Bevezetés a számításelméletbe II.
MEGOLDÁSOK
11. gyakorlat: Algebrai alapfogalmak

1. Akkor alkot csoportot egy struktúra egy halmazon definiált műveletre, ha az asszociatív, létezik egységelem, és minden elemnek van inverze a műveletre nézve.
   (a) Kommutatív csoport.
   (b) Kommutatív csoport (az előzővel izomorf).
   (c) Asszociatív, létezik egységelem (az egységmátrix), de nem minden elemnek van inverze (a nulla determinánsúaknak nincs!). Tehát egységelemes félcsoportról van szó (mely nem is kommutatív).
   (d) Kommutatív csoport. (n-ed rendű ciklikus csoport: C_n).

2. A csoportok Cayley-táblázatai a következők:

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

*	1	3	5	7
1	1	3	5	7
3	3	1	7	5
5	5	7	1	3
7	7	5	3	1

3. A szorzat a következő:
$\begin{pmatrix}1&2&3&4&5\\2&5&4&3&1\end{pmatrix}\cdot\begin{pmatrix}1&2&3&4&5\\5&4&1&2&3\end{pmatrix}=$ $(125)(34)\cdot(153)(24)=(14)(23)(5)$, tehát az 5-öt helyben hagyja a permutáció.

4. Nemkommutatív csoportra példa a nem-nulla determinánsú mátrixok csoportja a szorzásra nézve.

5. Azt kell belátnunk, hogy minden $g_1 \neq g_2 \in G$-re $ag_1 \neq ag_2$ tehát, hogy a leképezés injektív. Ez pedig azért igaz, mert $ag_1 = ag_2 \iff ag_1g_2^{-1} = a \iff g_1g_2^{-1} = e \iff g_1 = g_2$, mert egy csoportban az inverzképzés egyértelmű. Ha tetszőleges a-re ez a leképezés bijekció, akkor valóban minden elem egyértelműen előáll képként, vagyis a és egy másik halmazbeli elem szorzataként.

6. A csoport kommutatív, mert $\underline{ab} = ab(ab)^2 = ab(ba)(ba) = (a(bb)a)ba = aaba = \underline{ba}$.

7. a rendje k, ha k a legkisebb hatvány, melyre $a^k = e$. C_{12}-ben az elemek rendje a következő:

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

8. A csoport ciklikus, mert egy elem hatványaiként megkaphatjuk a csoport összes elemét. Pl: 5 hatványai (mod 7): $5, (25 \equiv)4, (20 \equiv)6, (30 \equiv)2, (10 \equiv)3, (15 \equiv)1$.

9. A két Cayley-tábla a következő:

*	1	3	5	7
1	1	3	5	7
3	3	1	7	5
5	5	7	1	3
7	7	5	3	1

+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	3

Ebből kiolvasható, hogy például az első csoportban két másodrendű elem van, viszont a második csoportban minden elem rendje 2. E miatt se lehetnek izomorfak.

10. Ha $\exists a \in G: \ a^{27} \neq 1$, akkor a rendje csak 81 lehet, mert minden elem rendje = az általa generált ciklikus csoport elemszáma, ez pedig osztja a csoport rendjét, vagyis 81-et. (Ha n nem osztja 27-et, és 81-et igen, akkor $n = 81$ lehet csak.) Ez viszont azt jelenti, hogy egy elem generálja az egész csoportot, vagyis a csoport ciklikus, a ciklikus csoportok pedig mindig kommutatívak.

11. Azt kell tehát belátnunk, hogy $(a^{-1}ba)^n = 1 \iff b^n = 1$. Ez pedig igaz, mert:
$(a^{-1}ba)^n = (a^{-1}ba)(a^{-1}ba)\dots(a^{-1}ba) = a^{-1}b(aa^{-1})b\dots(aa^{-1})ba = a^{-1}b^na = 1 \iff b^n = 1$.

12. Jobbról ab-vel, utána balról ba-val szorozva az az egyenletet adódik, hogy $ba = ab$, tehát a csoport kommutatív.

13. Mivel a ciklikus csoport kommutatív, ezért $1^2a^2a^4\dots a^{2(n-1)} = a^{n(n-1)} = (a^n)^{n-1} = 1^{n-1} = 1$.

14. Az additív csoport nulleleme (egységeleme) a 0. A többi elemnek egyértelműen létezik inverze: $\forall a$-ra $\exists a^{-1} : a+a^{-1} = 0$. Ha összeadjuk az összes elemet, és a kommutativitás miatt mindenkit az inverz párjával teszünk párba, akkor a párok összege 0, így az egész összeg is csak 0 lehet.

15. A H_2 csoport valóban részcsoport, hiszen az összeadás műveletre nézve zárt, és így a csoporttulajdonságok is öröklődnek az alamhalmazból. A H_3 viszont nem zárt, mert például: $a = (0,0,1,1,1,0)$, és $b = (0,1,1,1,0,0)$-ra, $a, b \in H_3$, de $a + b = (0,1,0,0,1,0) \notin H_3$.

16. Ha A és B részcsoportok G-ben, akkor elemszámaik: a és b is osztja G elemszámát, n-et. Ekkor viszont az is igaz, hogy $A \cap B$ is részcsoport G-ben, ezért elemszáma, c is osztja n-et. Ekkor igaz az is, hogy $c \mid a$ és $c \mid b$, mert a metszet is részcsoportja A-nak és B-nek is. Ekkor viszont $|A \cup B| = a + b - c = n$ nem lehet, mert egyik osztó sem lehet nagyobb $\frac{n}{2}$-nél.

17. Ha minden elem rendje n, vagyis $\forall e \neq a \in G$-re $a^n = 1$, akkor n prím kell, hogy legyen, mert ellenkező esetben $pq = n$, ahol p és q is 1-nél nagyobb egészek. Ekkor $(a^p)^q = 1$- ből adódik, hogy az a^p elem rendje q, tehát nem egyezik meg minden elem rendje.

18. Ha $a^k = 1$, akkor $(a^8)^k = (a^k)^8 = 1$, tehát a^8 rendje legfeljebb k, és az is biztos, hogy ennek osztója. Tegyük fel, hogy a^8 rendje l, ahol $l < k$. Ekkor $(a^8)^l = (a^l)^8 = 1$, amiből viszont következne, hogy $a^l = 1$, (mert ellenkező esetben a^l elem rendje 8 lenne, ami nem osztja a csoport rendjét, 55-öt.) Ez viszont ellentmond azzal, hogy k volt a legkisebb olyan index, amelyre $a^k = 1$.

19. Az asszocititás mindegyikre teljesül, de az egységlem és inverz nem mindig létezik, ezért:

    (a) Csoport, mert $e = -1$, és $a^{-1} = a - 1$ minden elemre.

    (b) Nem csoport. Ha m nem prím, akkor létezik olyan elem, melynek nincs inverze, pontosan azok a nem 1 számok, melyek osztják m-et. (Pl: $m = 12$-re 2-nek nincs inverze, mert minden többszöröse páros, sosem legyen egyenlő 1-el modulo 12.)

    (c) Nem csoport. Nem létezik egységelem, mert bár $a^1 = a$, de $1^a \neq a$.

    (d) Csoport. $(c, d) = (1, 0)$ egységelem, és egy tetszőleges (c, d) elem inverze $(c^{-1}, -\frac{d}{c})$.

    (e) Nem csoport. 0 egységelem, de -1-nek nincs inverze.

    (f) Nem csoport. Létezik egységeleme: 2002, de az inverzképzés nem egyértelmű.

20. Mivel a ciklikus csoport kommutatív, ezért minden részcsoportnak a jobb- és baloldali mellékosztályai megegyeznek, vagyis minden részcsoport normálosztó. C_{12}/C_3 faktorcsoportja pedig C_4 lesz.

21. A C_{12} ciklikus csoport normálosztói az összes részcsoport. A velük képzett faktorcsoportok a következők: $C_{12}/C_2 = C_6$, $C_{12}/C_3 = C_4$ és $C_{12}/C_6 = C_2$.