

אלגברה מופשטת 1 – תרגול 2

הקדמה לתורת המספרים :

הגדרה : יהי n טבעי נגדיר את $n\mathbb{Z} = \{0, \pm n, \pm 2n, \dots\}$. אוסף על המספרים השלמים שמתחלקים ב- n .

הגדרה : עבור $a, b \in \mathbb{Z}$ נאמר ש- a מחלק את b ונכתוב $a|b$ אם קיים $n \in \mathbb{Z}$ כך ש- $na=b$.

הגדרה : המחלק המשותף המקסימלי של $n, m \in \mathbb{Z}$ מסומן ב- \gcd (Greatest Common Divisor) או ב- $(m, n) = \gcd(m, n)$ ומוגדר להיות $(m, n) = \max\{d \in \mathbb{N} : d|m \wedge d|n\}$. אם $(n, m) = 1$ נאמר ש- m ו- n זרים.

הערה : אם $d|a$ ו- $d|b$ אזי d מחלק כל צירוף לינארי של a ו- b .

טענה : אם $n = qm + r$ אזי $(n, m) = (m, r)$.

הוכחה : נסמן $d = (n, m)$. אנחנו יודעים מכאן ש $d|n$ וגם $d|m$. כעת, מכיוון ש- r הוא צירוף לינארי של n, m ולכן $d|r$. ולכן $d \leq (m, r)$.

כעת נראה את הכיוון השני. $r|(m, r)$ וגם $m|(m, r)$ ז"א $n|(m, r)$ וגם ידוע ש- $(m, r)|m$ וגם $(m, r)|r$. לכן $(m, r) \leq d$. ובסה"כ קיבלנו כי $(m, r) = d = (n, m)$. ■ מ.ש.ל.

אלגוריתם אוקלידס :

יהי $n, m \in \mathbb{Z}$. ניתן להניח כי $0 \leq m < n$. אם $m=0$ ברור ש- $(m, n) = 0$. אחרת ($m > 0$), ניתן לכתוב $n=qm+r$ כאשר $0 \leq r < m$ ואז מתקיים $(n, m) = (m, r)$.

דוגמה (1) : חישוב GCD באמצעות אלגוריתם אוקלידס : $(53, 47) \stackrel{1 \cdot 47 + 6}{\cong} (47, 6) \stackrel{7 \cdot 6 + 5}{\cong} (6, 5) = (5, 1) = 1$

דוגמה (2) : $(224, 63) \stackrel{3 \cdot 63 + 35}{\cong} (63, 35) \stackrel{1 \cdot 35 + 28}{\cong} (35, 28) \stackrel{1 \cdot 28 + 7}{\cong} (28, 7) = 7$

משפט איפיון gcd

נגדיר $\gcd(a, b) = \min\{ua + vb > 0\}$, $u, v \in \mathbb{Z}$. ובפרט, קיימים $u, v \in \mathbb{Z}$ כך ש- $(a, b) = ua + vb$.

תרגיל : הוכיח שלכל a, b, c שלמים מתקיים : $(a, b) = 1$ וכך $a|bc$ אזי $a|c$.

פתרון: ידוע כי $(a, b) = 1$. לכן קיימים $\alpha, \beta \in \mathbb{Z}$ כך ש- $\alpha a + \beta b = 1$. נכפול את שתי האגפים ב- c , וקיבלנו $a|c$. ■ מ.ש.ל.

תכונות של GCD :

1. $d = (m, n)$ ויהי t כך ש $t|m$ וגם $t|n$ אזי $t|d$.

2. $(am, an) = a(m, n)$

3. אם p ראשוני ו- $p|a$ או $p|b$ אזי $p|a$ או $p|b$.

הגדרה : כפולה משותפת מינימלית (LCM=Least Common Multiple). ההגדרה פורמלית הינה :

$$lcm(m, n) = [m, n] = \min\{d : n|d \wedge m|d\}$$

תכונות של LCM:

1. אם $m|a$ וגם $n|a$ אזי $[m,n]|a$

2. $[n,m] \cdot (n,m) = |nm|$

תרגיל:

א. פתרו את המשוואה $7x=12 \pmod{34}$

ב. מצאו את הספרה האחרונה של 333^{333} .

פתרון:

א. נכפיל בהופכי, כמו בהרצאה, ונקבל $7x = 12 \pmod{34} \rightarrow 35x = 60 \pmod{34} \rightarrow x = 26 \pmod{34}$

אתנחתא קלה: מציאת ההופכי של a ב Z_n הוא בעצם אותו a שמקיים $ax-nk=1$ עבור $ax=1 \pmod{n}$

ב. $333^{333} \equiv x \pmod{10} = 3^{333} 111^{333} \pmod{10} = 1^{333} 111^{333} \pmod{10} = 111^{333} \pmod{10}$ אבל $333^{333} \equiv 1 \pmod{10}$

לכן ניתן לכתוב $x \pmod{10} = 3^{333}$. שוב נפרק ונקבל $x \pmod{10} = 3^{4 \cdot 83 + 1} = 81^{83} \cdot 3 = 1^{83} \cdot 3 = 3$. פתרנו.

חבורות ציקליות ותתי חבורות:

הגדרה: תהי G חבורה ויהי a ששייך ל G . אם כל איבר ב G מתקבל כחזקה חיובית או שלילית של a נאמר ש G נוצרת ע"י a ונקרא ל G חבורה ציקלית. סימון: $G = \langle a \rangle = \{a^k | k \in Z\}$.

דוגמאות:

1. Z נוצרת ע"י 1 ו-1.

2. $kZ = \langle k \rangle$

3. $Z_6 = \langle 1 \rangle = \langle 5 \rangle$ כל חבורה ציקלית הנוצרת ע"י איבר ניתן ליצור אותה גם בעזרת הנגדי.

הגדרה: תהי $(G, *)$ חבורה. אם $\emptyset \neq H \subseteq G$ כך ש $(H, *)$ היא בעצמה חבורה אזי H היא תת חבורה של G ונסמן $H \leq G$.

הקריטריון המקוצר לבדיקת היותו של G תת חבורו הינו: 1. $\emptyset \neq H \subseteq G$. 2. $\forall a, b \in H : ab^{-1} \in H$.

דוגמה (1): $C \leq R \leq Q \leq Z \leq 2Z \leq 4Z$. כל זה לגבי חיבור..

דוגמה (2): האם Z_n ת"ח של Z ? לא! כי לא מדובר באותה פעולה בכלל.

דוגמה (3): תהי G חבורה ויהי a שייך לה. אזי $\langle a \rangle \leq G$ היא תת החבורה הציקלית הנוצרת על ידי a .

דוגמה (4): $SL_n(F) \leq GL_n(F)$ (מטריצות עם דטרמיננטות 1)

תרגיל: $\Omega_n = \left\{ cis\left(\frac{2\pi k}{n}\right) : 0 \leq k \leq n-1 \right\}$. אוסף כל שורשי היחידה מסדר n .

צריך להוכיח כי: 1. $\Omega_n \leq (C^*, \cdot)$. 2. $\Omega_m \leq \Omega_n$ אזי m/n .

פתרון: 1. נוכיח לפי הקריטריון המקוצר. זה מוכל, בוודאות. זה לא ריק כי 1 שייך אליו. התנאי הראשון הוכח. עבור התנאי השני $(\forall a, b \in H : ab^{-1} \in H)$. בעצם צריך להוכיח כי $1 \cdot 1 = 1$. $(ab^{-1})^n = a^n (b^n)^{-1} = 1 \cdot 1 = 1$.

דביר חדד

ולכן זוהי תת חבורה. 2. אם m/n אזי $\Omega_m \leq \Omega_n$. בעצם נוכיח תכילה שזה מוכל, שזהו התנאי הראשון של הקריטריון המקוצר. נניח ש $a \in \Omega_m$ אבל בגלל ש m/n ניתן לרשום $n=mk$ ולכן $a^m = 1$.

$a^{mk} = (a^m)^k = 1^k = 1$ לסיכום, ראינו ש Ω_m היא תת קבוצה, בנוסף בסעיף א' ראינו ש Ω_m היא בעצמה חבורה, לכן לפי ההגדרה (אפילו לא לפי הקריטריון המקוצר!) נקבל ש Ω_m תת חבורה של Ω_n . ומ.ש.ל.

תרגיל: הוכיחו באמצעות לוחות כפל שכל חבורה עם שני איברים וכל חבורה עם 3 איברים היא ציקלית.

*	e	a
e	e	a
a	a	e

פתרון: $S=\{e,a\}$

$\langle a \rangle = S$

*	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

עבור $S=\{e,a,b\}$

$S=\langle a \rangle = \langle b \rangle$

$aa=b$ כי לא יכול להיות ש $aa=e$!