מבוא לחוגים ומודולים
מערכי תרגול קורס 88-212

מאי 2017, גרסה 0.7

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

Rng, or non-unital ring

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

Additive group

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

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

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:

Commutative

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

Ring
Unital ring

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

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. הקווטרניונים הרציונליים והקווטרניונים הממשיים הם חוגי חילוק לא חילופיים. עוד בדוגמה 1.21.
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?

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).

תרגיל 1.5. יהי R חוג חילופי. הוכיחו כי $M_n(R)$ הוא חוג לגבי הפעולות של חיבור וכפל מטריצות. הראו כי $A \in M_n(R)$ הפיכה אם ורק אם $\det A \in R$ הפיכה.

פתרון. קל לראות כי $(M_n(R), +)$ זו חבורה אבלית שאיבר היחידה בה הוא מטריצת האפס, ש-$(M_n(R), \cdot)$ הוא מונואיד שאיבר היחידה בו הוא מטריצת היחידה I_n, ושמתקיים חוק הפילוג. לכן $M_n(R)$ חוג עם יחידה.

צריך להראות שהדטרמיננטה היא כפלית גם כאשר עובדים מעל חוגים חילופיים, ולא רק מעל שדות. לא נעשה זאת כאן. נניח שקיימת מטריצה $B \in M_n(R)$ כך ש-$AB = BA = I_n$. אז

$$\det(AB) = \det(A) \cdot \det(B) = \det(I_n) = 1 = \det(B) \cdot \det(A) = \det(BA)$$

כלומר גם $\det(A)$ הפיכה (ההופכי הוא $\det(B)$). לכיוון השני נניח כי $\det(A)$ הפיכה עם הופכי $c \in R$. נעזר בתכונה

$$A \cdot \operatorname{adj}(A) = \operatorname{adj}(A) \cdot A = \det(A) \cdot I_n$$

וכשנכפיל ב-c נקבל $A \cdot (c \cdot \operatorname{adj}(A)) = (c \cdot \operatorname{adj}(A)) \cdot A = I_n$.

דוגמה 1.6. 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 1.7. הראו כי החוג $\mathbb{Z}[\sqrt{2}]$ אינו שדה, אבל שעדיין יש בו אינסוף איברים הפיכים.

פתרון. לאיבר $2 \in \mathbb{Z}[\sqrt{2}]$ אין הפיך כי $\frac{1}{2} \notin \mathbb{Z}[\sqrt{2}]$. לכן זה לא שדה. נשים לב כי

$$\left(3 + 2\sqrt{2}\right)\left(3 - 2\sqrt{2}\right) = 1$$

ולכן $3 + 2\sqrt{2}$, $3 - 2\sqrt{2}$ הם הפיכים בחוג $\mathbb{Z}[\sqrt{2}]$. כיוון ש-$3 + 2\sqrt{2} > 1$, אז קבוצת החזקות הטבעיות שלו היא אינסופית. בנוסף כל חזקה כזו היא הפיכה כי $\left(3+2\sqrt{2}\right)^n \left(3-2\sqrt{2}\right)^n = 1$, ואלו הם אינסוף איברים הפיכים שונים.

דוגמה 1.8. יהי V מרחב וקטורי מעל שדה F. נסמן ב-$\operatorname{End}(V)$ את מרחב ההעתקות הלינאריות $\varphi \colon V \to V$. זהו חוג ביחס לפעולות החיבור וההרכבה, כאשר איבר האפס הוא העתקת האפס, ואיבר היחידה הוא העתקת הזהות id.

אם נבחר $V = F^{\mathbb{N}} = \{(x_1, x_2, \dots) \mid x_i \in F\}$, ונתבונן בשני העתקות

$$\begin{aligned} D\left((x_1, x_2, \dots)\right) &= (x_2, x_3, \dots) \\ U\left((x_1, x_2, \dots)\right) &= (0, x_1, x_2, \dots) \end{aligned}$$

קל לראות כי $D \circ U = \operatorname{id}$, אבל $U \circ D \neq \operatorname{id}$ ולכן D הפיכה מימין, אך לא משמאל.

הגדרה 1.9. יהי R חוג. איבר $0 \neq a \in R$ נקרא מחלק אפס שמאלי (ימני) אם קיים $b \neq 0$ כך ש-$ab = 0$ ($ba = 0$). Left zero divisor

הגדרה 1.10. חוג ללא מחלקי אפס נקרא תחום. תחום חילופי נקרא תחום שלמות. Domain, Integral domain

דוגמה 1.11. 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.

הגדרה 1.12. יהי R חוג חילופי. חוג הפולינומים במשתנה x עם מקדמים ב-R מסומן $R[x]$. זהו גם חוג חילופי (למה?) Polynomial ring

אם R תחום שלמות, אז גם $R[x]$ תחום שלמות. אבל אם R שדה, אז $R[x]$ לא נשאר שדה. הרי $1 - x$ אינו הפיך. אפשר לראות זאת לפי פיתוח לטור טיילור:

$$\frac{1}{1-x} = 1 + x + x^2 + \dots$$

אבל הטור מימין אינו פולינום.

דוגמה 1.13. האיבר $1 + 2x \in \mathbb{Z}_4[x]$ הפיך כי $(1+2x)(1-2x) = 1 - 4x^2 = 1$.

1.2 תת־חוגים

הגדרה 1.14. 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. Subring

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). Subrng

טענה 1.15. 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 1.16.
1. $n\mathbb{Z}$ הוא תת־חוג של $\mathbb{Z}$ לכל $n \in \mathbb{Z}$.
2. יהי R חוג. אם S הוא תת־חוג של R, אז $M_n(S)$ הוא תת־חוג של $M_n(R)$.
3. אם איבר היחידה של R שייך לתת־חוג S, אז הוא איבר היחידה של S. האם ההפך נכון? בדקו מה קורה בשרשרת החוגים בלי יחידה הבאה:

$$\left\{\begin{pmatrix} * & 0 \\ 0 & 0 \end{pmatrix}\right\} \subset \left\{\begin{pmatrix} * & * \\ 0 & 0 \end{pmatrix}\right\} \subset \left\{\begin{pmatrix} * & * \\ 0 & * \end{pmatrix}\right\} \subset M_2(\mathbb{C})$$

תרגיל 1.17. יהי R חוג בלי יחידה, ויהי $0 \neq a \in R$. הוכיחו כי aRa הוא תת־חוג בלי יחידה של R.

פתרון. ברור כי aRa לא ריקה ומוכלת ב-R. יהיו $aba, aca \in aRa$. לפי טענה 1.15 מספיק לבדוק כי

$$\begin{aligned} aba - aca &= a(ba - ca) = a(b - c)a \in aRa \\ aba \cdot aca &= a(baac)a \in aRa \end{aligned}$$

תרגיל 1.18. נניח $e^2 = e \in R$ (איבר כזה נקרא אידמפוטנט). הוכיחו כי e הוא איבר היחידה של eRe. Idempotent

פתרון. יהי $eae \in eRe$. אז $e \cdot eae = e^2ae = eae = eae^2 = eae \cdot e$.

הגדרה 1.19. יהי R חוג. המֶרְכָּז של R הוא Center

$$Z(R) = \{r \in R \,|\, \forall a \in R, ar = ra\}$$

המְרַכֵּז של תת־קבוצה $S \subseteq R$ הוא Centralizer

$$C_R(S) = \{r \in R \,|\, \forall a \in S, ar = ra\}$$

דוגמה 1.20. יהי R חוג. הנה כמה תכונות ברורות, וכמה פחות לגבי מרכזים:

1. $Z(R)$ הוא תת־חוג חילופי של R.
2. R חילופי אם"ם $R = Z(R)$ אם"ם לכל $S \subseteq R$ מתקיים $C_R(S) = R$.
3. $Z(M_n(R)) = Z(R) \cdot I_n$.
4. $C_R(S)$ הוא תת־חוג של R.
5. $S \subseteq C_R(C_R(S))$.
6. $C_R(S) = C_R(C_R(C_R(S)))$ (העזרו בכך שאם $S \subseteq S'$, אז $C_R(S') \subseteq C_R(S)$).

דוגמה 1.21. 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 $\mathbb{H} = \mathrm{Span}_{\mathbb{R}} \{1, i, j, k\}$ ומתקיים $Z(\mathbb{H}) = \mathrm{Span}_{\mathbb{R}} \{1\} \cong \mathbb{R}$.

2 תרגול שני

תרגיל 2.1 (לדלג)**.** יהי F שדה עם מאפיין שונה מ-2, ויהי $a \in F$ כך ש-$a \notin (F^\times)^2$. נסמן

$$K = F[\sqrt{a}] = \left\{ \alpha + \beta\sqrt{a} \,\middle|\, \alpha, \beta \in F \right\}$$

ואפשר לבדוק כי K שדה. נניח וקיים $b \in F^\times$ כך שלכל $u, v \in F$ מתקיים $b \neq u^2 - av^2$ (לא לדאוג, קיימים שדות כאלו, כמו $F = \mathbb{Q}$, $a = -2$, $b = -5$). יהי $x = \alpha + \beta\sqrt{a}$, ונסמן $\bar{x} = \alpha - \beta\sqrt{a}$.

הוכיחו כי הקבוצה הבאה היא חוג חילוק לא חילופי:

$$D = \left\{ \begin{pmatrix} x & y \\ b\bar{y} & \bar{x} \end{pmatrix} \,\middle|\, x, y \in K \right\}$$

פתרון. נוכיח כי D הוא תת־חוג של $M_2(K)$. הסגירות להפרש היא ברורה.

עבור הסגירות לכפל נשים לב

$$\begin{pmatrix} x & y \\ b\bar{y} & \bar{x} \end{pmatrix} \begin{pmatrix} z & w \\ b\bar{w} & \bar{z} \end{pmatrix} = \begin{pmatrix} xz + yb\bar{w} & xw + y\bar{z} \\ b\bar{y}z + \bar{x}b\bar{w} & b\bar{y}w + \bar{x}\bar{z} \end{pmatrix} \in D$$

כדי להראות ש-D לא חילופי מספיק לבדוק

$$\begin{pmatrix} 0 & 1 \\ b & 0 \end{pmatrix} \begin{pmatrix} \sqrt{a} & 0 \\ 0 & -\sqrt{a} \end{pmatrix} \neq \begin{pmatrix} \sqrt{a} & 0 \\ 0 & -\sqrt{a} \end{pmatrix} \begin{pmatrix} 0 & 1 \\ b & 0 \end{pmatrix}$$

כעת נראה כי לכל איבר יש הופכי ב-D. מספיק להראות שלכל $0 \neq M \in D$ מתקיים $\det(M) \neq 0$. אכן

$$\det \begin{pmatrix} x & y \\ b\bar{y} & \bar{x} \end{pmatrix} = x\bar{x} - by\bar{y}$$

וזה יהיה שווה 0 אם ורק אם $x\bar{x} = by\bar{y}$. אם $y = 0$, אז $x\bar{x} = 0$, לכן $\alpha^2 - a\beta^2 = 0$ ולכן $\alpha = \beta = 0$, כי a אינו ריבוע ב-F. כלומר קיבלנו את מטריצת האפס. אם $y \neq 0$, אז

$$b = \frac{x\bar{x}}{y\bar{y}}$$

נניח $\frac{x}{y} = u + v\sqrt{a}$, אז $b = u^2 - av^2$, וזו סתירה להנחה. בסך הכל קיבלנו כי M הפיך ב-$M_2(K)$. כעת רק נותר להראות כי $M^{-1} \in D$, וזה חישוב שנשאיר לבית.

הגדרה 2.2. יהיו R, S חוגים. נאמר כי $\varphi \colon R \to S$ הוא הומומורפיזם של חוגים אם: Ring homomorphism

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 φ הוא הומומורפיזם של חוגים בלי יחידה.

דוגמה 2.3. הומומורפיזם האפס $\varphi(r) = 0_S$ לכל $r \in R$ הוא הומומורפיזם של חוגים בלי יחידה.

Epimorphism
Projection

דוגמה 2.4. הומומורפיזם על נקרא אפימורפיזם או הטלה. למשל $\varphi\colon \mathbb{Z} \to \mathbb{Z}_n$ המוגדר לפי $\varphi(x) = x \pmod n$ הוא אפימורפיזם של חוגים.

טענה 2.5. יהיו R, S חוגים עם יחידה, ויהי $\varphi\colon R \to S$ 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. $\square$

Monomorphism
Embedding

דוגמה 2.6. הומומורפיזם חח"ע נקרא מונומורפיזם או שיכון. למשל $\varphi\colon \mathbb{Z} \to \mathbb{Q}$ המוגדר לפי $\varphi(x) = x$ הוא מונומורפיזם של חוגים. מה לגבי $\phi\colon 2\mathbb{Z} \to \mathbb{Q}$ המוגדר לפי $\phi(x) = x$? זה מונומורפיזם של חוגים בלי יחידה.

דוגמה 2.7. יהי R חוג חילופי, ויהי A חוג המטריצות האלכסוניות ב-$M_2(A)$. נגדיר $\varphi\colon A \to A$ לפי

$$\varphi\left(\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}\right) = \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix}$$

אז φ הומומורפיזם של חוגים בלי יחידה כי

$$\begin{aligned}
\varphi\left(\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}\begin{pmatrix} c & 0 \\ 0 & d \end{pmatrix}\right) &= \varphi\left(\begin{pmatrix} ac & 0 \\ 0 & bd \end{pmatrix}\right) = \begin{pmatrix} ac & 0 \\ 0 & 0 \end{pmatrix} \\
&= \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} c & 0 \\ 0 & 0 \end{pmatrix} = \varphi\left(\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}\right)\varphi\left(\begin{pmatrix} c & 0 \\ 0 & d \end{pmatrix}\right) \\
\varphi\left(\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} + \begin{pmatrix} c & 0 \\ 0 & d \end{pmatrix}\right) &= \varphi\left(\begin{pmatrix} a+c & 0 \\ 0 & b+d \end{pmatrix}\right) = \begin{pmatrix} a+c & 0 \\ 0 & 0 \end{pmatrix} \\
&= \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} c & 0 \\ 0 & 0 \end{pmatrix} = \varphi\left(\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}\right) + \varphi\left(\begin{pmatrix} c & 0 \\ 0 & d \end{pmatrix}\right)
\end{aligned}$$

אבל

$$\varphi\left(1_A\right) = \varphi\left(\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\right) = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \neq 1_A$$

Isomorphism
Isomorphic

הגדרה 2.8. הומומורפיזם חח"ע ועל נקרא איזומורפיזם. נאמר שחוגים R, S שיש בינהם איזומורפיזם $\varphi\colon R \to S$ הם איזומורפיים ונסמן $R \cong S$.

דוגמה 2.9. העתקת הזהות היא תמיד איזומורפיזם. אבל יש עוד, למשל $\varphi\colon \mathbb{C} \to \mathbb{C}$ המוגדרת לפי $\varphi(z) = \bar{z}$ היא איזומורפיזם של חוגים.

תרגיל 2.10. יהי $\varphi\colon \mathbb{Q} \to \mathbb{Q}$ הומומורפיזם של חוגים. הוכיחו כי $\varphi = \mathrm{id}$.

פתרון. יהי $n \in \mathbb{N}$. אז

$$\varphi(n) = \varphi(\underbrace{1 + \cdots + 1}_{n \text{ times}}) = \underbrace{\varphi(1) + \cdots + \varphi(1)}_{n \text{ times}} = \underbrace{1 + \cdots + 1}_{n \text{ times}} = n$$

כי $\varphi(1) = 1$. לכל הומומורפיזם מתקיים $\varphi(0) = 0$, ולכן

$$\varphi(1) + \varphi(-1) = \varphi(1 - 1) = \varphi(0) = 0$$

נקבל כי $\varphi(-1) = -\varphi(1) = -1$. באופן דומה למספרים טבעיים נקבל שגם $\varphi(-n) = -n$. כמו כן

$$1 = \varphi(1) = \varphi\left(n \cdot \frac{1}{n}\right) = n\varphi\left(\frac{1}{n}\right)$$

ולכן $\varphi\left(\frac{1}{n}\right) = \frac{1}{n}$. לכל $m \in \mathbb{Z}$, נקבל ש-φ הוא הזהות עבור $\frac{m}{n}$:

$$\varphi\left(\frac{m}{n}\right) = \varphi\left(m \cdot \frac{1}{n}\right) = \varphi(m)\varphi\left(\frac{1}{n}\right) = \frac{m}{n}$$

כמו שראינו, עבור שדות אחרים התרגיל הזה לא בהכרח נכון. למשל $\phi\colon \mathbb{Q}[\sqrt{2}] \to \mathbb{Q}[\sqrt{2}]$ המוגדר לפי $\phi(a + b\sqrt{2}) = a - b\sqrt{2}$ הוא איזומורפיזם, אבל $\phi \neq \mathrm{id}$.

תרגיל 2.11. יהי R חוג. הוכיחו $M_n(R[x]) \cong M_n(R)[x]$.

הגדרה 2.12. יהי $\varphi\colon R \to S$ הומומורפיזם של חוגים. כמו בקורסים אלגברה לינארית ותורת החבורות אי אפשר להתחמק מההגדרות הבאות:

Image

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

Kernel

2. הגרעין של φ 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 $1_R \notin \operatorname{Ker}\varphi$.

Endomorphism
Automorphism

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

הגדרה 2.13. יהי R חוג, $I \subseteq R$ תת־חבורה חיבורית.

Left ideal

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

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 $I \leq_r R$. 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 2.14. בחוג חילופי ההגדרות השונות של אידאל מתלכדות.

דוגמה 2.15. 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 2.16. יהי $\varphi \colon R \to S$ הומומורפיזם. אז $\operatorname{Ker}\varphi \lhd R$. למעשה גם כל אידאל הוא גרעין של הומומורפיזם כלשהו.

דוגמה 2.17. האידאלים היחידים של $\mathbb{Z}$ הם $n\mathbb{Z}$.

דוגמה 2.18. נרחיב את הדוגמה הקודמת. יהי $a \in R$. אז הקבוצה $Ra = \{ra \,|\, r \in R\}$ היא אידאל שמאלי. הרי אם $x \in Ra$, אז קיים $r \in R$ כך ש-$x = ra$, ואז לכל $s \in R$ מתקיים

$$sx = s(ra) = (sr)a \in Ra$$

תת־קבוצה מהצורה Ra נקראת אידאל ראשי שמאלי. Left principal ideal

דוגמה 2.19. נמצא אידאל שמאלי שאינו אידאל ימני. נבחר $R = M_2(\mathbb{Q})$ ואת יחידת המטריצה e_{12}. אז

$$Re_{12} = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \,\middle|\, \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in R \right\} = \left\{ \begin{pmatrix} 0 & a \\ 0 & c \end{pmatrix} \,\middle|\, a, c \in \mathbb{Q} \right\}$$

הוא בודאי אידאל שמאלי. זהו לא אידאל ימני של R כי למשל

$$\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \notin Re_{12}$$

תרגיל 2.20. יהי $R = \mathbb{Z}[\sqrt{5}]$, ונבחר $I = \left\{ a + b\sqrt{5} \,\middle|\, a \in 5\mathbb{Z}, b \in \mathbb{Z} \right\}$. הוכיחו $I \lhd R$.

פתרון. קל לראות כי I חבורה חיבורית (שאיזומורפית ל-$5\mathbb{Z} \times \mathbb{Z}$). יהיו $a + b\sqrt{5} \in R$, $5n + m\sqrt{5} \in I$. אז

$$\left(a + b\sqrt{5}\right)\left(5n + m\sqrt{5}\right) = 5\,(an + bm) + (am + 5bn)\,\sqrt{5} \in I$$

מהחילופיות נובע ש-I הוא אידאל דו־צדדי.

תרגיל 2.21. 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 2.22. 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 2.23. אידאל נאות אף פעם לא מכיל את איבר היחידה של החוג. אף יותר, אידאל נאות לא מכיל איברים הפיכים כלל.

מסקנה 2.24. בחוג חילוק כל האידאלים הם טריוויאליים.

תרגיל 2.25. יהיו $a, b \in \mathbb{N}$. הוכיחו כי $b|a$ אם ורק אם $a\mathbb{Z} \subseteq b\mathbb{Z}$.

פתרון. מצד אחד, אם $a\mathbb{Z} \subseteq b\mathbb{Z}$, אזי בפרט $a \in b\mathbb{Z}$. לכן קיים $n \in \mathbb{Z}$ כך שמתקיים $a = bn$, כלומר $b|a$. מצד שני, אם $b|a$, אז קיים $n \in \mathbb{Z}$ כך שמתקיים $a = bn$. לכן אם $x \in a\mathbb{Z}$, קיים $m \in \mathbb{Z}$ כך ש-$x = am$ ולכן $x = bnm$, כלומר $x \in b\mathbb{Z}$.

תרגיל 2.26. הוכיחו שחיתוך אידאלים הוא אידאל.

פתרון. יהיו $I, J \lhd R$ אידאלים. לכל $r \in R$, $i \in I \cap J$ מתקיים $r \cdot i \in I$ וגם $r \cdot i \in J$ כי I, J הם אידאלים. לכן $r \cdot i \in I \cap J$. כידוע לנו חיתוך תת־חבורות הוא חבורה, ולכן $I \cap J$ אידאל. ודאו שאתם יכולים להראות שחיתוך כל קבוצה של אידאלים היא אידאל.

הגדרה 2.27. יהיו I, J אידאלים. נגדיר את סכום האידאלים האלו לפי

Sum of ideals

$$I + J = \{i + j \mid i \in I, j \in J\}$$

ודאו שאתם יודעים להוכיח שזהו אידאל. כתבו את ההגדרה לסכום אידאלים סופי.

דוגמה 2.28. יהיו $a, b \in \mathbb{Z}$. אז

$$a\mathbb{Z} \cap b\mathbb{Z} = \operatorname{lcm}(a, b)\mathbb{Z}, \qquad a\mathbb{Z} + b\mathbb{Z} = \gcd(a, b)\mathbb{Z}$$

משפט 2.29. אוסף האידאלים של חוג עם יחס ההכלה הוא סריג מודולרי מלא, שבו $I \vee J = I + J$, $I \wedge J = I \cap J$.

הגדרה 2.30. למשפחה Λ של אידאלים נגדיר את הסכום $\sum_{L \in \Lambda} L$ להיות אוסף הסכומים הסופיים $x_1 + \cdots + x_n$ עבור $x_i \in L_i \in \Lambda$.

ודאו שאתם יודעים להוכיח שהסכום של משפחת אידאלים (שמאליים, ימניים, דו־צדדיים) הוא אידאל (שמאלי, ימני, דו־צדדי), ושהוא איחוד של כל הסכומים הסופיים של אידאלים במשפחה Λ.

הגדרה 2.31. יהי R חוג, ויהי $x \in R$ איבר. האידאל שנוצר על ידי x הוא

Ideal generated by x

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

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

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

הערה 2.32. למה $\langle x\rangle$ הוא אכן אידאל? קל לראות שזו תת־חבורה חיבורית, ושלכל $r\in R$ מתקיים

$$r\cdot\left(\sum_{i=1}^{n}\alpha_i x\beta_i\right)=\sum_{i=1}^{n}(r\alpha_i)x\beta_i\in\langle x\rangle\,,\qquad\left(\sum_{i=1}^{n}\alpha_i x\beta_i\right)\cdot r=\sum_{i=1}^{n}\alpha_i x(\beta_i r)\in\langle x\rangle$$

זהו האידאל המינימלי המכיל את x והוא שווה לחיתוך כל האידאלים המכילים את x. בנוסף, אם $x\in Z(R)$, אז $\langle x\rangle=Rx=xR$.

דוגמה 2.33. בחוג $\mathbb{Z}[x]$ מתקיים

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

תרגיל 2.34. מצאו חוג R ואיבר $x\in R$ כך ש-$\langle x\rangle\neq Rx$.

פתרון. חייבים לבחור חוג לא חילופי. נשתמש בדוגמה 2.19 ונבחר $R=M_2(\mathbb{Q})$, $x=e_{12}$. אז

$$Re_{12}=\left\{\begin{pmatrix}a&b\\c&d\end{pmatrix}\begin{pmatrix}0&1\\0&0\end{pmatrix}\,\middle|\,\begin{pmatrix}a&b\\c&d\end{pmatrix}\in R\right\}=\left\{\begin{pmatrix}0&a\\0&c\end{pmatrix}\,\middle|\,a,c\in\mathbb{Q}\right\}$$

ואם נבחר $c\neq 0$ נקבל איבר ששייך ל-$\langle x\rangle$ אבל לא ל-Rx:

$$\begin{pmatrix}1&0\\0&1\end{pmatrix}\begin{pmatrix}0&1\\0&0\end{pmatrix}\begin{pmatrix}a&b\\c&d\end{pmatrix}=\begin{pmatrix}c&d\\0&0\end{pmatrix}\in\left\langle\begin{pmatrix}0&1\\0&0\end{pmatrix}\right\rangle$$

הגדרה 2.35. יהיו I,J אידאלים. נגדיר את מכפלת האידאלים האלו לפי Product of ideals

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

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

הערה 2.36. לכל זוג אידאלים I,J מתקיים $IJ\subseteq I\cap J$.

דוגמה 2.37. המכפלה "הנקודתית" של אידאלים אינה בהכרח אידאל. נבחר בחוג $\mathbb{Z}[x]$ את $I=\langle 2,x\rangle$ ואת $J=\langle 3,x\rangle$. אז הקבוצה

$$S=\{f\cdot g\,|\,f\in I,g\in J\}$$

אינה אידאל. האיברים באידאלים האלו הם מהצורה $f=2f_1+xf_2\in I$, $g=3g_1+xg_2\in J$. אם נבחר $f=2$, $g=3$, אז $6\in S$. אם נבחר $f=g=x$, אז $x^2\in S$. נוכיח כי $6+x^2\notin S$, ולכן S אינה תת־חבורה חיבורית של החוג, ובפרט

לא אידאל. נניח בשלילה כי קיימים $f_1, f_2, g_1, g_2 \in \mathbb{Z}[x]$ ממעלה לכל היותר 2, ובלי הגבלת הכלליות f_1, g_1 הם קבועים, כך ש-

$$\begin{aligned}(2f_1 + xf_2)(3g_1 + xg_2) &= 6 + x^2 \\ 6f_1g_1 + (2f_1g_2 + 3f_2g_1)x + f_2g_2x^2 &= 6 + x^2\end{aligned}$$

אז $f_1g_1 = f_2g_2 = 1$. לכן $f_1 = g_1 = \pm 1$, $f_2 = g_2 = \pm 1$. אבל אז לא יתכן כי

$$2f_1g_2 + 3f_2g_1 = 0$$

Comaximal ideals

הגדרה 2.38. יהי R חוג, ויהיו $I, J \lhd R$. נאמר כי I, J הם קו־מקסימליים אם $I + J = R$.

תרגיל 2.39. יהי R חוג חילופי. הוכיחו שאם I, J קו־מקסימליים, אז $IJ = I \cap J$.

פתרון. ראינו בהערה 2.36 כי $IJ \subseteq I \cap J$. נתון כי $I + J = R$. לכן קיימים $i \in I$, $j \in J$ כך ש-$i + j = 1$. יהי $a \in I \cap J$. אז

$$a = a \cdot 1 = a(i + j) = a \cdot i + a \cdot j = i \cdot a + a \cdot j \in IJ$$

ראינו דוגמה לכך בקורס בתורת החבורות. אם $R = \mathbb{Z}$, $I = 2\mathbb{Z}$ ו-$J = 3\mathbb{Z}$, אז

$$1 = 3 \cdot 1 + 2 \cdot (-1) \in I + J$$

ולכן $I + J = \mathbb{Z}$. לפי מה שהוכחנו $2\mathbb{Z} \cap 3\mathbb{Z} = 2\mathbb{Z} \cdot 3\mathbb{Z} = 6\mathbb{Z}$.

תרגיל 2.40. הוכיחו כי האידאלים $\langle x - 1 \rangle$, $\langle 2x - 1 \rangle$ הם קו־מקסימליים בחוג $\mathbb{Z}[x]$.

פתרון. פשוט נראה כי 1 שייך לסכום האידאלים. אכן

$$1 = (-2) \cdot (x - 1) + (2x - 1) \in \langle x - 1 \rangle + \langle 2x - 1 \rangle$$

3 תרגול שלישי

Principal ideal

Principal ideal domain (PID)

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.

דוגמה 3.2. $\mathbb{Z}$ הוא תחום ראשי. האידאלים שלו הם מן הצורה $m\mathbb{Z}$.

תרגיל 3.3. הוכיחו כי $\mathbb{Z}[x]$ אינו ראשי.

פתרון. נביט באידאל $\langle 2, x \rangle \lhd \mathbb{Z}[x]$. יהי $h(x) = 2f(x) + xg(x) \in \langle 2, x \rangle$. אז $h(0) \in 2\mathbb{Z}[x]$, ונסיק כי $1 \notin \langle 2, x \rangle$. לכן זה אידאל נאות. נניח בשלילה כי $\langle q \rangle = \langle 2, x \rangle$, אז $2 \in \langle q \rangle$ וגם $x \in \langle q \rangle$. כלומר q הוא מחלק משותף של 2 ושל x בחוג $\mathbb{Z}[x]$. לכן $q = \pm 1$, ונגיע לסתירה כי $\langle q \rangle = \mathbb{Z}[x]$ אינו נאות.

הערה 3.4. בחוג $\mathbb{Q}[x]$ האידאל $\langle 2,x\rangle$ הוא ראשי כי

$$\langle 2,x\rangle=\langle 2\rangle+\langle x\rangle=\mathbb{Q}[x]+\langle x\rangle=\mathbb{Q}[x]=\langle 1\rangle$$

תרגיל 3.5 (לבית)**.** הוכיחו שבחוג $\mathbb{Q}[x,y]$ האידאל $\langle x,y\rangle$ אינו ראשי.

טענה 3.6. 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.

דוגמה 3.7. חוג R יקרא פשוט אם אין לו אידאלים פרט ל-R ול-$\{0\}$. Simple

דוגמה 3.8. חוג חילוק הוא פשוט. האם ההפך נכון?

תרגיל 3.9. 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 $yx=1$. לכן R שדה.

תרגיל 3.10. הוכיחו שאם R חוג פשוט, אז $Z(R)$ שדה.

פתרון. ראינו כבר כי $Z(R)$ הוא תת־חוג חילופי. יהי $0\neq x\in Z(R)$. מפני ש-R פשוט נקבל $Rx=xR=R$. כמו בתרגיל הקודם קיבלנו כי x הפיך. נשאר להוכיח כי $x^{-1}\in Z(R)$. עבור כל $r\in R$ מתקיים $xr=rx$, לכן $r=x^{-1}xr=x^{-1}rx$, לכן $rx^{-1}=x^{-1}r$, ולכן $x^{-1}\in Z(R)$.

משפט 3.11. יהי $I\lhd R$. אז $M_n(I)\lhd M_n(R)$ וכל אידאל של $M_n(R)$ הוא מן הצורה הזו.

דוגמה 3.12. $M_n(2\mathbb{Z})\lhd M_n(\mathbb{Z})$.

הערה 3.13. 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 $Z(M_n(D))=\{d\cdot I_n\,|\,d\in Z(D)\}$.

תרגיל 3.14. יהי $M_n(R)\supseteq A$ תת־חוג, ויהי $I\lhd A$. האם קיים $J\lhd R$ כך ש-$I=A\cap M_n(J)$?

פתרון. לא. ניקח בתור A את המטריצות המשולשיות העליונות ב-$M_2(\mathbb{Z})$, ובתור I את המטריצות ב-A עם אפסים באלכסון. כל האידאלים של $M_2(\mathbb{Z})$ הם מן הצורה $M_2(m\mathbb{Z})$ והחיתוך שלהם עם A מכיל מטריצות שאינן ב-I.

תרגיל 3.15. יהי D חוג חילוק שאינו שדה. נסמן $F=Z(D)$. הוכיחו שלכל $d\in D\backslash F$ מתקיים $\langle x-d\rangle=D[x]$.

פתרון. נוכיח שהאידאל $\langle x-d\rangle$ מכיל איבר הפיך. יהי $e\in D$ כך ש-$ed\neq de$. אז

$$f(x)=-e(x-d)+(x-d)e\in\langle x-d\rangle$$

ובנוסף $f(x)=ed-de\in D$. מפני ש-D חוג חילוק, אז ל-$f(x)$ יש הופכי. לכן $\langle x-d\rangle=D[x]$.

שימו לב שאם $a\in F$, אז $\langle x-a\rangle\neq F[x]$ (לאיברים באידאל דרגה לפחות 1).

תרגיל 3.16. תנו דוגמה לחוגים R,S, הומומורפיזם $\varphi\colon R\to S$ ואידאל $I\lhd R$ 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 $\varphi=\mathrm{id}$. התמונה של $\mathbb{Z}$ תחת φ היא $\mathbb{Z}$, וזה לא אידאל של $\mathbb{Q}$, כי האידאלים היחידים שלו הם טריוויאלים.

הגדרה 3.17. יהי R חוג, ויהי $I\lhd R$ אידאל. חוג המנה הוא הקבוצה Quotient ring

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

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

דוגמה 3.19. $R=3\mathbb{Z}$, $I=18\mathbb{Z}$. אז

$$R/I=\{18\mathbb{Z},3+18\mathbb{Z},6+18\mathbb{Z},9+18\mathbb{Z},12+18\mathbb{Z},15+18\mathbb{Z}\}$$

החבורה החיבורית של חוג המנה איזומורפית לחבורה $\mathbb{Z}_6$ (בקורס בתורת החבורות היינו מסמנים $R/I\cong\mathbb{Z}/6\mathbb{Z}$). לפי טבלת הכפל נראה שכחוגים R/I לא איזומורפי ל-$\mathbb{Z}/6\mathbb{Z}$:

$\cdot$	0	3	6	9	12	15
0	0	0	0	0	0	0
3	0	9	0	9	0	9
6	0	0	0	0	0	0
9	0	9	0	9	0	9
12	0	0	0	0	0	0
15	0	9	0	9	0	9

דוגמה 3.20. יהי p ראשוני, אז

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

דוגמה 3.21. 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 $R/I\cong\mathbb{C}$.

תרגיל 3.22. יהי $R = \mathbb{Z}/3\mathbb{Z}[x]$, $I = \langle x^2+1 \rangle$. מה העוצמה של R/I?

פתרון. באופן דומה לתרגיל הקודם נקבל $R/I = \{\alpha + \beta\overline{x} \mid \alpha, \beta \in \mathbb{Z}/3\mathbb{Z}\}$. לכן $|R/I| = 9$.

הגדרה 3.23. איבר $x \in R$ הוא נילפוטנטי אם קיים $n \in \mathbb{N}$ כך ש-$x^n = 0$. Nilpotent

תרגיל 3.24. 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.

פתרון.

1. N אינו ריק כי $0 \in N$. יהיו $a, b \in N$. אז קיימים $n, m \in \mathbb{N}$ כך ש-$a^n = b^m = 0$. נוסחת הבינום של ניוטון נכונה גם בחוגים חילופיים. לכן

$$(a-b)^{n+m} = \sum_{k=0}^{n+m} (-1)^k \binom{n+m}{k} a^k b^{n+m-k}$$

אם $k \geq n$, אז $a^k = 0$. אחרת, $k < n$ ולכן $m < n+m-k$, כלומר $b^{n+m-k} = 0$. לכן $a - b \in N$. ברור שאם $r \in R$, אז $ra \in N$ כי $(ra)^n = r^n a^n = 0$.

2. נניח בשלילה כי $\overline{0} \neq \overline{x} = x + N \in R/N$ הוא נילפוטנטי. אז קיים $n \in \mathbb{N}$ כך ש-$\overline{x}^n = \overline{0}$. כלומר

$$N = \overline{0} = \overline{x}^n = (x+N)^n = x^n + N$$

ולכן $x^n \in N$. כלומר x^n הוא נילפוטנטי, ולכן קיים $k \in \mathbb{N}$ כך ש-$(x^n)^k = 0$. לכן $x^{nk} = 0$, ונקבל $x \in N$. אך זו סתירה כי הנחנו $\overline{x} \neq \overline{0} = N$.

3. נבחר $R = M_2(\mathbb{Q})$, $e_{21} = \left(\begin{smallmatrix} 0 & 0 \\ 1 & 0 \end{smallmatrix}\right)$, $e_{12} = \left(\begin{smallmatrix} 0 & 1 \\ 0 & 0 \end{smallmatrix}\right)$. אז $e_{12}^2 = e_{21}^2 = 0$, ולכן הם נילפוטנטיים. אבל לכל $n \in \mathbb{N}$

$$(e_{12} + e_{21})^n = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}^n \neq \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

ולכן $e_{12} + e_{21} \notin N$. כלומר N אינו סגור לחיבור, ובפרט אינו אידאל.

משפט 3.25 (משפט האיזומורפיזם הראשון)**.** יהי $f\colon R \to S$ הומומורפיזם, אז First isomorphism theorem

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

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

דוגמה 3.26. יהי $f\colon \mathbb{Z} \to \mathbb{Z}_n$ 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.

הגדרה 3.27. 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.

Subring generated by X

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

Finitely generated

הערה 3.28. $R_0[X]$ הוא תת־החוג הקטן ביותר (ביחס להכלה) של R המכיל את R_0 ואת X.

הערה 3.29. אם $a \in Z(R)$, אז $R_0[a]$ הוא אוסף הפולינומים ב-a עם מקדמים מ-R_0.

דוגמה 3.30. $R = \mathbb{Z}$ נוצר סופית מעל כל תת־חוג $R_0 = n\mathbb{Z}$ עבור $n \neq 0$, כי $R_0[1] = \mathbb{Z}$.

דוגמה 3.31. יהי $S = R[x_1, \ldots, x_n]$ חוג פולינומים ב-n-משתנים מעל R. אז S נוצר סופית מעל R עבור $X = \{x_1, \ldots, x_n\}$.

תרגיל 3.32. כל חוג חילופי שנוצר סופית מעל R_0 הוא מנה (ליתר דיוק, איזומורפי למנה, אבל אנחנו לא נדקדק) של חוג הפולינומים $R_0[x_1, \ldots, x_n]$ עבור n כלשהו.

פתרון. יהי S חוג שנוצר סופית מעל R_0. אז קיימת $X = \{a_1, \ldots, a_n\}$ כך ש-$S = R_0[a_1, \ldots, a_n]$. נגדיר העתקה $\pi\colon R_0[x_1, \ldots, x_n] \to S$ לפי $\pi(x_i) = a_i$, $\pi(r) = r$ לכל $r \in R_0$ והרחבת ההגדרה באופן שמכבד חיבור וכפל. כלומר לכל איבר של $R_0[x_1, \ldots, x_n]$ נגדיר $\pi(f(x_1, \ldots, x_n)) = f(a_1, \ldots, a_n)$. הוכיחו כי זו הומומורפיזם של חוגים.

אפשר לבדוק כי π הוא על: כל איבר של S ניתן להציג כפולינום $f(a_1, \ldots, a_n)$, ומקור אפשרי שלו הוא $f(x_1, \ldots, x_n)$. לפי משפט האיזומורפיזם הראשון $S \cong R/\operatorname{Ker}\pi$.

הערה 3.33. 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-$\mathbb{Z}/2\mathbb{Z}[x]$ (הוכיחו שקיים אפימורפיזם $\varphi\colon \mathbb{Z}[x] \to \mathbb{Z}/2\mathbb{Z}[x]$ שהגרעין שלו הוא $2\mathbb{Z}[x]$). אבל $\mathbb{Z}/2\mathbb{Z}[x]$ אינו נוצר סופית מעל $\mathbb{Z}$, כיוון שאינו מכיל תת־חוג האיזומורפי ל-$\mathbb{Z}$, שהרי לכל $a \in \mathbb{Z}/2\mathbb{Z}[x]$ מתקיים $2a = 0$.

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

דוגמה 3.34. יהי $a \in R$ (התוצאה תהיה נכונה כאשר R לא חילופי, אם $a \in Z(R)$), ונביט בהעתקת ההצבה $\varphi_a\colon R[x] \to R$ 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 $\operatorname{Ker}\varphi_0 = \langle x \rangle$, 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 3.35. הראו כי $\operatorname{Ker}\varphi_a = \langle x-a\rangle$.

פתרון. נסתכל על ההעתקה $\psi\colon R[x]\to R[x]$ המוגדרת לפי $\psi(1)=1$, $\psi(x)=x-a$ והרחבה להומומורפיזם. הוכיחו שקיבלנו למעשה איזומורפיזם. נשים לב ש-0 הוא שורש של $f(x)\in R[x]$ אם ורק אם a הוא שורש של $\psi(f(x))$, וגם שמקבלים $\psi(\langle x\rangle)=\langle x-a\rangle$.

השרשרת $R[x]\xrightarrow{\psi^{-1}}R[x]\xrightarrow{\varphi_0}R$ היא בעצם הצבת a, והגרעין שלה הוא $\langle x-a\rangle$.

דוגמה 3.36. כל פולינום $f(x)\in R[x]$ אפשר לזהות כפונקציה $f(x)\colon R\to R$. נסתכל על חוג הפונקציות מ-R ל-R, שנסמן R^R עם חיבור וכפל "נקודתי". כלומר $(fg)(x)=f(x)g(x)$, $(f+g)(x)=f(x)+g(x)$. מצאו את איבר היחידה ואיבר האפס בחוג הזה.

מכאן קל להגדיר הומומורפיזם $\varphi\colon R[x]\to R^R$. שימו לב שזה לא בהכרח שיכון. למשל אם $R={}^{\mathbb{Z}}/_{2\mathbb{Z}}$, אז $\varphi(x^2-x)=0$. בנוסף φ לא בהכרח על. למשל אם $R=\mathbb{R}$, אז לפונקציה e^x אין מקור. לפי משפט האיזומורפיזם הראשון, נקבל $R[x]/\operatorname{Ker}\varphi\cong\operatorname{Im}\varphi$, כאשר הגרעין הוא אוסף כל הפולינומים שהצבת כל ערך מ-R תתן 0. את התמונה נסמן $\operatorname{Im}\varphi=P(R)$, ונקרא לה חוג הפונקציות הפולינומיאליות מעל R. אפשר לקבל הגדרות דומות ליותר ממשתנה אחד.

Ring of polynomial functions

תרגיל 3.37. הוכיחו שהחוגים

$$R={}^{\mathbb{C}[x,y]}/_{\langle xy-1\rangle},\qquad S={}^{\mathbb{C}[x,y]}/_{\langle y-x^2\rangle}$$

אינם איזומורפיים.

פתרון. נראה כי $R\cong\mathbb{C}[t,t^{-1}]$, $S\cong\mathbb{C}[t]$ לפי בניית איזומורפיזמים:

$$R\xrightarrow[x\mapsto t,y\mapsto t^{-1}]{\sim}\mathbb{C}[t,t^{-1}],\qquad S\xrightarrow[x\mapsto t,y\mapsto t^2]{\sim}\mathbb{C}[t]$$

ועכשיו נותר להראות $\mathbb{C}[t,t^{-1}]\not\cong\mathbb{C}[t]$. נזכר בתרגיל לפיו אם T תחום, אז $(T[x])^\times=T^\times$. נקבל כי

$$S^\times\cup\{0\}\cong(\mathbb{C}[t])^\times\cup\{0\}=\mathbb{C}^\times\cup\{0\}$$

היא קבוצה הסגורה לחיבור, אבל $R^\times\cup\{0\}$ לא סגורה לחיבור כי $1,t\in\mathbb{C}[t,t^{-1}]$ ואילו $1+t$ לא הפיך.

4 תרגול רביעי

משפט 4.1 (משפט האיזומורפיזם השני)**.** יהי $I\lhd R$ אידאל, ויהי $S\subseteq R$ תת־חוג. אז

Second isomorphism theorem

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

דוגמה 4.2. הזכרו כי לכל $n, m \in \mathbb{Z}$ מתקיים

$$\gcd(n,m)\operatorname{lcm}(n,m) = |nm|$$

נראה דרך להוכיח זאת עם אידאלים של $\mathbb{Z}$. למשל לפי משפט האיזומורפיזם השני

$$\gcd(n,m)\mathbb{Z}/n\mathbb{Z} = n\mathbb{Z}+m\mathbb{Z}/n\mathbb{Z} \cong m\mathbb{Z}/n\mathbb{Z}\cap m\mathbb{Z} = m\mathbb{Z}/\operatorname{lcm}(n,m)\mathbb{Z}$$

תרגיל 4.3. 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 $\varphi \colon R/I \to R/J$ 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 φ אפימורפיזם.

משפט 4.4 (משפט האיזומורפיזם השלישי). יהיו $I \subseteq J$ אידאלים של חוג R. אז

Third isomorphism theorem

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

הגדרה 4.5. אידאל נאות $I \lhd R$ נקרא אידאל מקסימלי אם לא קיים אידאל נאות שמכיל אותו ממש.

Maximal ideal

דוגמה 4.6. בחוג $\mathbb{Z}/32\mathbb{Z}$ יש רק אידאל מקסימלי אחד והוא $2 \cdot \mathbb{Z}/32\mathbb{Z}$ (זה קיצור לכתיב $(2+32\mathbb{Z}) \cdot \mathbb{Z}/32\mathbb{Z}$). בחוג $\mathbb{Z}/45\mathbb{Z}$ יש שני אידאלים מקסימליים והם $3 \cdot \mathbb{Z}/45\mathbb{Z}$ ו-$5 \cdot \mathbb{Z}/45\mathbb{Z}$.

דוגמה 4.7. בחוג חילוק אין אידאלים לא טריוויאלים, ולכן אידאל האפס הוא אידאל מקסימלי.

דוגמה 4.8. לכל מספר ראשוני p, האידאל $p\mathbb{Z} \lhd \mathbb{Z}$ הוא מקסימלי. האם יש עוד?

דוגמה 4.9. 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.

תרגיל 4.10. יהי $f \colon R \to S$ אפימורפיזם, ויהי $I \lhd R$ אידאל נאות המכיל את $\operatorname{Ker} f$. הוכיחו שגם $f(I) \lhd S$ אידאל נאות.

פתרון. נשאיר כתרגיל לבית ש-$f(I)$ הוא אידאל. נניח בשלילה ש-$I \lhd R$ אידאל נאות, אבל $f(I) = S$. נבחר איבר $x \in R \setminus I$, וקיים איבר $y \in I$ כך ש-$f(x) = f(y)$. נשים לב כי $x = y + (x-y)$, וגם ש-$x - y \in \operatorname{Ker} f \subseteq I$. לכן $x \in I$, וזו סתירה.

שימו לב שאם I אינו מכיל את הגרעין, אז הטענה לא נכונה. למשל $f \colon \mathbb{Z} \to \mathbb{Z}/2\mathbb{Z}$ עם גרעין $\operatorname{Ker} f = 2\mathbb{Z}$. נבחר $I = 3\mathbb{Z}$ שהוא אידאל נאות, וגם $f(3\mathbb{Z}) = \mathbb{Z}/2\mathbb{Z}$.

מסקנה 4.11. יהי $f\colon R \to S$ אפימורפיזם. אם $J \lhd S$ אידאל מקסימלי, אז גם $f^{-1}(J)$ מקסימלי.

הוכחה. נניח בשלילה שקיים אידאל $R \lhd I \subset f^{-1}(J)$. אז $\operatorname{Ker} f = f^{-1}(0) \subseteq f^{-1}(J)$, ולכן $\operatorname{Ker} f \subset I$. אז גם $f(I) \lhd S$ הוא אידאל נאות לפי התרגיל הקודם. אבל הוא מכיל ממש את J, כי פרט ל-$f^{-1}(J)$ הוא מכיל איברים נוספים שלפי הגדרה לא נשלחים ל-J. לכן קיבלנו סתירה למקסימליות של J.

שימו לב שהטענה לא נכונה ללא הדרישה לאפימורפיזם. למשל ההכלה $\varphi\colon \mathbb{Z} \to \mathbb{Q}$ מקיימת $\varphi^{-1}(\{0\}) = \{0\}$. האידאל $\{0\}$ הוא מקסימלי ב-$\mathbb{Q}$ כי מדובר בשדה, אבל לא ב-$\mathbb{Z}$. $\square$

משפט 4.12. 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 4.13. האידאל $\langle x, p\rangle \lhd \mathbb{Z}[x]$ הוא מקסימלי לכל מספר ראשוני p מפני שחוג המנה $\mathbb{Z}[x]/\langle x,p\rangle \cong \mathbb{F}_p$ 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-$\langle x,p\rangle$).

משפט 4.14 (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.

Correspondence theorem

4.1 אידאלים ראשוניים

הגדרה 4.15. אידאל נאות $I \lhd R$ יקרא ראשוני אם לכל $A, B \lhd R$ המקיימים $AB \subseteq I$, אז $A \subseteq I$ או $B \subseteq I$.

Prime

הערה 4.16. 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 $\{0\} \lhd M_2(D)$ 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 4.17. בחוג פשוט אידאל האפס הוא תמיד ראשוני.

תרגיל 4.18. 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-$I \lhd C(\mathbb{R})$. 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 4.19. יהי R חוג חילופי. אז R הוא תחום שלמות אם ורק אם $\{0\}$ הוא אידאל ראשוני.

מסקנה 4.20. יהי R חוג. אז $I \lhd R$ ראשוני אם ורק אם $\{0\}$ הוא ראשוני בחוג המנה R/I.

מסקנה 4.21. יהי R חוג חילופי. אז אידאל נאות $I \lhd R$ הוא ראשוני אם ורק אם R/I תחום שלמות.

דוגמה 4.22. האידאל $\langle x \rangle \lhd \mathbb{Z}[x]$ הוא ראשוני כי חוג המנה $\mathbb{Z}[x]/\langle x \rangle \cong \mathbb{Z}$ הוא תחום שלמות.

דוגמה 4.23. האידאל $\langle x \rangle \lhd (\mathbb{Z}/4\mathbb{Z})[x]$ אינו ראשוני, כי $(\mathbb{Z}/4\mathbb{Z})[x]/\langle x \rangle \cong \mathbb{Z}/4\mathbb{Z}$ אינו תחום שלמות. השוו לדוגמה 1.13.

תרגיל 4.24. יהי R חוג חילופי, ו-$I \lhd R$ אידאל נאות. הוכיחו כי I ראשוני אם ורק אם $R \setminus I$ סגורה לכפל.

פתרון. בכיוון הראשון I ראשוני, ונניח בשלילה כי $a, b \in R \setminus I$, אבל $ab \notin R \setminus I$. אזי $ab \in I$, ומהראשוניות של I נקבל $a \in I$ או $b \in I$. כלומר $a \notin R \setminus I$ או $b \notin R \setminus I$, שזו סתירה.

בכיוון השני נניח סגירות לכפל של $R \setminus I$. אם $ab \in I$ וגם $a, b \notin I$, אזי $a, b \in R \setminus I$. לכן גם $ab \in R \setminus I$ וזו סתירה.

תרגיל 4.25. יהי R חוג חילופי שבו כל האידאלים הם ראשוניים. הוכיחו כי R שדה.

פתרון. מן הנתון נקבל בפרט ש-$\{0\}$ אידאל ראשוני, ולכן R תחום שלמות. יהי $0 \neq x \in R$ ונראה שהוא הפיך. נתבונן באידאל $\langle x^2 \rangle$, 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 4.26. אם $I, J \lhd R$ ראשוניים, אז $I \cap J$ לא בהכרח ראשוני. למשל בחוג $\mathbb{Z}$ האידאלים $2\mathbb{Z}$, $3\mathbb{Z}$ הם ראשוניים, אבל חיתוכם $2\mathbb{Z} \cap 3\mathbb{Z} = 6\mathbb{Z}$ אינו ראשוני.

טענה 4.27. יהי R חוג חילופי. כל אידאל מקסימלי של R הוא ראשוני.

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

טענה 4.28 (לדלג). יהי R חוג. כל אידאל מקסימלי של R הוא ראשוני.

הוכחה. נניח בשלילה כי $I \lhd R$ מקסימלי ואינו ראשוני. כלומר קיימים $A, B \lhd R$ כך ש-$AB \subseteq I$, אבל $A, B \nsubseteq I$. 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 בסתירה למקסימליות. $\square$

מסקנה 4.29. בחוג בלי יחידה, אידאל מקסימלי $M \lhd R$ הוא לא ראשוני אם ורק אם $R^2 \subseteq M$.

דוגמה 4.30. בחוג בלי יחידה $R = 2\mathbb{Z}$ האידאל $I = 4\mathbb{Z}$ הוא מקסימלי, אבל הוא לא ראשוני, כי $R^2 \subseteq I$.

תרגיל 4.31. 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 $P \lhd R$ אידאל ראשוני, ויהי $M \lhd R$ 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 $P = M$.

למה 4.32 (למת ההתחמקות מראשוניים)**.** יהי R חוג חילופי, ויהיו $P_1, \dots P_n \lhd R$ אידאלים ראשוניים. אם אידאל $I \lhd R$ מוכל באיחוד $\bigcup_i P_i$, אז $I \subseteq P_j$ עבור $1 \leq j \leq n$ כלשהו.

Prime avoidance lemma

הוכחה. נוכיח את הגרסה השקולה, שאם I אינו מוכל באף אחד מ-P_i, אז הוא לא מוכל באיחוד $\bigcup_i P_i$. נעשה זאת על ידי מציאת איבר $a \in I$ שאינו שייך לאף P_i.

נתחיל במקרה $n = 2$. לפי ההנחה ישנם איברים $a_1 \in I \setminus P_2$, $a_2 \in I \setminus P_1$. אם $a_1 \notin P_1$ או $a_2 \notin P_2$, אז מצאנו איבר שאינו שייך ל-$P_1 \cup P_2$ וסיימנו. לכן נניח כי $a_i \in P_i$. לכן $a_1 + a_2 \in I$, אבל לא באף P_i. הרי אם $a_1 + a_2 \in P_1$ נקבל ש-$a_2 = (a_1 + a_2) - a_1 \in P_1$ שזו סתירה.

נמשיך באינדוקציה על n. לפי הנחת האינדוקציה, I אינו מוכל באף איחוד של $n - 1$ אידאלים מ-$P_1, \dots, P_n$. נבחר

$$a_i \in I \setminus \bigcup_{j \neq i} P_j$$

כמו מקודם, ונוכל להניח כי $a_i \in P_i$. ניקח את האיבר $a = a_1 a_2 \dots a_{n-1} + a_n$ ששייך ל-I, אך לא לאיחוד $\bigcup_i P_i$. הרי אם $a \in P_n$, אז $a_1 a_2 \dots a_{n-1} \in P_n$, ומפני ש-$P_n$ ראשוני נקבל $a_i \in P_n$ עבור $i \leq n-1$ כלשהו, וזו סתירה. אילו $a \in P_i$ עבור $i \leq n-1$, אז נקבל $a_n \in P_i$, שזו שוב סתירה. $\square$

הערה 4.33. ישנן גרסאות רבות של למת ההתחמקות מראשוניים. בגרסה מעט יותר חזקה נניח שנתונה תת־קבוצה $E \subseteq R$ הסגורה לחיבור וכפל, ואידאלים $I, J, P_1, \ldots, P_n \lhd R$ כאשר P_i ראשוניים. אם E אינה מוכלת באף אחד מן האידאלים האלו, אז היא לא מוכלת באיחודם.

5 תרגול חמישי

5.1 חוגים ראשוניים

הגדרה 5.1. חוג R נקרא ראשוני אם לכל שני אידאלים $A, B \lhd R$ המקיימים $AB = 0$, אז $A = 0$ או $B = 0$. Prime ring

באופן שקול, חוג הוא ראשוני אם המכפלה של כל שני אידאלים השונים מאפס, שונה מאפס.

משפט 5.2. R ראשוני אם ורק אם לכל $0 \neq a, b \in R$ קיים $0 \neq x \in R$ כך ש-$axb \neq 0$.

משפט 5.3. כל תחום הוא ראשוני.

משפט 5.4. חוג חילופי הוא ראשוני אם ורק אם הוא תחום שלמות.

תרגיל 5.5. יהי R חוג ראשוני. הראו שהמרכז $Z(R)$ הוא תחום שלמות.

פתרון. נעזר במשפט 5.4 מפני ש-$Z(R)$ חילופי. יהיו $A, B \lhd Z(R)$ כך ש-$AB = 0$. לכן $AR, BR \lhd R$ ומתקיים $ARBR = ABR = 0$. מהראשוניות 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.

תרגיל 5.6. 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

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

היא אפס, אך הם כמובן שונים מאפס.

תרגיל 5.7 (ממבחן)**.** חוג R נקרא ראשוני למחצה אם לא קיים אידאל $0 \neq I \lhd R$ כך ש-$I^2 = 0$. אידאל P בחוג כלשהו R נקרא ראשוני למחצה אם R/P הוא חוג ראשוני למחצה. Semiprime

1. הוכח כי כל אידאל ראשוני הוא אידאל ראשוני למחצה.
2. הוכח כי P ראשוני למחצה אם ורק אם לכל אידאל $I \lhd R$, אם $I^2 \subseteq P$, אז $I \subseteq P$.

פתרון. קל לראות שהסעיף השני גורר את הראשון. לכן נוכיח רק את הסעיף השני. תהי $\varphi\colon R \to R/P$ ההטלה הטבעית. נניח כי P ראשוני למחצה, ולכן R/P ראשוני למחצה. יהי $R \rhd I$ אידאל המקיים $I^2 \subseteq P$. נפעיל את φ, שהיא אפימורפיזם, ולכן $R/P \rhd \varphi(I)$ 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 $R/P \rhd I \neq 0$ כך ש-$I^2 = 0$. האידאל $R \rhd \varphi^{-1}(I)$ מקיים $(\varphi^{-1}(I))^2 \subseteq P$, אבל $\varphi^{-1}(I) \not\subseteq P$, וזו סתירה.

5.2 מיקום מרכזי

הגדרה 5.8. יהי R חוג ותהי $S \subseteq R$ תת־קבוצה המקיימת:

1. כל איברי S הם רגולריים (כלומר לא מחלקי אפס).
2. S סגורה לכפל.
3. $S \subseteq Z(R)$
4. $1 \in S$

במילים: S היא תת־מונואיד כפלי מרכזי של איברים רגולריים. נסמן ב-$S^{-1}R$ את קבוצת מחלקות השקילות של $S \times R$ תחת היחס

$$(s,r) \sim (s',r') \Leftrightarrow rs' = sr'$$

ונסמן את המחלקה של (s,r) ב-$\frac{r}{s}$. יחד עם פעולות הכפל "שמגיעות" מ-R הקבוצה $S^{-1}R$ הוא חוג הנקרא המיקום של R ב-S. Semiprime

הערה 5.9. יש מונומורפיזם טבעי $\iota\colon R \to S^{-1}R$ לפי $\iota(r) = \frac{r}{1}$. הוא שולח את איברי S לאיברים הפיכים. התכונה האוניברסלית של מיקום היא שאם $f\colon R \to T$ הוא הומומורפיזם של חוגים כך ש-$f(S) \subseteq T^\times$, אז קיים הומומורפיזם יחיד $g\colon S^{-1}R \to T$ כך ש-$f = g \circ \iota$.

הערה 5.10. בדרישות מתת־הקבוצה S, ניתן לוותר על הדרישות ש-S סגורה לכפל, ועל $1 \in S$, ואת המיקום היינו מגדירים ביחס לסגור הכפלי של S. מפני שלרוב נדבר על מיקום בחוגים חילופיים, אז גם הדרישה $S \subseteq Z(R)$ מתייתרת.

דוגמה 5.11. נבחר $R = \mathbb{Z}$, $S = \left\{3^k \,\middle|\, k \in \mathbb{N}\right\}$. אז $S^{-1}R = \mathbb{Z}\left[\frac{1}{3}\right]$. שימו לב שהומומורפיזם ההצבה $\varphi\colon \mathbb{Z}[x] \to \mathbb{Z}\left[\frac{1}{3}\right]$ שבו $x \mapsto \frac{1}{3}$ אינו חח"ע, מפני שהגרעין לא טריוויאלי. למשל $3x - 1 \mapsto 0$.

Local ring **הגדרה 5.12.** יהי R חוג חילופי. נאמר שהוא חוג מקומי אם יש לו אידאל מקסימלי יחיד.

דוגמה 5.13. יהי $p \in \mathbb{Z}$ ראשוני. אז $S = \mathbb{Z} \setminus p\mathbb{Z}$ סגורה לכפל והחוג $\mathbb{Z}_{\langle p \rangle} = S^{-1}\mathbb{Z}$ הוא חוג מקומי. האידאל המקסימלי היחיד שלו הוא $\mathfrak{m} = p\mathbb{Z}_{\langle p \rangle}$.

כדי לראות ש-$\mathfrak{m}$ מקסימלי, אפשר להוכיח $\mathbb{Z}_{\langle p \rangle}/\mathfrak{m} \cong \mathbb{Z}/p\mathbb{Z}$ וזה שדה (האיזומורפיזם לא לגמרי טריוויאלי). כאשר R הוא תחום שלמות, אז אפשר לחשוב על מיקום שלו $S^{-1}R$ כמשוכן בשדה השברים של R (ראו הגדרה 5.16). לכן יותר קל לחשוב על החוג בתור הקבוצה

$$\mathbb{Z}_{\langle p \rangle} = \left\{ \frac{a}{b} \in \mathbb{Q} \,\middle|\, p \nmid b \right\}$$
$$\mathfrak{m} = \left\{ \frac{a}{b} \in \mathbb{Q} \,\middle|\, p | a, p \nmid b \right\}$$

קל לראות ש-$\mathfrak{m}$ הוא האידאל המקסימלי היחיד, שכן כל האיברים ב-$\mathbb{Z}_{\langle p \rangle} \setminus \mathfrak{m}$ הם הפיכים.

דוגמה 5.14. החוג $\mathbb{Z}/p^k\mathbb{Z}$ עבור p ראשוני ו-k טבעי הוא חוג מקומי.

טענה 5.15 (מההרצאה). חוג הוא מקומי אם ורק אם קבוצת האיברים הלא הפיכים שלו היא אידאל.

הוכחה. נניח כי R הוא חוג מקומי עם אידאל מקסימלי $\mathfrak{m}$. יהי $x \in R \setminus \mathfrak{m}$. אז בהכרח x הפיך, שכן אחרת x יוצר אידאל $\langle x \rangle$ שמוכל באידאל מקסימלי ששונה מ-$\mathfrak{m}$.

בכיוון השני, נניח שקבוצת האיברים הלא הפיכים I היא אידאל. אז כל אידאל אחר של R חייב להיות מוכל ב-I, כי אידאלים לא מכילים איברים הפיכים. לכן I אידאל מקסימלי יחיד. □

הגדרה 5.16. יהי R תחום שלמות. עבור $S = R \setminus \{0\}$ המיקום $S^{-1}R$ הינו שדה, הנקרא שדה השברים של R.

Fraction field, or field of quotients

דוגמה 5.17. $\mathbb{Q}$ הוא שדה השברים של $\mathbb{Z}$.

דוגמה 5.18. יהי F שדה. שדה השברים של $F[x]$ הוא שדה הפונקציות הרציונליות

$$F(x) = \left\{ \frac{f(x)}{g(x)} \,\middle|\, f, g \in F[x], g \neq 0 \right\}$$

משפט 5.19. נסתכל על התאמות בין שתי קבוצות של אידאלים

$$\left\{ J \lhd S^{-1}R \right\} \quad \left\{ I \lhd R \,|\, I \cap S = \varnothing \right\}$$
$$S^{-1}I \mapsfrom I$$
$$J \mapsto J \cap R$$

1. ההתאמה $I \mapsto S^{-1}I$ היא על.
2. ההתאמה $J \mapsto J \cap R$ היא חח"ע.

3. הטענות האלו נכונות גם כאשר נגביל את הקבוצות רק לאידאלים ראשוניים.

הערה 5.20. יתכן מצב שבו $I_0 \in \{I \lhd R \,|\, I \cap S = \varnothing\}$ אינו ראשוני, אבל $S^{-1}I_0$ כן ראשוני ב-$S^{-1}R$. למשל, $6\mathbb{Z} \lhd \mathbb{Z}$ אינו ראשוני, וכאשר נבחר את $S = \left\{2^k \,\middle|\, k \in \mathbb{N}\right\}$, אז $S^{-1}(6\mathbb{Z}) = S^{-1}(3\mathbb{Z})$ הוא ראשוני ב-$S^{-1}\mathbb{Z}$.

הגדרה 5.21. יהי R תחום שלמות, ויהי $P \lhd R$ אידאל ראשוני. אז $S = R \setminus P$ סגורה לכפל. החוג $R_P = S^{-1}R$ נקרא המיקוס של R ב-P. זהו חוג מקומי שהאידאל המקסימלי שלו הוא $PR_P = S^{-1}P$.

דוגמה 5.22. $R = \mathbb{Z}$, $P = p\mathbb{Z}$ עבור p מספר ראשוני. מתקבל החוג המקומי $\mathbb{Z}_{\langle p \rangle}$.

דוגמה 5.23. יהי R_0 תחום שלמות. נסמן $R = R_0[x]$, $a \in R_0$, $P = \langle x - a \rangle$, $S = R \setminus P$. אז יתקבל החוג המקומי

$$S^{-1}R = R_0[x]_{\langle x-a \rangle} = \left\{ \frac{f}{g} \,\middle|\, g \notin \langle x - a \rangle \right\}$$

תרגיל 5.24. יהי R חוג חילופי, ויהיו $I, J \lhd R$ אידאלים. נסמן I_P, J_P עבור האידאלים המתאימים במיקום R_P, כאשר $P \lhd R$ אידאל ראשוני. הוכיחו שאם לכל אידאל ראשוני P מתקיים $I_P = J_P$, אז $I = J$.

פתרון. נראה זאת בעזרת הכלה דו־כיוונית. בה"כ נניח בשלילה כי $I \nsubseteq J$, כלומר שקיים $x \in I \setminus J$. נתבונן באידאל

$$(J : x) = \{r \in R \,|\, rx \in J\}$$

ודאו שאתם מבינים למה זה אידאל, ולמה הוא נאות אם J נאות. שימו לב כי $J \subseteq (J : x)$. יהי M האידאל המקסימלי שמכיל את $(J : x)$. לפי ההנחה $I_M = J_M$, ולכן $\frac{x}{1} \in J_M$. כלומר $\frac{x}{1} = \frac{j}{r}$ עבור $r \in R \setminus M, j \in J$. לכן $rx = j$, ונקבל $r \in (J : x) \subseteq M$. זו סתירה לכך ש-$r \in R \setminus M$.

תרגיל 5.25. יהי $\mathfrak{m}$ אידאל מקסימלי בחוג R. הוכיחו שעבור $n \in \mathbb{N}$ החוג $R/\mathfrak{m}^n$ הוא חוג מקומי עם אידאל מקסימלי $\mathfrak{m}/\mathfrak{m}^n$.

פתרון. לפי משפט ההתאמה, כל אידאל מקסימלי של $R/\mathfrak{m}^n$ הוא מן הצורה $I/\mathfrak{m}^n$ עבור אידאל מקסימלי $I \lhd R$ המכיל את $\mathfrak{m}^n$. יהי I כזה. מפני ש-I מקסימלי, אז הוא גם ראשוני. לכן מההנחה $\mathfrak{m}^n \subseteq I$ נקבל ש-$\mathfrak{m} \subseteq I$. אבל $\mathfrak{m}$ מקסימלי, ולכן $I = \mathfrak{m}$. כלומר אין אידאלים מקסימליים ב-$R/\mathfrak{m}^n$ פרט ל-$\mathfrak{m}/\mathfrak{m}^n$.

דוגמה 5.26. יהי F שדה. אז $\langle x \rangle \lhd F[x]$ אידאל מקסימלי (למה? כי המנה איזומורפית לשדה). לכן החוג $F[x]/\langle x^n \rangle$ הינו חוג מקומי לכל $n \in \mathbb{N}$, והאידאל המקסימלי שלו הוא $xF[x]/\langle x^n \rangle$.

תארו את החוגים המקומיים המגיעים מהאידאל המקסימלי $\langle x, y \rangle \lhd F[x, y]$.

תרגיל 5.27. יהי F שדה ממאפיין שונה מ-2. האם $F[x]/\left\langle x^2-1\right\rangle \cong F[x]/\left\langle x^2\right\rangle$?

פתרון. לא. נשים לב כי $\left\langle x^2-1\right\rangle = \langle x+1\rangle\langle x-1\rangle$. מכיוון ש-$(x+1)-(x-1)=2$ הינו הפיך, אז $\langle x+1\rangle+\langle x-1\rangle = F[x]$. כלומר אלו הם אידאלים קו-מקסימליים. לכן

$$\langle x+1\rangle\langle x-1\rangle = \langle x+1\rangle\cap\langle x-1\rangle$$

ונקבל

$$F[x]/\left\langle x^2-1\right\rangle \cong F[x]/\left(\langle x+1\rangle\cap\langle x-1\rangle\right)\cong F[x]/\langle x+1\rangle\times F[x]/\langle x-1\rangle\cong F\times F$$

שהוא בודאי לא חוג מקומי. הרי יש לו שני אידאלים מקסימליים שונים $F\times\{0\}$ ו-$\{0\}\times F$.

משפט 5.28 (מההרצאה)**.** יהי R חוג חילופי. התנאים הבאים שקולים:

1. R הוא חוג מקומי.
2. אוסף האיברים הלא הפיכים הוא אידאל.
3. לכל $a,b\in R$, אם $a+b=1$, אז a הפיך או b הפיך.

מסקנה 5.29. בחוג מקומי R לכל $x\in R$ מתקיים ש-x הפיך או $1-x$ הפיך.

מסקנה 5.30. בחוג מקומי אין אידמפוטנטים לא טריוויאלים.

הוכחה. נניח בשלילה $R \ni e\neq 0$ אידמפוטנט. אז $e=e^2$, לכן $e(1-e)=0$, ונקבל שגם e וגם $1-e$ לא הפיכים (כי הם מחלקי אפס). זו סתירה למסקנה הקודמת. $\square$

תרגיל 5.31 (לבית)**.** מצאו את האיברים ההפיכים ב-$F[x]/\langle x^n\rangle$.

6 תרגול שישי

6.1 חוגי טורים פורמליים

הגדרה 6.1. יהי R תחום. חוג טורי לורן הפורמליים $R((x))$ כולל את כל הסכומים האינסופיים הפורמליים $\sum_{i=-n}^{\infty}a_ix^i$ 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 $\sum_{i=0}^{\infty}a_ix^i$.

Formal Laurent series
Formal power series

דוגמה 6.2. בחוג $R[[x]]$ האיבר $1-x$ הוא הפיך (השוו למצב ב-$R[x]$), אבל x אינו הפיך. לכן $R[[x]]$ אינו שדה.

אם יש זמן, הנה עוד קצת על חוגי טורים פורמליים:

דוגמה 6.3. אם D הוא חוג חילוק, אז $D[[x]]$ הוא חוג ראשי. כל אידאל שם הוא מן הצורה $\langle x^n \rangle$ או $\{0\}$ (בחרו לפי דרגה מינימלית של איברים באידאל). למשל $\mathbb{H}[[x]]$ הוא חוג ראשי שאינו חילופי.

הגדרה 6.4. לאיברים של $R((x))$ אין דרגה מוגדרת, אך כן ניתן להגדיר הערכה, שהיא פונקציה $v\colon R((x)) \to \mathbb{Z} \cup \{\infty\}$ המוגדרת לפי Valuation

$$v(0) = \infty, \qquad v\left(\sum_{i=-n}^{\infty} a_i x^i\right) = \min\{i \mid a_i \neq 0\}$$

טענה 6.5. מתקיים $v(f+g) \geq \min\{v(f), v(g)\}$ וגם $v(f \cdot g) \geq v(f) + v(g)$. אם R הוא תחום, אז יש שיוויון $v(f \cdot g) = v(f) + v(g)$.

טענה 6.6. אם R תחום, אז $R((x))$ הוא תחום. אם F הוא שדה, אז $F((x))$ הוא שדה.

הוכחה. נראה רק הוכחה חלקית למקרה של שדה:

$$0 \neq f(x) = \sum_{i=-n}^{\infty} a_i x^i = x^{-n}\left(a_{-n} + a_{-n+1}x + \dots\right) = x^{-n} g(x)$$

כאשר $v(f) = -n$, והמקדם החופשי של $g(x)$ הוא $0 \neq a_{-n} \in F$. לכן $g(x)$ הפיך. בנוסף x^{-n} הפיך, ולכן $f(x)$ הפיך. $\square$

הערה 6.7. ניתן לחזור על הבניה של חוגי טורים פורמליים כמה פעמים. שימו לב שבעוד שבחוגי פולינומים מתקיים $F[x][y] = F[y][x]$ (למעשה החוגים איזומורפיים, אבל נתעלם מכך), בחוגי טורים דברים מסתבכים. למשל

$$F[x,y] \subsetneq F[[x]][y] \subsetneq F[y][[x]] \subsetneq F[[x]][[y]] \subsetneq F[[y]]((x)) \subsetneq F((x))[[y]] \subsetneq F((x))((y))$$

בנוסף החוג $F((x,y))$ הוא שדה השברים של $F[[x,y]]$, אבל $F((x,y)) \subsetneq F((x))((y))$. הסבר לכך אפשר למצוא בקישור הזה.

תרגיל 6.8. יהי R חוג חילופי. הוכיחו שכל אידאל ראשוני $P \lhd R$ הוא מן הצורה $R \cap Q$ עבור אידאל ראשוני $Q \lhd R[[x]]$.

פתרון. עבור P נבנה את $Q = \langle P, x \rangle$. אפשר לראות ש-Q הוא ראשוני לפי המנה

$$R[[x]]/Q \cong R/P$$

6.2 חוגי פולינומים מעל תחומי שלמות

עבור הפרק הזה יהי R הוא תחום שלמות, ויהיו $a, b \in R$ איברים.

הגדרה 6.9. נאמר ש-a מחלק את b, ונסמן $a|b$, אם קיים $k \in R$ כך ש-$ak = b$.

דוגמה 6.10. ב-$\mathbb{Z}$ מתקיים $2|4$, אבל $3 \nmid 4$. לעומת זאת $3|4$ ב-$\mathbb{Q}$.

דוגמה 6.11. יהי F שדה. נתבונן בתת־החוג $S \subseteq F[x]$ של הפולינומים שהמקדם של x הוא 0 (כלומר האיברים בו הם פולינומים מן הצורה $a_n x^n + \dots + a_2 x^2 + a_0$. הוכיחו שזה חוג). שם $x^2 \nmid x^3$, אבל $x^2 | x^3$ ב-$F[x]$.