Algebra és számelmélet előadás

Waldhauser Tamás
2016. november 17.

Nyolcadik házi feladat az előadásra

$\cdot$	e	a	b	x	y	z
e	e					
a		b	e	y		
b						
x		z		e		
y						
z						

$ee = e \implies e$ az egységelem

$ab = e \implies a$ és b egymás inverze $\implies ba = e$

Nyolcadik házi feladat az előadásra

$\cdot$	e	a	b	x	y	z
e	e	a	b	x	y	z
a	a	b	e	y		
b	b	e				
x	x	z		e		
y	y					
z	z					

invertálhatóság/kancellativitás (sudoku):

$ay = z$, $az = x$

$ya = x$, $za = y$

Nyolcadik házi feladat az előadásra

$\cdot$	e	a	b	x	y	z
e	e	a	b	x	y	z
a	a	b	e	y	z	x
b	b	e				
x	x	z		e		
y	y	x				
z	z	y				

asszociativitás:

$bb = (aa)\,b = a\,(ab) = ae = a$
$bx = (aa)\,x = a\,(ax) = ay = z$
$by = (aa)\,y = a\,(ay) = az = x$
$bz = (aa)\,z = a\,(az) = ax = y$

$xb = x\,(aa) = (xa)\,a = za = y$
$yb = y\,(aa) = (ya)\,a = xa = z$
$zb = z\,(aa) = (za)\,a = ya = x$

Nyolcadik házi feladat az előadásra

$\cdot$	e	a	b	x	y	z
e	e	a	b	x	y	z
a	a	b	e	y	z	x
b	b	e	a	z	x	y
x	x	z	y	e		
y	y	x	z			
z	z	y	x			

asszociativitás:

$yz = (ax)(xa) = a(xx)a = aa = b$

$zy = (bx)(xb) = b(xx)b = bb = a$

Nyolcadik házi feladat az előadásra

$\cdot$	e	a	b	x	y	z
e	e	a	b	x	y	z
a	a	b	e	y	z	x
b	b	e	a	z	x	y
x	x	z	y	e		
y	y	x	z			b
z	z	y	x		a	

invertálhatóság/kancellativitás (sudoku):
$xy = b$, $xz = a$
$yx = a$, $zx = b$

Nyolcadik házi feladat az előadásra

$\cdot$	e	a	b	x	y	z
e	e	a	b	x	y	z
a	a	b	e	y	z	x
b	b	e	a	z	x	y
x	x	z	y	e	b	a
y	y	x	z	a		b
z	z	y	x	b	a	

invertálhatóság/kancellativitás (sudoku):
$yy = e$, $zz = e$

Nyolcadik házi feladat az előadásra

$\cdot$	e	a	b	x	y	z
e	e	a	b	x	y	z
a	a	b	e	y	z	x
b	b	e	a	z	x	y
x	x	z	y	e	b	a
y	y	x	z	a	e	b
z	z	y	x	b	a	e

$\cdot$	id	a	a^2	t	at	a^2t
id	id	a	a^2	t	at	a^2t
a	a	a^2	id	at	a^2t	t
a^2	a^2	id	a	a^2t	t	at
t	t	a^2t	at	id	a^2	a
at	at	t	a^2t	a	id	a^2
a^2t	a^2t	at	t	a^2	a	id

Ez a csoport izomorf D_3-mal; a megfelelő izomorfizmus:

$$e \mapsto \mathrm{id} \quad a \mapsto a \quad b \mapsto a^2$$

$$x \mapsto t \quad y \mapsto at \quad z \mapsto a^2t$$

Nyolcadik házi feladat az előadásra

$\cdot$	e	a	b	x	y	z
e	e	a	b	x	y	z
a	a	b	e	y	z	x
b	b	e	a	z	x	y
x	x	z	y	e	b	a
y	y	x	z	a	e	b
z	z	y	x	b	a	e

$\cdot$	id	(123)	(132)	(12)	(23)	(13)
id	id	(123)	(132)	(12)	(23)	(13)
(123)	(123)	(132)	id	(23)	(13)	(12)
(132)	(132)	id	(123)	(13)	(12)	(23)
(12)	(12)	(13)	(23)	id	(132)	(123)
(23)	(23)	(12)	(13)	(123)	id	(132)
(13)	(13)	(23)	(12)	(132)	(123)	id

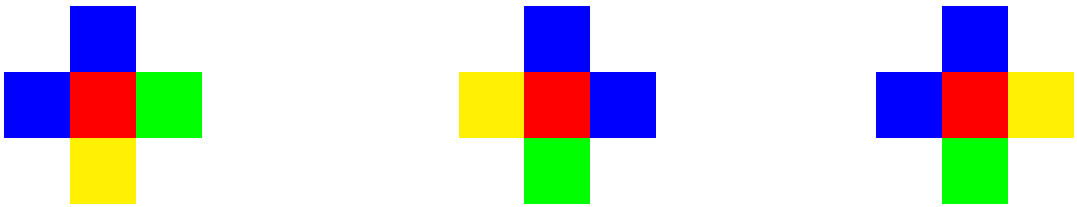
Ez a csoport izomorf S_3-mal; a megfelelő izomorfizmus:

$$e \mapsto \mathrm{id} \qquad a \mapsto (123) \qquad b \mapsto (132)$$

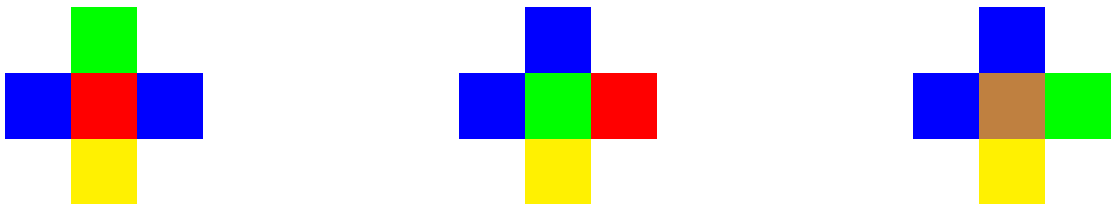
$$x \mapsto (12) \qquad y \mapsto (23) \qquad z \mapsto (13)$$

Tizedik házi feladat az előadásra

Hányféleképpen lehet kiszínezni az X-pentominót n színnel, ha a forgatással vagy tükrözéssel egymásba vihető színezéseket nem tekintjük különbözőnek? (Lehet $n > 5$ is, mert nem kötelező az összes színt felhasználni.) Például az alábbi három színezés egyformának számít



de a következő színezések már különböznek a fentiektől (és egymástól is):



- beküldendő emailben: `twaldha@math.u-szeged.hu`
- pdf fájl legyen (lehet szkennelt is)
- fájlnév: `EHA-eahf10.pdf` (például `WATHAAS-eahf10.pdf`)
- határidő: november 30, reggel 8 óra

Primitív egységgyökök

4.38. Definíció.

A $\mathbb{C}^*$ csoport véges rendű elemei éppen az egységgyökök. Ha $\varepsilon \in \mathbb{C}^*$ rendje n, akkor azt mondjuk, hogy ε *primitív n-edik egységgyök*

4.39. Tétel.

Egy $\varepsilon \in E_n$ egységgyök pontosan akkor primitív n-edik egységgyök, ha hatványaiként megkapható az összes n-edik egységgyök, azaz $[\varepsilon] = E_n$.

Bizonyítás.

Legyen ε egy tetszőleges n-edik egységgyök; ekkor nyilván $[\varepsilon] \subseteq E_n$.
Mivel $[\varepsilon]$ elemszáma éppen ε rendje, világos, hogy

- $o(\varepsilon) = n \implies [\varepsilon] = E_n$, és
- $o(\varepsilon) < n \implies [\varepsilon] \subset E_n$.

□

Primitív egységgyökök

4.40. Tétel.

Az $\varepsilon_k = \operatorname{cis}\frac{2k\pi}{n} \in E_n$ egységgyök akkor és csak akkor primitív n-edik egységgyök, ha k relatív prím n-hez.

Bizonyítás.

Mivel $\varepsilon_k = \varepsilon_1^k$ és nyilván $o(\varepsilon_1) = n$, a 4.33. Állítás alapján

$$o(\varepsilon_k) = o(\varepsilon_1^k) = \frac{n}{\operatorname{lnko}(k, n)}.$$

Tehát $o(\varepsilon_k) = n$ akkor és csak akkor, ha $\operatorname{lnko}(k, n) = 1$. □

5.1. Definíció.

Tetszőleges n természetes szám esetén legyen

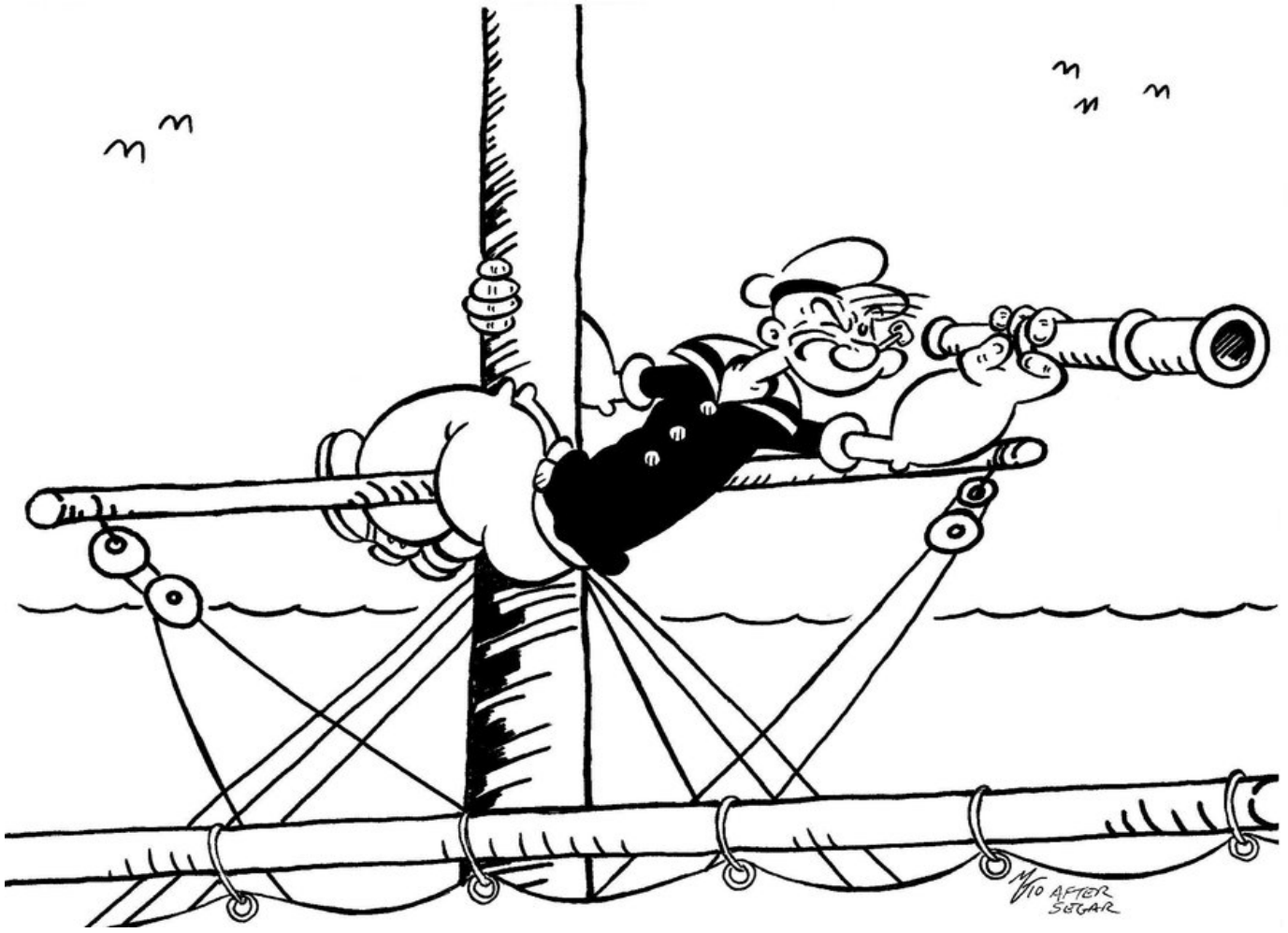
$$\varphi(n) = |\mathbb{Z}_n^*| = |\{a \in \mathbb{N} : 1 \leq a \leq n \text{ és } a \perp n\}|.$$

Az így definiált $\varphi\colon \mathbb{N} \to \mathbb{N}$ függvényt *Euler-féle φ függvénynek* nevezzük.

4.41. Következmény.

A primitív n-edik egységgyökök száma $\varphi(n)$.

Kitekintés: körosztási polinomok



Körosztási polinomok

Az a polinom, amelynek gyökei éppen az n-edik egységgyökök, nyilván

$$x^n - 1 = \prod_{\varepsilon \in E_n} (x - \varepsilon) = \prod_{k=1,\ldots,n} (x - \varepsilon_k)\,.$$

Definíció.

Az n-edik körosztási polinom az a Φ_n polinom, amelynek gyökei éppen a primitív n-edik egységgyökök:

$$\Phi_n = \prod_{\substack{k=1,\ldots,n \\ k \perp n}} (x - \varepsilon_k)\,.$$

Vegyük észre, hogy $\deg \Phi_n = \varphi(n)$.

Körosztási polinomok

- $\Phi_1 = x - 1$
- $\Phi_2 = x - (-1) = x + 1$
- $\Phi_3 = \left(x - \operatorname{cis}\frac{2\pi}{3}\right)\left(x - \operatorname{cis}\frac{4\pi}{3}\right) = \frac{x^3-1}{x-1} = x^2 + x + 1$
- $\Phi_4 = (x - i)(x + i) = \frac{x^4-1}{(x-1)(x+1)} = x^2 + 1$
- $\Phi_5 = \frac{x^5-1}{x-1} = x^4 + x^3 + x^2 + x + 1$
- $\Phi_6 = \frac{x^6-1}{\Phi_1\Phi_2\Phi_3} = \frac{x^6-1}{x^4+x^3-x-1} = x^2 - x + 1$
- $\Phi_7 = \frac{x^7-1}{\Phi_1} = \frac{x^7-1}{x-1} = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$
- $\Phi_8 = \frac{x^8-1}{\Phi_1\Phi_2\Phi_4} = \frac{x^8-1}{x^4-1} = x^4 + 1$
- $\ldots$
- $\Phi_{105} = x^{48} + x^{47} + x^{46} - x^{43} - x^{42} - 2x^{41} - x^{40} - x^{39} + x^{36} + x^{35} + x^{34} + x^{33} + x^{32} + x^{31} - x^{28} - x^{26} - x^{24} - x^{22} - x^{20} + x^{17} + x^{16} + x^{15} + x^{14} + x^{13} + x^{12} - x^9 - x^8 - 2x^7 - x^6 - x^5 + x^2 + x + 1$

Körosztási polinomok

Tétel.
Minden n természetes számra

$$\Phi_n = \frac{x^n - 1}{\prod\limits_{\substack{d \mid n \\ d < n}} \Phi_d}.$$

Következmény.
A körosztási polinomok egész együtthatósak.

Körosztási polinomok

Tétel.

A körosztási polinomok irreducibilisek $\mathbb{Q}$ felett.

Bizonyítás.

Nehéz. Ha p prím, akkor $\Phi_p = \frac{x^p-1}{x-1} = x^{p-1} + x^{p-2} + \cdots + x + 1$. Vezessük be az $y = x - 1$ új határozatlant; ekkor a polinom így alakul:

$$\begin{aligned}\Phi_p(y+1) &= \frac{(y+1)^p - 1}{(y+1) - 1} \\ &= \frac{y^p + py^{p-1} + \binom{p}{2}y^{p-2} + \cdots + \binom{p}{p-2}y^2 + py + 1 - 1}{y} \\ &= y^{p-1} + py^{p-2} + \binom{p}{2}y^{p-3} + \cdots + \binom{p}{p-2}y + p.\end{aligned}$$

Erre a polinomra pedig már alkalmazható a Schönemann–Eisenstein-féle irreducibilitási kritérium. □

Házi feladat a gyakorlatra

31. feladat. Adjon meg a megadott csoportban n-edrendű elemet, amennyiben lehetséges.

(a) $(\mathbb{C}^*, \cdot)$, $n = 12$; $(\mathbb{Z}_8^*, \cdot)$, $n = 5$; D_6, $n = 3$

pl. $\operatorname{cis}\frac{\pi}{6} \in \mathbb{C}^*$ rendje 12,

$\mathbb{Z}_8^*$-ban nincs ötödrendű elem,

pl. $a^2 \in D_6$ rendje 3

(b) S_6, $n = 6$

pl. (123456) vagy $(12)(345)$ vagy ...

(c) S_3, $n = 4$

(d) D_8, $n = 4$

(e) $\mathbb{Z}_{12}$, $n = 3$

Részcsoportok, generálás

Részcsoportok

4.42. Definíció.

Legyen $\mathbb{A} = (A; *)$ egy grupoid, és $B \subseteq A$. Azt mondjuk, hogy a B halmaz *zárt* a $*$ műveletre, ha

$$\forall b_1, b_2 \in B: \ b_1 * b_2 \in B.$$

Ha B nemüres zárt halmaz, akkor B grupoidot alkot a $*$ művelettel (pontosabban annak B-re való megszorításával). Az ilyen $\mathbb{B} = (B; *)$ grupoidot $\mathbb{A}$ *részgrupoidjának* nevezzük. Jelölés: $\mathbb{B} \leq \mathbb{A}$.

4.43. Definíció.

Ha $(G; \cdot)$ csoport, $\emptyset \neq H \subseteq G$, és a $(H; \cdot)$ részgrupoid maga is csoport, akkor azt mondjuk, hogy $(H; \cdot)$ *részcsoportja* $(G; \cdot)$-nek. Jelölés: $H \leq G$.

4.44. Állítás.

Tetszőleges G csoport és $\emptyset \neq H \subseteq G$ esetén H akkor és csak akkor részcsoportja G-nek, ha

(0) H zárt a szorzásra: $\forall h_1, h_2 \in H: \ h_1 \cdot h_2 \in H$;

(2) H tartalmazza G egységelemét: $1_G \in H$;

(3) H zárt az inverzképzésre: $\forall h \in H: \ h^{-1} \in H$.

Házi feladat a gyakorlatra

32. feladat. Döntse el, hogy a G csoportban részcsoportot alkot-e a megadott H részhalmaz.

(a) $G = S_4,\ H = \{\mathrm{id}, (13), (24), (13)(24)\}$ igen;
$G = D_6,\ H = \{\mathrm{id}, t, a^2, a^2 t\}$ nem

(b) $G = (\mathbb{C}^*, \cdot),\ H = (\{z \in \mathbb{C} : |z| = 1\}, \cdot)$
igen

(c) $G = (\mathbb{Z}, +),\ H = \mathbb{N}$

(d) $G = S_5,\ H = \{\mathrm{id}, (135), (153)\}$

(e) $G = (\mathbb{Z}_6, +),\ H = \mathbb{Z}_6^*$

Házi feladat a gyakorlatra

33. feladat. Döntse el, hogy igazak-e az alábbi állítások. A választ minden esetben indokolni kell!

(a) Minden páratlan rendű permutáció páros.

Igen, mert csupa ptl. hosszú ciklusból áll.

(b) Az S_4 csoportban pontosan 6 másodrendű elem van.

Nem, mert 9 van.

(c) Tetszőleges G csoport minden H, K részcsoportjára $H \cup K \leq G$.

(d) Minden páros permutáció rendje ~~páros~~ páratlan.

(e) Tetszőleges csoport tetszőleges a, b, x, y elemeire $axb = ayb \implies x = y$.

Részcsoportok metszete

4.45. Tétel.

Részcsoportok metszete is részcsoport: ha H_1 és H_2 részcsoportjai a G csoportnak, akkor $H_1 \cap H_2$ is részcsoport.

Bizonyítás.

Tfh. H_1 és H_2 részcsoportja G-nek.

(0) $H_1 \cap H_2$ zárt a szorzásra: Ha $h_1, h_2 \in H_1 \cap H_2$, akkor
$h_1 \cdot h_2 \in H_1$ (mert H_1 rcsop.) és $h_1 \cdot h_2 \in H_2$ (mert H_2 rcsop.).
Tehát $h_1 \cdot h_2 \in H_1 \cap H_2$.

(2) $H_1 \cap H_2$ tartalmazza G egységelemét:
$1_G \in H_1$ (mert H_1 rcsop.) és $1_G \in H_2$ (mert H_2 rcsop.).
Tehát $1_G \in H_1 \cap H_2$.

(3) $H_1 \cap H_2$ zárt az inverzképzésre: Ha $h \in H_1 \cap H_2$, akkor
$h^{-1} \in H_1$ (mert H_1 rcsop.) és $h^{-1} \in H_2$ (mert H_2 rcsop.).
Tehát $h^{-1} \in H_1 \cap H_2$. □

4.46. Megjegyzés.

A tétel nem csak kettő, hanem több részcsoportra is érvényes (végtelen sokra is!).

Generálás

4.47. Definíció.

Legyen G egy csoport, és $B \subseteq G$. A B halmaz által *generált részcsoport* a *legszűkebb* olyan részcsoport, ami tartalmazza B-t:

$$[B] = \bigcap_{B \subseteq H \leq G} H.$$

4.48. Megjegyzés.

Az üres halmaz generátuma a legszűkebb részcsoport: $[\emptyset] = \{1_G\}$.

4.49. Definíció.

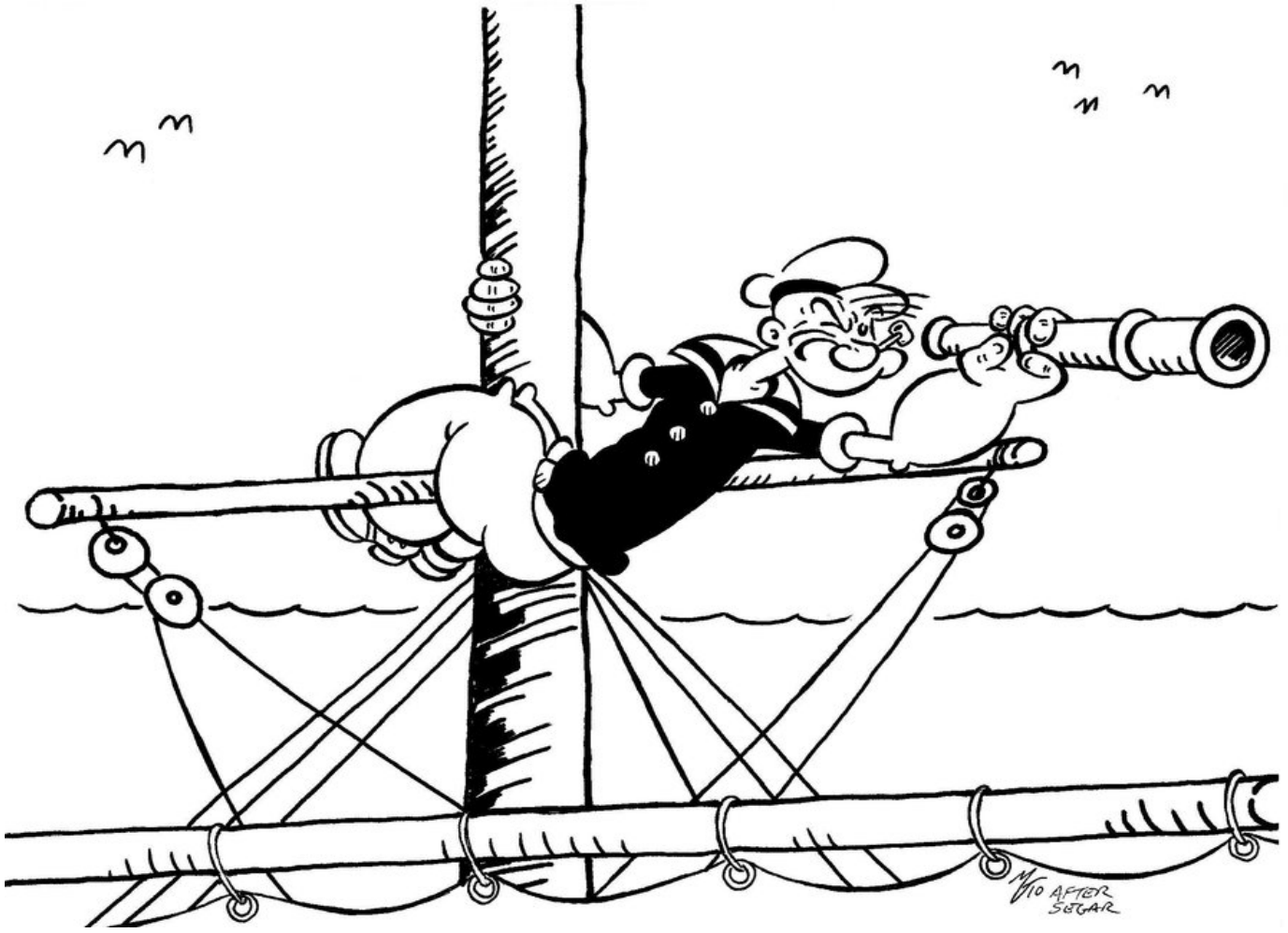
Ha $[B] = G$, akkor azt mondjuk, hogy B *generátorrendszere* a G csoportnak.

4.50. Állítás.

A G csoportban a $B \subseteq G$ részhalmaz által generált részcsoport azokból az elemekből áll, amelyek megkaphatók B elemeiből (és az egységelemből) szorzás és inverzképzés véges számú alkalmazásával:

$$[B] = \left\{ b_1^{\varepsilon_1} \cdots b_n^{\varepsilon_n} : n \in \mathbb{N}_0, b_1, \ldots, b_n \in B, \varepsilon_1, \ldots, \varepsilon_n = \pm 1 \right\}.$$

Kitekintés: permutációs játékok

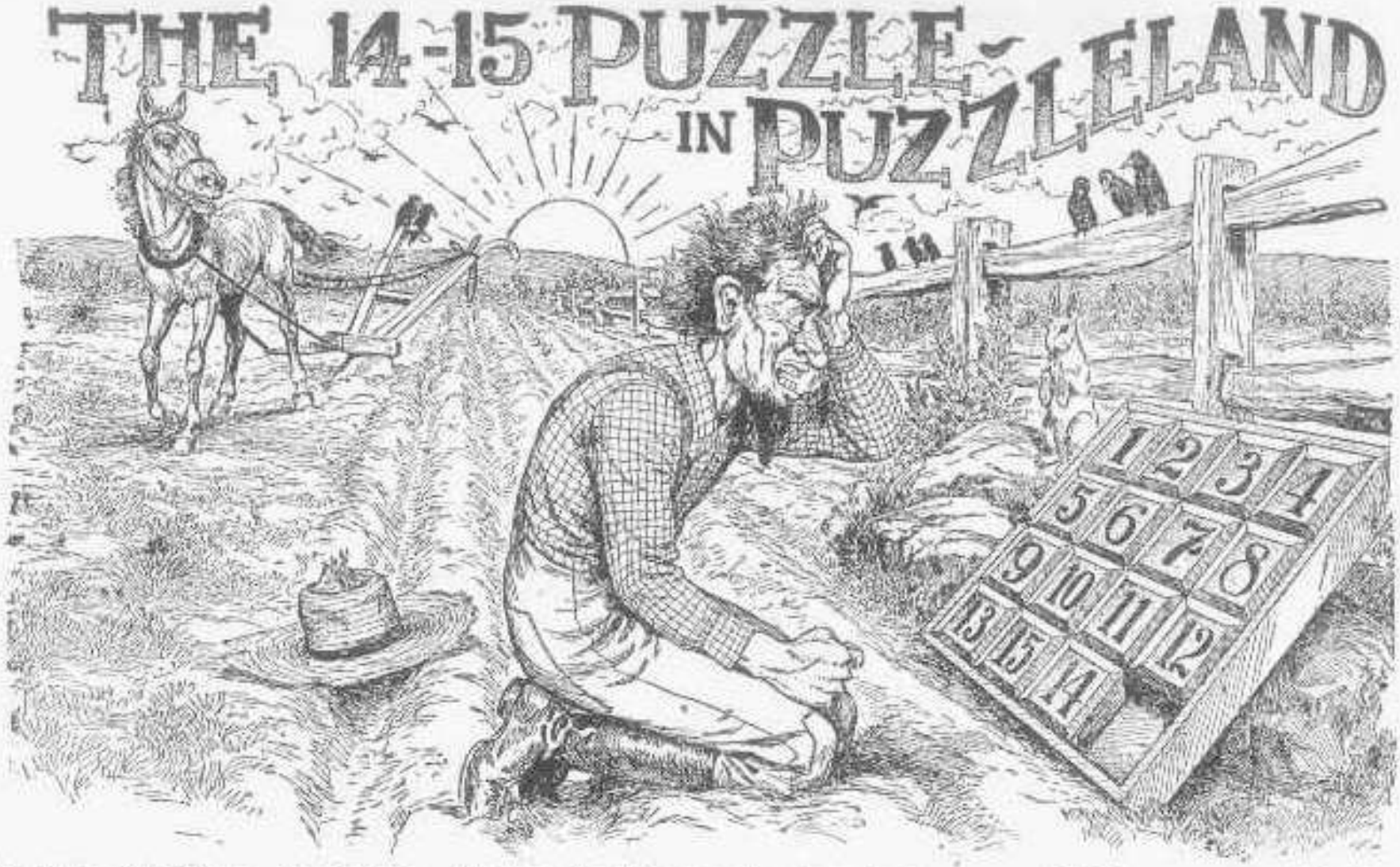


Tizenötös játék

Tizenötös játék

Samuel Loyd (1841-1911)

Tizenötös játék



The older inhabitants of Puzzleland will remember how in the early seventies I drove the entire world crazy over a little box of movable blocks which became known as the

he went for his noon lunch and was discovered by his frantic staff long past midnight pushing little pieces of pie around on a plate! Farmers are known to have deserted their plows

Fig 2.

	1	2	3
4	5	6	7

Fig 3.

1	2	3	4
5	6	7	8

Tizenötös játék

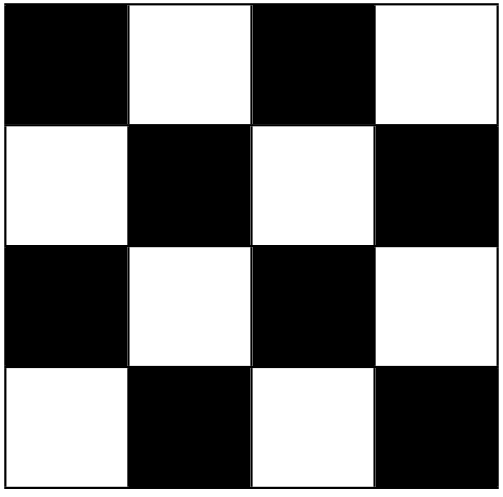
14	13	5	12
2	3	15	4
8		11	9
10	1	7	6

14	13	5	12
2		15	4
8	3	11	9
10	1	7	6

14 13 5 12 2 3 15 4 8 □ 11 9 10 1 7 6

14 13 5 12 2 □ 15 4 8 3 11 9 10 1 7 6

Tizenötös játék



Ha az üres hely visszakerült a jobb alsó sarokba, akkor páros számú csere történt, tehát a 15 számozott lap páros permutációit kaphatjuk csak meg így.

Tizenötös játék

16 kis négyzet:

$$16! = 20\,922\,789\,888\,000 \text{ permutáció}$$

párosság miatt csak a fele lehetséges:

$$\frac{16!}{2} = \underline{10\,461\,394\,944\,000} \text{ lehetőség}$$

$2 \times 2 \times 2$-es bűvös kocka

8 kis kocka:

$$8! = 40\,320 \text{ permutáció}$$

egy kis kocka 3-féleképpen állhat:

$$3 \cdot 3 \cdot 3 \cdot 3 \cdot 3 \cdot 3 \cdot 3 \cdot 3 = 3^8 = 6561 \text{ orientáció}$$

az utolsó kis kocka állása kötött:

$$8! \cdot 3^7 = \underline{88\,179\,840} \text{ lehetőség}$$

$3 \times 3 \times 3$-as bűvös kocka

8 sarokkocka:

$$8! = 40\,320 \text{ permutáció}, \qquad 3^8 = 6561 \text{ orientáció}$$

12 élkocka:

$$12! = 479\,001\,600 \text{ permutáció}, \qquad 2^{12} = 4096 \text{ orientáció}$$

párosság, utolsó sarok-, ill. élkocka:

$$\frac{8! \cdot 12!}{2} \cdot 3^7 \cdot 2^{11} = \underline{43\,252\,003\,274\,489\,856\,000} \text{ lehetőség}$$

Permutációs játékok

Ezekben a permutációs játékokban egy adott π permutációból kell eljutnunk az identikus permutációhoz bizonyos megengedett λ_i $(i \in I)$ lépések segítségével:

$$\pi \cdot \lambda_{i_1} \dots \lambda_{i_k} = \mathrm{id}\,.$$

Ez az egyenlőség ekvivalens azzal, hogy

$$\pi = \lambda_{i_k}^{-1} \dots \lambda_{i_1}^{-1},$$

tehát a feladat (játék) úgy is megfogalmazható, hogy a π permutációt kell kifejeznünk a λ_i permutációk segítségével.

A játékszer tehát gyakorlatilag egy $G = [\{\lambda_i : i \in I\}]$ csoport, és a játék abból áll, hogy egy $\pi \in G$ elemet próbálunk előállítani a λ_i generátorelemekből.

A (több, mint 43 trillió elemű) Rubik-csoportot hat elemmel generáljuk. A csoport minden eleme megkapható legfeljebb 20 lépésben.