# מבוא לחוגים ומודולים
# מערכי תרגול קורס 88-212

מהדורת קריאה מוקדמת

מרץ 2017, גרסה 0.4

אוניברסיטת בר־אילן סמסטר ב׳ תשע״ז

# תוכן העניינים

# 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.

This font

- 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: Rng, or non-unital ring

1. $(R,+,0)$ הוא חבורה אבלית. נקראת החבורה החיבורית של החוג. Additive group
2. $(R,\cdot)$ הוא חבורה למחצה.
3. מתקיים חוג הפילוג (משמאל ומימין). כלומר לכל $a,b,c\in R$ מתקיים

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

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:

1. $R$ הוא חילופי אם $(R,\cdot)$ היא חבורה למחצה חילופית. Commutative
2. $R$ הוא חוג (או חוג עם יחידה כשהבדל חשוב), אם $(R,\cdot)$ מונואיד. איבר היחידה של המונואיד נקרא גם היחידה של החוג. Ring, Unital ring
3. $R$ הוא חוג חילוק אם $(R\setminus\{0\},\cdot)$ חבורה. Division ring
4. $R$ הוא שדה אם $(R\setminus\{0\},\cdot)$ הוא חבורה אבלית. Field

**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. הקווטרניונים הרציונליים והקווטרניונים הממשיים הם חוגי חילוק לא חילופיים. עוד בדוגמה 1.12.
6. תהי $X$ קבוצה. אז $(P(X),\triangle,\cap)$ הוא חוג חילופי עם יחידה, כאשר $P(X)$ זו קבוצת החזקה של $X$, $\triangle$ זו פעולת ההפרש הסימטרי, הקבוצה הריקה היא איבר האפס ו-$X$ הוא איבר היחידה. האם זה שדה?

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

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). Unit

**דוגמה 1.5.** נסמן $\mathbb{Q}[\sqrt{2}] = \left\{ a + b\sqrt{2} \,\middle|\, a, b \in \mathbb{Q} \right\}$. 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 שעדיין יש בו אינסוף איברים הפיכים.

Left zero divisor

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

Domain

Integral domain

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

**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 $R$).

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

**דוגמה 1.12.** הקווטרניונים הממשיים הם דוגמה לחוג חילוק לא חילופי, שאפשר לחשוב עליהם כתת־החוג

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

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

## 2 תרגול שני

Ring homomorphism

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

1. לכל $x, y \in R$ מתקיים $\varphi(xy) = \varphi(x)\varphi(y)$.
2. לכל $x, y \in R$ מתקיים $\varphi(x+y) = \varphi(x) + \varphi(y)$.
3. $\varphi(1_R) = 1_S$. אם מוותרים על הדרישה הזו נאמר כי $\varphi$ 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.

Epimorphism Projection

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

טענה 2.4. יהיו $R, S$ חוגים עם יחידה, ויהי $\varphi : R \to S$ אפימורפיזם של חוגים בלי יחידה. הוכיחו כי $\varphi$ אפימורפיזם של חוגים.

הוכחה. מפני ש-$\varphi$ 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. $\square$

Monomorphism Embedding

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

Isomorphism Isomorphic

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

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

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

Image

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

Kernel

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

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

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

1. נאמר כי $I$ הוא אידאל שמאלי של $R$ אם $I$ לכל $r\in R$ ו-$i\in I$ מתקיים $r\cdot i\in I$. נסמן זאת $I\le_l R$ ולפעמים $I\le R$. Left ideal
2. נאמר כי $I$ הוא אידאל ימני של $R$ אם $I$ לכל $r\in R$ ו-$i\in I$ מתקיים $i\cdot r\in I$. נסמן זאת $I\le_r R$. Right ideal
3. נאמר כי $I$ הוא אידאל (דו־צדדי) של $R$ אם $I$ לכל $r\in R$ ו-$i\in I$ מתקיים $r\cdot i, i\cdot r\in I$. נסמן זאת $I\lhd R$. (Two-sided) Ideal

**דוגמה 2.10.** בחוג חילופי ההגדרות השונות של אידאל מתלכדות.

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

טענה 2.12. יהי $\varphi:R\to S$ הומומורפיזם. אז $\operatorname{Ker}\varphi\lhd R$. למעשה גם כל אידאל הוא גרעין של הומומורפיזם כלשהו.

**דוגמה 2.13.** האידאלים 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 אידאל של $A$.

**תרגיל 2.15.** יהי $R$ חוג, ויהי $I\lhd R$ אידאל. 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.** אידאל נאות אף פעם לא מכיל את איבר היחידה של החוג. אף יותר, אידאל נאות לא מכיל איברים הפיכים כלל.

**מסקנה 2.17.** בחוג חילוק כל האידאלים 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 אידאלים הוא אידאל.

## 3 תרגול שלישי

Ideal generated by $x$

**הגדרה 3.1.** יהי $R$ חוג, ויהי $x \in R$ איבר. האידאל שנוצר על ידי $x$ הוא

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

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

$$\langle x_1, \ldots, x_k \rangle = \langle x_1 \rangle + \cdots + \langle x_k \rangle$$

**דוגמה 3.2.** 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 3.3.** מצאו חוג $R$ ואיבר $x \in R$ כך ש-$\langle x \rangle \neq Rx$.

Product of ideals

**הגדרה 3.4.** יהיו $I, J$ אידאלים. נגדיר את מכפלת האידאלים האלו לפי

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

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

הערה 3.5. לכל זוג אידאלים $I, J$ מתקיים $IJ \subseteq I \cap J$.

Comaximal ideals

**הגדרה 3.6.** יהי $R$ חוג, ויהיו $I, J \lhd R$. נאמר כי $I, J$ הם קו־מקסימליים אם $I + J = R$.

**תרגיל 3.7.** הוכיחו כי האידאלים $\langle x-1 \rangle$, $\langle 2x-1 \rangle$ הם קו־מקסימליים בחוג $\mathbb{Z}[x]$.

Principal ideal

Principal ideal domain (PID)

**הגדרה 3.8.** 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.

**דוגמה 3.9** $\mathbb{Z}$ הוא תחום ראשי. אידאלים הם תמיד מן הצורה $m\mathbb{Z}$.

**תרגיל 3.10.** הוכיחו כי $\mathbb{Z}[x]$ אינו ראשי.

טענה 3.11. מנה של חוג ראשי היא ראשית (למה?). הסיקו כי החוג $\mathbb{Z}_n$ הוא ראשי. ודאו שאתם יודעים מתי $\mathbb{Z}_n$ הוא תחום ראשי.

Formal Laurent series

Formal power series

**הגדרה 3.12.** יהי $R$ תחום. חוג טורי לורן הפורמליים $R((x))$ כולל את כל הסכומים האינסופיים הפורמליים $\sum_{i=-n}^{\infty} a_i x^i$ עבור $n \in \mathbb{N}$ כלשהו ו-$a_i \in R$. הפעולות הן החיבור והכפל המוכללות מחוג הפולינומים. לחוג זה יש תת־חוג של טורי חזקות פורמליים $R[[x]]$ הכולל סכומים $\sum_{i=0}^{\infty} a_i x^i$.

**דוגמה 3.13.** בחוג $R[[x]]$ האיבר $x-1$ הוא הפיך (השוו למצב ב-$R[x]$), אבל $x$ אינו הפיך. לכן $R[[x]]$ אינו שדה.

Simple

**דוגמה 3.14.** חוג $R$ יקרא פשוט אם אין לו אידאלים פרט ל-$R$ ול-$\{0\}$.

**דוגמה 3.15.** חוג חילוק הוא פשוט. האם ההפך נכון?

**תרגיל 3.16.** הוכיחו שאם חוג (עם יחידה) $R$ הוא חילופי ופשוט, אז הוא שדה.

פתרון. יהי $0 \neq x \in R$. אז $Rx = R$, כי $R$ פשוט. בנוסף $x$ הפיך כי קיים $y \in R$ כך ש-$yx = 1$. עקב החילופיות, גם $xy = 1$. לכן $R$ שדה.

**תרגיל 3.17.** הוכיחו שאם $R$ חוג פשוט, אז $Z(R)$ שדה.

הערה 3.18. 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 3.19.** יהי $D$ חוג חילוק שאינו שדה. נסמן $F = Z(D)$. הוכיחו שלכל $d \in D \backslash F$ מתקיים $\langle x-d \rangle = D[x]$.

# 4 תרגול רביעי

**תרגיל 4.1.** תנו דוגמה לחוגים $R, S$, הומומורפיזם $\varphi : R \to S$ ואידאל $I \lhd R$ כך ש-$\varphi(I)$ אינו אידאל של $S$.

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

Quotient ring

**הגדרה 4.2.** יהי $R$ חוג, ויהי $I \lhd R$ 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 4.3. המחלקות $a+I$ ו-$-a+I$ הן אותו איבר בחוג המנה $^{R}/_{I}$.

**דוגמה 4.4.** יהי $p$ ראשוני, אז

$$^{\mathbb{Z}}/_{p\mathbb{Z}} = \{p\mathbb{Z}, 1+p\mathbb{Z}, \ldots, (p-1)+p\mathbb{Z}\} \cong \mathbb{Z}_p$$

**דוגמה 4.5.** נסמן $R=\mathbb{R}[x]$, $I=\langle x^2+1\rangle=\{f(x)(x^2+1)\mid f(x)\in R\}$. לכל איבר $a\in R$ נסמן $\overline{a}=a+I\in {}^{R}/_{I}$. מתקיים $x^2+I=x^2-(x^2+1)+I=-1+I$. לכן $\overline{x^2}=\overline{-1}$. באופן דומה אפשר להראות כי $\overline{x^3}=\overline{-x}$, $\overline{x^4}=\overline{1}$ וכו'. נקבל כי

$$^{R}/_{I}=\{\alpha+\beta\overline{x}\mid\alpha,\beta\in\mathbb{R}\}$$

כי כל איבר $\overline{x^n}$ הוא $\overline{\pm x}$ או $\overline{\pm 1}$, כשמתקיים $\overline{x}\cdot\overline{x}=\overline{-1}$. לבית: הוכיחו $^{R}/_{I}\cong\mathbb{C}$.

Nilpotent

**הגדרה 4.6.** איבר $x\in R$ הוא נילפוטנטי אם קיים $n\in\mathbb{N}$ כך ש-$x^n=0$.

**תרגיל 4.7.** יהי $R$ חוג חילופי ויהי $N$ אוסף האיברים הנילפוטנטיים ב-$R$.

1. הוכיחו כי $N\lhd R$.
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 4.8** (משפט האיזומורפיזם הראשון)**.** יהי $f:R\to S$ הומומורפיזם, אז

$$^{R}/_{\operatorname{Ker}f}\cong\operatorname{Im}f$$

בפרט אם $\varphi:R\to S$ אפימורפיזם, אז $^{R}/_{\operatorname{Ker}f}\cong S$.

**דוגמה 4.9.** יהי $f:\mathbb{Z}\to\mathbb{Z}_n$ הומומורפיזם המוגדר לפי $f(a)=a\pmod n$. אז $^{\mathbb{Z}}/_{n\mathbb{Z}}\cong\mathbb{Z}_n$.

Subring generated by $X$

**הגדרה 4.10.** 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 $X$.

Finitely generated

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 $R_0$.

הערה 4.11. אם $a\in Z(R)$, אז $R_0[a]$ הוא אוסף הפולינומים ב-$a$ עם מקדמים מ-$R_0$.

**תרגיל 4.12.** 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.

הערה 4.13. הכיוון השני של התרגיל הקודם אינו נכון. למשל נבחר $R=\mathbb{Z}[x]$, $R_0=\mathbb{Z}$ ואת האידאל $2\mathbb{Z}[x]$. המנה לגבי האידאל הזה איזומורפית ל-$\mathbb{Z}_2[x]$ (הוכיחו שקיים אפימורפיזם $\varphi:\mathbb{Z}[x]\to\mathbb{Z}_2[x]$ שהגרעין שלו הוא $2\mathbb{Z}[x]$). אבל $\mathbb{Z}_2[x]$ אינו נוצר סופית מעל $\mathbb{Z}$, כיוון שאינו מכיל תת־חוג האיזומורפי ל-$\mathbb{Z}$, שהרי לכל $a\in\mathbb{Z}_2[x]$ מתקיים $2a=0$.

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

**דוגמה 4.14.** יהי $a \in R$ (התוצאה תהיה נכונה כאשר $R$ לא חילופי, אם $a \in Z(R)$), ונביט בהעתקת ההצבה $\varphi_a : R[x] \to R$ המוגדרת לפי $\varphi_a(f(x)) = f(a)$. הוכיחו שמדובר באפימורפיזם.

Evaluation map

הגרעין של $\varphi_a$ הוא כל הפולינומים ש-$a$ הוא שורש שלהם. בפרט, עבור $a = 0$ נקבל $\operatorname{Ker}\varphi_0 = \langle x \rangle$, 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 4.15.** הראו כי $\operatorname{Ker}\varphi_a = \langle x - a \rangle$.

# 5 תרגול חמישי

**משפט 5.1** (משפט האיזומורפיזם השני)**.** יהי $I \lhd R$ אידאל, ויהי $S \subseteq R$ תת־חוג. אז

Second isomorphism theorem

$$S/_{S\cap I} \cong {}^{S+I}/_{I}$$

**תרגיל 5.2.** יהיו $I \subseteq J$ אידאלים של $R$. הוכיחו שקיים אפימורפיזם $R/I \to R/J$.

פתרון. מה כבר אפשר לעשות אחרי שיודעים איך נראים האיברים בחוגי המנה? נגדיר $\varphi : R/I \to R/J$ 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 $\varphi$ אפימורפיזם.

**משפט 5.3** (משפט האיזומורפיזם השלישי)**.** יהיו $I \subseteq J$ אידאלים של חוג $R$. אז

Third isomorphism theorem

$$^{R/I}/_{J/I} \cong {}^{R}/_{J}$$

**הגדרה 5.4.** אידאל נאות $I \lhd R$ נקרא אידאל מקסימלי אם לא קיים אידאל נאות שמכיל אותו ממש.

Maximal ideal

**דוגמה 5.5.** בחוג $\mathbb{Z}_{45}$ יש רק שני אידאלים מקסימליים והם $3\mathbb{Z}_{45}$ ו-$5\mathbb{Z}_{45}$. בחוג $\mathbb{Z}_{32}$ יש רק אידאל מקסימלי אחד והוא $2\mathbb{Z}_{32}$.

**דוגמה 5.6.** בחוג חילוק אין אידאלים לא טריוויאלים, ולכן אידאל האפס הוא אידאל מקסימלי.

**דוגמה 5.7.** לכל מספר ראשוני $p$, האידאל $p\mathbb{Z} \lhd \mathbb{Z}$ הוא מקסימלי. האם יש עוד?

**דוגמה 5.8.** עבור חוג חילופי $R$, האידאל $\langle x \rangle \lhd R[x,y]$ אינו מקסימלי. למשל כי האידאל הנאות $J = \{f(x,y) \mid f(0,0) = 0\}$ מכיל אותו ממש.

**דוגמה 5.9.** עבור שדה $F$, לחוג $F[[x]]$ יש רק אידאל מקסימלי אחד $\langle x \rangle$ (עדין לא הגדרנו חוג מקומי, אבל עדין אפשר להוכיח כאן שהאידאלים הם מן הצורה $\langle x^i \rangle$).

**תרגיל 5.10.** יהי $f : R \to S$ אפימורפיזם, ויהי $I \lhd R$ אידאל נאות המכיל את $\operatorname{Ker} f$. הוכיחו שגם $f(I) \lhd S$ אידאל נאות.

**משפט 5.11.** יהי $R$ חוג. אידאל נאות $I \lhd R$ הוא מקסימלי אם ורק אם $R/I$ הוא פשוט. אם בנוסף $R$ חילופי, אז $I$ מקסימלי אם ורק אם $R/I$ שדה.

**דוגמה 5.12.** האידאל $\langle x, p \rangle \lhd \mathbb{Z}[x]$ הוא מקסימלי לכל מספר ראשוני $p$ מפני שחוג המנה $\mathbb{Z}[x]/\langle x, p \rangle \cong \mathbb{Z}_p$ 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 5.13** (משפט ההתאמה)**.** יהי $I \lhd R$ 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 ומנות.