

מבוא לחוגים ומודולים
מערכי תרגול קורס 88-212

מהדורת קריאה מוקדמת

מרץ 2017, גרסה 0.5

תוכן העניינים

3	מבוא	
4	1 תרגול ראשון	
6	2 תרגול שני	
8	3 תרגול שלישי	
10	4 תרגול רביעי	

מבוא

כמה הערות טכניות לתחילת הקורס:

- דף הקורס נמצא באתר www.math-wiki.com.
- שאלות בנוגע לחומר הלימודי מומלץ לשאול בדף השיחה באתר של הקורס.
- הקפידו למלא את דו"ח תרגיל הבית.
- החומר בקובץ זה נאסף מכמה מקורות, ומבוסס בעיקרו על מערכי תרגול קודמים כשהקורס נקרא "אלגברה מופשטת 2".
- נשתדל לכתוב בגופן הזה כשהגדרות ומושגים חשובים מופיעים בפעם הראשונה. נוסיף בצד גם את השם באנגלית, שעשוי לעזור כשמחפשים חומר נוסף שאינו בעברית.
- נשמח לכל הערה על מסמך זה.

מחבר בשנת הלימודים תשע"ז: תומר באואר

1 תרגול ראשון

1.1 הגדרות בסיסיות

הגדרה 1.1. חוג בלי יחידה $(R, +, \cdot, 0)$ הוא מבנה אלגברי המקיים:

1. $(R, +, 0)$ הוא חבורה אבלית. נקראת החבורה החיבורית של החוג.

2. (R, \cdot) הוא חבורה למחצה.

3. מתקיים חוג הפילוג (משמאל ומימין). כלומר לכל $a, b, c \in R$ מתקיים

$$(a + b)c = ac + bc, \quad a(b + c) = ab + ac$$

כאשר ההקשר ברור, נכתוב רק R במקום $(R, +, \cdot, 0)$.

הגדרה 1.2. יהי R חוג בלי יחידה. לכמה סוגים מיוחדים של חוגים יש שם משלהם:

Commutative

1. R הוא חילופי אם (R, \cdot) היא חבורה למחצה חילופית.

Ring

2. R הוא חוג (או חוג עם יחידה כשהבדל חשוב), אם (R, \cdot) מונואיד. איבר היחידה של המונואיד נקרא גם היחידה של החוג.

Unital ring

Division ring

3. R הוא חוג חילוק אם $(R \setminus \{0\}, \cdot)$ חבורה.

Field

4. R הוא שדה אם $(R \setminus \{0\}, \cdot)$ הוא חבורה אבלית.

דוגמה 1.3. הרבה מבנים אלגבריים שפגשתם הם חוגים. למשל

1. $(\mathbb{Z}, +, \cdot)$ הוא חוג חילופי עם יחידה. למה הוא לא שדה?

2. $(2\mathbb{Z}, +, \cdot)$ הוא חוג חילופי בלי יחידה.

3. $(\mathbb{Z}_n, +, \cdot)$ הוא חוג חילופי עם יחידה. עבור n ראשוני, אפילו מדובר בשדה.

4. \mathbb{Q} ו- \mathbb{R} הם שדות עם הפעולות הרגילות של חיבור וכפל.

5. הקוטרניונים הרציונליים והקוטרניונים הממשיים הם חוגי חילוק לא חילופיים.

עוד בדוגמה 1.12

6. תהי X קבוצה. אז $(P(X), \Delta, \cap)$ הוא חוג חילופי עם יחידה, כאשר $P(X)$ זו קבוצת החזקה של X , Δ זו פעולת ההפרש הסימטרי, הקבוצה הריקה היא איבר האפס ו- X הוא איבר היחידה. האם זה שדה?

Left invertible

הגדרה 1.4. יהי R חוג. איבר $a \in R$ נקרא הפיך משמאל (מימין) אם קיים $b \in R$ כך ש- $ba = 1$ ($ab = 1$).

Unit

כמו בקורס מבוא לתורת החבורות, איבר הוא הפיך אם הוא הפיך משמאל ומימין, ובמקרה כזה ההופכי הוא יחיד. את אוסף האיברים ההפיכים נסמן R^\times (זה לא חוג! רק תת-חבורה כפלית).

דוגמה 1.5. נסמן $\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$. לגבי הפעולות הרגילות של חיבור וכפל זה שדה. בהמשך נוכל להבין את הסימון בתור פולינומים ב- $\sqrt{2}$ עם מקדמים רציונליים. קל לראות שכל הדרישות של שדה מתקיימות, ואנחנו נראה רק סגירות להופכי.

יהי $a + b\sqrt{2} \neq 0$ אז

$$\frac{1}{a + b\sqrt{2}} = \frac{1}{a + b\sqrt{2}} \cdot \frac{a - b\sqrt{2}}{a - b\sqrt{2}} = \frac{a - b\sqrt{2}}{a^2 - 2b^2} = \frac{a}{a^2 - 2b^2} - \frac{b}{a^2 - 2b^2}\sqrt{2} \in \mathbb{Q}[\sqrt{2}]$$

תרגיל 1.6. הראו כי החוג $\mathbb{Z}[\sqrt{2}]$ אינו שדה, אבל שעדין יש בו אינסוף איברים הפיכים.

Left zero divisor

הגדרה 1.7. יהי R חוג. איבר $a \in R$, $a \neq 0$ נקרא מחלק אפס שמאלי (ימני) אם קיים $b \neq 0$ כך ש- $ab = 0$ ($ba = 0$).

Domain

הגדרה 1.8. חוג ללא מחלקי אפס נקרא תחום. תחום חילופי נקרא תחום שלמות.

Integral domain

דוגמה 1.9. מצאו חוגים שאינם תחומים, תחומים שאינם תחומי שלמות ותחומי שלמות.

1. \mathbb{Z} הוא תחום שלמות.

2. \mathbb{Z}_6 אינו תחום כי $2 \cdot 3 \equiv 0 \pmod{6}$.

3. לכל חוג חילופי R ו- $n > 1$, החוג $M_n(R)$ אינו תחום.

4. חוג עם חילוק הוא תחום.

1.2 תת-חוגים

Subring

הגדרה 1.10. יהי R חוג. תת-קבוצה $S \subseteq R$ נקראת תת-חוג אם היא חוג לגבי הפעולות המושרות מ- R וכוללת את איבר היחידה של R .

Subrng

אם R חוג בלי יחידה, אז תת-קבוצה $S \subseteq R$ נקראת תת-חוג בלי יחידה של R אם היא חוג בלי יחידה לגבי הפעולות המושרות מ- R . שימו לב שאין מניעה כי S היא בעצמה חוג עם יחידה (אבל לאו דווקא היחידה של R).

1.11. טענה $S \subseteq R$ תת-קבוצה $\emptyset \neq S \subseteq R$ היא תת-חוג בלי יחידה של R אם ורק אם לכל $a, b \in S$ מתקיים $ab, a - b \in S$.

דוגמה 1.12. הקוטרניונים הממשיים הם דוגמה לחוג חילוק לא חילופי, שאפשר לחשוב עליהם כתת-חוג

$$\mathbb{H} = \left\{ \begin{pmatrix} a & b \\ -\bar{b} & \bar{a} \end{pmatrix} \mid a, b \in \mathbb{C} \right\} \subseteq M_2(\mathbb{C})$$

נסו לבנות אותם גם כתת-חוג של $M_4(\mathbb{R})$. אם נסמן

$$1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad i = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \quad j = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad k = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$$

אז $\mathbb{H} = \text{Span}_{\mathbb{R}} \{1, i, j, k\}$ ומתקיים $Z(\mathbb{H}) = \text{Span}_{\mathbb{R}} \{1\} \cong \mathbb{R}$.

2 תרגול שני

הגדרה 2.1. יהיו R, S חוגים. נאמר כי $\varphi : R \rightarrow S$ הוא הומומורפיזם של חוגים אם:

$$1. \text{ לכל } x, y \in R \text{ מתקיים } \varphi(xy) = \varphi(x)\varphi(y)$$

$$2. \text{ לכל } x, y \in R \text{ מתקיים } \varphi(x + y) = \varphi(x) + \varphi(y)$$

3. $\varphi(1_R) = 1_S$. אם מוותרים על הדרישה הזו נאמר כי φ הוא הומומורפיזם של חוגים בלי יחידה.

דוגמה 2.2. הומומורפיזם האפס $\varphi(r) = 0_S$ לכל $r \in R$ הוא הומומורפיזם של חוגים בלי יחידה.

דוגמה 2.3. הומומורפיזם על נקרא אפימורפיזם או הטלה. למשל $\varphi : \mathbb{Z} \rightarrow \mathbb{Z}_n$ המוגדר לפי $\varphi(x) = x \pmod{n}$ הוא אפימורפיזם של חוגים.

2.4. יהיו R, S חוגים עם יחידה, והי $\varphi : R \rightarrow S$ אפימורפיזם של חוגים בלי יחידה. הוכיחו כי φ אפימורפיזם של חוגים.

הוכחה. מפני ש- φ על, אז קיים $a \in R$ כך ש- $\varphi(a) = 1_S$. לכן

$$\varphi(1_R) = 1_S \cdot \varphi(1_R) = \varphi(a)\varphi(1_R) = \varphi(a \cdot 1_R) = \varphi(a) = 1_S$$

ולכן $\varphi(1_R) = 1_S$. כלומר זה אפימורפיזם של חוגים.
מה היה קורה אילו רק דרשנו ש- S הוא חוג בלי יחידה? הוכיחו שאז S הוא עדין חוג עם יחידה. \square

דוגמה 2.5. הומומורפיזם חח"ע נקרא מונומורפיזם או שיכון. למשל $\varphi : \mathbb{Z} \rightarrow \mathbb{Q}$ המוגדר לפי $\varphi(x) = x$ הוא מונומורפיזם של חוגים. מה לגבי $\phi : 2\mathbb{Z} \rightarrow \mathbb{Q}$ המוגדר לפי $\phi(x) = x$? זה מונומורפיזם של חוגים בלי יחידה.

הגדרה 2.6. הומומורפיזם חח"ע ועל נקרא איזומורפיזם. נאמר שחוגים R, S שיש ביניהם איזומורפיזם $\varphi : R \rightarrow S$ הם איזומורפיים ונסמן $R \cong S$.

דוגמה 2.7. העתקת הזהות היא תמיד איזומורפיזם. אבל יש עוד, למשל $\varphi : \mathbb{C} \rightarrow \mathbb{C}$ המוגדרת לפי $\varphi(z) = \bar{z}$ היא איזומורפיזם של חוגים.

הגדרה 2.8. יהי $\varphi : R \rightarrow S$ הומומורפיזם של חוגים. כמו בקורסים אלגברה לינארית ותורת החבורות אי אפשר להתחמק מההגדרות הבאות:

1. התמונה של φ היא $\text{Im } \varphi = \{\varphi(x) \mid x \in R\}$, והיא תת-חוג של S .

2. הגרעין של φ הוא $\text{Ker } \varphi = \{x \in R \mid \varphi(x) = 0\}$, והוא תת-חוג בלי יחידה של R . שימו לב שאם $\varphi \neq 0$, אז $1_R \notin \text{Ker } \varphi$.

Endomorphism Automorphism 3. אם $R = S$, נקרא ל- φ אנדומורפיזם. אם בנוסף φ הוא איזומורפיזם, אז הוא נקרא אוטומורפיזם.

הגדרה 2.9. יהי R חוג, $I \subseteq R$ תת-חבורה חיבורית.

Left ideal 1. נאמר כי I הוא אידיאל שמאלי של R אם I לכל $r \in R$ ו- $i \in I$ מתקיים $r \cdot i \in I$. נסמן זאת $I \leq_l R$ ולפעמים $I \leq R$.

Right ideal 2. נאמר כי I הוא אידיאל ימני של R אם I לכל $r \in R$ ו- $i \in I$ מתקיים $i \cdot r \in I$. נסמן זאת $I \leq_r R$.

(Two-sided) Ideal 3. נאמר כי I הוא אידיאל (זו-צדדי) של R אם I לכל $r \in R$ ו- $i \in I$ מתקיים $r \cdot i, i \cdot r \in I$. נסמן זאת $I \triangleleft R$.

דוגמה 2.10. בחוג חילופי ההגדרות השונות של אידיאל מתלכדות.

Proper ideal **דוגמה 2.11.** הקבוצה $\{0\}$ היא אידיאל של R הנקרא האידיאל הטריוויאלי. לפי הגדרה גם R הוא אידיאל, אבל בדרך כלל דורשים הכלה ממש $I \subset R$, ואז קוראים ל- I אידיאל נאות (או אמיתי). ברוב הקורס נתייחס רק לאידיאלים נאותים.

2.12. טענה יהי $\varphi : R \rightarrow S$ הומומורפיזם. אז $\text{Ker } \varphi \triangleleft R$. למעשה גם כל אידיאל הוא גרעין של הומומורפיזם כלשהו.

דוגמה 2.13. האידיאלים היחידים של \mathbb{Z} הם $n\mathbb{Z}$.

תרגיל 2.14. יהי R חוג חילופי, ויהי $A \subset M_n(R)$ חוג המטריצות המשולשיות העליונות. הוכיחו כי אוסף המטריצות המשולשיות העליונות עם אפסים באלכסון הוא אידיאל של A .

תרגיל 2.15. יהי R חוג, ויהי $I \triangleleft R$ אידיאל. הוכיחו שאם $1 \in I$, אז $I = R$.

פתרון. לפי הגדרה, לכל $r \in R$, $i \in I$ מתקיים $r \cdot i \in I$. בפרט $r \cdot 1 = r \in I$. לכן $I = R$.

מסקנה 2.16. אידיאל נאות אף פעם לא מכיל את איבר היחידה של החוג. אף יותר, אידיאל נאות לא מכיל איברים הפיכים כלל.

מסקנה 2.17. בחוג חילוק כל האידיאלים הם טריוויאליים.

תרגיל 2.18. יהיו $a, b \in \mathbb{N}$. הוכיחו כי $b|a$ אם ורק אם $a\mathbb{Z} \subseteq b\mathbb{Z}$.

תרגיל 2.19. הוכיחו שחיתוך אידיאלים הוא אידיאל.

הגדרה 2.20. יהי R חוג, ויהי $x \in R$ איבר. האידיאל שנוצר על ידי x הוא

Ideal generated by x

$$\langle x \rangle = \left\{ \sum_{i=1}^n \alpha_i x \beta_i \mid \alpha_i, \beta_i \in R, n \in \mathbb{N} \right\}$$

סימון מקובל אחר הוא RxR . באופן דומה לאיברים $x_1, \dots, x_k \in R$ מגדירים

$$\langle x_1, \dots, x_k \rangle = \langle x_1 \rangle + \dots + \langle x_k \rangle$$

דוגמה 2.21. בחוג $\mathbb{Z}[x]$ מתקיים

$$\langle 2, x \rangle = \{2f(x) + xg(x) \mid f(x), g(x) \in \mathbb{Z}[x]\} \subsetneq \mathbb{Z}[x]$$

תרגיל 2.22. מצאו חוג R ואיבר $x \in R$ כך ש- $Rx \neq \langle x \rangle$.

Product of ideals

הגדרה 2.23. יהיו I, J אידאלים. נגדיר את מכפלת האידאלים האלו לפי

$$IJ = \left\{ \sum_{k=1}^n i_k j_k \mid i_k \in I, j_k \in J, k \in \mathbb{N} \right\}$$

כאשר הסכומים בקבוצה הם סופיים, אבל n לא מוגבל. ודאו שאתם יודעים להוכיח שזהו אידאל. כתבו את ההגדרה למכפלת אידאלים סופית.

הערה 2.24. לכל זוג אידאלים I, J מתקיים $IJ \subseteq I \cap J$.

Comaximal
ideals

הגדרה 2.25. יהי R חוג, ויהיו $I, J \triangleleft R$. נאמר כי I, J הם קו־מקסימליים אם $I + J = R$.

תרגיל 2.26. הוכיחו כי האידאלים $\langle x-1 \rangle, \langle 2x-1 \rangle$ הם קו־מקסימליים בחוג $\mathbb{Z}[x]$.

3 תרגול שלישי

Principal ideal

הגדרה 3.1. אידאל מהצורה $\langle x \rangle$ נקרא אידאל ראשי. חוג שבו כל אידאל הוא ראשי נקרא חוג ראשי, אבל לא נשתמש בהם יותר מדי. תחום שלמות ראשי נקרא בקיצור תחום ראשי, ובהם נתמקד.

Principal ideal
domain (PID)

תרגיל 3.2. הוכיחו כי $\mathbb{Z}[x]$ אינו ראשי.

טענה 3.3. מנה של חוג ראשי היא ראשית (למה?). הסיקו כי החוג $\mathbb{Z}/n\mathbb{Z}$ הוא ראשי. ודאו שאתם יודעים מתי $\mathbb{Z}/n\mathbb{Z}$ הוא תחום ראשי.

Simple

דוגמה 3.4. חוג R יקרא פשוט אם אין לו אידאלים פרט ל- $\{0\}$.

דוגמה 3.5. חוג חילוק הוא פשוט. האם ההפך נכון?

תרגיל 3.6. הוכיחו שאם R חוג פשוט, אז $Z(R)$ שדה.

הערה 3.7. אם D הוא חוג חילוק, אז $M_n(D)$ הוא חוג פשוט כי ל- D אין אידאלים לא טריוויאלים. לכן $Z(M_n(D))$ הוא שדה, והוא איזומורפי ל- $Z(D)$. הראו כי $Z(M_n(D)) = \{d \cdot I_n \mid d \in D\}$.

תרגיל 3.8. יהי D חוג חילוק שאינו שדה. נסמן $F = Z(D)$. הוכיחו שלכל $d \in D \setminus F$ מתקיים $\langle x-d \rangle = D[x]$.

תרגיל 3.9. תנו דוגמה לחוגים R, S , הומומורפיזם $\varphi : R \rightarrow S$ ואידאל $I \triangleleft R$ כך ש- $\varphi(I)$ אינו אידאל של S .

פתרון. הזכרו שאם φ על, אז $\varphi(I)$ אידאל. אז ניקח $R = \mathbb{Z}$ ואת $S = \mathbb{Q}$ עם השיכון הטבעי $\varphi = \text{id}$. התמונה של \mathbb{Z} תחת φ היא \mathbb{Z} , וזה לא אידאל של \mathbb{Q} , כי האידאלים היחידים שלו הם טריוויאלים.

Quotient ring

הגדרה 3.10. יהי R חוג, ויהי $I \triangleleft R$ אידאל. חוג המנה הוא הקבוצה

$$R/I = \{a + I \mid a \in R\}$$

עם פעולות החיבור $(a + I) + (b + I) = (a + b) + I$ והכפל $(a + I)(b + I) = ab + I$. איבר האפס הוא I ואיבר היחידה הוא $1_R + I$.

הערה 3.11. המחלקות $a + I$ ו- $-a + I$ הן אותו איבר בחוג המנה R/I .

דוגמה 3.12. יהי p ראשוני, אז

$$\mathbb{Z}/p\mathbb{Z} = \{p\mathbb{Z}, 1 + p\mathbb{Z}, \dots, (p-1) + p\mathbb{Z}\} \cong \mathbb{F}_p$$

Nilpotent

הגדרה 3.13. איבר $x \in R$ הוא נילפוטנטי אם קיים $n \in \mathbb{N}$ כך ש- $x^n = 0$.

תרגיל 3.14. יהי R חוג חילופי ויהי N אוסף האיברים הנילפוטנטיים ב- R .

1. הוכיחו כי $N \triangleleft R$.

2. הוכיחו כי ב- R/N אין איברים נילפוטנטיים לא טריוויאליים (כלומר שונים מ-0).

3. תנו דוגמה לחוג לא חילופי שבו N אינו אידאל.

First isomorphism theorem

משפט 3.15 (משפט האיזומורפיזם הראשון). יהי $f : R \rightarrow S$ הומומורפיזם, אז

$$R/\text{Ker } f \cong \text{Im } f$$

בפרט אם $\varphi : R \rightarrow S$ אפימורפיזם, אז $R/\text{Ker } \varphi \cong S$.

דוגמה 3.16. יהי $f : \mathbb{Z} \rightarrow \mathbb{Z}_n$ הומומורפיזם המוגדר לפי $f(a) = a \pmod{n}$. אז $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n$.

מעתה נשתמש בסימון $\mathbb{Z}/n\mathbb{Z}$ (או $\mathbb{Z}/n\mathbb{Z}$) ונפסיק להשתמש בסימון \mathbb{Z}_n עבור החוג הזה, כדי לא להתבלבל עם הסימון לחוג המספרים ה- p -אדיים שנפגוש בעתיד.

Subring generated by X

הגדרה 3.17. יהי R חוג, $R_0 \subseteq R$ תת-חוג ו- $X \subseteq R$ תת-קבוצה. תת-החוג הנוצר (מעל R_0) על ידי X הוא חיתוך כל תת-החוגים $S \subseteq R$ המכילים את R_0 ואת X . נסמן תת-חוג זה בסימון $R_0[X]$. אם $R_0[X] = R$, אז נאמר כי R נוצר על ידי X .

אם $X = \{a_1, \dots, a_n\}$ סופית, אז נסמן $R_0[X] = R_0[a_1, \dots, a_n]$. אם קיימת קבוצה סופית X כך ש- $R_0[X] = R$, נאמר כי R נוצר סופית מעל R_0 .

Finitely generated

הערה 3.18. אם $a \in Z(R)$, אז $R_0[a]$ הוא אוסף הפולינומים ב- a עם מקדמים מ- R_0 .

תרגיל 3.19. כל חוג חילופי שנוצר סופית מעל R_0 הוא מנה (ליתר דיוק, איזומורפי למנה, אבל אנחנו לא נדקדק) של חוג הפולינומים $R_0[x_1, \dots, x_n]$ עבור n כלשהו.

נביא כמה דוגמאות לשימושים במשפט האיזומורפיזם הראשון להבנת חוגי פולינומים. יהי R חוג חילופי.

דוגמה 3.20. יהי $a \in R$ (התוצאה תהיה נכונה כאשר R לא חילופי, אם $a \in Z(R)$), ונביט בהעתקת ההצבה $\varphi_a : R[x] \rightarrow R$ המוגדרת לפי $\varphi_a(f(x)) = f(a)$. הוכיחו שמדובר באפימורפיזם.

Evaluation map

הגרעין של φ_a הוא כל הפולינומים ש- a הוא שורש שלהם. בפרט, עבור $a = 0$ נקבל $\text{Ker } \varphi_0 = \langle x \rangle$, שכן מדובר בכל הפולינומים שהמקדם החופשי שלהם הוא 0. לכן $R[x]/\langle x \rangle \cong R$. הראו שבאופן דומה גם $R[x, y]/\langle y \rangle \cong R[x]$.

תרגיל 3.21. הראו כי $\text{Ker } \varphi_a = \langle x - a \rangle$.

4 תרגול רביעי

Second isomorphism theorem

משפט 4.1 (משפט האיזומורפיזם השני). יהי $I \triangleleft R$ אידיאל, ויהי $S \subseteq R$ תת-חוג. אז

$$S/S \cap I \cong S+I/I$$

תרגיל 4.2. יהיו $I \subseteq J$ אידיאלים של R . הוכיחו שקיים אפימורפיזם $R/I \rightarrow R/J$.

פתרון. מה כבר אפשר לעשות אחרי שיודעים איך נראים האיברים בחוגי המנה? נגדיר $\varphi : R/I \rightarrow R/J$ לפי $\varphi(r+I) = r+J$. נבדוק שההעתקה הזו מוגדרת היטב. נניח $r+I = s+I$. אז $r-s \in I$, ולכן גם $r-s \in J$. לכן $r+J = s+J$. נבדוק שההעתקה הזו מכבדת את החיבור:

$$\varphi((r+I)+(s+I)) = \varphi((r+s)+I) = (r+s)+J = (r+J)+(s+J) = \varphi(r+I)+\varphi(s+I)$$

את הכפל הוכיחו בבית, ונשאר להוכיח שההעתקה על. לכל $r+J$ יש מקור, למשל $r+I$. לכן φ אפימורפיזם.

Third isomorphism theorem

משפט 4.3 (משפט האיזומורפיזם השלישי). יהיו $I \subseteq J$ אידיאלים של חוג R . אז

$$R/I/J/I \cong R/J$$

Maximal ideal

הגדרה 4.4. אידיאל נאות $I \triangleleft R$ נקרא אידיאל מקסימלי אם לא קיים אידיאל נאות שמכיל אותו ממש.

דוגמה 4.5. בחוג \mathbb{Z}_{45} יש רק שני אידיאלים מקסימליים והם $3\mathbb{Z}_{45}$ ו- $5\mathbb{Z}_{45}$. בחוג \mathbb{Z}_{32} יש רק אידיאל מקסימלי אחד והוא $2\mathbb{Z}_{32}$.

דוגמה 4.6. בחוג חילוק אין אידאלים לא טריוויאליים, ולכן אידאל האפס הוא אידאל מקסימלי.

דוגמה 4.7. לכל מספר ראשוני p , האידאל $p\mathbb{Z} \triangleleft \mathbb{Z}$ הוא מקסימלי. האם יש עוד?

דוגמה 4.8. עבור חוג חילופי R , האידאל $\langle x \rangle \triangleleft R[x, y]$ אינו מקסימלי. למשל כי האידאל הנאות $J = \{f(x, y) \mid f(0, 0) = 0\}$ מכיל אותו ממש.

תרגיל 4.9. יהי $f : R \rightarrow S$ אפימורפיזם, ויהי $I \triangleleft R$ אידאל נאות המכיל את $\text{Ker } f$. הוכיחו שגם $f(I) \triangleleft S$ אידאל נאות.

משפט 4.10. יהי R חוג. אידאל נאות $I \triangleleft R$ הוא מקסימלי אם ורק אם R/I הוא פשוט. אם בנוסף R חילופי, אז I מקסימלי אם ורק אם R/I שדה.

דוגמה 4.11. האידאל $\langle x, p \rangle \triangleleft \mathbb{Z}[x]$ הוא מקסימלי לכל מספר ראשוני p מפני שחוג המנה $\mathbb{Z}[x]/\langle x, p \rangle \cong \mathbb{F}_p$ הוא שדה. אבל $\langle x \rangle$ לא מקסימלי, כי $\mathbb{Z}[x]/\langle x \rangle \cong \mathbb{Z}$ אינו שדה (או כי $\langle x \rangle$ מוכל ממש ב- $\langle x, p \rangle$).

Correspondence
theorem

משפט 4.12 (משפט ההתאמה). יהי $I \triangleleft R$ אידאל. אז ההתאמה $A \mapsto A/I$ היא איזומורפיזם של סריגים בין האידאלים של R המכילים את I לבין האידאלים של R/I . ההתאמה שומרת הכלה, חיבור, כפל, חיתוך ופנות.

4.1 אידאלים ראשוניים

Prime

הגדרה 4.13. אידאל נאות $I \triangleleft R$ יקרא ראשוני אם לכל $A, B \triangleleft R$ המקיימים $AB \subseteq I$, אז $A \subseteq I$ או $B \subseteq I$.

הערה 4.14. עבור חוגים חילופיים ההגדרה לראשוניות גוררת את התנאי היותר חזק שלכל $a, b \in R$, המקיימים $ab \in I$, אז $a \in I$ או $b \in I$. בחוגים לא חילופיים, זה תנאי שעשוי להיות יותר חזק ממש. למשל, יהי חוג חילוק D ונתבונן בחוג הפשוט $M_2(D)$. אידאל האפס $\{0\} \triangleleft M_2(D)$ הוא ראשוני, אבל מתקיים

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

מבלי שאף אחד מן האיברים באגף שמאל שייך לאידאל האפס.

דוגמה 4.15. בחוג פשוט אידאל האפס הוא תמיד ראשוני.

תרגיל 4.16. יהי $C(\mathbb{R})$ חוג הפונקציות הממשיות הרציפות (עם חיבור וכפל נקודתיים). הוכיחו כי

$$I = \{f \in C(\mathbb{R}) \mid f(0) = 0\}$$

הוא אידאל ראשוני.

פתרון. אנחנו כבר יודעים מתרגיל הבית ש- $I \triangleleft C(\mathbb{R})$. נניח $f(x)g(x) \in I$, אז $f(0)g(0) = 0$. אך מפני ש- \mathbb{R} הוא תחום שלמות, אז $f(0) = 0$ או $g(0) = 0$. כלומר $f(x) \in I$ או $g(x) \in I$.

משפט 4.17. יהי R חוג חילופי. אז R הוא תחום שלמות אם ורק אם $\{0\}$ הוא אידיאל ראשוני.

מסקנה 4.18. יהי R חוג. אז $I \triangleleft R$ ראשוני אם ורק אם $\{0\}$ הוא ראשוני בחוג המנה R/I .

מסקנה 4.19. יהי R חוג חילופי. אז אידיאל נאות $I \triangleleft R$ הוא ראשוני אם ורק אם R/I תחום שלמות.

דוגמה 4.20. האידיאל $\langle x \rangle \triangleleft \mathbb{Z}[x]$ הוא ראשוני כי חוג המנה $\mathbb{Z}[x]/\langle x \rangle \cong \mathbb{Z}$ הוא תחום שלמות.

תרגיל 4.21. יהי R חוג שבו כל האידיאלים הם ראשוניים. הוכיחו כי R שדה.

פתרון. מן הנתון נקבל בפרט ש- $\{0\}$ אידיאל ראשוני, ולכן R תחום שלמות. יהי $0 \neq x \in R$ ונראה שהוא הפיך. נתבונן באידיאל $\langle x^2 \rangle$, שהוא ראשוני מהנתון, ולכן $x \in \langle x^2 \rangle$. כלומר קיים $a \in R$ כך ש- $x = ax^2$, ונקבל $x(ax - 1) = 0$. מפני ש- R תחום שלמות וגם $x \neq 0$, אז $ax = 1$. כלומר x הפיך, כדרוש.

הערה 4.22. אם $I, J \triangleleft R$ ראשוניים, אז $I \cap J$ לא בהכרח ראשוני. למשל בחוג \mathbb{Z} האידיאלים $2\mathbb{Z}, 3\mathbb{Z}$ הם ראשוניים, אבל חיתוכם $6\mathbb{Z} = 2\mathbb{Z} \cap 3\mathbb{Z}$ אינו ראשוני.

סענה 4.23. יהי R חוג חילופי. כל אידיאל מקסימלי של R הוא ראשוני.

הוכחה. יהי $I \triangleleft R$ מקסימלי. אז R/I הוא שדה כי R חילופי. בפרט, R/I הוא תחום שלמות, ולכן I ראשוני. \square

סענה 4.24. (לדלג). יהי R חוג. כל אידיאל מקסימלי של R הוא ראשוני.

הוכחה. נניח בשלילה כי $I \triangleleft R$ מקסימלי ואינו ראשוני. כלומר קיימים $A, B \triangleleft R$ כך ש- $AB \subseteq I$, אבל $A, B \not\subseteq I$. קל לראות כי

$$(A + I)(B + I) = AB + AI + IB + I^2 \subseteq I$$

מפני ש- I מקסימלי, נקבל $A + I = B + I = R$, ולכן $RR \subseteq I$. כלומר $I = R$, וזה \square בסתירה למקסימליות.

מסקנה 4.25. בחוג בלי יחידה, אידיאל מקסימלי $M \triangleleft R$ הוא לא ראשוני אם ורק אם $R^2 \subseteq M$.

דוגמה 4.26. בחוג בלי יחידה $R = 2\mathbb{Z}$ האידיאל $I = 4\mathbb{Z}$ הוא מקסימלי, אבל הוא לא ראשוני, כי $R^2 \subseteq I$.

תרגיל 4.27. יהי R חוג חילופי. הוכיחו שאם לכל $x \in R$ קיים $n > 1$ כך ש- $x^n = x$, אז כל אידאל ראשוני הוא מקסימלי.

פתרון. יהי $P \triangleleft R$ אידאל ראשוני, ויהי $M \triangleleft R$ אידאל מקסימלי המכיל את P (למה בהכרח קיים כזה?). נניח בשלילה שקיים $x \in M \setminus P$. מתקיים $x^n = x$ עבור $n > 1$. לכן

$$x(x^{n-1} - 1) = x^n - x = 0 \in P$$

לכן בהכרח $x^{n-1} - 1 \in P$. אבל אז גם $x^{n-1}, x^{n-1} - 1 \in M$, ולכן $1 \in M$, שזו סתירה למקסימליות של M . לכן $P = M$.

4.2 חוגים ראשוניים

Prime ring

4.28 הגדרה. חוג R נקרא ראשוני אם לכל שני אידאלים $A, B \triangleleft R$ המקיימים $AB = 0$, אז $A = 0$ או $B = 0$. באופן שקול, חוג הוא ראשוני אם המכפלה של כל שני אידאלים השונים מאפס, שונה מאפס.

4.29 משפט. R ראשוני אם ורק אם לכל $a, b \in R$ קיים $0 \neq x \in R$ כך ש- $axb \neq 0$.

4.30 משפט. כל תחום הוא ראשוני.

4.31 משפט. חוג חילופי הוא ראשוני אם ורק אם הוא תחום שלמות.

4.32 תרגיל. יהי R חוג ראשוני. הראו שהמרכז $Z(R)$ הוא תחום שלמות.

פתרון. נעזר במשפט 4.31 מפני ש- $Z(R)$ חילופי. יהיו $A, B \triangleleft Z(R)$ כך ש- $AB = 0$. לכן $AR, BR \triangleleft R$ ומתקיים $ARBR = ABR = 0$. מהראשונות של R נקבל $AR = 0$ או $BR = 0$, ומכאן מסיקים כי $A = 0$ או $B = 0$. כלומר $Z(R)$ ראשוני, ולכן הוא גם תחום שלמות.

4.33 תרגיל. ראינו כבר שתת-חוג של שדה הוא תחום שלמות. הפריכו את המקרה הלא חילופי: מצאו תת-חוג של חוג פשוט שאינו ראשוני.

פתרון. יהי F שדה. אז $R = M_2(F)$ הוא חוג פשוט, ונסמן ב- T את תת-החוג של מטריצות משולשיות עליונות ב- R . אז T הוא לא ראשוני כי מכפלת האידאלים

$$I = \begin{pmatrix} 0 & 0 \\ 0 & * \end{pmatrix}, \quad J = \begin{pmatrix} 0 & * \\ 0 & 0 \end{pmatrix}$$

היא אפס, אך הם כמובן שונים מאפס.

Semiprime

4.34 תרגיל. (ממבחן). חוג R נקרא ראשוני למחצה אם לא קיים אידאל $I \triangleleft R$ כך ש- $I^2 = 0$. אידאל P בחוג כלשהו R נקרא ראשוני למחצה אם R/P הוא חוג ראשוני למחצה.

1. הוכח כי כל אידאל ראשוני הוא אידאל ראשוני למחצה.

2. הוכח כי P ראשוני למחצה אם ורק אם לכל אידאל $I \triangleleft R$, אם $I^2 \subseteq P$, אז $I \subseteq P$.

פתרון. קל לראות שהסעיף השני גורר את הראשון. לכן נוכיח רק את הסעיף השני. תהי $\varphi : R \rightarrow R/P$ ההטלה הטבעית. נניח כי P ראשוני למחצה, ולכן R/P ראשוני למחצה. יהי אידאל $I \triangleleft R$ המקיים $I^2 \subseteq P$. נפעיל את φ , שהיא אפימורפיזם, ולכן $\varphi(I) \triangleleft R/P$ ובנוסף $(\varphi(I))^2 = 0$. מהראשוניות למחצה של R/P , נסיק כי $\varphi(I) = 0$ ולכן $I \subseteq P$.

בכיוון ההפוך, נניח כי P לא ראשוני למחצה, ולכן R/P לא ראשוני למחצה. לכן קיים אידאל $I \triangleleft R/P$ כך ש- $I \neq 0$ ו- $I^2 = 0$. האידאל $\varphi^{-1}(I) \triangleleft R$ מקיים $(\varphi^{-1}(I))^2 \subseteq P$, אבל $\varphi^{-1}(I) \not\subseteq P$, וזו סתירה.