

אלגברה מופשטת 2 – תרגיל בית 2

מתרגלים: ד"ר אפי כהן ואדם צ'פמן.

1. הוכיחו כי כל תחום שלמות סופי הוא שדה.

פיתרון: יהי a איבר שונה מאפס בתחום שלמות סופי כלשהו. הקבוצה $\{a^n : n \in \mathbb{N}\}$ היא

סופית בגלל סופיות החוג. לכן קיימים $n > m$ שעבורם $a^n = a^m$. לכן

$$a^n - a^m = a^m(a^{n-m} - 1) = 0. \text{ בגלל שמדובר בתחום שלמות, } a^m \neq 0, \text{ ולכן}$$

$$a^{n-m} = 1, \text{ משמע } a \text{ הפיך.}$$

2. הוכיחו:

a. אם החבורה החיבורית של חוג עם יחידה היא ציקלית אז החוג קומוטטיבי.

b. הוכיחו כי אם הגודל של חבורה זו ראשוני אז החוג הוא שדה.

פיתרון: סעיף ב נובע מסעיף א ומהתרגיל הקודם. נוכיח את סעיף א. החבורה החיבורית היא

ציקלית אזי היא נוצרת על ידי איבר כלשהו g . יהיו שני איברים כלשהם בחוג, בפרט הם

בחבורה אז אפשר לסמנם כ ng ו mg ל $m, n \in \mathbb{N}$ כלשהם $(ng = g + \dots + g)$ n -times.

כעת, $(mg)(ng) = (mn)g^2 = (nm)g^2 = (ng)(mg)$, ולכן החוג קומוטטיבי.

3. הוכיחו כי אידיאל שמאלי שונה מאפס מכיל איבר הפיך אם ורק אם הוא כל החוג

[כאשר מדובר בחוג עם יחידה].

פיתרון: אם האידיאל הוא כל החוג אז הוא מכיל את איבר היחידה, שהוא איבר הפיך. אם

האידיאל מכיל איבר הפיך a אזי לכל b בחוג, האיבר $(ba^{-1})a$ נמצא באידיאל השמאלי,

ולכן b נמצא שם, ולכן האידיאל הוא כל החוג.

4. הוכח או הפרך:

a. אם I אידיאל אזי הקבוצה $\{1 - a : a \in I\}$ סגורה לכפל.

b. $R(a + b) = Ra + Rb$ לכל a, b בחוג R .

c. איחוד של אידיאלים הוא אידיאל.

d. יהיו $R \subseteq S$ חוגים ויהי $I \triangleleft R$, אזי $I \triangleleft S$.

פיתרון: סעיף א נכון. לכל $a, b \in I$,

ולכן $a + b - ab \in I$ אבל $(1 - a)(1 - b) = 1 - a - b + ab = 1 - (a + b - ab)$

$(1 - a)(1 - b) \in \{1 - a : a \in I\}$

סעיף ב לא נכון. אם לוקחים $R = \mathbb{Z}$ ו $a = b = 1$ אזי

$R(a + b) = 2\mathbb{Z} \neq \mathbb{Z} = \mathbb{Z} + \mathbb{Z} = Ra + Rb$

סעיף ג לא נכון. ניקח $R = \mathbb{Z}$, $I = 2\mathbb{Z}$ ו $J = 3\mathbb{Z}$. הקבוצה $J \cup I$ אינה סגורה לחיבור

(למשל $2 + 3 = 5 \notin J \cup I$) ולכן איננה אידיאל.

סעיף ד לא נכון. ניקח למשל את $S = F[x : x^2 = 0]$ לאיזשהו שדה F , וניקח

$I = R = F$. מתקיים $I \triangleleft R$ אך לא $I \triangleleft S$.

5. נביט בחוג $R = \{a + bx : a, b \in \mathbb{Z}_7\}$, כאשר החיבור הוא חיבור של מקדמים

והכפל הוא הסטנדרטי על אברי \mathbb{Z}_7 וגם $x^2 = c$ לאיזשהו $c \in \mathbb{Z}_7$. קבעו האם

החוג הוא שדה במקרים הבאים:

a. $c = 2$

b. $c = 3$

פיתרון: המספר 2 הוא ריבוע ב \mathbb{Z}_7 , $3^2 = 2$, ולכן מתקיים

$(x - 3)(x + 3) = x^2 - 3^2 = 0$, משמע ישנם מחלקי אפס ב R ולכן הוא לא שדה.

נוכיח כי עבור $c = 3$ מקבלים שדה. מספיק להראות שאין מחלקי אפס (שמדובר בתחום

שלמות) לפי תרגיל קודם. יהיו שני איברים שונים מאפס $a + bx$ ו $c + dx$. אם $d = 0$ אז

$c + dx = c$ הפיף ולכן המכפלה שונה מאפס. תוצאה דומה מקבלים עבור $b = 0$. נניח

ש $r = ab^{-1}$ כאשר $(a + bx)(c + dx) = bd(r + x)(s + x)$ אזי $b, d \neq 0$
 ו $s = cd^{-1}$. המכפלה הזו שווה לאפס אם ורק אם $(r + x)(s + x)$ שווה לאפס. אם
 $r \neq -s$ אזי המקדם של x יוצא שונה מאפס ולכן $(r + x)(s + x)$ שונה מאפס. לכן
 $(r + x)(s + x)$ יכול להיות שווה לאפס רק במקרה ש $r = -s$. זה אומר שישנם מחלקי
 אפס רק אם קיים $s \in \mathbb{Z}_7$ כך ש $(x - s)(x + s) = x^2 - s^2 = 0$ במקרה שלנו $x^2 = 3$
 והוא איננו ריבוע ב \mathbb{Z}_7 ולכן אין מחלקי אפס.

6. קבעו האם קיים הומומורפיזם $\varphi : R \rightarrow S$ (לאו דוקא יוניטרי) $\varphi \neq 0$, כאשר:

a. $R = \mathbb{Z}_m$ ו $S = \mathbb{Z}_n$ כאשר $m | n$.

b. $R = \mathbb{Z}_m$ ו $S = \mathbb{Z}_n$ כאשר $n | m$ וגם $0 < m \neq n$.

פיתרון: בסעיף א קיים. אם ניקח $\varphi : R \rightarrow S$ להיות ההעתקה שלוקחת כל מספר מודולו m
 נקבל הומומורפיזם.

בסעיף ב קיים בתנאים מסויימים. נביט ב $\varphi(1)$. נביט ב $\varphi(1) = \varphi(1^2) = (\varphi(1))^2$. ולכן $\varphi(1)$
 צריך להיות אידמפוטנט. איך נראים האידמפוטנטים ב \mathbb{Z}_m ? אם הפירוק של m לראשוניים
 הוא $p_1^{d_1} \dots p_k^{d_k}$ אזי נביט במשוואה $x \equiv x^2 \pmod{m}$. מכיוון שלכל $i \neq j$, $\mathbb{Z}_{p_i^{d_i}}$
 ו $\mathbb{Z}_{p_j^{d_j}}$ הם קומקסיליים, לפי משפט השאריות הסיני צריך למצוא פיתרון למערכת

המשוואות $x \equiv x^2 \pmod{p_i^{d_i}}$ כאשר $1 \leq i \leq k$. ב $\mathbb{Z}_{p_i^{d_i}}$ כל אידמפוטנט הוא או

נילפוטנטי או הפיך. אולם האידמפוטנט הנילפוטנטי היחיד הוא 0 וההפיך היחיד הוא 1, ולכן
 ישנם רק שני פתרונות למשוואה והם 0 ו 1.

כלומר, יש אידמפוטנט אחד בדיוק לכל תת-קבוצה של $\{1, \dots, k\}$ והוא מתחלק

ב $\prod_{i \in I} p_i^{d_i}$ ולא באף אחד משאר הראשוניים בקבוצה, כלומר $\prod_{i \in I} p_i^{d_i}$ זהו גם המחלק

המשותף המקסימלי של אותו אידמפוטנט עם m . נגיד ש $\varphi(1)$ הוא האידמפוטנט המתאים

לתת-קבוצה $I \subseteq \{1, \dots, k\}$, אזי מתקיים

$$o(\varphi(1)) = \frac{m}{\gcd(\varphi(1), m)} = \prod_{i \in \{1, \dots, k\} \setminus I} p_i^{d_i} \mid n$$

איזומורפית לתת-חבורה חיבורית של \mathbb{Z}_n .

משמע, כדי שיהיה קיים איזומורפיזם כזה (לא אפסי), n צריך להתחלק ב $p_i^{d_i}$ עבור לפחות אחד בין 1 ל k .

זה תרגיל די פשוט להראות את הכיוון השני, כלומר שאם n מתחלק ב $p_i^{d_i}$ אז ההומורפיזם הלוקח את $\varphi(1)$ לאידמפוטנט המתאים הוא מוגדר היטב.

[הערה: אם במקום ההומורפיזם רוצים מונומורפיזם, אזי זה קיים אם ורק אם קיימת תת-

$$[\prod_{i \in \{1, \dots, k\}} p_i^{d_i} = n \text{ שעבורה } I \subseteq \{1, \dots, k\}$$

7. נביט בחוג הפולינומים $R[x]$ מעל תחום שלמות R . האם I אידיאל כאשר

$$I = \{f \in R[x] : f(137) = 0\} \quad .a$$

$$I = \{f \in R[x] : f(1) = 10\} \quad .b$$

$$I = \{f \in R[x] : f(0) = 0\} \quad .c$$

פיתרון: סעיף א נכון. אם ניקח מכפלה gf ונציב בה 137 אזי בגלל הקומוטטיביות של החוג

זה יהיה שקול ללהציב 137 בכל אחד מהפולינומים ולהכפיל את התוצאות, ובגלל שבאחד

מהם נקבל אפס התוצאה תהייה גם כן אפס. מאותה הסיבה גם סעיף ג נכון.

סעיף ב לא נכון. אם ניקח $f \cdot f$ אזי הצבת 1 תיתן 100 ולכן לא מדובר באידיאל.