מבוא לחוגים ומודולים
מערכי תרגול קורס 88-212

אפריל 2018, גרסה 1.6

אוניברסיטת בר-אילן סמסטר ב׳ תשע״ח

תוכן העניינים

מבוא . . . 3
1 תרגול ראשון . . . 4
2 תרגול שני . . . 7
3 תרגול שלישי . . . 12
4 תרגול רביעי . . . 15
5 תרגול חמישי . . . 20
6 תרגול שישי . . . 25
7 תרגול שביעי . . . 28
8 תרגול שמיני . . . 33
9 תרגול תשיעי . . . 37
10 תרגול עשירי . . . 40
11 תרגול אחת עשר . . . 44
12 תרגול שניים עשר . . . 50

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.
- יתקיים בוחן בערך באמצע הסמסטר.
- 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. This font נוסיף בצד גם את השם באנגלית, שעשוי לעזור כשמחפשים חומר נוסף שאינו בעברית.
- נשמח לכל הערה על מסמך זה.

מחבר בתשע"ז ותשע"ח: 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:

1. Commutative — R הוא חילופי אם $(R,\cdot)$ היא חבורה למחצה חילופית.
2. Ring, Unital ring — R הוא חוג (או חוג עם יחיזה כשהבדל חשוב), אם $(R,\cdot)$ מונואיד. איבר היחידה של המונואיד נקרא גם היחידה של החוג.
3. Division ring — R הוא חוג חילוק אם $(R\setminus\{0\},\cdot)$ חבורה.
4. Field — 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 3.1.
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 $V = F^{\mathbb{N}} = \{(x_1, x_2, \dots) \,|\, x_i \in F\}$, ונתבונן בשני העתקות

$$D\left((x_1, x_2, \dots)\right) = (x_2, x_3, \dots)$$
$$U\left((x_1, x_2, \dots)\right) = (0, x_1, x_2, \dots)$$

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

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

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

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.

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

Subring
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.

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 1.15. 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 בלי יחידה 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

$$aba - aca = a(ba - ca) = a(b - c)a \in aRa$$
$$aba \cdot aca = a(baac)a \in aRa$$

Idempotent

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

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

Center

הגדרה 1.19. יהי R חוג. המֶרְכָּז של R הוא

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

Centralizer

המְרַכֵּז של תת־קבוצה $R \supseteq S$ הוא

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

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 $C_R(S') \subseteq C_R(S)$).

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.

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. (Epimorphism, Projection)

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 עדיין חוג עם יחידה. □

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:

1. התמונה של φ היא $\operatorname{Im}\varphi = \{\varphi(x) \mid x \in R\}$, והיא תת־חוג של S. (Image)
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 $1_R \notin \operatorname{Ker}\varphi$. (Kernel)
3. אם $R = S$, נקרא ל-φ אנדומורפיזם. אם בנוסף φ הוא איזומורפיזם, אז הוא נקרא אוטומורפיזם. (Endomorphism, Automorphism)

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

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 $I \leq R$. (Left ideal)
2. נאמר כי I הוא אידאל ימני של R אם 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 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 $Ra = \{ra \mid r \in R\}$ היא אידאל שמאלי. קל לבדוק שהיא תת־חבורה חיבורית. בנוסף 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

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

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.

הגדרה 2.22. 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.

הערה 2.23. 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 $\langle x \rangle = Rx = xR$.

3 תרגול שלישי

דוגמה 3.1. 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 $Z(\mathbb{H})=\operatorname{Span}_{\mathbb{R}}\{1\}\cong\mathbb{R}$.

תרגיל 3.2. 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 3.3. אידאל נאות אף פעם לא מכיל את איבר היחידה של החוג. אף יותר, אידאל נאות לא מכיל איברים הפיכים כלל.

מסקנה 3.4. בחוג חילוק כל האידאלים הם טריוויאלים.

דוגמה 3.5. יהי $\mathbb{H}$ חוג הקווטרניונים הממשיים שפגשנו בדוגמה 3.1. אפשר לחשב כי

$$Z(\mathbb{H})=\left\{\begin{pmatrix} r & 0 \\ 0 & r\end{pmatrix}\middle|\, r\in\mathbb{R}\right\}\cong\mathbb{R}$$

וקל לראות שמדובר בתת־חוג, וגם שישנה הטלה $\varphi\colon\mathbb{H}\to Z(\mathbb{H})$, אבל עדין לא מדובר באידאל של $\mathbb{H}$! הרי לפי המסקנה האחרונה, בחוג חילוק אין אידאלים לא טריוויאלים.

תרגיל 3.6. 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 3.7. 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.

Sum of ideals

הגדרה 3.8. יהיו I, J אידאלים. נגדיר את סכום האידאלים האלו לפי

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

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

דוגמה 3.9. 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 3.10. אוסף האידאלים של חוג עם יחס ההכלה הוא סריג מודולרי מלא, שבו $I \vee J = I + J$, $I \wedge J = I \cap J$.

הגדרה 3.11. למשפחה Λ של אידאלים נגדיר את הסכום $\sum_{L\in\Lambda} L$ להיות אוסף הסכומים הסופיים $x_1 + \cdots + x_n$ עבור $x_i \in L_i \in \Lambda$.

הערה 3.12. 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.

לאיברים $x_1, \ldots, x_k \in R$ נסמן בקיצור

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

דוגמה 3.13. 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 3.14. 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:

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

Product of ideals

הגדרה 3.15. 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 3.16. לכל זוג אידאלים I, J מתקיים $IJ \subseteq I \cap J$.

דוגמה 3.17. 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

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

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 $f_1g_1 = 1$ (כי הם קבועים) וגם $f_2g_2 = 1$ (קצת יותר קשה להבין למה המעלה שלהם צריכה להיות אפס). לכן $f_1 = g_1 = \pm 1$, $f_2 = g_2 = \pm 1$. אבל אז לא יתכן כי

$$2f_1g_2 + 3f_2g_1 = 0$$

במקרה שלנו מכפלת האידאלים היא $IJ = \langle 6, x\rangle$. נסו להראות כי x אינו יכול להכתב בצורה $x = f \cdot g$ כאשר $f \in I$ ו-$g \in J$.

הגדרה 3.18. יהי R חוג, ויהיו $I, J \lhd R$. נאמר כי I, J הם קו־מקסימליים אם $I + J = R$. Comaximal ideals

תרגיל 3.19. יהי R חוג חילופי. הוכיחו שאם I, J קו־מקסימליים, אז $IJ = I \cap J$.

פתרון. ראינו בהערה 3.16 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 3.20. 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

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

הגדרה 3.21. 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

Principal ideal domain (PID)

דוגמה 3.22. $\mathbb{Z}$ הוא תחום ראשי. האידאלים שלו הם מן הצורה $m\mathbb{Z}$.

תרגיל 3.23. 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 3.24. 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 3.25 (לבית). הוכיחו שבחוג $\mathbb{Q}[x,y]$ האידאל $\langle x,y\rangle$ אינו ראשי.

טענה 3.26. 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.

4 תרגול רביעי

דוגמה 4.1. חוג R יקרא פשוט אם אין לו אידאלים פרט ל-R ול-$\{0\}$.

Simple

דוגמה 4.2. חוג חילוק הוא פשוט. האם ההפך נכון?

תרגיל 4.3. 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 4.4. 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 4.5. יהי $I \lhd R$. אז $M_n(I) \lhd M_n(R)$ וכל אידאל של $M_n(R)$ הוא מן הצורה הזו.

דוגמה 4.6. $M_n(2\mathbb{Z}) \lhd M_n(\mathbb{Z})$.

הערה 4.7. 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 $Z(M_n(D)) = \{d \cdot I_n \,|\, d \in Z(D)\}$.

תרגיל 4.8. יהי $A \subseteq M_n(R)$ 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 4.9. 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 4.10. 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 $\varphi(a) = a$. התמונה של $\mathbb{Z}$ תחת φ היא $\mathbb{Z}$, וזה לא אידאל של $\mathbb{Q}$, כי האידאלים היחידים שלו הם טריוויאלים.

הגדרה 4.11. יהי R חוג, ויהי $I \lhd R$ אידאל. חוג המנה הוא הקבוצה Quotient ring

$$R/I = \{a + I \,|\, a \in R\}$$

עם פעולות החיבור $(a+I)+(b+I) = (a+b)+I$ והכפל $(a+I)(b+I) = ab+I$. איבר האפס הוא $0_R + I = I$ ואיבר היחידה הוא $1_R + I$.

דוגמה 4.12. $R = 3\mathbb{Z}$, $I = 18\mathbb{Z}$. 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 $\mathbb{Z}/6\mathbb{Z}$ (יש איזומורפיזם של חבורות $R/I \cong \mathbb{Z}/6\mathbb{Z}$). לפי טבלת הכפל נראה שכחוגים החוג 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 4.13. 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 4.14. 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 $\pm\overline{x}$ או $\pm\overline{1}$, כשמתקיים $\overline{x}\cdot\overline{x} = \overline{-1}$. לבית: הוכיחו $R/I \cong \mathbb{C}$.

תרגיל 4.15. 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 4.16. איבר $x \in R$ הוא נילפוטנטי אם קיים $n \in \mathbb{N}$ כך ש-$x^n = 0$. Nilpotent

תרגיל 4.17. 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.

First isomorphism theorem

משפט 4.18 (משפט האיזומורפיזם הראשון)**.** יהי $f\colon R \to S$ הומומורפיזם, אז

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

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

דוגמה 4.19. 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.

Subring generated by X

הגדרה 4.20. 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 4.21. $R_0[X]$ הוא תת־החוג הקטן ביותר (ביחס להכלה) של R המכיל את R_0 ואת X.

הערה 4.22. אם $a \in Z(R)$, אז $R_0[a]$ הוא אוסף הפולינומים ב-a עם מקדמים מ-R_0.

דוגמה 4.23. $R = \mathbb{Z}$ נוצר סופית מעל כל תת־חוג $R_0 = n\mathbb{Z}$ עבור $n \neq 0$, כי $R_0[1] = \mathbb{Z}$.

דוגמה 4.24. יהי $S = R[x_1, \dots, x_n]$ חוג פולינומים ב-n-משתנים מעל R. אז S נוצר סופית מעל R עבור $X = \{x_1, \dots, x_n\}$.

תרגיל 4.25. 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.

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

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

הערה 4.26. 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 4.27. 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 4.28. 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 4.29. 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 4.30. 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 $S \cong \mathbb{C}[t]$, $R \cong \mathbb{C}[t, t^{-1}]$ לפי הגדרת 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 $\mathbb{C}[t] \ncong \mathbb{C}[t,t^{-1}]$. 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.

5 תרגול חמישי

Second isomorphism theorem

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

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

דוגמה 5.2. 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 5.3. 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.

Third isomorphism theorem

משפט 5.4 (משפט האיזומורפיזם השלישי). יהיו $I \subseteq J$ אידאלים של חוג R. אז

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

Chinese remainder theorem

משפט 5.5 (משפט השאריות הסיני). יהיו $I_1, \dots I_n \lhd R$ אידאלים קו־מקסימליים בזוגות. אז קיים איזומורפיזם

$$R/_{(I_1\cap\cdots\cap I_n)} \cong R/_{I_1} \times \cdots \times R/_{I_n}$$

דוגמה 5.6. נבחר $R = \mathbb{Z}_3[x]$. נראה למה איזומורפי חוג המנה $R/_{\langle x^2-x\rangle}$.

נשים לב כי $x^2 - x = x(x-1)$. האידאלים $\langle x\rangle$ ו-$\langle x-1\rangle$ הם קו־מקסימליים כי $x \in \langle x\rangle$ ו-$-(x-1) \in \langle x-1\rangle$ ולכן

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

לכן לפי תרגיל שעשינו $\langle x-1\rangle \cap \langle x\rangle = \langle x-1\rangle \cdot \langle x\rangle$. ממשפט השאריות הסיני נקבל

$$R/\langle x^2-x\rangle = R/\langle x\rangle \times R/\langle x-1\rangle$$

אם נשתמש בהומומורפיזם ההצבה, נקבל $R/\langle x\rangle \cong R/\langle x-1\rangle \cong \mathbb{Z}_3$, ולכן חוג המנה שלנו איזומורפי לחוג $\mathbb{Z}_3 \times \mathbb{Z}_3$.

משפט 5.7 (משפט השאריות הסיני לשלמים). תהא $\{m_1, \ldots, m_k\}$ קבוצת מספרים טבעיים הזרים בזוגות (כלומר כל זוג מספרים בקבוצה הוא זר). נסמן את מכפלתם ב-m. בהנתן קבוצה כלשהי של שאריות $\{a_i \pmod{m_i} \mid 1 \le i \le k\}$, קיימת שארית יחידה x מודולו m המהווה פתרון למערכת המשוואות

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ \vdots \\ x \equiv a_k \pmod{m_k} \end{cases}$$

הוכחה חלקית. נראה שקיים פתרון עבור זוג מספרים. מפני ש-$(m_1, m_2) = 1$, אזי קיימים $s, t \in \mathbb{Z}$ כך ש-$sm_1 + tm_2 = 1$. נתבונן במספר $x = bsm_1 + atm_2$ המקיים

$$\begin{aligned} bsm_1 + atm_2 \equiv atm_2 \equiv a \cdot 1 \equiv a \pmod{m_1} \\ bsm_1 + atm_2 \equiv bsm_1 \equiv b \cdot 1 \equiv b \pmod{m_2} \end{aligned}$$

ולכן x הוא פתרון אפשרי. ברור כי גם $x' = x + nm_1m_2$ לכל $n \in \mathbb{Z}$ הוא פתרון תקף.
להוכחת היחידות מודולו m_1m_2, נניח שגם y הוא פתרון. אז $m_1 | x-y$ וגם $m_2 | x-y$.
מהנתון $(m_1, m_2) = 1$ נקבל כי $m_1m_2 | x-y$ ולכן $x \equiv y \pmod{m_1m_2}$. □

הערה 5.8. עם הסימונים כמו קודם, ניסוח אחר של המשפט הוא שקיים איזומורפיזם של חוגים

$$\mathbb{Z}_m \cong \mathbb{Z}_{m_1} \times \cdots \times \mathbb{Z}_{m_k}$$

דוגמה 5.9. נמצא $x \in \mathbb{Z}$ כך ש-$x \equiv 1 \pmod 3$ וגם $x \equiv 2 \pmod 5$. ידוע כי $(5,3) = 1$, ולכן $-1 \cdot 5 + 2 \cdot 3 = 1$. במקרה זה $m_1 = 5, m_2 = 3$ וכן $s = -1, t = 2$, ולפי משפט השאריות הסיני אפשר לבחור את $x = 1 \cdot (-5) + 2 \cdot 6 = 7$. אכן מתקיים $7 \equiv 1 \pmod 3$ וגם $7 \equiv 2 \pmod 5$.

דוגמה 5.10. נמצא $y \in \mathbb{Z}$ כך ש-ש-$y \equiv 1 \pmod 3$, $y \equiv 2 \pmod 5$ וגם $y \equiv 3 \pmod 7$. נשים לב שהפתרון $y = 7$ מן הדוגמה הקודמת הוא נכון כדי כדי הוספה של $3 \cdot 5 = 15$ (כי $15 \equiv 0 \pmod 3$ וגם $15 \equiv 0 \pmod 5$). לכן את שתי המשוואות $y \equiv 1 \pmod 3$, $y \equiv 2 \pmod 5$ ניתן להחליף במשוואה אחת $y \equiv 7 \pmod{15}$.
נשים לב כי $(15, 7) = 1$ ולכן אפשר להשתמש במשפט השאריות הסיני בגרסה לזוג משוואות. בדקו כי $y = 52$ מהווה פתרון.

5.1 אידאלים מקסימליים

הגדרה 5.11. אידאל נאות $R \lhd I$ נקרא אידאל מקסימלי אם לא קיים אידאל נאות שמכיל אותו ממש. Maximal ideal

דוגמה 5.12. 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 5.13. בחוג חילוק אין אידאלים לא טריוויאלים, ולכן אידאל האפס הוא אידאל מקסימלי.

דוגמה 5.14. לכל מספר ראשוני p, האידאל $\mathbb{Z} \lhd p\mathbb{Z}$ הוא מקסימלי. האם יש עוד?

דוגמה 5.15. עבור חוג חילופי R, האידאל $R[x,y] \lhd \langle x \rangle$ אינו מקסימלי. למשל כי האידאל הנאות $J = \{f(x,y) \mid f(0,0) = 0\}$ מכיל אותו ממש.

תרגיל 5.16. יהי $f\colon R \to S$ אפימורפיזם, ויהי $R \lhd I$ אידאל נאות המכיל את $\operatorname{Ker} f$. הוכיחו שגם $S \lhd f(I)$ אידאל נאות.

פתרון. נשאיר כתרגיל לבית ש-$f(I)$ הוא אידאל. נניח בשלילה ש-$R \lhd I$ אידאל נאות, אבל $S = f(I)$. נבחר איבר $x \in R \setminus I$, וקיים איבר $y \in I$ כך ש-$f(y) = f(x)$. 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 5.17. יהי $f\colon R \to S$ אפימורפיזם. אם $S \lhd J$ 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 $S \lhd f(I)$ 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 5.18. יהי R חוג. אידאל נאות $R \lhd I$ הוא מקסימלי אם ורק אם R/I הוא פשוט. אם בנוסף R חילופי, אז I מקסימלי אם ורק אם R/I שדה.

דוגמה 5.19. האידאל $\mathbb{Z}[x] \lhd \langle x,p \rangle$ 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 5.20 (משפט ההתאמה). יהי $R \lhd I$ 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

5.2 אידאלים ראשוניים

הגדרה 5.21. 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

דוגמה 5.22. בחוג פשוט אידאל האפס הוא תמיד ראשוני.

הערה 5.23. עבור חוגים חילופיים ההגדרה לראשוניות גוררת את התנאי היותר חזק שלכל $a, b \in R$ המקיימים $ab \in I$, אז $a \in I$ או $b \in I$. במקרה כזה האידאל נקרא ראשוני לחלוטין. Completly prime

בחוגים לא חילופיים, אידאל יכול להיות ראשוני מבלי להיות ראשוני לחלוטין. למשל, יהי D חוג חילוק 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.

תרגיל 5.24. 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 5.25. יהי R חוג חילופי. אז R הוא תחום שלמות אם ורק אם $\{0\}$ הוא אידאל ראשוני.

מסקנה 5.26. יהי R חוג. אז $I \lhd R$ ראשוני אם ורק אם $\{0\}$ הוא ראשוני בחוג המנה R/I.

מסקנה 5.27. יהי R חוג חילופי. אז אידאל נאות $I \lhd R$ הוא ראשוני אם ורק אם R/I תחום שלמות.

דוגמה 5.28. 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 5.29. 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 5.30. 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 $R\backslash I$. אם $ab\in I$ וגם $a,b\notin I$, אזי $a,b\in R\backslash I$. לכן גם $ab\in R\setminus I$ וזו סתירה.

בגרסה לחוגים לא חילופיים, האידאל I ראשוני אם ורק אם $R\setminus I$ מקיימת את התנאי הבא: לכל $a,b\in R\setminus I$ קיים $r\in R$ כך ש-$arb\in R\setminus I$.

תרגיל 5.31. 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 5.32. 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 5.33. 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. □

טענה 5.34 (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. □

מסקנה 5.35. בחוג בלי יחידה, אידאל מקסימלי $M\lhd R$ הוא לא ראשוני אם ורק אם $R^2\subseteq M$.

דוגמה 5.36. בחוג בלי יחידה $R=2\mathbb{Z}$ האידאל $I=4\mathbb{Z}$ הוא מקסימלי, אבל הוא לא ראשוני, כי $R^2\subseteq I$.

תרגיל 5.37. 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 5.38 (למת ההתחמקות מראשוניים)**.** יהי R חוג חילופי, ויהיו $P_1, \ldots P_n \lhd R$ אידאלים ראשוניים. אם אידאל $I \lhd R$ מוכל באיחוד $\bigcup_i P_i$, אז $I \subseteq P_j$ עבור $1 \le j \le n$ 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-$P_1, \ldots, P_n$. 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 $a = a_1 a_2 \ldots a_{n-1} + a_n$ ששייך ל-I, אך לא לאיחוד $\bigcup_i P_i$. הרי אם $a \in P_n$, אז $a_1 a_2 \ldots a_{n-1} \in P_n$, ומפני ש-$P_n$ ראשוני נקבל $a_i \in P_n$ עבור $i \le n-1$ כלשהו, וזו סתירה. אילו $a \in P_i$ עבור $i \le n-1$, אז נקבל $a_n \in P_i$, שזו שוב סתירה. □

הערה 5.39. 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.

6 תרגול שישי

6.1 חוגים ראשוניים

הגדרה 6.1. 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 6.2. R ראשוני אם ורק אם לכל $0 \neq a, b \in R$ קיים $x \in R$ כך ש-$axb \neq 0$.

משפט 6.3. כל תחום הוא ראשוני.

משפט 6.4. חוג חילופי הוא ראשוני אם ורק אם הוא תחום שלמות.

תרגיל 6.5. יהי R חוג ראשוני. הראו שהמרכז $Z(R)$ הוא תחום שלמות.

פתרון. נעזר במשפט 6.4 מפני ש-$Z(R)$ חילופי. יהיו $A, B \lhd Z(R)$ כך ש-$AB = 0$. לכן $R \lhd AR, BR$ 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 6.6. 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

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

היא אפס, אך הם כמובן שונים מאפס.

6.2 מיקום מרכזי

הגדרה 6.7. 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-$\frac{r}{s}$. הקבוצה $S^{-1}R$, יחד עם פעולות הכפל והחיבור "שמגיעות" כשברים מ-R, הוא חוג הנקרא המיקום של R ב-S. Localization

הערה 6.8. 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 6.9. 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 6.10. 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 6.11. יהי R חוג חילופי. נאמר שהוא חוג מקומי אם יש לו אידאל מקסימלי יחיד.

דוגמה 6.12. 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 6.15). 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 6.13. החוג $\mathbb{Z}/p^k\mathbb{Z}$ עבור p ראשוני ו-k טבעי הוא חוג מקומי.

טענה 6.14 (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. □

Fraction field, or field of quotients

הגדרה 6.15. יהי R תחום שלמות. עבור $S=R\setminus\{0\}$ המיקום $S^{-1}R$ הינו שדה, הנקרא שדה השברים של R.

דוגמה 6.16. $\mathbb{Q}$ הוא שדה השברים של $\mathbb{Z}$.

דוגמה 6.17. 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 6.18. נסתכל על התאמות בין שתי קבוצות של אידאלים

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

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 6.19. 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 6.20. 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 6.21. $R = \mathbb{Z}$, $P = p\mathbb{Z}$ עבור p מספר ראשוני. מתקבל החוג המקומי $\mathbb{Z}_{\langle p \rangle}$.

דוגמה 6.22. 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 6.23. 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-$r \in R \setminus M$, ולכן $I \subseteq J$.
שימו לב שאפשר להסתפק בכך שהתנאי $I_P = J_P$ נכון רק לאידאלים מקסימליים.

7 תרגול שביעי

משפט 7.1 (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 7.2. בחוג מקומי R לכל $x\in R$ מתקיים ש-x הפיך או $x-1$ הפיך.

מסקנה 7.3. 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 7.4. 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 7.5. 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 7.6. יהי F שדה ממאפיין שונה מ-2. האם $F[x]/\langle x^2\rangle\cong F[x]/\langle x^2-1\rangle$?

פתרון. לא. נשים לב כי $\langle x^2-1\rangle=\langle x+1\rangle\langle x-1\rangle$. מכיוון ש-$2=(x+1)-(x-1)$ הינו הפיך, אז $F[x]=\langle x-1\rangle+\langle x+1\rangle$. 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-$\{0\}\times F$.

תרגיל 7.7 (לבית). מצאו את האיברים ההפיכים ב-$F[x]/\langle x^n\rangle$.

7.1 חוגי טורים פורמליים

הגדרה 7.8. 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 $\sum_{i=0}^{\infty}a_ix^i$. כקבוצה, טורי חזקות פורמליים הם $R^{\mathbb{N}}$, אבל כחוג פעולת הכפל היא לא רכיב־רכיב!

Formal Laurent series

Formal power series

דוגמה 7.9. 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 7.10. 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 7.11. 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

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

טענה 7.12. 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 7.13. 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 $F \ni a_{-n} \neq 0$. לכן $g(x)$ הפיך. בנוסף x^{-n} הפיך, ולכן $f(x)$ הפיך. $\square$

הערה 7.14. 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 7.15. יהי R חוג חילופי. הוכיחו שכל אידאל ראשוני $R \lhd P$ 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

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

7.2 חוגי פולינומים מעל תחומי שלמות

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

הגדרה 7.16. נאמר ש-a מחלק את b, ונסמן $a|b$, אם קיים $k \in R$ כך ש-$ak = b$.

Divides

דוגמה 7.17. ב-$\mathbb{Z}$ מתקיים $2|4$, אבל $4 \nmid 3$. לעומת זאת $3|4$ ב-$\mathbb{Q}$.

דוגמה 7.18. יהי F שדה. נתבונן בתת־החוג $S \subseteq F[x]$ של הפולינומים שהמקדם של x הוא 0 (כלומר האיברים בו הם פולינומים מן הצורה $a_n x^n + \cdots + a_2 x^2 + a_0$. הוכיחו שזה חוג). שם $x^2 \nmid x^3$, אבל $x^2 | x^3$ ב-$F[x]$.

הערה 7.19. יש קשר הדוק בין יחס החלוקה לאידאלים: $a|b$ אם ורק אם $Rb \subseteq Ra$, שכן $ak = b$.

הגדרה 7.20. יהיו $a, b \in R$. אם $a|b$ וגם $b|a$, נאמר כי a ו-b חברים ונסמן זאת $a \sim b$. ודאו שאתם יודעים להוכיח שיחס החברות הוא יחס שקילות.

Equivalent up to multiplication by a unit

כמה תכונות של יחס זה:

1. מתקיים $a \sim b$ אם ורק אם $Ra = Rb$.
2. נניח $a, b \in R \setminus \{0\}$. אז $a \sim b$ אם ורק אם קיים $u \in R^\times$ כך ש-$a = bu$. למה? שהרי $ak = b$ וגם $bm = a$, נציב ונקבל $bmk = b$. אז $b(1 - mk) = 0$ וכיוון ש-R תחום שלמות ו-$b \neq 0$, אז $mk = 1$. כעת אפשר לבחור $u = m \in R^\times$.
3. בפרט, $a \sim 1$ אם ורק אם a הפיך אם ורק אם $Ra = R$.

תרגיל 7.21. מצאו את ההפיכים בחוגים $\mathbb{Z}$, $\mathbb{Z}[i]$, $F[x]$.

פתרון. בחוג $\mathbb{Z}$ רק $\{-1, 1\}$ הפיכים. בחוג $F[x]$ לפי תרגיל שעשינו $(F[x])^\times = F^\times = F \setminus \{0\}$.

עבור $\mathbb{Z}[i]$ נתבונן בנורמה $N \colon \mathbb{Z}[i] \to \mathbb{N} \cup \{0\}$ של האיבר $a + bi$ המוגדרת לפי

$$N(a + bi) = (a + bi)(a - bi) = a^2 + b^2$$

זהו צמצום של הנורמה מ-$\mathbb{C}$ אל תת־החוג $\mathbb{Z}[i]$. לכן זו פונקציה כפלית. כלומר $N(\alpha\beta) = N(\alpha)N(\beta)$. יהיו $\alpha, \beta \in \mathbb{Z}[i]$ הפיכים כך ש-$\alpha\beta = 1$. לכן $N(\alpha\beta) = 1 = N(1)$. כיוון שהנורמה בחוג הזה מקבלת רק מספרים שלמים לא שליליים, נקבל $N(\alpha) = N(\beta) = 1$. נניח $\alpha = a + bi$. הפתרונות היחידים למשוואה $N(\alpha) = a^2 + b^2 = 1$ הם

$$(a = 0, b = \pm 1) \vee (a = \pm, b = 0)$$

כלומר האיברים ההפיכים בחוג $\mathbb{Z}[i]$ הם רק $\pm 1, \pm i$.

הגדרה 7.22. יהי $D \in \mathbb{Z}$ חופשי מריבועים. עבור השדה $\mathbb{Q}[\sqrt{D}] = \left\{ a + b\sqrt{D} \,\middle|\, a, b \in \mathbb{Q} \right\}$ נגדיר את חוג השלמים שלו להיות

Ring of integers

$$\mathcal{O}_D = \begin{cases} \mathbb{Z}[\sqrt{D}], & D \equiv 2, 3 \pmod 4 \\ \mathbb{Z}[\frac{1+\sqrt{D}}{2}], & D \equiv 1 \pmod 4 \end{cases}$$

Norm

הגדרה 7.23. יהי $D \in \mathbb{Z}$ חופשי מריבועים. נגדיר לכל איבר $\alpha = a + b\sqrt{D}$ את הנורמה $N \colon \mathcal{O}_D \to \mathbb{Z}$ לפי

$$N(\alpha) = \alpha\overline{\alpha} = \left(a + b\sqrt{D}\right)\left(a - b\sqrt{D}\right)$$

שימו לב שהאינוולוציה $\overline{\alpha}$ היא לא בהכרח הצמוד המרוכב. כמה מן התכונות השימושיות של נורמה: $N(xy) = N(x)N(y)$, $N(x) = 0$ אם ורק אם $x = 0$.

Pell's equation

הערה 7.24. משוואת פל היא כל משוואה דיופנטית מן הצורה

$$x^2 - Dy^2 = 1$$

כאשר D שלם לא ריבועי. לגראנז' הוכיח שכאשר D טבעי ואינו ריבוע, למשוואה יש אינסוף פתרונות שלמים. מה הקשר לנורמה בחוגי שלמים ריבועיים? מה הקשר לפיתוח $\sqrt{D}$ כשבר משולב?

בעיה 7.25 (משפט דיריכלה לשדות ריבועיים עם דיסקרימיננטה חיובית)**.** יהי $D > 0$ חופשי מריבועים. אז קיים $\alpha_0 \in \mathcal{O}_D$ כך שכל איבר הפיך הוא מן הצורה $\pm\alpha_0^n$ עבור $n \in \mathbb{Z}$. הדרכה להוכחה:

1. יהיו $\alpha = a + b\sqrt{D}$, $\alpha' = a' + b'\sqrt{D}$ פתרונות למשוואת פל. הוכיחו שגם

$$\alpha\alpha' = (aa' + Dbb') + (ab' + a'b)\sqrt{D}$$

הוא פתרון למשוואת פל. הסיקו שאוסף הפתרונות למשוואת פל הוא תת־חבורה של $\mathcal{O}_D^\times$.

2. נאמר כי $\alpha > 0$ אם $a > 0$ וגם $b > 0$.
הראו שאם $\alpha, \alpha' > 0$, אז גם $\alpha\alpha', \alpha + \alpha' > 0$.

3. הניחו כי $\alpha, \alpha' > 0$ הפיכים. נאמר כי $\alpha > \alpha'$ אם $\alpha - \alpha' > 0$.
הוכיחו ש-$a > a'$ אם ורק אם $b > b'$ אם ורק אם $\alpha > \alpha'$.

4. הניחו $\alpha > \alpha' > 0$ פתרונות למשוואת פל. הוכיחו כי $\alpha' > \alpha'\alpha^{-1} > 0$.

5. הוכיחו שקיים $\alpha_0 \in \mathcal{O}_D$ כך שכל פתרון למשוואת פל הוא מן הצורה α_0^n עבור $n \in \mathbb{Z}$. רמז: בחרו $\alpha_0 > 0$ מינימלי, והניחו בדרך השלילה שקיים פתרון $\beta > 0$ שאינו חזקה של α_0.

6. סיימו את הוכחת משפט דיריכלה לשדות ריבועיים עם דיסקרימיננטה חיובית.

תרגיל 7.26. מצאו את כל ההפיכים של $\mathcal{O}_3 = \mathbb{Z}[\sqrt{3}]$.

פתרון. הפתרון המינימלי של המשוואה $a^2 - 3b^2 = \pm 1$ הוא $a = 2, b = 1$. נסמן $\alpha_0 = 2 + \sqrt{3}$. לפי משפט דיריכלה לעיל האיברים ההפיכים של $\mathcal{O}_3$ הם רק $\pm\alpha_0^n$ עבור $n \in \mathbb{Z}$ וזהו.

תרגיל 7.27. עבור $D = -3$ מצאו את ההפיכים ב-$\mathcal{O}_{-3}$.

פתרון. לפי הגדרה $\mathcal{O}_{-3} = \mathbb{Z}[\frac{1+\sqrt{-3}}{2}]$. נסמן $\omega = \frac{1+\sqrt{-3}}{2}$. באופן דומה לתרגיל 7.21 עבור $\mathbb{Z}[i]$ נעזר בנורמה של איבר $\alpha = a + b\omega \in \mathbb{Z}[\frac{1+\sqrt{-3}}{2}]$. נחשב ונראה שגם כאן הנורמה היא מספר שלם לא שלילי:

$$N(\alpha) = \left(a + \frac{1}{2}b + \frac{\sqrt{-3}}{2}bi\right)\left(a + \frac{1}{2}b - \frac{\sqrt{-3}}{2}bi\right) = \left(a + \frac{1}{2}b\right)^2 + \frac{3}{4}b^2 = a^2+ab+b^2$$

(תרגיל: הראו שהנורמה תמיד מקבלת ערכים שלמים על $\mathbb{Z}[\sqrt{D}]$, ואילו על $\mathcal{O}_D$ היא תקבל ערכים שלמים אם ורק אם $D \equiv 1 \pmod 4$.) גם כאן אפשר לראות ש-α הפיך אם ורק אם $N(\alpha) = 1$. אם $|b| > 2$, אז $\frac{3}{4}b^2 \geq 3$, ולכן $N(\alpha) > 1$. כלומר אם נרצה איבר הפיך נדרוש $|b| \leq 1$. מפני ש-$a^2 + ab + b^2$ סימטרי בהחלפת a ו-b, אז בהכרח גם $|a| \leq 1$. הפתרונות היחידים למשוואה $a^2 + ab + b^2 = 1$ הם

$$(a = 0, b = \pm 1) \vee (a = \pm 1, b = 0) \vee (a = \pm 1, b = \mp 1)$$

כלומר האיברים ההפיכים בחוג $\mathcal{O}_{-3}$ הם רק $\pm 1, \pm\omega, \pm(1-\omega)$.

טענה 7.28. מפני שאנו עוסקים בתחומי שלמות, אז עבור $a \neq 0$ מתקיים $a|b$ אם ורק אם $ba^{-1} \in R$. המכפלה האחרונה מחושבת בשדה השברים של R (שקיים!) ולא מדקדקים בכך שאנו עובדים עם השיכון לשדה השברים.

דוגמה 7.29. בחוג $\mathbb{Z}$ מתקיים $2|4$. לכן $4 \cdot 2^{-1} \in \mathbb{Z}$, אף על פי ש-2 לא הפיך ב-$\mathbb{Z}$.
באופן דומה בחוג $\mathbb{Z}[\sqrt{5}]$ מתקיים $2 + \sqrt{5} | 7 + \sqrt{5}$ כי

$$\left(7 + \sqrt{5}\right)\left(2 + \sqrt{5}\right)^{-1} = \left(7 + \sqrt{5}\right)\left(-2 + \sqrt{5}\right) = -9 + 5\sqrt{5} \in \mathbb{Z}[\sqrt{5}]$$

8 תרגול שמיני

הגדרה 8.1. איבר $0 \neq a \in R$ בתחום שלמות תמיד אפשר לפרק כ-$a = au \cdot u^{-1}$ כאשר $u \in R^\times$ איבר הפיך. לפירוק כזה נקרא פירוק טריוויאלי.
נאמר שאיבר $0 \neq a \in R$ לא הפיך הוא אי פריק אם אין לו פירוק לא טריוויאלי. Irreducible

טענה 8.2. התנאים הבאים שקולים:

1. a אי פריק.
2. אם $a = xy$, אז $x \sim a$ או $y \sim a$.
3. אם $a = xy$, אז x הפיך או y הפיך.
4. אם $a = xy$, אז $x \sim a$ או x הפיך.
5. אם $x|a$, אז $x \sim a$ או x הפיך.

דוגמה 8.3. $x \in F[x]$ הוא אי פריק. קל לבדוק לפי דרגה שלא קיימים $f(x), g(x) \in F[x]$ לא הפיכים כך ש-$x = f(x) \cdot g(x)$.

דוגמה 8.4. חשוב לדעת באיזה חוג נמצאים: האיבר $x^2 + 1$ הוא אי פריק ב-$\mathbb{R}[x]$, אבל פריק ב-$\mathbb{C}[x]$.

דוגמה 8.5. כל מספר ראשוני הוא אי פריק ב-$\mathbb{Z}$ (נסו לנחש הכללה). לעומת זאת, האיבר $2 \in \mathbb{Z}[i]$ פריק כי $2 = (1+i)(1-i)$, וראינו ש-$1+i, 1-i$ אינם הפיכים ב-$\mathbb{Z}[i]$.

הערה 8.6. בשדה, או בחוג חילוק, העניין בפריקות נהפך טריוויאלי, כי כל איבר ששונה מאפס הוא הפיך.

תרגיל 8.7. יהי $p \in R$ אי פריק, ויהי $p \sim q$. הוכיחו ש-q אי פריק.

פתרון. מהתכונות של יחס החברות, קיים $u \in R^\times$ כך ש-$q = up$. נניח $q = bc$, ונרצה להראות ש-b או c הפיכים. נחשב

$$p = u^{-1}q = (u^{-1}b) \cdot c$$

ומפני ש-p אי פריק, נקבל ש-$u^{-1}b$ או c הפיכים. אם c הפיך, סיימנו. אחרת, $u^{-1}b$ הפיך ונקבל ש-$b = u \cdot u^{-1}b$ הפיך כמכפלת איברים הפיכים.

תרגיל 8.8. הוכיחו שאם $x|y$ ב-$\mathcal{O}_D$, אז $N(x)|N(y)$ ב-$\mathbb{Z}$. הסיקו ש-x הפיך ב-$\mathcal{O}_D$ אם ורק אם $N(x) = \pm 1$.

פתרון. כמעט מייד מכפליות הנורמה. נתון $x|y$, ולכן $y = xc$ עבור $c \in \mathcal{O}_D$. לכן

$$N(y) = N(xc) = N(x)N(c)$$

ולכן $N(x)|N(y)$. אם x הפיך, אז קיים x^{-1} כך ש-$xx^{-1} = 1$, לכן $N(x)N(x^{-1}) = 1$ ולכן $N(x) = \pm 1$ כי $N(x) \in \mathbb{Z}$. אם $N(x) = \pm 1$, אז $x \cdot \overline{x} = \pm 1$. כלומר $x^{-1} = \pm \overline{x}$ הוא ההופכי של x.

תרגיל 8.9. יהי $a \in \mathcal{O}_D$. הוכיחו שאם $N(a)$ אי פריק, אז a אי פריק.

פתרון. נניח $a = xy$. אזי $N(a) = N(x)N(y)$. מפני ש-$N(a)$ אי פריק ב-$\mathbb{Z}$, אז הוא מספר ראשוני (או הנגדי שלו). לכן $N(x)$ או $N(y)$ הם ± 1, ולכן x או y הפיכים. כלומר a אי פריק.

תרגיל 8.10. תנו דוגמה לאיבר $a \in \mathcal{O}_D$ אי פריק עבורו $N(a)$ אינו ראשוני.

פתרון. נבחר $D = 10$. נראה ש-$a = 4 \pm \sqrt{10} \in \mathcal{O}_{10} = \mathbb{Z}[\sqrt{10}]$ אי פריקים.
נניח $a = xy$. אזי $N(a) = N(x)N(y) = 6$. נניח בשלילה ש-x, y לא הפיכים. לכן $N(x) \neq \pm 1$, או למעשה $N(x) \in \{\pm 2, \pm 3\}$. יהי $c + d\sqrt{10} \in \mathcal{O}_{10}$, אזי

$$N(c + d\sqrt{10}) = c^2 - 10d^2 = k \in \mathbb{Z}$$

נחשב מודולו 10 ונקבל $c^2 \equiv k \pmod{10}$. הריבועים מודולו 10 הם $\{0, 1, 4, 5, 6, 9\}$. נשים לב שמפני ש-$2, 3, 7, 8$ אינם ריבועים מודולו 10, אז $k \neq \pm 2, \pm 3$. כלומר ב-$\mathcal{O}_{10}$ אין איברים מנורמה $\pm 2, \pm 3$. זו סתירה לכך ש-x לא הפיך.
באופן דומה $N(2 \pm \sqrt{10}) = -6$, $N(2) = 4$ ו-$N(3) = 9$ הם אי פריקים כי אין איברים מנורמה $\pm 2, \pm 3$. שימו לב ש-$3 \pm \sqrt{10}$ הפיכים.

תרגיל 8.11. הוכיחו ש-$a = 1 + \sqrt{-5} \in \mathcal{O}_{-5} = \mathbb{Z}\left[\sqrt{-5}\right]$ אינו פריק.

פתרון. נניח $a = xy$. אזי $N(a) = N(x)N(y) = 6$. נניח בשלילה ש-x, y לא הפיכים. כלומר

$$N(x) = 2, N(y) = 3 \quad \vee \quad N(x) = 3, N(y) = 2$$

מפני שהנורמה ב-$\mathcal{O}_{-5}$ אינה שלילית, הרי $N(c + d\sqrt{-5}) = c^2 + 5d^2$. אבל למשוואות $c^2 + 5d^2 = 2, 3$ אין פתרון בשלמים (ניתן לחשב מודולו 5 ולראות ששם הריבועים הם רק 1 ו-4). סתירה.

תרגיל 8.12. הוכיחו כי $\mathbb{Z}[\sqrt{-5}]$ אינו חוג ראשי. כלומר שקיים אידאל שלא נוצר על ידי איבר אחד.

פתרון. נבחר את $I = \left\langle 2, 1 + \sqrt{-5} \right\rangle$. תחילה נראה כי I נאות. יהי $2a + (1 + \sqrt{-5})b \in I$ איבר כלשהו. הנורמה שלו היא

$$N(2a + (1 + \sqrt{-5})b) = 4a\bar{a} + 2\left((1 + \sqrt{-5})b\bar{a} + \overline{(1 + \sqrt{-5})b\bar{a}}\right) + 6b\bar{b}$$

והיא תמיד מתחלקת ב-2. לכן $1 \notin I$, כלומר I נאות. נניח $I = \langle m \rangle$. אז קיימים $c, d \in \mathbb{Z}[\sqrt{-5}]$ כך ש-

$$cm = 2, \quad dm = 1 + \sqrt{-5}$$

ולכן

$$N(c)N(m) = 4, \quad N(d)N(m) = 6$$

מכאן נקבל ש-$N(m) | 4, 6$. כלומר $N(m) \in \{1, 2\}$. בתרגיל הקודם ראינו שאין איברים מנורמה 2 ב-$\mathbb{Z}[\sqrt{-5}]$, ולכן $N(m) = 1$. כלומר m הפיך ונקבל $\langle m \rangle = \mathbb{Z}[\sqrt{-5}] \neq I$ שזו סתירה.

Prime

הגדרה 8.13. איבר $0 \neq p \in R$ יקרא ראשוני אם p לא הפיך ואם $p|ab$ גורר ש-$p|a$ או $p|b$ לכל $a, b \in R$.

תרגיל 8.14. כל איבר ראשוני הוא אי פריק.

פתרון. נניח בשלילה $0 \neq p \in R$ ראשוני ופריק. אז $p = ab$ עבור a, b לא הפיכים כלשהם. לכן $p|ab$ ונניח בה"כ כי $p|a$. כלומר קיים $c \in R$ כך ש-$a = pc$. לכן $p = ab = pcb$, לכן $p(1-cb) = 0$ ומפני ש-$p \neq 0$ נקבל ש-$bc = 1$ (כזכור R תחום שלמות). סתירה לכך ש-b לא הפיך.

הערה 8.15. $p \in R$ איבר ראשוני אם ורק אם Rp אידאל ראשוני אם ורק אם R/Rp תחום שלמות.

תרגיל 8.16. הראו כי $1 + i \in \mathbb{Z}[i]$ הוא ראשוני.

פתרון. נוכיח כי $\mathbb{Z}[i]/\langle 1+i \rangle$ הוא תחום שלמות, ולפי ההערה האחרונה זה מספיק. נסמן את תמונת איבר $x \in \mathbb{Z}[i]$ בהטלה הטבעית למנה ב-$\overline{x} = x + \langle 1 + i \rangle$. נבדוק

$$a + bi - (a - b) = b + bi \in \langle 1 + i \rangle$$

ולכן $\overline{a - b} = \overline{a + bi}$. כלומר לכל מחלקה בחוג המנה יש נציג שהוא מספר שלם. בנוסף

$$N(1 + i) = (1 + i)(1 - i) = 2 \in \langle 1 + i \rangle$$

ולכן

$$\begin{aligned} \mathbb{Z}[i]/\langle 1+i \rangle &= \{a + bi + \langle 1 + i \rangle \mid a, b \in \mathbb{Z}\} = \left\{\overline{a - b} \,\middle|\, a, b \in \mathbb{Z}\right\} \\ &= \left\{\overline{(a - b) \pmod 2} \,\middle|\, a, b \in \mathbb{Z}\right\} = \left\{\overline{0}, \overline{1}\right\} \cong \mathbb{Z}/2\mathbb{Z} \end{aligned}$$

הערה 8.17. כמו בשאר ההגדרות, ראשוניות איבר תלויה בחוג. למשל $2 \in \mathbb{Z}$ ראשוני, ואילו $2 \in \mathbb{Z}[i]$ פריק, ולכן גם לא ראשוני.

דוגמה 8.18. ישנם איברים אי פריקים שאינם ראשוניים. למשל ראינו כי $3 \in \mathbb{Z}[\sqrt{10}]$ אי פריק, ונראה שהוא לא ראשוני. נשים לב כי

$$3|6 = \left(4 + \sqrt{10}\right)\left(4 - \sqrt{10}\right)$$

אבל 3 לא מחלק את $4 \pm \sqrt{10}$ משיקולי נורמה. כלומר אם $\left(4 \pm \sqrt{10}\right) = 3\alpha$ עבור $\alpha \in \mathbb{Z}[\sqrt{10}]$, אז

$$6 = N(4 \pm \sqrt{10}) = N(3)N(\alpha) = 9N(\alpha)$$

ונקבל $N(\alpha) = \frac{6}{9} \in \mathbb{Z}$ שזו סתירה.

תרגיל 8.19. הוכיחו שכל אידאל $0 \neq I \lhd \mathbb{Z}[\sqrt{D}]$ מכיל מספר טבעי, והסיקו כי $\mathbb{Z}[\sqrt{D}]/I$ סופי.

פתרון. יהי $\alpha = a + b\sqrt{D} \in I$. מצד אחד, $N(\alpha) = a^2 - Db^2 \in \mathbb{Z}$ ומצד שני

$$N(\alpha) = \left(a + b\sqrt{D}\right)\left(a - b\sqrt{D}\right) \in I$$

נסמן $k = N(\alpha)$. אז

$$\mathbb{Z}[\sqrt{D}]/I = \left\{a + b\sqrt{D} + I \,\middle|\, a, b \in \mathbb{Z}\right\} = \left\{a + b\sqrt{D} + I \,\middle|\, 0 \leq a, b \leq k\right\}$$

מסקנה מן התרגיל: אם $0 \neq I \lhd \mathbb{Z}[\sqrt{D}]$ ראשוני, אז $\mathbb{Z}[\sqrt{D}]/I$ תחום שלמות סופי, ולכן מדובר בשדה. כלומר I הוא מקסימלי.

שאלה למחשבה: מה ניתן לומר על אוסף הפתרונות של משוואת פל המוכללת $x^2 - Dy^2 = k$?

תרגיל 8.20. הוכיחו כי $x^2 + 2 \in \mathbb{Z}[x]$ הוא איבר ראשוני.

פתרון. נוכיח כי $\mathbb{Z}[x]/\langle x^2+2\rangle \cong \mathbb{Z}[\sqrt{-2}]$ בעזרת הומומורפיזם ההצבה $\varphi\colon \mathbb{Z}[x] \to \mathbb{Z}[\sqrt{-2}]$ השולח את $f(x)$ ל-$f(\sqrt{-2})$. הגרעין הוא בדיוק $\langle x^2 + 2\rangle$ ונקבל את האיזומורפיזם הדרוש לפי משפט האיזומורפיזם הראשון.

מפני שהנורמה ב-$\mathbb{Z}[\sqrt{-2}]$ מתאפסת רק עבור 0, אז מדובר בתחום שלמות. לכן האידאל $\langle x^2 + 2\rangle$ הוא ראשוני, ולכן $x^2 + 2$ ראשוני.

9 תרגול תשיעי

הגדרה 9.1. תחום שלמות R נקרא אטומי אם לכל $0 \neq a \in R$ קיים פירוק לגורמים אי פריקים. Atomic domain

דוגמה 9.2. הנה רשימה של כמה תחומים אטומיים: $\mathbb{Z}$, כל שדה F (באופן ריק), כל חוג שלמים ריבועיים $\mathcal{O}_D$, $F[x]$ ו-$\mathbb{Z}[x]$.

דוגמה 9.3. הפירוק לגורמים אי פריקים בתחום אטומי הוא לא בהכרח יחיד, ואפילו האורך של הפירוק הוא לא בהכרח קבוע (או חסום). למשל בחוג $\mathbb{Z}[\sqrt{-7}]$ מתקיים $2 \cdot 2 \cdot 2 = \left(1 - \sqrt{-7}\right)\left(1 + \sqrt{-7}\right)$, שהם שני פירוקים שונים לגורמים אי פריקים.

דוגמה 9.4 (מההרצאה). לא כל תחום שלמות הוא אטומי. למשל החוג

$$R = \left\{\sum_{\text{finite}} a_i x^{b_i} \,\middle|\, a_i \in \mathbb{Z}, 0 \leq b_i \in \mathbb{Q}\right\}$$

כאשר הסכומים לעיל הם סופיים.

סקירת הוכחה. קל לראות ש-R הוא חוג חילופי ושהוא תחום שלמות. לכל $0 < r \in \mathbb{Q}$ האיבר $x^r \in R$ הוא פריק כי הוא לא הפיך (ההפכי הוא x^{-r} שאינו ב-R), מתקיים $x^r = x^{r/2} \cdot x^{r/2}$, ובאופן דומה $x^{r/2}$ אינו הפיך.

נראה שאם $\alpha \in R$ הוא מחלק אמיתי של x, אז α הוא מן הצורה $\pm x^r$ עבור $0 < r < 1$. נניח $x = \alpha\beta$ הוא פירוק לא טריוויאלי כאשר α ו-β אינם מן הצורה $\pm x^r$. אז ניתן להוציא מהמכפלה $\alpha\beta$ את החזקה x^r עבור r מקסימלי (בהכרח $r < 1$), ולקבל $x = x^r\gamma$ כאשר ל-γ יש מקדם חופשי. נקבל כי $\gamma = x^{1-r}$, אבל האגף הימני מתאפס כאשר מציבים $x = 0$, ואילו אגף שמאל לא, וזו סתירה. לכן אין ל-x מחלק אי פריק, ומכאן ש-R אינו אטומי. □

הגדרה 9.5. חוג אטומי R יקרא תחום פריקות יחידה (תפ"י) אם בכל שני פירוקים של אותו איבר

Unique factorization domain (UFD)

$$a = up_1 \dots p_r = vq_1 \dots q_s$$

האורכים מקיימים $r = s$, וקיימת תמורה σ של הגורמים האי פריקים כך ש-$p_i \sim q_{\sigma(i)}$.

דוגמה 9.6. החוג $\mathbb{Z}[\sqrt{10}]$ אינו תחום פריקות יחידה, שכן $6 = 2 \cdot 3 = \left(4 + \sqrt{10}\right)\left(4 - \sqrt{10}\right)$. ראינו כי האיברים בפירוקים הם אי פריקים. נשאר להוכיח שהאיברים מפירוקים שונים לא חברים. זה קל להוכחה מחישוב הנורמות.

משפט 9.7. כל תחום ראשי הוא תחום פריקות יחידה.

מסקנה 9.8. החוג $\mathbb{Z}[\sqrt{10}]$ אינו ראשי.

משפט 9.9. יהי R תחום ראשי. אזי $a \in R$ אי פריק אם ורק אם $\langle a \rangle$ אידאל מקסימלי.

הוכחה. נניח a אי פריק. נניח $\langle a \rangle \lhd I \lhd R$. מפני ש-$R$ ראשי, אז קיים b לא הפיך כך ש-$I = \langle b \rangle$. כמו כן קיים $c \in R$ כך ש-$a = bc$. מפני ש-b לא הפיך ו-a אי פריק, אזי c הפיך. לכן $I = \langle b \rangle = \langle a \rangle$.

כעת נניח כי $\langle a \rangle$ מקסימלי. אם $a = bc$ עבור b לא הפיך, אז $b|a$. לכן $\langle a \rangle \subseteq \langle b \rangle \lhd R$. מפני ש-$a$ מקסימלי, אז $\langle a \rangle = \langle b \rangle$. לכן $a \sim b$, וקיבלנו ש-a אי פריק. שימו לב שבכיוון הזה לא היה צורך להניח שתחום השלמות R הוא ראשי. □

משפט 9.10. יהי R תחום ראשי. אז $p \in R$ אי פריק אם ורק אם הוא ראשוני.

הוכחה. כזכור, בתחום שלמות כל ראשוני הוא אי פריק. נניח כי p אי פריק. אז לפי המשפט הקודם $\langle p \rangle$ מקסימלי, ולכן $\langle p \rangle$ אידאל ראשוני, ולכן p איבר ראשוני. □

תרגיל 9.11. יהי p מספר ראשוני אי זוגי, ויהי $D \in \mathbb{Z}$ כך ש-$p \nmid D$. הוכיחו שאם למשוואה

$$x^2 \equiv D \pmod{p}$$

יש פתרון, אז בחוג $\mathbb{Z}[\sqrt{D}]$ מתקיים $\langle p \rangle = P_1P_2$ עבור אידאלים נאותים $P_1 \neq P_2$.

Quadratic residue

פתרון. אם יש פתרון לחפיפה לעיל, נקרא ל-D שארית ריבועית מודולו p. נניח a הוא פתרון. איבר כללי במכפלת האידאלים $\left\langle p, a+\sqrt{D}\right\rangle \left\langle p, a-\sqrt{D}\right\rangle$ הוא מן הצורה

$$c_1p^2 + c_2p\left(a+\sqrt{D}\right) + c_3p\left(a-\sqrt{D}\right) + c_4\left(a+\sqrt{D}\right)\left(a-\sqrt{D}\right)$$

ולכן המכפלה שווה

$$\left\langle p, a+\sqrt{D}\right\rangle \left\langle p, a-\sqrt{D}\right\rangle = \langle p\rangle \left\langle p, a+\sqrt{D}, a-\sqrt{D}, \frac{a^2-D}{p}\right\rangle$$

נרצה להראות שאגף ימין שווה $\langle p\rangle$. אם $p|a$, אז $p|a^2$, ולכן $p|D$ שזו סתירה לנתון. לכן $p\nmid a$. נשים לב ש-$2a = \left(a-\sqrt{D}\right) + \left(a+\sqrt{D}\right)$, ולכן $\gcd(2a,p)=1$. לכן

$$1 = \gcd(2a,p) \in \left\langle p, a+\sqrt{D}, a-\sqrt{D}, \frac{a^2-D}{p}\right\rangle$$

כלומר האידאל הזה הוא כל $\mathbb{Z}[\sqrt{D}]$. קיבלנו $\left\langle p, a+\sqrt{D}\right\rangle \left\langle p, a-\sqrt{D}\right\rangle = \langle p\rangle$, ונותר לנמק למה האידאלים באגף שמאל הם שונים. לו הם היו שווים, אז $2a, p \in \left\langle p, a+\sqrt{D}\right\rangle$, ומאותם שיקולים נקבל $\left\langle p, a+\sqrt{d}\right\rangle = \mathbb{Z}[\sqrt{D}]$, ולכן $\langle p\rangle = \mathbb{Z}[\sqrt{D}]$ שזו סתירה.

Euclidean function

הגדרה 9.12. יהי R תחום שלמות. פונקציה $d\colon R\to \mathbb{N}\cup\{0,-\infty\}$ המקיימת $d(0) < d(x)$ לכל $x\neq 0$ נקראת פונקציה אוקלידית אם

1. לכל $b\neq 0$ ולכל a קיימים $q,r\in R$ כך ש-$a=qb+r$ וגם $d(r)<d(b)$.
2. $d(a)\le d(b)$ לכל $a|b$.

Euclidean domain

אם קיימת פונקציה כזו עבור R, נאמר שהוא תחום אוקלידי.

דוגמה 9.13. כל שדה הוא תחום אוקלידי, באופן טריוויאלי. פשוט נגדיר $d(x)=1$ לכל $x\neq 0$.

החוג $\mathcal{O}_{-1}=\mathbb{Z}[i]$ הוא אוקלידי, עם פונקציית הנורמה $d(a+bi)=a^2+b^2$. אגב, ישנם בדיוק 21 חוגי שלמים ריבועיים $\mathcal{O}_D$ שפונקציית הנורמה שלהם היא אוקלידית.

משפט 9.14. יהי R חוג חילופי. יהיו $f,g\in R[x]$ כאשר g פולינום מתוקן. אז קיימים $r,q\in R[x]$ כך ש-$f=gq+r$ וגם $\deg(r)<\deg(g)$.

משפט 9.15. כל תחום אוקלידי הוא תחום ראשי.

הוכחה. יהי $0\neq I\lhd R$. ניקח $0\neq b\in I$ כך ש-$d(b)=\min\{d(c)\,|\,0\neq c\in I\}$. מן האוקלידיות, נקבל ש-$b$ מחלק כל איבר אחר ב-I (אחרת זו סתירה למינימליות), ולכן $I=\langle b\rangle$. $\square$

דוגמה 9.16. עבור $D<0$, החוג $\mathcal{O}_D$ אוקלידי אם ורק אם

$$D\in\{-1,-2,-3,-7,-11\}$$

במקרים אלו פונקציית הנורמה היא אוקלידית. החוג $\mathcal{O}_D$ הוא תחום ראשי שאינו אוקלידי עבור $D<0$ אם ורק אם $D\in\{-19,-43,-67,-163\}$.

תרגיל 9.17. הראו שהחוג $\mathbb{Z}[x]$ אינו תחום אוקלידי.

פתרון. אנחנו כבר יודעים כי $\mathbb{Z}[x]$ אינו ראשי. למשל, האידאל $\langle 2,x\rangle$ אינו ראשי. לכן $\mathbb{Z}[x]$ גם לא אוקלידי.

למה פונקציית הדרגה של הפולינום אינה אוקלידית? כי לא תמיד קיימת חלוקה עם שארית מדרגה נמוכה יותר כאשר המחלק אינו מתוקן. לדוגמה $2x$ אינו מחלק "טוב" את x.

תרגיל 9.18. יהי F שדה. הוכיחו ש-$F[[x]]$ תחום אוקלידי.

פתרון. נשתמש בפונקציית ההערכה

$$d\left(\sum_{n=0}^{\infty}a_nx^n\right)=\min\{i\,|\,a_i\neq 0\}$$

ונראה שהיא אוקלידית. קל לראות כי $d(fg)=d(f)+d(g)>d(f)$ עבור $f,g\in F[[x]]$ השונים מאפס.

נניח $g\neq 0$, ויש להראות שיש $r,q\in F[[x]]$ כך ש-$f=qg+r$ וגם $d(r)<d(g)$. אם $d(f)<d(g)$ נבחר $r=f$ ו-$q=0$.

אחרת, נסמן $n=d(g)\geq d(f)=m$. לכן $g=x^ng_0$, $f=x^mf_0$ כאשר $d(f_0)=d(g_0)=0$. לכן f_0,g_0 הפיכים. נבחר $q=x^{m-n}g_0^{-1}f_0$ ו-$r=0$, ולכן d היא פונקציה אוקלידית.

תרגיל 9.19. יהי $a\in R$ איבר בתחום אוקלידי. הוכיחו ש-a הפיך אם ורק אם $d(a)=d(1)$.

פתרון. אם a הפיך, אז $a|1$ ולכן $d(a)\leq d(1)$, וגם $1|a$ ולכן $d(1)\leq d(a)$. בסך הכל $d(a)=d(1)$.

אם $d(a)=d(1)$, אז נוכל לרשום $1=qa+r$ עבור $d(r)<d(a)=d(1)$. אם $r\neq 0$ נקבל סתירה (כי $d(1)\leq d(r)$), לכן $a\sim 1$, ולכן a הפיך.

10 תרגול עשירי

10.1 אי פריקות של פולינומים

משפט 10.1. יהי F שדה, ויהי $f(x)\in F[x]$ פולינום ממעלה $n\geq 1$. אז ל-f יש לכל היותר n שורשים שונים ב-F.

הערה 10.2. המשפט לעיל אינו נכון כאשר F אינו שדה. למשל לפולינום x^2+x יש ארבעה פתרונות בחוג $\mathbb{Z}/6\mathbb{Z}$.

משפט 10.3. יהי R חוג חילופי, ויהיו $c \in R$ ו-$f(x) \in R[x]$. אז $f(c)=0$ אם ורק אם $(x-c)|f(x)$ ב-$R[x]$.

משפט 10.4. יהי F שדה, ויהי $f(x) \in F[x]$ פולינום ממעלה 2 או 3. אז $f(x)$ אי פריק אם ורק אם אין לו שורשים ב-F.

הערה 10.5. המשפט לעיל אינו נכון לפולינומים ממעלות גבוהות יותר. למשל הפולינום $(x^2+1)^2$ פריק ב-$\mathbb{R}[x]$, אבל אין לו שורשים ב-$\mathbb{R}$.

תרגיל 10.6. יהי פולינום

$$f(x) = a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$$

ונניח שישנו שבר מצומצם $\frac{c}{d} \in \mathbb{Q}$ שהוא שורש של f. הוכיחו ש-$d|a_n$ ו-$c|a_0$.

פתרון. נציב את השורש $\frac{c}{d}$ ונכפיל ב-d^n:

$$\begin{aligned} f\left(\frac{c}{d}\right) &= a_n\left(\frac{c}{d}\right)^n + \cdots + a_1\left(\frac{c}{d}\right) + a_0 \\ 0 &= a_n c^n + \cdots + a_1 c d^{n-1} + a_0 d^n \\ -a_0 d^n &= a_n c^n + \cdots + a_1 c d^{n-1} = c\left(a_n c^{n-1} + \cdots + a_1 d^{n-1}\right) \end{aligned}$$

ולכן $c|a_0 d^n$. הנחנו שהשבר $\frac{c}{d}$ הוא מצומצם, כלומר $(c,d)=1$. לכן $c|a_0$, כדרוש.

באופן דומה מוכיחים $d|a_n$. נעיר שהתרגיל תקף עבור כל תחום פריקות יחידה R במקום $\mathbb{Z}$, ושדה השברים של R במקום $\mathbb{Q}$.

תרגיל 10.7. יהי p מספר ראשוני. הראו שלכל $n>1$ טבעי המספר $\sqrt[n]{p}$ הוא אי רציונלי.

פתרון. נתבונן בפולינום $f(x)=x^n-p$. ברור כי $\sqrt[n]{p}$ הוא שורש של f. אם $\frac{c}{d} \in \mathbb{Q}$ שורש של f, אז $c \in \{\pm 1, \pm p\}$ ו-$d \in \{\pm 1\}$ לפי תרגיל 10.6. אבל לכל $n>1$ מתקיים

$$f\left(\frac{c}{d}\right) = (\pm p)^n - p \neq 0$$

ולכן אין שורש רציונלי ל-f.

לשאר התרגול נניח כי R הוא תחום פריקות יחידה, ו-F הוא שדה השברים שלו, אלא אם נאמר אחרת.

האינטואיציה הראשונית היא לחשוב שבשדה השברים יותר דברים מתפרקים, בדומה לכך ש-x^2+1 אי פריק מעל $\mathbb{R}$ אבל פריק מעל $\mathbb{C}$. מסתבר שזה לא ממש כך:

דוגמה 10.8. הפולינום $2x+2$ פריק מעל $\mathbb{Z}$: $2x+2=2(x+1)$ וזה פירוק אמיתי. אבל מעל $\mathbb{Q}$ הפירוק הזה לא אמיתי (כי 2 הפיך) והפולינום אי פריק. אבל הפירוק הזה מעל $\mathbb{Z}$, הוא לא באמת "הוגן" ולכן אנחנו קוראים לפירוק של פולינום כשאחד הגורמים הוא סקלר פירוק לא אמיתי. פירוק אמיתי של פולינומים הוא פירוק לפולינומים מדרגות נמוכות יותר.

Content

הגדרה 10.9. יהי $f(x) = a_nx^n + \cdots + a_1x + a_0 \in R[x]$ פולינום. התכולה של f היא המחלק המשותף המירבי של המקדמים $a_0, a_1, \ldots, a_n$ ומסמנים אותה ב-$c(f)$.

Primitive

הגדרה 10.10. פולינום $f \in R[x]$ יקרא פרימיטיבי אם מקדמיו זרים, כלומר $c(f) = 1$.

Eisenstein's criterion

משפט 10.11 (קריטריון אייזנשטיין). יהי R ◁ P אידאל ראשוני. יהי $f(x) = a_nx^n + \cdots + a_1x + a_0 \in R[x]$ פולינום המקיים

- $a_i \in P$ לכל $i \neq n$
- $a_n \notin P$
- $a_0 \notin P^2$

אז f אי פריק ב-$F[x]$ (אין לו פירוק אמיתי מעל R). אם f פרימיטיבי ב-R, אז f אי פריק ב-$R[x]$.

במקרה הפרטי שבו $P = \langle p \rangle$ עבור איבר ראשוני p התנאים לעיל שקולים לכך ש-p לא מחלק את a_n, מחלק את a_i עבור $i \neq n$ ו-p^2 לא מחלק את a_0.

הוכחה. נניח בשלילה כי $f = g \cdot h$ פירוק אמיתי. נסמן

$$g(x) = c_kx^k + \cdots + c_1x + c_0, \qquad h(x) = b_{n-k}x^{n-k} + \cdots + b_1x + b_0$$

עבור $0 < k < n$. יהי b_i המקדם עם אינדקס מינימלי ב-h שלא שייך ל-P ויהי c_j המקדם עם אינדקס מינימלי ב-g שלא שייך ל-P. נתבונן בפירוק הפולינומים מעל תחום השלמות R/P, ונקבל $b_ic_j \equiv a_{i+j} \pmod P$. מפני ש-$P$ ראשוני, אז $b_ic_j \notin P$, ולכן $a_{i+j} \notin P$. זה יתכן רק כאשר $i + j = n$, ולכן $i = n - k$ ו-$j = k$. בפרט, $b_0, c_0 \in P$ ולכן $a_0 = b_0c_0 \in P^2$, שזו סתירה. לכן אין פירוק אמיתי. □

דוגמה 10.12. הפולינום $f(x) = 22x^5 + 27x + 15$ הוא אי פריק מעל $\mathbb{Z}$ כי הוא מקיים את קריטריון אייזנשטיין עבור $p = 3$. כלומר 3 לא מחלק את 22, מחלק את 27 ואת 15, אבל 3^2 לא מחלק את 15.

דוגמה 10.13. הפולינום $f(x) = x^6 - 30x + 15$ הוא אי פריק מעל $\mathbb{Z}[i]$ כי הוא מקיים את קריטריון אייזנשטיין עבור $P = \langle 3 \rangle$, והראינו כי 3 ראשוני ב-$\mathbb{Z}[i]$.

תרגיל 10.14. הוכיחו האם $f(x, y) = y^2 + (x^2 + 2)y + (x^2 + 2)(x^2 + 3)$ אי פריק ב-$\mathbb{Z}[x, y]$?

פתרון. הוא אי פריק. נסמן $S = \mathbb{Z}[x]$ (שהוא תחום פריקות יחידה) ויהי $p(x) = x^2 + 2$ שהוא איבר ראשוני ב-S. כעת ניתן להשתמש בקריטריון אייזנשטיין לגבי האידאל $\langle p \rangle$ ב-$S[y] = \mathbb{Z}[x, y]$ ולהוכיח כי f אי פריק שם.

תרגיל 10.15. הוכיחו האם $f(x) = x^2 - 3$ אי פריק ב-$\mathbb{Z}[\sqrt{-2}][x]$.

פתרון. בחוג $S=\mathbb{Z}[\sqrt{-2}]$ אי אפשר להשתמש בקריטריון אייזנשטיין עם $P=\langle 3\rangle$ כי $\left(1+\sqrt{-2}\right)\left(1-\sqrt{-2}\right)=3$, כלומר 3 פריק, ולכן אינו ראשוני. אבל $1+\sqrt{-2}\in S$ הוא אי פריק, מפני שהנורמה שלו היא ראשונית, $N(1+\sqrt{-2})=1^2+2\cdot 1^2=3$.
בנוסף, ראינו כי S אוקלידי, ובתחום אוקלידי מתקיים שכל איבר אי פריק הוא ראשוני. כלומר ניתן להשתמש בקריטריון אייזנשטיין עם $P=\left\langle 1+\sqrt{-2}\right\rangle$, ולהוכיח ש-$f$ אי פריק ב-$\mathbb{Z}[\sqrt{-2}][x]$.

הערה **10.16**. קריטריון אייזנשטיין נותן תנאי מספיק, אך לא הכרחי לאי פריקות של פולינומים. לדוגמה x^2+4 או x^2+1 אי פריקים מעל $\mathbb{Q}$, למרות שאינם מקיימים את הקריטריון. לעומת זאת x^4+4 פריק ב-$\mathbb{Q}$, שכן

$$x^4+4=\left(x^2+2x+2\right)\left(x^2-2x+2\right)$$

טענה **10.17**. יהיו $a,b\in F$, ונניח $a\neq 0$. אז $f(x)\in F[x]$ אי פריק אם ורק אם $f(ax+b)$ אי פריק.

דוגמה 10.18. כדי להוכיח ש-$f(x)=8x^3+6x^2+1$ אי פריק מעל $\mathbb{Q}$ נציב $x\mapsto x+1$ ונקבל

$$f(x+1)=8x^3+30x^2+36x+15$$

שמקיים את קריטריון אייזנשטיין עבור $p=3$. לכן $f(x+1)$ אי פריק, ולכן $f(x)$ אי פריק מעל $\mathbb{Q}$.

דוגמה 10.19. כדי להוכיח ש-$f(x)=x^4+4x^3+6x^2+2x+1$ אי פריק מעל $\mathbb{Q}$ נציב $x\mapsto x-1$ ונקבל

$$f(x-1)=x^4-2x+2$$

שמקיים את קריטריון אייזנשטיין עבור $p=2$. לכן $f(x-1)$ אי פריק, ולכן $f(x)$ אי פריק מעל $\mathbb{Q}$.

תרגיל 10.20. הוכיחו כי $x^n-y\in F[[y]][x]$ הוא אי פריק.

פתרון. נרצה להשתמש בקריטריון אייזנשטיין עבור $y\in F[[y]]$. לשם כך נראה כי y ראשוני שם.
תחילה נוכיח שהוא אי פריק. נניח שיש פירוק $y=\alpha(y)\cdot\beta(y)=\left(\sum a_ny^n\right)\left(\sum b_my^m\right)$. נשווה מקדמים ונקבל

$$a_0b_0=0,\qquad a_0b_1+a_1b_0=1$$

בלי הגבלת הכלליות קיבלנו $b_0=0$, ואז מהמשוואה השנייה נקבל $a_0b_1=1$. לכן $a_0\neq 0$, ולכן $\alpha(y)$ הפיך ב-$F[[y]]$. כלומר y הוא אי פריק.
הוכחנו ש-$F[[y]]$ הוא אוקלידי ולכן y גם ראשוני. כל מה שנשאר הוא לשים לב ש-x^n-y מקיים את קריטריון אייזנשטיין עבור $P=\langle y\rangle$ ולכן הוא אי פריק.

משפט 10.21 (אחת הגרסאות של הלמה של גאוס). יהי $f(x)\in R[x]$ פרימיטיבי. אז $f(x)$ אי פריק מעל R אם ורק אם f אי פריק מעל F.

מסקנה 10.22. תחת אותם תנאים, נניח $g(x) \in R[x]$. אז $g|f$ ב-$R[x]$ אם ורק אם $g|f$ ב-$F[x]$.
כלומר בעיות פירוק וחלוקה של פולינומים מעל $\mathbb{Q}$ "שקולות" לבעיות פירוק וחלוקה של פולינומים מעל $\mathbb{Z}$.

תרגיל 10.23. יהי $f(x,y,z) = x^2 + y^2 + z^2 \in F[x,y,z]$. נניח $\operatorname{char} F \neq 2$. הוכיחו כי f אי פריק.

פתרון. נעיר שאם $\operatorname{char} F = 2$, אז f פריק מפני ש-$f(x,y,z) = (x+y+z)^2$.
נסמן $S = F[y,z]$, ואז $F[x,y,z] = S[x]$. מעל S הפולינום f הוא פולינום מתוקן ממעלה 2 עם מקדם חופשי $y^2 + z^2$. נרצה להראות שקיים $p \in S$ ראשוני כך ש-p מחלק את $y^2 + z^2$, אבל p^2 לא מחלק אותו.
החוג S הוא תחום פריקות יחידה, ולכן כל איבר מתפרק למכפלת ראשוניים. יהי $p \in S$ איבר ראשוני עם חזקה לא טריוויאלית של z המחלק את $y^2 + z^2$. נסמן $T = F[y]$, וב-k את שדה השברים שלו (כלומר $k = F(y)$). נשים לב כי $S = T[z]$. מכיוון ש-$y^2 + z^2$ פולינום מתוקן ב-$T[z]$, אז לכל פולינום $g(z) \in T[z]$, לפי המסקנה $g|f$ ב-$T[z]$ אם ורק אם $g|f$ ב-$k[z]$.
נניח בשלילה כי p^2 מחלק את $y^2 + z^2$ ב-$k[z]$. אז $y^2 + z^2 = p^2 \cdot h(z)$, ואז $\frac{\partial(y^2+z^2)}{\partial z} = 2z$. לכן כל צירוף לינארי (עם מקדמים מ-$k[z]$) של $y^2 + z^2$ ו-$\frac{\partial(y^2+z^2)}{\partial z}$ מתחלקת ב-p. אבל

$$\frac{1}{y^2}(y^2 + z^2) - \frac{z}{2y^2} \cdot \frac{\partial(y^2 + z^2)}{\partial z} = 1$$

(כאן אנחנו משתמשים בכך שהמאפיין שונה מ-2), וזו סתירה. כלומר p^2 לא מחלק את $y^2 + z^2$ ב-$k[z]$, ולכן הוא לא מחלק את $y^2 + z^2$ ב-$T[z]$.
כלומר קיים ראשוני $p \in S$ המחלק את $y^2 + z^2$, אבל p^2 לא מחלק אותו. לכן מתקיים קריטריון אייזנשטיין, ולכן f אי פריק ב-$S[x] = F[x,y,z]$.

11 תרגול אחת עשר

11.1 מבוא למודולים

הגדרה 11.1. מודול שמאלי מעל חוג R הוא חבורה חיבורית אבלית $(M,+)$ עם פעולה $\mu \colon R \times M \to M$, נסמן $\mu(r,a) = ra$ ונדרוש שיתקיים לכל $r,s \in R$ ולכל $a,b \in M$: Left module

1. $r(a+b) = ra + rb$
2. $(r+s)a = ra + sa$
3. $r(sa) = (rs)a$
4. $1 \cdot a = a$

הערה 11.2. לכל $a \in M$ מתקיים $0_R \cdot a = 0_M$, ולכל $r \in R$ מתקיים $r \cdot 0_M = 0_M$.

דוגמה 11.3. כל מרחב וקטורי מעל שדה הוא מודול (מעל השדה).

דוגמה 11.4. כל חבורה אבלית היא מודול מעל $\mathbb{Z}$.

תרגיל 11.5. תהי G חבורה אבלית. נסמן ב-$\mathrm{End}(G)$ את קבוצת ההומומורפיזמים מ-G לעצמה. בתרגיל הבית הראתם כי $\mathrm{End}(G)$ הוא חוג ביחס לחיבור והרכבה. יהי R חוג ויהי $\varphi\colon R \to \mathrm{End}(G)$ הומומורפיזם של חוגים. מצאו דרך להפוך את G למודול מעל R.

פתרון. לפי הנתון, G היא כבר חבורה אבלית. נותר להגדיר את הכפל בין R לבין G, ולבדוק שמתקיימות הדרישות בהגדרת מודול. אנחנו נגדיר $rg = \varphi(r)(g)$ לכל $r \in R$ ו-$g \in G$. בבית תוכלו לבדוק שכל הדרישות מתקיימות (זה נובע מכך ש-φ הומומורפיזם של חוגים).

אתגר: הראו שהתנאי בתרגיל הוא גם תנאי הכרחי לכך ש-G היא מודול מעל R.

הגדרה 11.6. יהי M מודול מעל R. תת־חבורה $N < M$ תקרא *תת־מודול* של M אם לכל $r \in R$ ו-$n \in N$ מתקיים $rn \in N$. Submodule

דוגמה 11.7. לא כל תת־חבורה של מודול היא תת־מודול. למשל, $\mathbb{Q}$ הוא מודול מעל $\mathbb{Q}$ ו-$\mathbb{Z} \leq \mathbb{Q}$ היא תת־חבורה שאינה תת־מודול.

דוגמה 11.8. יהי G מודול מעל $\mathbb{Z}$, אז תת־המודולים של G הם בדיוק תת־החבורות של G (זכרו כי G הוא למעשה חבורה אבלית). באופן דומה, אם V הוא מודול מעל שדה F, אז תת־המודולים של V הם בדיוק תת־המרחבים של V כמרחב וקטורי מעל F.

דוגמה 11.9. יהי V מרחב וקטורי מעל שדה F, ותהי $T\colon V \to V$ העתקה לינארית. אפשר להעניק ל-V מבנה של מודול מעל $F[x]$ על ידי הגדרת הכפל $f(x)\cdot v = f(T)(v)$.

תרגיל 11.10. תהי העתקה לינארית $T\colon V \to V$, ויהי $W \subseteq V$ תת־מרחב T-אינווריאנטי (כלומר הוא נשמר תחת הפעולה של T, דהיינו $T(W) \subseteq W$). הוכיחו כי W הוא תת־מודול של V כמודול מעל $F[x]$.

פתרון. מהנתון ש-W הוא תת־מרחב, מייד נקבל שהוא תת־חבורה חיבורית של V. נותר להוכיח שלכל $f(x) \in F[x]$ ו-$w \in W$ שמתקיים $f(x) \cdot w \in W$.

מפני ש-W הוא T-אינווריאנטי, אז $T(w) \in W$. באינדוקציה נקבל $T^n(w) \in W$. מפני ש-W הוא מרחב וקטורי מעל F, אז גם כל צירוף לינארי של איברים מן הצורה $T^n(w)$ שייך ל-W. בפרט, האיבר $f(T)(w)$ הוא צירוף כזה, ולכל שייך ב-W.

כמו למבנים אלגבריים אחרים, גם למודולים ישנן הגדרות למנות, הומומורפיזם ומשפטי איזומורפיזמים.

הגדרה 11.11. יהי M מודול מעל R, ויהי $N \leq M$ תת־מודול. כחבורות, ברור ש-N הוא תת־חבורה נורמלית, ומסתבר שלחבורת המנה M/N יש מבנה של מודול מעל R, הנקרא *מודול מנה*. Quotient module

Module homomorphism

הגדרה 11.12. יהיו M, N מודולים מעל R. פונקציה $f\colon M \to N$ היא הומומורפיזם של מודולים מעל R אם f היא הומומורפיזם של חבורות המקיים $f(rm) = r \cdot f(m)$ לכל $r \in R$ ו-$m \in M$.

משפט 11.13. יהי $f\colon M \to N$ הומומורפיזם של מודולים. נסמן את הגרעין $\mathrm{Ker}(f) = \{m \in M \,|\, f(m) = 0\}$, שהוא תת־מודול של M. אז מתקיימים משפטי האיזומורפיזמים של נתר, ובפרט $M/\mathrm{Ker}(f) \cong \mathrm{Im}(f)$.

תרגיל 11.14. יהי R חוג חילופי. יהי n מספר טבעי, ותהי E קבוצת הפונקציות $f\colon \{1, \dots, n\} \to R$. הוכיחו שאפשר לתת ל-$E$ מבנה של מודול מעל R, וכי $E \cong R^n$ כמודולים.

פתרון. בקיצור: פונקציה ב-E שקולה ל-n-יה סדורה של תמונת $\{1, \dots, n\}$.
נגדיר חיבור של פונקציות איבר־איבר, כלומר $(f+g)(x) = f(x) + g(x)$. קל להראות כי E היא חבורה חיבורית שאיבר היחידה שלה הוא הפונקציה הקבוצה $z(x) = 0$. נגדיר כפל $R \times E \to E$ לפי $r \cdot f = f_r$ כאשר

$$f_r(x) = rf(x)$$

לכל $1 \leq x \leq n$ (ודאו את הדרישות). נגדיר פונקציה $\varphi\colon E \to R^n$ לפי

$$\varphi(f) = (f(1), \dots, f(n))$$

נראה שזהו הומומורפיזם של מודולים:

$$\begin{aligned}
\varphi(f+g) &= ((f+g)(1), \dots, (f+g)(n)) \\
&= (f(1), \dots, f(n)) + (g(1), \dots, g(n)) = \varphi(f) + \varphi(g) \\
\varphi(rf) &= ((rf)(1), \dots (rf)(n)) = (rf(1), \dots rf(n)) \\
&= r \cdot (f(1), \dots f(n)) = r\varphi(f)
\end{aligned}$$

נראה ש-φ חח"ע: יהי $f \in \mathrm{Ker}(\varphi)$, אזי $(f(1), \dots, f(n)) = (0, \dots, 0)$. לכן $f(x) = 0$ לכל $1 \leq x \leq n$ שהיא איבר היחידה ב-E. נותר להראות כי φ על: יהי $(r_1, \dots, r_n) \in R^n$, אז המקור שנבחר לאיבר זה הוא ברור, $f(x) = r_x$ לכל $1 \leq x \leq n$. קיבלנו ש-φ איזומורפיזם של מודולים, ושימוש במשפט האיזומורפיזם הראשון מסיים את ההוכחה.

Simple

הגדרה 11.15. מודול M יקרא פשוט אם אין לו תת־מודולים לא טריוויאלים.

הערה 11.16. כל חוג הוא מודול מעל עצמו. במקרה זה כל אידאל שמאלי היא תת־מודול, ולהיפך. לכן חוג הוא פשוט אם ורק אם הוא מודול פשוט מעל עצמו.

Cyclic submodule

הגדרה 11.17. יהי M מודול מעל R, ויהי $a \in M$. תת־המודול הציקלי הנוצר על ידי a הוא

$$Ra = \{ra \,|\, r \in R\} \leq M$$

דוגמה 11.18. יהי R חוג. אז R^n הוא מודול ציקלי מעל $M_n(R)$, כי $R^n \cong M_n(R)e_{11}$.

טענה 11.19. מודול M הוא פשוט אם ורק אם לכל $0 \leq a \in M$ מתקיים $Ra = M$.

הוכחה. הכיוון הישיר הוא ברור. נראה את הכיוון ההפוך: נניח בשלילה כי M אינו פשוט, אבל שלכל $0 \leq a \in M$ מתקיים $Ra = M$. יהי $N \leq M$ תת־מודול לא טריוויאלי, ומפני שאינו טריוויאלי, אז קיים $0 \neq a \in N$. נקבל כי $0 \neq Ra \subseteq N$, ומצד שני $Ra = M$, וזו סתירה. □

תרגיל 11.20. יהי M מודול ציקלי מעל R, ויהי $N \leq M$ תת־מודול. הוכיחו ש-M/N הוא מודול ציקלי.

פתרון. קיים $a \in M$ כך ש-$M = Ra$. כלומר לכל $b \in M$ קיים $r \in R$ כך ש-$b = ra$. יהי איבר כללי $b + N \in M/N$. אזי $b + N = ra + N$, ומפני ש-$rN = N$, נקבל

$$ra + N = ra + rN = r(a + N)$$

כלומר M/N ציקלי, ונוצר על ידי $a + N$.

דוגמה 11.21. יתכן כי M/N וגם N מודולים ציקליים, אבל M איננו. למשל, $M = \mathbb{Z} \times \mathbb{Z}$ ו-$N = \mathbb{Z} \times \{0\}$ (כמודולים מעל $\mathbb{Z}$ לצורך העניין).

משפט 11.22. יהי M מודול מעל R. אז M הוא ציקלי אם ורק אם קיים אידאל שמאלי $I \lhd R$ כך ש-$R/I \cong M$.

הגדרה 11.23. נאמר שמודול M נפרש על ידי תת־קבוצה $\{a_j\}_{j \in J} \subseteq M$ מעל R אם לכל $m \in M$ קיימים $r_1, \ldots, r_n \in R$ כך ש-$m = \sum_{i=1}^n r_i a_i$ עבור $a_1, \ldots, a_n$ כלשהם מהקבוצה. Spanned by

אם ל-M יש קבוצה פורשת סופית, נאמר ש-M הוא מודול נוצר סופית מעל R. Finitely generated

הגדרה 11.24. תהי $\{a_j\}_{j \in J} \subseteq M$ קבוצה פורשת של M. אם הקבוצה בלתי תלויה לינארית, כלומר

$$\sum_{i=1}^n r_i a_i = 0 \quad \Rightarrow \quad r_1 = r_2 = \cdots = r_n = 0$$

נקרא לקבוצה בסיס. מודול שיש לו בסיס נקרא חופשי. Basis Free

הערה 11.25. בקורס באלגברה לינארית קרה דבר מופלא: לכל שני בסיסים של מרחב וקטורי יש עוצמה זהה. קראנו לעוצמה זו המימד של המרחב הוקטורי, והוא שמורה חשובה מאוד בחקירת מרחבים וקטוריים.
במודולים כלליים טענה זו לא נכונה. למשל, יהי $V = F^{\aleph_0}$ מרחב וקטורי מעל שדה F, אז ל-$\operatorname{End}_F V$ כמודול מעל עצמו יש בסיס מכל גודל.

דוגמה 11.26. הזכרו בטענה לגבי מרחבים וקטוריים U,V ממימד n: אם $U \subseteq V$, אז $U = V$. לעומת זאת במודולים, נסתכל על $2\mathbb{Z}, \mathbb{Z}$ כמודולים מעל $\mathbb{Z}$. קל לראות ש-$\{1\}$ הוא בסיס של $\mathbb{Z}$ וש-$\{2\}$ הוא בסיס של $2\mathbb{Z}$, אבל $2\mathbb{Z} \neq \mathbb{Z}$. ניתן עדין ללמוד ש-$2\mathbb{Z} \cong \mathbb{Z}$ כמודולים.

תרגיל 11.27. מצאו בסיס לתת־המודול הבא של $\mathbb{Z}^3$ מעל $\mathbb{Z}$:

$$M = \left\{ (x,y,z) \;\middle|\; \begin{array}{c} x+2y+3z=0 \\ x+4y+9z=0 \end{array} \right\}$$

פתרון. המודול M הוא למעשה מרחב הפתרונות (האפסים) של המטריצה $A = \left(\begin{smallmatrix} 1 & 2 & 3 \\ 1 & 4 & 9 \end{smallmatrix}\right)$. נדרג אותה על ידי פעולות **שורה** למציאת קבוצה פורשת (שימו לב שפעולות עמודה משנות את מרחב הפתרונות):

$$A \xrightarrow{-R_1+R_2\to R_2} \begin{pmatrix} 1 & 2 & 3 \\ 0 & 2 & 6 \end{pmatrix} \xrightarrow{(*)} \begin{pmatrix} 1 & 2 & 3 \\ 0 & 1 & 3 \end{pmatrix} \xrightarrow{-2R_2+R_1\to R_1} \begin{pmatrix} 1 & 0 & -3 \\ 0 & 1 & 3 \end{pmatrix}$$

במעבר המסומן $(*)$ זה נראה כאילו חילקנו ב-2, אבל 2 הרי אינו הפיך ב-$\mathbb{Z}$, ולכן חלוקה ב-2 "אסורה". למעשה השורה הזו היא המשוואה $2y+6z = 2(y+3z) = 0$, ומפני שאנחנו בתחום שלמות, זה מחייב כי $y + 3z = 0$.

קיבלנו $y = -3z$ ו-$x = 3z$. לכן איברי M הם $(3z,-3z,z) = (3,-3,1)\,z$ והקבוצה הפורשת היא $\{(3,-3,1)\}$.

דוגמה 11.28. המודול R^n הוא חופשי ונוצר סופית מעל R על ידי $\{e_1,\ldots,e_n\}$. אתגר: הוכיחו שלמודול חופשי הנוצר סופית, יש בסיס סופי.

דוגמה 11.29. נתבונן ב-$\mathbb{Z}/n\mathbb{Z}$ כמודול מעל $\mathbb{Z}$. אין לו בסיס, שהרי מהדרישה $r \cdot a = 0$ עבור $a \in \mathbb{Z}/n\mathbb{Z}$, $r \in \mathbb{Z}$ גוררת ש-$r = 0$ לו היה בסיס. אבל ניתן לקחת גם את $r = n$, ומצד שני $\{1\}$ היא כן קבוצה פורשת עבור $\mathbb{Z}/n\mathbb{Z}$.

טענה 11.30. כל מודול נוצר סופית מעל R הוא מנה של R^n עבור $n \in \mathbb{N}$ כלשהו.

הוכחה. נניח שמודול M נוצר על ידי $\{a_1,\ldots,a_n\}$. בעזרת הקבוצה הפורשת $\{e_1,\ldots,e_n\}$ של R^n נגדיר הומומורפיזם $f\colon e_i \mapsto a_i$, שאותו נרחיב לכל R^n:

$$f\left(\sum_{i=1}^{n} r_i e_i\right) = \sum_{i=1}^{n} r_i a_i$$

ולפי משפט האיזומורפיזם הראשון נקבל $M \cong R/\operatorname{Ker} f$. □

הגדרה 11.31. יהי M מודול מעל R. נגדיר את המאפס (השמאלי) של $x \in M$ הוא Annihilator

$$\operatorname{Ann}_R(x) = \{r \in R \,|\, rx = 0\}$$

וקל לראות כי $\operatorname{Ann}_R(x) \lhd R$. באופן דומה לתת־קבוצה $S \subseteq M$ אפשר להגדיר את המאפס (השמאלי) להיות

$$\operatorname{Ann}_R(S) = \{r \in R \,|\, rS = 0\}$$

הגדרה 11.32. יהי M מודול מעל R. נאמר שאיבר $0 \neq x \in M$ הוא מפותל אם קיים $0 \neq r \in R$ כך ש-$rx = 0$ (אם R אינו תחום שלמות, נאמר ש-x מפותל רק אם קיים r רגולרי כך ש-$rx = 0$). Torsion

נגדיר את הפיתול של M להיות הקבוצה Torsion

$$\mathrm{Tor}_R(M) = \{m \in M \mid \exists (0 \neq r \in R),\, r \cdot m = 0\}$$

נקרא ל-M מפותל אם כל איבריו מפותלים, כלומר $\mathrm{Tor}_R(M) = M$. נאמר ש-M חסר פיתול אם אין בו איברים מפותלים. Torsion free

דוגמה 11.33. נבחר $R = \mathbb{Z}$ ואת $M = \mathbb{Z}/6\mathbb{Z}$. אז $\mathrm{Tor}_R(M) = M$, כלומר M הוא מפותל, שכן לכל $m \in M$ נוכל לבחור את $r = 6 \in R$ ולקבל $r \cdot m = 0$.

אם לעומת זאת נתבונן ב-$\mathbb{Z}/6\mathbb{Z}$ כמודול מעל עצמו נקבל $\mathrm{Tor}_{\mathbb{Z}/6\mathbb{Z}}(\mathbb{Z}/6\mathbb{Z}) = \{0, 2, 3, 4\}$. כאן

$$\mathrm{Ann}_{\mathbb{Z}/6\mathbb{Z}}(3) = \{0, 2, 4\}$$

דוגמה 11.34. יהי R תחום שלמות, ונסתכל עליו כמודול מעל עצמו. מתקיים $\mathrm{Tor}_R(R) = 0$, כי אין ב-R מחלקי אפס. במקרה זה, גם R^n כמודול מעל R הוא חסר פיתול.

יהי $0 \neq a \in R$. אז $R/\langle a \rangle$ הוא מודול מפותל מעל R, שהרי אם $r + \langle a \rangle \in R/\langle a \rangle$, אז

$$a \cdot (r + \langle a \rangle) \in \langle a \rangle = 0_{R/\langle a \rangle}$$

דוגמה 11.35. תהי $(G, +)$ חבורה אבלית סופית. אז G כמודול מעל $\mathbb{Z}$ היא מודול מפותל. לפי משפט לגראנז' נקבל שלכל $a \in G$ מתקיים $|G| \cdot a = 0$.

טענה 11.36. יהי R תחום שלמות. אז $\mathrm{Tor}(M)$ הוא תת־מודול של M.

במקרה כזה, ראוי לקרוא ל-$\mathrm{Tor}(M)$ תת־מודול הפיתול של M. Torsion submodule

הוכחה. יהי $x \in \mathrm{Tor}(M)$ כלשהו. צריך להראות כי $r \cdot x \in \mathrm{Tor}(M)$ לכל $r \in R$. לפי הגדרה, קיים $s \in R$ כך ש-$s \cdot x = 0$. לכן $s \cdot (rx) = r \cdot (sx) = 0$ וקיבלנו כי $rx \in \mathrm{Tor}(M)$.

אם $x, y \in \mathrm{Tor}(M)$, אז קיימים $s, s' \in R$ כך ש-$sx = s'y = 0$, ולכן

$$ss'(x - y) = s'(sx) - s(s'y) = 0$$

ונסיק כי $x - y \in \mathrm{Tor}(M)$. □

טענה 11.37. יהי M מודול מעל R עבורו $\mathrm{Tor}(M)$ הוא תת־מודול. אז $M/\,\mathrm{Tor}(M)$ הוא מודול חסר פיתול מעל R.

הוכחה. יהי $m \notin \mathrm{Tor}(M)$ ונניח בשלילה שקיים $r \in R$ שאינו מחלק אפס עבורו

$$r\,(m + \mathrm{Tor}(M)) = rm + \mathrm{Tor}(M))0_{M/\,\mathrm{Tor}(M)} = \mathrm{Tor}(M)$$

כלומר $rm \in \mathrm{Tor}(M)$. לכן קיים $s \in R$ שאינו מחלק אפס כך ש-$s(rm) = 0$, ולכן $(sr)m = 0$, וקיבלנו סתירה לפיה $m \in \mathrm{Tor}(M)$. □

הערה 11.38. כל מודול M מעל תחום שלמות R ניתן להצגה כסכום ישר של מודולים

$$M \cong \operatorname{Tor}(M) \oplus (M / \operatorname{Tor}(M))$$

דוגמה 11.39. יהי $M = \mathbb{Z}^3 \times (\mathbb{Z}/4\mathbb{Z})$ מודול מעל $\mathbb{Z}$. אז $\operatorname{Tor}(M) \cong \mathbb{Z}/4\mathbb{Z}$ ו-$M/\operatorname{Tor}(M) \cong \mathbb{Z}^3$.

12 תרגול שניים עשר

הגדרה 12.1. יהי M מודול מעל R. נאמר כי M הוא נאמן אם $\operatorname{Ann}_R(M) = 0$. Faithful

הערה 12.2. כל מודול חסר פיתול הוא נאמן.

דוגמה 12.3. יתכן שמודול יהיה נאמן ומפותל. למשל $\mathbb{Q}/\mathbb{Z}$ כמודול מעל $\mathbb{Z}$.

דוגמה 12.4. אם $M = \mathbb{Z}/n\mathbb{Z}$ כמודול מעל $\mathbb{Z}$, אז $\operatorname{Ann}(\mathbb{Z}/n\mathbb{Z}) = n\mathbb{Z}$.

תרגיל 12.5. הראו כי M הוא מודול מעל $R/\operatorname{Ann}(M)$.

פתרון. יהי $r + \operatorname{Ann}(M) \in R/\operatorname{Ann}(M)$. אנחנו רק נראה שהפעולה

$$(r + \operatorname{Ann}(M)) \cdot m = rm$$

מוגדרת היטב לכל $m \in M$, ואת שאר הדרישות ממודול תוכלו להוכיח בבית. נניח

$$r + \operatorname{Ann}(M) = r' + \operatorname{Ann}(M)$$

כלומר $r - r' \in \operatorname{Ann}(M)$. לכן קיים $s \in \operatorname{Ann}(M)$ כך ש-$r = r' + s$. אז

$$rm = (r + \operatorname{Ann}(M)) \cdot m = (r' + s + \operatorname{Ann}(M)) \cdot m = (r' + s)\, m = r'm$$

מסקנה 12.6. אם $I \subseteq \operatorname{Ann}(M)$ הוא אידאל של R, אז M הוא גם מודול מעל R/I.

דוגמה 12.7. יהי $V = \mathbb{R}^3$ ותהי

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

מטריצה שמשרה ל-V מבנה של מודול מעל $\mathbb{R}[x]$ (תזכורת: $f(x) \cdot v = f(A)v$). הפולינום האופייני של A הוא

$$f(\lambda) = |\lambda I - A| = \begin{vmatrix} \lambda & -1 & 0 \\ -1 & \lambda & 0 \\ 0 & 0 & \lambda - 1 \end{vmatrix} = (\lambda - 1)(\lambda^2 - 1)$$

לפי משפט קיילי המילטון $f(A) = 0$, ולכן לכל $v \in V$ מתקיים $f(x)v = f(A)v = 0 \cdot v = 0$. לכן $\langle f(x) \rangle \subseteq \operatorname{Ann}(V)$ ומן המסקנה נקבל ש-V הוא גם מודול מעל $\mathbb{R}[x]/\langle f(x) \rangle$.

טענה 12.8. יהיו N, M מודולים איזומורפיים מעל R. אז $\operatorname{Ann}(M) = \operatorname{Ann}(N)$.

הוכחה. יהי $\varphi\colon M \to N$ איזומורפיזם של מודולים מעל R. יהי $r \in \operatorname{Ann}(M)$, אזי לכל $m \in M$ מתקיים $rm = 0$. לכן

$$0 = \varphi(0) = \varphi(rm) = r\varphi(m)$$

כלומר $r \in \operatorname{Ann}(\operatorname{Im}\varphi) = \operatorname{Ann}(N)$. משיקולי סימטריה, נסיק כי $\operatorname{Ann}(M) = \operatorname{Ann}(N)$. □

מסקנה 12.9. יהי R חוג חילופי ויהיו $L, L' \leq_l R$ אידאלים שמאליים. לכן $R/L \cong R/L'$ איזומורפיים כמודולים מעל R אם ורק אם $L = L'$. (למה? כי מתקיים $\operatorname{Ann}(R/L) = L$ לכל אידאל שמאלי.)

12.1 מודולים מעל תחומים ראשיים

בחלק זה נניח כי R הוא תחום ראשי, ונדבר על המבנה של מודולים נוצרים סופית מעליו. התיאוריה אינה זהה לתורת מרחבים וקטוריים ממימד סופי, אבל לא הכל אבוד.

משפט 12.10. כל תת־מודול של R^n הוא חופשי מדרגה הקטנה או שווה n (כלומר יש לו בסיס מגודל לכל היותר n).

משפט 12.11. כל תת־מודול של R^n הוא מן הצורה $A \cdot R^n$ עבור $A \in M_n(R)$.

המשפט האחרון מאפשר לנו למצוא בסיס של תת־מודול של R^n: בהנתן קבוצה פורשת של תת־המודול, למשל עמודות A, אז נוכל לדרג את המטריצה ומשם לקבל את הבסיס.

תרגיל 12.12. מצאו בסיס של תת־המודול של $\mathbb{Z}^3$, כמודול מעל $\mathbb{Z}$, הנפרש על ידי

$$\{(1,0,-1), (2,-3,1), (4,-3,-1)\}$$

פתרון. המטריצה המתאימה לתת־המודול היא

$$A = \begin{pmatrix} 1 & 2 & 4 \\ 0 & -3 & -3 \\ -1 & 1 & -1 \end{pmatrix}$$

ונדרג אותה בעזרת פעולות עמודה (שימו לב שפעולות שורה משנות את מרחב העמודות):

$$\begin{pmatrix} 1 & 2 & 4 \\ 0 & -3 & -3 \\ -1 & 1 & -1 \end{pmatrix} \xrightarrow[C_3-4C_1\to C_3]{C_2-2C_1\to C_2} \begin{pmatrix} 1 & 0 & 0 \\ 0 & -3 & -3 \\ -1 & 3 & 3 \end{pmatrix} \xrightarrow{C_3-C_2\to C_3} \begin{pmatrix} 1 & 0 & 0 \\ 0 & -3 & 0 \\ -1 & 3 & 0 \end{pmatrix}$$

ולכן תת־המודול נפרש על ידי $\{(1,0,-1), (0,-3,3)\}$. לא חילקנו את $(0,-3,3)$ ב־3, שכן זה איבר לא הפיך ב־$\mathbb{Z}$. האיברים במודול הם

$$\{a\cdot(1,0,-1) + b\cdot(0,-3,3) \mid a,b\in\mathbb{Z}\} = \{(a,-3b,3b-a) \mid a,b\in\mathbb{Z}\}$$

מה לגבי מודול שנוצר סופית, אבל שאינו חופשי? ראינו בטענה 11.30 שהוא מנה של מודול חופשי R^n. כך ניתן להסיק את המשפט הבא:

משפט 12.13. כל מודול נוצר סופית מעל תחום ראשי R הוא מן הצורה $M_A = R^n/AR^n$ עבור $A \in M_n(R)$.

ראינו כיצד מוצאים את המטריצה A (לפעמים נקראת מטריצת היחסים של M_A): ישנו אפימורפיזם $f\colon R^n \to M_A$ שבו $\operatorname{Ker} f = AR^n$, כאשר $A = (a_{ij})$ ו-$\sum a_{ij}e_i$ היא קבוצה פורשת של $\operatorname{Ker} f$. לכן בהנתן קבוצת יוצרים סופית של M_A, אם מוצאים יוצרים לגרעין (למשל על ידי דירוג) ומשלימים באפסים, אז מצאנו את A עד כדי כפל בשמאל ומימין במטריצות הפיכות מעל R.

דוגמה 12.14. יהי $k \in \mathbb{Z}$ ותהי $A = \operatorname{diag}(k, \ldots, k)$ מטריצה אלכסונית. נראה למה איזמורפי המודול $M_A = \mathbb{Z}^n/A\mathbb{Z}^n$:

$$\begin{aligned} M_A &= \{(a_1, \ldots, a_n) + k \cdot \alpha \mid a_i \in \mathbb{Z}, \alpha \in \mathbb{Z}^n\} \\ &= \{(a_1, \ldots, a_n) \,(\operatorname{mod} k) \mid a_i \in \mathbb{Z}\} \cong (\mathbb{Z}/k\mathbb{Z})^n \end{aligned}$$

הגדרה 12.15. תהינה $A, B \in M_n(R)$. נסמן $A \sim B$ ונאמר שהמטריצות דומות אם קיימות $P, Q \in GL_n(R)$ כך ש-$B = PAQ$. (זאת ההגדרה אצלנו, יש כאלו שמגדירים דימיון מטריצות רק עבור $P = Q^{-1}$ שהוא מקרה פרטי של הצמדה.) Similar

הכפל במטריצות הפיכות מעל חוג ראשי הוא למעשה סדרה (סופית) של הפעולות הבאות:

1. הוספת כפולה של עמודה (שורה) לעמודה (לשורה) אחרת.
2. החלפת עמודות והחלפת שורות.
3. כפל בהופכי.

טענה 12.16. מתקיים $A \sim B$ אם ורק אם $M_A \cong M_B$.

רעיון ההוכחה. מעל תחום ראשי ניתן על ידי כפל במטריצות הפיכות להביא כל מטריצה A לצורה אלכסונית $A \sim \operatorname{diag}(d_1, \ldots, d_n, 0, \ldots, 0)$ כאשר $d_1 | d_2 | \ldots | d_n$ ויש m אפסים. צורה כזו היא יחידה עד כדי חברות ונקראת סדורה קנונית. לאיברים d_i קוראים הגורמים המשתמרים של M_A, ומתקיים Invariant factors

$$M_A \cong R^m \oplus {}^{R}\!/_{Rd_1} \oplus \cdots \oplus {}^{R}\!/_{Rd_n}$$

□

מסקנה 12.17. מתקיים

$$\operatorname{Tor}(M) = {}^{R}\!/_{Rd_1} \oplus \cdots \oplus {}^{R}\!/_{Rd_n}$$

ו-M הוא חסר פיתול אם ורק אם M חופשי (כלומר $n = 0$).

דוגמה 12.18. נתבונן בחבורה $M = \{ax + by \mid a, b \in \mathbb{Z}\}$ ונחשוב עליה כמודול מעל $\mathbb{Z}[i]$ לפי

$$ix = y, \quad iy = -x$$

בבית, אפשר וכדאי לוודא שזה אכן מודול. יש אפימורפיזם $\varphi \colon \mathbb{Z}[i]^2 \to M$ המוגדר לפי $e_1 \mapsto x, e_2 \mapsto y$. הגרעין נוצר על ידי $ie_1 - e_2$ (קל לראות לפי הכלה ומשיקולי דרגה). לכן מטריצת היחסים היא $\left(\begin{smallmatrix} i & 0 \\ -1 & 0 \end{smallmatrix}\right)$ ומתקיים

$$M \cong \mathbb{Z}[i]^2 / \begin{pmatrix} i & 0 \\ -1 & 0 \end{pmatrix} \mathbb{Z}[i]^2$$

מפני שהמטריצה מוגדרת עד כדי דימיון, נוכל להגיע לצורה אלכסונית:

$$\begin{pmatrix} i & 0 \\ -1 & 0 \end{pmatrix} \xrightarrow{-iR_1} \begin{pmatrix} 1 & 0 \\ -1 & 0 \end{pmatrix} \xrightarrow{R_1 + R_2 \to R_2} \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$$

ולכן $M \cong 0 \oplus \mathbb{Z}[i]$ בתור מודול מעל $\mathbb{Z}[i]$.

דוגמה 12.19. נתבונן במודול נוצר סופית מעל $\mathbb{Z}$:

$$M = \langle x, y \mid nx = 0, my = 0 \rangle$$

נבחר את הקבוצה הפורשת $\{x, y\}$. ישנו אפימורפיזם של מודולים $\varphi \colon \mathbb{Z}^2 \to M$ לפי $e_1 \mapsto x$ ו-$e_2 \mapsto y$. ברור שהגרעין $\operatorname{Ker} \varphi$ נוצר על ידי היחסים שמגדירים את M. מטריצת היחסים היא $A = \left(\begin{smallmatrix} n & 0 \\ 0 & m \end{smallmatrix}\right)$ ומתקיים

$$M \cong (\mathbb{Z}/n\mathbb{Z}) \times (\mathbb{Z}/m\mathbb{Z})$$

תרגיל 12.20. חשבו את הסדר של החבורה האבלית

$$G = \left\langle a, b, c \;\middle|\; \begin{aligned} 2a + 4b + 3c &= 0 \\ a + 2b + 3c &= 0 \\ a + 4b + 9c &= 0 \end{aligned} \right\rangle$$

פתרון. חבורה אבלית היא מודול מעל $\mathbb{Z}$. היא נוצרת סופית בתור מודול, למשל עם הקבוצה הפורשת $\{a, b, c\}$. ישנו אפימורפיזם של מודולים $\varphi \colon \mathbb{Z}^3 \to G$ לפי $a \mapsto e_1$, $b \mapsto e_2$ ו-$c \mapsto e_3$. ברור שהגרעין $\operatorname{Ker} \varphi$ נוצר על ידי היחסים שמגדירים את G ונרצה למצוא דירוג קנוני של מטריצת היחסים שלה:

$$\begin{pmatrix} 2 & 4 & 3 \\ 1 & 2 & 3 \\ 1 & 4 & 9 \end{pmatrix} \xrightarrow{R_1 \leftrightarrow R_2} \begin{pmatrix} 1 & 2 & 3 \\ 2 & 4 & 3 \\ 1 & 4 & 9 \end{pmatrix} \xrightarrow[R_3 - R_1 \to R_3]{R_2 - 2R_1 \to R_2} \begin{pmatrix} 1 & 2 & 3 \\ 0 & 0 & -3 \\ 0 & 2 & 6 \end{pmatrix} \xrightarrow[C_3 - 3C_1 \to C_3]{C_2 - 2C_1 \to C_2}$$

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & -3 \\ 0 & 2 & 6 \end{pmatrix} \xrightarrow{R_2 + R_3 \to R_2} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 3 \\ 0 & 2 & 6 \end{pmatrix} \xrightarrow{C_3 - C_2 \to C_2} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 3 \\ 0 & 4 & 6 \end{pmatrix} \xrightarrow{R_3 - 4R_2 \to R_3}$$

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 3 \\ 0 & 0 & -6 \end{pmatrix} \xrightarrow{C_3 - 3C_2 \to C_3} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -6 \end{pmatrix}$$

ולכן $G \cong \mathbb{Z}/6\mathbb{Z}$, כלומר $|G| = 6$.

דוגמה 12.21. נמצא צורה אלכסונית קנונית למטריצה הבאה:

$$\begin{pmatrix} 4 & 2 & 2 \\ 1+3i & 1+3i & 0 \\ 5+3i & 3+3i & 2 \end{pmatrix} \sim \begin{pmatrix} 2 & 2 & 4 \\ 0 & 1+3i & 1+3i \\ 2 & 3+3i & 5+3i \end{pmatrix} \sim \begin{pmatrix} 2 & 2 & 4 \\ 0 & 1+3i & 1+3i \\ 0 & 1+3i & 1+3i \end{pmatrix} \sim$$

$$\begin{pmatrix} 2 & 0 & 0 \\ 0 & 1+3i & 1+3i \\ 0 & 1+3i & 1+3i \end{pmatrix} \sim \begin{pmatrix} 2 & 0 & 0 \\ 0 & 1+3i & 0 \\ 0 & 0 & 0 \end{pmatrix} \sim \begin{pmatrix} 2 & 1+i & 0 \\ 0 & 1+3i & 0 \\ 0 & 0 & 0 \end{pmatrix} \sim$$

$$\begin{pmatrix} 1+i & 2 & 0 \\ 1+3i & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \sim \begin{pmatrix} 1+i & 0 & 0 \\ 0 & -4-2i & 0 \\ 0 & 0 & 0 \end{pmatrix} \sim \begin{pmatrix} 1+i & 0 & 0 \\ 0 & 4+2i & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

כדי להגיע לדירוג קנוני (ולא דירוג גאוס) בכל שלב נביא את האיבר הכי קטן לפינה ונאפס את השורה והעמודה המתאימות. בשלבים האחרונים נעזרנו בחישוב

$$\gcd(2, 1+3i) = 1+i = -i \cdot 2 + 1 \cdot (1+3i)$$

תרגיל 12.22. יהי $R = \mathbb{Q}[x]$ ונתונה המטריצה

$$A = \begin{pmatrix} x+1 & 2 & -6 \\ 1 & x & -3 \\ 1 & 1 & x-4 \end{pmatrix}$$

יהי $M = R^3/AR^3$. הוכיחו כי $\langle 1-x^2 \rangle \subseteq \mathrm{Ann}(M)$.

פתרון. נחליף בין שתי השורות הראשונות של A ונחשב

$$\begin{pmatrix} 1 & x & -3 \\ x+1 & 2 & -6 \\ 1 & 1 & x-4 \end{pmatrix} \xrightarrow[R_3-R_1\to R_3]{R_2-(x+1)R_1\to R_2} \begin{pmatrix} 1 & x & -3 \\ 0 & -x^2-x+2 & 3(x-1) \\ 0 & 1-x & x-1 \end{pmatrix} \xrightarrow[C_3+3C_1\to C_3]{C_2-xC_1\to C_2}$$

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & (1-x)(x+2) & 3(x-1) \\ 0 & 1-x & x-1 \end{pmatrix} \xrightarrow{R_2\leftrightarrow R_3} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1-x & x-1 \\ 0 & (1-x)(x+2) & 3(x-1) \end{pmatrix} \xrightarrow{R_3-(x+2)R_2\to R_2}$$

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1-x & x-1 \\ 0 & 0 & -(x-1)^2 \end{pmatrix} \xrightarrow{C_3+C_2\to C_3} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1-x & 0 \\ 0 & 0 & -(x-1)^2 \end{pmatrix} = D$$

כלומר

$$M \cong R^3/DR^3 \cong (R/\langle 1-x \rangle) \times \left(R/\left\langle (1-x)^2 \right\rangle\right)$$

כשמסתכלים על איבר כללי $a = (f + \langle 1-x \rangle, g + \langle (1-x)^2 \rangle) \in M$ קל לראות כי $(1-x)^2 \cdot a = 0_M$, ולכן $\langle 1-x^2 \rangle \subseteq \mathrm{Ann}(M)$ (למעשה יש שיוויון).