

פתרון מבחן בקורס מבנים אלגבריים להנדסה 83-218

מועד א', סמסטר קיץ תשע"ז

מראה: תומר באואר **מתרגלת:** עדי בן צבי **משך המבחן:** שעתיים וחצי
הוראות: יש לענות על 4 שאלות מתוך חמש השאלות הראשונות, ובנוסף יש שאלת בונוס. סמנו באופן ברור בראש כל עמוד לאיזו שאלה הוא מתייחס, ונא לא לפתור סעיפים משאלות שונות באותו עמוד.
חומר עזר: אין, גם לא מחשבון.

שאלה 1. תהינה G, H חבורות.

1. (9 נק') הוכיחו או הפריכו: אם G, H הן ציקליות, אז $G \times H$ ציקלית.

2. (8 נק') הוכיחו או הפריכו: אם $G \times H$ אבלית, אז G, H הן אבליות.

3. (8 נק') הוכיחו או הפריכו: אם $|G| = |H| = 6$, אז $G \cong H$.

פתרון. כאשר מפריכים טענה יש להביא דוגמה נגדית. לא מספיק לומר "יתכן שאין כאלו..." או "לפעמים הטענה לא נכונה...".

1. הפרכה. הדוגמה הנפוצה ביותר הייתה לבחור $G = H = \mathbb{Z}_2$ שהן ציקליות, ואילו $G \times H = \mathbb{Z}_2 \times \mathbb{Z}_2$ אינה ציקלית. בחבורה ציקלית הסדר של יוצר הוא סדר החבורה, ובחבורה $G \times H$ מתקיים לכל איבר (a, b) כי

$$(a, b) + (a, b) = (2a, 2b) = (0, 0) = e_{G \times H}$$

כי החיבור הוא מודולו 2. לכן הסדר של כל איבר הוא לכל היותר 2, אבל הסדר של החבורה הוא $|G \times H| = 4$. טעויות שהופיעו: לטעון כי $\mathbb{Z}_2 \times \mathbb{Z}_3$ היא לא ציקלית (יוצר לדוגמה הוא האיבר $(1, 1)$) או להוכיח כי $G \times H$ ציקלית על ידי בדיקת חזקות של איבר אחד ספציפי.

2. כל תת-חבורה של חבורה אבלית היא אבלית. לכן תת-החבורות $G \times \{e_H\}$ ו- $\{e_G\} \times H$ של $G \times H$ הן אבליות. כמו כן $G \cong G \times \{e_H\}$ ו- $\{e_G\} \times H \cong H$. אבליות נשמרת תחת איזומורפיזם, ולכן G ו- H הן אבליות. דרך הוכחה אחרת (ונכונה לחלוטין) להוכחת הסעיף הייתה לטעון שלכל $(g_1, h_1), (g_2, h_2) \in G \times H$ מתקיים

$$(g_1 g_2, h_1 h_2) = (g_1, h_1) (g_2, h_2) = (g_2, h_2) (g_1, h_1) = (g_2 g_1, h_2 h_1)$$

עקב האבליות של $G \times H$. בהשוואת איבר איבר נקבל שלכל $g_1, g_2 \in G$ מתקיים $g_1 g_2 = g_2 g_1$ ולכל $h_1, h_2 \in H$ מתקיים $h_1 h_2 = h_2 h_1$, וזו בדיקת ההגדרה לכך ש- G, H הן אבליות.

3. הפרכה. נבחר $G = \mathbb{Z}_6$ ו- $H = S_3$. החבורה G אבלית, אבל H לא (למשל $(12)(13) \neq (13)(12)$). אבליות נשמרת תחת איזומורפיזם, ולכן G ו- H הן לא איזומורפיות. טעויות נפוצות: לבחור $H = \mathbb{Z}_2 \times \mathbb{Z}_3$ ולטעון שאינה איזומורפית ל- \mathbb{Z}_6 , אף על פי שהן כן איזומורפיות; לבחור חבורות מסדר שאינו 6; להוכיח שהעתקה ספציפית $\varphi: G \rightarrow H$ אינה איזומורפיזם ולכן הן לא איזומורפיות; למעשה עד כדי איזומורפיזם יש שתי חבורות מסדר 6 והן \mathbb{Z}_6 ו- S_3 , ולכן כל הפרכה תחייב לבחור את החבורות האלו או חבורות שאיזומורפיות אליהן.

שאלה 2. תהי G חבורה. הגדרנו שהמרכז של G הוא הקבוצה

$$Z(G) = \{g \in G \mid \forall h \in G, gh = hg\}$$

1. (15 נק') הוכיחו כי $Z(G) \triangleleft G$. יש להוכיח שהיא תת-חבורה ושהיא נורמלית.

2. (10 נק') הוכיחו כי $Z(Z(G)) = Z(G)$.

פתרון.

1. אנחנו נוכיח ש- $Z(G)$ תת-חבורה של G לפי האיפיון שראינו בכיתה לפיו מספיק להראות כי $Z(G)$ אינה ריקה, סגורה להופכי וסגורה לפעולה.

נראה כי $e \in Z(G)$ מפני שלכל $g \in G$ לפי הגדרת איבר יחידה מתקיים $eg = ge$. עבור סגירות להופכי נניח $g \in Z(G)$. אזי לכל $h \in G$ מתקיים $gh = hg$. נכפיל משמאל ומימין ב- g^{-1} ונקבל $hg^{-1} = g^{-1}h$, ולכן $g^{-1} \in Z(G)$. עבור סגירות לפעולה נניח $g_1, g_2 \in Z(G)$. אזי לכל $h \in G$ מתקיים $g_i h = h g_i$ עבור $i \in \{1, 2\}$. לכן $g_1 g_2 h = g_1 h g_2 = h g_1 g_2$, ונסיק כי $g_1 g_2 \in Z(G)$. בסך הכל הראנו $Z(G) \leq G$.

עבור הוכחת הנורמליות ניתן להוכיח שיוויון מחלקות שמאליות וימניות, אך אנחנו נוכיח סגירות להצמדה. לכל $g \in Z(G)$ ולכל $h \in G$ מתקיים $hgh^{-1} = ghg^{-1} = g \in Z(G)$ ולכן $Z(G) \triangleleft G$, כדרוש.

טעויות נפוצות: רבים ניסו להוכיח עם הקריטריון המקוצר לתת-חבורה והסתבכו. כפי שאמרנו בכיתה, בדרך כלל הקריטריון המקוצר אינו חוסך זמן, ובמקרה הספציפי הזה מצריך בפועל את כל ההוכחה לעיל. בכל מקרה, הדרישות בקריטריון המקוצר הן ש- $Z(G)$ אינה ריקה ושכל $g_1, g_2 \in Z(G)$ גם $g_1 g_2^{-1} \in Z(G)$. הדרישה האחרונה משמעה שלכל $h \in G$ מתקיים $h g_1 g_2^{-1} = g_1 g_2^{-1} h$. טעות נוספת הייתה שאחרי שמראים כי $e \in Z(G)$, אז כדי להוכיח את הסגירות להופכי נטען שאם $g \in Z(G)$, אז קיים הופכי $g^{-1} \in G$, לכן $g^{-1} \in Z(G)$ ואז $Z(G)$ סגורה להופכי. אך זו טענה שנכונה לכל תת-קבוצה שמכילה את e , שאינה מוכיחה כי $g^{-1} \in Z(G)$.

נעיר שניתן להוכיח כי $Z(G)$ תת-חבורה נורמלית "בבת-אחת" על ידי זה שמראים שזהו גרעין של הומומורפיזם כלשהו שתחמומו G . ישנו איזומורפיזם $G/Z(G) \cong \text{Inn}(G)$ כאשר $\text{Inn}(G)$ היא חבורת האוטומורפיזמים הפנימיים של G , עליה לא דיברנו בכיתה. ההוכחה של איזומורפיזם זה כנראה יותר מסובכת מההוכחה הישירה לעיל.

2. דרך נוחה להוכחה היא על ידי הכלה דו-כיוונית. קל לראות כי $Z(Z(G)) \subseteq Z(G)$, שהרי

$$Z(Z(G)) = \{g \in Z(G) \mid \forall h \in Z(G), gh = hg\}$$

כלומר לפי הגדרה איברי $Z(Z(G))$ הם איברים של $Z(G)$. בכיוון השני כל איבר של $Z(G)$ מתחלף עם כל איברי G , ובפרט עם איברי $Z(G)$ (שהיא תת-קבוצה של G), ולכן שייך ל- $Z(Z(G))$.

טעויות נפוצות בהוכחה היו להוכיח רק את הכיוון הקל, או להתבלבל בין הגדרת איבר הפיך (בחבורה כל איבר הוא הפיך) ובין איברים מתחלפים.

בדרך אחרת, אפשר להוכיח שחבורה G היא אבלית אם ורק אם $Z(G) = G$. בסעיף הקודם הוכחנו כי $Z(G)$ חבורה, והיא אבלית כי כל האיברים שלה מתחלפים אחד עם השני, ולכן $Z(Z(G)) = Z(G)$.

שאלה 3. יהי R חוג, ויהיו $I, J \triangleleft R$ אידאלים.

1. (13 נק') הוכיחו או הפריכו: תמיד מתקיים $I \cap J \triangleleft R$.

2. (12 נק') הוכיחו או הפריכו: תמיד מתקיים $I \cup J \triangleleft R$.

פתרון. שימו לב שתכונת הבליעה מתקיימת גם לחיתוך אידאלים וגם לאיחוד אידאלים, ולכן השאלה בודקת האם החיתוך או האיחוד הם תת-חבורות חיבוריות. השאלה האם חיתוך או איחוד תת-חבורות הוא תת-חבורה הוא תרגיל שכבר פתרם.

1. תחילה נראה כי $I \cap J$ היא תת־חבורה חיבורית: נראה $I \cap J \neq \emptyset$. ידוע לנו כי I, J הם תת־חבורות חיבוריות של R . לכן $0 \in I, J$ ולכן $0 \in I \cap J$. יהי $i \in I \cap J$. אזי $-i \in I$ וגם $-i \in J$ כי I, J סגורות להופכי (של פעולת החיבור!) ולכן $-i \in I \cap J$ וקיבלנו סגירות להופכי. יהיו $i_1, i_2 \in I, J$. אזי $i_1 + i_2 \in I$ וגם $i_1 + i_2 \in J$ כי I, J סגורות לפעולה ולכן גם $i_1 + i_2 \in I + J$ וקיבלנו סגירות לפעולה.
 נותר להוכיח את תכונת הבליעה. לכל $i \in I \cap J, r \in R$ מתקיים $i \cdot r, r \cdot i \in I$ וגם $i \cdot r, r \cdot i \in J$ כי I, J הם אידאלים. לכן $i \cdot r, r \cdot i \in I \cap J$ לכל בסך הכל $I \cap J$ אידאל של R .

2. נפריך עם הדוגמה שראינו לגבי איחוד תת־חבורות. נבחר $R = \mathbb{Z}$ ואת האידאלים $I = 2\mathbb{Z}, J = 3\mathbb{Z}$ (אלו אידאלים ראשיים, ובפרט אידאלים). אזי $I \cup J$ אינו אידאל כי אינו סגור לפעולה. למשל $2, 3 \in I \cup J$, אבל $2 + 3 = 5 \notin I \cup J$.
 למעשה $I \cup J$ הוא אידאל אם ורק אם $I \subseteq J$ או $J \subseteq I$. לכן כל דוגמה נגדית מחייבת זוג אידאלים שלא מוכל אחד בשני.

שאלה 4. יהי F שדה ויהי $f(x) \in F[x]$. נגדיר כי $a \in F$ הוא שורש של $f(x)$ אם $f(a) = 0$.

1. (10 נק') הוכיחו כי a הוא שורש של $f(x)$ אם ורק אם $(x - a) | f(x)$.
 רמז: בכיוון הקשה העזרו בחלוקה אוקלידית.

2. (10 נק') נניח כי $f(x)$ הוא פריק ומקיים $\deg f(x) \leq 3$. הוכיחו שיש לו שורש ב- F .
 רמז: העזרו בסעיף הראשון.

3. (5 נק') הפריכו, בעזרת דוגמה נגדית, את הסעיף השני כאשר $\deg f(x) > 3$ ו- F סופי. פתרו. כדאי מאוד לעבור על ההגדרות לפתרון שאלה זאת.

1. בכיוון הקל נניח כי $(x - a) | f(x)$. לכן $f(x) = (x - a)g(x)$ עבור איזשהו $g(x) \in F[x]$. נציב $x = a$ ונקבל

$$f(a) = (a - a)g(a) = 0 \cdot g(a) = 0$$

לכן $f(a) = 0$, כלומר a הוא שורש של $f(x)$.
 בכיוון הקשה נניח כי a הוא שורש של $f(x)$. צריך להוכיח ש- $(x - a)$ מחלק את $f(x)$. מה אפשר לעשות? לנסות לחלק "בכוח" בעזרת חלוקה אוקלידית של פולינומים. לפי מה שהוכחנו בכיתה קיימים $q(x), r(x) \in F[x]$ עבורם

$$f(x) = (x - a)q(x) + r(x)$$

וגם $\deg r(x) < \deg(x - a) = 1$. לכן $r(x)$ הוא פולינום קבוע, נניח $r(x) = c$ לכל x . נציב $x = a$ ונקבל

$$0 = f(a) = (a - a)q(a) + c = c$$

וקיבלנו כי $c = 0$. כלומר $f(x) = (x - a)q(x)$, ולכן $(x - a) | f(x)$.

2. לפי הגדרה, אם $f(x)$ פריק ניתן להציג אותו כמכפלה $f(x) = p(x)q(x)$ כאשר

$$0 < \deg p(x), \deg q(x) < \deg f(x) \leq 3$$

ראינו שהמעלה של מכפלת פולינומים היא סכום המעלות. נסיק שבפתרונות האפשריים בשלמים של המשוואה

$$\deg p(x) + \deg q(x) = \deg f(x) \leq 3$$

נקבל כי $\deg p(x) = 1$ או $\deg q(x) = 1$ (אולי שניהם אם $\deg f(x) = 2$). בלי הגבלת הכלליות נניח כי $p(x) = bx + c$ כאשר $b \neq 0$ (אחרת $q(x)$ ממעלה 1). לכן $f(x) = (x + b^{-1}c) \cdot (b \cdot q(x))$, ולפי הסעיף הקודם נקבל כי $-b^{-1}c \in F$ הוא שורש של $f(x)$.

3. הדרך הקלה ביותר היא לבחור פולינום אי פריק ממעלה 2 או 3 שלפי הסעיף הקודם אפשר להוכיח אי פריקות על ידי זה שנבדוק שאין לו שורשים ב- F , ולהעלות אותו בריבוע. נבחר למשל $g(x) = x^2 + x + 1$ מעל השדה $F = \mathbb{F}_2$. נבדוק

$$g(0) = 0^2 + 0 + 1 = 1, \quad g(1) = 1^2 + 1 + 1 = 1$$

לכן $f(x) = g(x)^2$ פריק לפי בנייתו ומתקיים $\deg f(x) = 4 > 3$, אבל אין לו שורשים ב- \mathbb{F}_2 . טעויות נפוצות: לבחור פולינום אי פריק, לבחור פולינום עם שורשים בשדה, לא לציין מעל איזה שדה מדובר (פריקות פולינומים תלויה בשדה) או לא להוכיח שהפולינום אי פריק.

שאלה 5. הזכרו כי \mathbb{F}_{27} מציין את השדה בן 27 איברים.

1. (15 נק') בנו באופן מפורש את \mathbb{F}_{27} כמנה של חוג הפולינומים $\mathbb{F}_3[x]$.

2. (10 נק') הוכיחו שכל איבר של \mathbb{F}_{27} הוא שורש של הפולינום $x^{27} - x$.
רמז: אפשר להעזר במסקנה ממשפט לגראנז'.

פתרון.

1. נשים לב כי $27 = 3^3$. כל שדה סופי מסדר p^k ניתן להציג כחוג מנה $\mathbb{F}_p[x]/I(f)$ כאשר $I(f)$ הוא האידיאל הראשי הנוצר על ידי פולינום אי פריק f מעל $\mathbb{F}_p = \mathbb{Z}_p$ ממעלה k . לפי שאלה 4 אפשר להוכיח שפולינום ממעלה 3 הוא אי פריק מעל \mathbb{F}_3 על ידי זה שנראה שאין לו שורשים ב- \mathbb{F}_3 (בסך הכל צריך שלוש הצבות).

תמיד אפשר לבחור את f להיות מתוקן, ומבין 27 הפולינומים המתוקנים ממעלה 3 מעל \mathbb{F}_3 ישנם שמונה שהם אי פריקים. כלומר יש בערך 30 אחוז סיכוי לבחור באקראי פולינום אי פריק, ואם מתעלמים מפולינומים שהם בודאי פריקים כמו x^3 או $x^3 + x$, הסיכוי עולה. אנחנו נבחר $f(x) = x^3 + 2x + 1$. נבדוק שהוא אי פריק על ידי הצבה

$$f(0) = 0^3 + 2 \cdot 0 + 1 \equiv 1 \pmod{3}$$

$$f(1) = 1^3 + 2 \cdot 1 + 1 \equiv 1 \pmod{3}$$

$$f(2) = 2^3 + 2 \cdot 2 + 1 \equiv 1 \pmod{3}$$

ולכן $\mathbb{F}_{27} \cong \mathbb{F}_3[x]/I(f)$.

2. נבדוק עבור $x = 0$ שאכן מתקיים $0^{27} - 0 = 0$. עבור כל איבר אחר $a \in \mathbb{F}_{27}^* = \mathbb{F}_{27} \setminus \{0\}$ נזכר שבמסקנה ממשפט לגראנז' לפיה לכל איבר $g \in G$ בחבורה סופית מתקיים $g^{|G|} = e_G$. בחבורה הכפלית של השדה \mathbb{F}_{27}^* מתקיים $a^{26} = 1$. נכפיל ב- a ונקבל $a^{27} - a = 0$, כלומר $a^{27} - a = 0$ הוא שורש של $x^{27} - x$.

שאלת בונוס (7 נק') יהיו $n, m, r \in \mathbb{N}$. הוכיחו (בקצרה!) בעזרת משפט מהקורס כי

$$n! \cdot m! \cdot r! \mid (n + m + r)!$$

פתרון. תהינה $X \subseteq Y$ קבוצות. אז החבורה S_X איזומורפית לתת-החבורה של S_Y שבה נמצאות כל התמורות $\sigma: Y \rightarrow Y$ המקבעות את איברי $Y \setminus X$ (כלומר $\sigma(a) = a$ לכל $a \in Y \setminus X$). אם $X_1, \dots, X_n \subseteq Y$ תת-קבוצות כאשר X_i הן זרות בזוגות, אז ישנה תת-חבורה $S_{X_1} \times \dots \times S_{X_n} \leq S_Y$ במקרה שלנו נבחר $Y = \{1, \dots, n + m + r\}$. אז לחבורה S_{n+m+r} יש תת-חבורה

$$S_{\{1, \dots, n\}} \times S_{\{n+1, \dots, n+m\}} \times S_{\{n+m+1, \dots, n+m+r\}} \leq S_{n+m+r}$$

שאיזומורפית ל- $S_n \times S_m \times S_r$. לפי משפט לגראנז' הסדר של תת-חבורה מחלק את סדר החבורה, ולכן $n! \cdot m! \cdot r! \mid (n + m + r)!$

בהצלחה!