פתרון תרגיל בית 3 בתורת החבורות

88-218 סמסטר א' תשע"ט

שאלות חימום

שאלות החימום הן שאלות קלות יותר בדרך כלל, אבל כדאי מאוד לוודא שיודעים איך לפתור אותן, אפילו בעל פה.

1. עבור כל אחת מהטענות הבאות, קבע האם היא נכונה ואם לא מצא דוגמא נגדית:

   (א) כל חבורה צקלית היא אבלית.

   (ב) כל חבורה אבלית היא צקלית.

   (ג) אם $o(a) = n$, אז $a^{-1} = a^{n-1}$.

פתרון:

(א) נכון.

(ב) לא נכון.

(ג) נכון.

2. כתבו את לוחות הכפל של U_5, U_8. האם מדובר באותה חבורה (עד כדי שינוי שמות)?

פתרון:

$\cdot$	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

לוח הכפל של U_5

$\cdot$	1	3	5	7
1	1	3	5	7
3	3	1	7	5
5	5	7	1	3
7	7	5	3	1

לוח הכפל של U_8

בנוסף, החבורה U_5 היא ציקלית ואילו U_8 לא ציקלית, ולכן אלו חבורות שונות.

שאלות רגילות

1. יהי F שדה. קבעו (והוכיחו את קביעתכם) האם תת־הקבוצות הבאות הן תת־חבורות של החבורות הנתונות או לא:

(א) $O_n(F)=\left\{A\in GL_n(F)|A^T=A^{-1}\right\}\subseteq GL_n(F)$ המטריצות האורתוגונליות ביחס לכפל מטריצות.

(ב) $\{A\in M_n(F)|\det A=0\}\subseteq M_n(F)$ ביחס לחיבור מטריצות.

פתרון:

(א) כן, זו תת־חבורה. בהוכחה כנראה תעזרו בזהויות מאלגברה לינארית לפיהן $(A^{-1})^T=(A^T)^{-1}$ ו־$(AB)^T=B^TA^T$ לכל $A,B\in GL_n(F)$.

ברור ש־$O_n(F)\neq\varnothing$ כי $I^T=I=I^{-1}$ ולכן $I\in O_n(F)$. הסגירות להופכי נובעת מהזהות לעיל, שכן אם $A\in O_n(F)$, אז $(A^{-1})^T=(A^T)^{-1}=(A^{-1})^{-1}$ ולכן $A^{-1}\in O_n(F)$. הסגירות לפעולה נובעת מהזהות השנייה, שכן אם $A,B\in O_n(F)$, אז $(AB)^T=B^TA^T=B^{-1}A^{-1}=(AB)^{-1}$ ולכן $AB\in O_n(F)$.

(ב) לא, זו אינה תת־חבורה של $M_n(F)$. נבחר $n=2$ ועבור כל שדה קל לראות שתת־הקבוצה לא סגורה לפעולה, למשל

$$\begin{pmatrix}1&0\\0&0\end{pmatrix}+\begin{pmatrix}0&0\\0&1\end{pmatrix}=\begin{pmatrix}1&0\\0&1\end{pmatrix}\notin\{A\in M_n(F)|\det A=0\}$$

2. תהי G חבורה ו־H,K תת־חבורות שלה. הוכיחו או הפריכו את הטענות הבאות:

(א) $H\cap K$ היא תת־חבורה.

(ב) $H\cup K$ היא תת־חבורה.

(ג) $HK=\{hk|h\in H,k\in K\}$ היא תת־חבורה.

(ד) אם G אבלית אז HK היא תת־חבורה.

(ה) $\Delta_H=\{(h,h)|h\in H\}$ היא תת־חבורה של $G\times G$.

פתרון:

(א) כן, $H\cap K\leq G$. החיתוך $H\cap K$ אינו ריק כי H,K הן תת־חבורות G. לכן $e\in H,K$, ולכן $e\in H\cap K$. יהי $g\in H\cap K$. אזי $g^{-1}\in H$ וגם $g^{-1}\in K$ כי H,K סגורות להופכי (כי הן תת־חבורות) ולכן $g^{-1}\in H\cap K$ וקיבלנו סגירות להופכי. יהיו $g_1,g_2\in H,K$. אזי $g_1g_2\in H$ וגם $g_1g_2\in K$ כי H,K סגורות לפעולה ולכן גם $g_1g_2\in H\cap K$ וקיבלנו סגירות לפעולה.

(ב) לא, $H\cup K$ אינה תת־חבורה. נבחר $G=\mathbb{Z}$ ואת תת־החבורות $H=2\mathbb{Z}$, $K=3\mathbb{Z}$ (ראינו בכיתה שאלו תת־חבורות של G). אזי $H\cup K$ אינו תת־חבורה כי אינו סגור לפעולה. למשל $2,3\in H\cup K$, אבל $2+3=5\notin H\cup K$.
למעשה $H\cup K$ הוא תת־חבורה אם ורק אם $H\subseteq K$ או $K\subseteq H$. לכן כל דוגמה נגדית מחייבת זוג תת־חבורות שלא מוכלות אחת בשנייה.

(ג) הפרכה. בדרך כלל זו לא תת־חבורה. נבחר $G=S_3$, ואת תת־החבורות $H=\langle(1\ 2)\rangle$ ו־$K=\langle(1\ 3)\rangle$. נקבל כי

$$HK=\{\mathrm{id},(1\ 2),(1\ 3),(1\ 3\ 2)\}$$

שהיא לא תת־חבורה, למשל כי אין סגירות להופכי לאיבר $(1\ 3\ 2)$, או כי מספר האיברים ב־HK לא מחלק את $|S_3|=6$.

(ד) הוכחה. הקבוצה HK לא ריקה כי $e\in H$ וגם $e\in K$ ולכן $e\cdot e=e\in HK$. יש סגירות להופכי כי אם $hk\in HK$, אז גם $(hk)^{-1}=k^{-1}h^{-1}=h^{-1}k^{-1}\in HK$ כאשר השתמשנו באבליות של G בשוויון השני, ובכך ש־H,K הן תת־חבורות ולכן $h^{-1}\in H$ ו־$k^{-1}\in K$. הסגירות לפעולה גם דורשת את האבליות: אם $h_1k_1,h_2k_2\in HK$, אז גם $h_1k_1h_2k_2=h_1h_2k_1k_2\in HK$. שימו לב שהשתמשנו בכך ש־H,K סגורות לפעולה ולכן $h_1h_2\in H$ ו־$k_1k_2\in K$.

(ה) נוכיח כי $\Delta_H \leq G \times G$. היא לא ריקה כי $e \in H$ ולכן $(e,e) \in \Delta_H$. מהסגירות לפעולה של H, אם $(h,h) \in \Delta_H$, אז גם $\left(h^{-1},h^{-1}\right) \in \Delta_H$ ולכן Δ_H סגורה להופכי. מהסגירות לפעולה של H, אם $(h_1,h_1),(h_2,h_2) \in \Delta_H$, אז גם

$$(h_1,h_1)(h_2,h_2) = (h_1h_2, h_1h_2) \in \Delta_H$$

ולכן Δ_H סגורה לפעולה. בסך הכל $\Delta_H \leq G$. שימו לב שזהו לא מקרה פרטי של סעיף 4ג!

3. תהי G חבורה, ותהי $\varnothing \neq H \subseteq G$ תת־קבוצה לא ריקה.

(א) הוכיחו שאם G חבורה סופית, אז כדי להוכיח ש־H היא תת־חבורה של G מספיק לבדוק סגירות לפעולה.

(ב) הפריכו את הסעיף הקודם כאשר G אינסופית.

פתרון:

(א) צריך להראות שבמקרה זה סגירות לפעולה מבטיחה קיום יחידה וסגירות להופכי. לשם כך נראה שבחבורה סופית ההופכי של כל איבר הוא חזקה שלו. נניח $|G| = n$, אז כפי שידוע לנו $o(g) \leq n$ לכל $g \in G$. נסמן $o(g) = m$, אזי

$$\underbrace{(g * \cdots * g)}_{m\ times} = \underbrace{(g * \cdots * g)}_{m-1\ times} * g = e$$

ולכן g^{m-1} הוא ההופכי של g. כעת, אם $g \in H$, אז גם $g^k \in H$ לכל $k \in \mathbb{Z}$ בגלל הסגירות לפעולה. בפרט, $g^m = e \in H$ ולכן H מכילה את היחידה של G, וכן $g^{m-1} = g^{-1} \in H$ ולכן יש סגירות להופכי. בסך הכל קיבלנו כי H תת־חבורה של G.

הדרישה $H \neq \varnothing$ הכרחית, שכן אחרת H אינה חבורה (אפילו שמתקיימת סגירות לפעולה).

(ב) יש הרבה אפשרויות כאן. החבורה האינסופית "הראשונה" שפגשנו תתאים. נבחר $G = \mathbb{Z}$ ואת $H = \mathbb{N} \cup \{0\}$ שבודאי אינה ריקה. אז H סגורה לפעולה (אם $a,b \geq 0$, אז גם $a+b \geq 0$) ומכילה אפילו את איבר היחידה 0, אבל אינה סגורה להופכי. לכן H אינה תת־חבורה.

4. תהי G חבורה ויהיו $a,b \in G$ איברים.

(א) הוכיחו כי $o(ab) = o(ba)$.

(ב) הוכיחו כי $o(a) = o(a^{-1})$

זהירות: לא הנחנו שהחבורה אבלית או שהסדרים סופיים.

פתרון:

(א) נפריד למקרים בהם הסדר סופי ובהם הסדר אינסופי.

תחילה נניח $o(ab) = n < \infty$. נשים לב שמכך נובע $(ab)^{-1} = (ab)^{n-1}$. כעת

$$(ba)^n = \underbrace{baba\ldots ba}_{n} = b(ab)(ab)\cdots(ab)a = b(ab)^{n-1}a =$$
$$= b(ab)^{-1}a = bb^{-1}a^{-1}a = e$$

ולכן $o(ba)|n$. באופן דומה אפשר להראות ש $n|o(ba)$, ולכן $o(ab) = o(ba)$.

אם $o(ab) = \infty$, ונניח בשלילה כי $o(ba) = m \neq \infty$, אז לפי המקרה שבו הסדר סופי, נקבל בסתירה שגם $o(ab) = m$ מסדר סופי. לכן $o(ba) = \infty = o(ab)$.

(ב) מקרה ראשון, נניח $o(a) = n$, מספיק להראות ש־$o(a^{-1}) \leq o(a)$ (כי $a = (a^{-1})^{-1}$). אז $a^n = 1$. $(a^{-1})^n = e^{-1} = (a^n)^{-1}$. לכן $o(a^{-1}) \leq n$.

מקרה שני, נניח שהסדר של a אינסופי. אז גם הסדר של a^{-1} אינסופי, כי אם הוא היה איזשהו n, אז מהמקרה הראשון, היינו מקבלים ש־$o(a) = n$, בסתירה.

5. פתרו את המשוואות הבאות. כלומר מצאו כל $x \in \mathbb{Z}$ המקיים אותן, ולא רק אחד.

(א) $33x \equiv 1 \pmod{218}$

(ב) $-7x + 3 \equiv 9 \pmod{30}$

פתרון:

(א) אנו בעצם נדרשים לחשב את ההופכי של 33 בחבורה U_{218}. בעזרת אלגוריתם אוקלידס המורחב נחשב

$$\begin{aligned}(218, 33) &= [218 = 6 \cdot 33 + 20] \\ (33, 20) &= [33 = 1 \cdot 20 + 13] \\ (20, 13) &= [20 = 1 \cdot 13 + 7] \\ (13, 7) &= [13 = 1 \cdot 7 + 6] \\ (7, 6) &= [7 = 1 \cdot 6 + 1] \\ (6, 1) &= 1\end{aligned}$$

ולכן $(218, 33) = 1$. קיבלנו שאכן $33 \in U_{218}$. בעזרת הצבה לאחור נקבל

$$\begin{aligned}1 &= 7 - 1 \cdot 6 = 7 - 1 \cdot (13 - 1 \cdot 7) = -1 \cdot 13 + 2 \cdot 7 = -1 \cdot 13 + 2 \cdot (20 - 1 \cdot 13) = \\ &= 2 \cdot 20 - 3 \cdot 13 = 2 \cdot 20 - 3 \cdot (33 - 1 \cdot 20) = -3 \cdot 33 + 5 \cdot 20 = \\ &= -3 \cdot 33 + 5 \cdot (218 - 6 \cdot 33) = 5 \cdot 218 - 33 \cdot 33\end{aligned}$$

ולכן ההופכי של 33 הוא -33, ונקבל $x \equiv -33 \equiv 185 \pmod{218}$.

(ב) נסדר את המשוואה כך שנקבל $-7x \equiv 6 \pmod{30}$ ולצורך נוחות $23x \equiv 6 \pmod{30}$. בעזרת אלגוריתם אוקלידס המורחב נחשב

$$\begin{aligned}(30, 23) &= [30 = 1 \cdot 23 + 7] \\ (23, 7) &= [23 = 3 \cdot 7 + 2] \\ (7, 2) &= [7 = 3 \cdot 2 + 1] \\ (2, 1) &= 1\end{aligned}$$

ולכן $(30, 23) = 1$ ומכאן שאכן $23 \in U_{30}$. בעזרת הצבה לאחור נקבל

$$\begin{aligned}1 &= 7 - 3 \cdot 2 = 7 - 3 \cdot (23 - 3 \cdot 7) = -3 \cdot 23 + 10 \cdot 7 \\ &= -3 \cdot 23 + 10 \cdot (30 - 1 \cdot 23) = 10 \cdot 30 - 13 \cdot 23\end{aligned}$$

ולכן ההופכי של 23 ב־U_{30} הוא $-13 \equiv 17 \pmod{30}$. נכפיל את המשוואה ב־17 ונקבל

$$17 \cdot 23x \equiv 17 \cdot 6 \equiv 12 \pmod{30}$$

והפתרון המבוקש הוא $x \equiv 12 \pmod{30}$.

שאלות אתגר

אם פתרתם את שאלות האתגר, ואין לשאלה פתרון, בבקשה שלחו לי את הפתרון שלהן.

1. הזכרו בהגדרת פונקציית אוילר

$$\varphi(n) = |\{a|0 \leq a < n,\ (a,n) = 1\}|$$

הוכיחו כי $\varphi(nm) = \varphi(n)\varphi(m)$ אם ורק אם $(n,m) = 1$.

רמז: משפט השאריות הסיני.

טענה: משפט השאריות הסיני: אם n, m זרים, אזי לכל $a, b \in \mathbb{Z}$ קיים x יחיד עד כדי שקילות מודולו nm כך ש־$x \equiv a \pmod{n}$ וגם $x \equiv b \pmod{m}$.

הוכחה: מפני ש־$(n,m) = 1$, אזי קיימים $s, t \in \mathbb{Z}$ כך ש־$sn + tm = 1$. כדי להוכיח קיום של x נתבונן ב־$bsn + atm$. מתקיים

$$bsn + atm \equiv atm \equiv a \cdot 1 \equiv a \pmod{n}$$
$$bsn + atm \equiv bsn \equiv b \cdot 1 \equiv b \pmod{m}$$

ולכן $x = bsn + atm$ הוא פתרון אפשרי. ברור כי גם $x' = x + kmn$ לכל $k \in \mathbb{Z}$ הוא פתרון תקף.

כדי להראות יחידות של x מודולו nm נשתמש בטיעון קומבינטורי. לכל זוג (a,b) יש x (לפחות אחד) המתאים לו מודולו nm. ישנם בסה"כ nm זוגות שונים (a,b) (מודולו nm), וכן רק nm ערכים אפשריים ל־x (מודולו nm). ההתאמה הזו היא פונקציה חח"ע בין קבוצות סופיות שוות עוצמה, ולכן ההתאמה היא גם על. דרך אחרת: אם קיים מספר y המקיים את הטענה, אז $n|x-y$ וגם $m|x-y$. מהנתון $(n,m) = 1$ נקבל כי $nm|x-y$ ולכן $x \equiv y \pmod{nm}$.

פתרון:

תחילה נניח $(n,m) = 1$ ונוכיח $\varphi(nm) = \varphi(n)\varphi(m)$.

לכל $a \in \{1, 2, \ldots, n\}$ ו־$b \in \{1, 2, \ldots, m\}$ נתאים $x \in \{1, 2, \ldots, nm\}$ כך ש־$x \equiv a \pmod{n}$, $x \equiv b \pmod{m}$ לפי משפט השאריות הסיני. נניח $n = p_1^{n_1} \ldots p_k^{n_k}$ ו־$m = q_1^{m_1} \ldots q_r^{m_r}$ הוא פירוק לראשוניים של n ו־m, בהתאמה. אז $p_i \neq q_j$ לכל i, j מפני ש־$(n,m) = 1$. אנו יודעים כי

$$(x, nm) = (x,n)\,(x,m) = (a,n)\,(b,m)$$

שהרי אם p ראשוני ו־$p \mid (x, nm)$, אז $p|x$ והוא מחלק בדיוק אחד מ־n או m. ולהפך, אם $p \mid (a,n)$ (בלי הגבלת הכלליות), אז p מחלק את $x = bsn + atm$, אבל לא מחלק את m.

לכן $(x, nm) = 1$ אם ורק אם $(a,n) = 1$ וגם $(b,m) = 1$. מספר הטבעיים שזרים ל־nm וקטנים ממנו זה בדיוק $\varphi(nm)$, ונסיק שמספר זה שווה למספר הזוגות (a,b) כאשר a זר ל־n וקטן מ־n (יש $\varphi(n)$ כאלו), ו־b זר ל־m וקטן מ־m (יש $\varphi(m)$ כאלו). כלומר $\varphi(nm) = \varphi(n)\varphi(m)$.

מהוכחת כיוון זה נסיק את הנוסחה שראינו בכיתה: $\varphi(n) = n\prod_{p|n}\left(1 - \frac{1}{p}\right)$ כאשר המכפלה רצה על כל הראשוניים שמחלקים את n.

לכיוון ההפוך, נניח $\varphi(nm) = \varphi(n)\varphi(m)$. נסמן $d = (n,m)$. אז

$$\begin{aligned}\varphi(nm) &= nm\prod_{p|nm}\left(1 - \frac{1}{p}\right) = nm\frac{\prod_{p|n}\left(1-\frac{1}{p}\right)\prod_{p|m}\left(1-\frac{1}{p}\right)}{\prod_{p|d}\left(1-\frac{1}{p}\right)} \\ &= n\prod_{p|n}\left(1-\frac{1}{p}\right)m\prod_{p|m}\left(1-\frac{1}{p}\right)\frac{d}{d\prod_{p|d}\left(1-\frac{1}{p}\right)} = \varphi(n)\varphi(m)\frac{d}{\varphi(d)}\end{aligned}$$

ונקבל $\varphi(d) = d$ שנכון אם ורק אם $d = 1$.

1. תהי G חבורה סופית. הוכיחו כי מספר האיברים מסדר 3 הוא זוגי (אולי אפס).

מה לגבי מספר האיברים מסדר p כאשר p מספר ראשוני אי זוגי? $|\{g|o(g) = p\}| \equiv 0 \pmod{p-1}$

2. מצאו חבורה אינסופית שלכל $n \in \mathbb{N}$ קיים בה איבר מסדר n. האם אתם יכולים גם להבטיח שהסדר של כל האיברים הוא סופי?

כמו כן, לכל $m > 1$ מצאו חבורה אינסופית G_m שהסדר של כל איבר בה הוא לכל היותר m.

האם אתם יכולים למצוא דוגמאות לשאלות האלו כך שהחבורות הן מעוצמה $\aleph_0$?

בהצלחה!