathbb{F}$ függvényeket nevezzük, amelyekre

(1) $\langle tx, y\rangle = t\langle x, y\rangle$ ha $t \in \mathbb{F}, x \in V$,

(2) $\langle x + z, y\rangle = \langle x, y\rangle + \langle z, y\rangle$, ha $x, y, z \in V$,

(3) $\langle x, x\rangle = 0$.

Ha választunk egy $B$ bázist és $V$ vektorait abban írjuk fel, akkor minden szimplektikus alakhoz tartozik egy $H$ mátrix, amire igaz, hogy $\langle x, y\rangle = x^T H y$. Ennek a rangja nem függ $B$ választásától, így mondhatjuk azt, hogy ez magának a szimplektikus alaknak a rangja.

**11.5. Állítás.** Minden $f \in \mathcal{C}^*$-ra $\tilde{f}$ egy szimplektikus alak.

**Bizonyítás:** Az első két tulajdonság nyilvánvalóan teljesül, $[x,x] = 0$ miatt a harmadik is. □

**11.6. Jelölés.** Legyen $\phi_{ij} \in \mathcal{C}^*$ az a függvény, ami minden $\mathcal{C}$-beli elemhez hozzárendeli azt a számot, ami $E(i, \mathrm{k} + l + j)$ együtthatója ebben az elemben (azaz megadja, hogy az $(i, \mathrm{k} + l + j)$ mezőjén a mátrixnak milyen szám áll). Minden $f \in \mathcal{C}^*$ előáll $\sum_{i=1}^{\mathrm{k}} \sum_{j=1}^{\mathrm{m}} t_{ij}^f \phi_{ij}$ alakban, ahol $\{t_{ij}^f$ az $f$-re jellemző együttható-sorozat. Legyen $L^f$ az a mátrix, aminek az $(i,j)$ mezőjén $t_{ij}^f$ áll. Válasszuk ki $L^f$-nek azon sorait, amelyek sorszáma $K_\nu$-beli és azon oszlopait, amelyek sorszáma $M_\nu$-beli. Ezek metszete egy $|K_\nu| \times |M_\nu|$ mátrix, nevezzük ezt $L_\nu^f$-nek.

**11.7. Tétel.** ([5] Lemma 4.2.) Ekkor $\tilde{f}$ rangját a következő képlet határozza meg:

$$r(\tilde{f}) = 2\sum_{\nu=1}^{l} r(L_\nu) \tag{8}$$

**Bizonyítás:** Válasszunk bázist úgy, hogy először $\mathcal{D}$-nek választjuk egy bázisát majd utána $\mathcal{C}$-nek. Az ilyen bázisokban az $\tilde{f}$-et leíró mátrixnak csak a bal felső ($\mathcal{D}\times\mathcal{D}$-hez tartozó) sarkában lehetnek nem-nulla elemek, ugyanis $\tilde{f}(x,y)=0$ ha $x\in\mathcal{C}$ vagy $y\in\mathcal{C}$. Tehát csak ezzel a résszel kell foglalkoznunk. Itt a báziselemek halmaza a $A_{\mathcal{A}}\cup B_{\mathcal{A}}$ halmaz lesz. A báziselemek sorrendje legyen a következő: ($u\prec v$ azt jelenti, hogy $u$ előbb van mint $v$)

· Ha $a\in A, b\in B$, akkor $E(a)\prec E(b)$

· Ha $(i,\mathrm{k}+\nu),(i',\mathrm{k}+\nu')\in A$, akkor $(\nu<\nu'\vee(\nu=\nu'\wedge i<i'))\Rightarrow E(i,\mathrm{k}+\nu)\prec E(i',\mathrm{k}+\nu')$.

· Ha $(\mathrm{k}+\nu,\mathrm{k}+l+j),(\mathrm{k}+\nu',\mathrm{k}+l+j')\in B$, akkor $(\nu<\nu'\vee(\nu=\nu'\wedge i<i'))\Rightarrow E(\mathrm{k}+\nu,\mathrm{k}+l+j)\prec E(\mathrm{k}+\nu',\mathrm{k}+l+j')$.

A következő állításból következne a tétel:

**11.8. Állítás.** Emellett a bázissorend mellett $\tilde{f}$ mátrix-alakjának a $\mathcal{D}\times\mathcal{D}$-re vonatkozó része a következőképpen néz ki (blokkokban felírva):

$$\begin{bmatrix} 0 & \dots & 0 & L_1^f & \dots & 0 \\ \vdots & \ddots & \vdots & \ddots & \vdots & \\ 0 & \dots & 0 & 0 & \dots & L_l^f \\ -L_1^{f^T} & \dots & 0 & 0 & \dots & 0 \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & \dots & -L_l^{f^T} & 0 & \dots & 0 \end{bmatrix}$$

**Bizonyítás:** Az $A_{\mathcal{A}}$-beli elemek egymással felcserélhetők és a $B_{\mathcal{A}}$-beliek is egymással felcserélhetők, tehát $\tilde{f}(a,a')=f([a,a']_{\mathcal{A}})=f(0)=f([b,b']_{\mathcal{A}})=\tilde{f}(b,b')$ ha $a,a'\in A_{\mathcal{A}}, b,b'\in B_{\mathcal{A}}$. Emiatt csupa nulla $\tilde{f}$ mátricának bal fölső és jobb alsó negyede. Adott $a=E(i,\mathrm{k}+\nu)\in A_{\mathcal{A}}, b=E(\mathrm{k}+\nu',\mathrm{k}+l+j)\in B_{\mathcal{A}}$. Ha $\nu\neq\nu'$, akkor ezek is felcserélhetőek, tehát itt is $\tilde{f}(a,b)=0$. Tehát csak $E(i,\mathrm{k}+\nu)$-hez tartozó sorok és $E(\mathrm{k}+\nu,\mathrm{k}+l+j)$-hez tartozó oszlopok, illetve $E(\mathrm{k}+\nu,\mathrm{k}+l+j)$-hez tartozó sorok és $E(i,\mathrm{k}+\nu)$-hez tartozó oszlopok metszetében lehet nem-nulla eleme a mátrixnak.
Az $E(i,\mathrm{k}+\nu), i\in K_\nu$ alakú báziselemeket a sorbarakással egy helyre gyűjtöttük, tehát ezekhez egymást követő sorok (illetve oszlopok) tartoznak a mátrixban. Hasonlóan az $E(\mathrm{k}+\nu,\mathrm{k}+l+j), j\in M_\nu$ elemeket is egybegyűjtöttük, és egymás melletti oszlopoknak feleltethetők meg. Az $E(i,\mathrm{k}+\nu), i\in K_\nu$-hez tartozó sorok és az $E(\mathrm{k}+\nu,\mathrm{k}+l+j), j\in M_\nu$-hez tartozó oszlopok metszete valóban $L_\nu^f$, ugyanis

$$\tilde{f}(E(i,\mathrm{k}+\nu),E(\mathrm{k}+\nu,\mathrm{k}+l+j))=f(E(i,\mathrm{k}+l+j))=L_\nu(i,j)^f.$$

Megfordítva az oszlopok és sorok szerepét

$$\tilde{f}(E(\mathrm{k}+\nu,\mathrm{k}+l+j),E(i,\mathrm{k}+\nu))=f(-E(i,\mathrm{k}+l+j))=-L_\nu^f(i,j)=-L_\nu^{f^T}(j,i).\quad\square\quad\square$$

**11.9. Megjegyzés.** $L_\nu^f(i,j)=L^f(i,j)=t_{ij}^f$ az $L^f$ mátrix $(i,j)$ mezője. Azért jelöltem most így, hogy látszódjon, hogy $L_\nu^f$ blokként benne van a vizsgált mátrixban.

# 12. Minimális rangú $\tilde{f}$ függvények

**12.1. Jelölés.** Legyen $K^i = \{\nu \in \{1,...,l\} : i \in K_\nu\}$, $M^j = \{\nu \in \{1,...,l\} : j \in M_\nu\}$ és $\mathcal{L}^{ij} = K^i \cap M^j$.

**12.2. Megjegyzés.** Ekkor $\mathcal{L}^{ij} = \{\nu : r(L_\nu^{\phi_{ij}}) > 0\}$.

**12.3. Jelölés.** Jelöljük $\mathbb{I}$-vel azt a k × m halmazt ahonnan $K^i, M^j$-nél és $\mathcal{L}_{ij}$-nél, illetve $\phi_{ij}$-nél és $E(i, \mathrm{k} + l + j)$-nél az $(i, j)$ párt választjuk.

**12.4. Tétel.** Legyen $\mathcal{I}$ egy szűkített (k, l) típusú minta, $f \in \mathcal{C}^*$ a hozzá tartozó mintaalgebra $\mathcal{C}$ részalgebráján értelmezett lineáris leképezés. Ekkor ha $t_{ij}^f(f(E(i, \mathrm{k} + l + j)) \neq 0$, akkor $r(\tilde{f}) \geq r(\tilde{\phi}_{ij})$ és egyenlőség csak akkor állhat, ha minden $(i', j')$-re, amire $t_{i'j'}^f \neq 0 : \mathcal{L}^{ij} \supseteq \mathcal{L}^{i'j'}$. (A $\phi_{ij}$ és $t_{ij}$ jelöléseket 11.6-ban vezettük be.)

**Bizonyítás:** A $\phi_{ij}$-hez tartozó $L^{\phi_{ij}}$ mátrix az $(i, j)$ helyen 1 és minden más mezője 0. Ezért a $L_\nu^{\phi_{ij}}$ mátrixokban akkor szerepel egyetlen darab 1-es, ha $i \in K_\nu$ és $j \in M_\nu$, egyébként azok nullmátrixok. A megfelelő $L_\nu^f$ mátrixokban az $L_\nu^{\phi_{ij}}$-beli 1-ek helyén $f(E(i, \mathrm{k} + l + j)) \neq 0$ szerepel. Ezért

$$r(L_\nu^f) \geq r(L_\nu^{\phi_{ij}}) \text{ minden } \nu \in \{1,...,l\}\text{-re.} \tag{9}$$

Alkalmazva az (8) egyenletet, ez bizonyítja azt, hogy $r(\tilde{f}) \geq r(\tilde{\phi}_{ij})$.
Most legyen $(i', j') \in \mathbb{I}$ olyan, hogy $f(E(i', \mathrm{k} + l + j')) \neq 0$. Ha $\exists \nu \in (\mathcal{L}^{i'j'} \setminus \mathcal{L}^{ij})$, akkor $r(L_\nu^f) \geq 1 > 0 = r(L_\nu^{\phi_{ij}})$, tehát (9) miatt $r(\tilde{f}) > r(\tilde{\phi}_{ij})$. □

**12.5. Jelölés.** $C^* = \{\phi_{ij} | (i, j) \in \mathbb{I}\}$

**12.6. Definíció.** Legyen $x, y \in \mathbb{I}$. Nevezzük őket **ekvivalens**nek, ha $\mathcal{L}^x = \mathcal{L}^y$. Ez $C^*$-n is definiál egy ekvivalencia-relációt. Vegyük $\mathcal{C}^*$-on az eszerinti ekvivalenciaosztályok lineáris lezártját, ezek a $V_1, ..., V_s$ lineáris alterek.

**12.7. Állítás.** Ekkor $i \neq j \Rightarrow V_i \cap V_j = \{0\}$.

**Bizonyítás:** Egy bázis diszjunkt részhalmazai null-metszetű altereket generálnak és $C^*$ egy bázisa $\mathcal{C}^*$-nak. □

**12.8. Jelölés.** Legyen $V = \bigcup_{i=1}^s V_i$.

**12.9. Eljárás.** A $\mathcal{C}^*$ vektortéren az $f \to r(\tilde{f})$ egy súlyozást határoz meg. Keressünk ezen a vektortéren mohó algoritmussal egy minimális súlyú bázist. Minden lépésnél jegyezzük meg, hogy milyen alteret generálnak a már bevett báziselemek. Így kapunk egy $S_1 < ... < S_{\dim(\mathcal{C}^*)} = \mathcal{C}^*$ altérláncot.

**12.10. Tétel.** Minden $S_u$ halmaz felírható $V$-beli elemek generátumaként. Továbbá legfeljebb egy olyan $V_v$ halmaz van, aminek szerepel eleme az $S_u$-t generáló $V$-beliek között, de nem minden eleme van benne $S_u$-ban.

**Bizonyítás:** Indukcióval $|S_u| = u$-ra:
Kezdőlépés: legyen $f$ olyan, hogy $r(\tilde{f})$ minimális. Ekkor az 12.4 tétel miatt

$$f = \sum_{x \in X} \mu_x \phi_x, \tag{10}$$

ahol $0 \neq \mu_x \in \mathbb{F}_q$ és $x, y \in X \Rightarrow \mathcal{L}^x = \mathcal{L}^y$, és ez pont az, hogy $f$ előáll mint ekvivalens elemek lineáris kombinációja, azaz $f \in V_u$ valamely $u$-ra.
Most adott $S_u$ és egy $f \in \mathcal{C}^*$ ami minimális súlyú az $S_u$-n kívüli elemek körében. Ha $(i, j)$ olyan, hogy $f(E(i, \mathrm{k} + l + j)) \neq 0$, akkor:

- Vagy $r(\tilde{f}) > r(\tilde{\phi}_{ij})$. Ez esetben $f$ minimális súlyúsága miatt $\phi_{ij} \in S_u$.
- Vagy $r(\tilde{f}) = r(\tilde{\phi}_{ij})$. Ez esetben (a 12.4 tétel szerint) minden $(i', j')$-re, amire $f(E(i', \mathrm{k} + l + j') \neq 0$ igaz, hogy $\mathcal{L}^{ij} \supseteq \mathcal{L}^{i'j'}$. Ha $\phi_{i'j'} \notin S_u$, akkor $r(\tilde{f})$ minimálitása miatt $r(\tilde{\phi}_{ij}) = r(\tilde{f}) = r(\tilde{\phi}_{i'j'})$. Szerepcserével elmondva ezt a gondolatmenetet $\mathcal{L}^{i'j'} \supseteq \mathcal{L}^{ij}$-nek is igaznak kell lennie, tehát $\mathcal{L}^{ij} = \mathcal{L}^{i'j'}$.

Tehát azok az $(i, j)$-k, amik $f$ előállításában szerepelnek és nincsenek benne $S_u$-ban ekvivalensek egymással. Ez azt jelenti, hogy bizonyos $\phi_{ij}$-ken kívül csak egyetlen $V_v$-ből van szükségünk elemekre $f$ és így $S_{u+1}$ generálásához. □

**12.11. Állítás.** Ha az $u$-adik lépésben bevett vektor súlya nagyobb az előbb bevetteknél, akkor van olyan $V_v$, aminek szerepel eleme $S_u$-ban de nem szerepel eleme $S_{u-1}$-ben.

**Bizonyítás:** Adott $V_v$-n belül a vektorok azonos súlyúak és ha olyan vektort veszünk be, amitől $S_u$ generátorában új $V_v$-beli elem jelenik meg, akkor a bevett vektor súlya megegyezik a $V_v$-beli vektorok súlyával. Ezért ha az előzőeknél nagyobb súlyú vektort vettünk be, akkor eddig nem értintett $V_v$-ből került be generátor.

**12.12. Megjegyzés.** Az eljárás végrehajtásához nem szükséges a mintacsoportként való ábrázolás ismerete, csupán a csoport kommutátor-relációt kell ismernünk, ugyanis a csoport centruma egy $\mathbb{Z}_p \times ... \times \mathbb{Z}_p$ csoport, amit tekinthetünk vektortérnek. Így a rajta értelmezett lineáris függvényeket is ismerjük.

# 13. Mintacsoport-reprezentáció keresése adott generátorokkal

**13.1. Probléma.** Meg van adva nekünk egy csoport a következő módon: adott két halmaz, $A$ és $B$. A csoport mint az $F_{A \cup B}$ szabadcsoport faktora van megadva a következő relációkkal:

I A csoport nilpotencia-osztálya 2 (azaz bármely $x, y, z$ elemére $[[x, y], z] = 1$).

II Minden $x \in (A \cup B)$-re $x^p = 1$ ($p \neq 2$ prím)

III Minden $a_1, a_2 \in A$-ra $[a_1, a_2] = 1$, hasonlóan $\forall b_1, b_2 \in B : [b_1, b_2] = 1$.

IV Ezen kívül adott néhány $[a_i, b_i] = [a_i', b_i']$ egyenlet ($a_i, a_i' \in A, b_i, b_i' \in B$). Azaz a generátorok kommutátorai időnként megegyeznek.

A kérdés az az, hogy van-e olyan $\mathcal{G}(\mathcal{I})$ szűkített (k, m)-típusú mintacsoport ami izomorf ezzel a csoporttal úgy, hogy az $A$-beli elemek képe $A_{\mathcal{G}}$-beli és a $B$-beli elemek képe $B_{\mathcal{G}}$-beli.

**13.2. Megjegyzés.** A 1.18 állítás szerint $p \neq 2$-re egy $\mathbb{F}_p$ feletti 2-nilpotencia-osztályú mintacsoportban (az 1-en kívül) minden elemnek a rendje $p$. Ez indokolja az (ii) feltételt. A 10.12 tétel szerint ha egy csoportban $G' = Z(G)$ és ez a csoport ábrázolható mintacsoporttal, akkor ábrázolható szűkített (k, m)-típusú mintacsoporttal, tehát a kérdés nem sokkal specifikusabb annál, hogy van-e mintacsoporttal való ábrázolása $G$-nek, ahol $A \cup B$ képei kanonikus csoportgenerátorok.

**13.3. Definíció.** Definiáljunk $K := \{[a, b] | a \in A, b \in B\} \setminus 1$-en két relációt a következő módon:

$$\text{Ha } a \in A, b \in B, 1 \neq [a, b] = c, \text{ akkor legyen } a \sim_x c \text{ és } c \sim_y b.$$

Definiáljunk most egy relációt $A \cup B$-n. Mondjuk azt, hogy

$$\text{Ha } a \in A, b \in B, [a, b] \neq 1 \text{ akkor } a \sim_z b$$

Mindhárom relációt bővítsük ki ekvivalenciarelációvá (azaz vegyük a legszűkebb ekvivalenciarelációt, ami tartalmazza ezeket). A $\sim_x$-nek csak az $A \cup K$-re eső részét tekintsük, a $\sim_y$-nak csak a $B \cup K$-re eső részét. Számozzuk meg az ekvivalenciaosztályokat. Jelöljük a $\sim_x$ típusú ekvivalenciaosztályok közül az $i$-ediket $X_i$-vel, a $\sim_y$ szerintiek közül a $i$-ediket $Y_i$-vel és a $\sim_z$ szerinti $i$-edik ekvivalencia-osztályt $Z_i$-vel.

**13.4. Megjegyzés.** A $K$-beli elemek képei $C_{\mathcal{G}}$-ben lesznek egy megfelelő $\phi$ ábrázolás esetén.

**13.5. Tétel.** Akkor és csak akkor létezik olyan szűkített (k, m)-típusú mintacsoporttal való reprezentációja a $G$ csoportnak, ahol minden $A$-beli elem képe $A_{\mathcal{G}}$-beli és minden $B$-beli elem képe $B_{\mathcal{G}}$-beli, ha teljesülnek a következő feltételek:

1. $a \in A, b \in B, a \sim_z b \Rightarrow [a, b] \neq 1$.
2. $|X_i \cap Y_j| \leq 1$.
3. $|X_i \cap Z_j| \leq 1$.
4. $|Y_i \cap Z_j| \leq 1$.

**13.6. Megjegyzés.** Az első feltétel triviálisnak tűnhet, ha megfeledkezünk arról, hogy $\sim_z$-be beletartoznak azok az elempárok, amiket azért vettünk be, hogy $\sim_z$ ekvivalenciarelációvá váljon. Valójában ez a feltétel azt mondja ki, hogy $\sim_z$ kibővítésénél $A$ és $B$ közé nem kellett új 'élt' behúzni.

**Bizonyítás:** Ha létezik ilyen reprezentáció, akkor nézzük a következő kibővítését a relációknak:

(i) Legyen $E(i,j) \sim_x E(i',j') \Leftrightarrow i = i'$.

(ii) Legyen $E(i,j) \sim_y E(i',j') \Leftrightarrow j = j'$.

(iii) Legyen $E(i,j) \sim_z E(i',j') \Leftrightarrow j = i'$ vagy $E(i,j), E(i',j') \in A_{\mathcal{G}}, j = j'$ vagy $E(i,j), E(i',j') \in B_{\mathcal{G}}, i = i'$.

Ezek is ekvivalenciarelációk. Ebből kapunk ekvivalencia-relációkat $A \cup B$-n is, melyek valóban kibővítik az eredeti relációkat, ugyanis

(i) Ha $[I + E(i,j), x] = (I + E(i',j')]$ akkor $i = i'$.

(ii) Hasonlóan $[x, (I + E(i,j))] = (I + E(i',j')]$ akkor $j = j'$.

(iii) Ha $[(I+E(i,j)), (I+E(i',j'))] \neq 0$, akkor $j = i'$. Ha van $x$, amire $[(I+E(i,j)), x] \neq 0$ és $[(I + E(i',j')), x] \neq 0$ akkor $j = j'$ és ha van $y$ amire $[y, (I + E(i,j))] \neq 0$ és $[y, (I + E(i',j'))] \neq 0$, akkor pedig $i = i'$. Ha két elem ekvivalens az eredeti reláció szerint, akkor lesz köztük a definiáló reláció szerinti lánc ami ilyen lépésekből áll.

Az így definiált ekvivalencia-osztályokra viszont képzenfekvő módon teljesül a négy feltétel. (Az első azt jelenti, hogy $[(I + E(i,j)), (I + E(i',j')) \neq 1$ ha $j = i'$. A második azt jelenti, hogy két oszlop metszete legfeljebb 1 elemű. A harmadik és negyedik esetben is csak $i = i', j = j'$ esetén lehet egy elem benne a metszetben.)
Most vegyünk egy $G$ csoportot ami a 13.1 problémában meghatározott módon van definiálva. Tegyük fel, hogy teljesülnek rá a feltételek. Legyen a $\sim_x$ ekvivalenciaosztályok száma k, a $\sim_y$ ekvivalenciaosztályok száma $m$ és a legnagyobb $\sim_x$ vagy $\sim_y$ ekvivalenciaosztály mérete $l$. Definiálunk egy $\phi : A \cup B \cup K \leftrightarrow A_{\mathcal{G}} \cup B_{\mathcal{G}} \cup C_{\mathcal{G}}$ függvényt.

1. Ha $|X_i \cap Y_j| \neq 0$ (azaz $|X_i \cap Y_j| = 1$), akkor legyen $\phi(X_i \cap Y_j) = (I + E(i, \mathrm{k} + l + j))$.

2. Ha $|X_i \cap Z_j| \neq 0$ akkor legyen $\phi(X_i \cap Z_j) = (I + E(i, \mathrm{k} + j))$.

3. Ha $|Z_i \cap Y_j| \neq 0$ akkor legyen $\phi(Z_i \cap Y_j) = (I + E(\mathrm{k} + i, \mathrm{k}k + l + j))$.

Így minden $A \cup B \cup K$-beli elem képét meghatároztuk egyértelműen, mivel minden $A$-beli elem egyértelműen előáll $X_i \cap Z_j$ alakban valamilyen $i, j$-re, minden $B$-beli elem előáll $Z_i \cap Y_j$ alakban és minden $[A, B]$-beli elem előáll $A_i \cap B_j$ alakban.
Ezek szerint $\phi$ bijekció $A \cup B \cup K$ és $A_{\mathcal{G}} \cup B_{\mathcal{G}} \cup C_{\mathcal{G}}$ között (és rendre $A$-t $A_{\mathcal{G}}$-be, $B$-t $B_{\mathcal{G}}$-be, $K$-t $C_{\mathcal{G}}$-be viszi).
Próbáljuk meg $\phi$-t kiterjeszteni A $\phi|_{\langle A \rangle}, \phi|_{\langle B \rangle}, \phi|_{\langle K \rangle}$ függvényeket könnyű definiálni, ugyanis ezek elemi Abel $p$-csoportról elemi Abel $p$-csoportra képeznek. Ez alapján mindenhol máshol is definiálható: $\phi(a, b, z) := \phi(a)\phi(b)\phi(c)$.

**13.7. Lemma.** Legyen $G$ egy olyan csoport amiben $G' = Z(G)$. Legyen $A$ és $B$ két kommutatív részcsoportja amik együtt generálják $G$-t. Ekkor bármely $g \in G$ felírható $abz$ alakban, ahol $a \in A, b \in B, z \in Z(G)$, továbbá két ilyen módon felírt elem szorzata a következő:

$$(a_1b_1z_1)(a_2b_2z_2) = (a_1a_2)(b_1b_2)(z_1z_2[a_2, b_1]).$$

**Bizonyítás:** Ha egy szorzatban egy $A$-beli elemet felcserélünk egy $B$-belivel, akkor ha (bárhol) megszorozzuk az eredményt a kettő (megfelelő sorrendű) kommutátorával, akkor az eredeti elemet kapjuk vissza. Így tetszőleges elem berendezhető $abz$-alakúvá. Két ilyen alakú elem szorzásakor csak $a_2$ és $b_1$ felcserélése lényeges, ugyanis a $z_1, z_2$ elemek a centrumban vannak. Így teljesül a bizonyítandó képlet. □
Eszerint elég azt igazolnunk, hogy $\phi([a, b]) = [\phi(a), \phi(b)]$ ha $a \in A, b \in B$. Legyen $a = X_i \cap Z_j$, $b = Z_{i'} \cap Y_{j'}$. Ekkor az (i) feltétel szerint $[a, b] \neq 1 \Leftrightarrow j = i'$. Ha $j = i'$ akkor $[a, b] \in X_i \cap Y_{j'}$ az ekvivalencia-relációk definíciója szerint, tehát $\phi([a, b]) = \phi(X_i \cap Y_{j'}) = (I + E(i, \mathrm{k} + l + j))$. Másrészt $\phi(a) = (I + E(i, \mathrm{k} + j))$ és $\phi(b) = (I + E(\mathrm{k} + i', \mathrm{k} + l + j'))$, $[\phi(a), \phi(b)] = (I + E(i, j)E(i', j'))$ ami épp az ami kellett. □

# 14. Incidencia-algebrák

([4] Section 1.2-1.3 alapján)

**14.1. Definíció.** Legyen $X$ egy véges részbenrendezett halmaz, $\mathbb{F}$ pedig egy test. Az ehhez tartozó **incidencia-algebra** a

$$I(X, \mathbb{F}) := \{f : X \times X \to \mathbb{F} | f(x, y) = 0 \text{ ha } x \not\leq y\}$$

halmazon van értelmezve és a műveletei a következők:

$$(f + g)(x, y) = f(x, y) + g(x, y)$$
$$(f \cdot g)(x, y) = \sum_{x \leq z \leq y} f(x, z) \cdot g(z, y)$$
$$(t \cdot f)(x, y) = t \cdot f(x, y)$$

ahol $f, g \in I(X, \mathbb{F}), t \in \mathbb{F}$ és $x, y, z \in X$.

**14.2. Megjegyzés.** Az incidencia-algebrák általánosabban is definiálhatók ha az alaptest helyett kommutatív gyűrűt veszünk és $X$ végességi feltételét a lokális végességre cseréljük. Ennek a résznek a fő tétele (14.14) azonban csak testek fölött igaz.
A következő állítás mutatja, hogy az incidencia-algebrák természetes kibővítései a mintacsoportoknak illetve mintaalgebráknak.

**14.3. Állítás.** Ha $I(X, \mathbb{F})$ egy incidencia-algebra, akkor a

$$G = \{f \in I(X, \mathbb{F}) | f(x, x) = 1\}$$

halmaz csoportot alkot az $I(X, \mathbb{F})$ szerinti szorzásra. Ez a csoport izomorf az $X$-hez mint zárt mintához tartozó mintacsoporttal, azaz $G \cong \mathcal{G}(X)$.

**Bizonyítás:** Először képezzük le $I(X,\mathbb{F})$-et $M_{|X|}(\mathbb{F})$-be. Ehhez vegyük $X$-nek egy $\tau : X \leftrightarrow \{1,...,|X|\}$ topologikus sorrendjét. Ekkor $x < y \Rightarrow \tau(x) < \tau(y)$. Legyen $\phi : I(X,\mathbb{F}) \to M_{|X|}(\mathbb{F})$ a következő:

$$\phi(f) := \sum_{x,y\in X} f(x,y)E(\tau(x),\tau(y)).$$

Máshogy mondva, $\phi(f)_{ij} = f(\tau^{-1}(i),\tau^{-1}(j))$ azaz a $\phi(f)$ mátrix $(i,j)$ mezőjén álló szám $f(\tau^{-1}(i),\tau^{-1}(j))$-vel egyenlő.

**14.4. Lemma.** Ekkor $\phi$ egy művelettartó leképezés.

**Bizonyítás:** Közvetlenül látszik, hogy $\phi(f+g) = \phi(f) + \phi(g)$ és $\phi(tf) = t\phi(f)$.

$$\phi(f\cdot g)_{\tau(x)\tau(y)} = (f\cdot g)(x,y) = \sum_{x\le z\le y} f(x,z)\cdot g(z,y) =^1 \sum_{z\in X} f(x,z)g(z,y)$$
$$=^2 \sum_{i=1}^{|X|} f(x,\tau^{-1}(i))g(\tau^{-1}(i),y) =^3 \sum_{i=1}^{|X|} \phi(f)_{\tau(x)i}\phi(g)_{i\tau(y)} =^4 (\phi(f)\cdot\phi(g))_{\tau(x)\tau(y)}$$

1: ha $x \not\le z$ akkor $f(x,z) = 0$ és ha $z \not\le y$ akkor $g(z,y) = 0$, tehát csak 0 értékű tagokkal bóvíttettük a szummát.
2: $\tau$ egy egy-egyértelmű megfeleltetés $X$ és $\{1,...,|X|\}$ között, így itt csak átparaméterezték a szummát.
3: $\phi$ definíciója szerint
4: a mátrix-szorzás definíciója szerint
Azt kaptuk, hogy $\phi(f\cdot g)_{\tau(x)\tau(y)} = (\phi(f)\cdot\phi(g))_{\tau(x)\tau(y)}$ ami épp azt jelenti, hogy $\phi$ szorzattartó leképezés. □
A $G = \{f \in I(X,\mathbb{F}|\forall x : f(x,x) = 1\}$ halmaz $\phi$ szerinti képének az elemei megegyeznek $\mathcal{G}(X)$ elemeivel. Mivel $\phi$ szorzattartó bijekció, ez azt jelenti, hogy $\{f \in I(X,\mathbb{F}|\forall x : f(x,x) = 1\}$ zárt a szorzásra. A $\phi$ függvény azt is bizonyítja, hogy $G \cong \mathcal{G}(X)$. □

**14.5. Definíció.** Egy $X$ részbenrendezett halmaz $x \le y$ elemeire az $[x,y]$ **intervallum** az $x$ és $y$ "közötti" elemekből áll, azaz

$$[x,y] = \{z \in X | x \le z \le y\}.$$

**14.6. Megjegyzés.** A továbbiakban ha intervallumok helyett egyszerűen rendezett párokra gondolunk, akkor ugyanazokat a fogalmakat és eredményeket kapjuk.

**14.7. Definíció.** Legyen $E$ egy ekvivalencia-reláció egy $X$ halmaz intervallumain. Az $f \in I(X,\mathbb{F})$ függvényt ***E*-függvény**nek nevezzük, ha

$$[x,y]E[u,v] \Rightarrow f(x,y) = f(u,v)$$

(ahol $[x,y]E[u,v]$ azt jelöli, hogy $[x,y]$ és $[u,v]$ ugyanabba az $E$-szerinti ekvivalenciaosztályba tartozik). Jelöljük $I(X_E,\mathbb{F})$-fel az $E$-függvények halmazát.

**14.8. Definíció.** Az olyan $E$ ekvivalencia-relációkat amelyekre $f, g \in I(X_E, \mathbb{F}) \Rightarrow (f \cdot g) \in I(X_E, \mathbb{F})$ nevezzük **rend-kompatibilis**nek (angolul 'order compatible').

**14.9. Megjegyzés.** Ez a jelölés valamelyest félrevezető lehet: $I(X_E, \mathbb{F})$ speciális esetektől eltekintve nem incidencia-algebra.

**14.10. Definíció.** Ha $E$ egy rend-kompatibilis ekvivalencia-reláció $X$ intervallumain, akkor a hozzá tartozó $I(X_E, \mathbb{F})$ algebrát **redukált incidencia-algebrá**nak nevezzük.

**14.11. Megjegyzés.** Egy redukált incidencia-algebrát úgy kapunk egy mintaalgebrából, hogy hozzávesszük az $E(i, i)$ elemeket és bizonyos $x, y \in \mathcal{I}$ párokra kikötjük, hogy $E(x)$ és $E(y)$ együtthatója mindig megegyezzen. Ha amit így kapunk az egy algebra, akkor az redukált incidencia-algebra.

**14.12. Jelölés.** Két $x, y \in I((X, \mathbb{F})$ elem **Hadamard szorzatá**nak a

$$(f * g)(x, y) = f(x, y) \cdot g(x, y)$$

által definiált függvényt nevezzük. (Ezt felfoghatjuk úgy, mint $f$ és $g$ "pontonkénti" szorzatát.)

**14.13. Jelölés.** Legyen

$$\zeta(x, y) = \begin{cases} 1, \text{ ha } x \leq y \\ 0 \text{ különben.} \end{cases}$$

(Ekkor $\zeta \in I(X, \mathbb{F})$.)

**14.14. Tétel.** ([4] Proposition 1.3.9) Legyen $A$ egy részalgebrája $I(X, \mathbb{F})$-nek. Ekkor $A$ pontosan akkor redukált incidencia-algebra, ha

(i) $\zeta \in A$

(ii) ha $f, g \in A$, akkor $f * g \in A$.

**Bizonyítás:** Tegyük fel, hogy $A = I(X_E, \mathbb{F})$ valamely $E$ ekvivalencia-relációra. Minden $[x, y]$ intervallumra $x \leq y$, így $\zeta(x, y) = 1$, tehát $\zeta \in I(X_E, \mathbb{F})$. Ha $[x_1, y_1]E[x_2, y_2]$, akkor $f, g \in A$-ra

$$(f * g)(x_1, y_1) = f(x_1, y_1)g(x_1, y_1) = f(x_2, y_2)g(x_2, y_2) = (f * g)(x_2, y_2).$$

A másik irányhoz definiáljuk az $E$ ekvivalencia-relációt a következő módon:

$$[x_1, y_1]E[x_2, y_2] \Leftrightarrow f(x_1, y_1) = f(x_2, y_2) \text{ minden } f \in A\text{-ra.}$$

(Ez valóban ekvivalencia-reláció). Legyenek az ekvivalencia-osztályai az $\alpha_1, ..., \alpha_n$ intervallumhalmazok. Ha $i \neq j$ akkor létezik $f_{ij} \in A$, amire $f_{ij}(\alpha_i) \neq f_{ij}(\alpha_j)$ (ahol $f(\alpha_i) = f(x, y)$ tetszőleges $[x, y] \in \alpha_i$-re). Legyen

$$\phi_{ij} := \frac{f_{ij} - f_{ij}(\alpha) \cdot \zeta}{f_{ij}(\alpha_i) - f_{ij}(\alpha_j)}.$$

Ekkor $\phi_{ij} \in A$ mert feltettük, hogy $\zeta \in A$. Továbbá $\phi_{ij}(\alpha_i) = 1$, $\phi ij(\alpha_j) = 0$ (ha $j \neq i$). Legyen $\Phi_i$ a $\phi_{ij}(j \in (\{1, ..., n\} \setminus \{i\}))$ függvények Hadamard-szorzata. A Hadamard-szorzatokról tett feltevésünk szerint $\Phi_i \in A$. Ekkor

$$\Phi_i(\alpha_j) = \prod_{k \neq i} \phi_{ik}(\alpha_j).$$

Ha $j = i$, akkor a szorzat minden tagja 1, így $\Phi_i(\alpha_i) = 1$. Ha $j \neq i$, akkor a szorzatban szerepel a $\phi_{ij}(\alpha_j) = 0$ tag, tehát $\Phi_i(\alpha_j) = 0$. A $\{\Phi_1, ..., \Phi_n\}$ halmaz (lineárisan) generálja $I(X_E, \mathbb{F})$-et, ugyanis minden $f \in I(X_E, \mathbb{F})$-re $f = \sum_i f(\alpha_i)\Phi_i$. Mivel $A \subseteq I(X_E, \mathbb{F})$ és $\{\Phi_1, ..., \Phi_n\} \subset A$, $A = I(X_E, \mathbb{F})$-nek kell lennie. □

# Hivatkozások


[1] Pálfy Péter Pál: Csoportelmélet, kiadatlan jegyzet 2016

[2] P. Diaconis and N. Thiem. Supercharacter formulas for pattern groups. *Trans. Amer. Math. Soc.* **361** (2009), 3501-3533.

[3] A. J. Weir. Sylow $p$-subgroups of the general linear groups over finite fields of characteristic $p$. *Proc. Amer. Math. Soc.* **6** (1955), 454-464.

[4] E. Spiegel; C. O'Donnell *Incidence algebras*, Monographs and textbooks in pure mathematics **206**, Marcel Dekker, Inc., New York: 1997.

[5] Z. Halasi; P. P. Pálfy The number of conjugacy classes in a pattern group is not a polynomial function. *J. Group Theory* **14** (2011), no. 6, 841-854.