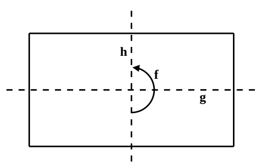
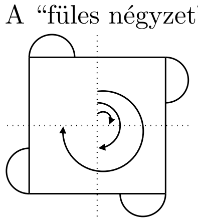
Bevezetés a számításelméletbe II.
2010. MÁJUS 3.
11. gyakorlat: Csoportelmélet

1. Csoportot alkotnak-e az alábbi halmazon definiált műveletek? Ha igen, akkor vizsgáljuk meg, hogy a csoport kommutatív-e?
   (a) {egész számok, összeadás},
   (b) {páratlan számok, összeadás},
   (c) {páros számok, összeadás},
   (d) $\{2 \times 2$-es mátrixok, mátrixszorzás$\}$,
   (e) a síkvektorok halmaza; a síkvektorok összeadása.
   (f) egy tetszőleges X halmaz összes részhalmazainak halmaza; a halmazok uniója.
   (g) egy tetszőleges X halmaz összes részhalmazainak halmaza; a halmazok szimmetrikus differenciája. (Az A és B halmazok szimmetrikus differenciája alatt definíció szerint az $A\Delta B = (A \setminus B) \cup (B \setminus A)$ halmazt értjük.)
2. Csoportot illetve félcsoportot alkot-e az alábbi H halmaz a $*$ művelettel?
   (a) H az egész számok halmaza és az a, $b \in H$ számokra $a * b = a + b + 1$, ahol a szokásos összeadás szerepel;
   (b) Legyen m egy rögzített szám és $H = \{1, 2, \ldots, m-1\}$. Továbbá $a * b = ab \pmod{m}$;
   (c) H a valós számok halmaza és $a * b = a + b + ab$;
   (d) H a 2002 pozitív osztóinak halmaza és az $a, b \in H$ számokra $a * b = (a, b)$, azaz a és b legnagyobb közös osztója.
3. Bizonyítsuk be, hogy minden csoportban $(ab)^{-1} = b^{-1}a^{-1}$.
   Igaz-e, mindig, hogy $(ab)^{-1} = a^{-1}b^{-1}$?
4. Bizonyítsd be, hogy ha G csoportban teljesül, hogy $a^2 = 1 \quad \forall a \in G$-re $\Longrightarrow G$ Abel-csoport!
5. Írjuk fel az alábbi csoportok Cayley-táblázatát! Melyek izomorfak egymással?
   (a) {mod 4 maradékosztályok, összeadás}
   (b) {mod 8 redukált maradékosztályok, szorzás}
   (c) A téglalap szimmetriacsoportja:
   (szimmetriacsoport = a rajzot önmagába vivő egybevágósági transzformációk halmaza a kompozícióra, mint műveletre nézve!)



   (d) A "füles négyzet" szimmetriacsoportja:



6. Mi az egyes elemek rendje C_{12}-ben (a 12 rendű ciklikus csoportban)?
7. Legyen a G csoport elemeinek halmaza $\{1, 2, 3, 4, 5, 6\}$, a művelet a mod 7 szorzás. Igazoljuk, hogy a G csoport ciklikus!
8. $|G| = 81$ és $\exists a \in G: \ a^{27} \neq 1 \Longrightarrow$ a csoport kommutatív.
9. Van-e olyan 20 rendű csoport, melyben van 5 rendű elem, de nincs 20 rendű elem?
   És van-e olyan 20 rendű csoport, melyben van 20 rendű elem, de nincs 5 rendű elem?