מבוא לחוגים ומודולים
מערכי תרגול קורס 88-212

מהדורת קריאה מוקדמת

מאי 2017, גרסה 0.8

אוניברסיטת בר־אילן סמסטר ב׳ תשע״ז

תוכן העניינים

מבוא

כמה הערות טכניות לתחילת הקורס:

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

מחבר בשנת הלימודים תשע"ז: תומר באואר

1 תרגול ראשון

1.1 הגדרות בסיסיות

Rng, or non-unital ring

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

Additive group

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

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

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

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

Commutative

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

Ring

Unital ring

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

Division ring

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

Field

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

דוגמה 1.3. הרבה מבנים אלגבריים שפגשתם הם חוגים. למשל

1. $(\mathbb{Z},+,\cdot)$ הוא חוג חילופי עם יחידה. למה הוא לא שדה?
2. $(2\mathbb{Z},+,\cdot)$ הוא חוג חילופי בלי יחידה.
3. $(\mathbb{Z}_n,+,\cdot)$ הוא חוג חילופי עם יחידה. עבור n ראשוני, אפילו מדובר בשדה.
4. $\mathbb{Q}$ ו-$\mathbb{R}$ הם שדות עם הפעולות הרגילות של חיבור וכפל.
5. הקווטרניונים הרציונליים והקווטרניונים הממשיים הם חוגי חילוק לא חילופיים. עוד בדוגמה 1.12.
6. תהי X קבוצה. אז $(P(X),\triangle,\cap)$ הוא חוג חילופי עם יחידה, כאשר $P(X)$ זו קבוצת החזקה של X, $\triangle$ זו פעולת ההפרש הסימטרי, הקבוצה הריקה היא איבר האפס ו-X הוא איבר היחידה. האם זה שדה?

Left invertible

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

Unit

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

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

יהי $a + b\sqrt{2} \neq 0$. אז

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

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

Left zero divisor

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

Domain

Integral domain

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

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

1. $\mathbb{Z}$ הוא תחום שלמות.
2. $\mathbb{Z}_6$ אינו תחום כי $2 \cdot 3 \equiv 0 \pmod 6$.
3. לכל חוג חילופי R ו-$n > 1$, החוג $M_n(R)$ אינו תחום.
4. חוג עם חילוק הוא תחום.

1.2 תת־חוגים

Subring

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

Subrng

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

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

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

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

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

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

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

2 תרגול שני

Ring homomorphism

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

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

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

Epimorphism
Projection

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

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

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

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

ולכן $\varphi(1_R)=1_S$. כלומר זה אפימורפיזם של חוגים.

מה היה קורה אילו רק דרשנו ש-S הוא חוג בלי יחידה? הוכיחו שאז S הוא עדין חוג עם יחידה. □

Monomorphism
Embedding

דוגמה 2.5. 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.

Isomorphism
Isomorphic

הגדרה 2.6. 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 2.7. 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.

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

Image

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

Kernel

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

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

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

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

דוגמה 2.10. בחוג חילופי ההגדרות השונות של אידאל מתלכדות.

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

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

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

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

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

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

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

מסקנה 2.17. בחוג חילוק כל האידאלים הם טריוויאלים.

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

תרגיל 2.19. הוכיחו שחיתוך אידאלים הוא אידאל.

הגדרה 2.20. יהי R חוג, ויהי $x \in R$ איבר. האידאל שנוצר על ידי x הוא Ideal generated by x

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

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

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

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

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

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

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

Product of ideals

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

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

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

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

Comaximal ideals

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

3 תרגול שלישי

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

Principal ideal

Principal ideal domain (PID)

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

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

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

Simple

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

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

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

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

תרגיל 3.9. תנו דוגמה לחוגים R,S, הומומורפיזם $\varphi\colon R\to S$ ואידאל $I\lhd R$ כך ש-$\varphi(I)$ אינו אידאל של S.

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

Quotient ring

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

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

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

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

דוגמה 3.12. יהי p ראשוני, אז

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

Nilpotent

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

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

1. הוכיחו כי $N\lhd R$.
2. הוכיחו כי ב-R/N אין איברים נילפוטנטיים לא טריוויאליים (כלומר שונים מ-0).
3. תנו דוגמה לחוג לא חילופי שבו N אינו אידאל.

First isomorphism theorem

משפט 3.15 (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 3.16. 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 3.17. יהי R חוג, $R_0\subseteq R$ תת־חוג ו-$X\subseteq R$ תת־קבוצה. תת־החוג הנוצר (מעל R_0) על ידי X הוא חיתוך כל תת־החוגים $S\subseteq R$ המכילים את R_0 ואת X. נסמן תת־חוג זה בסימון $R_0[X]$. אם $R_0[X]=R$, אז נאמר כי R נוצר על ידי X.

Finitely generated

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

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

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

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

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

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

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

4 תרגול רביעי

תרגיל 4.1. יהיו $I \subseteq J$ אידאלים של R. הוכיחו שקיים אפימורפיזם $R/I \to R/J$.

משפט 4.2 (משפט האיזומורפיזם השלישי). יהיו $I \subseteq J$ אידאלים של חוג R. אז Third isomorphism theorem

$$\left. {}^{R/I} \middle/ {}_{J/I} \right. \cong \left. {}^{R} \middle/ {}_{J} \right.$$

הגדרה 4.3. אידאל נאות $I \lhd R$ נקרא אידאל מקסימלי אם לא קיים אידאל נאות שמכיל אותו ממש. Maximal ideal

דוגמה 4.4. בחוג $\mathbb{Z}/32\mathbb{Z}$ יש רק אידאל מקסימלי אחד והוא $2 \cdot \mathbb{Z}/32\mathbb{Z}$ (זה קיצור לכתיב $(2 + 32\mathbb{Z}) \cdot \mathbb{Z}/32\mathbb{Z}$). בחוג $\mathbb{Z}/45\mathbb{Z}$ יש שני אידאלים מקסימליים והם $3 \cdot \mathbb{Z}/45\mathbb{Z}$ ו-$5 \cdot \mathbb{Z}/45\mathbb{Z}$.

דוגמה 4.5. לכל מספר ראשוני p, האידאל $p\mathbb{Z} \lhd \mathbb{Z}$ הוא מקסימלי. האם יש עוד?

משפט 4.6. יהי R חוג. אידאל נאות $I \lhd R$ הוא מקסימלי אם ורק אם R/I הוא פשוט. אם בנוסף R חילופי, אז I מקסימלי אם ורק אם R/I שדה.

דוגמה 4.7. האידאל $\langle x, p \rangle \lhd \mathbb{Z}[x]$ הוא מקסימלי לכל מספר ראשוני p מפני שחוג המנה $\mathbb{Z}[x]/\langle x, p \rangle \cong \mathbb{F}_p$ הוא שדה. אבל $\langle x \rangle$ לא מקסימלי, כי $\mathbb{Z}[x]/\langle x \rangle \cong \mathbb{Z}$ אינו שדה (או כי $\langle x \rangle$ מוכל ממש ב-$\langle x, p \rangle$).

משפט 4.8 (משפט ההתאמה). יהי $I \lhd R$ אידאל. אז ההתאמה $A \mapsto A/I$ היא איזומורפיזם של סריגים בין האידאלים של R המכילים את I לבין האידאלים של R/I. ההתאמה שומרת הכלה, חיבור, כפל, חיתוך ומנות. Correspondence theorem

4.1 אידאלים ראשוניים

הגדרה 4.9. אידאל נאות $R \lhd I$ יקרא ראשוני אם לכל $A, B \lhd R$ המקיימים $AB \subseteq I$, אז $A \subseteq I$ או $B \subseteq I$. Prime

תרגיל 4.10. 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.

משפט 4.11. יהי R חוג חילופי. אז R הוא תחום שלמות אם ורק אם $\{0\}$ הוא אידאל ראשוני.

מסקנה 4.12. יהי R חוג. אז $I \lhd R$ ראשוני אם ורק אם $\{0\}$ הוא ראשוני בחוג המנה R/I.

תרגיל 4.13. יהי R חוג חילופי שבו כל האידאלים הם ראשוניים. הוכיחו כי R שדה.

תרגיל 4.14. יהי R חוג חילופי. הוכיחו שאם לכל $x \in R$ קיים $n > 1$ כך ש-$x^n = x$, אז כל אידאל ראשוני הוא מקסימלי.

5 תרגול חמישי

5.1 חוגים ראשוניים

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

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

משפט 5.2. חוג חילופי הוא ראשוני אם ורק אם הוא תחום שלמות.

תרגיל 5.3. יהי R חוג ראשוני. הראו שהמרכז $Z(R)$ הוא תחום שלמות.

תרגיל 5.4. ראינו כבר שתת־חוג של שדה הוא תחום שלמות. הפריכו את המקרה הלא חילופי: מצאו תת־חוג של חוג פשוט שאינו ראשוני.

5.2 מיקום מרכזי

הגדרה 5.5. 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 **5.6.** 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-$f = g \circ \iota$.

Local ring

הגדרה 5.7. יהי R חוג חילופי. נאמר שהוא חוג מקומי אם יש לו אידאל מקסימלי יחיד.

דוגמה 5.8. יהי $p \in \mathbb{Z}$ ראשוני. אז $S = \mathbb{Z} \setminus p\mathbb{Z}$ סגורה לכפל והחוג $\mathbb{Z}_{\langle p\rangle} = S^{-1}\mathbb{Z}$ הוא חוג מקומי. האידאל המקסימלי היחיד שלו הוא $\mathfrak{m} = p\mathbb{Z}_{\langle p\rangle}$.

כדי לראות ש-$\mathfrak{m}$ מקסימלי, אפשר להוכיח $\mathbb{Z}_{\langle p\rangle}/\mathfrak{m} \cong \mathbb{Z}/p\mathbb{Z}$ וזה שדה (האיזומורפיזם לא לגמרי טריוויאלי). כאשר R הוא תחום שלמות, אז אפשר לחשוב על מיקום שלו $S^{-1}R$ כמשוכן בשדה השברים של R (ראו הגדרה 5.9). 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.

Fraction field, or field of quotients

הגדרה 5.9. יהי R תחום שלמות. עבור $S = R \setminus \{0\}$ המיקום $S^{-1}R$ הינו שדה, הנקרא שדה השברים של R.

דוגמה 5.10. $\mathbb{Q}$ הוא שדה השברים של $\mathbb{Z}$.

משפט 5.11. נסתכל על התאמות בין שתי קבוצות של אידאלים

$$\begin{aligned} \{J \lhd S^{-1}R\} &\quad \{I \lhd R \,|\, I \cap S = \varnothing\} \\ S^{-1}I &\hookleftarrow I \\ J &\mapsto J \cap R \end{aligned}$$

1. ההתאמה $I \hookleftarrow S^{-1}I$ היא על.

2. ההתאמה $J \cap R \mapsto J$ היא חח"ע.

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

הערה 5.12. 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-$S^{-1}\mathbb{Z}$.

6 תרגול שישי

משפט 6.1 (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 6.2. בחוג מקומי R לכל $x \in R$ מתקיים ש-x הפיך או $1 - x$ הפיך.

מסקנה 6.3. בחוג מקומי אין אידמפוטנטים לא טריוויאלים.

הוכחה. נניח בשלילה $0 \neq e \in R$ 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 6.4. יהי $\mathfrak{m}$ אידאל מקסימלי בחוג R. הוכיחו שעבור $n \in \mathbb{N}$ החוג $R/\mathfrak{m}^n$ הוא חוג מקומי עם אידאל מקסימלי $\mathfrak{m}/\mathfrak{m}^n$.

תרגיל 6.5 (לבית)**.** מצאו את האיברים ההפיכים ב-$F[x]/\left\langle x^n \right\rangle$.

6.1 חוגי טורים פורמליים

הגדרה 6.6. יהי R תחום. חוג טורי לורן הפורמליים $R((x))$ כולל את כל הסכומים האינסופיים הפורמליים $\sum_{i=-n}^{\infty} a_i x^i$ עבור $n \in \mathbb{N}$ כלשהו ו-$a_i \in R$. הפעולות הן החיבור והכפל המוכללות מחוג הפולינומים. לחוג זה יש תת־חוג של טורי חזקות פורמליים $R[[x]]$ הכולל סכומים $\sum_{i=0}^{\infty} a_i x^i$. כקבוצה, טורי חזקות פורמליים הם $R^{\mathbb{N}}$, אבל כחוג פעולת הכפל היא לא רכיב־רכיב!

Formal Laurent series

Formal power series

דוגמה 6.7. בחוג $R[[x]]$ האיבר $1 - x$ הוא הפיך (השוו למצב ב-$R[x]$), אבל x אינו הפיך. לכן $R[[x]]$ אינו שדה.

6.2 חוגי פולינומים מעל תחומי שלמות

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

Divides

הגדרה 6.8. נאמר ש-a מחלק את b, ונסמן $a|b$, אם קיים $k\in R$ כך ש-$b=ak$.

דוגמה 6.9. ב-$\mathbb{Z}$ מתקיים $2|4$, אבל $4\nmid 3$. לעומת זאת $4|3$ ב-$\mathbb{Q}$.

Equivalent up to multiplication by a unit

הגדרה 6.10. 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.

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 $b=ak$ וגם $a=bm$, נציב ונקבל $b=bmk$. 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, $1\sim a$ אם ורק אם a הפיך אם ורק אם $Ra=R$.

תרגיל 6.11. מצאו את ההפיכים בחוגים $\mathbb{Z}$, $\mathbb{Z}[i]$, $F[x]$.

Ring of integers

הגדרה 6.12. 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

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

Norm

הגדרה 6.13. 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 $x=0$.

תרגיל 6.14. עבור $D=-3$ מצאו את ההפיכים ב-$\mathcal{O}_{-3}$.

טענה 6.15. 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.

7 תרגול שביעי

הגדרה 7.1. תמיד אפשר לפרק איבר $0 \neq a \in R$ בתחום שלמות כ-$a = au \cdot u^{-1}$ כאשר $u \in R^{\times}$ איבר הפיך. לפירוק כזה נקרא פירוק טריוויאלי.

Irreducible

נאמר שאיבר $0 \neq a \in R$ לא הפיך הוא אי פריק אם אין לו פירוק לא טריוויאלי.

טענה 7.2. 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 7.3. חשוב לדעת באיזה חוג נמצאים: האיבר x^2+1 הוא אי פריק ב-$\mathbb{R}[x]$, אבל פריק ב-$\mathbb{C}[x]$.

תרגיל 7.4. יהי $p \in R$ אי פריק, ויהי $q \sim p$. הוכיחו ש-q אי פריק.

תרגיל 7.5. 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 $N(x) = \pm 1$.

תרגיל 7.6. יהי $a \in \mathcal{O}_D$. הוכיחו שאם $N(a)$ אי פריק, אז a אי פריק.

תרגיל 7.7. הוכיחו ש-$a = 1 + \sqrt{-5} \in \mathcal{O}_{-5} = \mathbb{Z}\left[\sqrt{-5}\right]$ אינו פריק.

פתרון. נניח $a = xy$. אזי $6 = N(a) = N(x)N(y)$. 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 7.8. הוכיחו כי $\mathbb{Z}[\sqrt{-5}]$ אינו חוג ראשי. כלומר שקיים אידאל שלא נוצר על ידי איבר אחד.

Prime

הגדרה 7.9. 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 7.10. כל איבר ראשוני הוא אי פריק.

תרגיל 7.11. הראו כי $1 + i \in \mathbb{Z}[i]$ הוא ראשוני.

הערה 7.12. 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 7.13. 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

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

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

תרגיל 7.14. 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 $\varphi : \mathbb{Z}[x] \to \mathbb{Z}[\sqrt{-2}]$ 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.

הגדרה 7.15. תחום שלמות R נקרא אטומי אם לכל $0 \neq a \in R$ קיים פירוק לגורמים אי פריקים. Atomic domain

דוגמה 7.16. 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 7.17. 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 $\left(1+\sqrt{-7}\right)\left(1-\sqrt{-7}\right) = 2\cdot 2\cdot 2$, שהם שני פירוקים שונים לגורמים אי פריקים.