Algebra és számelmélet előadás

Waldhauser Tamás
2016. november 10.

Egységgyökök

4.12. Példa.

A komplex egységgyökök csoportot alkotnak a szorzás műveletével; ezen belül az n-edik egységgyökök egy E_n részcsoportot alkotnak minden $n \geq 2$ egész számra. Az E_n csoport izomorf a $\mathbb{Z}_n$ csoporttal: $(E_n; \cdot) \cong (\mathbb{Z}_n; +)$.

Bizonyítás.

Informálisan: Minden n-edik egységgyök előáll $\operatorname{cis} \frac{2k\pi}{n}$ alakban, ahol a k paraméter csak modulo n „számít". Amikor két ilyen számot összeszorzunk, akkor a megfelelő k paramétereket össze kell adni. Formálisan:

A $\varphi\colon \mathbb{Z}_n \to E_n$, $\overline{k} \mapsto \operatorname{cis} \frac{2k\pi}{n}$ leképezés izomorfizmus, mert ...

- φ jóldefiniált: $\overline{k} = \overline{\ell} \implies \operatorname{cis} \frac{2k\pi}{n} = \operatorname{cis} \frac{2\ell\pi}{n}$
- φ injektív: $\operatorname{cis} \frac{2k\pi}{n} = \operatorname{cis} \frac{2\ell\pi}{n} \implies \overline{k} = \overline{\ell}$
- φ szürjektív: $\forall z \in E_n \; \exists k \in \mathbb{Z}\colon z = \operatorname{cis} \frac{2k\pi}{n}$
- φ felcserélhető a műveketekkel:

$$\left(\overline{k} + \overline{\ell}\right)\varphi = \overline{k + \ell}\varphi = \operatorname{cis} \frac{2\left(k + \ell\right)\pi}{n} = \operatorname{cis} \frac{2k\pi}{n} \cdot \operatorname{cis} \frac{2\ell\pi}{n} = \overline{k}\varphi \cdot \overline{\ell}\varphi$$

□

Kvaterniócsoport

Példa.

A $\{\pm 1, \pm i, \pm j, \pm k\}$ halmaz csoportot alkot az alábbi szorzással. Ezt a csoportot *kvaterniócsoportnak* nevezzük, és Q-val jelöljük.

$\cdot$	1	-1	i	$-i$	j	$-j$	k	$-k$
1	1	-1	i	$-i$	j	$-j$	k	$-k$
-1	-1	1	$-i$	i	$-j$	j	$-k$	k
i	i	$-i$	-1	1	k	$-k$	$-j$	j
$-i$	$-i$	i	1	-1	$-k$	k	j	$-j$
j	j	$-j$	$-k$	k	-1	1	i	$-i$
$-j$	$-j$	j	k	$-k$	1	-1	$-i$	i
k	k	$-k$	j	$-j$	$-i$	i	-1	1
$-k$	$-k$	k	$-j$	j	i	$-i$	1	-1

Megjegyzés.

A táblázatból elég az $ij = k = -ji$, $jk = i = -kj$, $ki = j = -ik$ és $i^2 = j^2 = k^2 = -1$ szorzatokat megjegyezni, a többi már magától értetődő.

Az $a + bi + cj + dk$ $(a, b, c, d \in \mathbb{R})$ alakú kifejezéseken természetes módon lehet definiálni az összeadás és szorzás műveletét, így kapjuk a kvaterniók ferdetestét („majdnem" test, csak éppen a szorzás nem kommutatív).

Permutációk

4.13. Példa.

Egy tetszőleges nemüres A halmaz összes transzformációi monoidot alkotnak a leképezésszorzás műveletével, a bijektív transzformációk (azaz permutációk) pedig csoportot alkotnak. Ez utóbbit nevezzük az A feletti *szimmetrikus csoportnak* (jelölés: S_A, illetve $A = \{1, 2, \ldots, n\}$ esetén S_n).

4.14. Példa.

Az S_4 csoportban a $V = \{\mathrm{id}, (12)(34), (13)(24), (14)(23)\}$ részcsoportot *Klein-féle csoportnak* nevezzük.

Szimmetriák

4.15. Példa.

A sík összes egybevágósági transzformációi csoportot alkotnak a leképezésszorzás műveletével, egy adott síkidomot önmagába képező egybevágóságok pedig részcsoportot alkotnak ebben a csoportban (a síkidom *szimmetriacsoportja*).

Megjegyzés.

A szimmetriacsoportot természetesen három- (vagy magasabb) dimenziós térbeli alakzatokra is értelmezhetjük. Ha csak az irányítástartó egybevágóságokat engedjük meg, akkor *mozgáscsoportról* beszélünk (ez részcsoportja a szimmetriacsoportnak).

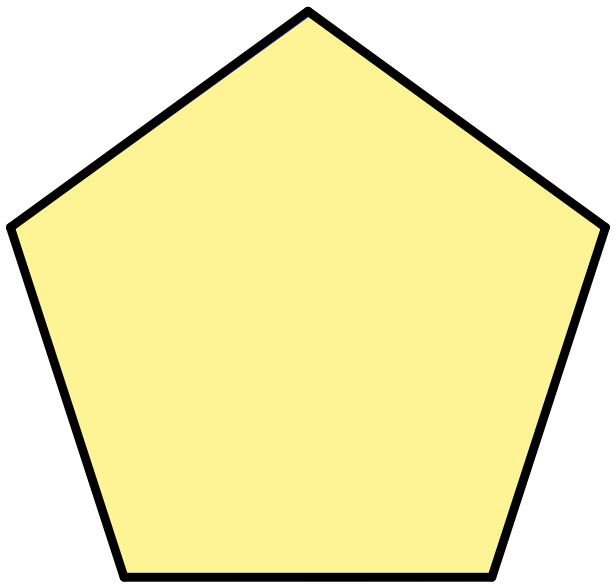
Példa.

Huszonnégy olyan térbeli forgatás van, ami egy adott kockát önmagába visz, és ezek csoportja (azaz a kocka mozgáscsoportja) izomorf S_4-gyel.
`http://demonstrations.wolfram.com/CubicSymmetryTypes`

4.16. Definíció.

A szabályos n-szög szimmetriacsoportját *n-edfokú diédercsoportnak* nevezzük és D_n-nel jelöljük.

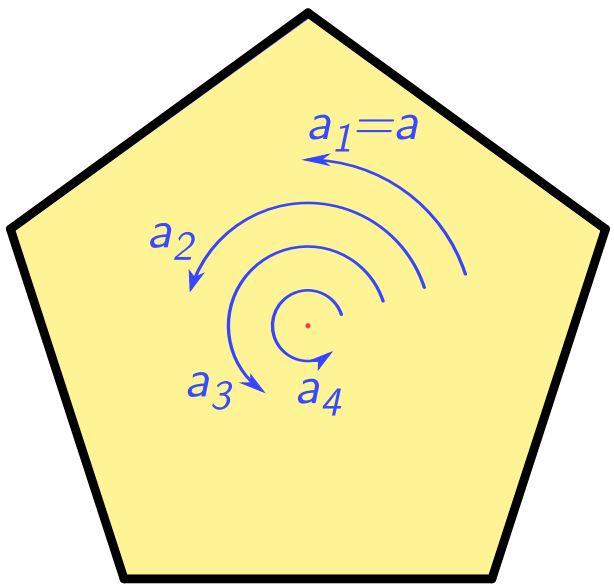
A diédercsoport elemei



A szabályos n-szög szimmetriacsoportja a középpont körüli forgatásokat és a szimmetriatengelyekre való tükrözéseket tartalmaz.

Forgatások

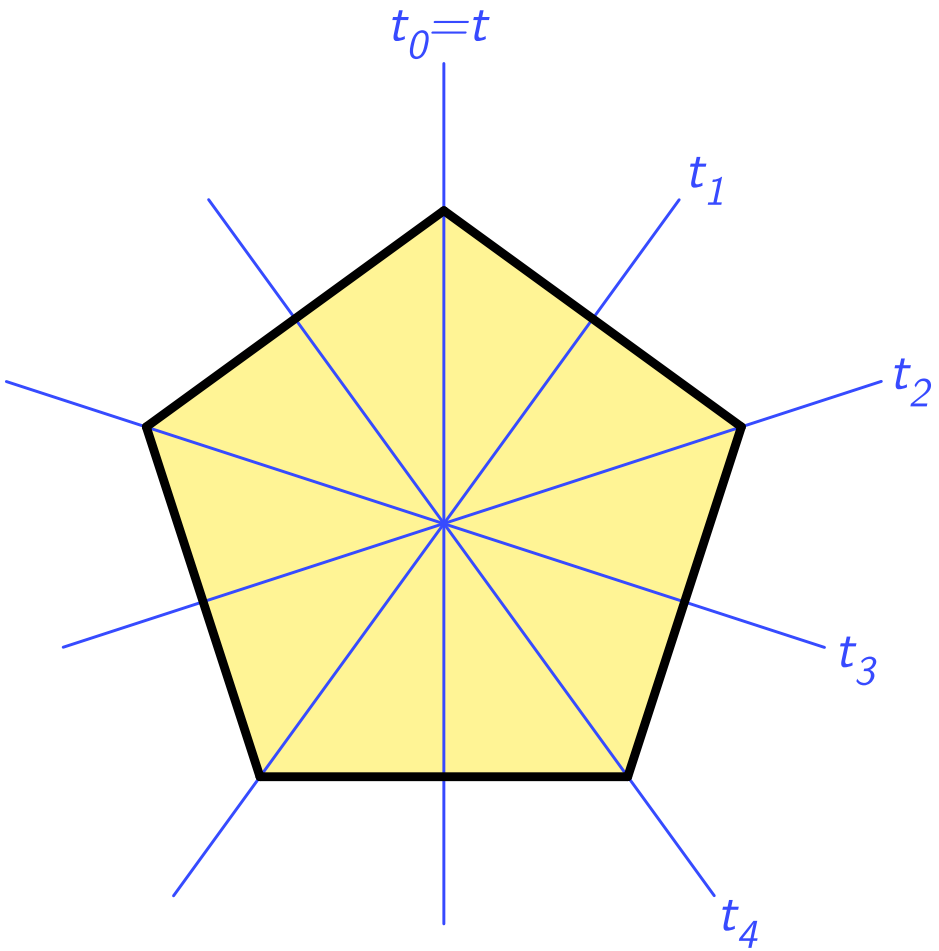
Jelölje a_k a sokszög középpontja körüli $\frac{2k\pi}{n}$ szögű forgatást $(k = 0, 1, \ldots, n-1)$:



Vegyük észre, hogy $a_k = a_1^k$. A továbbiakban a_1 helyett egyszerűen csak a-t írunk. Így az n-szög mozgáscsoportja: $\{\mathrm{id}, a, a^2, \ldots, a^{n-1}\} \cong \mathbb{Z}_n$.

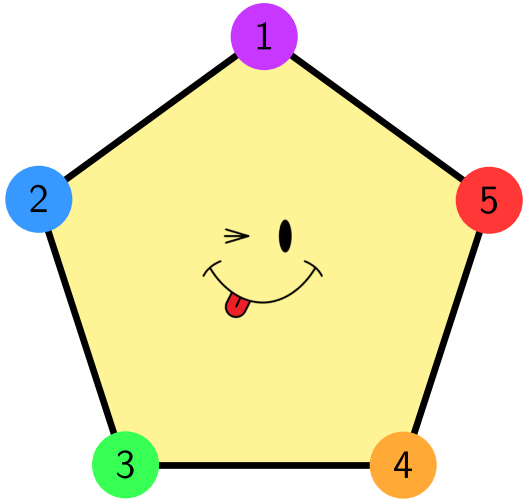
Tükrözések

Legyenek a szimmetriatengelyekre való tükrözések $t_0, t_1, \ldots, t_{n-1}$:

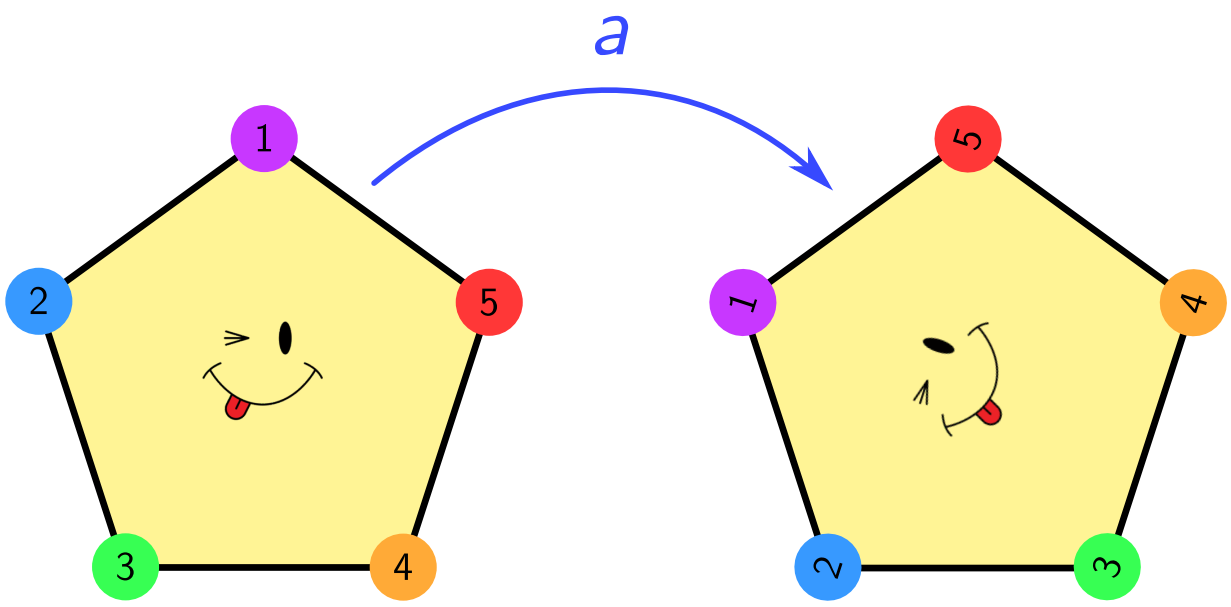


A továbbiakban t_0 helyett egyszerűen csak t-t írunk, és szeretnénk a többi tükrözést is t és a segítségével kifejezni.

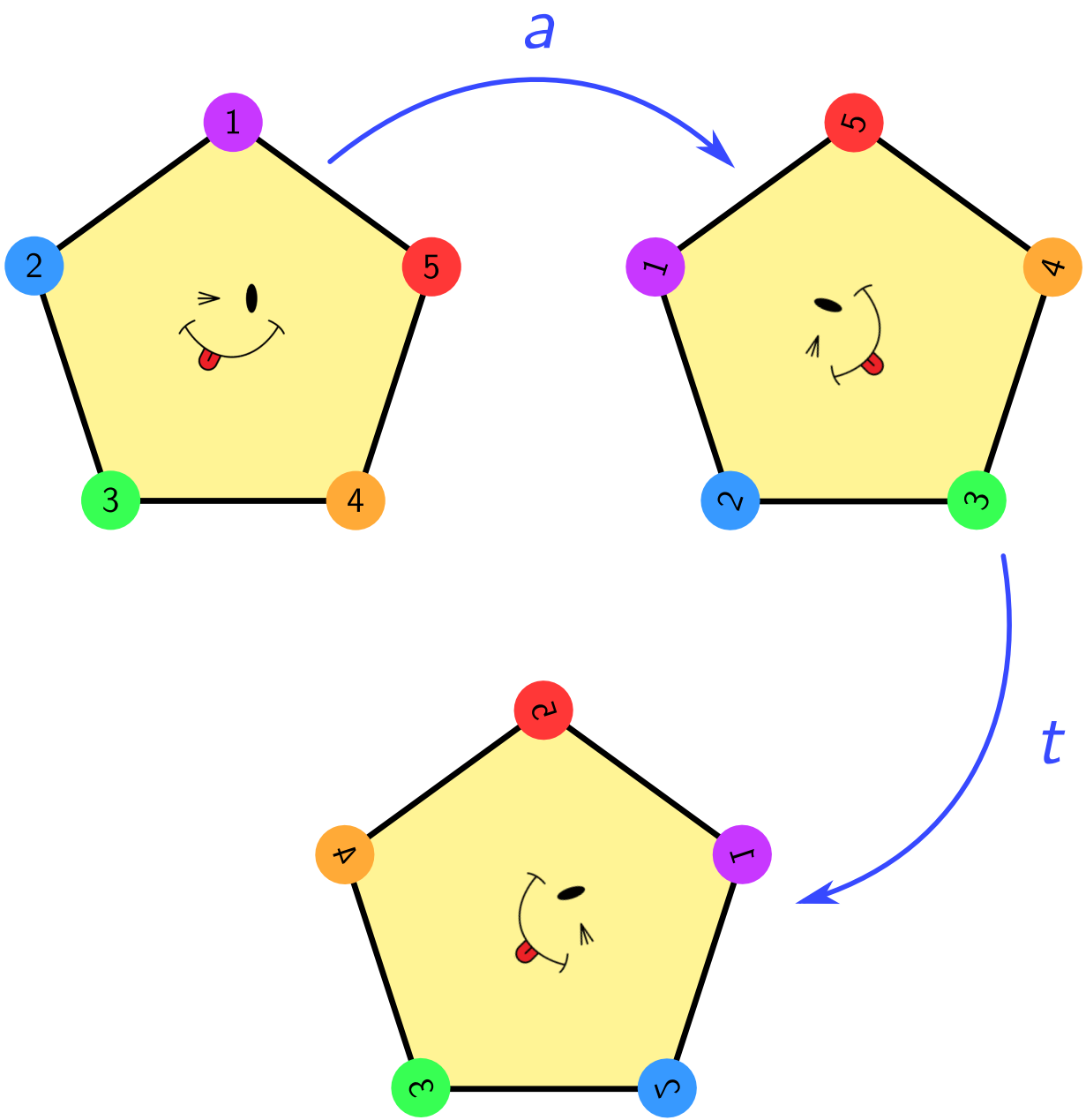
$at = ?$



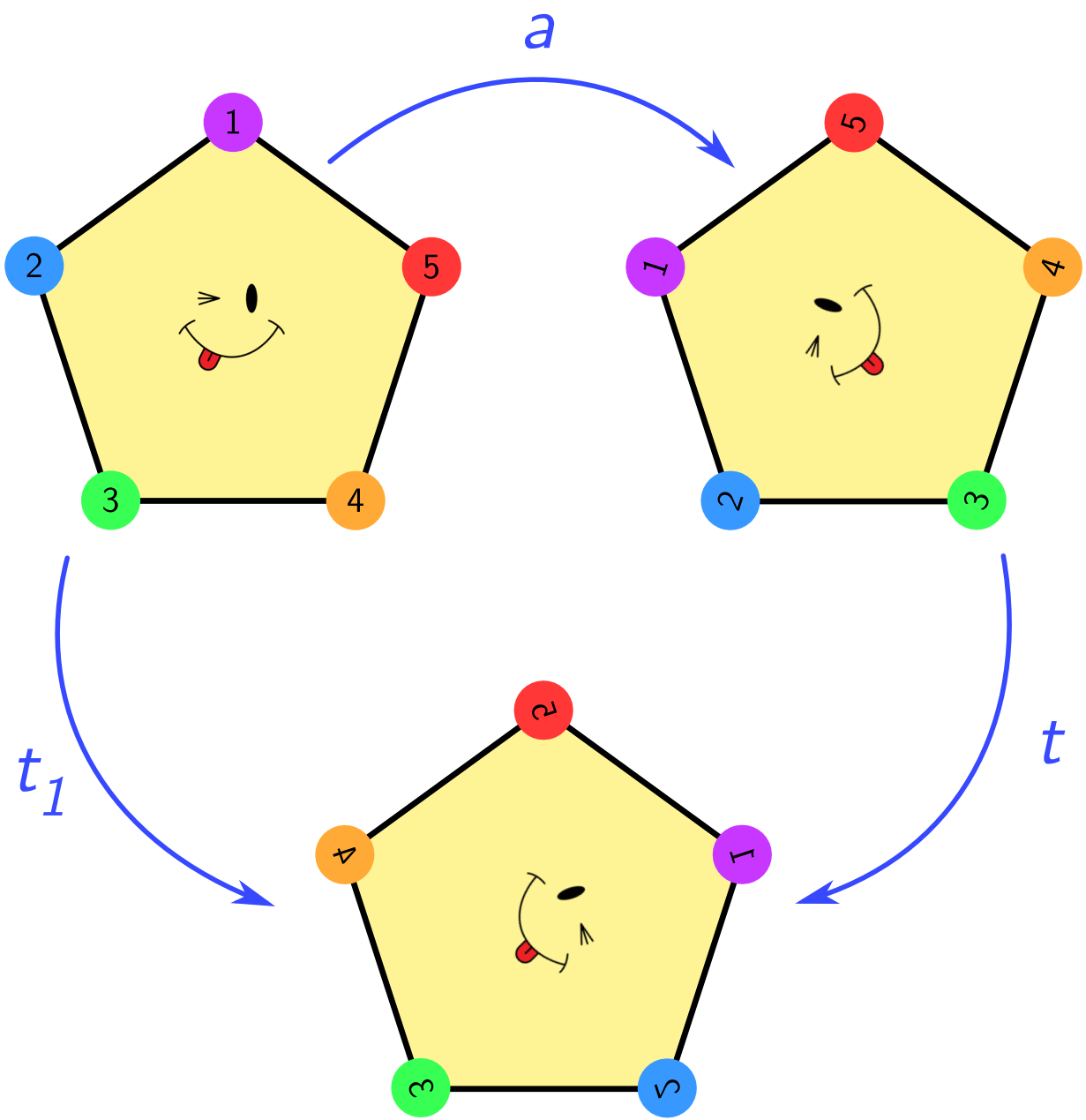
$at = ?$



$at = ?$



$at = t_1$



Diédercsoport

Hasonlóan (be)látható, hogy $t_k = a^k t$ minden $k \in \{0, 1, \ldots, n-1\}$ esetén.
Tehát ...

4.17. Tétel.

A D_n csoportnak $2n$ eleme van: $D_n = \{\mathrm{id}, a, a^2, \ldots, a^{n-1}, t, at, a^2t, \ldots, a^{n-1}t\}$, ahol

- a: a középpont körüli $\frac{2\pi}{n}$ szögű forgatás,
- t: egy szimmetriatengelyre való tükrözés.

Ekkor a^k a középpont körüli $\frac{2k\pi}{n}$ szögű forgatás ($0 \leq k \leq n-1$),
a $t, at, a^2t, \ldots, a^{n-1}t$ transzformációk pedig tengelyes tükrözések
(két „szomszédos" tengely $\frac{\pi}{n}$ szöget zár be egymással).

Fennáll továbbá a $ta = a^{-1}t$ összefüggés.

Házi feladat a gyakorlatra

28. feladat. Számítsa ki D_{15}-ben az alábbi elemeket. Az eredményt a^k vagy $a^k t$ $(k = 0, 1, \ldots, 14)$ alakban adja meg.

(a) $a^{154},\ a^7 t \cdot a^{12} t$

$a^{154} = a^4,\ a^7 t \cdot a^{12} t = a^{10}$

(b) $a^{23} t \cdot a^{18},\ \left(at \cdot a^{-5} t\right)^{-3}$

$a^{23} t \cdot a^{18} = a^5 t,\ \left(at \cdot a^{-5} t\right)^{-3} = a^{12}$

(c) $a^{10} t \cdot a^8 t$

(d) $(a^{-1} t a)^4$

(e) $(a^{10} t)^3$

Házi feladat a gyakorlatra

29. feladat. Oldja meg D_{15}-ben az alábbi egyenleteket. Az eredményt a^k vagy $a^k t$ $(k = 0, 1, \ldots, 14)$ alakban adja meg.

(a) $x \cdot ta^3 = a, \;\; a^4 t \cdot y \cdot a = ta^9$

$x = a^{13} t, \;\; y = a^{12}$

(b) $ta^7 \cdot x \cdot a^2 t = a^{23} t$

$x = a^2 t$

(c) $ta^5 \cdot x \cdot a^2 = t$

(d) $t \cdot x \cdot ta^5 = (ta)^2$

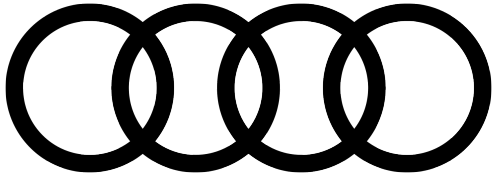
(e) $ta^3 \cdot x = a$

Kilencedik házi feladat az előadásra

Határozza meg a következő ábrák szimmetriacsoportját (melyik ismert csoporttal izomorf a szimmetriacsoport?).

- beküldendő emailben: `twaldha@math.u-szeged.hu`
- pdf fájl legyen (lehet szkennelt is)
- fájlnév: `EHA-eahf9.pdf` (például `WATHAAS-eahf9.pdf`)
- határidő: november 23, reggel 8 óra

Kilencedik házi feladat az előadásra

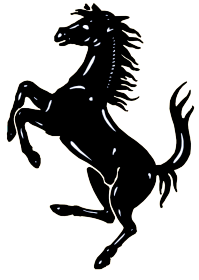
(a) 

(b) 

(c) 

(d) 

(e) 

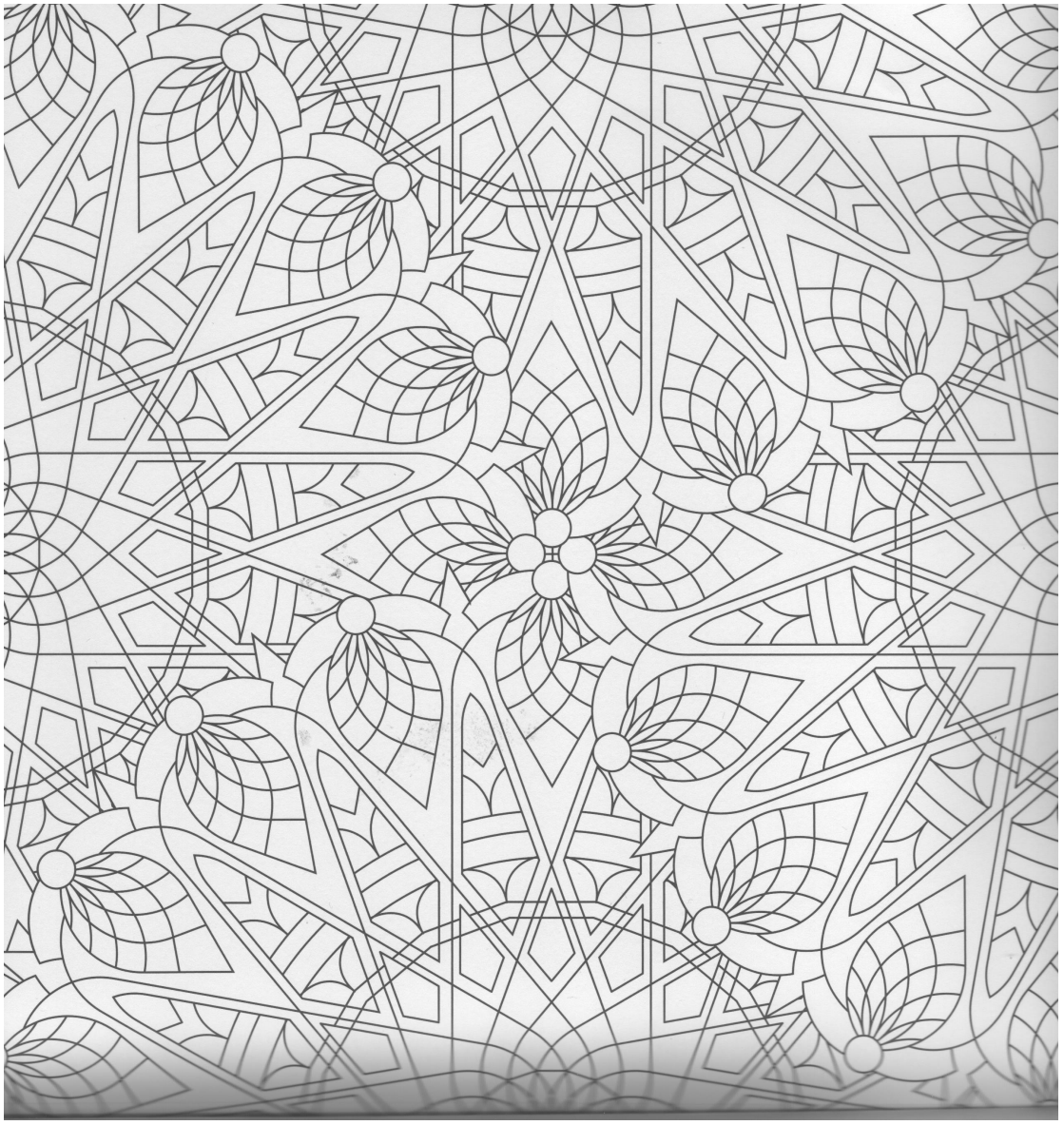
(f) 

Kilencedik házi feladat az előadásra

(g)

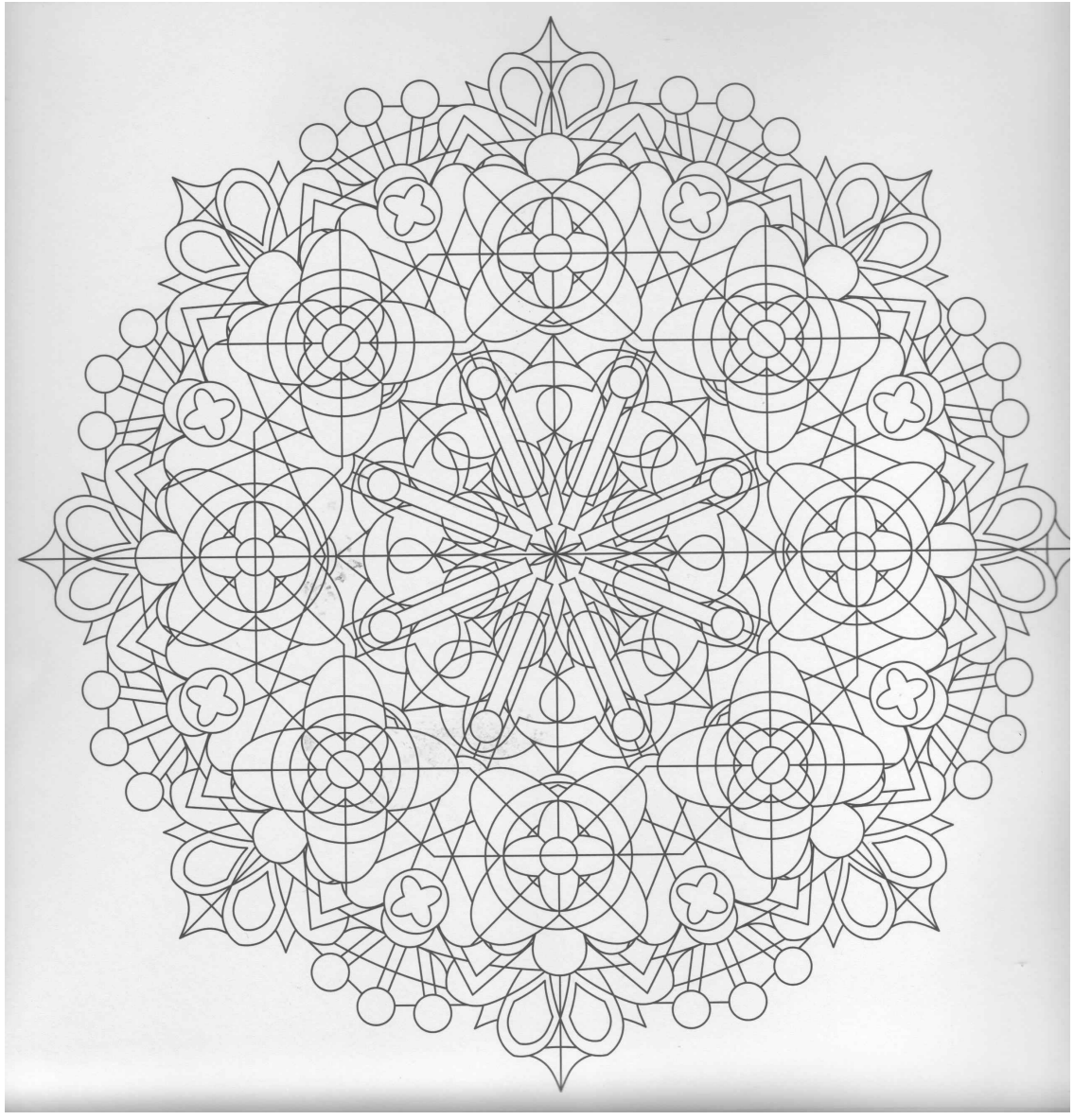
Kilencedik házi feladat az előadásra

(h)



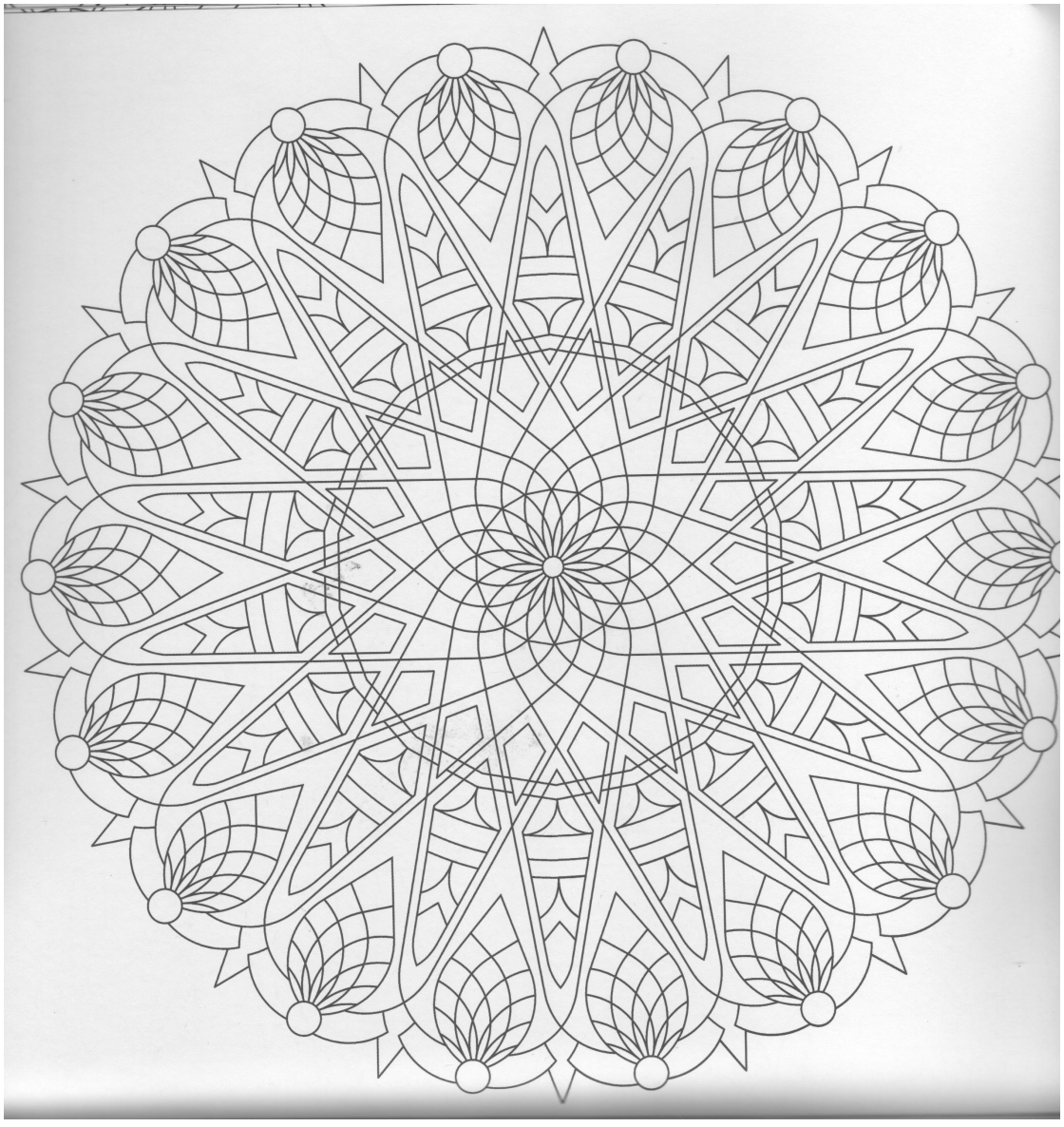
Kilencedik házi feladat az előadásra

(i)



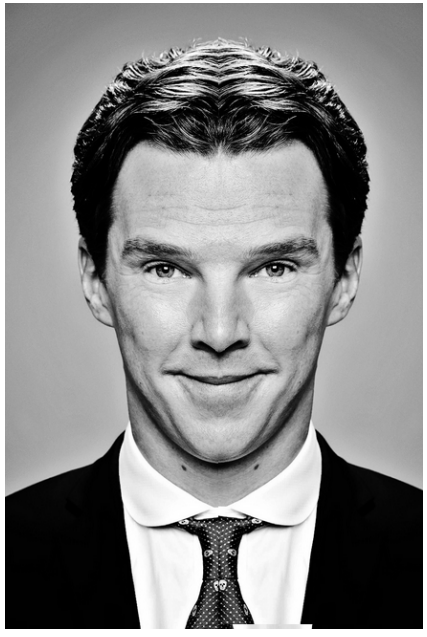
Kilencedik házi feladat az előadásra

(j)



Kilencedik házi feladat az előadásra

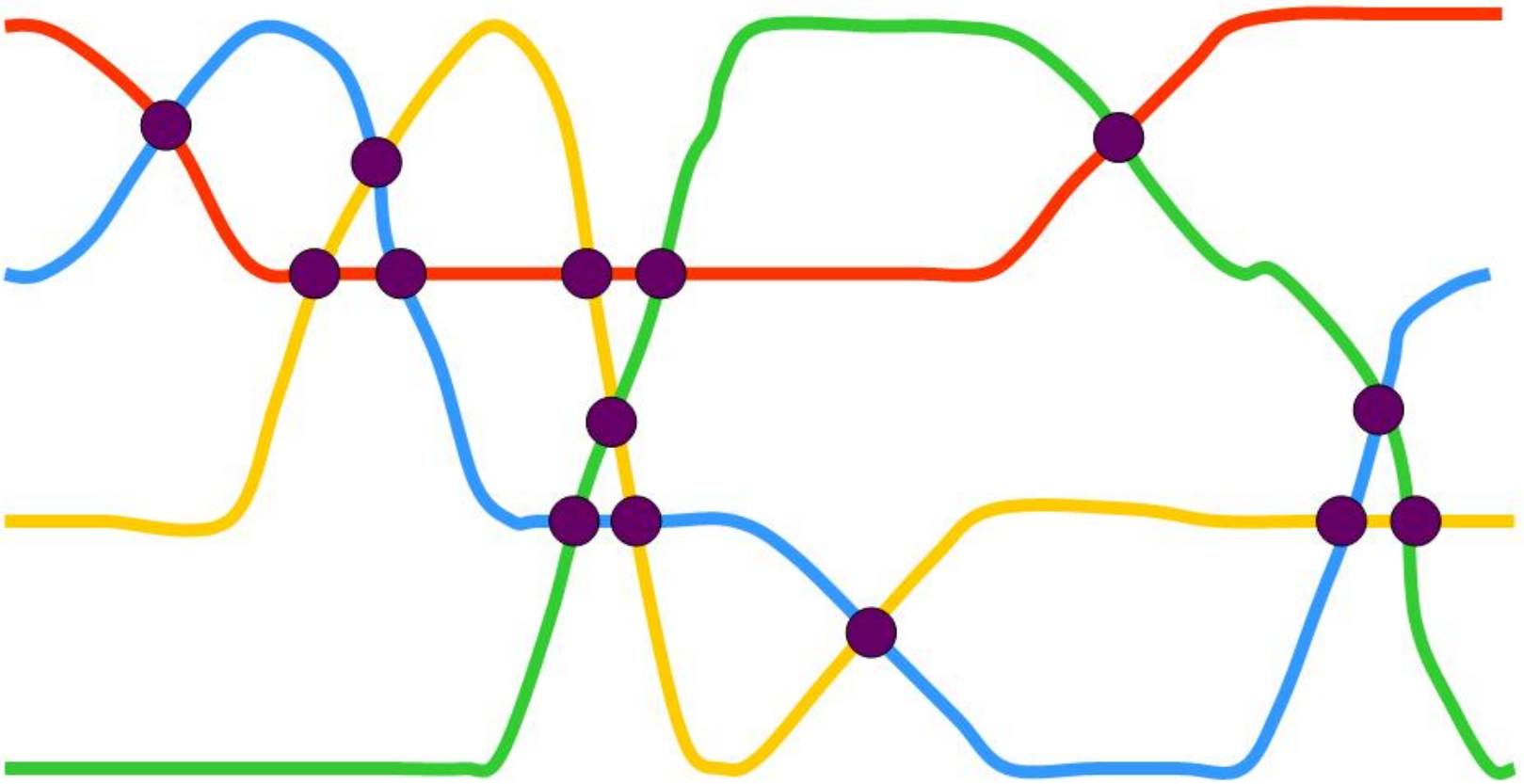
(k)



(l)

(m) Rajzoljon valamit, aminek $\mathbb{Z}_5$-tel izomorf a szimmetriacsoportja.

Permutációcsoportok



Permutációcsoportok

4.18. Definíció.

A nemüres A halmaz összes permutációi alkotta S_A szimmetrikus csoport részcsoportjait *permutációcsoportoknak* nevezzük.

4.19. Definíció.

Az $A = \{1, 2, \ldots, n\}$ halmaz összes permutációi alkotta csoportot *n-edfokú szimmetrikus csoportnak* nevezzük, és S_n-nel jelöljük.

Megjegyzés.

Egy $\pi \in S_n$ permutációt megadhatunk úgy, hogy $\{1, 2, \ldots, n\}$ minden eleme alá odaírjuk a π melletti képét:

$$\begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ 1\pi & 2\pi & 3\pi & \cdots & n\pi \end{pmatrix}.$$

Vegyük észre, hogy π bijektivitása azt jelenti, hogy a mátrix alsó sorában az $1, 2, \ldots, n$ számok egy permutációja van.

Ciklusfelbontás

4.20. Definíció.

Legyenek $a_1, \ldots, a_k \in \{1, 2, \ldots, n\}$ különböző elemek, és legyen $\pi \in S_n$ az alábbi permutáció:

$$a_1\pi = a_2, \quad a_2\pi = a_3, \ \ldots, \ a_{k-1}\pi = a_k, \quad a_k\pi = a_1 \quad \text{és}$$
$$b\pi = b \text{ ha } b \notin \{a_1, \ldots, a_k\}.$$

Ezt a π permutációt így jelöljük: $\pi = (a_1\, a_2\, \cdots\, a_{k-1}\, a_k)$ és *ciklikus permutációnak* vagy röviden *ciklusnak* nevezzük.

4.21. Definíció.

Két permutáció *idegen*, ha *mozgatott elemeik* halmaza diszjunkt.

4.22. Tétel.

Ha π és ρ idegen permutációk, akkor fölcserélhetőek, azaz $\pi\rho = \rho\pi$.

4.23. Tétel.

Minden S_n-beli permutáció előáll páronként idegen ciklusok szorzataként, és ez az előállítás a tényezők sorrendjétől eltekintve egyértelmű.

Transzpozíciók

4.24. Definíció.

A 2 hosszúságú ciklusokat, vagyis az $(i\,j)$ alakú permutációkat *transzpozícióknak* nevezzük.

4.25. Tétel.

Az S_n csoportot *generálják* a transzpozíciók, azaz minden S_n-beli permutáció előáll transzpozíciók szorzataként.

Bizonyítás.

Elég ciklusokra bizonyítani: $(a_1\,a_2\,\cdots\,a_{k-1}\,a_k) = (a_1\,a_2)\,(a_1\,a_3)\cdots(a_1\,a_k)$. □

4.26. Tétel.

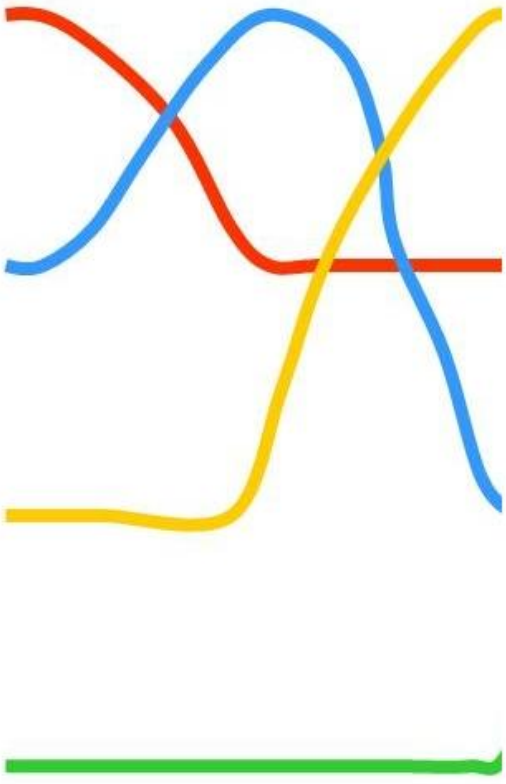
Egy S_n-beli permutáció transzpozíciók szorzataként való felírásában a tényezők számának paritása egyértelműen meghatározott.

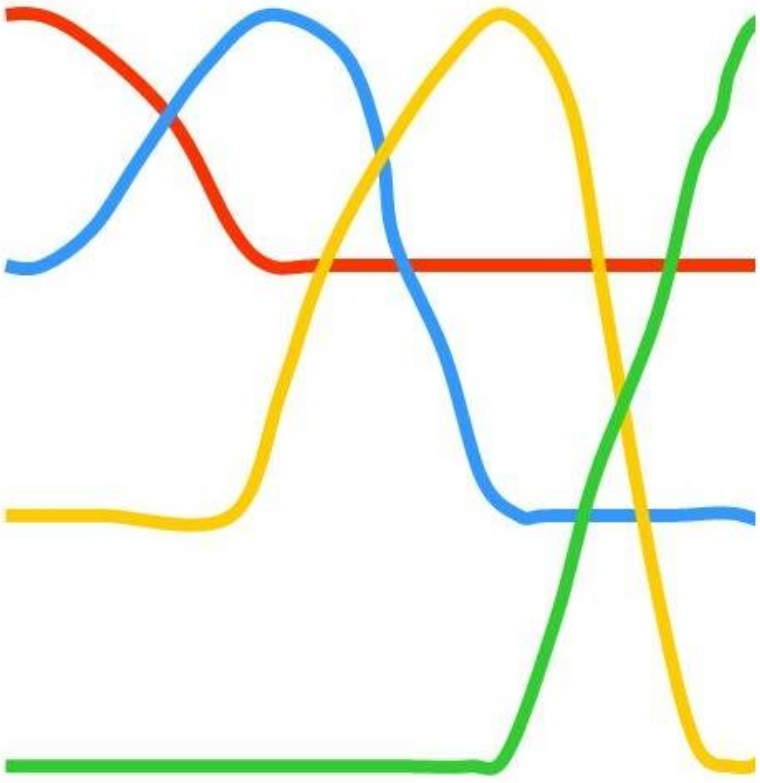
Bizonyítás.

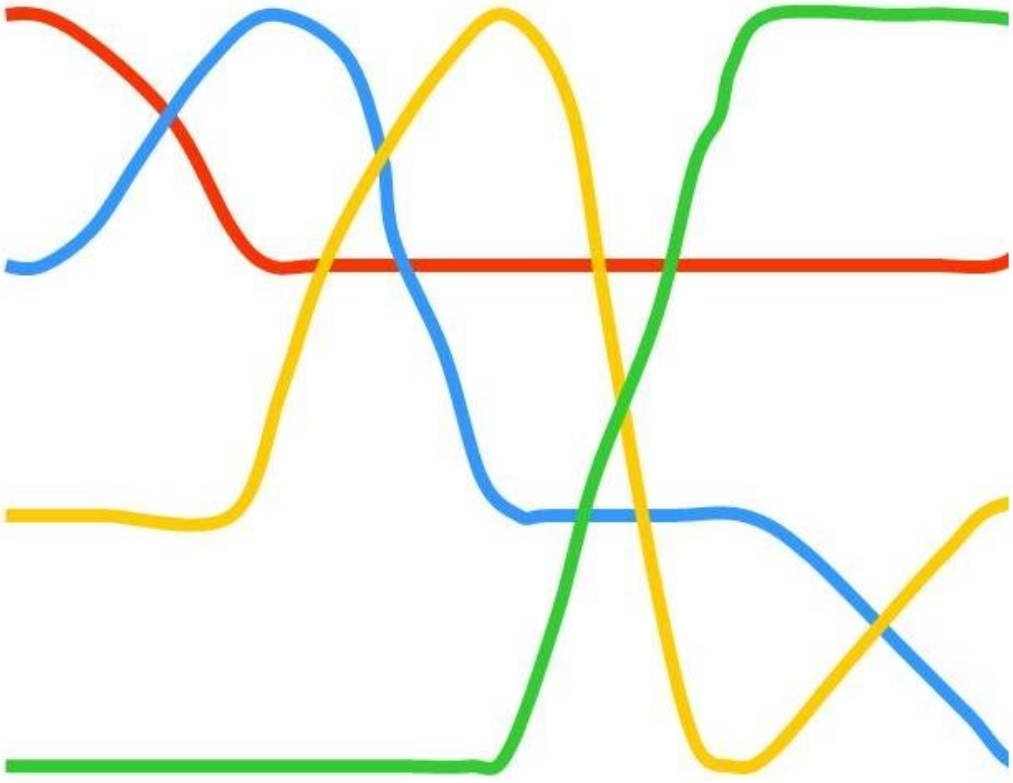
Tegyük fel, hogy $\tau_1\tau_2\cdots\tau_{2k+1} = \sigma_1\sigma_2\cdots\sigma_{2l}$, ahol mindegyik τ_i és σ_j transzpozíció. Ekkor az identikus permutáció előáll páratlan sok transzpozíció szorzataként:

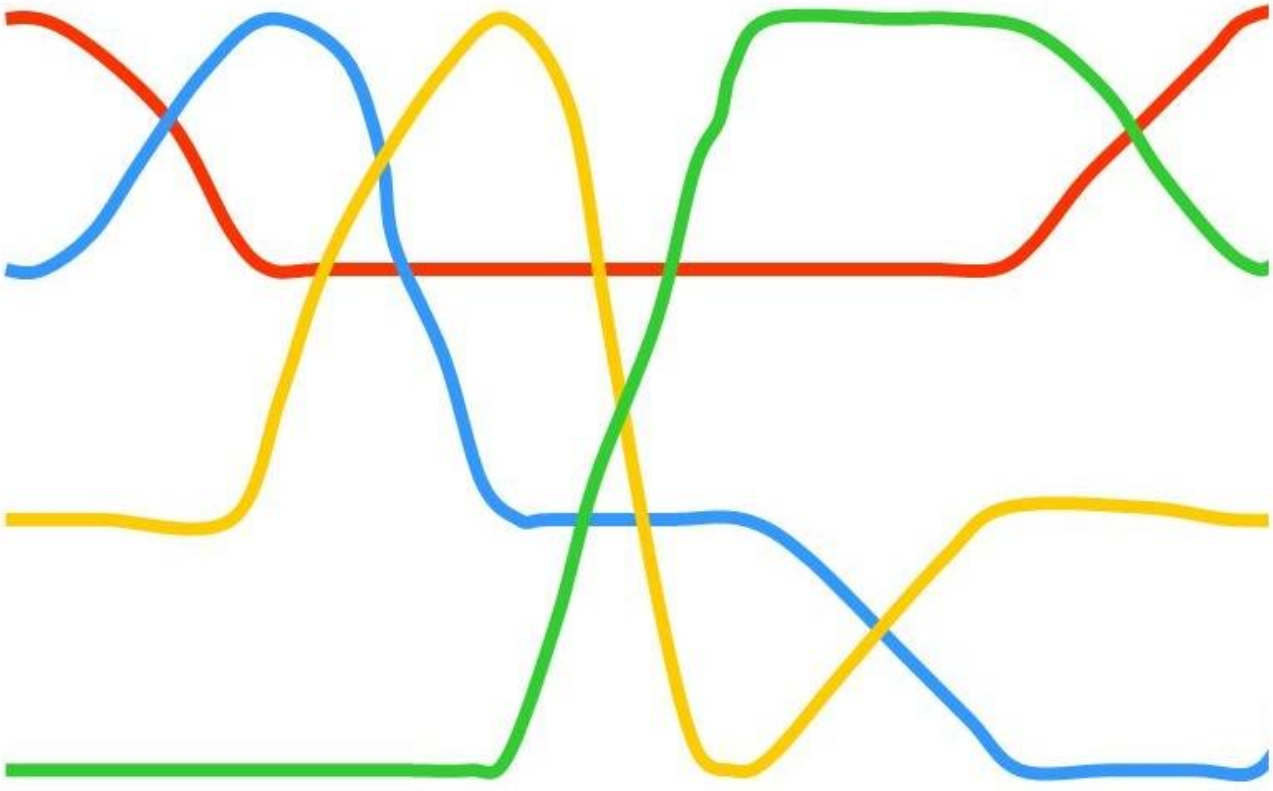
$$\mathrm{id} = \tau_1\tau_2\cdots\tau_{2k+1}\sigma_{2l}\cdots\sigma_2\sigma_1.$$

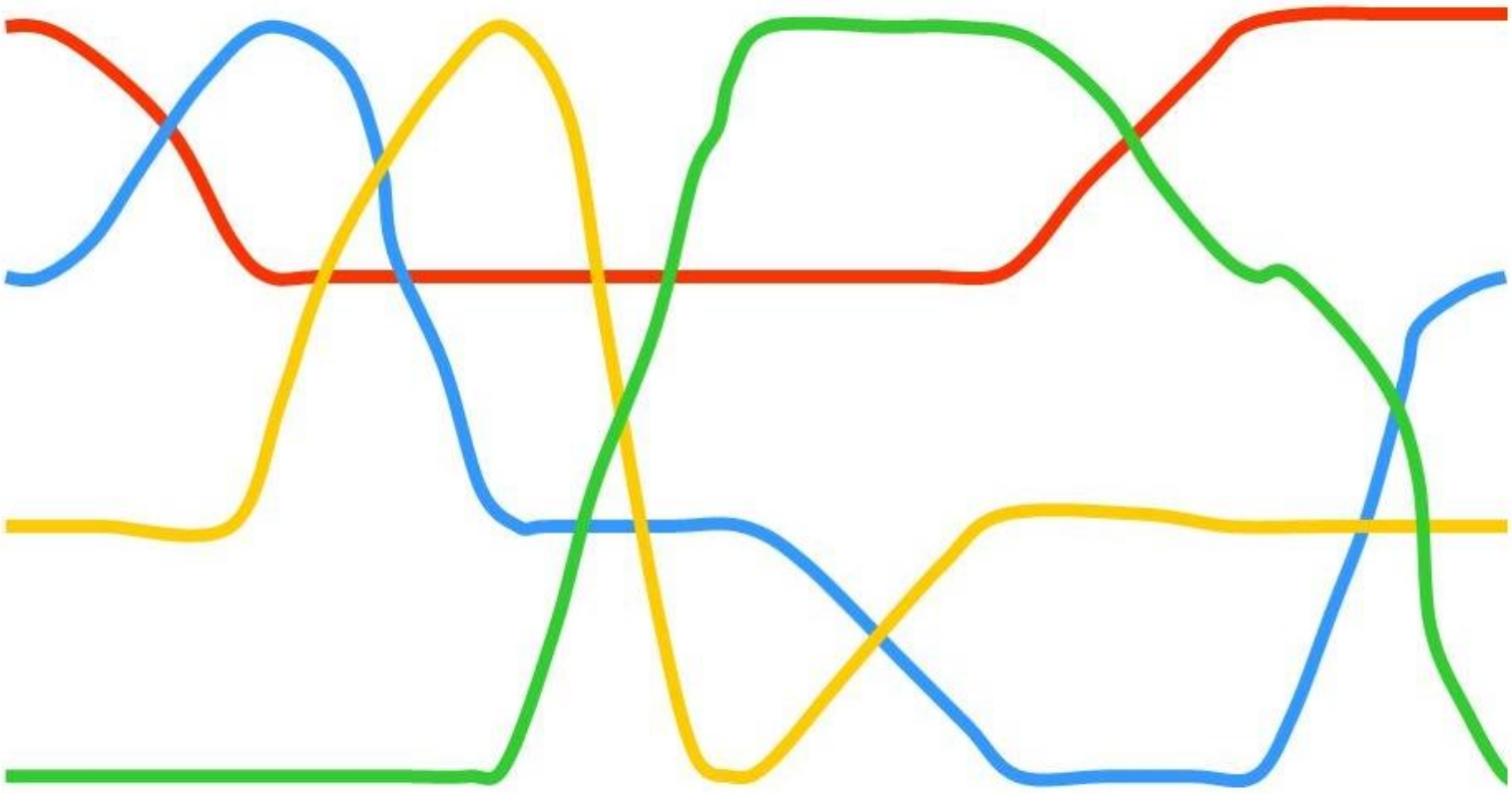
Megmutatjuk, hogy ez lehetetlen ...

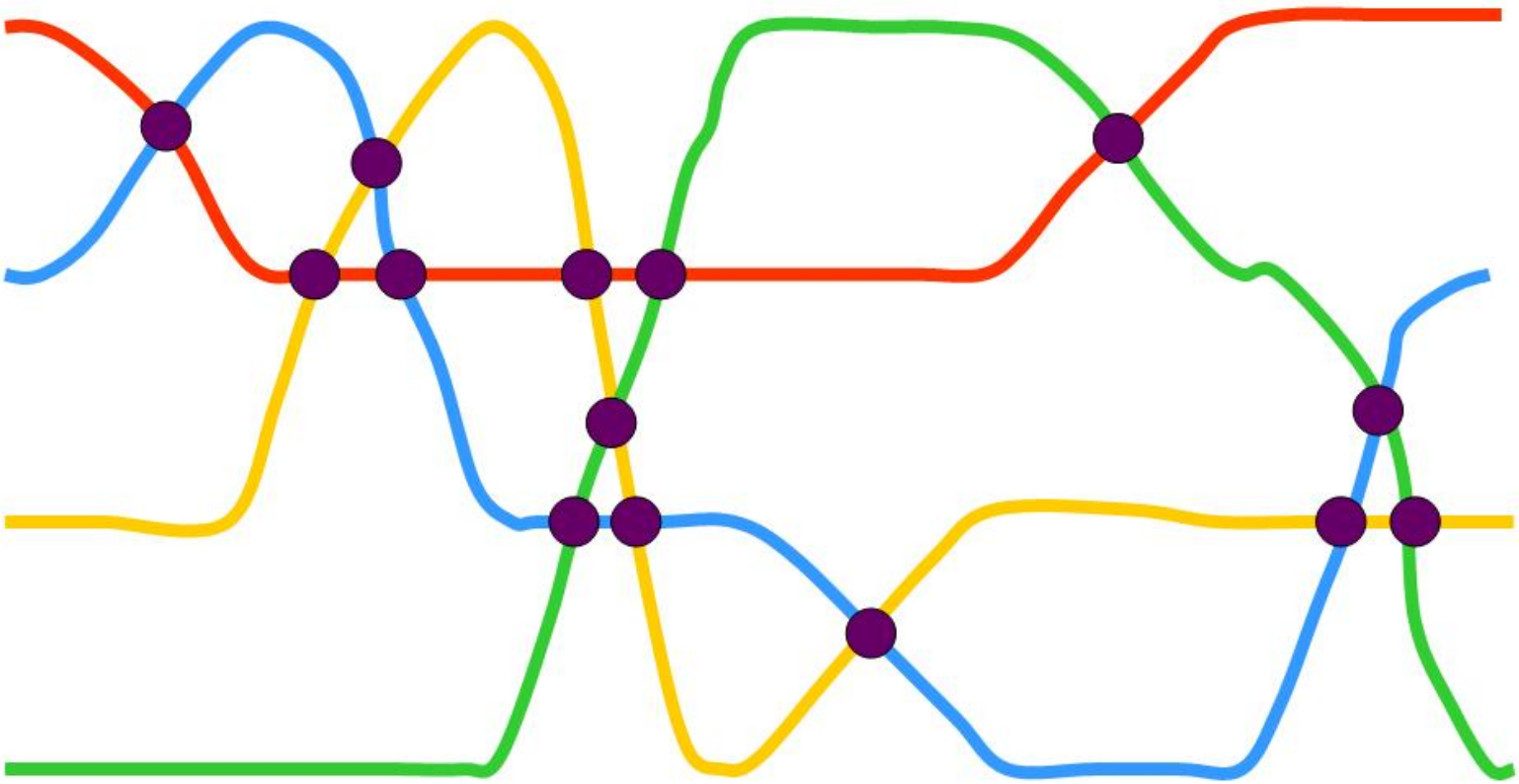


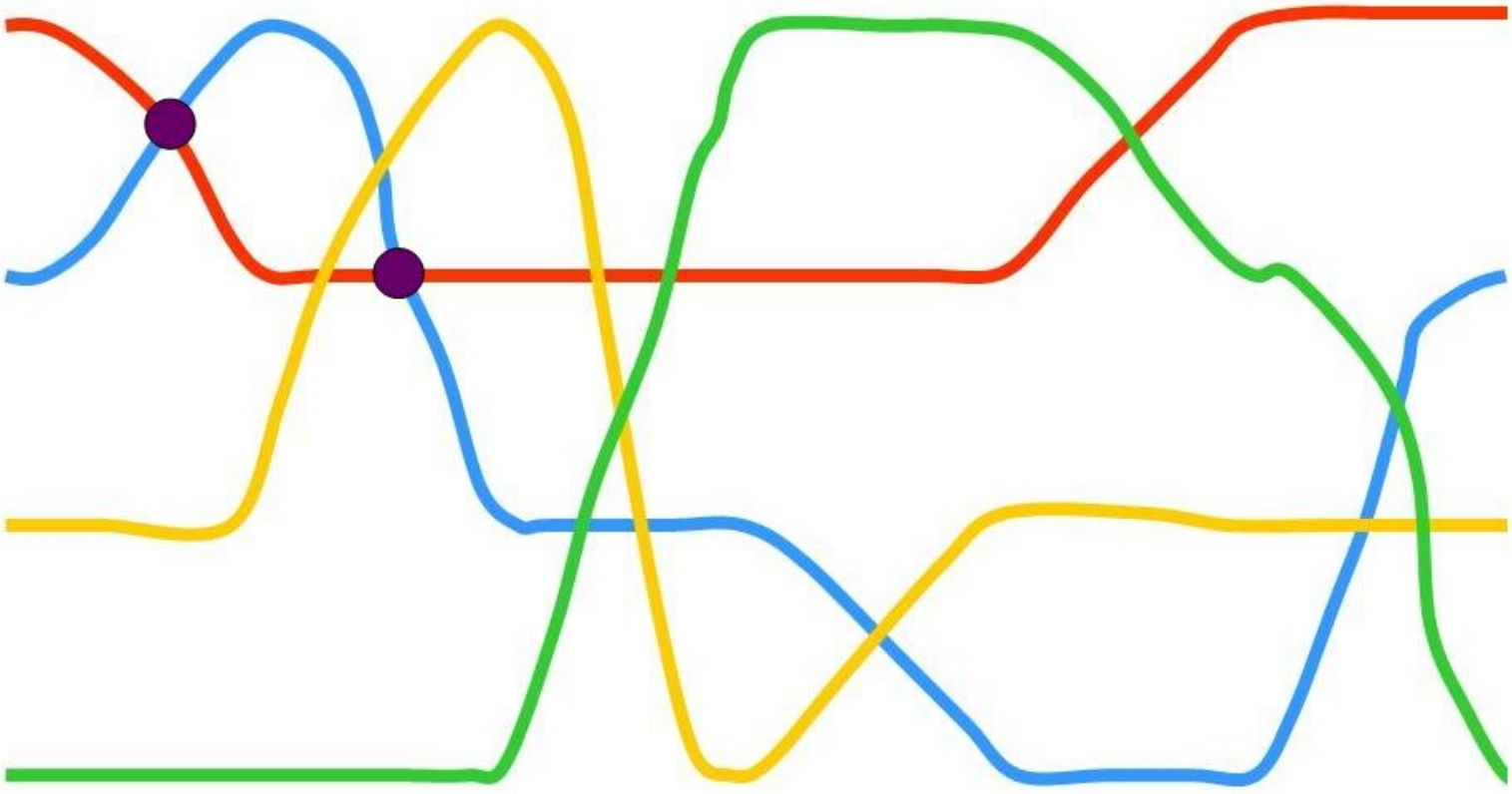




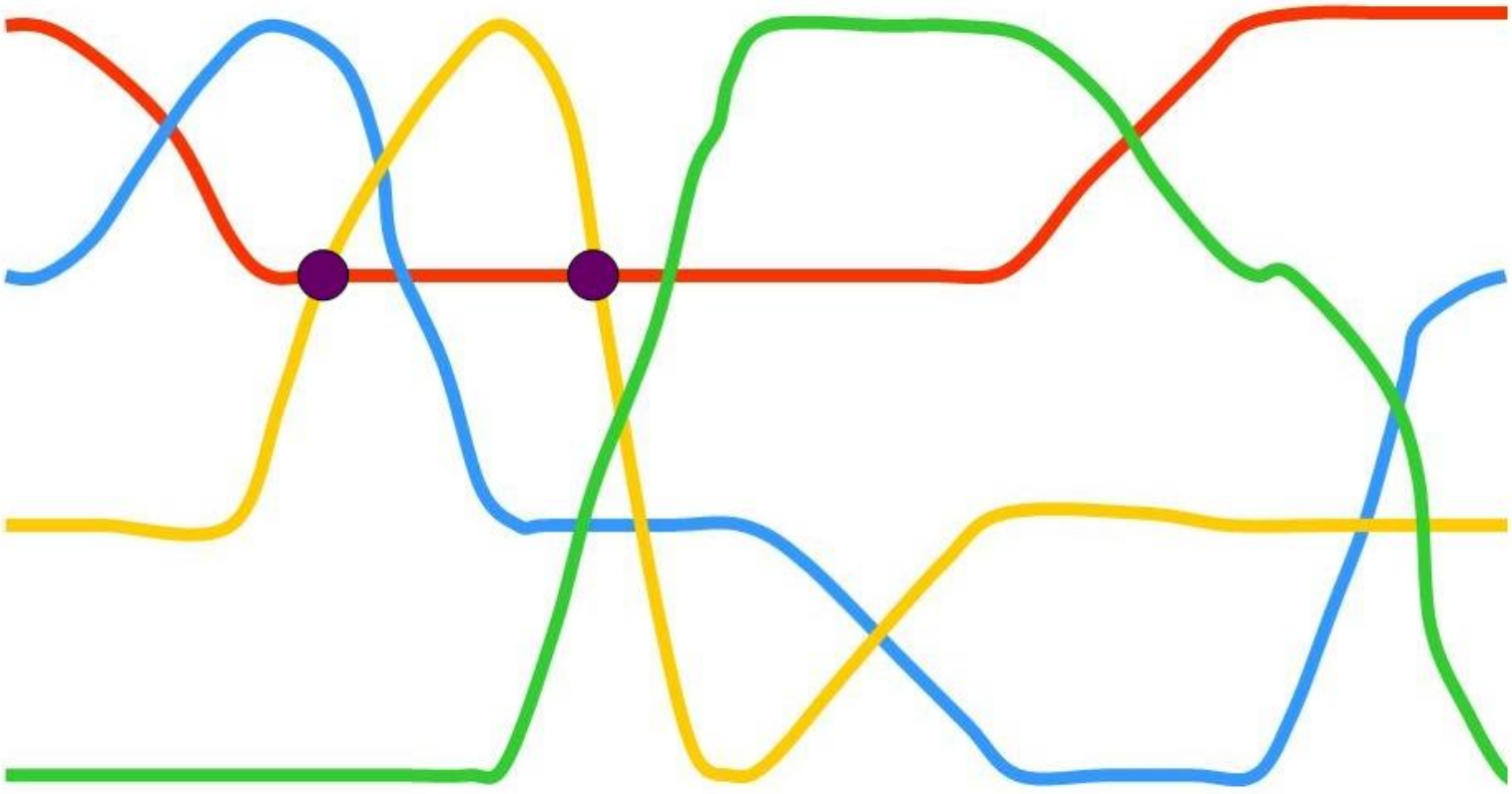




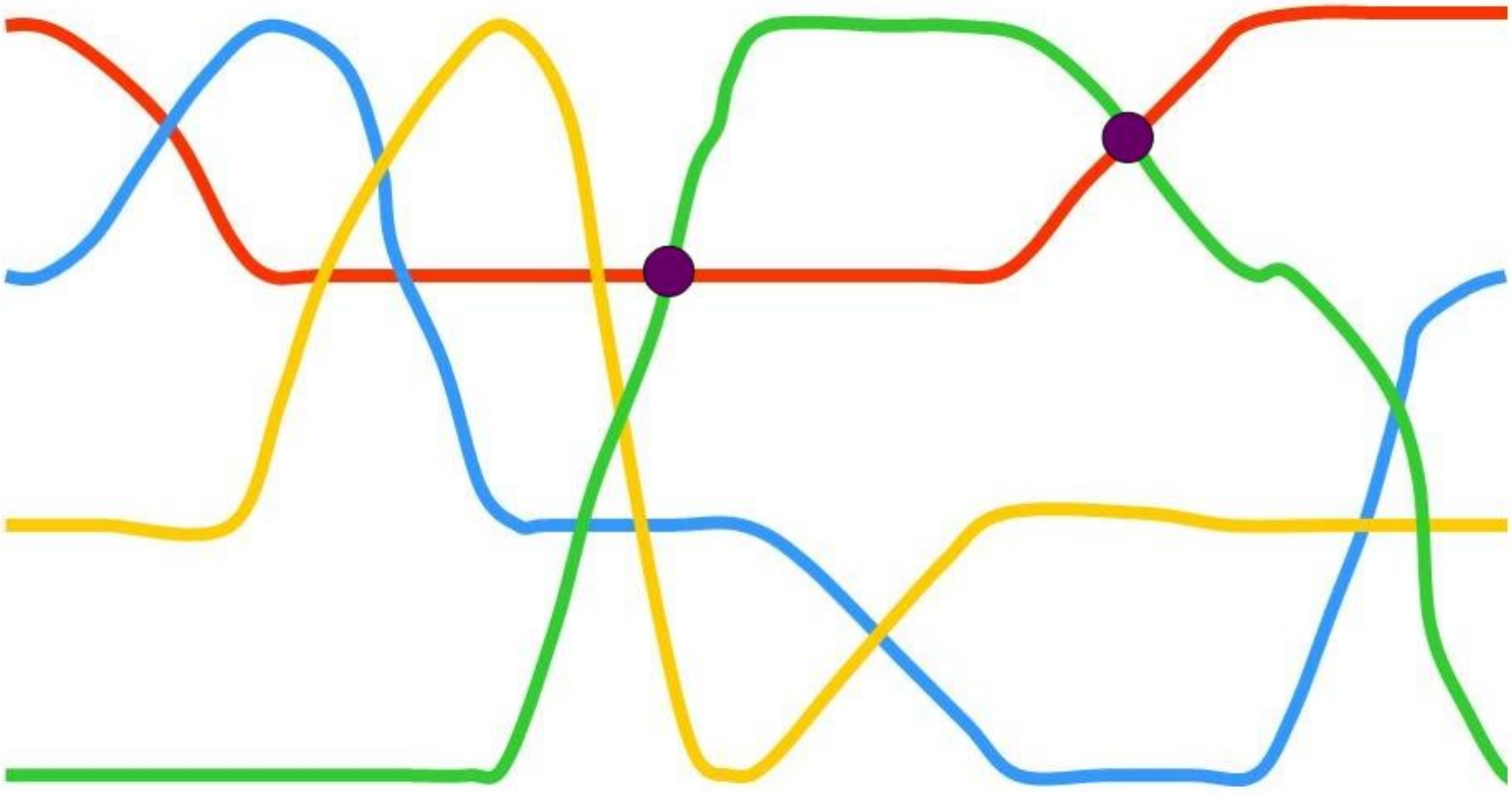




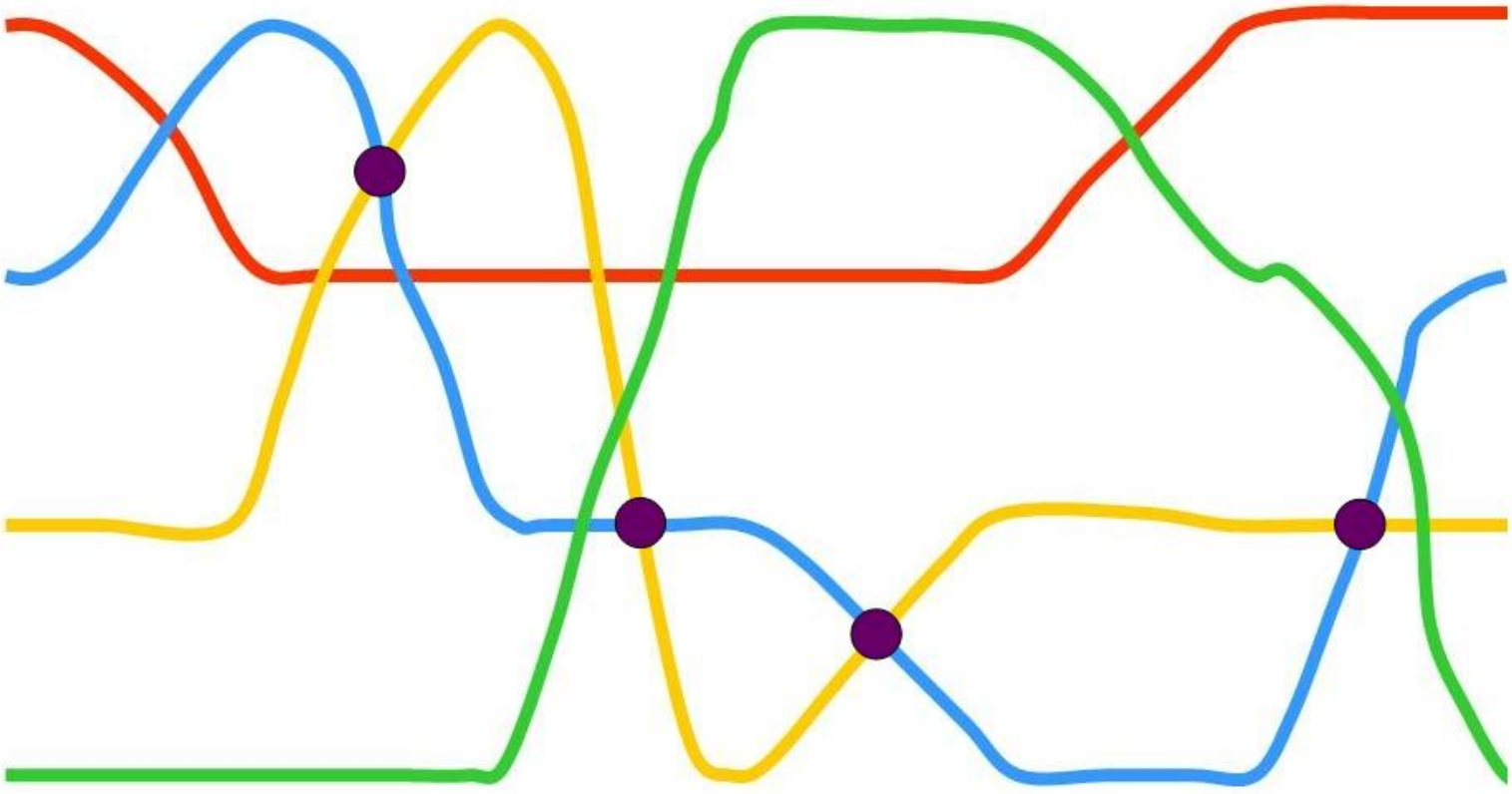
metszéspontok: 2



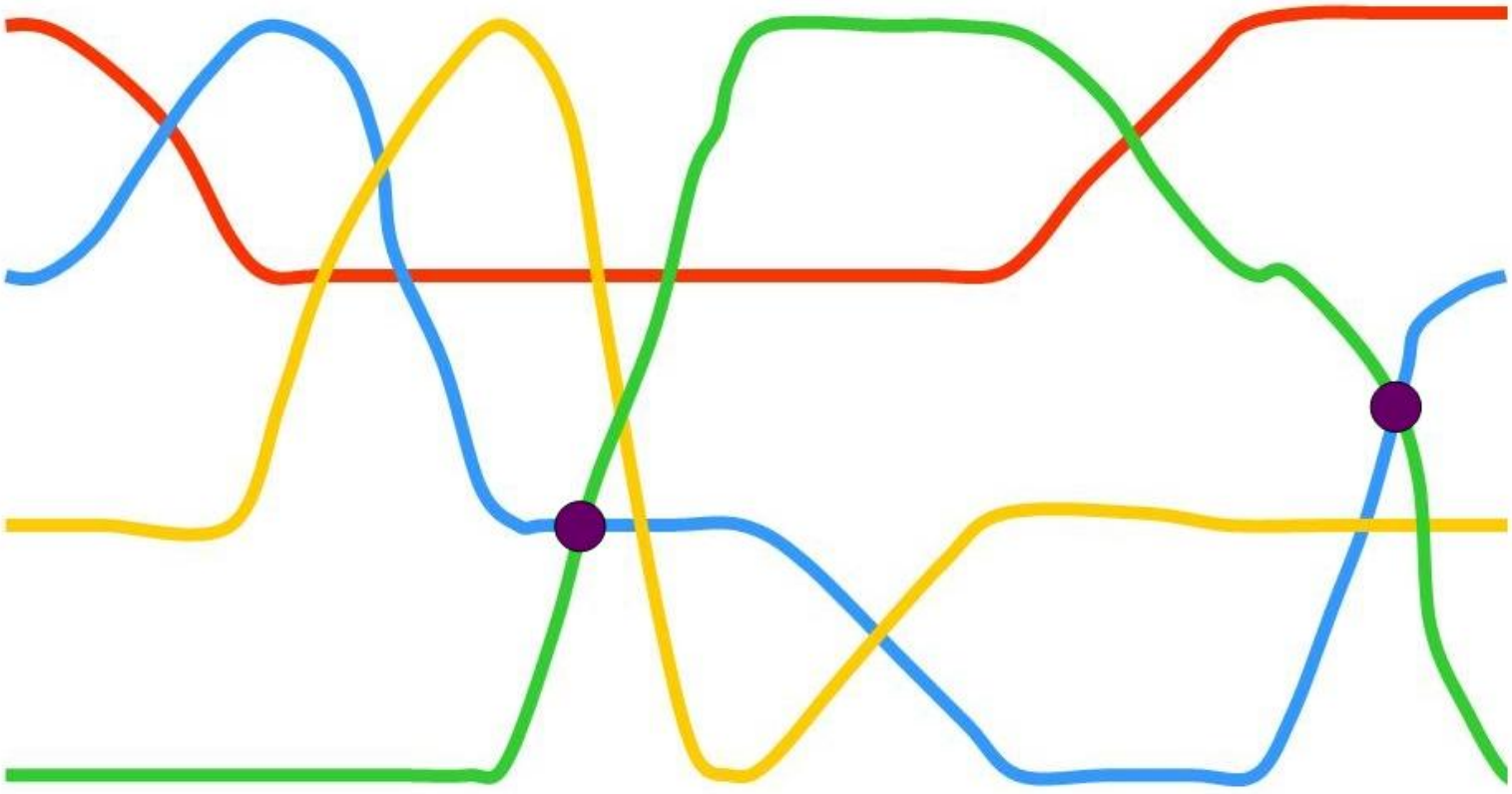
metszéspontok: $2 + 2$



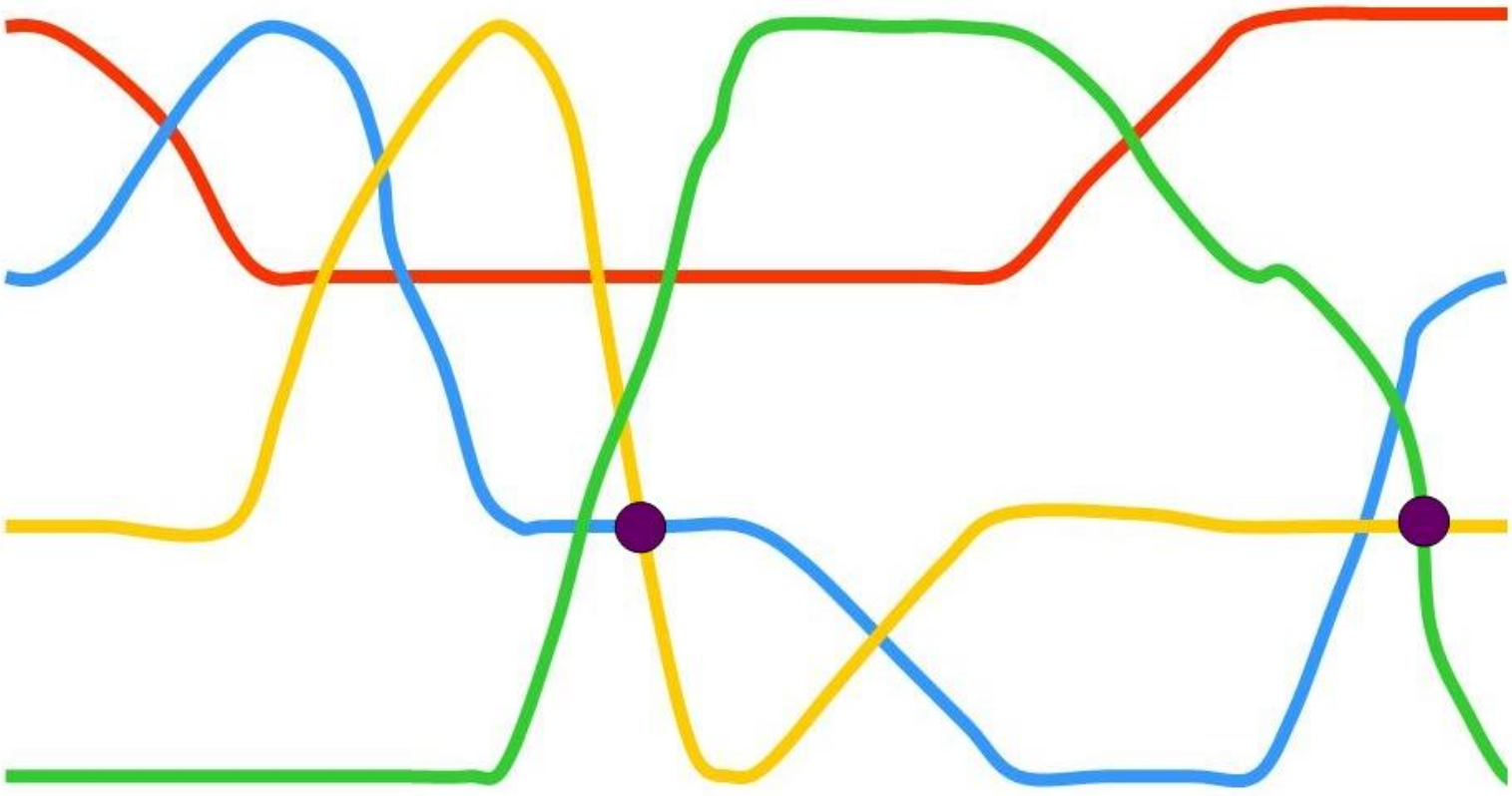
metszéspontok: $2 + 2 + 2$



metszéspontok: $2 + 2 + 2 + 4$



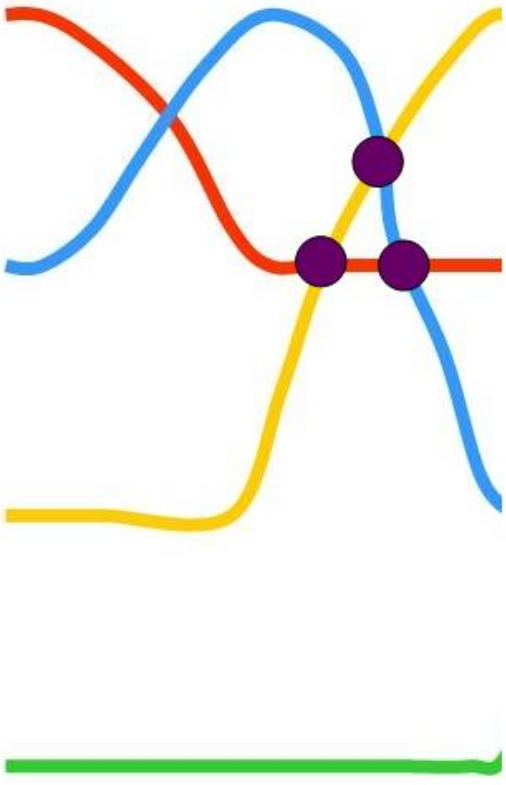
metszéspontok: $2 + 2 + 2 + 4 + 2$



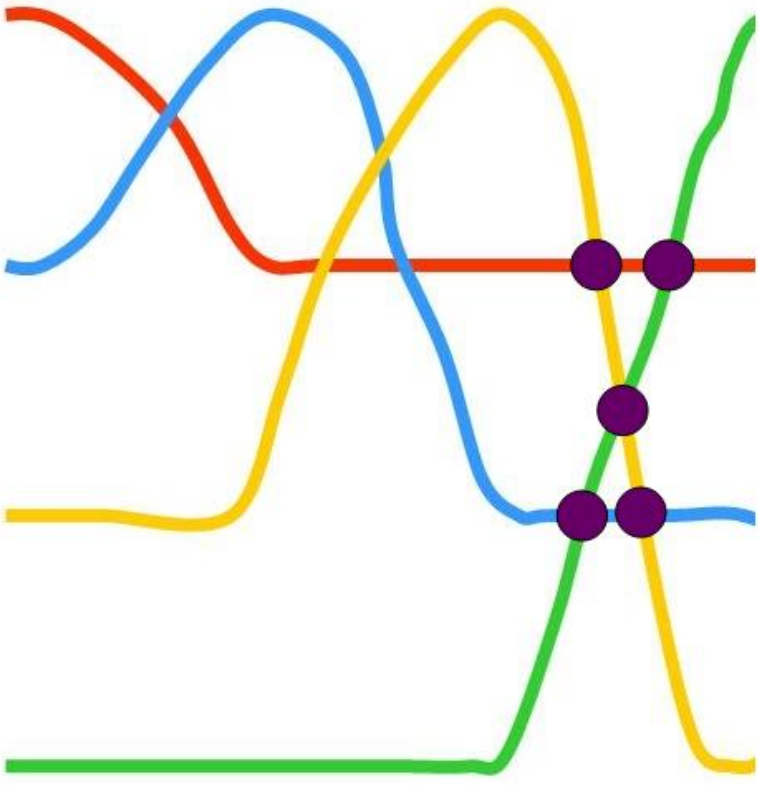
metszéspontok: $2 + 2 + 2 + 4 + 2 + 2 \equiv 0 \pmod 2$



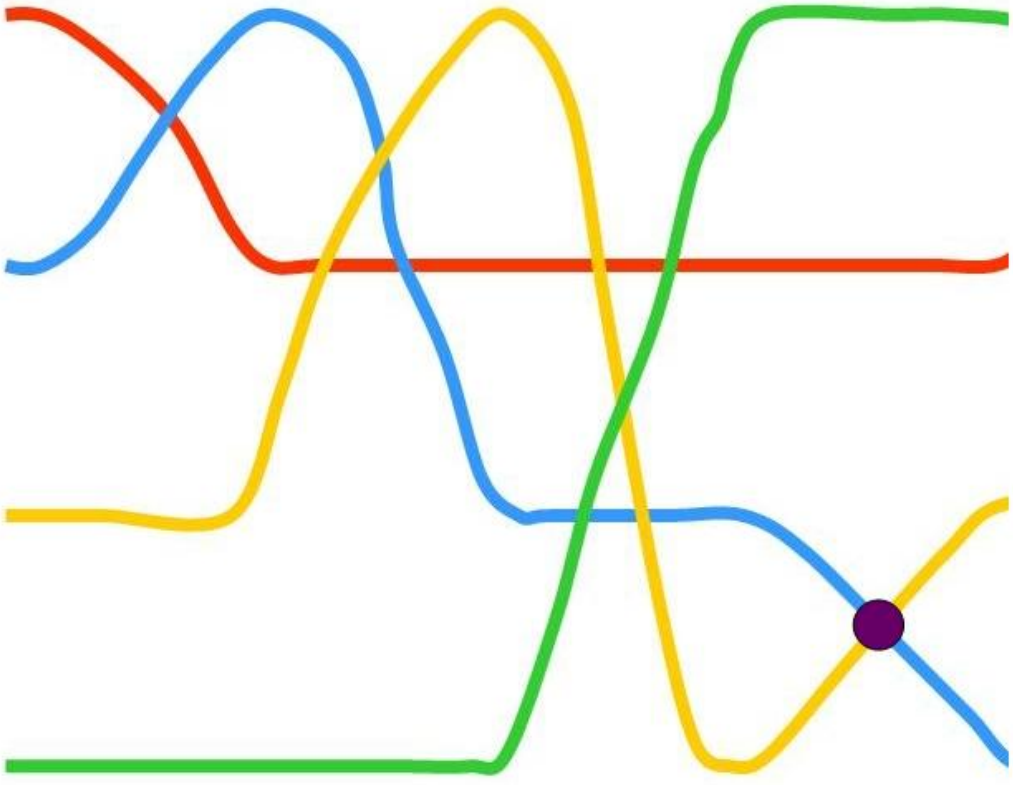

metszéspontok: 1



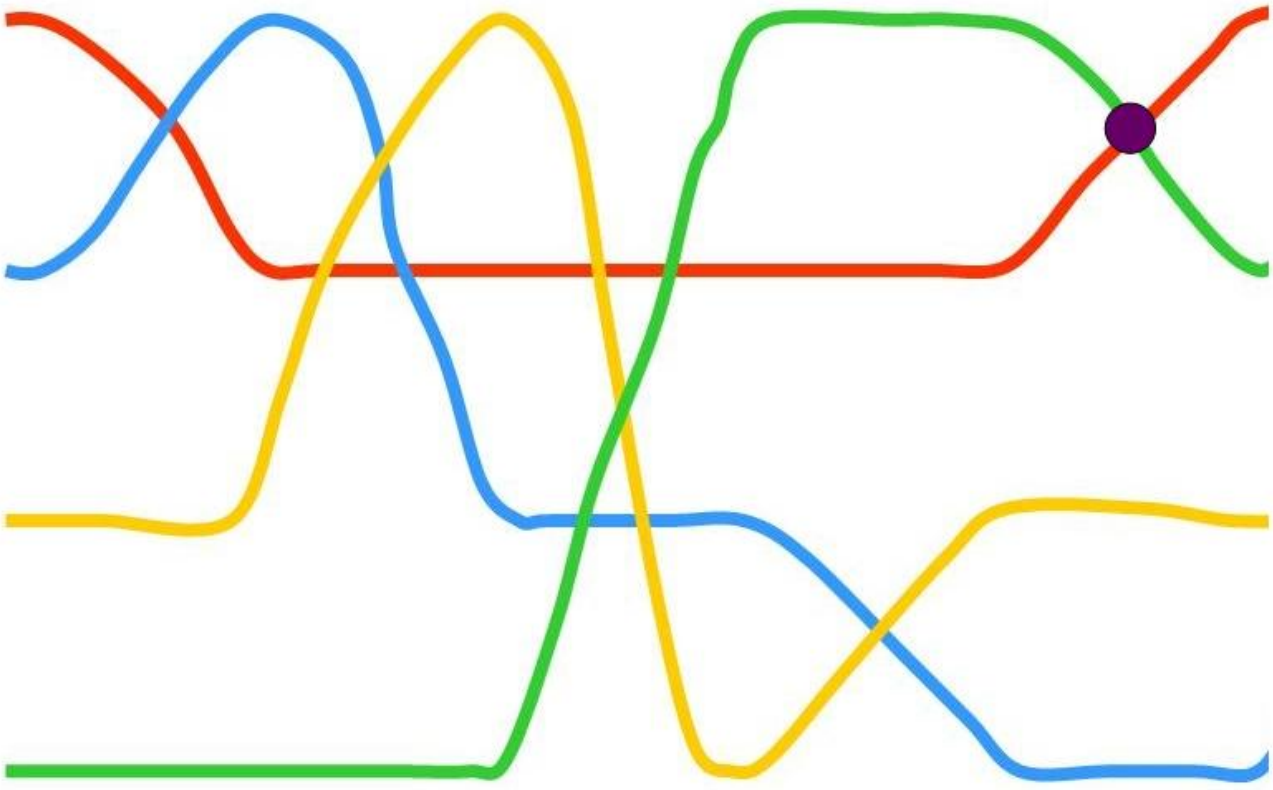
metszéspontok: $1 + 3$



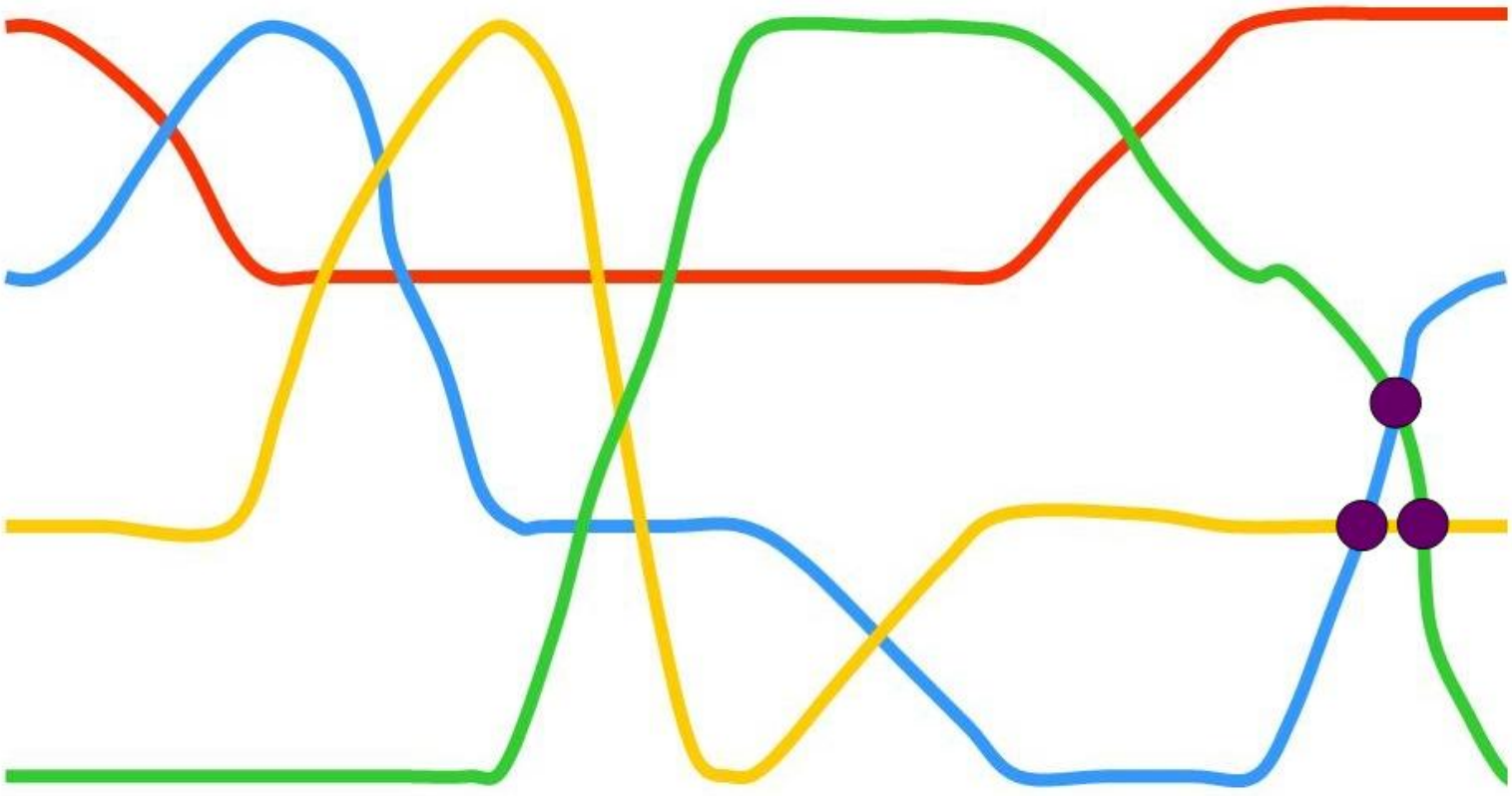
metszéspontok: $1 + 3 + 5$



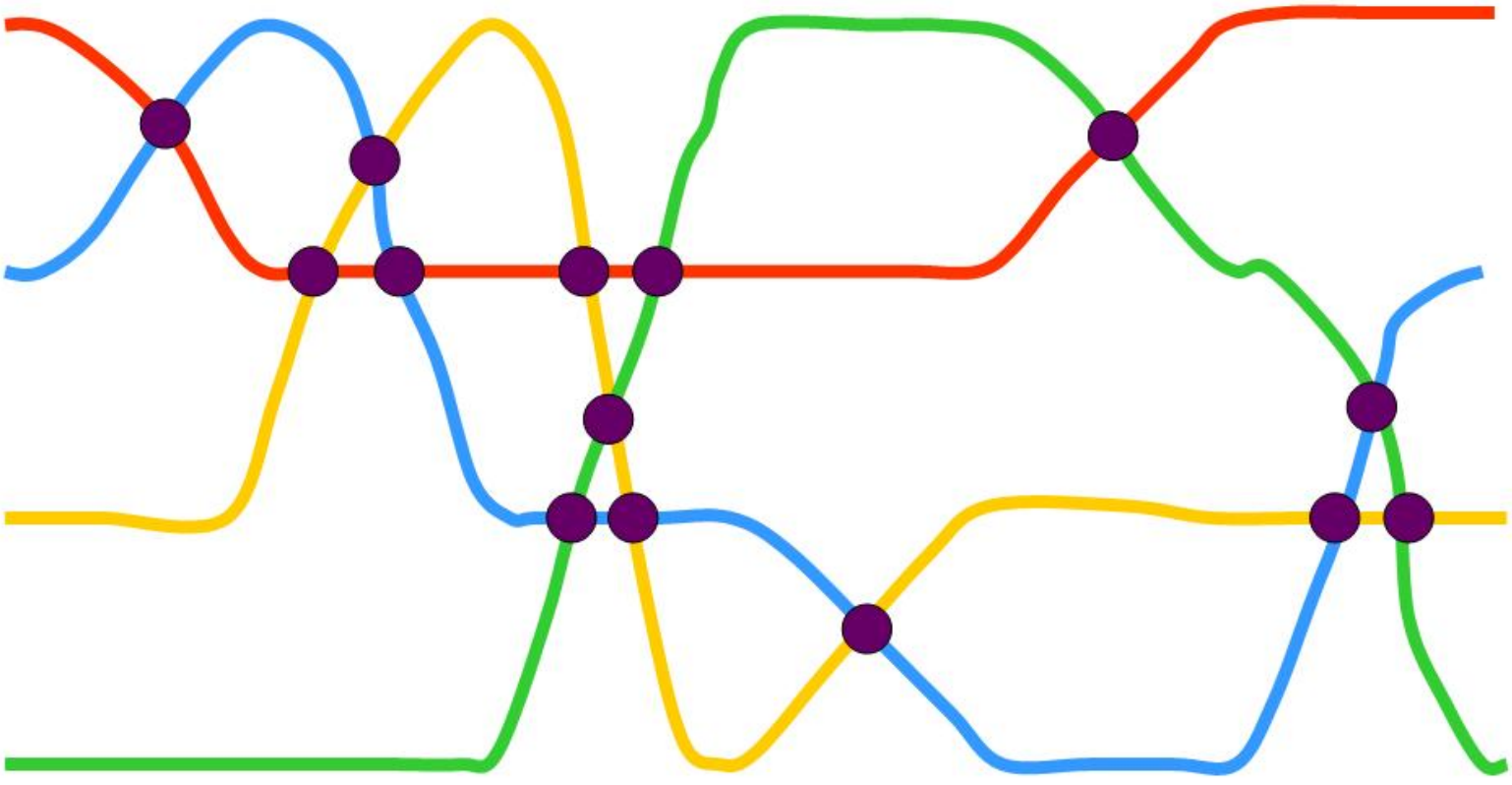
metszéspontok: $1 + 3 + 5 + 1$



metszéspontok: $1 + 3 + 5 + 1 + 1$



metszéspontok: $1 + 3 + 5 + 1 + 1 + 3 \equiv$ cserék száma $\pmod 2$



metszéspontok: $0 \equiv$ cserék száma $\pmod 2$ 

Az alternáló csoport

4.27. Állítás.

A páros hosszúságú ciklusok páratlan permutációk, míg a páratlan hosszúságú ciklusok páros permutációk.

4.28. Tétel.

A páros permutációk egy 2 indexű részcsoportot alkotnak S_n-ben. Ezt a csoportot *alternáló csoportnak* nevezzük, és A_n-nel jelöljük.

Megjegyzés.

Tekintsük az alábbi n-változós polinomfüggvényt (pl. $\mathbb{R}$ felett):

$$V(x_1, \ldots, x_n) = \prod_{i<j} (x_i - x_j).$$

A változók bármely permutációja esetén V vagy nem változik, vagy előjelet vált:

$$V(x_{1\pi}, \ldots, x_{n\pi}) = \pm V(x_1, \ldots, x_n) = \operatorname{sgn} \pi \cdot V(x_1, \ldots, x_n).$$

A $\pi \in S_n$ permutáció előjele aszerint 1 vagy -1, hogy π páros-e vagy páratlan.

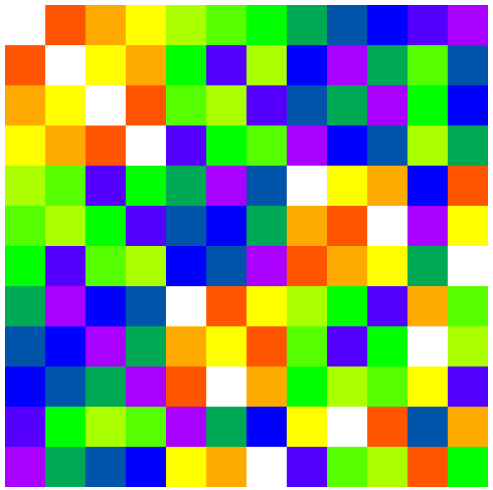
Az alternáló csoport

Példa.

- $A_2 = \{\mathrm{id}\}$
- $A_3 = \{\mathrm{id}, (123), (132)\} \cong \mathbb{Z}_3$
- $A_4 = \{\mathrm{id}, (123), (132), (124), (142), (134), (143), (234), (243), (12)(34), (13)(24), (14)(23)\}$

4.29. Tétel.

Az alternáló csoportot generálják a 3 hosszúságú ciklusok, azaz minden A_n-beli permutáció előáll 3 hosszúságú ciklusok szorzataként.



http://nicflic.blogspot.hu

Hatványozás, elem rendje, ciklikus csoportok

Hatványozás

Jelölés.

Ezentúl G mindig egy tetszőleges csoportot jelöl, a csoportműveletet szorzásnak nevezzük (és úgy is írjuk), az egységelemet 1, az a elem inverzét pedig a^{-1} jelöli.

4.30. Definíció.

Az $a \in G$ elem egész kitevős hatványait a következőképpen értelmezzük: tetszőleges n pozitív egészre legyen

- $a^n = a \cdot \ldots \cdot a$ (n db a szorzata),
- $a^{-n} = a^{-1} \cdot \ldots \cdot a^{-1}$ (n db a^{-1} szorzata),
- $a^0 = 1$.

4.31. Tétel.

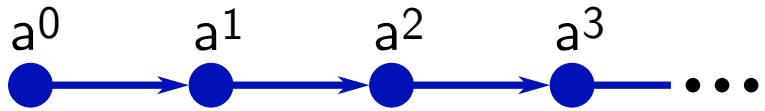
Tetszőleges G csoport, $a, b \in G$ és $m, n \in \mathbb{Z}$ esetén teljesülnek az alábbiak:

1. $a^m \cdot a^n = a^{m+n}$;
2. $(a^m)^n = a^{mn}$;
3. ha $ab = ba$, akkor $(ab)^n = a^n \cdot b^n$;
4. $(ab)^{-1} = b^{-1}a^{-1}$.

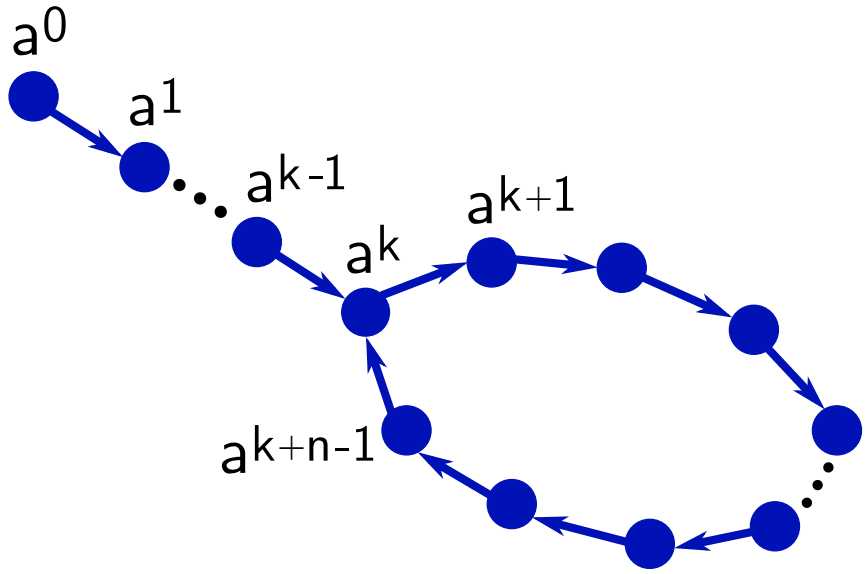
Hatványozás

Egy monoidban egy a elem hatványainak sorozata kétféleképpen viselkedhet:

1. A hatványok mind különbözők:



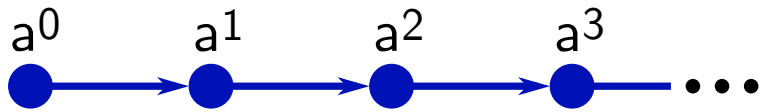
2. Előbb-utóbb ismétlődés lép fel, azaz $\exists k, n \in \mathbb{N}$: $a^k = a^{k+n}$:



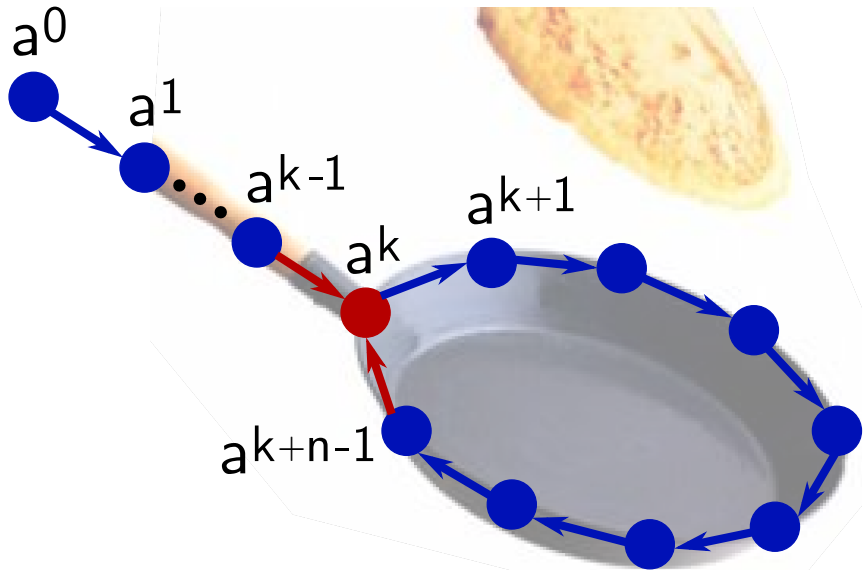
Hatványozás

Egy monoidban egy a elem hatványainak sorozata kétféleképpen viselkedhet:

1. A hatványok mind különbözők:



2. Előbb-utóbb ismétlődés lép fel, azaz $\exists k, n \in \mathbb{N}$: $a^k = a^{k+n}$:



Ha csoportról van szó, akkor csak $k = 0$ lehet, mert máskülönben $a \cdot a^{k-1} = a \cdot a^{k+n-1}$ ellentmondana a kancellativitásnak.

Csoportelem rendje

Csoportban tehát így fest a két lehetőség:

1. A hatványok mind különbözők:

$$1 = a^0,\ a^1,\ a^2,\ a^3,\ \ldots$$

   Ilyenkor azt mondjuk, hogy az a elem rendje végtelen.

2. Előbb-utóbb (mondjuk az n-edik lépésben) fellép az egységelem. Odáig nincs ismétlődés, utána viszont n-esével ismétlődnek a hatványok:

$$1 = a^0,\ a^1,\ a^2,\ a^3,\ \ldots,\ a^n = 1,\ a^{n+1} = a,\ a^{n+2} = a^2,\ \ldots$$

   Ilyenkor azt mondjuk, hogy az a elem rendje n.

4.32. Definíció.

Az $a \in G$ *elem rendje* az a legkisebb n pozitív egész szám, amelyre $a^n = 1$.
Ha nincs ilyen n, akkor a rendje végtelen. Az a elem rendjét $o(a)$ jelöli.
Egy véges *csoport rendjén* pedig elemeinek számát értjük.

Házi feladat a gyakorlatra

30. feladat. Határozza meg az alábbi csoportokban a megadott elemek rendjét.

(a) $i \in \mathbb{C}^*,\ \overline{2} \in \mathbb{Z}_5^*$

$o(i) = 4,\ o\left(\overline{2}\right) = 4$

(b) $(134)(52) \in S_5$

$o((134)(52)) = 6$

(c) $(1245)(234) \in S_5$

(d) $\overline{5} \in \mathbb{Z}_9^*$

(e) $\frac{\sqrt{2}}{2} - \frac{\sqrt{2}}{2}i \in \mathbb{C}^*$

A rend tulajdonságai

4.33. Állítás.

Ha az $a \in G$ elem rendje n (véges), akkor bármely $k, \ell \in \mathbb{Z}$ esetén

1. $a^k = 1 \iff n \mid k$;
2. $a^k = a^\ell \iff k \equiv \ell \pmod{n}$;
3. $o(a^k) = \dfrac{n}{\operatorname{lnko}(k, n)}$.

Bizonyítás.

Az első két állítás következik a korábbiakból. A harmadikhoz vizsgáljuk meg, hogy a^k mely hatványai adják az egységelemet:

$$(a^k)^j = 1 \overset{\text{Miért?}}{\iff} a^{kj} = 1 \overset{\text{Miért?}}{\iff} n \mid kj \overset{\text{Miért?}}{\iff} \frac{n}{\operatorname{lnko}(k, n)} \,\Big|\, j.$$

Tehát a^k „jó kitevői” pontosan $\dfrac{n}{\operatorname{lnko}(k, n)}$ többszörösei, ezért a^k rendje (vagyis a legkisebb jó kitevő) éppen $\dfrac{n}{\operatorname{lnko}(k, n)}$. □

Ciklikus csoportok

Jelölés.

Tetszőleges $a \in G$ esetén jelölje $[a]$ az a elem összes hatványainak halmazát (beleértve a negatív kitevőseket is!):

$$[a] = \{a^k : k \in \mathbb{Z}\} = \{\dots, a^{-3}, a^{-2}, a^{-1}, 1, a, a^2, a^3, \dots\}.$$

(Ezt nevezzük majd később az a elem által *generált részcsoportnak*; lásd a 4.47. Definíciót.)

4.34. Definíció.

A G csoportot *ciklikus csoportnak* nevezzük, ha egyetlen elemmel generálható, azaz létezik olyan $a \in G$, amelyre $[a] = G$.

4.35. Tétel.

Legyen G egy tetszőleges csoport és $a \in G$. Ha a rendje végtelen, akkor $([a]\,;\cdot) \cong (\mathbb{Z}, +)$, ha pedig $o(a) = n \in \mathbb{N}$, akkor $([a]\,;\cdot) \cong (\mathbb{Z}_n, +)$.

Bizonyítás.

1. Ha $o(a) = \infty$, akkor $\varphi\colon\ (\mathbb{Z}, +) \to ([a]\,;\cdot)\,,\ k \mapsto a^k$ izomorfizmus.
2. Ha $o(a) = n$, akkor $\varphi\colon\ (\mathbb{Z}_n, +) \to ([a]\,;\cdot)\,,\ \overline{k} \mapsto a^k$ izomorfizmus.

□

Ciklikus csoportok

4.36. Következmény.

Egy nemtriviális csoport akkor és csak akkor ciklikus, ha izomorf a $\mathbb{Z}$, $\mathbb{Z}_2$, $\mathbb{Z}_3$, $\mathbb{Z}_4$, ... csoportok valamelyikével.

4.37. Tétel.

Ciklikus csoport minden részcsoportja is ciklikus.

Bizonyítás.

Tfh. $G = [a]$ és $H \subseteq G$ maga is csoport. Ha $H \neq \{1\}$, akkor létezik olyan $k \in \mathbb{N}$, amelyre $a^k \in H$ (miért?); vegyük a legkisebb ilyen kitevőt. Cél: $[a^k] = H$.

- $[a^k] \overset{?}{\subseteq} H$: Mivel H zárt a szorzásra és az inverzképzésre, a^k minden hatványa is H-ban van, azaz $[a^k] \subseteq H$.
- $H \overset{?}{\subseteq} [a^k]$: Legyen $h \in H$; ÁMNTFH $h = a^j$. Osszuk el j-t maradékosan k-val: $j = qk + r$ és $0 \leq r < k$. Ha $r = 0$, akkor készen vagyunk: $a^j = \left(a^k\right)^q \in [a^k]$. Ha $r > 0$, akkor

$$a^r = a^{j-qk} = a^j \cdot \left(a^k\right)^{-q} \in H,$$

ami ellentmond k minimalitásának. □

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

□