ELTE TTK Matematika BSc Szakdolgozat

Nem szokványos algebrai struktúrák nemzetközi és hazai matematikaversenyeken

Írta:

Tóth Réka Judit

(Matematika BSc (2009), tanári szakirány)

Témavezető: Hegyvári Norbert, főiskolai tanár
Leadás dátuma: 2012. május 31.

1. Bevezetés

Szakdolgozatomban néhány nem szokványos, nagyrészt nem kommutatív struktúráról lesz szó, amellyel már a magasabb szintű versenyeken akár a középiskolások is találkozhatnak. Némi elméleti háttér után konkrét versenyfeladatokon szemléltetjük, hogy az egyetemen tanult módszerek segítségével szinte triviálisan megoldhatóak, ezek az amúgy a középiskolások számára nagyon nehéznek bizonyuló feladatok. Főként nem kommutatív csoportokkal foglalkozunk, ezen belül is a mátrixok témakörével, de még más érdekes struktúrák is elő fognak fordulni.

2. Csoportok

2.1. Csoport axiómák:

Először is tudnunk kell mit nevezünk csoportnak.
Adott $G \neq \emptyset$ egy $\circ$ műveletre nézve zárt halmaz. Akkor nevezünk G-t csoportnak, ha:

- asszociatív: $\forall a, b, c \in G$ esetén

$$(a \circ b) \circ c = a \circ (b \circ c) \tag{1}$$

- létezik egységelem: $\exists e \in G$, úgy hogy $\forall a \in G$ esetén

$$e \circ a = a \circ e = a \tag{2}$$

- létezik inverz: $\forall a \in G$ esetén $\exists a^{-1}$, úgy hogy

$$a \circ a^{-1} = a^{-1} \circ a = e \tag{3}$$

Lényeges hogy a kommutativitást nem tettük fel, ha még ezt is feltesszük, akkor már kommutatív csoportról beszélünk.

1. Definíció. *A $G \neq \emptyset$ $a \circ$ műveletre nézve kommutatív csoport ha teljesülnek a fenti (1),(2),(3) axiómák, továbbá: $\forall a, b \in G$ esetén*

$$a \circ b = b \circ a \tag{4}$$

Ezt szokás Abel-csoportnak is nevezni.

Néhány példa:

A szokásos összeadásra nézve csoport: $\mathbb{Z}, \mathbb{Z}_n, \mathbb{Z}_{[x]}, \mathbb{Q}, \mathbb{R}, \mathbb{C}, T_{[x]}, T^{n \times k}$

A szorzásra nézve: $\mathbb{Q} \setminus \{0\}, \mathbb{R} \setminus \{0\}, \mathbb{C} \setminus \{0\}$.

De például $\mathbb{Z}_{10}$ már nem csoport a szorzásra nézve, mert pl. a 2-nek nincs inverze. Az $\mathbb{R}^{n \times n} \setminus \{0\}$ sem jó, mert van nullosztó, és az inverzzel is baj van, de ha $T^{n \times n}$-ben vesszük az invertálható mátrixok halmazát, az már jó lesz. (Ez a későbbiekben még egy fontos nem kommutatív csoport lesz.)

Most nézzünk két versenyfeladatot, melyekhez nem lesz szükségünk további ismeretekre!

A következő feladat a William Lowell Putnam Mathematics Competition 2001-es versenyének A-1-es feladata:

1. Feladat. *Adott egy S halmaz egy $*$ bináris művelettel, azaz*

$$\forall a, b \in S, a * b \in S \tag{5}$$

. Tegyük fel, hogy

$$(a * b) * a = b \ \forall a, b \in S. \tag{6}$$

Bizonyítsuk be, hogy $a * (b * a) = b \ \forall a, b \in S$!

Érdemes még a megoldás előtt egy pillanatra megállni, hogy megnézzük tulajdonképpen miről is lesz szó. Ha sikerül belátni az állítást, akkor az S halmazon a $*$ művelet egyfajta speciális asszociativitását is beláttuk, mivel akkor

$$a * (b * a) = b = (a * b) * a$$

Megoldás:

Induljunk ki a (6) egyenletből:

$$(a * b) * a = b$$

Vegyük a $*$ műveletét az egyenlet mindkét oldalának jobbról $(a * b)$-vel!

$$[(a * b) * a] * (a * b) = b * (a * b)$$

A (5) összefüggés miatt $(a * b) := c \in S$.

$$(c * a) * c = b * (a * b)$$

A baloldalra alkalmazva a (6)-ot:

$$a = b * (a * b)$$

Már csak az egyenletet kell megfordítanunk, és szereposztást cserélnünk a bizonyítandó összefüggéshez:

$$a * (b * a) = b \ \square$$

Ismét egy William Lowell Putnam Mathematics Competition feladat 1971-ből:

2. Feladat. *Egy* $(S, \circ)$ *struktúráról a következőket tudjuk:*

1. $\forall x \in S$*-re* $x \circ x = x$.
2. $\forall x, y, z \in S$ *esetén* $(x \circ y) \circ z = (y \circ z) \circ x$.

Bizonyítsuk be, hogy a művelet kommutatív!

I.Megoldás:

Vegyük (2.)-t $y = x$ szereposztással:

$$\underbrace{(x \circ x)}_{=x \text{ (1.)miatt}} \circ z = (x \circ z) \circ x$$

Mindkét oldal $\circ x$-ét véve:

$$(x \circ z) \circ x = ((x \circ z) \circ x) \circ x$$

(2.)-t alkalmazva a jobb oldalra:

$$(x \circ z) \circ x = \underbrace{(x \circ x)}_{=x \text{ (1.)miatt}} \circ (x \circ z)$$

Vagyis $x' = x \circ z$-t véve:

$$x' \circ x = x \circ x'$$

Ezzel a kommutativitást beláttuk! □

II.Megoldás:

Az eleje eléggé hasonlít az előzőhöz, de mégis a folytatás miatt másnak tekinthető.
Vegyük (2.)-t $y = x$ szereposztással:

$$\underbrace{(x \circ x)}_{=x \text{ (1.)miatt}} \circ z = (x \circ z) \circ x$$

„Szorozzuk" meg jobbról z-vel:

$$(x \circ z) \circ z = ((x \circ z) \circ x) \circ z$$

Az egyenlet mindkét oldalára (2.)-t alkalmazva:

$$\underbrace{(z \circ z)}_{=z \text{ (1.)miatt}} \circ x = \underbrace{(x \circ z) \circ (x \circ z)}_{=(x \circ z) \text{ (1.)miatt}}.$$

Vagyis

$$z \circ x = x \circ z. \ \square$$

3. Miből következhet a kommutativitás?

3.1. Leképezések

A következőkben látni fogunk a csoportokkal kapcsolatos példák között leképezéses feladatot is, ahol a kommutativitás a homomorfizmus tulajdonságain múlik, így nézzük át ennek is a definícióit!

2. Definíció (homomorfizmus). *Legyenek V_1, V_2 vektorterek ugyanazon T test fölött. A $\varphi : V_1 \to V_2$ hozzárendelést lineáris leképezésnek (vektortér homomorfizmusnak) nevezzük, ha: $\forall v_1, v_2 \in V_1$ esetén $\varphi(v_1 \otimes v_2) = \varphi(v_1) \otimes \varphi(v_2)$ és $\forall v \in V_1$, $\forall \lambda \in T$ esetén $\varphi(\lambda v) = \lambda \varphi(v)$.*

3. Definíció (injektív leképezés). *φ lineáris leképezés injektív, ha $a \neq b$ esetén $\varphi(a) \neq \varphi(b)$.*

3.2. Kommutativitás a homomorfizmusból

Mielőtt rátérnénk a komolyabb feladatra, nézzük egy triviális „kis testvérét" ami segíthet majd a bonyolultabb feladat átlátásában is.

3. Feladat. *Legyen $\langle G, \cdot \rangle$ egy csoport, úgy hogy $\forall a, b \in G$ esetén*

$$(ab)^2 = a^2 b^2$$

Igazoljuk, hogy $\langle G, \cdot \rangle$ kommutatív!

Megoldás:

Induljunk ki a feladat szövegéből:

$$(ab)^2 = a^2 b^2$$

Ezt kifejtve

$$abab = aabb$$

Mivel G csoport, $\exists a^{-1}, b^{-1}$, vagyis az egyenletet ezekkel balról, ill. jobbról megszorozva:

$$ba = ab \ \square$$

A következő ismert feladat megoldására nem olyan egyszerű rájönni, bár a megoldás az előzőek fényében már nem is tűnhet olyan bonyolultnak:

4. Feladat. *Legyen $\langle G, \cdot \rangle$ egy csoport, melyen definiálunk egy leképezést: $\varphi : G \to G\varphi(x) = x^3$. Tegyük fel φ-ről, hogy homomorfizmus, és hogy injektív. Igazoljuk, hogy ekkor a csoport kommutatív.*

Megoldás:

Mivel φ homomorfizmus (lásd 2. definíció), ezért:

$$(xy)^3 = \varphi(xy) = \varphi(x) \cdot \varphi(y) = x^3 \cdot y^3$$

Vagyis

$$xyxyxy = xxxyyy \;\Big| x^{-1}\cdot, \cdot y^{-1}$$

Mivel G csoport, és $x, y \in G$ (3.) axióma alapján $\exists x^{-1}, y^{-1}$.

$$yxyx = xxyy \;\Big| yx\cdot$$

Ismét kihasználva a homomorfizmust a baloldalon ($(yx)^3 = y^3x^3$):

$$\begin{gathered} yyyxxx = yxxxyy \;\Big| y^{-1}\cdot \\ y^2x^3 = x^3y^2 \end{gathered}$$

Legyen $x = a^2$ és $y = b^3$. Az egyenletünk így:

$$\begin{gathered} (b^3)^2(a^2)^3 = (a^2)^3(b^3)^2 \\ (b^2a^2)^3 = (a^2b^2)^3 \end{gathered}$$

Most φ injektivitását használjuk ki (lásd 3. definíció), vagyis:

$$\begin{gathered} b^2a^2 = a^2b^2 \;\Big| a\cdot, \cdot b \\ ab^2a^2b = a^3b^3 \end{gathered}$$

Jobb oldalon ismét a homomorfizmust használva ki:

$$abbaab = ababab \;\Big| a^{-1}\cdot, b^{-1}\cdot, \cdot b^{-1}, \cdot a^{-1}$$

Tehát:

$$ba = ab \;\square$$

4. Mátrixokról általában

4. Definíció (Mátrix). *Legyen T egy test. Ekkor a $T^{n\times m}$ felett értelmezett $n \times m$-es mátrixnak azokat a függvényeket nevezzük, melyek $A : \{1, 2, 3, \dots n\} \times \{1, 2, \dots m\} \to T$ és minden rendezett$\langle i, j\rangle$ párhoz egy $a_{ij} \in T$-t rendelnek.*

Jelölés: Általában pl. egy 3×4-es mátrix: $A = \begin{pmatrix} a_{11} & a_{12} & a_{13} & a_{14} \\ a_{21} & a_{22} & a_{23} & a_{24} \\ a_{31} & a_{32} & a_{33} & a_{34} \end{pmatrix}$

5. Definíció (mátrixok összeadása). *Csak azonos dimenziójú mátrixok adhatóak össze. Legyen $A, B \in T^{n\times m}$, ekkor $(A + B) \in T^{n\times m}$ és $A_{[i,j]} = a_{i,j}$ jelöléssel: $(A + B)_{[i,j]} = A_{[i,j]} + B_{[i,j]}$.*

1. Állítás. *Az $n\times m$-es mátrixok a fent definiált összeadásra nézve kommutatív csoportot alkotnak.*

Bizonyítás: Először meg kell vizsgálnunk, hogy az így definiált összeadásra zárt-e az

$n \times m$-es mátrixok halmaza, ami a definícióból triviálisan következik. Ezután végig kell vennünk a csoportaxiómákat: Mindig nézzük a mátrixok adott $[i, j]$ elemét, hiszen ha a mátrixok minden elemére igaz valami, akkor a mátrixokra is.

1. $((A+B)+C)_{[i,j]} = (A+B)_{[i,j]} + C_{[i,j]} = A_{[i,j]} + B_{[i,j]} + C_{[i,j]} = A_{[i,j]} + (B+C)_{[i,j]} = (A + (B + C))_{[i,j]}$
2. $(I + A)_{[i,j]} = I_{[i,j]} + A_{[i,j]} = A_{[i,j]} + I_{[i,j]} = A_{[i,j]} \Rightarrow \forall[i, j] I_{[i,j]} = 0$ az egységelem.

   Megjegyezzük, itt az I nem az egységmátrixot jelöli, hanem az összeadás egységelemét, a nullmárixot!
3. $(A + A^{-1})_{[i,j]} = A_{[i,j]} + A^{-1}_{[i,j]} = I_{[i,j]} = 0 \Rightarrow \forall[i, j] A^{-1}_{[i,j]} = -A_{[i,j]}$

És kommutatív: $(A + B)_{[i,j]} = A_{[i,j]} + B_{[i,j]} = B_{[i,j]} + A_{[i,j]} = (B + A)_{[i,j]}$.
Itt kihasználjtuk, hogy a mátrixok elemei egy T testből valóak, ami kommutatív.

6. Definíció (Szimmetrikus mátrix). *Egy A mátrixot szimmetrikusnak nevezünk, ha $\forall[i, j]$-re $A_{[i,j]} = A_{[j,i]}$. (Természetesen ennek csak $n \times n$-es, négyzetes mátrixok esetén van értelme.)*

7. Definíció (Transzponált). *Minden $A \in T^{n\times m}$ mátrixhoz definiálhatunk egy $A^T \in T^{m\times n}$ transzponált mátrixot, melyet úgy kapunk, hogy $A^T_{[i,j]} = A_{[j,i]}$. (A szimmetrikus mátrixoknál tehát $A = A^T$.)*

8. Definíció (Mátrix szorzás). *Két mátrixot csak akkor szorozhatunk össze, ha a baloldali mátrix oszlopainak száma megegyezik a jobboldali sorainak számával. Vagyis ha* $A \in T^{(n\times m)}$ *és* $B \in T^{(m\times k)}$*, akkor* $A \cdot B \in T^{(n\times k)}$ *és* $(A \cdot B)_{[i,j]} = \sum_{l=1}^{m}(A_{[i,l]}B_{[l,j]})$.

Megjegyzés: A mátrixszorzás nem kommutatív, ami már a definícióból is látszik, ezért is van a mátrixoknak kiemelt fontossága ebben a dolgozatban, mivel a mátrixok azok, amelyekkel a nem kommutatív struktúrák közül, már a középiskolások is találkozhatnak nemzetközi versenyeken.

Ezzekkel az alapokkal már bőségesen megoldható a következő 1990-es William Lowell Putnam Mathematics Competition A-5-ös feladata:

5. Feladat. *Ha* A *és* B *ugyanakkora négyzetes mátrixok, és tudjuk, hogy* $ABAB = 0$*, következik-e, hogy* $BABA = 0$*?*

Megoldás:

Elég egy ellenpéldát mutatnunk rá:

Legyen $A = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$ és $B = \begin{pmatrix} 0 & 1 & 1 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix}$.

Ekkor

$$ABAB = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}\begin{pmatrix} 0 & 1 & 1 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix}\begin{pmatrix} 0 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}\begin{pmatrix} 0 & 1 & 1 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix} =$$

$$= \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix}\begin{pmatrix} 0 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}\begin{pmatrix} 0 & 1 & 1 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix} =$$

$$= \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 & 1 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}.$$

Ugyanakkor

$$BABA = \begin{pmatrix} 0 & 1 & 1 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix}\begin{pmatrix} 0 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}\begin{pmatrix} 0 & 1 & 1 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix}\begin{pmatrix} 0 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} =$$

$$= \begin{pmatrix} 0 & 1 & 2 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 & 1 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} =$$

$$= \begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}. \square$$

Ehhez a feladathoz persze hozzá kell tennünk, hogy nem olyan egyszerű ilyen példát találni, habár elég sok van.

Kiindulási alap lehet, hogy ha A-nak vagy B-nek lenne inverze akkor triviálisan megoldható lenne a feladat, hiszen ha $\exists A^{-1}$, vagy $\exists B^{-1}$, akkor

$$ABAB = 0$$

balról A^{-1}-gyel, jobbról A-val; vagy jobbról B^{-1}-gyel, balról B-vel megszorozva kapjuk:

$$BABA = 0$$

Az invertálhatósággal még a következő fejezetben fogunk foglalkozni. (Hogy miért nem foglalkozunk azzal, hogy baloldali/jobboldali inverz-e, lásd majd (2). tétel)

Tehát ha ellenpéldát akarunk keresni akkor a nem invertálható mátrixok körében kell szétnéznünk, vagyis olyan mátrixokat keresünk, aminek a determinánsa zérus. (lásd majd (6). tétel)

Hasonló alapon például jó ellenpélda lenne:
$A = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$ és $B = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix}$.

...

Ezzel már át is tértünk a következő témánkra.

5. Mátrixok invertálhatósága

Azt láttuk, hogy az $(n \times m)$-es mátrixok az összeadásra nézve csoportot alkotnak. Azonban azt, hogy a szorzásra nézve is csoportot alkotnak-e már nem olyan egyszerű eldönteni. Azt szintén láttuk, hogy a mátrixszorzás nem kommutatív (lásd 8. definíciónál), de csoport-e egyáltalán, vagy milyen megszorítások mellett az?

Egyszerüsítsük a vizsgálódásunkat a négyzetes mátrixokra.

9. Definíció. *Ha egy $A \in T^{n\times n}$ mátrixhoz létezik olyan $A_j^{-1} \in T^{n\times n}$ mátrix, hogy $A \cdot A_j^{-1} = I$, akkor A_j^{-1}-et az A mátrix jobboldali inverzének nevezzük.(Hasonlóan definiálható $A_b^{-1}A = I$ balinverz.)*

2. Tétel (Négyzetes mátrixok inverze). *Ha egy A négyzetes mátrixnak van jobboldali inverze, akkor van baloldali inverze is, és a kettő egyenlő. (Azaz, ha* $\exists A_j^{-1}$ *akkor* $\exists A_b^{-1}$ *is, és* $A_j^{-1} = A_b^{-1}$*.)*

Bizonyítás:

A négyzetes mátrixok szorzásának asszociativitásából következik.
Először bizonyítsuk azt a részt, hogy ha $\exists A_j^{-1}$ és $\exists A_b^{-1}$ is akkor egyenlőek.

$$A_j^{-1} = IA_j^{-1} = (A_b^{-1}A)A_j^{-1} = A_b^{-1}(AA_j^{-1}) = A_b^{-1}I = A_b^{-1} \ \square$$

Indirekt módon tegyük fel, hogy $\exists A_j^{-1}$, de $\nexists A_b^{-1}$. Ekkor $A_j^{-1}A = K \neq I$. Vagyis: $A = IA = (AA_j^{-1})A = A(A_j^{-1}A)$. Vagyis $A(A_j^{-1}A) = A$ ami csak úgy lehet, ha $A_j^{-1}A = I$ így ellentmondásra jutottunk. $\square$

A következő 1991-es William Lowell Putnam Mathematics Competition A-2-es versenyfeladatához a mátrixokról elég annyit ismerni, hogy a szorzás nem kommutatív, illetve az inverz definícióját.

6. Feladat. *Legyen A és B két különböző* $n \times n$*-es valós mátrix. Ha* $A^3 = B^3$ *és* $A^2B = B^2A$*, akkor* $A^2 + B^2$ *lehet-e invertálható?*

Megjegyzés: a (8.), (5.) definíciók alapján $(A^2+B^2) \in T^{n\times n}$, vagyis a 2. tétel alapján, elég ha belátjuk, hogy jobb/bal oldali inverz létezik-e vagy sem.

Mindkét megoldásban a feladat összefüggéseit arra vezetjük vissza, hogy ha invertálható lenne, akkor A és B egyenlő lenne.

I.Megoldás:

Vizsgáljuk $(A^2 + B^2)B$ mátrixot! A feladat összefüggéseit felhasználva:

$$(A^2 + B^2)B = A^2B + B^3 = B^2A + A^3 = (B^2 + A^2)A = (A^2 + B^2)A \tag{7}$$

Indirekt módon tegyük fel, hogy létezik egy K mátrix, hogy $K \cdot (A^2 + B^2) = I$, akkor a (7) egyenlet két végét K-val balról beszorozva:
$\underbrace{K(A^2 + B^2)}_{I} B = \underbrace{K(A^2 + B^2)}_{I} A \Rightarrow B = A$ ami a feladat szövege szerint nem lehetséges.
Ellentmondásra jutottunk, tehát hibás volt a feltevés, nem létezik ilyen mátrix. $\square$

II.Megoldás:

Ebben is indirekt bizonyítást használunk, mégis kicsit eltér az előzőtől: Tegyük fel, hogy létezik K inverz: $K \cdot (A^2 + B^2) = I$. Ekkor $A - B = I(A - B) = K(A^2 + B^2) \cdot (A - B) = K(\underbrace{A^3 - B^3}_{0} - \underbrace{A^2B - B^2A}_{0}) = K \cdot 0 = 0$, ekkor ellentmondásra jutottunk, hiszen ha A és B különböző, $A - B$ nem lehet 0. $\square$

Most nézzük a International Mathematics Competition for University Students (IMC) 2009-es versenyének 2. feladatát:

7. Feladat. *Legyenek $A, B, C \in \mathbb{R}^{n\times n}$-es mátrixok, továbbá tegyük fel, hogy A invertálható. Bizonyítsuk be, hogy ha*

$$(A - B)C = BA^{-1} \Rightarrow C(A - B) = A^{-1}B!$$

Megoldás:

Vegyük a kiindulási egyenlőséget:

$$(A - B)C = BA^{-1}$$

Vonjunk le az egyenlet mindkét oldalából BA^{-1}-t, majd adjunk hozzá I-t:

$$(A - B)C - BA^{-1} + I = I$$

Az egyenlet baloldalán lévő I-t átírhatjuk AA^{-1}-re, amit kiemelve az utolsó két tagból:

$$(A - B)C + (A - B)A^{-1} = I$$

Vagyis

$$(A - B)(C + A^{-1}) = I$$

Tehát $(A - B)$ és $(C + A^{-1})$ egymás inverzei, és mivel A, B, C $n \times n$-es mátrixok, ezért ezek is négyzetesek, vagyis a 2. tétel alapján:

$$(A - B)(C + A^{-1}) = (C + A^{-1})(A - B) = I$$

Azaz

$$C(A - B) + \underbrace{A^{-1}A}_{I} - A^{-1}B = I$$

I-t, és $A^{-1}B$-t levonva mindkét oldalból kapjuk,

$$C(A - B) = A^{-1}B \ \square$$

A következő feladat a William Lowell Putnam Mathematics Competition 1986-os versenyének B-6-os feladata. Ez egy kifejezetten érdekes és középiskolás szinten igencsak nehéznek bizonyuló feladat, amelyről elsőre nem is látszik, hogy köze lenne az inverzekhez:

8. Feladat. *Legyenek $A, B, C, D \in T^{n\times n}$ mátrixok, úgy, hogy AB^T és CD^T mátrixok szimmetrikusak, továbbá $AD^T - BC^T = I$. Bizonyítsuk be, hogy $A^TD - C^TB = I$!*

Megoldás:

Először vegyünk néhány egyszerű megállapítást, amelyek ugyan a 7. definícióból adódnak, de a megoldáshoz szükségünk lehet rájuk:

1. $(A^T)^T = A$
2. $(AB)^T = B^TA^T$
3. $(A - B)^T = A^T - B^T$

Vegyük a AB^T és a CD^T mátrixokat. A feladat szerint ezek szimmetrikusak, tehát

$$AB^T = (AB^T)^T \underbrace{=}_{2.} (B^T)^TA^T \underbrace{=}_{1.} BA^T$$

$$AB^T - BA^T = 0 \tag{8}$$

Hasonlóan:

$$CD^T - DC^T = 0 \tag{9}$$

Tudjuk továbbá, hogy

$$AD^T - BC^T = I \tag{10}$$

Vegyük ennek a transzponáltját!

$$(AD^T - BC^T)^T \overset{3.}{=} (AD^T)^T - (BC^T)^T \overset{2.}{=} (D^T)^TA^T - (C^T)^TB^T = \underbrace{=}_{1.} DA^T - CB^T = I^T = I.$$

Tehát

$$DA^T - CB^T = I \tag{11}$$

Az A, B, C, D $(n\times n)$-es mátrixokból az alábbi módon építsünk $(2n\times 2n)$-es mátrixokat: $\alpha = \begin{pmatrix} A & B \\ C & D \end{pmatrix}$, és $\beta = \begin{pmatrix} D^T & -B^T \\ -C^T & A^T \end{pmatrix}$.

Ekkor a (8),(9),(10),(11) egyletek felírhatóak, mint:

$$\alpha \cdot \beta = I$$

Itt I természetesen már a $(2n \times 2n)$-es egységmátrixot jelöli.

Vagyis β az α-nak a baloldali inverze. Mivel α és β is $(2n \times 2n)$ négyzetes mátrixok ezért β a jobboldali inverze is α-nak (lásd 2. tétel), vagyis

$$I = \beta \cdot \alpha = \begin{pmatrix} D^T & -B^T \\ -C^T & +A^T \end{pmatrix} \begin{pmatrix} A & B \\ C & D \end{pmatrix} = \begin{pmatrix} D^T A - B^T C & D^T B - B^T D \\ -C^T A + A^T C & -C^T B + A^T D \end{pmatrix}$$

Ebből négy egyenlet adódik, amelyből az egyik épp

$$-C^T B + A^T D \ \square$$

6. Determináns

Mielőtt egyáltalán értelmezni tudnánk ezt a fogalmat, szólnunk kell pár szót a permutációkról.

6.1. Permutációk

10. Definíció. *Az $1, 2, 3, \ldots, n$ számok permutációinak halmazát jelöljük S_n-nel. ($|S_n| = n!$)*

A lehetséges jelölésmódok közül a következőt választjuk:

1	2	...	n
$\pi(1)$	$\pi(2)$	...	$\pi(1)$

$\pi\{1, 2, \ldots, n\} \to \{1, 2, \ldots, n\}$ bijekció.

11. Definíció. *Bevezetünk S_n-en egy szorzást, ami nem más, mint a permutációknak, mint leképezéseknek a kompozíciója.*

Vagyis

$$\forall \sigma, \pi \in S_n\text{-re } \sigma\pi \overbrace{=}^{\text{def.}} \sigma \circ \pi, \text{ tehát } \sigma\pi(i) = \sigma(\pi(i)). \tag{12}$$

3. Állítás. *A permutációk csoportot alkotnak a 11. definícióban bevezetett szorzásra nézve.*

Bizonyítás:

Ismét a csoportaxiómákhoz nyúlunk vissza. Az (1),(2),(3) axiómák teljesülését akarjuk belátni. A (12) összefüggéseket használjuk ki sok helyen:

1. Asszociativitás: $\tau(\sigma\pi)(i) = \tau(\sigma\pi(i)) = \tau(\sigma(\pi(i))) = \tau\sigma(\pi(i)) = (\tau\sigma)\pi(i)$
2. Létezik egységeleme, az identitás: $id(i) = i$, vagyis $\forall\pi \in S_n$-re $id\pi(i) = id(\pi(i)) = \pi(i) = \pi(id(i)) = \pi id(i)$
3. Inverz: $\forall\pi \in S_n$-hez $\exists\pi^{-1} \in S_n$ úgy, hogy $\pi^{-1}\pi = \pi\pi^{-1} = id$. Ha $\pi(i) = j \Rightarrow \pi^{-1}(j) = i$. Mivel π bijekció, ez megtehető, és $\pi^{-1}\pi(i) = \pi^{-1}(\pi(i)) = \pi^{-1}(j) = i = id(i)$ és $\pi\pi^{-1}(j) = \pi(\pi^{-1}(j)) = \pi(i) = j = id(j)$

Ezzel beláttuk, hogy az $1, 2, \ldots, n$ számok permutációinak halmaza valóban csoportot alkot a (11.) definícióban bevezetett szorzásra nézve. □

6.2. Inverziószám

12. Definíció. *Az $I(\pi)$ inverziószám azt mondja meg, hogy a π permutációban hány olyan $\langle i, j\rangle$ pár van, amelyre $i < j$ azonban $\pi(i) > \pi(j)$*

4. Tétel. $I(\pi^{-1}) = I(\pi)$

Bizonyítás:

$\forall\pi(i) > \pi(j)$ esetén, $\pi^{-1}(\pi(i)) = i$ és $\pi^{-1}(\pi(j)) = j$, vagyis épp akkor kell növelni $I(\pi^{-1})$-t, ha $i < j$, de ekkor $I(\pi)$-t is növelnünk kell definíció szerint. Vagyis $I(\pi^{-1}) = I(\pi)$. □

13. Definíció. $sgn(\pi) = (-1)^{I(\pi)}$

Az inverziószám néhány tulajdonsága:

1. $I(id) = 0$, $sgn(id) = +1$
2. Általában nem igaz, hogy $I(\sigma\pi) = I(\sigma) + I(\pi)$, de $(mod\ 2)$ igaz.

5. Tétel (Permutációk előjelének szorzástétele). $sgn(\sigma\pi) = sgn(\sigma)sgn(\pi)$

Bizonyítás:

$sgn(\sigma\pi) \underbrace{=}_{13.def.} (-1)^{I(\sigma\pi)}$ 2. tulajdonság alapján, mivel -1 hatványainál csak az számít, hogy a kitevő mod 2 mennyit ad, ezért $= (-1)^{I(\sigma)+I(\pi)} = (-1)^{I(\sigma)}(-1)^{I(\pi)} \underbrace{=}_{13.def.} sgn(\sigma)sgn(\pi)$.

Ezzel a tételt igazoltuk. □

6.3. Determináns

14. Definíció (Determináns). *Egy $A \in T^{n\times n}$ mátrix determinánsa $det(A) \in T$, melyet úgy kapunk, hogy a mátrixból kiveszünk n elemet úgy, hogy minden sorból, és minden oszlopból pontosan egyet vegyünk ki, ezeket összeszorozzuk, és az összes ilyen lehetséges kiválasztásra összegezzük. Képlettel:*

$$\sum_{\pi\in S_n} sgn(\pi)a_{1\pi(1)}a_{2\pi(2)}\dots a_{n\pi(n)}$$

6.3.1. Determinánsok néhány tulajdonsága:

1. Diagonális, alsó- vagy felsőháromszög mátrix determinánsa = a főátlóban lévő elemek szorzata.
2. Ha A valamelyik sorának $\forall$ eleme $0 \Rightarrow det(A)$ is zérus.
3. Ha A egyik s_i sorát λ-val szorozzuk, akkor $det(A') = det(A)\lambda$.
4. A, A' és B mátrixok minden sora megegyezik, kivéve az $i.$, és $B_i = A_i + A'_i \Rightarrow det(B) = det(A) + det(A')$
5. Ha A-nak van két egyenlő sora$\Rightarrow det(A) = 0$.
6. Ha a mátrix egy sorához hozzáadom egy másik sorának λ-szorosát, a determináns nem változik.
7. Ha a mátrix két sorát kicserélem, a determináns a -1-szeresére változik.
8. $det(A^T) = det(A)$

Ezen tulajdonságok viszonylag egyszerűen bizonyíthatóak a definíció, és a permutációknál, illetve az inverziószámnál leírt definíciók, tételek segítségével.

6.3.2. Determinánssal kapcsolatos hasznos tételek

Nézzünk néhány tételt, amelyre a példák megoldása során még sokat fogunk hivatkozni:

6. Tétel. *Egy $A \in T^{n\times n}$ mátrix pontosan akkor invertálható, ha $det(A) \neq 0$.*

7. Tétel. *Ha $det(A) \neq 0$, akkor ${}_i[A^{-1}]_j = \frac{A_{ji}}{det(A)}$.*

Következménye: Ha $A \in \mathbb{Z}^{n\times n}$, és $det(A) = 1$, (vagyis nem 0), akkor $\exists A^{-1}$ és $A^{-1} \in \mathbb{Z}^{n\times n}$

8. Tétel (Determinánsok szorzástétele). *$A, B \in T^{n\times n}$ esetén $det(AB) = det(A)det(B)$.*

6.3.3. Néhány szép feladat

Kezdjük egy egyszerű, középiskolai órán is feladható ismert feladattal:

9. Feladat. *Legyen $S = \{n | n = a^2 + b^2; a, b \in \mathbb{N}\}$. Bizonyítsuk be, hogy S a szorzásra nézve zárt.*

I. Megoldás:

Lássuk, be hogy $\forall a, b, c, d \in \mathbb{N}$ esetén $(a^2 + b^2) \cdot (c^2 + d^2) = A^2 + B^2$, $A, B \in \mathbb{N}$. Vagyis, hogy S bármely két elemét összeszorozva S-beli elemet kapunk.

$$(a^2 + b^2) \cdot (c^2 + d^2) = a^2c^2 + a^2d^2 + b^2c^2 + b^2d^2 =$$

$$= (a^2c^2 + b^2d^2) + (a^2d^2 + b^2c^2) = ((ac)^2 + 2acbd + (bd)^2) + ((ad)^2 - 2adbc + (bc)^2) =$$

$$= (\underbrace{ac + bd}_{A})^2 + (\underbrace{ad - bc}_{B})^2 \ \square$$

Ez egy egészen természetes megoldás. Most nézzünk egy kissé nyakatekertet, ami az előzőnél se nem szebb, se nem frappánsabb, de ha ezen a példán megértjük a későbbiekben még hasznunkra lehet.

II. Megoldás:

Vegyük S-nek egy $n = a^2 + b^2$ ill. egy $m = c^2 + d^2$ elemét. Ekkor ha vesszük

$$N = \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \text{ és } M = \begin{pmatrix} d & c \\ -c & d \end{pmatrix} \text{ mátrixokat,}$$

akkor $det(N) = n$ és $det(M) = m$. Vagyis

$$n \cdot m = det(N) \cdot det(M) =,$$

ami a determinánsok szorzástétele alapján (lásd 8. tétel):

$$= det(N \cdot M) = \begin{vmatrix} ad - bc & ac + bd \\ -bd - ac & ad - bc \end{vmatrix} =$$

A determinánst kifejtve kapjuk, hogy

$$n \cdot m = (ac + bd)^2 + (ad - bc)^2 \ \square$$

Ezzel megkaptuk az előző megoldás eredményét.

Hogy ez a megoldás miért is fontos, azt talán a következő példa szemléltetheti:

10. Feladat. *Bizonyítsuk be, hogy az*

$$S = \{x | \exists a, b, c \in \mathbb{N}; x = a^3 + b^3 + c^3 - 3abc\}$$

halmaz zárt a szorzásra nézve.

Hát ezt a feladatot már igencsak nehéz lenne elemi módszerekkel bizonyítani, és ha sikerülne is, elég hosszadalmas lenne, úgyhogy nézzünk inkább az előző feladat II. megoldásához hasonló, frappánsabb bizonyítást:

Megoldás:

Vegyük S-nek egy $n = a^3 + b^3 + c^3 - 3abc$ ill. egy $m = d^3 + e^3 + f^3 - 3def$ elemét. Ekkor ha vesszük

$$N = \begin{pmatrix} a & b & c \\ c & a & b \\ b & c & a \end{pmatrix} \text{ és } M = \begin{pmatrix} d & e & f \\ f & d & e \\ e & f & d \end{pmatrix} \text{ mátrixokat,}$$

akkor $det(N) = n$ és $det(M) = m$. Vagyis a 8. tétel alapján:

$$n \cdot m = det\left(\begin{pmatrix} a & b & c \\ c & a & b \\ b & c & a \end{pmatrix} \cdot \begin{pmatrix} d & e & f \\ f & d & e \\ e & f & d \end{pmatrix}\right) =$$

$$= \begin{vmatrix} ad+bf+ce & ae+bd+cf & af+be+cd \\ af+be+cd & ad+bf+ce & ae+bd+cf \\ ae+bd+cf & af+be+cd & ad+bf+ce \end{vmatrix}$$

Ami $ad + bf + ce = A; ae + bd + cf = B; af + be + cd = C; A, B, C \in \mathbb{N}$ jelöléssel:

$$= A^3 + B^3 + C^3 - 3ABC \ \square$$

7. Heisenberg-csoport

Vizsgáljuk a $H = \begin{pmatrix} 1 & x & z \\ 0 & 1 & y \\ 0 & 0 & 1 \end{pmatrix}$ alakú mátrixok halmazát, ahol $x, y, z \in \mathbb{Z}$!

7.1. Lássuk be róla, hogy valóban csoport a mátrixszorzásra nézve!

Először is be kell látnunk, hogy zárt a szorzásra nézve, vagyis $\forall A, B \in H$ estén $A \cdot B \in H$. Legyen

$$A = \begin{pmatrix} 1 & x_A & z_A \\ 0 & 1 & y_A \\ 0 & 0 & 1 \end{pmatrix} \text{ és } B = \begin{pmatrix} 1 & x_B & z_B \\ 0 & 1 & y_B \\ 0 & 0 & 1 \end{pmatrix}. \tag{13}$$

Ekkor

$$A \cdot B = \begin{pmatrix} 1 & x_A + x_B & z_A + z_B + x_A \cdot y_B \\ 0 & 1 & y_A + y_B \\ 0 & 0 & 1 \end{pmatrix}, \tag{14}$$

vagyis valóban $A \cdot B \in H$, és $x_{AB} = x_A + x_B \in \mathbb{Z}$; $y_{AB} = y_A + y_B \in \mathbb{Z}$; $z_{AB} = z_A + z_B + x_A \cdot y_B \in \mathbb{Z}$.

Most már csak meg kell vizsgálnunk, hogy az (1),(2),(3) csoportaxiómák teljesülnek-e.

- (1): $A, B, C \in H$ esetén igaz-e, hogy $(A \cdot B)C = A(B \cdot C)$? Mivel a zártságot már beláttuk, elég megvizsgálnunk, hogy a keletkező két mátrix x, y, z elemei megegyeznek-e. A (14) egyenletet felhasználva:
  - $x_{(AB)C} = x_{AB} + x_C = x_A + x_B + x_C = x_A + x_{BC} = x_{A(BC)}$
  - $y_{(AB)C} = y_{AB} + y_C = y_A + y_B + y_C = y_A + y_{BC} = y_{A(BC)}$
  - $z_{(AB)C} = z_{AB} + z_C + x_{AB} \cdot y_C = (z_A + z_B + x_A \cdot y_B) + z_C + x_A \cdot y_C + x_B \cdot y_C = z_A + (z_B + z_C + x_B \cdot y_C) + x_A \cdot (y_B + y_C) = z_A + z_{BC} + x_A \cdot y_{BC} = z_{A(BC)}$
- (2): $\exists$ egységelem, jelöljük I-vel, ez a szokásos egységmátrix lesz, ahol $x_I = y_I = z_I = 0$.
  - $x_{IA} = x_I + x_A = x_A + x_I = x_{AI} = x_A + 0 = x_A$
  - $y_{IA} = y_I + y_A = y_A + y_I = y_{AI} = y_A + 0 = y_A$
  - $z_{IA} = z_I + z_A + \underbrace{\underbrace{x_I}_{0} \cdot y_A}_{0} = z_A + z_I + \underbrace{x_A \cdot \underbrace{y_I}_{0}}_{0} = z_A$
- (3): $\forall A \in H$ esetén $\exists A^{-1}$ úgy, hogy $A \cdot A^{-1} = I$
  - $0 = x_I = x_{AA^{-1}} = x_A + x_{A^{-1}} \Rightarrow$

$$x_{A^{-1}} = -x_A \in \mathbb{Z} \tag{15}$$

  - $0 = y_I = y_{AA^{-1}} = y_A + y_{A^{-1}} \Rightarrow$

$$y_{A^{-1}} = -y_A \in \mathbb{Z} \tag{16}$$

  - $0 = z_I = z_{AA^{-1}} = z_A + z_{A^{-1}} + x_A \cdot y_{A^{-1}} = z_A + z_{A^{-1}} - x_A \cdot y_A \Rightarrow$

$$z_{A^{-1}} = x_A \cdot y_A - z_A \tag{17}$$

Vagyis jogos az elnevezés, a Heisenberg-csoport valóban csoport!

7.2. Keressük a H-csoport egy S generátorát!

Legyen $g_1 = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$ és $g_2 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$. Mutassuk meg, hogy az így előálló $S = \left\{e, g_1, g_2, g_1^{-1}, g_2^{-1}\right\}$ egy generátora H-nak!

Először is számoljuk ki g_1 és g_2 inverzét! Az előbb levezetett (15),(16),(17) egyenlőségek alapján:

$g_1^{-1} = \begin{pmatrix} 1 & -1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$ és $g_2^{-1} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & -1 \\ 0 & 0 & 1 \end{pmatrix}$. $e = I$ a szokásos egységmátrix.

Néhány hasznos megállapítás a konstrukciónkhoz:

1. Tetszőleges $A \in H$ mátrixra $A \cdot g_1 = A' \in H$ ahol $x'_A = x_A + 1$, y,z változatlan.
2. Hasonlóan $A \cdot g_1^{-1} = A' \in H$ ahol $x'_A = x_A - 1$, y,z változatlan.
3. k szerinti teljes indukcióval könnyen belátható, hogy $M = g_2^k, k \in \mathbb{Z}$ esetén $x_M = z_M = 0$ és $y_M = k$.

Ezzel már tetszőleges mátrixot elő tudunk állítani, ahol z=0. Ha találnánk egy N mátrixot, ami S elemeinek szorzatából áll, úgy, hogy $x = y = 0$ és $z = \pm 1$, akkor már z-t is tetszőlegesre tudnánk állítani.
Ez a következő két mátrix:

$N_1 = g_1 g_2 g_1^{-1} g_2^{-1} = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$ és $N_2 = g_1 \cdot g_2^{-1} \cdot g_1^{-1} \cdot g_2 = \begin{pmatrix} 1 & 0 & -1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$.

Tehát egy tetszőleges H-beli mátrixot a következő képpen fogunk előállítani:

- Először g_2 vagy g_2^{-1} egymás után vett szorzatával beállítjuk az előállítani kívánt mátrix y elemét. Ezt „büntetlenül” megtehetjük, mivel a 3. megállapítás szerint, ezzel x, és z értéke nem változik (marad zérus).
- Az így kapott mátrixot N_1 vagy N_2-vel megfelelően sokszor megszorozva be állíthatjuk z értéket is, mivel x még mindig zérus. Így a beállított y érték is megmarad.
- Végül az első két megállapítás alapján, ha az így kapott mátrixot még g_1 vagy g_1^{-1}-nel többször egymás után megszorozzuk, x érteket is beállíthatjuk, anélkül, hogy a már beállított y, z érték megváltozna.

Tehát egy tetszőleges $M \in H$ mátrixot a következő képpen állíthatunk elő:
Ha $z_M < 0$

$$M = (g_2)^{y_M} \cdot (g_1 \cdot g_2^{-1} \cdot g_1^{-1} \cdot g_2)^{-z_M} \cdot (g_1)^{x_M} \tag{18}$$

Ha $z_M > 0$

$$M = (g_2)^{y_M} \cdot (g_1 \cdot g_2 \cdot g_1^{-1} \cdot g_2^{-1})^{-z_M} \cdot (g_1)^{x_M} \tag{19}$$

Ezzel generáltuk S-sel H minden elemét!

8. Kommutátorok

15. Definíció (Kommutátor). *Legyen g_1 és g_2 két tetszőleges eleme G csoportnak. Ekkor g_1 és g_2 kommutátora:* $[g_1, g_2] = g_1 g_2 g_1^{-1} g_2^{-1}$

16. Definíció (Kommutátor általánosan). *N db G-beli elem kommutátara alatt* $[g_1, g_2, \dots g_N] = [[g_1, g_2, \dots g_{N-1}], g_N]$ *kifejezést értjük.*

17. Definíció (k-nilpotens csoport). *G csoportra azt mondjuk, hogy k-nilpotens, ha minden k+1-tagú kommutátora $\forall g_1, g_2, \dots g_k \in G$-re az egységet adja.*

Például a kommutatív csoportok 1-nilpotensek, mivel ekkor

$$g_1 g_2 g_1^{-1} g_2^{-1} = 1 \Rightarrow g_1 g_2 = g_2 g_1$$

9. Tétel. *A Heisenberg csoport egy 2-nilpotens csoport!*

Bizonyítás:

A bizonyítás mindössze abból áll, hogy keresnünk kell egy 3-as kommutátort H-ban, ami épp az egységet adja.

Ez az előző fejezetet végiggondolva már nem nehéz feladat. Néhány érdekes megállapítás az előző fejezethez kapcsolódóan, ami segíthet a bizonyítás menetében:

- Ha jobban megnézzük, N_1 mátrixot úgy definiáltuk, hogy $N_1 = g_1 g_2 g_1^{-1} g_2^{-1}$ ami épp $[g_1, g_2]$.
- Érdemes arra is felfigyelni, hogy N_1 és N_2 épp egymás inverzei.

Vegyük tehát a

$$[g_1, g_2, g_1]$$

kommutátort, amit az előzőek fényében így írhatunk:

$$[[g_1, g_2], g_1] = [N_1, g_1] =$$

$$= N_1 g_1 N_1^{-1} g_1^{-1} = N_1 g_1 N_2 g_1^{-1}$$

Azt pedig tudjuk, hogy az egységmátrixhoz képest N_1 a z értéket növeli eggyel, g_1 az x értéket, N_2 z-t csökkenti, vagyis a z érték így újra zérus, ezután g_1^{-1} pedig az x értéket állítja vissza 0-ra, tehát valóban visszakaptuk az egységmátrixot.

Kifejtve:

$$N_1 g_1 N_2 g_1^{-1} = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & -1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & -1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} =$$

$$\begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & -1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & -1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} =$$

$$\begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & -1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

□

9. Szabad csoportok

Ebben a fejezetben még visszatérünk a Heisenberg-csoporthoz, csak most egy kicsit más megközelítésből, más szemszögből akarjuk vizsgálni, ehhez azonban ismét némi elméleti háttér szükségeltetik.

18. Definíció (Szabad generátorrendszer). *A G csoport egy $g_1, g_2, \ldots, g_n$ generátorrendszere szabad, ha $\forall H$ csoportra, és $h_1, h_2, \ldots, h_n$ elemekre $\exists! \varphi : G \to H$ homomorfizmus úgy, hogy $\forall 1 \leq i \leq n$ esetén $\varphi(g_i) = h_i$.*

19. Definíció (Szabad csoport). *A G csoport szabad, ha van szabad generátorrendszere.*

10. Tétel. *Minden S halmazhoz létezik olyan csoport, amelyet szabadon generál, és ez az izomorfia erejéig egyértelmű.*

Jelölés: A szabadcsoportokat F-el jelöljük. Az S által szabadon generált csoport: $F(S)$.

9.1. Csoportok növekedésének sebessége

Először is meg kell határoznunk mit értünk növekedési sebességnek.

20. Definíció (Növekedési sebesség). *Legyen $\langle G, * \rangle$ egy végtelen csoport, S a generátora. ($\langle S \rangle = G$) Ekkor $S^n = \left\{ g = g_1 * g_2 * \cdots * g_n \middle| g_1, g_2, \ldots, g_n \in S \right\}$ és ennek elemszáma a G csoport növekedésének sebessége.*

Nézzünk néhány példát különböző csoportok növekedési sebességére:

9.1.1. Lineáris

Lineáris növekedésre könnyen mutathatunk egy egészen egyszerű példát:

Nézzük $G = \langle \mathbb{Z}, + \rangle$ csoportot. Vegyük $S = \{-1, 0, 1\}$ generátorát.
Ekkor

$$S^n = \{-n, -n+1, \ldots, n-1, n\}$$

Tehát

$$|S^n| = 2n + 1.$$

9.1.2. Exponenciális

A szabad csoportok ismeretében már erre is találhatunk példát:

Vizsgáljuk F_2 szabad csoportot. Ezt szabadon generálja egy $S = \{a, a^{-1}, b, b^{-1}, e\}$ generátor (e az egységelem).

S^n-ben olyan tag ami pontosan n db S-beli elem szorzataként áll elő, és nem egyszerűsíthető van

$$4 \cdot 3^{n-1},$$

mivel kezdhetem e-n kívül bármelyik másik elemmel, és utána e-n és az előzőleg vett szám inverzén kívül mindig folytathatom bármelyikkel a maradék 3-ból.

De S^n-ben benne van az összes olyan tag is, amelyik $k \leq n$ db S-beli elem szorzataként áll elő, mivel akármennyiszer megszorozhatom még e-vel, hogy épp n tényezős szorzat legyen.
Ezekből a fentiek alapján épp

$$4 \cdot 3^{k-1} \text{ db van.}$$

Továbbá még S^n-be tartozik az egységelem is.

Így összesen:

$$|S^n| = 1 + 4 \cdot \textstyle\sum_{k=1}^{n} 3^{k-1}.$$

9.1.3. Mi a Heisenberg-csoport növekedésének sebessége?

A továbbiakban egy egyszerűbb jelölést fogunk alkalmazni:

$$\begin{pmatrix} 1 & x & z \\ 0 & 1 & y \\ 0 & 0 & 1 \end{pmatrix} = [x, y, z]$$

Mivel már a 7. fejezetben beláttuk, hogy csoport, és valóban csak ez a három paramétere változhat, így elég ezekkel jellemeznünk a mátrixokat.

Ekkor a (14.) egyenlet alapján ezzel a jelöléssel két H-beli mátrix szorzata:

$$[x_A, y_A, z_A] \cdot [x_B, y_B, z_B] = [x_A + x_B, y_A + y_B, z_A + z_B + x_A \cdot y_B] \tag{20}$$

A 7. fejezetben már találtunk egy S generátorát a Heisenberg csoportnak:

$$S = \left\{g_1, g_1^{-1}, g_2, g_2^{-1}, e\right\},$$

ahol

$$g_1 = [1, 0, 0]\,, g_1^{-1} = [-1, 0, 0]\,, g_2 = [0, 1, 0]\,, g_2^{-1} = [0, -1, 0].$$

Bár ennek az S generátornak a felépítése nagyon hasonlít az előző példában tárgyalt F_2 csoportéhoz, mégis érdekes kérdés, hogy vajon itt mekkora a növekedési sebesség, van-e valami zárt alak?

Az 20 egyenlet és a generáló elemek ismeretében egy S^n-beli $[x, y, z]$-ről azt mondhatjuk, hogy x, és y éppen olyan, mint amilyent a lineáris résznél tárgyaltaknál láttunk; generáló elem a $0, -1, 1$ és egyszerűen S hatványaival csak az egész számok közti összeadás a művelet.

Így a következőt mondhatjuk:

$$|x| \leq n, \text{ és } |y| \leq n$$

Továbbá felső becslést adhatunk z-re is, ha feltesszük, hogy x,y-tól független:

$$|z| \leq n^2$$

Természetesen ez csak felső becslés, mert valójában nem független, és nem is jöhet ki minden szám n^2-ig.

Vagyis ebből tudunk S^n elemszámára egy felső becslést adni:

$$|S^n| \leq C \cdot n^4, \text{ ahol C konstans.}$$

Vagyis a Heisenberg-csoport növekedési sebessége polinomiális.

9.1.4. A növekedési sebesség generátortól való függése

Legyen G csoport, S egy generátora, növekedési üteme n^d. Ekkor $\exists c > 0$ rögzített konstans, hogy $|S^n| \leq c \cdot n^d$.

11. Állítás. *Ekkor G növekedési üteme nem függ a generátortól.*

Bizonyítás:

Legyen S_1 G-nek egy másik generátora ($S_1 \subseteq G$). Ekkor $\exists c_1$ rögzített konstans, hogy $|S^n| \leq c_1 \cdot n^d$.

Ekkor $\exists t$ úgy, hogy $S_1 \subseteq S^t$.
Vagyis

$$|S^n| \leq |S^{n \cdot t}| \leq c \cdot n \cdot t^d = \underbrace{c \cdot t^d}_{c_1} \cdot n^d. \ \square$$

10. Vegyes Feladatok

A következő feladat a Kürchák József matematika versenyen 1967-ben volt az első feladat. A feladat és a megoldás is egyszerűnek, és természetesnek mondható, mégis jól rávilágít, milyen nehéz még a középiskolásoknak strúktúrákban, halmazokbeli műveletekkel gondolkodniuk.

11. Feladat. *Egy egész számokból álló halmaz tartalmazza minden elemének kétszeresét és bármely két elemének összegét. A halmaz elemei között van pozitív és negatív is. Bizonyítsuk be, hogy a halmaz bármely két elemének különbsége is a halmazhoz tartozik.*

Megoldás:
A megoldásunk három lépésből fog állni:

1. Belátjuk, hogy ha egy a elem benne van a halmazban, akkor $n \cdot a$ is, $\forall n \in \mathbb{N}$ esetén.

2. Ezután azt is megmutatjuk, hogy ez igaz $\forall n \in \mathbb{Z}$ esetén is.

3. Végül bebizonyítjuk, hogy ezen kívül nem is lehet más eleme a halmaznak.

Ha a fenti három pontot sikerül belátnunk, akkor világos, hogy a megoldással kész vagyunk, mivel, akkor minden a-val osztható szám benne van a halmazban, és csak ezek vannak. Ekkor a halmaz bármely két eleme a-nak többszöröse, vagyis a két elem különbsége is, tehát benne van a halmazban.

Akkor lássuk a bizonyítást! Legyen A a halmazunk.

1. Tegyük fel, hogy $\exists a \neq 0 \in A$. Ekkor $a + a = 2a \in A$. Teljes indukcióval lássuk be, hogy ha $na \in A \Rightarrow (n+1)a \in A$. De $(n+1)a = \underbrace{na}_{\in A} + \underbrace{a}_{\in A} \Rightarrow (n+1)a \in A$!

2. Mivel az egész számokon létezik rendezés, és a halmaznak van pozitív és negatív eleme is, legyen a a legkisebb pozitív eleme a halmaznak, és b a legkisebb abszolútértékű negatív eleme a halmaznak.

Ekkor $a + b$ is $\in A$, de $b < a + b < a$. Vagyis $a + b$ nem lehet negatív, mert akkor nem b lenne a legkisebb abszolútértékű negatív eleme a halmaznak, de nem is pozitív, mert akkor nem a lenne a legkisebb pozitív eleme a halmaznak. Vagyis $a + b = 0$. Vagyis $b = -a$ Ekkor már az előbb belátottak alapján, $n \cdot a \in A$ és $n \cdot b = -n \cdot a \in A$ illetve most láttuk, hogy $0 \in A$, vagyis valóban igaz, hogy ha $a \in A$ akkor $n \cdot a \in A \forall n \in \mathbb{Z}$ esetén is.

3. Indirekt módon tegyük fel, hogy van a halmaznak egy c eleme, ami nem írható fel a többszöröseként, vagyis $c = r \cdot a + q$, $0 < q < a; r \in \mathbb{Z}$. De ekkor $q = c + (-r) \cdot a$ vagyis előáll két A-beli elem összegeként. Tehát q is benne van a halmazban. Vegyük észre, hogy ez ellentmondás, mivel ekkor megint nem a lenne a legkisebb pozitív eleme a halmaznak. Tehát hibás volt a feltevés, nem létezik más eleme a halmaznak.

Ezzel a megoldás elején leírtak alapján be is bizonyítottuk a feladatot. □

International Mathematical Olympiad 1965-as évi 2. feladata:

12. Feladat. *Az*

$$\begin{aligned} a_{11}x_1 + a_{12}x_2 + a_{13}x_3 &= 0 \\ a_{21}x_1 + a_{22}x_2 + a_{23}x_3 &= 0 \\ a_{31}x_1 + a_{32}x_2 + a_{33}x_3 &= 0 \end{aligned}$$

egyenletrendszer együtthatóiról a következőket tudjuk:

a) a_{11}, a_{22}, a_{33} *mindegyike pozitív,*

b) *a többi együttható mind negatív,*

c) *minden egyes egyenletben az együtthatók összege is pozitív.*

Bizonyítsuk be, hogy az egyenletrendszer egyetlen megoldása:

$$x_1 = x_2 = x_3 = 0.$$

I.Megoldás:

Először az egyetemi matematika segítségével megmutatjuk, hogy a feladat bizonyos módszerek ismeretében egyszerűen kezelhető, míg egy középiskolás számára kifejezetten nehéz feladatnak bizonyulhat, ezt fogja bemutatni a II. megoldás.

Az egyenletrendszert felfoghatjuk, egy mátrix-vektor szorzásnak, ahol a_{ij} az A mátrix elemei, és $\underline{x} = (x_1, x_2, x_3)$. Vagyis:

$$A \cdot \underline{x} = 0$$

Ez csak abban az esetben ad más megoldást $\underline{x}$-re a triviális $\underline{x} = 0$-n kívül, ha A-nak sajátértéke a 0.

Pontosan akkor sajátérték a $\lambda = 0$, ha $detA = 0$. Vagyis

$$a_{11}a_{22}a_{33} + a_{12}a_{23}a_{31} + a_{13}a_{21}a_{32} - a_{11}a_{23}a_{32} - a_{13}a_{22}a_{31} - a_{12}a_{21}a_{33} = 0.$$

A feladat c) állítása miatt $a_{ii} > -aij - aik$. Legyen $a_{22} = -a_{21} - a_{23} + l$, ahol $l > 0$. Ekkor a fenti két megállapítást használva:

$$a_{11}a_{22}a_{33} = a_{11}(-a_{21} - a_{23} + l)a_{33} = -a_{11}a_{21}a_{33} - a_{11}a_{23}a_{33} + l \cdot a_{11}a_{33} >$$

$$> (a_{12}a_{21}a_{33} + a_{13}a_{21}a_{33}) + (a_{11}a_{23}a_{31} + a_{11}a_{23}a_{32}) + l \cdot a_{11}a_{33} >$$

$$> a_{12}a_{21}a_{33} + a_{11}a_{23}a_{32}(-a_{13}a_{21}a_{31} - a_{13}a_{21}a_{32}) + (-a_{12}a_{23}a_{31} - a_{13}a_{23}a_{31}) + l \cdot a_{11}a_{33} =$$

$$= a_{12}a_{21}a_{33} + a_{11}a_{23}a_{32} - a_{13}a_{21}a_{32} - a_{12}a_{23}a_{31} + (a_{13}a_{22}a_{31} - l \cdot a_{13}a_{31}) + l \cdot a_{11}a_{33}.$$

Ezt átrendezve kapjuk:

$$det(A) > -l \cdot a_{13}a_{31} + l \cdot a_{11}a_{33} = l \cdot (\underbrace{a_{11}a_{33}}_{>0 \text{ a) miatt}} - \underbrace{a_{13}a_{31}}_{>0 \text{ b) miatt}}).$$

De c) pont miatt meg tudjuk, hogy $|a_{ii}| > |a_{ij}|$, tehát

$$det(A) > l \cdot (\underbrace{a_{11}a_{33} - a_{13}a_{31}}_{>0}) > 0.$$

Így valóban csak a triviális megoldás létezik. □

II.Megoldás:

Ez a megoldás Reiman István-Dobos Sándor: „Nemzetközi Matematikai Diákolimpiák 1959-2003" című könyvéből való, középiskolás szinten könnyen elérhető, ötletes bizonyítás:

„Tegyük fel, hogy az egyenletrendszernek van olyan megoldása, amelyben nem minden $x_i = 0$. Mivel (x_1, x_2, x_3)-mal együtt $(-x_1, -x_2, -x_3)$ is megoldás, feltehetjük, hogy az x_i-k között van pozitív, legyen közülük a legnagyobb pl. x_1. Válasszuk ki az első egyenletet (ha x_i a legnagyobb, az i-edik egyenletet választjuk) és vegyük figyelembe, hogy pl. $x_2 \leq x_1$-ből $a_{12}x_2 \geq a_{12}x_1$ következik:

$$0 = a_{11}x_1 + a_{12}x_2 + a_{13}x_3 \geq a_{11}x_1 + a_{12}x_1 + a_{13}x_1 = (a_{11}a_{12}a_{13})x_1 > 0,$$

ami nyilván ellentmondás, tehát nem lehet 0-tól különböző az x_i-k között."

[6]

A következő feladatot a 20. Vojtěch Jarník International Mathematical Competition keretében adták föl 2010-ben Ostravában. Ez a második kategóriások 3. feladata volt.

13. Feladat. *Legyen $A, B \in \mathbb{Z}^{n\times n}$. Tegyük fel, hogy*

$$A, A + B, A + 2B, \ldots, A + (2n)B$$

invertálhatóak, és az inverzek is $\mathbb{Z}^{n\times n}$-ből valóak. Mutassuk meg, hogy $A + (2n + 1)B$ is invertálható, és az inverze szintén $\mathbb{Z}^{n\times n}$-ből való!

Megoldás:

Legyen $C \in \mathbb{Z}^{n\times n}$ invertálható, és C^{-1} is $\in \mathbb{Z}^{n\times n}$. Ekkor $det(C)$ és $det(C^{-1})$ is egész szám, továbbá

$1 = det(I) = det(CC^{-1}) = det(C)det(C^{-1})$. Ez csak úgy lehet, ha $det(C) = \pm 1$.

Mivel $A, B \in \mathbb{Z}^{n\times n}$ ezért $\forall k \in \mathbb{Z}$ esetén $(A + kB) \in \mathbb{Z}^{n\times n}$. Legyen $C = (A + kB)$.

Ekkor a determinánsát kifejtve k egy polinomját kapjuk, ahol a legmagasabb fokú tag $k^n det(B)$. Azt tudjuk, hogy $k = 0, 1, 2, \ldots, 2n$-re létezik $C^{-1} \in \mathbb{Z}^{n\times n}$ vagyis a fenti gondolatmenet alapján a polinomunk itt ± 1-et vesz fel.
Vagyis legalább $n+1$-szer felveszi ugyanazt az értéket ($+1$ vagy -1-et), ami egy n-edfokú polinomnál csak úgy lehetséges, ha ő a konstans $+1$ vagy -1.

Vagyis $k = 2n + 1$ esetén is $det(A + (2n + 1)B) = \pm 1$, vagyis a kérdéses mátrix invertálható. És a (7.) tétel következménye miatt ez $\in \mathbb{Z}^{n\times n}$. $\square$

Hivatkozások

[1] William Lowell Putnam Mathematics Competition; 1971, 1986/B-6, 1990/A-5, 1991/A-2, 2001/A-1 feladatok

[2] International Mathematical Olympiad (IMO); 1965/2. feladata

[3] International Mathematics Competition for University Students (IMC); 2009/2.

[4] Kürschák József matematika verseny; 1967/1.

[5] Vojtěch Jarník International Mathematical Competition; 2010/II. kategória, 3.feladata

[6] Reiman István-Dobos Sándor: „Nemzetközi Matematikai Diákolimpiák 1959-2003" című könyve (Typotex 2003, Budapest)

[7] Hegyvári Norbert: „Elemi matematika az iskolában" című jegyzete

[8] Kiss Emil: „Bevezetés az algebrába" című könyve (Typotex 2007, Budapest)

Tartalomjegyzék