פתרון מטלה 02 — מבנים אלגבריים 1 (80445)

18 במאי 2024

שאלה 1

נוכיח שכל חבורה ציקלית איזומורפית ל־$\mathbb{Z}$ או ל־$\mathbb{Z}/n$ בלבד.

הוכחה. תהי חבורה G ציקלית הנוצרת על־ידי $\langle a\rangle$, כאשר $a \in G$.

נניח תחילה כי G סופית, ולכן קיים $n > 0$ כך ש־$a^n = e$ כאשר e איבר נייטרלי של G.

נסיק אם כן כי הסדר של G הוא בעצמו n, ונגדיר פונקציה $\varphi : \mathbb{Z} \to G/n$ על־ידי

$$\varphi(n) = a^n$$

נשים לב שלכל $x, y \in \mathbb{Z}/n$ מתקיים $\varphi(x +_n y) = a^{x+y} = a^x a^y = \varphi(x)\varphi(y)$ ולכן על־פי התנאי ההכרחי φ הומומורפיזם.

מהגדרת החבורה וההומומורפיזם ניתן להסיק בנקל כי היא חד־חד ערכית, ומהגדרתה הישירה נסיק כי היא גם על, ולכן היא איזומורפיזם, ובהתאם $G \xrightarrow{\sim} \mathbb{Z}/n$.

נניח עתה כי G איננה סופית ונגדיר את $\varphi : G \to \mathbb{Z}$ באותו האופן אשר הוגדרה בו עד כה, אך נגדיר גם $\varphi(-n) = (a^{-1})^n$.

הפונקציה φ מוגדרת לכל $n \in \mathbb{Z}$, ומהציקליות אנו יודעים שכל איבר $x \in G$ ניתן לכתיבה כ־a^n שלם כלשהו, ולכן נסיק כי φ היא איזומורפיזם ובהתאם $G \xrightarrow{\sim} \mathbb{Z}$.

מצאנו כי G ציקלית איזומורפית ל־$\mathbb{Z}/n$ כלשהו או ל־$\mathbb{Z}$. $\square$

שאלה 2

סעיף א'

נוכיח שלכל $n \geq 1$ החבורה S_n נוצרת על־ידי $H = \langle (ij) \mid 1 \leq i < j \leq n \rangle$.

הוכחה. יהי l־מחזור $\sigma = (\lambda_1 \dots \lambda_l)$ ויהי $\tau = (\lambda_l \lambda_{l+1})$, אז $\tau \circ \sigma = (\lambda_1 \dots \lambda_l \lambda_{l+1})$ $l+1$־מחזור.
זאת אנו מקבלים על־ידי בדיקה ישירה של הפונקציה. נוכל להשתמש בטענה כדי להוכיח שכל l־מחזור נתון ניתן להרכבה על־ידי l 2־מחזורים.
על־ידי צירוף הטענה שכל תמורה ניתנת לייצוג על־ידי הרכבת מספר סופי של מחזורים נקבל כי $H = S_n$. $\square$

סעיף ב'

נוכיח כי גם $H_1 = \langle (i, i+i) \mid 1 \leq i < n \rangle$ יוצרת את S_n.

הוכחה. נבחין כי הרכבת המחזורים $(at)(tb)(ta)$ מניבה את המחזור (ab), ונוכיח באינדוקציה שכל המחזורים מהצורה $(1, n)$ מוכלים ב־H_1.
בסיס אינדוקציה: נראה כי $(13) = (21)(23)(12)$.
מהלך אינדוקציה: נניח כי $(1n) \in H_1$ ולכן $(1\ n+1) = (21)(n+1\ 2)(12)$, וקיבלנו כי הטענה מתקיימת.
עתה נראה כי לכל $1 \leq x, y \leq n$ מתקיים $(1x), (1y) \in H_1$ ולכן ההרכבה $(x1)(1y)(x1) = (xy) \in H_1$ וקיבלנו כי תנאי הסעיף הקודם מתקיימים ונובע $H_1 = H = S_n$. $\square$

סעיף ג'

נוכיח כי גם $H_2 = \langle (1\ 2)(1\ 2 \dots n) \rangle$ יוצר את S_n.

הוכחה. נראה כי

$$(1\ 2 \dots n)^k (1\ 2) = (k\ k+1)$$

נובע ישירות מתהליך ההרכבה, לכן $H_2 = H_1$ ובהתאם גם $H_2 = S_n$. $\square$

שאלה 3

יהי $n \geq 3$ ונגדיר $\sigma, \tau \in S_n$ על־ידי

$$\sigma(k) = k + 1 \mod n, \qquad \tau(k) = n - k + 1$$

ונגדיר את החבורה הדיהדרלית $D_n = \langle \sigma, \tau \rangle \leq S_n$.

סעיף א'

נשים לב שהחבורה D_4 זהה להגדרתה המקורית על־ידי ריבוע. אני משוכנע.

סעיף ב'

נראה כי

$$\tau(\tau(k)) = n - (n - k + 1) + 1 = k \implies \tau^2 = Id$$

בנוסף נבחין כי מהגדרתה נובע כי $\sigma^t(k) = k + t \mod n$ ולכן כאשר $t = n$ נקבל

$$\sigma^n(k) = k + n \mod n = k \implies \sigma^n = Id$$

נבחין כי עבור הפעולות מודולו מתקיים

$$(\sigma^t \circ \tau)(k) = (n - k + 1) + t = n - k + 1 + t = n - (k - t) + 1 = \tau \circ \sigma^{n-t}$$

ולכן כל איבר ב־D_n ניתן לכתיבה בצורה $\tau^{0,1}\sigma^n$ ולכן בהתאם נקבל כי $|D_n| = 2n$.

סעיף ג'

נבדוק לאילו $n \geq 3$ החבורה D_n מכילה תת־חבורה איזומורפית $\mathbb{Z}/2 \times \mathbb{Z}/2$.

נבחין כי כל תנאי ש־n זוגי נוכל לבחור $\langle \tau, \sigma^{\frac{n}{2}} \rangle$ תת־חבורה בעלת ארבעה איברים ונוכל להגדיר $\varphi : D_4 \xrightarrow{\sim} \mathbb{Z}/2 \times \mathbb{Z}/2$ על־ידי $\varphi(\tau^x \sigma^y) = (x, y)$.

שאלה 4

סעיף א'

נוכיח שמתקיים לכל $a, b \in \mathbb{N}$

$$\operatorname{lcm}(a,b) = \frac{ab}{\gcd(a,b)}$$

ואף שערך זה קיים תמיד והוא יחיד.

הוכחה. נגדיר $d = \gcd(a,b)$. נראה כי $d \mid b$ ולכן נגדיר $b_1 = b/d$.
בהתאם $\gcd(a, b_1) = 1$, כנביעה מהגדרת המחלק המשותף המקסימלי ישירות.
נגדיר גם $a_1 = a/d$ ולכן $a_1 b_1 d = ab$.
נשים לב שמהגדרת d נובע כי אין מספר קטן יותר כך ש־$eb_1 = b$ או $ea_1 = a$ ובהתאם $a_1 b_1$ הוא הכפולה המינימלית המשותפת ומתקיים

$$\operatorname{lcm}(a,b) = \frac{ab}{\gcd(a,b)}$$

והוא קיים לכל שני מספרים טבעיים ויחיד מיחידות gcd. $\square$

סעיף ב'

נוכיח כי מתקיים גם

$$\operatorname{lcm}(a,b)\mathbb{Z} = a\mathbb{Z} \cap b\mathbb{Z}$$

הוכחה. נשים לב כי קבוצת המספרים המתחלקים על־ידי a ו־b על־פי הגדרה מתחלקת גם ב־$\operatorname{lcm}(a,b)$, ולכן

$$\operatorname{lcm}(a,b)\mathbb{Z} \subseteq a\mathbb{Z} \cap b\mathbb{Z}$$

נראה גם כי כל מספר $c \in \operatorname{lcm}(a,b)\mathbb{Z}$ הוא כפולה של a וכן של b מהגדרת הכפולה המינימלית המשותפת, ולכן נובע

$$\operatorname{lcm}(a,b)\mathbb{Z} = a\mathbb{Z} \cap b\mathbb{Z}$$

$\square$

שאלה 5

סעיף א'

תהינה $H \leq G$ חבורה ותת־חבורה שלה. נוכיח שיש פונקציה הפיכה בין G/H לבין $H\backslash G$.

הוכחה. יהי $a, b \in G$, אם $aH = bH$ אם ורק אם קיימים איברים $h_1, h_2 \in H$ כך ש־$ah_1 = bh_2$ ולכן גם $h_1^{-1}a^{-1} = h_2^{-1}b^{-1}$.
אבל $h_1^{-1}, h_2^{-1} \in H$ שכן היא סגורה להופכי ונקבל כי $Ha^{-1} = Hb^{-1}$ אם ורק אם $aH = bH$.
נגדיר פונקציה $\varphi : G/H \to H\backslash G$ על־ידי

$$\varphi(aH) = Ha^{-1}$$

הפונקציה היא חד־חד ערכית על־פי הטענה שהוכחנו זה עתה, ונראה כי היא על:
נבחר Ha מחלקה ימנית כלשהי ב־$H\backslash G$. אז $\varphi(a^{-1}H) = Ha$ לכל $a \in G$ ולכן היא על.
מצאנו כי $G/H \xrightarrow{\sim} H\backslash G$.
נסיק כי החבורות מאותו סדר, ולכן $|G : H|$ הוא בלתי תלוי בבחירת מחלקה ימנית או שמאלית. □

סעיף ב'

תהינה $K \leq H \leq G$ חבורה ותת־חבורות כך ש־G/H ו־H/K סופיות.
נוכיח כי G/K סופי ומתקיים $|G/K| = |G/H| \cdot |H/K|$.

הוכחה. יהי $g \in G, h \in H$ ונראה כי gH, hK הן מחלקות של G/H ו־H/K בהתאמה.
לכל $h \in H$ קיים $g_1 \in G$ כך ש־$g = g_1 h$. לכן $gK = g_1 hK = g_1(hK)$.
נשים לב שיש כמות סופית של מחלקות hK ו־$g_1 H$ ולכן יש כמות קומבינציות סופית של בחירות כאלה שנוכל לעשות (לבחירות זרות).
מכאן נסיק ש־G/K עצמה היא סופית.
בחירת g, h היא קומבינציה בלתי תלויה ולכן חל עליה חוק הכפל של קומבינטוריקה ומתקיים $|G/K| = |G/H| \cdot |H/K|$. □

סעיף ג'

נמצא את האינדקס $|SL_n(\mathbb{F}_p) : GL_n(\mathbb{F}_p)|$
נגדיר $H = SL_n(\mathbb{F}_p)$, אז $\forall h \in H : |h| = 1$ על־פי הגדרת תת־החבורה.
תהי $a \in GL_n(\mathbb{F}_p)$, ונגדיר $k = |a|$, ידוע כי $0 < k < p$ בהתאם להגדרת השדה.
מתקיים גם $\forall h \in H : |ah| = |a| \cdot |h| = k$ על־פי חוקי דטרמיננטות.
נסיק כי כל מחלקת שקילות שומרת על גודל הדטרמיננטה, וידוע כי ישנם $k - 1$ גדלים אפשריים, ולכן נסיק גם

$$|SL_n(\mathbb{F}_p) : GL_n(\mathbb{F}_p)| = k - 1$$

שאלה 6

נוכיח שניתן ליצור את $SL_n(\mathbb{Z})$ על־ידי n^2-n איברים.

הוכחה. נבחן את המטריצות ההפיכות בעלות דטרמיננטה 1 מעל השלמים.

כל מטריצה הפיכה ניתן ליצור מצירוף של מטריצות אלמנטריות, ולכן נבחן את הקבוצה שלהן בלבד.

לא יתכן ששורה תהיה מוכפלת בסקלר שכן על שורה אחרת להיות מוכפלת בסקלר ההופכי, והוא לא קיים בשלמים, לכן כל איברי המטריצה הם 0 או 1.

בהתאם יש רק שני סוגים של פעולות אלמנטריות על המטריצה, החפלת שורות וצירוף לינראי של שורות.

על־ידי השיטה $\forall a,b\in\mathbb{Z}: a:=a+b, b:=a-b, a:=a-b$ ניתן להחליף את ערכם של שני משתנים, נשתמש באלגוריתם זה כדי להיות מסוגלים להחליף ערכי שורות שלמות על־ידי הוספת צירופים לינאריים של שורות. מסיבה זו אין צורך לכלול את המטריצות האלמנטריות להחלפת שורות בקבוצה, ונשארו מטריצות הוספת הצירוף הלינארי.

נשים לב שנוכל להוסיף כל שורה לכל שורה שונה ממנה שוב ושוב כדי להגיע לצירוף הלינארי השלם הרצוי, ולכן ישנן $n(n-1)$ מטריצות כאלה.

נוכל כמובן להשתמש בפעולות ההופכיות שלהן הנוצאות על־ידיהן בבנייה כדי להגיע לחיסור שורות, ולכן קבוצת מטריצות זו בונה את $SL_n(\mathbb{Z})$. $\square$