

פתרון תרגיל בית 7 במבנים אלגבריים 89-214 סמסטר א' תש"ף

שאלה 1 (חימום). אם U_n ציקלית, כמה יוצרים יש לה?
פתרון. ראינו שלחבורה ציקלית מסדר k יש $\varphi(k)$ יוצרים. לפי הגדרה הסדר של U_n הוא $\varphi(n)$. לכן אם U_n ציקלית, אז מספר היוצרים שלה הוא $\varphi(\varphi(n))$.

שאלה 2 (חימום). חשבו את $\varphi(1000)$, $\varphi(480)$ ו- $\varphi(540)$.
פתרון. נחשב לפי הנוסחה שראינו בכיתה לחישוב פונקציית אוילר:

$$\varphi(1000) = 1000 \left(1 - \frac{1}{2}\right) \left(1 - \frac{1}{5}\right) = 400$$

$$\varphi(480) = 480 \left(1 - \frac{1}{2}\right) \left(1 - \frac{1}{3}\right) \left(1 - \frac{1}{5}\right) = 128$$

$$\varphi(540) = 540 \left(1 - \frac{1}{2}\right) \left(1 - \frac{1}{3}\right) \left(1 - \frac{1}{5}\right) = 144$$

שאלה 3. חשבו בעזרת חבורת אוילר ומשפט אוילר את הסעיפים הבאים:

א. שלוש הספרות האחרונות של $2143^{1598} + 9009^{200} + 5780$.

ב. $89^{214} \pmod{91}$.

פתרון.

א. חישוב שלוש הספרות האחרונות הוא למעשה חישוב הנציג מודולו 1000, ולכן מספיק לחשב את

$$2143^{1598} + 9009^{200} + 5780 \equiv 143^{1598} + 9^{200} + 780 \pmod{1000}$$

וכל מחובר ניתן לחשב בנפרד. לפי שאלת החימום ראינו כי $\varphi(1000) = 400$, ולכן לכל $a \in U_{1000}$ מתקיים $a^{400} \equiv 1 \pmod{1000}$. מפני ש- $1000 = 2^3 \cdot 5^3$ קל לבדוק כי $(3, 1000) = 1$, לכן $3 \in U_{1000}$ ומכאן $3^{400} \equiv 1 \pmod{1000}$. בעזרת אלגוריתם אוקלידס נחשב

$$(1000, 143) = [1000 = 6 \cdot 143 + 142]$$

$$(143, 142) = [143 = 1 \cdot 142 + 1]$$

$$(142, 1) = 1$$

לכן $143 \in U_{1000}$ ונוכל למצוא את ההופכי שלו עם אלגוריתם המורחב:

$$1 = 1 \cdot 143 - 1 \cdot 142 = 1 \cdot 143 - (1 \cdot 1000 - 6 \cdot 143) = -1 \cdot 1000 + 7 \cdot 143$$

ולכן $143^{-1} \equiv 7 \pmod{1000}$. כך נחשב

$$143^{1598} \equiv 143^{1600-2} \equiv (143^4)^{400} \cdot 143^{-2} \equiv 1 \cdot 7^2 \equiv 49 \pmod{1000}$$

כך שלסיכום קיבלנו ששלוש הספרות האחרונות הן 830 כי

$$2143^{1598} + 9009^{200} + 5780 \equiv 49 + 1 + 780 \equiv 830 \pmod{1000}$$

ב. באופן דומה לסעיף הקודם, נחשב

$$\varphi(91) = 91 \left(1 - \frac{1}{7}\right) \left(1 - \frac{1}{13}\right) = 72$$

ושוב נוכל להשתמש במשפט אוילר כי $(89, 91) = 1$

$$89^{214} \equiv 89^{3 \cdot 72 - 2} \equiv 89^{-2} \pmod{91}$$

בעזרת אלגוריתם אוקלידס המורחב (חשבו!) נמצא את ההופכי הכפלי של 89 בחבורה U_{91} , שהוא 45. לכן

$$89^{-2} \equiv 45^2 \equiv 23 \pmod{91}$$

שאלה 4. בכל סעיף מצאו במפורש פונקציה המקיימת את התנאים והוכיחו את קביעתכם.

א. איזומורפיזם $f: U_{18} \rightarrow U_{14}$.

ב. אפימורפיזם $f: 2\mathbb{Z} \rightarrow U_{10}$.

ג. איזומורפיזם $f: U_{12} \times U_5 \rightarrow \mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_2$. רמז: $U_5 \cong \mathbb{Z}_4$.

ד. מונומורפיזם $f: A_4 \rightarrow S_5$ שבו $f((123)) \neq (123)$ וגם $f((12)(34)) \neq (23)(45)$.

ה. מונומורפיזם $f: \mathbb{Z}_{ab+3} \times \mathbb{Z}_{1ab0} \rightarrow S_{7ab}$ כאשר a, b הן שתי הספרות האחרונות בת"ז שלכם. המספר $ab+3$ הוא $10 \cdot a + b + 3$, המספר $1ab0$ הוא $1000 + 100 \cdot a + 10 \cdot b$ והמספר $7ab$ הוא $700 + 10 \cdot a + b$.

פתרון.

א. קל לחשב את הסדר של החבורות האלו:

$$|U_{14}| = \varphi(14) = \varphi(2)\varphi(7) = (2-1)(7-1) = 6$$

$$|U_{18}| = \varphi(18) = \varphi(2)\varphi(3^2) = (2-1)(3^2-3) = 6$$

כלומר הסדרים שווים, וייתכן כי הן איזומורפיות (עוד רגע נראה שהן איזומורפיות). המספרים 14 ו-18 קטנים מספיק שאפשר לחשב מי הם ששת האיברים בכל חבורה

$$U_{14} = \{1, 3, 5, 9, 11, 13\} \quad U_{18} = \{1, 5, 7, 11, 13, 17\}$$

חישוב ישיר יראה שהסדר של האיברים $3, 5 \in U_{14}$ הוא 6 ולכן זו חבורה ציקלית. כך גם הסדר של האיברים $5, 11 \in U_{18}$ הוא 6 ולכן גם זו חבורה ציקלית. כל שתי חבורות ציקליות מאותו סדר הן איזומורפיות. ברור כיצד נראה איזומורפיזם בין חבורות ציקליות: הוא יעביר יוצר ליוצר, ושאר התמונות של האיברים יקבעו לפי זה. אנחנו נבחר (למשל) את $f(5) = 11$, ולכן $f(5^i) = 11^i$ לכל i . מפני שמתקיים $U_{14} = \langle 5 \rangle$, אז מצאנו את התמונות של כל איבר של U_{14} . ברור שזו העתקה על, כי 5 עובר לאיבר מסדר 6 בחבורה U_{18} . מפני שהחבורות סופיות מאותו גודל, אז ההעתקה היא גם חח"ע. נותר להראות שזהו הומומורפיזם, ואכן לכל $5^i, 5^j \in U_{14}$ מתקיים

$$f(5^i \cdot 5^j) = f(5^{i+j}) = 11^{i+j} = 11^i \cdot 11^j = f(5^i)f(5^j)$$

ב. קל לחשב את הסדר של U_{10} לפי $4 = (2-1)(5-1) = \varphi(2)\varphi(5) = \varphi(10)$, כמו בסעיף הקודם. בכיתה כבר חישבנו כי $U_{10} = \{1, 3, 7, 9\}$, שהיא ציקלית, וכי 3 (או 7) הוא יוצר. גם החבורה $2\mathbb{Z}$ היא ציקלית, ונוצרת למשל על ידי 2. לכן אפימורפיזם אפשרי הוא $f(2k) = 3^k$. קל לבדוק שהפונקציה הזו היא על

$$f(0) = 3^0 \equiv 1, \quad f(2) = 3^1 \equiv 3, \quad f(4) = 3^2 \equiv 9, \quad f(6) = 3^3 \equiv 7$$

כאשר השיויונות הם מודולו 10. נותר לבדוק כי f הומומורפיזם. לכל $2k, 2k' \in 2\mathbb{Z}$ נחשב

$$f(2k + 2k') = 3^{2k+2k'} = 3^{2k} \cdot 3^{2k'} = f(2k)f(2k')$$

ולכן זה הומומורפיזם. כמה אפימורפיזמים כאלו ישנם?

ג. בדומה לסעיפים הקודמים מחשבים $\varphi(5) = 4$ ו- $\varphi(12) = \varphi(3)\varphi(2^2) = 2$. הרמז גילה לנו כי $U_5 \cong \mathbb{Z}_4$. מפני ש-5 ראשוני, קל לדעת שהאיברים בחבורה U_5 הם $\{1, 2, 3, 4\}$, ונשים לב שהאיבר 2 הוא מסדר 4, ולכן יוצר של U_5 . עבור $U_{12} = \{1, 5, 7, 11\}$ יש לנו משהו חדש. האיברים הם מסדר 1 או 2, ולכן U_{12} לא ציקלית. לפי השאלה, די ברור שאנחנו צריכים לחפש איזומורפיזם לחבורה $\mathbb{Z}_2 \times \mathbb{Z}_2$. ברור שהאיבר $1 \in U_{12}$ ישלח תמיד לאיבר $(0, 0)$. מסתבר שכל פונקציה חח"ע ועל מהקבוצה $\{5, 7, 11\}$ לשלושת האיברים האחרים ב- $\mathbb{Z}_2 \times \mathbb{Z}_2$ תעזור להגדיר איזומורפיזם. נבחר למשל את $f_1: \mathbb{Z}_5 \rightarrow \mathbb{Z}_4$ להיות $f_1(2^i) = i$ שמוכיחים שזה איזומורפיזם כמו בסעיפים הקודמים, ונבחר את $f_2: U_{12} \rightarrow \mathbb{Z}_2 \times \mathbb{Z}_2$ לפי

$$f_2(1) = (0, 0) \quad f_2(5) = (1, 0) \quad f_2(7) = (0, 1) \quad f_2(11) = (1, 1)$$

שברור שזו פונקציה על, ומפני שהגדלים שווים היא גם חח"ע. החבורות אבליות, אז מספיק לבדוק

$$\begin{aligned} f_2(5 \cdot 5) &= f_2(1) = (0, 0) = (1, 0) + (1, 0) = f_2(5) + f_2(5) \\ f_2(5 \cdot 7) &= f_2(11) = (1, 1) = (1, 0) + (0, 1) = f_2(5) + f_2(7) \\ f_2(5 \cdot 11) &= f_2(7) = (0, 1) = (1, 0) + (1, 1) = f_2(5) + f_2(11) \\ f_2(7 \cdot 7) &= f_2(1) = (0, 0) = (0, 1) + (0, 1) = f_2(7) + f_2(7) \\ f_2(7 \cdot 11) &= f_2(5) = (1, 0) = (0, 1) + (1, 1) = f_2(7) + f_2(11) \\ f_2(11 \cdot 11) &= f_2(1) = (0, 0) = (1, 1) + (1, 1) = f_2(11) + f_2(11) \end{aligned}$$

והבדיקה עם $1 \in U_{12}$ קלה. כך נוכל להגדיר איזומורפיזם חדש בעזרת שני האיזומורפיזמים האלו:

$$\begin{aligned} f: U_{12} \times U_5 &\rightarrow \mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_2 \\ (x, 2^i) &\mapsto (f_{2,1}(x), i, f_{2,2}(x)) \end{aligned}$$

כאשר בסימון $f_{2,1}(x)$ (או $f_{2,2}(x)$) הכוונה לרכיב הראשון (או השני) של $f_2(x)$.

ד. יש שיכון טבעי $\varphi: A_4 \rightarrow S_5$ שבו $\varphi(\sigma) = \hat{\sigma}$ כאשר $\hat{\sigma}$ היא התמורה שבה $\hat{\sigma}(5) = 5$ ועבור שאר המספרים $1 \leq i \leq 4$ היא מתנהגת בדיוק כמו σ , כלומר $\hat{\sigma}(i) = \sigma(i)$. קל לבדוק שזאת פונקציה חח"ע ושהיא הומומורפיזם. זה בעצם לקחת את העתקת הזהות $\text{id}: A_4 \rightarrow A_4$ ולהרחיב את הטווח לאיברים של S_5 . הבעיה היא שהשיכון הטבעי לא מקיים את המגבלות המופיעות בשאלה.

אפשרות אחת היא להזכר בתרגיל בית על הומומורפיזמים, שבהנתן איבר בחבורה $x \in G$ הוכחתם שהפונקציה $\gamma_x: G \rightarrow G$ המוגדרת לפי $\gamma_x(g) = xgx^{-1}$ היא אוטומורפיזם, ובפרט חח"ע. יש המון אפשרויות לבחירה, וניקח משהו שידאג כי

ההגבלות יתקיימו. למשל נבחר את $x = (345)$ ואת האוטומורפיזם $\gamma_x: S_5 \rightarrow S_5$. נרכיב את השיכון הטבעי עם γ_x שבחרנו ונקבל כי $f = \gamma_x \circ \varphi$ היא שיכון שעומד בתנאי השאלה.

הזכרו שהרכבה של הומומורפיזמים היא הומומורפיזם, והרכבה של פונקציות חח"ע היא חח"ע. לכן f שיכון. נותר לבדוק את ההגבלות

$$\begin{aligned} f((123)) &= (345)(123)(345)^{-1} = (124) \neq (123) \\ f((12)(34)) &= (345)(12)(34)(345)^{-1} = (12)(45) \neq (23)(45) \end{aligned}$$

שצריך לדעת לחשב בעצמכם (וגם היה תרגיל שמראה כיצד נראית הצמדה של תמורה). שימו לב כי הפונקציה $\iota: A_4 \rightarrow S_5$ המוגדרת לפי $\iota(\sigma) = \sigma^{-1}$ היא לא הומומורפיזם, ובפרט לא מונומורפיזם. למשל

$$\iota((123)(234)) = \iota((12)(34)) = (12)(34) \neq (13)(24) = (132)(243) = \iota((123))\iota((234))$$

וכבר ראינו בתרגול שפונקציה $i: G \rightarrow G$ השולחת איבר להופכי היא הומומורפיזם אם ורק אם G אבלית, אבל A_4 אינה אבלית.

דרך אחרת למציאת שיכון היא להזכר בהגדרה של החבורה הסימטרית. בהנתן קבוצה X , החבורה הסימטרית S_X היא אוסף הפונקציות החח"ע ועל $\sigma: X \rightarrow X$ עם פעולת ההרכבה. עבור הקבוצה $X = \{1, \dots, n\}$ סימנו בקיצור S_n . הבינו למה ברור שבמקרה ויש קבוצות X, Y מאותה עוצמה, אז $S_X \cong S_Y$. נסו להבין שזה אומר שיש פונקציה חח"ע ועל $\Psi: X \rightarrow Y$ ואיך בעזרתה בונים איזומורפיזם מהחבורה S_X לחבורה S_Y .

לכן למשל $S_4 \cong S_{\{1,3,4,5\}}$, ואז כדי לפתור את השאלה משתמשים בשיכון הטבעי $A_4 \rightarrow S_4$ ואז מרכיבים אותו עם האיזומורפיזם הזה.

ה. בכיתה פתרנו תרגיל שביקש למצוא תת-חבורה מסדר 45 של S_{15} . הדרך שפתרנו הייתה למצוא איבר $\sigma \in S_{15}$ מסדר 45 ולשים לב כי תת-החבורה $\langle \sigma \rangle \leq S_{15}$ היא מסדר 45. האיבר שמצאנו היה

$$\sigma = (1, 2, 3, 4, 5)(6, 7, 8, 9, 10, 11, 12, 13, 14)$$

עכשיו נעזר ברמז שפורסם באתר, ונתחיל לנסות לשכן את $\mathbb{Z}_n$ ב- S_{7ab} . איך נמצא מונומורפיזם $f: \mathbb{Z}_{45} \rightarrow S_{15}$? זה ממש אותו תרגיל מהכיתה. החבורה $\mathbb{Z}_{45}$ היא ציקלית ומסדר 45, והתמונה $\text{im } f$ של ההומומורפיזם חייבת גם היא להיות ציקלית. כדי לדאוג לחח"ע חייבים שהתמונה תהיה מסדר 45, שאת זה אנחנו יודעים לעשות. בכל מקרה כל חבורה ציקלית מסדר 45 איזומורפית ל- $\mathbb{Z}_{45}$ והאיזומורפיזם ישלח יוצר ליוצר. למשל אפשר לבחור $f(1) = \sigma$ עבור σ לעיל. מהתכונה של ההומומורפיזם בהכרח $f(i) = \sigma^i$, ומוכיחים שזה הומומורפיזם כמו בסעיפים הקודמים. אם $\sigma^i = \text{id}$, אז $i \in 45\mathbb{Z}$, או במילים אחרות $i \equiv 0 \pmod{45}$. כלומר $i = 0 \in \mathbb{Z}_{45}$, שהוא איבר היחידה ולכן f מונומורפיזם.

אם נרצה לשכן את $S_{100} \rightarrow \mathbb{Z}_{200}$, נשים לב שאין לנו בחבורה מחזורים מאורך 200. נפרק לגורמים ראשוניים $200 = 2^3 \cdot 5^2$ ונבנה תמורה שהיא מכפלה של שני מחזורים זרים $\tau = \tau_1 \tau_2$ כאשר τ_1 הוא מאורך 2^3 ו- τ_2 הוא מאורך 5^2 . אז $2^3 + 5^2 = 33 < 100$ מספרים נכנסים בבטחה בתמורות בחבורה S_{100} . באופן דומה לבחירה הקודמת, ההומומורפיזם שנבחר יהיה כמובן $f'(j) = \tau^j$ כאשר $j \in \mathbb{Z}_{200}$. כעת אם נרצה לשכן את $\mathbb{Z}_{45} \times \mathbb{Z}_{200}$ ב- S_{100} , נשים לב כי $5 + 9 + 2^3 + 5^2 = 47 < 100$ ולכן נוכל לדאוג כי σ ו- τ הן תמורות זרות. כך נוכל להגדיר "מכפלה ישרה" של ההומומורפיזמים לעיל

$$\begin{aligned} \varphi: \mathbb{Z}_{45} \times \mathbb{Z}_{200} &\rightarrow S_{100} \\ (i, j) &\mapsto \sigma^i \tau^j \end{aligned}$$

זהו יוצא הומומורפיזם כי σ - τ מתחלפות. בפירוט, לכל זוג איברים $(i_1, j_1), (i_2, j_2) \in \mathbb{Z}_{45} \times \mathbb{Z}_{200}$ מתקיים

$$\begin{aligned}\varphi((i_1, j_1) + (i_2, j_2)) &= \varphi((i_1 + i_2, j_1 + j_2)) = \sigma^{i_1+i_2} \tau^{j_1+j_2} \\ &= \sigma^{i_1} \sigma^{i_2} \tau^{j_1} \tau^{j_2} = \sigma^{i_1} \tau^{j_1} \sigma^{i_2} \tau^{j_2} = \varphi((i_1, j_1)) \varphi((i_2, j_2))\end{aligned}$$

ואם $0 < i < 45$ וגם $0 < j < 200$, אז $\varphi((i, j)) = \sigma^i \tau^j \neq \text{id}$ כי הסדר של σ הוא 45 והסדר של τ הוא 200. לכן φ הוא שיכון. כך גם בפתרון לשאלה הזאת, מפרקים את המספרים $ab+3$ ו- $1ab0$ לגורמים ראשוניים. כך מוצאים תמורה σ מסדר $ab+3$, כמו שעשינו עבור 15, ותמורה τ מסדר $1ab0$, ובונים מונומורפיזם. דאגנו לכך שהמספר $7ab$ יהיה גדול מספיק כך שיתאפשר למצוא תמורות זרות כמו σ ו- τ מהסדרים המתאימים. מי שבפתרון שלו מופיעה המילה "מחרוזת" ודוגמה כלשהי עם $(2, 3)$ ככל הנראה טעה (או יותר גרוע).

שאלה 5. מצאו את כל המספרים n כך ש- $\varphi(n) = 4$ וכל המספרים m כך ש- $\varphi(m) = 8$. זה בסדר להשתמש במחשבון עבור פעולות חשבון פשוטות.

פתרון. אם ראשוני $p \geq 7$ מחלק את n , אז $n = p^k n'$ עבור $k \geq 1$ עם n' שזר ל- p ולכן

$$\varphi(n) = \varphi(p^k n') = \varphi(p^k) \varphi(n') = (p^k - p^{k-1}) \varphi(n') > 4$$

כי $n = 2^a 3^b 5^c$ מהצורה $\varphi(n') > 4$ ו- $p^{k-1}(p-1) > 4$. בדיקה זריזה אחר הפתרונות למשוואה $\varphi(n) = 4$ בקבוצה הסופית הזאת, תגלה שהם רק 5, 8, 10, 12.

באופן דומה, אם ראשוני $p \geq 11$ מחלק את m , אז $\varphi(m) > 6$. לכן מחפשים מספרים מהצורה $m = 2^a 3^b 5^c 7^d$ עם הדרישות $a < 4, b < 3, c < 2, d < 2$. בדיקה זריזה אחרי פתרונות בקבוצה הסופית הזאת למשוואה $\varphi(m) = 8$ תגלה שהם רק 15, 16, 20, 24, 30.

שאלה 6. בחבורה A_{10} , מצאו איברים מהסדרים 4, 7, 12, 14, 15, 18, 19, 20, או הוכיחו שלא קיים איבר מסדר כזה.

פתרון. כל איבר של A_{10} אפשר להציג כמכפלת מחזורים זרים. לכן אנחנו צריכים לבדוק חלוקות של 10 כך שתקבל תמורה זוגית. למעשה מתוך 16 הסדרים האפשריים לאיברים של S_{10} , יש רק 13 אפשרויות לסדרים ב- A_{10} .

יש איברים מהסדרים 4, 7, 12, 15. מסדר 4 יש את $(1, 2, 3, 4)(5, 6)$ שהוא תמורה זוגית מסדר 4. שימו לב שזה חשוב להכפיל בחילוף $(5, 6)$ כדי להבטיח את הסימן הזוגי של התמורה. אפשר גם לבחור את $(1, 2, 3, 4)(5, 6, 7, 8)$. עבור איבר מסדר 7 פשוט בוחרים מחזור מאורך 7, שהוא תמורה זוגית. עבור סדר 12 נציג שתי אפשרויות, $(1, 2, 3, 4)(5, 6, 7, 8, 9, 10)$ או $(1, 2, 3)(4, 5, 6, 7, 8)(9, 10)$. לבסוף תמורה זוגית מסדר 15 היא למשל $(1, 2, 3)(4, 5, 6, 7, 8)(9, 10)$. אין תמורות מהסדרים 14, 18, 19, 20 בחבורה A_{10} . בוודאי אין מחזורים מהאורך הזה, ולכן צריך לפרק את הסדר לגורמים ראשוניים. למשל $14 = 7 \cdot 2$, ואז אם נבחר מחזור מאורך 7 וחילוף שזר לו, נקבל תמורה אי זוגית. השתמשנו ב-9 מספרים, ולכן אין לנו דרך להוסיף חילוף זר נוסף כדי להפוך את התמורה לזוגית. כך גם עם $18 = 2 \cdot 9$ או 19 הראשוני, שעבורם אין אפילו מספיק מספרים 1, ..., 10. עבור $20 = 2^2 \cdot 5$ גם אם ניקח מחזור מאורך 4 ומחזור שזר לו מאורך 5 נקבל שמכפלתם היא תמורה אי זוגית, ואין עוד מספיק מספרים להוסיף חילוף שמכפלה בו תספק תמורה זוגית.

שאלה 7 (רשות). הוכיחו שלכל $n, s > 1$ מתקיים כי $n | \varphi(s^n - 1)$.

בהצלחה!