פתרון תרגיל בית 6 במבנים אלגבריים
89-214 סמסטר א' תש"ף

שאלה 1 (חימום)**.** הוכיחו כי לכל $a,n,m\in\mathbb{Z}$ מתקיים $(an,am)=|a|\,(n,m)$.

פתרון. נסמן $d=(n,m)$. בשורה אחת, שאינה הוכחה מלאה,

$$(an,am)=|a|\cdot d\Leftrightarrow\left(\frac{an}{d},\frac{am}{d}\right)=|a|\Leftrightarrow|a|\left(\frac{n}{d},\frac{m}{d}\right)=|a|\Leftrightarrow\left(\frac{n}{d},\frac{m}{d}\right)=1\Leftrightarrow(n,m)=d$$

דרך אחרת, דו־כיוונית (ומפורטת יותר): מצד אחד, ישנם מספרים u,v כך שמתקיים $(an,am)=uan+vam$. ידוע כי d מחלק כל צירוף לינארי של n ו-m, ובפרט את $un+vm$. לכן $|a|\cdot d$ מחלק את $uan+vam$, ולכן $|a|\cdot d)\,|\,(an,am)$.

מצד שני, ישנם מספרים s,t כך שמתקיים $d=sn+tm$. נכפיל ב-$|a|$ ונקבל $|a|\,d=s'an+t'am$ עבור s',t' מתאימים. ידוע כי (an,am) מחלק כל צירוף לינארי של an ו-am, ובפרט את $s'an+t'am$. לכן $(an,am)\,|\,|a|\,d$. לסיכום קיבלנו $(an,am)=|a|\,d$, כדרוש.

ניתן להוכיח את הטענה גם בעזרת שימוש בהצגה של ממ"מ כמכפלת חזקות ראשוניים. במקרה זה מוכיחים כי $\min(n+a,m+a)=\min(n,m)+a$, שהיא אנלוגית להוכחת $(an,am)=|a|\,(n,m)$.

שאלה 2 (חימום)**.** תהי G חבורה מסדר n ויהי $\Phi:G\to S_n$ שיכון קיילי. הוכיחו שאיבר $g\in G$ הוא מסדר m אם ורק אם $\Phi(g)$ הוא מכפלה של $\frac{n}{m}$ מחזורים זרים מאורך m.

פתרון. נניח כי g הוא מסדר m. לכן $g^m=e_G$ וגם לכל $0<i<m$ $g^i\neq e_G$. שיכון קיילי מוגדר לפי $\Phi(g)=l_g$ כאשר l_g הוא הפונקציה של כפל משמאל ב-g. כדי להבין את מבנה המחזורים של $l_g\in S_n$ צריך להבין לאן l_g שולחת כל איבר של G. נראה הרכבה חוזרת שלו על איבר $x\in G$ מסוים:

$$x\xrightarrow{l_g}gx\xrightarrow{l_g}g^2x\xrightarrow{l_g}g^3x\xrightarrow{l_g}\ldots\xrightarrow{l_g}g^{m-1}x\xrightarrow{l_g}g^mx=x$$

לכן $x\in G$ שייך למחזור מאורך m. כך אפשר להמשיך באינדוקציה על איבר מ-G שאינו במחזור לעיל (כלומר לא g^ix עבור האיבר x שבחרנו). לבסוף נקבל שישנם בדיוק $\frac{n}{m}$ מחזורים, וכל אחד מהם מאורך m.

בכיוון השני, זה בסך הכל לחשב סדר של תמורה. הסדר של $\Phi(g)$ הוא כמ"מ אורכי המחזורים בהצגה של התמורה כמכפלת מחזורים זרים, ואצלנו זה $\mathrm{lcm}(m,\ldots,m)=m$, לפי הנתון. מפני ש-$\Phi$ הוא שיכון, אז גם הסדר של g הוא m.

שאלה 3. נסמן כמה איברים של החבורה $GL_2(\mathbb{C})$:

$$I=\begin{pmatrix}i&0\\0&-i\end{pmatrix},\quad J=\begin{pmatrix}0&1\\-1&0\end{pmatrix},\quad K=\begin{pmatrix}0&i\\i&0\end{pmatrix}$$

ונסמן ב-Q את תת־החבורה הקטנה ביותר של $GL_2(\mathbb{C})$ שמכילה את I,J,K. היא נקראת חבורת הקווטרניונים. מצאו באופן מפורש שיכון של Q ב-S_8. כלומר חשבו והוכיחו לאן עובר כל איבר.

רמז: מצאו את איברי Q וזה שבתאריך 16 באוקטובר 1843 חרט ויליאם רואן המילטון על גשר בְּרוּם

$$i^2 = j^2 = k^2 = ijk = -1$$

פתרון. להעשרה, שימוש נפוץ בקווטרניונים הוא לתיאור סיבובים במרחב כפי שמוסבר כאן.
בדיקה ישירה תראה שהמילטון לא טעה. כלומר, אם נסמן את ב-1 את מטריצת היחידה, שהיא איבר היחידה של $GL_2(\mathbb{C})$, נקבל

$$I^2 = J^2 = K^2 = IJK = -1 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$$

ברור ש-1 הוא איבר היחידה של Q, כי זהו איבר היחידה של $GL_2(\mathbb{C})$ (ולמי שלא משוכנע, זכרו שאם I שייך ל-Q, אז מסגירות נובע שגם I^n שייך ל-Q לכל n, בפרט עבור $n = 0$).
כמו ברמז, תחילה ננסה למצוא את כל האיברים של Q.
אם $I^2 = -1$, אז $-1 \in Q$. נשים לב כי ± 1 הם מטריצות סקלריות ולכן מתחלפות עם כל מטריצה. את הסדר של I קל למצוא כי

$$I^4 = (I^2)^2 = (-1)^2 = 1$$

לכן הסדר שלו מחלק את 4, וראינו כבר כי $I^2 \neq 1$. לכן $I^{-1} = I^3 = -I$. באופן דומה רואים כי $J^{-1} = -J$ וכן $K^{-1} = -K$ כי שניהם איברים מסדר 4. כל האיברים שהוזכרו עד עכשיו חייבים להיות שייכים ל-Q. הפרט היחיד מהחריטה של המילטון שלא השתמשנו בו הוא $IJK = -1$. נכפיל ב-K^{-1} מימין ונקבל $IJ = K$. לכן כל איבר שניתן לתאר עם חזקות של K אפשר לתאר גם עם מכפלות של IJ, למשל

$$-IJ = -K = K^{-1} = (IJ)^{-1} = J^{-1}I^{-1} = (-J)(-I) = JI$$

מכאן אפשר להסיק שהאיברים של Q הם בדיוק

$$Q = \{1, -1, I, -I, J, -J, IJ, -IJ\}$$

והקבוצה הזו מכילה את ההופכי של כל איבר, וכל מכפלה של שני איברים מהקבוצה הזו.
הסדר של 1 הוא בוודאי 1, הסדר של -1 הוא 2, והסדר של שאר האיברים הוא 4.
קיבלנו שהסדר של Q הוא 8. משפט קיילי מבטיח שקיים שיכון $\Phi : Q \to S_8$, ונמצא אותו במפורש. באופן נאיבי, נצטרך לבצע 64 הכפלות של מטריצות, אבל כמו שראינו למעלה, הסתפקנו בהרבה פחות (בערך 6 הכפלות). מפני שכל איבר של Q ניתן להציג כמכפלות וחזקות של I ושל J, אז מספיק לבדוק לאן שיכון קיילי שולח את I ואת J, ואז רק להרכיב תמורות. לכן מכאן אין כבר צורך בכפל מטריצות, אלא רק בחריטה של המילטון והרכבת תמורות.
נמספר את האיברים של Q שרירותית:

$$1 \leftrightarrow 1, \quad 2 \leftrightarrow -1, \quad 3 \leftrightarrow I, \quad 4 \leftrightarrow -I, \quad 5 \leftrightarrow J, \quad 6 \leftrightarrow -J, \quad 7 \leftrightarrow IJ, \quad 8 \leftrightarrow -IJ$$

התמונה $\Phi(I)$ של I תחת שיכון קיילי היא $l_I : X \mapsto IX$, כלומר הכפל משמאל ב-I. באופן דומה $\Phi(J) = l_J$. נחשב בעזרת השיוויונות שראינו (כמו $I^2 = -1$):

$*$	1	-1	I	$-I$	J	$-J$	IJ	$-IJ$
I	I	$-I$	-1	1	IJ	$-IJ$	$-J$	J
J	J	$-J$	$-IJ$	IJ	-1	1	I	$-I$

ולמי שלא בטוח: $JIJ = -IJJ = -I(-1) = I$. לכן

$$l_I = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 4 & 2 & 1 & 7 & 8 & 6 & 5 \end{pmatrix} = (1324)(5768)$$

$$l_J = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 5 & 6 & 8 & 7 & 2 & 1 & 3 & 4 \end{pmatrix} = (1526)(3847)$$

מכאן בעזרת העובדה ש-Φ הומומורפיזם נשלים את החישוב לאן עוברים שאר האיברים

$$\begin{aligned}
\Phi(1) &= \Phi(I^4) = \Phi(I)^4 = \mathrm{id} = \Phi(J)^4 \\
\Phi(-1) &= \Phi(I^2) = \Phi(I)^2 = (12)(34)(56)(78) = \Phi(J)^2 = \Phi(IJ)^2 \\
\Phi(I) &= (1324)(5768) \\
\Phi(-I) &= \Phi(I^{-1}) = \Phi(I)^{-1} = (1423)(5867) = \Phi(I)^3 \\
\Phi(J) &= (1526)(3847) \\
\Phi(-J) &= \Phi(J^{-1}) = \Phi(J)^{-1} = (1625)(3748) = \Phi(J)^3 \\
\Phi(IJ) &= \Phi(I)\Phi(J) = (1728)(3546) \\
\Phi(-IJ) &= \Phi(JI) = \Phi(J)\Phi(I) = (1827)(3645)
\end{aligned}$$

אנחנו יכולים לעשות מבחן שפיות לפתרון שלנו לפי תרגיל החימום. למשל, הסדר של I הוא 4 והוא אכן נשלח למכפלה של $\frac{8}{4} = 2$ מחזורים זרים מאורך 4, ואילו האיבר -1 הוא מסדר 2 ונשלח למכפלה של $\frac{8}{2} = 4$ חילופים זרים. כך גם כל שאר האיברים.

שאלה 4. מצאו בעזרת אלגוריתם אוקלידס את המ"מ הבאים:

א. $(892, 140)$

ב. $(17840, -2800)$, רמז: העזרו בחימום.

פתרון.

א. נשתמש באלגוריתם אוקלידס:

$$\begin{aligned}
(892, 140) &= [892 = 6 \cdot 140 + 52] \\
(140, 52) &= [140 = 2 \cdot 52 + 36] \\
(52, 36) &= [52 = 1 \cdot 36 + 16] \\
(36, 16) &= [36 = 2 \cdot 16 + 4] \\
(16, 4) &= [16 = 4 \cdot 4 + 0] \\
(4, 0) &= 4
\end{aligned}$$

ולכן $(892, 140) = 4$.

ב. נשים לב כי $-2800 = -20 \cdot 140$ וכן $17840 = 20 \cdot 892$. לכן לפי השאלה בחימום

$$(17840, -2800) = |20| \cdot (892, 140) = 20 \cdot 4 = 80$$

שאלה 5. פתרו את בעיה 5 מפרוייקט אוילר: המספר 2520 הוא המספר הקטן ביותר שהחלוקה שלו בכל אחד מן המספרים מ-1 עד ל-10 היא ללא שארית.
מה הוא המספר החיובי הקטן ביותר שמתחלק ללא שארית בכל המספרים מ-1 עד ל-20?
הסבירו אם השיטה שלכם תעבוד בזמן סביר (פחות מדקה) גם למספרים מ-1 עד ל-100.
מותר, ואפילו מומלץ, לתכנת כאן, ואז צריך להוסיף להגשה את התוכנה שכתבתם.

פתרון. למעשה מבקשים לחשב את הכמ"מ של $\{1,\ldots,20\}$. ניתן לכתוב פונקציה המחשבת כמ"מ של קבוצת מספרים, ולקבל את התשובה $\operatorname{lcm}(1,\ldots,20) = 232792560$.

אגב, זהו גם המעריך של S_{20}. כלומר לכל $\sigma \in S_{20}$ מתקיים כי $\sigma^{232792560} = \mathrm{id}$, וזהו המספר הקטן ביותר עם התכונה הזאת. כמובן שמספר זה הרבה יותר קטן מאשר $20!$.

חישוב כמ"מ של שני מספרים יכול להעשות ביעילות בעזרת אלגוריתם אוקלידס לחישוב הממ"מ ושימוש בנוסחה $\gcd(a,b)\operatorname{lcm}(a,b) = |ab|$. לחישוב כמ"מ של קבוצת מספרים נעזרים באינדוקציה

$$\operatorname{lcm}(a_1,\ldots,a_n) = \operatorname{lcm}(\operatorname{lcm}(a_1,\ldots,a_{n-1}),a_n)$$

דרך אחרת היא לפרק כל מספר לראשוניים, ואז למצוא את החזקה המרבית של כל ראשוני שמופיע בפירוקים השונים. מפני שהמספרים עד 100 הם די קטנים ויש רק 25 ראשוניים עד 100, זה יכול להיות להעשות מהר.

גישה נאיבית שמנסה לרוץ על המספרים הטבעיים ולבדוק עבור כל n האם הוא מחלק את המספרים מ-1 עד 100 ואם הוא לא להמשיך עם $n+1$ לא תצליח לסיים לרוץ על המחשב שלכם עד הרבה אחרי סוף הסמסטר.

שאלה 6. הוכיחו שלכל מספר שלם n מתקיים $(5n+4, 9n+7) = 1$, ומצאו s,t (התלויים ב-n) כך ש-$(5n+4)s + (9n+7)t = 1$.

רמז: אלגוריתם אוקלידס המורחב עובד גם עם פרמטרים.

פתרון. נשתמש כמה פעמים בכך שאם $x = qm + r$, אז $(x,m) = (m,r)$. כלומר נשתמש באלגוריתם אוקלידס מבלי לוודא את גודל השארית:

$$\begin{aligned}
(5n+4, 9n+7) &= \\
(9n+7, 5n+4) &= [9n+7 = 1\cdot(5n+4) + (4n+3)] \\
(5n+4, 4n+3) &= [5n+4 = 1\cdot(4n+3) + (n+1)] \\
(4n+3, n+1) &= [4n+3 = 4\cdot(n+1) - 1] \\
(n+1, -1) &= [n+1 = -n\cdot(-1) + 1] \\
(-1, 1) &= 1
\end{aligned}$$

מפני ש-1 הוא המספר הטבעי הקטן ביותר, אז זה חייב להיות הממ"מ המבוקש. למציאת המקדמים s,t משתמשים למעשה באלגוריתם אוקלידס המורחב. לפי החישובים מקודם:

$$\begin{aligned}
(4n+3) &\overset{\star}{=} 1\cdot(9n+7) - 1\cdot(5n+4) \\
(n+1) &\overset{\diamond}{=} 1\cdot(5n+4) - 1\cdot(4n+3) \\
1 &= -1\cdot(4n+3) + 4\cdot(n+1) \\
1 &= -1\cdot(4n+3) + 4\cdot(1\cdot(5n+4) - 1\cdot(4n+3)) \qquad (\text{by } \diamond) \\
1 &= -5\cdot(4n+3) + 4(5n+4) \\
1 &= -5\cdot(1\cdot(9n+7) - 1\cdot(5n+4)) + 4\cdot(5n+4) \qquad (\text{by } \star) \\
1 &= -5\cdot(9n+7) + 9\cdot(5n+4)
\end{aligned}$$

ולכן נקבל $s = 9, t = -5$, שאינם תלויים ב-n!

שאלה 7. מצאו את כל המספרים השלמים n כך ש-$(n+2) | (n^2+8)$.

פתרון. נשים לב כי $n+2$ מחלק את עצמו, ואם הוא מחלק את n^2+8, הוא גם יחלק את הממ"מ שלהם (ולכן גם יחלק כל צירוף לינארי של $n+2$ ושל n^2+8). בעזרת החישוב

$$n^2 + 8 = (n-2)\cdot(n+2) + 12$$

ושימוש בטענה שאם $n = qm + r$, אז $(n, m) = (m, r)$, נקבל

$$\left(n^2 + 12, n + 2\right) = (n + 2, 12)$$

כלומר מספיק למצוא את המספרים n כך ש-$(n+2)|12$. המחלקים של 12 הם ידועים, ולכן המספרים המבוקשים הם $-14, -8, -6, -5, -4, -3, -1, 0, 1, 2, 4, 10$.
החישוב שעשינו היה למעשה

$$\frac{n^2+8}{n+2} = \frac{n^2-4+12}{n+2} = \frac{(n+2)(n-2)}{n+2} + \frac{12}{n+2} = (n-2) + \frac{12}{n+2}$$

ומפני ש-$n-2$ הוא שלם, נותר לבדוק מתי $\frac{12}{n+2}$ שלם.

שאלה 8. תהינה G, H חבורות, יהיו $g \in G$, $h \in H$ איברים מסדר אי זוגי, ונסתכל על האיבר $(g^2, h^2) \in G \times H$. הוכיחו $o((g^2, h^2)) = [o(g), o(h)]$.
כלומר הוכיחו שהסדר של (g^2, h^2) הוא הכפולה המשותפת המינימלית של $o(g)$ ו-$o(h)$.

פתרון. הסדרים $o(g)$ ו-$o(h)$ מחלקים את הסדר של G, לפי מסקנה ממשפט לגראנז'. הסדר של G הוא אי זוגי, ולכן $o(g)$ וגם $o(h)$ הם אי זוגיים. ראינו שאם a איבר מסדר סופי, אז את הסדר של חזקה של האיבר a^k ניתן לחישוב מהסדר של a לפי הנוסחה

$$o(a^k) = \frac{o(a)}{(o(a), k)}$$

בפרט, עבור $k = 2$, אם $o(a)$ אי זוגי, נקבל

$$o(a^2) = \frac{o(a)}{(o(a), 2)} = o(a)$$

בחבורה שבשאלה נסיק $o(g^2) = o(g), o(h^2) = o(h)$. לכן מספיק להוכיח

$$o((g^2, h^2)) = [o(g^2), o(h^2)]$$

הסדר של (g^2, e_H) בחבורה $G \times H$ שווה לסדר $o(g^2)$ בחבורה G, כי בחישוב הסדר של (g^2, e_H) הרכיב השני לא משפיע. כלומר $(g^2, e_H)^k = (g^{2k}, e_H)$ לכל k, וכדי להגיע לאיבר היחידה (e_G, e_H) צריך להעלות לפחות בחזקת $o(g^2)$. באופן דומה הסדר של (e_G, h^2) בחבורה $G \times H$ שווה לסדר $o(h^2)$ בחבורה H.
האיברים (g^2, e_H) ו-(e_G, h^2) מתחלפים כי

$$(g^2, e_H)(e_G, h^2) = (g^2, h^2) = (e_G, h^2)(g^2, e_H)$$

וחיתוך תת־החבורות הציקליות שהם יוצרים הוא טריוויאלי, כי

$$\left\langle (g^2, e_H) \right\rangle \cap \left\langle (e_G, h^2) \right\rangle = \left\{ (g^{2k}, e_H) \,\middle|\, k \in \mathbb{Z} \right\} \cap \left\{ (e_G, h^{2t}) \,\middle|\, t \in \mathbb{Z} \right\} = \{(e_G, e_H)\}$$

ולכן לפי תרגיל שעשינו בכיתה נקבל

$$o((g^2, h^2)) = o((g^2, e_H)(e_G, h^2)) = [o(g^2), o(h^2)] = [o(g), o(h)]$$

אפשר גם להוכיח באופן יותר ישיר עם שני השלבים של היתכנות ומינימליות, כמו שעשינו לא פעם בכיתה. בדרך כנראה נשתמש בנוסחה לסדר של חזקה כמו שמופיע למעלה.

שאלה 9 (רשות)**.** תהי G חבורה ונתבונן בפונקציות $f(x) = x^3$, $g(x) = x^4$ ו-$h(x) = x^5$ מהחבורה לעצמה. הוכיחו שהפונקציות האלו הן הומומורפיזמים (כולן יחד) אם ורק אם G אבלית.

בהצלחה!