מבנים אלגבריים 89-214

פרופ' ע. וישנה

מועד ב', תשס"ט ־ פתרון

ענו על שאלות 1, 2 ו־3, ועל שתיים מבין השאלות 4–7. לכל השאלות ניקוד שווה. אפשר לקנות את ההגדרה של כל מושג המופיע במבחן, פרט לאלו המופיעים בשאלה 1, בשתי נקודות.
משך המבחן. שעתיים וחצי (לאחר הארכה).
חומר עזר מותר בשימוש: מחשבון מדעי וגרפי.

1. דייק וענה בקיצור:

(א) השלם: H היא תת־חבורה של $G = S_6$, ולכן, לפי משפט לגרנז', ... **פתרון**. הסדר שלה מחלק את 720.

(ב) הגדר מהי חבורת אוילר U_n. **פתרון**. U_n היא קבוצתה מספרים השלמים $1 \leq a \leq n$, הזרים ל־n, עם פעולת הכפל מודולו n.

(ג) פרש את הטענה "σ היא מחזור בחבורה S_n", בלי להשתמש בסימון המיוחד מהצורה (123).
פתרון. קיימים $a_1, \dots, a_m \in \{1, \dots, n\}$, שונים זה מזה, כך ש־ $\sigma(a_i) = a_{i+1}$ לכל $i = 1, \dots, m-1$, $\sigma(a_m) = a_1$, ו־ $\sigma(b) = b$ לכל b השונה מכל המספרים $a_1, \dots, a_m$.

(ד) נסח מחדש במונחים אלמנטריים (אינך מתבקש **להוכיח** את הטענה, אלא **לתרגם** אותה): האיבר 3 הוא אי־פריק בחוג $\mathbb{Z}[\sqrt{-6}] = \left\{n + m\sqrt{-6} :\ n, m \in \mathbb{Z}\right\}$, אבל אינו ראשוני שם. **פתרון**. לכל $x, y \in \mathbb{Z}[\sqrt{-6}]$, אם $3 = xy$, אז x או y הפיכים. מאידך, קיימים $u, v \in \mathbb{Z}[\sqrt{-6}]$ כך ש־ $3 \mid uv$ למרות ש־ $3 \nmid u$, $3 \nmid v$.

2. תן דוגמא נגדית לשלוש מבין ארבע הטענות (השגויות) הבאות. נמק בקיצור נמרץ מדוע הדוגמא עונה על הדרישות:

(א) כל תת־חבורה קומוטטיבית של חבורה G היא נורמלית. **פתרון**. תת־החבורה $\langle (12)(34) \rangle$ של A_5 קומוטטיבית כי היא ציקלית, אבל אינה נורמלית כי אין ל־ A_5 תת־חבורות נורמליות לא טריוויאליות.

(ב) כל שתי תמורות מאותו סדר, צמודות זו לזו. **פתרון**. התמורות $(12), (12)(34)$ מסדר 2, ואינן צמודות ב־ S_4 כי מבנה המחזורים שלהן שונה.

(ג) אם A, B חבורות אבליות מסדר 32 ו־ $A^4 \cong B^4$, אז $A \cong B$ (הערה: $H^4 = \left\{x^4 :\ x \in H\right\}$).
פתרון. החבורות $A = \mathbb{Z}_4 \times \mathbb{Z}_4 \times \mathbb{Z}_2$ ו־ $B = (\mathbb{Z}_2)^5$ מאותו סדר ו־ $A^4 = B^4 = 0$, אבל לראשונה אקספוננט 4 ולשניה 2, ולכן הן אינן איזומורפיות.

(ד) אם שני אברים בחבורה מתחלפים, אז אחד מהם הוא חזקה של השני. **פתרון**. האברים $3, 5 \in U_8$ מתחלפים, אבל $3 \notin \langle 5 \rangle$ ו־ $5 \notin \langle 3 \rangle = \langle 1, 3 \rangle$.

3. בכל אחת מן השלשות הבאות יש שתי חבורות איזומורפיות, ואחת יוצאת דופן, שאינה איזומורפית להן. הסבר בקיצור מדוע החבורות בזוג אחד איזומורפיות זו לזו, ומדוע החבורות בזוג אחר אינן איזומורפיות.

(א) $A = D_4$, $B = \mathbb{Z}_4 \times \mathbb{Z}_2$, $C = U_{30}$. **פתרון**. החבורה D_4 אינה אבלית, ולכן אינה איזומורפית לחבורות האחרות, שהן אבליות. $C \cong U_6 \times U_5 \cong \mathbb{Z}_2 \times \mathbb{Z}_4$.

(ב) $X = \mathbb{Z}_{30} \times \mathbb{Z}_{30}$, $Y = \mathbb{Z}_6 \times \mathbb{Z}_{10} \times \mathbb{Z}_{15}$, $V = \mathbb{Z}_{20} \times \mathbb{Z}_{45}$. **פתרון**. $X \cong (\mathbb{Z}_2 \times \mathbb{Z}_3) \times (\mathbb{Z}_2 \times \mathbb{Z}_5) \times (\mathbb{Z}_3 \times \mathbb{Z}_5) \cong \mathbb{Z}_6 \times \mathbb{Z}_{10} \times \mathbb{Z}_{15}$; לחבורות האלה אקפוננט 30, ולכן הן אינן איזומורפיות ל־ V שהאקספוננט שלה $\operatorname{lcm}(20, 45) = 90$.

(ג) $A_4 \times \mathbb{Z}_5$, A_5, ותת־החבורה $C = \langle (123), (124), (56789) \rangle$ של S_9. **פתרון**. הערה. כל החבורות מסדר 60 ואינן אבליות; לא הגדרנו את האקספוננט של חבורה לא אבלית, אבל לו היינו מגדירים, האקספוננט של כל החבורות האלה הוא 30. החבורה $C = \langle (123), (124), (56789) \rangle \cong \langle (123), (124) \rangle \times \langle (56789) \rangle$, משום שהיוצרים מתחלפים. $(123), (124)$ יוצרות תת־חבורה מסדר המתחלק ב־3 וגדול ממנו, של A_4, ולכן $C \cong A_4 \times \mathbb{Z}_5$. בחבורה הזו יש איבר מסדר 15 ($((123), 1)$), וב־ A_5 אין איבר כזה, ולכן הן אינן איזומורפיות.

4. הוכח שאם $G/\mathrm{Z}(G)$ היא חבורה ציקלית, אז G אבלית. **הערה**. לחבורה D_4 יש מרכז $\langle \sigma^2 \rangle$, והיא אינה אבלית, למרות ש־ $D_4/\langle \sigma^2 \rangle \cong \mathbb{Z}_2^2$ אבלית. בכל חבורה אבלית G, $G/\mathrm{Z}(G)$ ציקלית (טריוויאלית), ולא ניתן להסיק מכך שהחבורה עצמה ציקלית. **פתרון**. לפי הנתון קיים $g \in G$ כך ש־ $G/\mathrm{Z}(G) = \{g^i\mathrm{Z}(G)\}$. יהיו $x, y \in G$, אז קיימים $i, j \in \mathbb{Z}$ ו־ $z, z' \in \mathrm{Z}(G)$ כך ש־ $x = g^i z$ ו־ $y = g^j z'$. לכן $xy = g^i z g^j z' = g^{i+j} z z' = g^{j+i} z' z = g^j z' g^i z = yx$.

5. הוכח את 'משפט N/C': תהי $A \leq G$ תת־חבורה. הוכח שקיים הומומורפיזם חד־חד־ערכי של $\mathrm{N}_G(A)/\mathrm{C}_G(A)$ לתוך $\mathrm{Aut}(A)$, כאשר $\mathrm{N}_G(A)$ הוא המנרמל ו־ $\mathrm{C}_G(A)$ הוא המרכֵּז של A. **פתרון**. לכל $g \in \mathrm{N}_G(A)$ אפשר להגדיר $\gamma_g : A \to A$ לפי $\gamma_g(a) = gag^{-1}$, וההעתקה מוגדרת היטב משום ש־ $gAg^{-1} \subseteq A$. חישוב ישיר מראה ש־ $\psi : \mathrm{N}_G(A) \to \mathrm{Aut}(A)$ המוגדר לפי $\psi(g) = \gamma_g$ הוא הומומורפיזם, ו־ $\mathrm{Ker}(\psi) = \{g \in \mathrm{N}_G(A) : \gamma_g = 1\} = \mathrm{C}_G(A)$. לפי משפט האיזומורפיזם הראשון $\mathrm{N}_G(A)/\mathrm{C}_G(A) \cong \mathrm{Im}(\psi) \leq \mathrm{Aut}(A)$. **הערה**. התמונה אינה בהכרח מוכלת ב־ $\mathrm{Inn}(A)$; למשל כאשר A אבלית.

6. (א) הוכח שכל איבר ראשוני בתחום שלמות הוא אי־פריק. **פתרון**. יהי $p \in D$ ראשוני. אם $p = ab$ אז $p \,|\, p = ab$ ולכן p מחלק את אחד הגורמים, למשל $p \,|\, a$. מכאן ש־ $a = pc$ עבור $c \in R$ מתאים, ואז $p = ab = pbc$, ומכאן $bc = 1$ ו־ b הפיך.

   (ב) הוכח שבתחום ראשי, כל איבר אי־פריק הוא ראשוני. **פתרון**. יהי $a \in R$ איבר אי־פריק. ראשית נראה ש־ Ra אידיאל מקסימלי. הרי אם $Ra \subseteq I \langle R \rangle$ אפשר לכתוב $I = Rx$ לאיבר $x \in R$ מתאים, וכך $x \,|\, a$; אבל a אי־פריק, ולכן x הפיך (אז $I = R$) או חבר של a (ואז $I = Ra$). פתרון ראשון: כאידיאל מקסימלי, Ra ראשוני, ולכן היוצר שלו a ראשוני. פתרון שני: נניח ש־ $xy \in Ra$, אבל $x, y \notin Ra$. בגלל המקסימליות $Ra + Rx = Ra + Ry = R$, אבל אז $R = R \cdot R = (Ra + Rx)(Ra + Ry) = Ra^2 + Rax + Ray + Rxy \subseteq Ra$, סתירה.

7. ענה על שניים מתוך שלושת הסעיפים:

   (א) הוכח שהחוג $\left\{ \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} : a, b \in \mathbb{Z}/5\mathbb{Z} \right\}$ אינו איזומורפי לשדה מסדר 25. **פתרון**. בחוג הזה יש איבר, $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$, שריבועו 0 ולכן הוא מחלק אפס; לכן זה אינו שדה.

   (ב) נסמן ב־ $\mathbb{F}_8$ את השדה מסדר 8. כתוב כסכום ישר של חבורות ציקליות, עד־כדי איזומורפיזם, את החבורות $(\mathbb{F}_8, +, 0)$, ו־ $(\mathbb{F}_8 - \{0\}, \cdot, 1)$. **פתרון**. לחבורה החיבורית יש אקספוננט 2, ולכן היא איזומורפית ל־ $(\mathbb{Z}_2)^3$. החבורה הכפלית מסדר 7, ולכן היא ציקלית ואיזומורפית ל־ $\mathbb{Z}_7$. **הערה**. לכן כל איבר $1 \neq 0, 1$ הוא מסדר 7.

   (ג) פרק לגורמים אי־פריקים מעל $\mathbb{Z}/3\mathbb{Z}$ את הפולינום $x^9 - x$. **פתרון**. $x^9 - x = x(x^4 - 1)(x^4 + 1) = x(x^2 - 1)(x^2 + 1)(x^4 + 1) = x(x - 1)(x + 1)(x^2 + 1)(x^2 - x - 1)(x^2 + x - 1)$. הגורמים מסדר 2 אי־פריקים כי הדיסקרימיננטה שלהם -1 אינה ריבוע, ולכן אין להם שורשים. **הערה**. הפולינום $x^4 + 1$ מוכרח להיות פריק, כי הוא מחלק את $x^9 - x$, ולכן השורשים שלו הם איברים של השדה $\mathbb{F}_9$, שהוא ממימד 2 מעל $\mathbb{F}_3$, ואין בו מקום לתת־שדה ממימד 4.