SzA XIV. gyakorlat, 2013. december. 10/12.

Drótos Márton
drotos@cs.bme.hu

Absztrakt algebrát akarunk alkalmazni, továbbá egyebek, meg a félévnek is vége

---

1. Csoportot alkotnak-e az alábbi H halmazok a megadott műveletekre?
   (a) $H = \{2k : k \in \mathbb{Z}\}$, a művelet pedig az összeadás.
   (b) $H = \mathbb{Z}$ az egész számok halmaza, a művelet pedig az osztás.
   (c) $H = \mathbb{R} \setminus \{0\}$ a valós számok halmaza 0-t kivéve, a művelet pedig a hatványozás.
   (d) $H = \mathbb{Z}^+$ a pozitív egész számok halmaza, a művelet pedig a hatványozás.
   (e) H egy tetszőleges X halmaz összes részhalmazainak halmaza, a művelet a halmazok szimmetrikus differenciája. Az A és B halmazok szimmetrikus differenciája alatt az $A \triangle B = (A \setminus B) \bigcup (B \setminus A)$ halmazt értjük.

2. Mik a D_3 diédercsoport elemei? Mik az elemek rendjei?

3. Írjuk fel $\pi \circ \rho$-t, ha

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 5 & 1 & 8 & 4 & 2 & 7 & 6 & 3 \end{pmatrix}$$

$$\rho = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 5 & 2 & 1 & 8 & 7 & 4 & 6 & 3 \end{pmatrix}$$

4. Tekintsünk egy páratlan rendű Abel-csoportot, ahol a művelet neve az összeadás. Bizonyítsuk be, hogy az összes elem összege 0, azaz az egység! (Vagyis a csoport összes elemét összeadjuk.)

5. Tudjuk, hogy a G csoport rendje 100, a g elemre pedig teljesül, hogy $g^{21} = e$. Mit tudunk g-ről?

6. Melyik alkot gyűrűt, és melyik alkot testet?
   (a) $\langle\{a + b\sqrt{2} : \ a, b \in \mathbb{Q}\}, \{+, \cdot\}\rangle$
   (b) $\langle\{a + b\sqrt[3]{2} : \ a, b \in \mathbb{Q}\}, \{+, \cdot\}\rangle$
   (c) $\langle\{\frac{a}{b} : \ a, b \in \mathbb{Z}, 2 \nmid b, 5 \nmid b\}, \{+, \cdot\}\rangle$
   (d) $\langle\{f(x) : \ x \in \mathbb{R}\}, \{+, \circ\}\rangle$ – valós függvények összeadásra és kompozícióra

7. Gyorshatványozással számítsuk ki $7^{19} \pmod 5$ értékét!

---

8. Csoportot alkotnak-e az alábbi H halmazok a megadott műveletekre?
   (a) $H = \mathbb{R}$ a valós számok halmaza, a művelet pedig a hagyományos szorzás.
   (b) $H = \mathbb{R} \setminus \{0\}$, ahol $\mathbb{R}$ a valós számok halmaza, a művelet pedig a következő: $a * b = 2ab$, ahol a jobboldalon a hagyományos szorzás szerepel.
   (c) $H = \{2k + 1 : k \in \mathbb{Z}\}$, a művelet pedig az összeadás.
   (d) $H = \{2k : k \in \mathbb{Z}\}$, a művelet pedig a szorzás.
   (e) $H = \{2k + 1 : k \in \mathbb{Z}\}$, a művelet pedig a szorzás.
   (f) H a $\pmod m$ szerint vett teljes maradékrendszer ($H = \{0, 1, \ldots m - 1\}$), a művelet pedig a maradékosztályokon értelmezett összeadás.

9. Legyen G olyan csoport, ahol $a^2 = e$ teljesül minden $a \in G$ elemre. Bizonyítsuk be, hogy G Abel-csoport!

10. Egy G csoportban minden $a, b \in G$ elempárra teljesül, hogy $(ab)^{-1} = a^{-1}b^{-1}$. Bizonyítsuk be, hogy ekkor G Abel-csoport!

11. Legyen $(G_1, *) \leq (G, *)$ és $(G_2, *) \leq (G, *)$ a $(G, *)$ csoport két részcsoportja! Részcsoportok-e: $(G_1 \cap G_2, *)$, $(G_1 \cup G_2, *)$?

12. A valós számsorozatok halmaza csoportot alkot a számsorozatok összeadására nézve, mint műveletre. Az alábbi részhalmazok közül melyek alkotnak részcsoportot ebben a csoportban?

    (a) a konvergens számsorozatok halmaza,

    (b) a divergens számsorozatok halmaza,

    (c) a korlátos számsorozatok halmaza,

    (d) a monoton növő számsorozatok halmaza.

13. Bizonyítsuk be, hogy tetszőleges csoportban $o(gh) = o(hg)$ tetszőleges g-re és h-ra!

14. R egy nullosztómentes gyűrű. Bizonyítsuk be, hogy

    (a) ha $a^2 = a$ valamilyen $a \in R$-re, akkor $a \in \{0, 1\}$

    (b) ha $a^k = 0$ valamilyen $a \in R$-re, akkor $a = 0$

15. Az órán tanult prímtesztelés segítségével bizonyítsuk be, hogy 8 összetett szám, és 7 valószínűleg prím! Aki szeret sokat számolni, az 561-ről (ami összetett szám, és egyébként a legkisebb Carmichael szám) azt is beláthatja, hogy a módszer szerint valószínűleg prím!

16. Egy közbeszerzési pályázat eredményhirdetése előtt néhány nappal a döntőbizottságban ülő egyik politikus emailt küldött egyik, megfigyelt ismerősének, melynek tárgya: `Re: Mi lesz az eredmény?`. Úgy tűnik, hogy politikusunk és ismerősi köre a szokásosnál tájékozottabb, így hallottak már a titkosításról. Szerencsére az elméleti hátterét a dolognak nem ismerik eléggé, ezért az ismerős nyilvános kulcsa $(85, 43)$, ráadásul úgy tűnik, hogy a szöveg karakterenként van titkosítva. Igazságügyi szakértőként a mi feladatunk, hogy megtudjuk, lehet-e vádat emelni az említett emberek ellen. Az üzenetben a következő számokat látjuk: 58, 48, 27, 3, 6, 48, 67, 76, 38. A (titkosítatlan) karakterkódolás az alábbi táblázat szerint történik:

A	2	B	3	C	4	D	6	E	7	F	8	G	11	H	12	I	13
J	21	K	22	L	23	M	26	N	27	O	28	P	31	Q	32	R	33
S	36	T	37	U	38	V	41	W	42	X	43	Y	46	Z	47		48

---

17. Igény szerint kérdések feltevése a gyakvezérnek, pl. email segítségével.

18. Tanulás. Megértés.

19. ???

20. Profit! (Jól sikerült vizsga. Öröm.)

Hasznos tudnivalók

- $(G, *)$ félcsoport, ha $*$ G-n zárt és asszociatív.
- $(G, *)$ csoport, ha félcsoport, $\exists$ e egységelem és $\forall g \in G$ $\exists$ g^{-1} inverz.
- $(G, *)$ Abel-csoport, ha csoport és $*$ kommutatív.
- Lagrange: ha $H \leq G$, akkor $|H| \mid |G|$, ahol G egy csoport.
- $\langle G, \{+, \cdot\}\rangle$ gyűrű, ha $(G, +)$ Abel-csoport, $(G, \cdot)$ félcsoport, valamint teljesülnek a disztributív tulajdonságok: $a \cdot (b + c) = a \cdot b + a \cdot c$ és $(a + b) \cdot c = a \cdot c + b \cdot c$ $(\forall a, b, c \in G)$. Jelölések: $e_+ = 0$, $e_\cdot = 1$ (ha létezik), $g_+^{-1} = -g$.
- $\langle G, \{+, \cdot\}\rangle$ kommutatív gyűrű, ha gyűrű, és $\cdot$ kommutatív (vagyis $(G, \cdot)$ Abel-félcsoport).
- $\langle G, \{+, \cdot\}\rangle$ integritási tartomány, ha kommutatív gyűrű, és nullosztómentes.
- $\langle G, \{+, \cdot\}\rangle$ ferdetest, ha gyűrű, és $(G \setminus \{0\}, \cdot)$ csoport.
- $\langle G, \{+, \cdot\}\rangle$ test, ha ferdetest, és $\cdot$ kommutatív.
- RSA: p, q prímek (választjuk), $n = pq$, $m = \varphi(n) = (p - 1)(q - 1)$, $1 \leq e \leq n$ úgy, hogy $(e, m) = 1$ (választjuk), d-hez megoldjuk $ed \equiv 1 \mod m$-et. Nyilvános kulcs: (n, e), titkos kulcs: (n, d). Kódolófüggvény: $f(X) = X^e \mod n$, dekódolófüggvény: $f^{-1}(Y) = Y^d \mod n$.