Algebra és számelmélet előadás

Waldhauser Tamás
2016. november 24.

Házi feladat a gyakorlatra

34. feladat. Határozza meg a G csoportban a B részhalmaz által generált részcsoportot.

(a) $G = \mathbb{Z},\ B = \{30, 42, 105\}$ $\quad [B] = \{3k : k \in \mathbb{Z}\} \cong \mathbb{Z}$

$G = D_{12},\ B = \{a^3, a^2 t\}$ $\quad [B] = \{\mathrm{id},\ a^3,\ a^6,\ a^9,\ a^2 t,\ a^5 t,\ a^8 t,\ a^{11} t\} \cong D_4$

(b) $G = \mathbb{Z}_{30},\ B = \{\overline{6}, \overline{10}\}$

$[B] = \{\overline{0}, \overline{2}, \overline{4}, \overline{6, 8}, \overline{10}, \overline{12}, \overline{14}, \overline{16}, \overline{18}, \overline{20}, \overline{22}, \overline{24}, \overline{26}, \overline{28}\} \cong \mathbb{Z}_{15}$

$G = S_4,\ B = \{(1234), (13)\}$

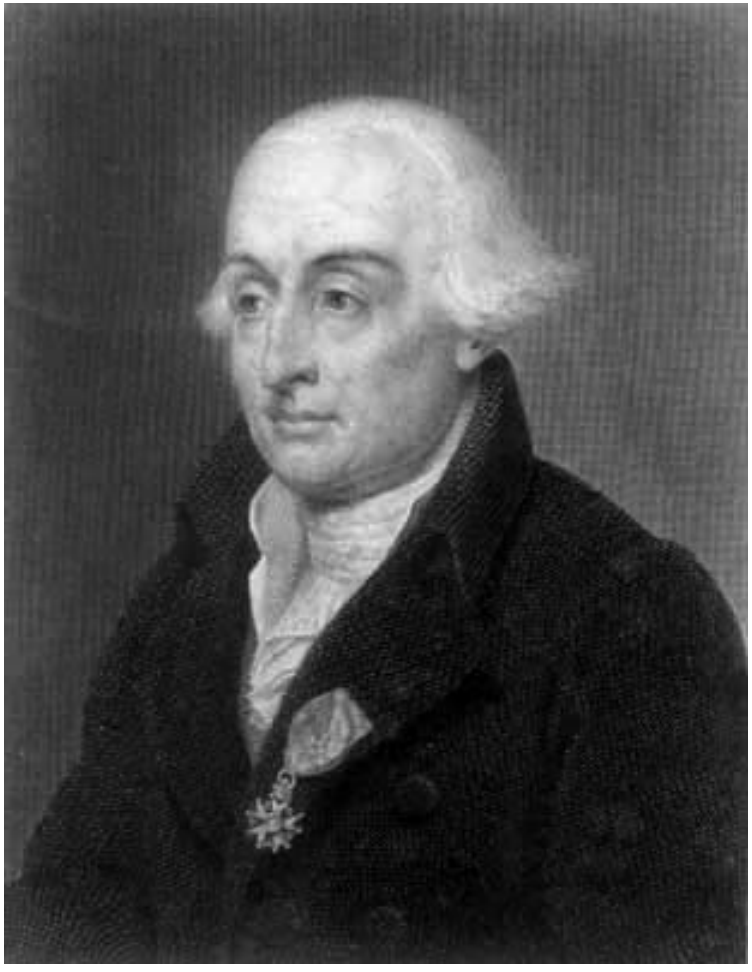
$[B] = \{\mathrm{id}, (1234), (13)(24), (1432), (13), (24), (12)(34), (14)(23)\} \cong D_4$

(c) $G = \mathbb{Z}_{31},\ B = \{\overline{6}, \overline{10}\}$

(d) $G = \mathbb{C}^*,\ B = \left\{i,\ \frac{1}{2} + \frac{\sqrt{3}}{2} i\right\}$

(e) $G = D_{10},\ B = \{a^4, a^5 t\}$

Lagrange tétele



Joseph-Louis Lagrange

(1736, Torino – 1813, Párizs)

Mellékosztályok

4.51. Tétel.

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

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

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

$$aH = \{ah \colon h \in H\}.$$

4.52. Definíció.

Az aH halmazt az a elem H szerinti *bal oldali mellékosztályának* nevezzük.

4.53. Következmény.

Egy $H \leq G$ részcsoport szerinti bal oldali mellékosztályok a G csoport egy osztályozását alkotják.

4.54. Megjegyzés.

Hasonló módon definiálhatóak a *Ha jobb oldali mellékosztályok*, amelyek szintén osztályozást alkotnak.

Mellékosztályok

Megjegyzés.

Ha G Abel-csoport, akkor persze $aH = Ha$ minden $a \in G$ esetén.
Ha G nem kommutatív, akkor is előfordulhat, hogy a H részcsoport szerinti bal oldali mellékosztályozás megegyezik a jobb oldalival. Az ilyen részcsoportokat normálosztóknak nevezzük; ezek kitüntetett szerepet játszanak a csoportelméletben.

Példa.

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

$$\overline{0} + H = \{\overline{0}, \overline{3}\}, \ \overline{1} + H = \{\overline{1}, \overline{4}\}, \ \overline{2} + H = \{\overline{2}, \overline{5}\}$$
$$\overline{3} + H = \{\overline{3}, \overline{0}\}, \ \overline{4} + H = \{\overline{4}, \overline{1}\}, \ \overline{5} + H = \{\overline{5}, \overline{2}\}$$

A mellékosztályozás: $\{\{\overline{0}, \overline{3}\}, \{\overline{1}, \overline{4}\}, \{\overline{2}, \overline{5}\}\}$.

Példa.

Határozzuk meg a $G = \mathbb{Z}$ csoportban a $H = [m]$ részcsoporthoz tartozó mellékosztályokat.

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

Tehát itt a mellékosztályok éppen a modulo m maradékosztályok.

Mellékosztályok

Példa.

Határozzuk meg a $H = \{\mathrm{id}, (23)\} \leq S_3$ részcsoporthoz tartozó bal és jobb oldali mellékosztályokat.

- Bal oldali mellékosztályok:

  $$\mathrm{id} \cdot H = \{\mathrm{id}, (23)\} = (23) \cdot H,$$
  $$(13) \cdot H = \{(13), (123)\} = (123) \cdot H$$
  $$(12) \cdot H = \{(12), (132)\} = (132) \cdot H.$$

  A bal oldali mellékosztályozás: $\{\{\mathrm{id}, (23)\}, \{(13), (123)\}, \{(12), (132)\}\}$.

- Jobb oldali mellékosztályok:

  $$H \cdot \mathrm{id} = \{\mathrm{id}, (23)\} = H \cdot (23),$$
  $$H \cdot (13) = \{(13), (132)\} = H \cdot (132)$$
  $$H \cdot (12) = \{(12), (123)\} = H \cdot (123),$$

  A jobb oldali mellékosztályozás: $\{\{\mathrm{id}, (23)\}, \{(13), (132)\}, \{(12), (123)\}\}$.

Mellékosztályok

Példa.

Legyen A egy tetszőleges halmaz, $G \leq S_A$, és legyen H az $a \in A$ elem stabilizátora:

$$H = \{\pi \in G \colon a\pi = a\}.$$

Tetszőleges $\rho, \sigma \in G$ esetén

$$\begin{aligned} H\rho = H\sigma \iff \rho\sigma^{-1} \in H &\iff a\left(\rho\sigma^{-1}\right) = a \\ &\iff (a\rho)\,\sigma^{-1} = a \\ &\iff a\rho = a\sigma. \end{aligned}$$

Tehát két G-beli permutáció akkor és csak akkor tartozik ugyanabba a jobb oldali mellékosztályba, ha ugyanoda viszik az a elemet.

Hasonlóan belátható, hogy a bal oldali mellékosztályozásnál aszerint vannak osztályozva a permutációk, hogy melyik elemet viszik a-ba.

Részcsoport indexe

4.55. Definíció.

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

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.

Bizonyítás.

Legyen $\tau \in S_n$ egy tetszőleges páratlan permutáció, pl. $\tau = (12)$. Célunk igazolni, hogy $\tau \cdot A_n = S_n \setminus A_n$.

- $\tau \cdot A_n \subseteq S_n \setminus A_n$: Ha $\pi \in A_n$, akkor $\tau \cdot \pi \in S_n \setminus A_n$ (miért?).
- $\tau \cdot A_n \supseteq S_n \setminus A_n$: Ha $\rho \in S_n \setminus A_n$, akkor létezik olyan $\pi \in A_n$, amelyre $\rho = \tau \cdot \pi$ (valóban, $\pi = \tau^{-1} \cdot \rho \in A_n$).

Tehát két mellékosztály van: $\mathrm{id} \cdot A_n = A_n$ és $\tau \cdot A_n = S_n \setminus A_n$, így $[S_n : A_n] = 2$. □

Lagrange tétele

4.56. Tétel (Lagrange tétele).

Tetszőleges G véges csoport és $H \leq G$ részcsoport esetén $|G| = |H| \cdot [G : H]$.

Bizonyítás.

Mindegyik mellékosztálynak ugyanannyi eleme van, mint H-nak, ugyanis bármely $a \in G$ esetén a $H \to aH$, $x \mapsto ax$ leképezés bijekció H és aH között. (A szürjektivitás világos, az injektivitást pedig a kancellativitás garantálja.)
Tehát G előáll $[G : H]$ darab $|H|$ elemszámú diszjunkt halmaz egyesítéseként. □

4.57. Következmény.

Legyen G egy n-elemű csoport.

(1) Minden $H \leq G$ részcsoportra $|H| \mid n$. . . . . 4.56.: $n = |H| \cdot [G : H]$

(2) Minden $a \in G$ esetén $o(a) \mid n$. . . . . (1): $H = [a]$

(3) Minden $a \in G$ esetén $a^n = 1$. . . . . (2) & 4.33.

(4) Minden $a \in G$ esetén $a^{-1} = a^{n-1}$. . . . . $(3) \cdot a^{-1}$

(5) Ha n prímszám, akkor G ciklikus, tehát izomorf $\mathbb{Z}_n$-nel. . . . . .

. . . . . $\forall a \in G : a \neq 1 \overset{(2)}{\Longrightarrow} o(a) = n \implies G = [a] \overset{4.35.}{\cong} \mathbb{Z}_n$

Kis csoportok

4.58. Tétel.

A legfeljebb 7-elemű csoportok (izomorfia erejéig) a következők:

$$\{1\};\quad \mathbb{Z}_2;\quad \mathbb{Z}_3;\quad \mathbb{Z}_4,\ V;\quad \mathbb{Z}_5;\quad \mathbb{Z}_6,\ S_3;\quad \mathbb{Z}_7.$$

Bizonyítás.

Tfh. $n = |G| \leq 7$. Ha $n \in \{2, 3, 5\}$, akkor az előző tétel szerint $G \cong \mathbb{Z}_n$.

Az $n = 4$ esetben, ha G tartalmaz negyedrendű elemet, akkor $G \cong \mathbb{Z}_4$,
ha pedig minden eleme legfeljebb másodrendű, akkor $G \cong V$ (sudoku).

Ha $n = 6$ és G tartalmaz hatodrendű elemet, akkor $G \cong \mathbb{Z}_6$.
Végül tegyük fel, hogy $n = 6$, és G-ben minden elem rendje $1, 2$ vagy 3.

- Ha nincs harmadrendű elem, akkor $\forall g \in G\colon g^2 = 1$, azaz $\forall g \in G\colon g^{-1} = g$.
  Ebből következik, hogy

  $$\forall x, y \in G\colon xy = (xy)^{-1} = y^{-1}x^{-1} = yx,$$

  tehát G kommutatív.

  Node ekkor bármely két $a, b \neq 1$ elem esetén $V \cong \{1, a, b, ab\} \leq G$, ami ellentmond a Lagrange-tételnek.

Kis csoportok

Bizonyítás (folyt.)

- Tehát G-ben van harmadrendű elem. A harmadrendű elemek párosával lépnek fel: $o(a) = 3 \implies o\left(a^{-1}\right) = 3$ (és persze $a^{-1} \neq a$).
  Nyilván $o(1) = 1$, és a maradék öt elem nem lehet mind harmadrendű.
- Tudjuk már, hogy G-ben van harmadrendű és másodrendű elem is:
  legyen $o(a) = 3$, $b = a^{-1}$ és $o(x) = 2$. Ekkor $\mathbb{Z}_3 \cong [a] = \{1, a, b\} \leq G$.

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

- Invertálhatóság/kancellativitás (sudoku): $ax, xa \in \{y, z\}$.

Kis csoportok

Bizonyítás (folyt.)

- Nem lehet $ax = xa$, mert akkor ax nem lenne se másod-, se harmadrendű:

$$(ax)^2 = a^2 \cdot x^2 = b \cdot 1 = b \neq 1,$$
$$(ax)^3 = a^3 \cdot x^3 = 1 \cdot x = x \neq 1.$$

- Tehát $\{ax, xa\} = \{y, z\}$; AÁMNTFH $ax = y$ és $xa = z$:

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

- Innen pedig már eahf8 szerint következik, hogy $G \cong S_3$. □

Házi feladat a gyakorlatra

35. feladat. Melyek izomorfak az alábbi csoportok közül? (A választ minden esetben indokolni kell!)

(a) $\mathbb{Z}_2^3,\ \mathbb{Z}_{20}^*,\ \mathcal{P}(\{a,b,c\}),\ Q$

$\mathcal{P}(\{a,b,c\}) \cong \mathbb{Z}_2^3$ (karakterisztikus vektorok),

$\mathbb{Z}_{20}^* \ncong \mathcal{P}(\{a,b,c\}), \mathbb{Z}_2^3$ (mert $\mathbb{Z}_{20}^*$-ban van negyedrendű elem, pl. $\overline{3}$),

$Q \ncong \mathcal{P}(\{a,b,c\}), \mathbb{Z}_2^3, \mathbb{Z}_{20}^*$ (mert Q nem kommutatív)

(b) $D_6,\ A_4,\ \mathbb{Z}_{13}^*,\ \mathbb{Z}_{12}$

$\mathbb{Z}_{13}^* \cong \mathbb{Z}_{12}$ (mert $\mathbb{Z}_{13}^* = [\overline{2}]$),

$D_6, A_4 \ncong \mathbb{Z}_{13}^*, \mathbb{Z}_{12}$ (mert D_6 és A_4 nem kommutatív),

$D_6 \ncong A_4$ (mert D_6-ban van hatodrendű elem)

(c) $D_3,\ S_3,\ \mathbb{Z}_7^*,\ \mathbb{Z}_9^*$

(d) $\mathbb{Z}_5^*,\ \mathbb{Z}_8^*,\ \mathbb{Z}_{10}^*,\ \mathbb{Z}_{12}^*$

(e) $D_4,\ Q,\ \mathbb{Z}_{15}^*,\ E_8$

Részcsoportháló

Jelölje $\mathrm{Sub}\,(G)$ a G csoport részcsoportjainak halmazát. Például

$$\mathrm{Sub}\,(\mathbb{Z}_4) = \{\{\overline{0}\},\ \{\overline{0},\overline{2}\},\ \{\overline{0},\overline{1},\overline{2},\overline{3}\}\}.$$

A $(\mathrm{Sub}\,(G)\,;\subseteq)$ részbenrendezett halmaz háló, amelyet G részcsoporthálójának nevezünk. A hálóműveletek:

$H \wedge K = H \cap K$ (a legbővebb részcsoport, ami része H-nak is és K-nak is);

$H \vee K = [H \cup K]$ (a legszűkebb részcsoport, ami tartalmazza H-t is és K-t is).

$\mathbb{Z}_{12}$ részcsoporthálója

Minden részcsoport ciklikus:

- $[\overline{1}] = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}, \overline{6}, \overline{7}, \overline{8}, \overline{9}, \overline{10}, \overline{11}\}$
- $[\overline{2}] = \{\overline{0}, \overline{2}, \overline{4}, \overline{6}, \overline{8}, \overline{10}\}$
- $[\overline{3}] = \{\overline{0}, \overline{3}, \overline{6}, \overline{9}\}$
- $[\overline{4}] = \{\overline{0}, \overline{4}, \overline{8}\}$
- $[\overline{5}] = \{\overline{0}, \overline{5}, \overline{10}, \overline{3}, \overline{8}, \overline{1}, \overline{6}, \overline{11}, \overline{4}, \overline{9}, \overline{2}, \overline{7}\}$
- $[\overline{6}] = \{\overline{0}, \overline{6}\}$
- $[\overline{7}] = \{\overline{0}, \overline{7}, \overline{2}, \overline{9}, \overline{4}, \overline{11}, \overline{6}, \overline{1}, \overline{8}, \overline{3}, \overline{10}, \overline{5}\}$
- $[\overline{8}] = \{\overline{0}, \overline{8}, \overline{4}\}$
- $[\overline{9}] = \{\overline{0}, \overline{9}, \overline{6}, \overline{3}\}$
- $[\overline{10}] = \{\overline{0}, \overline{10}, \overline{8}, \overline{6}, \overline{4}, \overline{2}\}$
- $[\overline{11}] = \{\overline{0}, \overline{11}, \overline{10}, \overline{9}, \overline{8}, \overline{7}, \overline{6}, \overline{5}, \overline{4}, \overline{3}, \overline{2}, \overline{1}\}$
- $[\overline{0}] = \{\overline{0}\}$

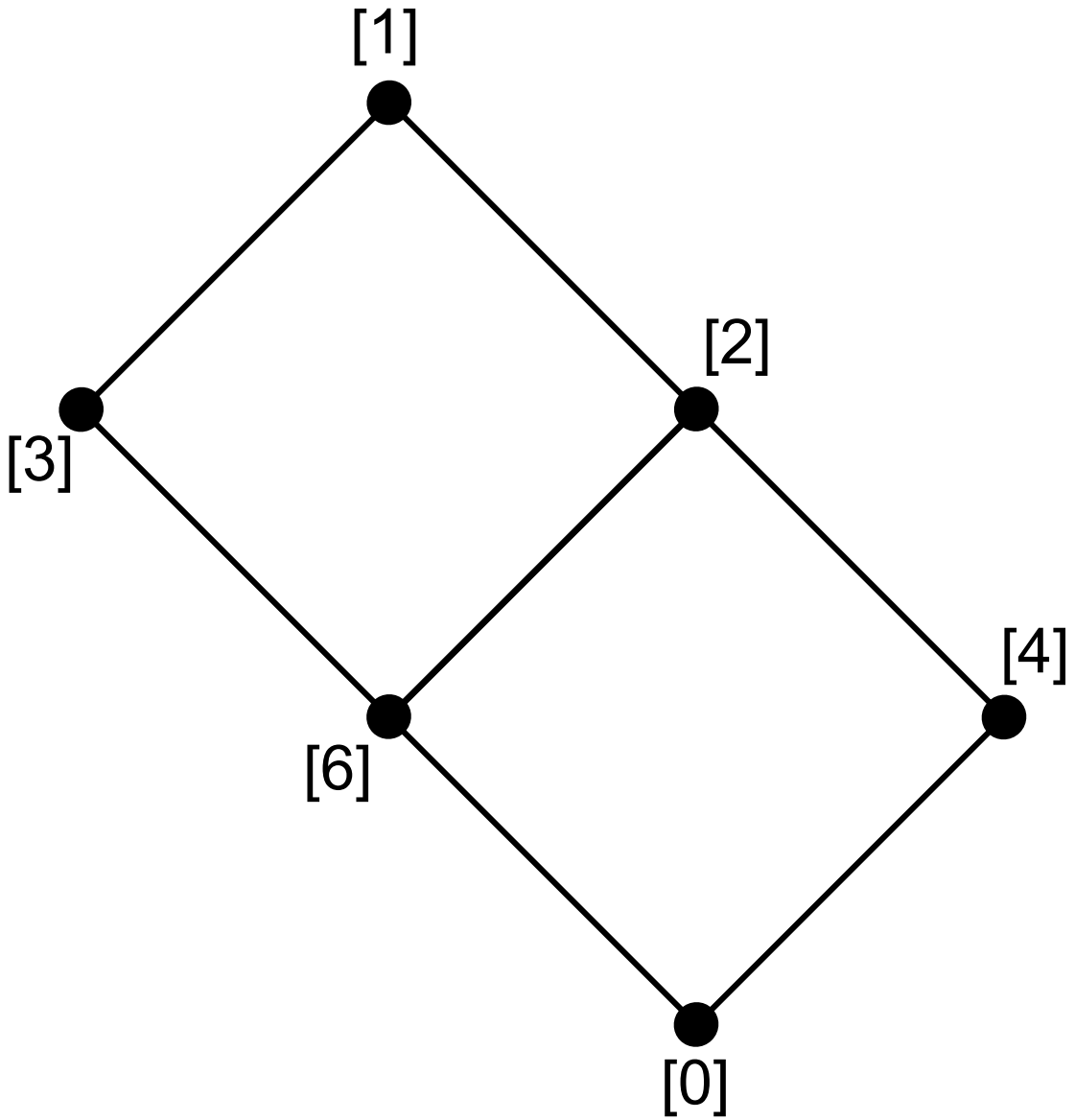
$\mathbb{Z}_{12}$ részcsoporthálója

Minden részcsoport ciklikus:

- $[\overline{1}] = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}, \overline{6}, \overline{7}, \overline{8}, \overline{9}, \overline{10}, \overline{11}\} = [\overline{5}] = [\overline{7}] = [\overline{11}]$
- $[\overline{2}] = \{\overline{0}, \overline{2}, \overline{4}, \overline{6}, \overline{8}, \overline{10}\} = [\overline{10}]$
- $[\overline{3}] = \{\overline{0}, \overline{3}, \overline{6}, \overline{9}\} = [\overline{9}]$
- $[\overline{4}] = \{\overline{0}, \overline{4}, \overline{8}\} = [\overline{8}]$
- $[\overline{6}] = \{\overline{0}, \overline{6}\}$
- $[\overline{0}] = \{\overline{0}\}$

$\mathbb{Z}_{12}$ részcsoporthálója

A részcsoporthálóról:



D_4 részcsoporthálója

$D_4 = \{\mathrm{id}, a, a^2, a^3, t, at, a^2t, a^3t\}$

A ciklikus részcsoportok:

- $[\mathrm{id}] = \{\mathrm{id}\}$
- $[t] = \{\mathrm{id}, t\}$
- $[at] = \{\mathrm{id}, at\}$
- $[a^2t] = \{\mathrm{id}, a^2t\}$
- $[a^3t] = \{\mathrm{id}, a^3t\}$
- $[a] = \{\mathrm{id}, a, a^2, a^3\} = [a^3]$
- $[a^2] = \{\mathrm{id}, a^2\}$

D_4 részcsoporthálója

$D_4 = \{\mathrm{id}, a, a^2, a^3, t, at, a^2t, a^3t\}$

A ciklikus részcsoportok:

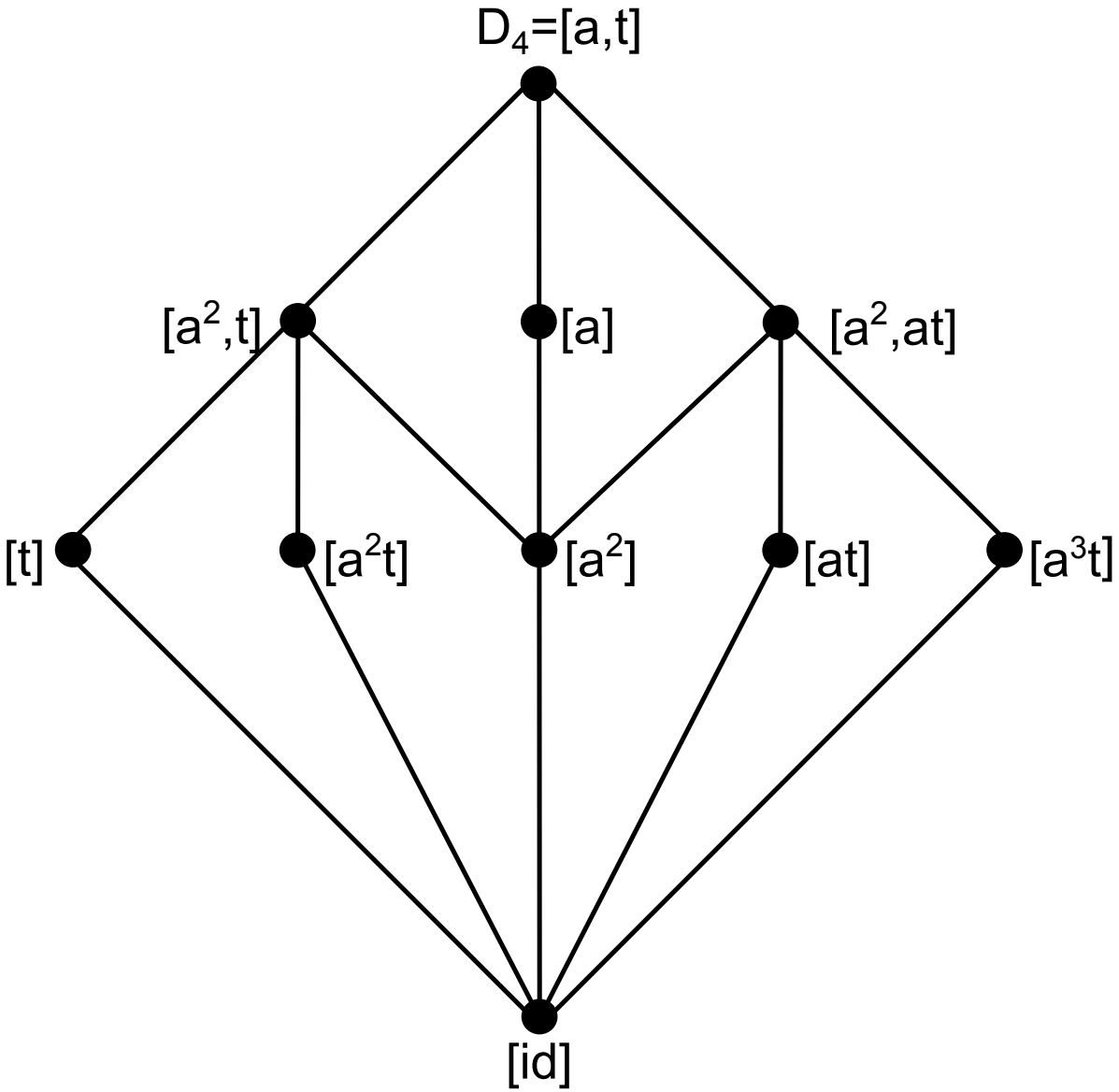
- $[\mathrm{id}] = \{\mathrm{id}\}$
- $[t] = \{\mathrm{id}, t\}$
- $[at] = \{\mathrm{id}, at\}$
- $[a^2t] = \{\mathrm{id}, a^2t\}$
- $[a^3t] = \{\mathrm{id}, a^3t\}$
- $[a^2] = \{\mathrm{id}, a^2\}$
- $[a] = \{\mathrm{id}, a, a^2, a^3\} = [a^3]$

További részcsoportok:

- $[a^2, t] = \{\mathrm{id}, a^2, t, a^2t\} = [a^2, a^2t] = [t, a^2t] \cong V$
- $[a^2, at] = \{\mathrm{id}, a^2, at, a^3t\} = [a^2, a^3t] = [at, a^3t] \cong V$
- $[a, t] = D_4$

D_4 részcsoporthálója

A részcsoporthálóról:



$\mathbb{Z}_{21}^*$ részcsoporthálója

$\mathbb{Z}_{21}^* = \{\overline{1}, \overline{2}, \overline{4}, \overline{5}, \overline{8}, \overline{10}, \overline{11}, \overline{13}, \overline{16}, \overline{17}, \overline{19}, \overline{20}\}$

A ciklikus részcsoportok:

- $[\overline{1}] = \{\overline{1}\}$
- $[\overline{2}] = \{\overline{1}, \overline{2}, \overline{4}, \overline{8}, \overline{16}, \overline{11}\} = [\overline{11}]$
- $[\overline{4}] = \{\overline{1}, \overline{4}, \overline{16}\} = [\overline{16}]$
- $[\overline{5}] = \{\overline{1}, \overline{5}, \overline{4}, \overline{20}, \overline{16}, \overline{17}\} = [\overline{17}]$
- $[\overline{8}] = \{\overline{1}, \overline{8}\}$
- $[\overline{10}] = \{\overline{1}, \overline{10}, \overline{16}, \overline{13}, \overline{4}, \overline{19}\} = [\overline{19}]$
- $[\overline{13}] = \{\overline{1}, \overline{13}\}$
- $[\overline{20}] = \{\overline{1}, \overline{20}\}$

$\mathbb{Z}_{21}^*$ részcsoporthálója

$\mathbb{Z}_{21}^* = \{\overline{1}, \overline{2}, \overline{4}, \overline{5}, \overline{8}, \overline{10}, \overline{11}, \overline{13}, \overline{16}, \overline{17}, \overline{19}, \overline{20}\}$

A ciklikus részcsoportok:

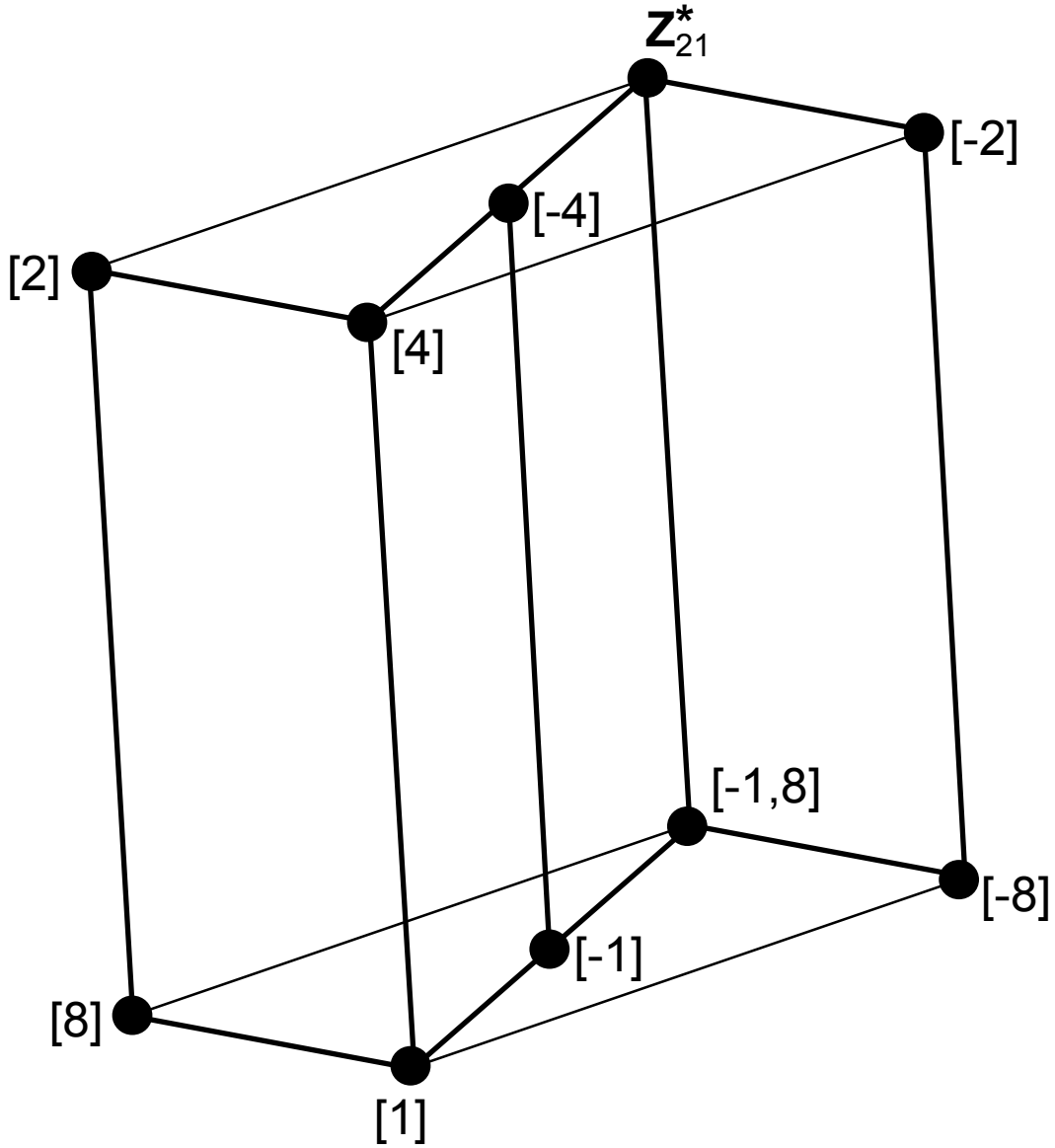
- $[\overline{1}] = \{\overline{1}\}$
- $[-\overline{1}] = \{\overline{1}, -\overline{1}\}$
- $[\overline{8}] = \{\overline{1}, \overline{8}\}$
- $[-\overline{8}] = \{\overline{1}, -\overline{8}\}$
- $[\overline{4}] = \{\overline{1}, \overline{4}, -\overline{5}\}$
- $[\overline{2}] = \{\overline{1}, \overline{2}, \overline{4}, -\overline{5}, \overline{8}, -\overline{10}\}$
- $[-\overline{2}] = \{\overline{1}, -\overline{2}, \overline{4}, -\overline{5}, -\overline{8}, \overline{10}\}$
- $[-\overline{4}] = \{\overline{1}, -\overline{1}, \overline{4}, -\overline{4}, \overline{5}, -\overline{5}\}$

További részcsoportok:

- $[-\overline{1}, \overline{8}] = \{\overline{1}, -\overline{1}, \overline{8}, -\overline{8}\} \cong V$
- $\mathbb{Z}_{21}^*$

$\mathbb{Z}_{21}^*$ részcsoporthálója

A részcsoporthálóról:



Házi feladat a gyakorlatra

36. feladat. Számítsa ki az alábbi csoportokban az egyes elemek generátumait (azaz a ciklikus részcsoportokat), majd határozza meg az összes részcsoportot, végül rajzolja fel a részcsoportháló Hasse-diagramját.

(a) $\mathbb{Z}_{12}$, $\mathbb{Z}_{21}^*$

(b) D_4

(c) $\mathbb{Z}_{15}^*$

(d) Q

(e) S_3

5. Hatványozás modulo m

Az Euler-féle φ függvény

Leonhard Euler

(1707, Bázel – 1783, Szentpétervár)

Gyenge multiplikativitás

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.

5.2. Tétel.

Az Euler-féle φ függvény *gyengén multiplikatív*, azaz $m \perp n$ esetén

$$\varphi(mn) = \varphi(m)\,\varphi(n).$$

Bizonyítás.

Tegyük fel, hogy $m \perp n$. Mivel

$$\varphi(mn) = |\mathbb{Z}_{mn}^*|,$$
$$\varphi(m) \cdot \varphi(n) = |\mathbb{Z}_m^*| \cdot |\mathbb{Z}_n^*| = |\mathbb{Z}_m^* \times \mathbb{Z}_n^*|,$$

elegendő bijekciót megadnunk a $\mathbb{Z}_{mn}^*$ és $\mathbb{Z}_m^* \times \mathbb{Z}_n^*$ halmazok között.

Először a $\mathbb{Z}_{mn}$ és $\mathbb{Z}_m \times \mathbb{Z}_n$ halmazok között adunk meg bijekciót.

Gyenge multiplikativitás

Bizonyítás (folyt.).

Íme:

$$\beta\colon \mathbb{Z}_{mn} \to \mathbb{Z}_m \times \mathbb{Z}_n,\ \overline{x} \mapsto (x \bmod m,\ x \bmod n)\,.$$

A β leképezés (állítólagos) bijektivitása azt jelenti, hogy tetszőleges $a, b \in \mathbb{Z}$ esetén pontosan egy olyan $\overline{x} \in \mathbb{Z}_{mn}$ létezik, amelyre

$$\left.\begin{aligned} x &\equiv a \pmod m \\ x &\equiv b \pmod n \end{aligned}\right\}$$

A kínai maradéktétel szerint ennek a kongruenciarendszernek valóban létezik megoldása (szürjektivitás), és a megoldás modulo lkkt $(m, n) = mn$ egyértelműen meghatározott (injektivitás).

Világos, hogy minden x-re

$$x \perp mn \iff x \perp m \text{ és } x \perp n.$$

Ez azt jelenti, hogy β bijekciót létesít a $\mathbb{Z}_{mn}^*$ és $\mathbb{Z}_m^* \times \mathbb{Z}_n^*$ halmazok között. □

Képlet

5.3. Tétel.

Legyen az n természetes szám prímtényezős felbontása $n = \prod_{i=1}^{k} p_i^{\alpha_i}$. Ekkor

$$\varphi(n) = n \cdot \prod_{i=1}^{k} \left(1 - \frac{1}{p_i}\right) = \prod_{i=1}^{k} \left(p_i^{\alpha_i} - p_i^{\alpha_i - 1}\right) = \prod_{i=1}^{k} p_i^{\alpha_i - 1} (p_i - 1).$$

Bizonyítás.

Prímhatványokra egyszerű a bizonyítás:

$$\varphi(p^\alpha) = |\{a : 1 \leq a \leq p^\alpha \text{ és } a \perp p^\alpha\}|$$

$$= |\{a : 1 \leq a \leq p^\alpha \text{ és } p \nmid a\}| \quad = \quad p^\alpha - p^{\alpha-1}.$$

A gyenge multiplikativitás segítségével ezután már tetszőleges természetes számra tudjuk igazolni az állítást:

$$\varphi\left(p_1^{\alpha_1} \cdot \ldots \cdot p_k^{\alpha_k}\right) = \varphi\left(p_1^{\alpha_1}\right) \cdot \ldots \cdot \varphi\left(p_k^{\alpha_k}\right) = \left(p_1^{\alpha_1} - p_1^{\alpha_1 - 1}\right) \cdot \ldots \cdot \left(p_k^{\alpha_k} - p_k^{\alpha_k - 1}\right).$$

□

http://www.math.u-szeged.hu/∼twaldha/algszambsc/fi360.pdf

Összegzés

5.4. Tétel.

Minden n természetes szám esetén $\sum_{d|n} \varphi(d) = n$.

Bizonyítás.

Jelölje P_d a primitív d-edik egységgyökök halmazát:

$$P_d = \{\varepsilon \in \mathbb{C}^* : o(\varepsilon) = d\}.$$

A 4.33. Állítás szerint $\varepsilon^n = 1 \iff o(\varepsilon) \mid n$. Ez azt jelenti, hogy

$$E_n = \bigcup_{d|n} P_d.$$

A 4.41. Következményből tudjuk, hogy $|P_d| = \varphi(d)$. Tehát

$$n = |E_n| = \sum_{d|n} |P_d| = \sum_{d|n} \varphi(d).$$

□