

Csoportok

Waldhauser Tamás
2021 őszi félév

Állítás

Bármely grupoidban legföljebb egy egységelem létezhet.

Bizonyítás.

Ha e_1 és e_2 is egységelem az $(A; *)$ grupoidban, akkor

- ▶ $e_1 * e_2 = e_1$ (mert e_2 egységelem), és
- ▶ $e_1 * e_2 = e_2$ (mert e_1 egységelem).
- ▶ Tehát $e_1 = e_2$.



Állítás

Bármely monoidban egy elemnek legföljebb egy inverze lehet.

Bizonyítás.

Ha az a elemnek inverze b és c is, akkor

- ▶ $(b * a) * c = e * c = c$, és
- ▶ $b * (a * c) = b * e = b$.
- ▶ Tehát $b = (b * a) * c = b * (a * c) = c$.



Definíció

Legyen $*$ egy kétváltozós művelet a nemüres A halmazon.

- ▶ Azt mondjuk, hogy $*$ **invertálható** művelet, ha bármely $a, b \in A$ elemek esetén az $a * x = b$, illetve $y * a = b$ egyenleteknek **legalább** egy megoldása van.
- ▶ Azt mondjuk, hogy $*$ **kancellatív** művelet, ha bármely $a, b \in A$ elemek esetén az $a * x = b$, illetve $y * a = b$ egyenleteknek **legfeljebb** egy megoldása van.

Megjegyzés

A kancellativitás így is megfogalmazható: $\forall a, x_1, x_2, y_1, y_2 \in A$:

$$a * x_1 = a * x_2 \implies x_1 = x_2;$$

$$y_1 * a = y_2 * a \implies y_1 = y_2.$$

Megjegyzés

Az invertálhatóság azt jelenti, hogy a művelet táblázat minden sorában és minden oszlopában az A halmaz minden eleme **legalább** egyszer fellép.

A kancellativitás pedig azt jelenti, hogy minden sorban és minden oszlopban minden elem **legfeljebb** egyszer lép fel.

Definíció

Legyen $*$ egy kétváltozós művelet a nemüres A halmazon. Tetszőleges $a \in A$ esetén definiáljuk az a -val való **balról szorzást** és az a -val való **jobbról szorzást**:

$$\lambda_a: A \rightarrow A, x \mapsto a * x, \quad \rho_a: A \rightarrow A, x \mapsto x * a.$$

Állítás

Legyen $*$ egy kétváltozós művelet a nemüres A halmazon.

- ▶ $*$ invertálható $\iff \forall a \in A: \lambda_a$ és ρ_a szürjektív.
- ▶ $*$ kancellatív $\iff \forall a \in A: \lambda_a$ és ρ_a injektív.

Bizonyítás.

HF



Állítás

Véges alaphalmaz esetén az invertálhatóság és a kancellativitás egymással ekvivalens.

Bizonyítás.

HF (skatulya-elv)



Tétel

Csoport művelete mindig invertálható és kancellatív.

Bizonyítás.

Tfh. $(A; *)$ csoport, és legyen $a, b \in A$. Ekkor

$$a * x = b \quad \implies \quad x = a^{-1} * b \quad (\text{balról beszorzunk } a^{-1}\text{-zel});$$

$$x = a^{-1} * b \implies a * x = b \quad (\text{balról beszorzunk } a\text{-val}).$$

Hasonlóan: az $y * a = b$ egyenlet egyetlen megoldása $y = b * a^{-1}$. □

Tétel

Ha az A halmazon értelmezett $*$ kétváltozós művelet asszociatív és invertálható, akkor $(A; *)$ csoport.

Megjegyzés

A fenti tételben véges alaphalmaz esetén kicserélhetjük az invertálhatóságot a kancellativitással, de végtelen alaphalmaz esetén nem. Keressünk olyan végtelen kancellatív félcsoportot, ami nem csoport!

Az általános asszociativitás tétele

Ha $(S; \cdot)$ félcsoport, akkor minden $n \in \mathbb{N}$ és $a_1, \dots, a_n \in S$ esetén az $a_1 \cdot \dots \cdot a_n$ „szorzat” eredménye független a zárójelezéstől.

Bizonyítás. Tekintsük az a_1, \dots, a_n ($\in S; n \geq 1$) elemeket. Legyen

$$A = (\dots((a_1 \cdot a_2) \cdot a_3) \cdot \dots) \cdot a_n.$$

Jelöljük az a_1, \dots, a_n elemeknek (az adott sorrendben) egy tetszőleges zárójelezés melletti műveleti eredményét B -vel. Bizonyítandó, hogy $A=B$. A bizonyítást n szerinti teljes indukcióval végezzük. Az $n=1, 2$ esetben az állítás semmitmondó. Az $n=3$ esetben az állítás az asszociativitás miatt igaz. Legyen ezután $n \geq 4$, és tegyük fel az állítás helyességét k ($< n$) elemre. B minden esetben felírható $C \cdot D$ alakban, ahol C az a_1, \dots, a_r ($1 \leq r < n$) elemek, D pedig az a_{r+1}, \dots, a_n elemek valamilyen zárójelezés melletti műveleti eredménye. Mivel D -ben az elemek száma n -nél kevesebb, azért az indukciófeltevés miatt

$$D = E \cdot a_n$$

alakú, ahol E az a_{r+1}, \dots, a_{n-1} elemek műveleti eredménye valamilyen zárójelezés mellett. Ennélfogva az asszociativitás és az indukciófeltevés miatt igaz a következő:

$$B = C \cdot D = C \cdot (E \cdot a_n) = (C \cdot E) \cdot a_n = (\dots(a_1 \cdot a_2) \cdot \dots) \cdot a_n = A.$$

Ezzel a tételt bebizonyítottuk.

Dr. Szendrei János: Algebra és számelmélet (Tankönyvkiadó, 1989.)

Az általános kommutativitás tétele

Ha $(S; \cdot)$ kommutatív félcsoport, akkor minden $n \in \mathbb{N}$ és $a_1, \dots, a_n \in S$ esetén az $a_1 \cdot \dots \cdot a_n$ „szorzat” eredménye független a zárójelezéstől és az elemek sorrendjétől.

Hatványozás félcsoportban

Legyen $(A; *)$ egy félcsoport és $a \in A$, $n \in \mathbb{N}$. Az a elem n -edik hatványán az

$$\underbrace{a * \cdots * a}_n$$

elemet értjük. Attól függően, hogy a műveletet szorzással (multiplikatív írásmód) vagy összeadással (additív írásmód) jelöljük, a hatványozást és a hatványozás nevezetes azonosságait (amelyek pozitív egész kitevő esetén minden félcsoportban érvényesek) a következőképpen írjuk:

	multiplikatív írásmód	additív írásmód
művelet	$a \cdot b$	$a + b$
hatvány	a^n	na
$\forall a \in A \forall n \in \mathbb{N}$:	$a^n \cdot a^m = a^{n+m}$	$na + ma = (n + m)a$
$\forall a \in A \forall n, m \in \mathbb{N}$:	$(a^n)^m = a^{nm}$	$m(na) = (mn)a$
$\forall a, b \in A \forall n \in \mathbb{N}$		
ha a és b felcserélhetőek:	$(a \cdot b)^n = a^n \cdot b^n$	$n(a + b) = na + nb$

Hatványozás monoidban

Ha $(A; \cdot)$ egységelemes félcsoport, akkor tetszőleges $a \in A$ esetén a^0 legyen az egységelem, amit multiplikatív írásmód esetén szokás 1-gyel jelölni, tehát $a^0 = 1$. Additív írásmódnál is az egységelemként értelmezzük a nulladik hatványt: $0a = 0$. Így a korábbi azonosságok nemnegatív egész kitevőkre is érvényben maradnak.

Hatványozás csoportban

Ha $(A; \cdot)$ csoport, akkor tetszőleges $a \in A$ esetén a^{-n} legyen a inverzének n -edik hatványa: $a^{-n} = (a^{-1})^n$.

Additív írásmóddal így fest a negatív kitevős hatványozás: $(-n)a = n(-a)$.

A korábbi azonosságok egész kitevőkre is érvényben maradnak.

Állítás

Ha $(A; \cdot)$ csoport, akkor tetszőleges $a, b \in A$ esetén $(ab)^{-1} = b^{-1}a^{-1}$.

Bizonyítás.

Ellenőrizzük, hogy ab -nek valóban $b^{-1}a^{-1}$ az inverze:

$$(ab) \cdot (b^{-1}a^{-1}) = a \cdot (bb^{-1}) \cdot a^{-1} = a \cdot 1 \cdot a^{-1} = aa^{-1} = 1,$$

$$(b^{-1}a^{-1}) \cdot (ab) = b^{-1} \cdot (a^{-1}a) \cdot b = b^{-1} \cdot 1 \cdot b = b^{-1}b = 1.$$



Példák

Tetszőleges R gyűrű esetén $(R; +)$ Abel-csoport:

- ▶ $(\mathbb{C}; +)$, $(\mathbb{R}; +)$, $(\mathbb{Q}; +)$, $(\mathbb{Q}(\sqrt[3]{2}); +)$, $(\mathbb{Z}; +)$, $(\{\text{páros számok}\}; +)$, ...;
- ▶ $(T[x]; +)$ tetszőleges T testre (vagy akár csak gyűrűre);
- ▶ $(T^{n \times n}; +)$ tetszőleges T testre (vagy akár csak gyűrűre);
- ▶ $(\mathbb{Z}_n; +)$ tetszőleges $n \geq 2$ esetén.

Tetszőleges R egységelemes gyűrű esetén $(R^*; \cdot)$ csoport, ahol R^* a multiplikatív inverzzel rendelkező R -beli elemek halmaza (**egységscsoport**):

- ▶ $(\mathbb{C} \setminus \{0\}; \cdot)$, $(\mathbb{R} \setminus \{0\}; \cdot)$, $(\mathbb{Q} \setminus \{0\}; \cdot)$, $(\{1, -1\}; \cdot)$, ...;
- ▶ $T[x]$ egységscsoportja $(T \setminus \{0\}; \cdot)$ tetszőleges T testre;
- ▶ $T^{n \times n}$ egységscsoportja $(GL_n(T); \cdot)$ tetszőleges T testre:

$$GL_n(T) = \{A \in T^{n \times n} : \det(A) \neq 0\};$$

- ▶ $(\mathbb{Z}_n^*; \cdot)$ tetszőleges $n \geq 2$ esetén.

Példa

A komplex n -edik egységgyökök csoportot alkotnak:

$$E_n = (\{z \in \mathbb{C} : z^n = 1\}; \cdot).$$

Állítás

Az E_n csoport izomorf a \mathbb{Z}_n csoporttal: $(E_n; \cdot) \cong (\mathbb{Z}_n; +)$.

Bizonyítás.

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

Formálisan: A $\varphi: \mathbb{Z}_n \rightarrow E_n, \bar{k} \mapsto \text{cis } \frac{2k\pi}{n}$ leképezés izomorfizmus, mert ...

- ▶ φ jóldefiniált: $\bar{k} = \bar{\ell} \implies \text{cis } \frac{2k\pi}{n} = \text{cis } \frac{2\ell\pi}{n}$;
- ▶ φ injektív: $\text{cis } \frac{2k\pi}{n} = \text{cis } \frac{2\ell\pi}{n} \implies \bar{k} = \bar{\ell}$;
- ▶ φ szürjektív: $\forall z \in E_n \exists k \in \mathbb{Z} : z = \text{cis } \frac{2k\pi}{n}$;
- ▶ φ felcserélhető a műveetekkel:

$$(\bar{k} + \bar{\ell})\varphi = \overline{k + \ell}\varphi = \text{cis } \frac{2(k + \ell)\pi}{n} = \text{cis } \frac{2k\pi}{n} \cdot \text{cis } \frac{2\ell\pi}{n} = \bar{k}\varphi \cdot \bar{\ell}\varphi. \quad \square$$

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

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).

Példák

Tetszőleges A halmaz esetén A permutációi (vagyis az $A \rightarrow A$ bijekciók) csoportot alkotnak a leképezésszorzás műveletével. Az $A = \{1, 2, \dots, n\}$ esetben ezt a csoportot **n -edfokú szimmetrikus csoportnak** nevezzük és S_n -nel jelöljük.

Az S_n csoport részcsoportjait **permutációcsoportoknak** nevezzük.

Az S_n -beli páros permutációk csoportot alkotnak; ez az A_n **alternáló csoport**.

$$S_3 = \{\text{id}, (12), (13), (23), (123), (132)\}, \quad A_3 = \{\text{id}, (123), (132)\}.$$

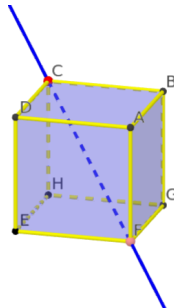
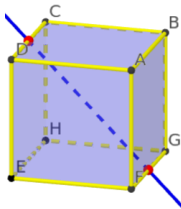
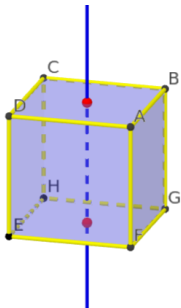
$$A_4 = \{\text{id}, (123), (132), (124), (142), (134), (143), (234), (243), \\ (12)(34), (13)(24), (14)(23)\}.$$

Az A_4 csoport alábbi részcsoportját **Klein-csoportnak** nevezzük:

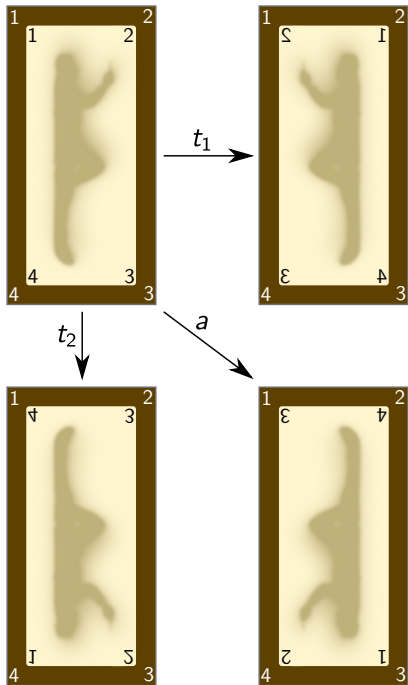
$$V = \{\text{id}, (12)(34), (13)(24), (14)(23)\}.$$

Példák

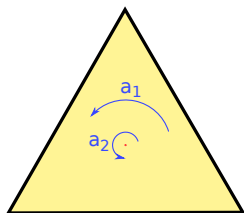
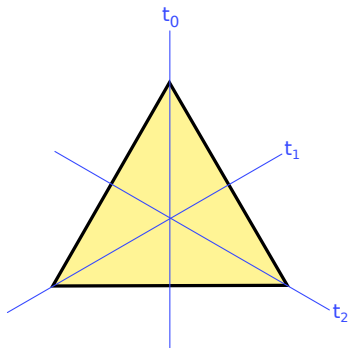
A sík (tér) egybevágósági transzformációi csoportot alkotnak a leképezésszorzás műveletével. Egy adott ponthalmazt önmagába képező egybevágóságok részcsoportot alkotnak ebben a csoportban; ezt nevezzük a ponthalmaz **szimmetriacsoportjának**. Ha csak az irányítástartó egybevágóságokat engedjük meg, akkor a ponthalmaz **mozgáscsoportját** kapjuk.



A kocka mozgáscsoportja (forgáscsoportja) izomorf S_4 -gyel.



\cdot	id	a	t_1	t_2	
id	id	a	t_1	t_2	
a	a	id	t_2	t_1	$\cong V$
t_1	t_1	t_2	id	a	
t_2	t_2	t_1	a	id	

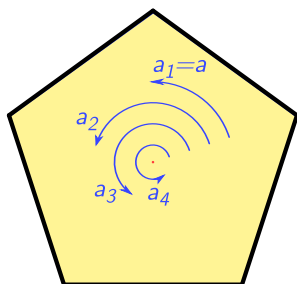


\cdot	a_0	a_1	a_2	t_0	t_1	t_2	
a_0	a_0	a_1	a_2	t_0	t_1	t_2	
a_1	a_1	a_2	a_0	t_1	t_2	t_0	
a_2	a_2	a_0	a_1	t_2	t_0	t_1	$\cong S_3$
t_0	t_0	t_2	t_1	a_0	a_2	a_1	
t_1	t_1	t_0	t_2	a_1	a_0	a_2	
t_2	t_2	t_1	t_0	a_2	a_1	a_0	

Definíció

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

Jelölje a_k a középpont körüli $\frac{2k\pi}{n}$ szögű forgatást ($k = 0, 1, \dots, n - 1$).

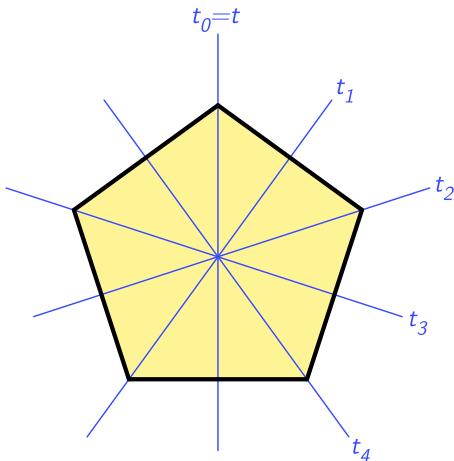


Vegyük észre, hogy $a_k = a_1^k$. A továbbiakban a_1 helyett egyszerűen csak a -t írunk. Így az n -szög mozgáscsoportja: $\{\text{id}, a, a^2, \dots, a^{n-1}\} \cong \mathbb{Z}_n$.

Definíció

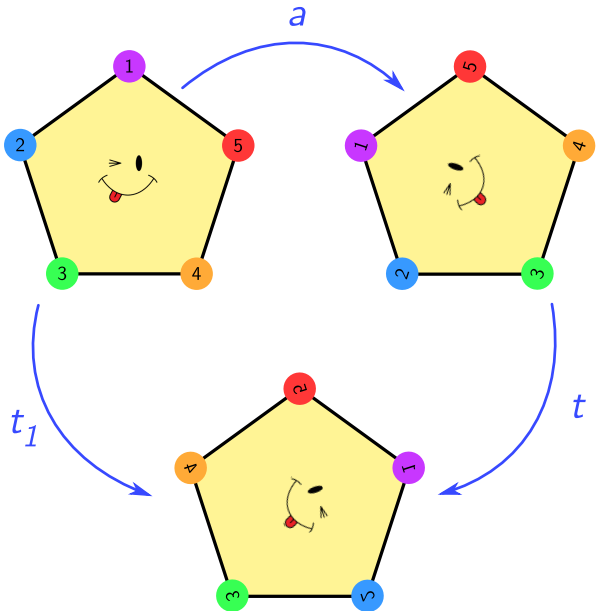
A szabályos n -szög szimmetriacsoportját **n -edfokú diédercsoportnak** nevezzük és D_n -nel jelöljük.

Legyenek a szimmetriatengelyekre vonatkozó tükrözések: t_0, t_1, \dots, t_{n-1} .



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

$$at = t_1$$



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

Tétel

A D_n csoportnak $2n$ eleme van: $D_n = \{\text{id}, a, a^2, \dots, a^{n-1}, t, at, a^2t, \dots, a^{n-1}t\}$,
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 $t, at, a^2t, \dots, a^{n-1}t$ transzformációk pedig tengelyes tükrözések
(két „szomszédos” tengely $\frac{\pi}{n}$ szöget zár be egymással).

Fennáll továbbá a $ta = a^{-1}t$ összefüggés. (Mert ta tükrözés, és így $tata = \text{id}$.)

- $D_n = \{\text{id}, a, a^2, \dots, a^{n-1}, t, at, a^2t, \dots, a^{n-1}t\}$
- $a^n = \text{id}$ és $t^2 = \text{id}$
- $ta = a^{-1}t$

Példa

$$D_3 = \begin{array}{c|cccccc} \cdot & a_0 & a_1 & a_2 & t_0 & t_1 & t_2 \\ \hline a_0 & a_0 & a_1 & a_2 & t_0 & t_1 & t_2 \\ a_1 & a_1 & a_2 & a_0 & t_1 & t_2 & t_0 \\ a_2 & a_2 & a_0 & a_1 & t_2 & t_0 & t_1 \\ t_0 & t_0 & t_2 & t_1 & a_0 & a_2 & a_1 \\ t_1 & t_1 & t_0 & t_2 & a_1 & a_0 & a_2 \\ t_2 & t_2 & t_1 & t_0 & a_2 & a_1 & a_0 \end{array} = \begin{array}{c|cccccc} \cdot & \text{id} & a & a^2 & t & at & a^2t \\ \hline \text{id} & \text{id} & a & a^2 & t & at & a^2t \\ a & a & a^2 & \text{id} & at & a^2t & t \\ a^2 & a^2 & \text{id} & a & a^2t & t & at \\ t & t & a^2t & at & \text{id} & a^2 & a \\ at & at & t & a^2t & a & \text{id} & a^2 \\ a^2t & a^2t & at & t & a^2 & a & \text{id} \end{array}$$

Példa

Számoljunk D_{15} -ben! Az eredmény $\text{id}, a, \dots, a^{14}, t, at, \dots, a^{14}t$ valamelyike legyen.

$$a^{153} = a^3, \quad a^{13} \cdot a^6t = a^4t, \quad a^{23}t \cdot a^{18} = a^5t, \quad a^7t \cdot a^{12}t = a^{10}$$

Definíció

Legyen $(A; *)$ egy grupoid és $\emptyset \neq B \subseteq A$. Azt mondjuk, hogy a B halmaz **zárt** a $*$ műveletre, ha

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

Ekkor van értelme megszorítani a $*$ műveletet a B halmazra, és így egy $(B; *)$ grupoidot kapunk, amelyet $(A; *)$ **részgrupoidjának** nevezünk.

Definíció

Ha $(G; \cdot)$ csoport, és $(H; \cdot)$ olyan részgrupoid, ami maga is csoport, akkor azt mondjuk, hogy H **részcsoportja** G -nek, és ezt így jelöljük: $H \leq G$.

Tétel

Bármely G csoport és $H \subseteq G$ esetén H akkor és csak akkor részcsoportja G -nek, ha

1. H zárt a szorzásra: $\forall h_1, h_2 \in H: h_1 \cdot h_2 \in H$;
2. H tartalmazza G egységelemét: $1 \in H$;
3. H zárt az inverzképzésre: $\forall h \in H: h^{-1} \in H$.

Tétel

Bármely G csoport és $H \subseteq G$ esetén H akkor és csak akkor részcsoporthja G -nek, ha

1. H zárt a szorzásra: $\forall h_1, h_2 \in H: h_1 \cdot h_2 \in H$;
2. H tartalmazza G egységelemét: $1 \in H$;
3. H zárt az inverzképzésre: $\forall h \in H: h^{-1} \in H$.

Bizonyítás.

Az nyilvánvaló, hogy a fenti feltételek teljesülése esetén H valóban részcsoporthja G -nek. A másik irány bizonyításához tfh. H részcsoporthja G -nek.

1. Ez világos.
2. Legyen 1_G a G csoport egységeleme, és legyen 1_H a H (rész)csoport egységeleme. Ekkor tetszőleges $h \in H$ esetén

$$1_G \cdot h = 1_H \cdot h, \text{ és így } 1_G = 1_H \in H.$$

3. Bármely $h \in H$ elemnek van inverze a H (rész)csoportban (legyen ez h') és a G csoportban is (legyen ez h^{-1}).

$$h^{-1} = h^{-1} \cdot 1 = h^{-1}(hh') = (h^{-1}h)h' = 1 \cdot h' = h' \in H. \quad \square$$

Állítás

Részcsoportok metszete is részcsoport: $H_1, H_2 \leq G \implies H_1 \cap H_2 \leq G$.

Bizonyítás.

1. szorzásra való zártság:

$$a, b \in H_1 \cap H_2 \implies a, b \in H_1, H_2 \implies a \cdot b \in H_1, H_2 \implies a \cdot b \in H_1 \cap H_2$$

2. egységelem:

$$1 \in H_1, H_2 \implies 1 \in H_1 \cap H_2$$

3. inverzképzésre való zártság:

$$a \in H_1 \cap H_2 \implies a \in H_1, H_2 \implies a^{-1} \in H_1, H_2 \implies a^{-1} \in H_1 \cap H_2$$

□

Megjegyzés

Az állítás igaz kettőnél több részcsoportra is (végtelen sokra is):

$$\forall i \in I: H_i \leq G \implies \bigcap_{i \in I} H_i \leq G.$$

Definíció

Legyen G egy csoport és $B \subseteq G$. A B halmaz által **generált részcsoport** a legrövidebb olyan részcsoport, ami tartalmazza B -t (jelölése $[B]$):

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

Megjegyzés

Az üres halmaz generátuma: $[\emptyset] = \{1\}$.

Állítás

Ha $\emptyset \neq B \subseteq G$, akkor $[B]$ azokból az elemekből áll, amelyek felépíthetők B elemeiből kiindulva a szorzás és az inverzképzés segítségével:

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

Definíció

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

Tétel

Az S_n szimmetrikus csoportot generálják a transzpozíciók, sőt, már a „szomszédos transzpozíciók” is:

$$S_n = [(12), (23), \dots, (n-1n)].$$

Tétel

Az A_n alternáló csoportot generálják a hármas ciklusok, sőt, már a „szomszédos hármasok” is:

$$A_n = [(123), (234), \dots, (n-2n-1n)].$$

Állítás

Tetszőleges G csoport és $a \in G$ esetén

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

Bizonyítás.

Triviális (HF). □

Példa

A \mathbb{C}^* csoportban:

k	\dots	-4	-3	-2	-1	0	1	2	3	4	5	6	7	\dots
2^k	\dots	$\frac{1}{16}$	$\frac{1}{8}$	$\frac{1}{4}$	$\frac{1}{2}$	1	2	4	8	16	32	64	128	\dots
i^k	\dots	1	i	-1	$-i$	1	i	-1	$-i$	1	i	-1	$-i$	\dots

Az első esetben a hatványok mind különbözőek, ezért $[2] \cong \mathbb{Z}$.

A második esetben négyes periodicitást tapasztalunk, ezért $[i] \cong \mathbb{Z}_4$.

Egy tetszőleges $(G; \cdot)$ csoportban egy a elemet hatványozva két eset lehetséges:

(1) A hatványok mind különbözőek.

Ekkor $\varphi: (\mathbb{Z}, +) \rightarrow ([a]; \cdot)$, $k \mapsto a^k$ izomorfizmus, ezért $([a]; \cdot) \cong (\mathbb{Z}, +)$.

- ▶ Szürjektivitás: $[a]$ minden eleme előáll a^k alakban.
- ▶ Injektivitás: feltettük, hogy $k \neq \ell$ esetén $a^k \neq a^\ell$.
- ▶ Művelettartás: $(k + \ell) \varphi = a^{k+\ell} = k\varphi \cdot \ell\varphi = a^k \cdot a^\ell$.

Egy tetszőleges $(G; \cdot)$ csoportban egy a elemet hatványozva két eset lehetséges:

(2) A hatványok között van ismétlődés: $\exists i < j : a^i = a^j \implies a^{j-i} = 1$.

Legyen n a legkisebb **pozitív** kitevő, amelyre $a^n = 1$.

Az $a^0, a^1, a^2, \dots, a^{n-1}$ hatványok páronként különbözőek (miért?)

és minden más hatvány ezek valamelyikével megegyezik:

$k = nq + r$ esetén $a^k = a^{nq+r} = (a^n)^q \cdot a^r = 1^q \cdot a^r = a^r$.

Ekkor $\varphi: (\mathbb{Z}_n, +) \rightarrow ([a]; \cdot), \bar{k} \mapsto a^k$ izomorfizmus,

ezért $([a]; \cdot) \cong (\mathbb{Z}_n, +)$.

- ▶ Jóldefiniáltság: $k \equiv \ell \pmod{n} \implies a^k = a^\ell$.
- ▶ Szürjektivitás: $[a]$ minden eleme előáll a^k ($k = 0, 1, \dots, n-1$) alakban.
- ▶ Injektivitás: $k \not\equiv \ell \pmod{n} \implies a^k \neq a^\ell$.
- ▶ Művelettartás: $(\bar{k} + \bar{\ell}) \varphi = \overline{k + \ell} \varphi = a^{k+\ell} = \bar{k} \varphi \cdot \bar{\ell} \varphi = a^k \cdot a^\ell$.

Definíció

Az $a \in G$ elem **rendjén** azt a legkisebb n pozitív egész számot értjük, amelyre $a^n = 1$. Ha nincs ilyen n , akkor azt mondjuk, hogy a rendje végtelen.

Az a elem rendjét $o(a)$ jelöli (olvasd: *ordó*):

$$o(a) = \min \{n \in \mathbb{N} : a^n = 1\} \quad (\min \emptyset = \infty \text{ megállapodással}).$$

Definíció

A G véges csoport **rendjén** elemeinek számát értjük.

Megjegyzés

Az a elem rendje nem más, mint az általa generált részcsoport rendje: $o(a) = |[a]|$.

Definíció

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

Tétel

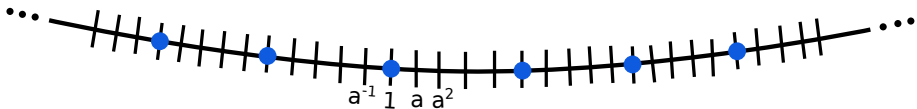
Egy csoport akkor és csak akkor ciklikus, ha izomorf a következő csoportok valamelyikével:

$$\{1\}, \mathbb{Z}_2, \mathbb{Z}_3, \mathbb{Z}_4, \dots, \mathbb{Z}.$$

Bizonyítás.

Ha G ciklikus, akkor $G = [a]$ alkalmas $a \in G$ elemre, és korábban már láttuk, hogy $[a] \cong \mathbb{Z}$ (első eset) vagy $[a] \cong \mathbb{Z}_{o(a)}$ (második eset).

Fordítva, a felsorolt csoportok valóban ciklikusak: $\mathbb{Z}_n = [\bar{1}]$ és $\mathbb{Z} = [1]$. □



Tétel

Ciklikus csoport minden részcsoportja is ciklikus.

Bizonyítás.

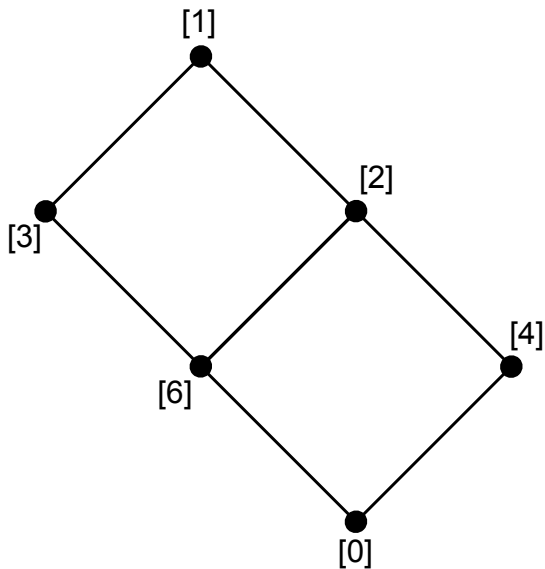
Tfh. $G = [a]$ és $H \leq G$. Ha $H \neq \{1\}$, akkor létezik olyan $k \in \mathbb{N}$, amelyre $a^k \in H$ (miért?); vegyük a legkisebb ilyen kitevőt. Cél: $[a^k] = H$.

- ▶ $[a^k] \stackrel{?}{\subseteq} H$: Mivel H zárt a szorzásra és az inverzképzésre, a^k minden hatványa is H -ban van, azaz $[a^k] \subseteq H$.
- ▶ $H \stackrel{?}{\subseteq} [a^k]$: 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: $a^j = (a^k)^q \in [a^k]$. Ha $r > 0$, akkor

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

ami ellentmond k minimalitásának. □

\mathbb{Z}_{12} részcsoporthálója



\mathbb{Z}_n részcsoportjai

- ▶ Bármely $\bar{k} \in \mathbb{Z}_n$ esetén $[\bar{k}] = [\bar{d}]$, ahol $d = \text{Inko}(k, n)$.



Tetszőleges $\bar{b} \in \mathbb{Z}_n$ esetén

$$\begin{aligned} \bar{b} \in [\bar{k}] &\iff \exists x \in \mathbb{Z}: \bar{b} = x\bar{k} \\ &\iff \exists x \in \mathbb{Z}: b \equiv x \cdot k \pmod{n} \\ &\iff d = \text{Inko}(k, n) \mid b \\ &\iff \exists \ell \in \mathbb{Z}: b = \ell \cdot d \\ &\iff \bar{b} \in [\bar{d}]. \end{aligned}$$

- ▶ \mathbb{Z}_n részcsoportjai kölcsönösen egyértelműen megfelelnek n osztóinak:

$$d \mid n \rightsquigarrow [\bar{d}] \cong \mathbb{Z}_{n/d}.$$

- ▶ \mathbb{Z}_n -nek $\varphi(n)$ db generátoreleme van:

$$[\bar{k}] = \mathbb{Z}_n \iff \text{Inko}(k, n) = 1.$$

A rend tulajdonságai

Tudjuk, hogy ha $o(a) = n$, akkor $[a] \cong \mathbb{Z}_n$, az $a^k \mapsto \bar{k}$ izomorfizmus mellett.

$[a]$	\mathbb{Z}_n
a^k	\bar{k}
$a^k = a^\ell \iff k \equiv \ell \pmod{n}$	$\bar{k} = \bar{\ell} \iff k \equiv \ell \pmod{n}$
$a^k = 1 \iff n \mid k$	$\bar{k} = \bar{0} \iff n \mid k$
$o(a^k) = [a^k] = \frac{n}{\text{Inko}(k,n)}$	$ \bar{k} = \bar{d} = \frac{n}{d},$ ahol $d = \text{Inko}(k,n)$

Primitív egységgyökök

Tetszőleges $z \in \mathbb{C}^*$ komplex szám esetén

$$o(z) = n \iff |[z]| = n \iff [z] = E_n.$$

Az ilyen tulajdonságú számokat nevezzük **primitív n -edik egységgyököknek**.

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

Definíció

A G csoport nemüres részhalmazait **komplexusoknak** nevezzük. Komplexusok szorzatát és inverzét elemenként értelmezzük:

$$AB = \{ab : a \in A, b \in B\}, \quad A^{-1} = \{a^{-1} : a \in A\} \quad (\emptyset \neq A, B \subseteq G).$$

Egyelemű komplexusok esetén az alábbi egyszerűsített jelölést használjuk:

$$\{a\}B = aB, \quad B\{a\} = Ba \quad (a \in G, \emptyset \neq B \subseteq G).$$

Tétel

Egy $H \subseteq G$ komplexus akkor és csak akkor részcsoportha, ha

$$HH \subseteq H, \quad 1 \in H, \quad H^{-1} \subseteq H.$$

Bizonyítás.

Ez csak a részcsoporthokat leíró korábbi tétel átfogalmazása. □

Megjegyzés

Ha $H \leq G$, akkor nemcsak $HH \subseteq H$, de $H \subseteq HH$ is teljesül, mert $H = \{1\}H \subseteq HH$, tehát $HH = H$. Hasonlóan $H^{-1} = H$ is teljesül.

Definíció

Tetszőleges $H \leq G$ és $g \in G$ esetén a gH , illetve Hg komplexusokat a g elem H szerinti bal, illetve jobb oldali **mellékosztályának** nevezzük.

Példa

Határozzuk meg a $G = \mathbb{Z}_6$ csoportban a $H = \{\bar{0}, \bar{3}\}$ részcsoporthoz tartozó mellékosztályokat.

$$\begin{aligned}\bar{0} + H &= \{\bar{0}, \bar{3}\}, & \bar{1} + H &= \{\bar{1}, \bar{4}\}, & \bar{2} + H &= \{\bar{2}, \bar{5}\}, \\ \bar{3} + H &= \{\bar{3}, \bar{0}\}, & \bar{4} + H &= \{\bar{4}, \bar{1}\}, & \bar{5} + H &= \{\bar{5}, \bar{2}\}.\end{aligned}$$

Példa

Határozzuk meg a $G = \mathbb{Z}$ csoportban a $H = \{3k : k \in \mathbb{Z}\}$ részcsoporthoz tartozó mellékosztályokat.

$$\bar{0} + H = \{3k : k \in \mathbb{Z}\}, \quad \bar{1} + H = \{3k + 1 : k \in \mathbb{Z}\}, \quad \bar{2} + H = \{3k + 2 : k \in \mathbb{Z}\}.$$

Tetszőleges a egész szám esetén, $a + H$ nem más, mint a modulo 3 maradékosztálya. Következésképp

$$a + H = b + H \iff a \equiv b \pmod{3} \iff 3 \mid a - b \iff a - b \in H.$$

Tétel

Legyen $H \leq G$, és definiáljunk a G halmazon egy \sim relációt:

$$a \sim b \iff ab^{-1} \in H.$$

Ekkor \sim ekvivalenciareláció, és egy $a \in G$ elem ekvivalenciaosztálya Ha .

Bizonyítás.

HF



Következmény

Tetszőleges $H \leq G$ esetén a H szerinti jobb oldali mellékosztályok a G halmaz egy osztályozását alkotják. Hasonló érvényes a bal oldali mellékosztályokra is.

Példa

Határozzuk meg a $G = \mathbb{Z}_{13}^*$ csoportban a $H = [\bar{5}] = \{\bar{1}, \bar{5}, \bar{8}, \bar{12}\}$ részcsoporthoz tartozó mellékosztályokat.

$$\bar{1} \cdot H = \{\bar{1}, \bar{5}, \bar{8}, \bar{12}\} = \bar{5} \cdot H = \bar{8} \cdot H = \bar{12} \cdot H,$$

$$\bar{2} \cdot H = \{\bar{2}, \bar{10}, \bar{3}, \bar{11}\} = \bar{10} \cdot H = \bar{3} \cdot H = \bar{11} \cdot H,$$

$$\bar{4} \cdot H = \{\bar{4}, \bar{7}, \bar{6}, \bar{9}\} = \bar{7} \cdot H = \bar{6} \cdot H = \bar{9} \cdot H.$$

Példa

Határozzuk meg a $G = S_3$ csoportban a $H = \{\text{id}, (23)\}$ részcsoporthoz tartozó jobb oldali mellékosztályokat.

$$H \cdot \text{id} = \{\text{id}, (23)\} = (23) \cdot H,$$

$$H \cdot (12) = \{(12), (123)\} = H \cdot (123),$$

$$H \cdot (13) = \{(13), (132)\} = H \cdot (132).$$

Példa

Határozzuk meg a $G = S_3$ csoportban a $H = \{\text{id}, (23)\}$ részcsoporthoz tartozó bal oldali mellékosztályokat.

$$\text{id} \cdot H = \{\text{id}, (23)\} = (23) \cdot H,$$

$$(12) \cdot H = \{(12), (132)\} = (132) \cdot H,$$

$$(13) \cdot H = \{(13), (123)\} = (123) \cdot H.$$

Definíció

A G véges csoport H részcsoportja szerinti bal (vagy jobb) oldali mellékosztályok számát H **indexének** nevezzük. Jelölés: $[G : H]$.

Lagrange tétele

Tetszőleges G véges csoport és H részcsoport esetén

$$|G| = |H| \cdot [G : H].$$

Bizonyítás.

Bármely $g \in G$ esetén

$$\lambda_g: H \rightarrow gH, h \mapsto gh$$

bijektív leképezés (miért?), ezért $|gH| = |H|$, azaz a mellékosztályok mind egyforma méretűek (akkorák, mint H).

Tehát a mellékosztályok a G halmazt felbontják $[G : H]$ darab $|H|$ -elemű részhalmozra, és így $|G| = |H| \cdot [G : H]$. □

Következmény

Véges csoportban minden részcsoport rendje osztója a csoport rendjének: $|H| \mid |G|$.

Következmény

Véges csoportban minden elem rendje osztója a csoport rendjének: $o(a) \mid |G|$.

Bizonyítás.

Alkalmazzuk a fenti következményt a $H = [a]$ részcsoporthoz: $o(a) = |[a]| \mid |G|$. \square

Következmény

Ha G egy n -elemű csoport, akkor minden $a \in G$ elemre $a^n = 1$.

Bizonyítás.

Alkalmazzuk a fenti következményt: $a^n = (a^{o(a)})^{n/o(a)} = 1^{n/o(a)} = 1$. \square

Következmény (Euler–Fermat-tétel)

Ha a és m relatív prímek ($m \geq 2$), akkor $a^{\varphi(m)} \equiv 1 \pmod{m}$.

Bizonyítás.

Alkalmazzuk a fenti következményt a $G = \mathbb{Z}_m^*$ csoportra (itt $|G| = \varphi(m)$). \square

Következmény

Ha G egy n -elemű csoport, akkor minden $a \in G$ elemre $a^{-1} = a^{n-1}$.

Következmény

Minden prímmrendű csoport ciklikus.

Bizonyítás.

Tfh. $|G| = p$ prímszám. Legyen $g \in G \setminus \{1\}$ tetszőleges elem.
Ekkor $o(g) = p$ (miért?), és így $\langle g \rangle = G$. □

Tétel

A kis elemszámú csoportok (izomorfia erejéig) a következők:

1. egyelemű: $\{1\}$;
2. kételemű: \mathbb{Z}_2 ;
3. háromelemű: \mathbb{Z}_3 ;
4. négyelemű: \mathbb{Z}_4, V ;
5. ötelemű: \mathbb{Z}_5 ;
6. hatelemű: $\mathbb{Z}_6, D_3 \cong S_3$;
7. hételemű: \mathbb{Z}_7 .

\mathbb{Z}_n elemeinek rend-szerezése

Legyen $r(d)$ a d -edrendű elemek száma \mathbb{Z}_n -ben. Mivel minden d -edrendű elem egy d -elemű ciklikus részcsoporthot generál, és minden d -elemű ciklikus részcsoporthnak $\varphi(d)$ generátora van,

$$r(d) = \varphi(d) \cdot (\text{a } d\text{-elemű ciklikus részcsoporthok száma}).$$

- ▶ Ha $d \nmid n$, akkor $r(d) = 0$ (Lagrange).
- ▶ Ha $d \mid n$, akkor egyetlen d -elemű ciklikus részcsoporth van, ezért $r(d) = \varphi(d)$.

A rendjeik szerint összeszámolva az elemeket, ezt kapjuk:

$$|\mathbb{Z}_n| = n = \sum_{d|n} r(d) = \sum_{d|n} \varphi(d).$$

\mathbb{Z}_p^* elemeinek rend-szerezése

Legyen p prímszám, és legyen $r(d)$ a d -edrendű elemek száma \mathbb{Z}_p^* -ban.

- ▶ Ha $d \nmid p-1$, akkor $r(d) = 0$ (Lagrange).
- ▶ Ha $H \leq \mathbb{Z}_p^*$ egy d -elemű ciklikus részcsoport, akkor $\forall h \in H: h^d = \bar{1}$.
Tehát H elemei mind gyökei az $x^d - \bar{1} \in \mathbb{Z}_p[x]$ polinomnak.
Mivel \mathbb{Z}_p test, a polinomnak nem lehet több gyöke, mint amennyi a fokszáma.
Ezért legfeljebb egy d -elemű ciklikus részcsoport létezhet.
Következésképp $r(d) = \varphi(d)$ vagy $r(d) = 0$.

A rendjeik szerint összeszámolva az elemeket, ezt kapjuk:

$$|\mathbb{Z}_p^*| = p-1 = \sum_{d|p-1} r(d) \leq \sum_{d|p-1} \varphi(d) = p-1.$$

Ha akár csak egyetlen $d \mid p-1$ esetén is $r(d) = 0$ lenne, akkor a $p-1 < p-1$ ellentmondást kapnánk. Tehát

$$\forall d \mid p-1: r(d) = \varphi(d).$$

Tétel

Ha p prímszám, akkor minden $d \mid p - 1$ esetén létezik d -edrendű elem \mathbb{Z}_p^* -ban.

Következmény

Ha p prímszám, akkor \mathbb{Z}_p^* ciklikus csoport; a generátorelemeinek száma $\varphi(p - 1)$.

Definíció

Ha $\bar{g} \in \mathbb{Z}_m^*$ hatványaiként minden modulo m redukált maradékosztály megkapható (azaz $\mathbb{Z}_m^* = [\bar{g}]$), akkor azt mondjuk, hogy g **primitív gyök** modulo m .

Tétel

Akkor és csak akkor létezik primitív gyök modulo m (azaz \mathbb{Z}_m^* akkor és csak akkor ciklikus), ha $m = 1, 2, 4, p^\alpha$ vagy $2p^\alpha$ (p páratlan prím).

Példa

Nincs primitív gyök modulo 100, azaz \mathbb{Z}_{100}^* -ban nincs 40-edrendű elem.

Meg lehet mutatni (HF), hogy $a \perp 100 \implies a^{20} \equiv 1 \pmod{100}$.

Megjegyzés

Ha $m \perp 10$, akkor $\frac{1}{m}$ végtelen periodikus tizedes tört, és a periódus hossza nem más, mint $\overline{10}$ rendje a \mathbb{Z}_m^* csoportban.

Ha g primitív gyök modulo m , akkor $\mathbb{Z}_m^* \cong \mathbb{Z}_{\varphi(m)}$ az alábbi izomorfizmus mellett:

$$\begin{aligned} \psi : \mathbb{Z}_{\varphi(m)} &\longrightarrow \mathbb{Z}_m^* \\ i &\longmapsto g^i \end{aligned}$$

$$\begin{aligned} \mathbb{Z}_{\varphi(m)} &\longleftarrow \mathbb{Z}_m^* : \psi^{-1} \\ \text{ind}_g a &\longleftarrow a \end{aligned}$$

Definíció

Ha g primitív gyök modulo m és $a \perp m$, akkor létezik olyan (modulo $\varphi(m)$ egyértelműen meghatározott) i egész szám, amelyre $g^i \equiv a \pmod{m}$. Ezt az i kitevőt az a egész szám g alapú **indexének** nevezzük (az m modulusra nézve). Jelölés: $i = \text{ind}_g a$.

Példa

Indextáblázat a $g = 2$ primitív gyökkel a $p = 11$ modulushoz:

i	0	1	2	3	4	5	6	7	8	9
2^i	1	2	4	8	5	10	9	7	3	6

a	1	2	3	4	5	6	7	8	9	10
$\text{ind}_g a$	0	1	8	2	4	9	7	3	6	5

Állítás

Legyen g primitív gyök modulo m , és legyen $k, a, b \in \mathbb{Z}$, $a, b \perp m$.

1. $\text{ind}_g 1 \equiv 0 \pmod{\varphi(m)}$
2. $\text{ind}_g(ab) \equiv \text{ind}_g a + \text{ind}_g b \pmod{\varphi(m)}$
3. $\text{ind}_g(ab^{-1}) \equiv \text{ind}_g a - \text{ind}_g b \pmod{\varphi(m)}$
4. $\text{ind}_g(a^k) \equiv k \cdot \text{ind}_g a \pmod{\varphi(m)}$

Bizonyítás.

Következik abból, hogy $\psi^{-1}: \mathbb{Z}_m^* \rightarrow \mathbb{Z}_{\varphi(m)}$, $a \mapsto \text{ind}_g a$ izomorfizmus.

(Belátható közvetlenül is az index definíciójából, a logaritmus azonosságaihoz hasonlóan.) □

Példa

Oldjuk meg az indextáblázat segítségével az $x^6 \equiv 5 \pmod{11}$ kongruenciát.

a	1	2	3	4	5	6	7	8	9	10
$\text{ind}_g a$	0	1	8	2	4	9	7	3	6	5

A megoldást kereshetjük $x \equiv 2^i \pmod{11}$ alakban (ugye?).

$$x^6 \equiv 5 \pmod{11} \iff 2^{6i} \equiv 2^4 \pmod{11}$$

$$\iff 6i \equiv 4 \pmod{10}$$

$$\iff i \equiv 4 \pmod{5}$$

$$\iff i \equiv 4, 9 \pmod{10}$$

$$\iff 2^i \equiv 5, 6 \pmod{11}$$

$$\iff x \equiv 5, 6 \pmod{11}$$

Definíció

Azt mondjuk, hogy az a egész szám **n -edik hatványmaradék** modulo m , ha van olyan x egész szám, amelyre $x^n \equiv a \pmod{m}$.

Tétel

Legyen g primitív gyök modulo m és tfh. $a \perp m$. Ekkor a pontosan akkor n -edik hatványmaradék modulo m , ha $\text{Inko}(n, \varphi(m)) \mid \text{ind}_g a$.

Bizonyítás.

Az $x^n \equiv a \pmod{m}$ kongruencia megoldását kereshetjük $x \equiv g^i \pmod{m}$ alakban.

$$\begin{aligned}x^n \equiv a \pmod{m} &\iff g^{ni} \equiv g^{\text{ind}_g a} \pmod{m} \\ &\iff ni \equiv \text{ind}_g a \pmod{\varphi(m)}\end{aligned}$$

Ez egy lineáris kongruencia (az i ismeretlenre nézve), amelynek akkor és csak akkor van megoldása, ha $\text{Inko}(n, \varphi(m)) \mid \text{ind}_g a$. □

Definíció

Azt mondjuk, hogy az a egész szám **négyzetes maradék** modulo m , ha van olyan x egész szám, amelyre $x^2 \equiv a \pmod{m}$. Ellenkező esetben azt mondjuk, hogy a **négyzetes nemmaradék** modulo m .

Tétel

Legyen p páratlan prím, g primitív gyök modulo p és tfh. $p \nmid a$. Ekkor a pontosan akkor négyzetes maradék modulo p , ha $\text{ind}_g a$ páros.

Bizonyítás.

Az előző tételt alkalmazva azt kapjuk, hogy a pontosan akkor négyzetes maradék modulo p , ha $\text{lnc}_o(2, p-1) \mid \text{ind}_g a$. Mivel p páratlan, $\text{lnc}_o(2, p-1) = 2$.



Definíció

Tetszőleges p páratlan prímszám és p -vel nem osztható a egész szám esetén értelmezzük az $\left(\frac{a}{p}\right)$ **Legendre-szimbólumot** a következőképpen:

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & \text{ha } a \text{ négyzetes maradék mod } p; \\ -1, & \text{ha } a \text{ négyzetes nemmaradék mod } p. \end{cases}$$

Tétel (Euler-kritérium)

Ha p páratlan prímszám és $p \nmid a$, akkor

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}.$$

Következmény

Tetszőleges p páratlan prímszám és p -vel nem osztható a, b egész számok esetén teljesülnek az alábbiak:

1. $a \equiv b \pmod{p} \implies \left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$;
2. $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right) \left(\frac{b}{p}\right)$;
3. $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = \begin{cases} 1, & \text{ha } p \equiv 1 \pmod{4}; \\ -1, & \text{ha } p \equiv 3 \pmod{4}. \end{cases}$

Tétel (négyzetes reciprocitás)

Tetszőleges p, q különböző páratlan prímszámok esetén

$$\left(\frac{p}{q}\right) \left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2} \frac{q-1}{2}} = \begin{cases} 1, & \text{ha } p \equiv 1 \pmod{4} \text{ vagy } q \equiv 1 \pmod{4}; \\ -1, & \text{ha } p \equiv 3 \pmod{4} \text{ és } q \equiv 3 \pmod{4}. \end{cases}$$

Tétel

Ha p páratlan prímszám, akkor

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} 1, & \text{ha } p \equiv 1, 7 \pmod{8}; \\ -1, & \text{ha } p \equiv 3, 5 \pmod{8}. \end{cases}$$

Tétel (Cayley-reprezentáció)

Minden csoport izomorf egy permutációcsoporttal (azaz egy szimmetrikus csoport részcsoporthal).

Bizonyítás.

Legyen G egy tetszőleges csoport, és tekintsük a G halmaz összes permutációi alkotta S_G szimmetrikus csoportot. Meg fogjuk mutatni, hogy G izomorf S_G egy részcsoporthal. Tudjuk, hogy a $\rho_g: G \rightarrow G, x \mapsto xg$ leképezés bármely $g \in G$ elemre bijektív, tehát $\rho_g \in S_G$. Minden $g, h \in G$ esetén teljesülnek az alábbiak:

- $\rho_g \rho_h = \rho_{gh}$ $(\forall x \in G: x(\rho_g \rho_h) = (x\rho_g)\rho_h = (xg)h = x(gh) = x\rho_{gh})$
- $\rho_1 = \text{id}$ $(\forall x \in G: x\rho_1 = x1 = x = x \text{id})$
- $\rho_g^{-1} = \rho_{g^{-1}}$ $(\rho_g \rho_{g^{-1}} = \rho_{gg^{-1}} = \rho_1 = \text{id})$
- $\rho_g = \rho_h \implies g = h$ $(\rho_g = \rho_h \implies g = 1g = 1\rho_g = 1\rho_h = 1h = h)$

Mindezekből következik, hogy a $\{\rho_g : g \in G\}$ halmaz részcsoporthal alkot az S_G csoportban (1,2,3), és a

$$\rho: G \rightarrow \{\rho_g : g \in G\}, \quad g \mapsto \rho_g$$

leképezés izomorfizmus (1,4).

