

מבוא לחוגים ומודולים
מערכי תרגול קורס 88-212

מהדורת קריאה מוקדמת

מאי 2017, גרסה 0.11

תוכן העניינים

3	מבוא	
4	תרגול ראשון	1
6	תרגול שני	2
8	תרגול שלישי	3
10	תרגול רביעי	4
11	תרגול חמישי	5
13	תרגול שישי	6
15	תרגול שביעי	7
17	תרגול שמיני	8

מבוא

כמה הערות טכניות לתחילת הקורס:

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

מחבר בשנת הלימודים תשע"ז: תומר באואר

1 תרגול ראשון

1.1 הגדרות בסיסיות

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

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

2. (R, \cdot) הוא חבורה למחצה.

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

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

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

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

Commutative

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

Ring

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

Unital ring

Division ring

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

Field

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

דוגמה 1.3. הרבה מבנים אלגבריים שפגשתם הם חוגים. למשל

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

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

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

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

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

עוד בדוגמה 1.12

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

Left invertible

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

Unit

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

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

יהי $a + b\sqrt{2} \neq 0$ אז

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

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

Left zero divisor

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

Domain

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

Integral domain

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

1. \mathbb{Z} הוא תחום שלמות.

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

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

4. חוג עם חילוק הוא תחום.

1.2 תת-חוגים

Subring

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

Subrng

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

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

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

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

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

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

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

2 תרגול שני

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

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

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

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

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

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

Epimorphism
Projection

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

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

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

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

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

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

Monomorphism
Embedding

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

Isomorphism
Isomorphic

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

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

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

Image

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

Kernel

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

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

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

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

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

דוגמה 2.10. בחוג חילופי ההגדרות השונות של אידיאל מתלכדות.

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

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

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

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

תרגיל 2.15. יהי R חוג, ויהי $I \triangleleft R$ אידיאל. הוכיחו שאם $1 \in I$, אז $I = R$. פתרו. לפי הגדרה, לכל $r \in R$, $i \in I$ מתקיים $r \cdot i \in I$. בפרט $r \cdot 1 = r \in I$. לכן $I = R$.

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

מסקנה 2.17. בחוג חילוק כל האידיאלים הם טריוויאליים.

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

תרגיל 2.19. הוכיחו שחיתוך אידיאלים הוא אידיאל.

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

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

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

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

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

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

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

Product of ideals

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

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

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

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

Comaximal
ideals

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

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

3 תרגול שלישי

Principal ideal

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

Principal ideal
domain (PID)

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

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

Simple

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

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

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

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

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

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

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

Quotient ring

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

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

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

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

דוגמה 3.12. יהי p ראשוני, אז

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

Nilpotent

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

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

1. הוכיחו כי $N \triangleleft R$.

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

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

First isomorphism theorem

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

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

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

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

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

Subring generated by X

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

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

Finitely generated

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

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

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

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

Evaluation map

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

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

4 תרגול רביעי

תרגיל 4.1. יהיו $I \subseteq J$ אידיאלים של R . הוכיחו שקיים אפימורפיזם $R/I \rightarrow R/J$.

Third isomorphism theorem

משפט 4.2 (משפט האיזומורפיזם השלישי). יהיו $I \subseteq J$ אידיאלים של חוג R . אז

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

Maximal ideal

הגדרה 4.3. אידיאל נאות $I \triangleleft R$ נקרא אידיאל מקסימלי אם לא קיים אידיאל נאות שמכיל אותו ממש.

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

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

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

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

Correspondence theorem

משפט 4.8 (משפט ההתאמה). יהי $I \triangleleft R$ אידיאל. אז ההתאמה $A \mapsto A/I$ היא איזומורפיזם של סריגים בין האידיאלים של R המכילים את I לבין האידיאלים של R/I . ההתאמה שופרת הכלה, חיבור, כפל, חיתוך ופנות.

4.1 אידאלים ראשוניים

Prime

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

4.10 תרגיל. 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.

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

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

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

4.14 תרגיל. 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

Prime ring

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

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

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

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

5.4 תרגיל. 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

5.5 הגדרה. יהי R חוג ותהי $S \subseteq R$ תת-קבוצה המקיימת:

1. כל איברי S הם רגולריים (כלומר לא מחלקי אפס).

2. S סגורה לכפל.

$$S \subseteq Z(R) \quad .3$$

$$1 \in S \quad .4$$

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 המיקוס של R -ב- S .

Localization

הערה 5.6. יש מונומורפיזם טבעי $\iota: R \rightarrow S^{-1}R$ לפי $\iota(r) = \frac{r}{1}$. הוא שולח את איברי S לאיברים הפיכים. התכונה האוניברסלית של מיקוס היא שאם $f: R \rightarrow T$ הוא הומומורפיזם של חוגים כך ש- $f(S) \subseteq T^\times$, אז קיים הומומורפיזם יחיד $g: S^{-1}R \rightarrow T$ 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 $\mathbb{Z}_{(p)} = S^{-1}\mathbb{Z}$ הוא חוג מקומי. האידאל המקסימלי היחיד שלו הוא $\mathfrak{m} = p\mathbb{Z}_{(p)}$. כדי לראות ש- \mathfrak{m} מקסימלי, אפשר להוכיח $\mathbb{Z}_{(p)}/\mathfrak{m} \cong \mathbb{Z}/p\mathbb{Z}$ וזה שדה (האיזומורפיזם לא לגמרי טריוויאלי). כאשר R הוא תחום שלמות, אז אפשר לחשוב על מיקוס שלו $S^{-1}R$ כמשוכן בשדה השברים של R (ראו הגדרה 5.9). לכן יותר קל לחשוב על החוג בתור הקבוצה

$$\mathbb{Z}_{(p)} = \left\{ \frac{a}{b} \in \mathbb{Q} \mid p \nmid b \right\}$$

$$\mathfrak{m} = \left\{ \frac{a}{b} \in \mathbb{Q} \mid p \mid a, p \nmid b \right\}$$

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

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

Fraction field, or field of quotients

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

משפט 5.11. נסתכל על התאמות בין שתי קבוצות של אידאלים

$$\{J \triangleleft S^{-1}R\} \quad \{I \triangleleft R \mid I \cap S = \emptyset\}$$

$$S^{-1}I \leftrightarrow I$$

$$J \mapsto J \cap R$$

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

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

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

הערה 5.12. יתכן מצב שבו $I_0 \in \{I \triangleleft R \mid I \cap S = \emptyset\}$ אינו ראשוני, אבל $S^{-1}I_0$ כן ראשוני ב- $S^{-1}R$. למשל, $6\mathbb{Z} \triangleleft \mathbb{Z}$ אינו ראשוני, וכאשר נבחר את $S = \{2^k \mid k \in \mathbb{N}\}$, 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 $e \in R$, $e \neq 0$ 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 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- $F[x]/\langle x^n \rangle$.

6.1 חוגי טורים פורמליים

Formal Laurent series

Formal power series

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!

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- $ak = b$.

דוגמה 6.9. ב- \mathbb{Z} מתקיים $2|4$, אבל $3 \nmid 4$. לעומת זאת $3|4$ 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 $ak = b$ 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 6.11. מצאו את ההפיכים בחוגים $\mathbb{Z}, \mathbb{Z}[i], \mathbb{Z}[x]$.

Ring of integers

הגדרה 6.12. יהי $D \in \mathbb{Z}$ חופשי מריבועים. עבור השדה $\mathbb{Q}[\sqrt{D}] = \{a + b\sqrt{D} \mid a, b \in \mathbb{Q}\}$ נגדיר את חוג השלמים שלו להיות

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

Norm

הגדרה 6.13. יהי $D \in \mathbb{Z}$ חופשי מריבועים. נגדיר לכל איבר $\alpha = a + b\sqrt{D}$ את הנורמה לפי $N: \mathcal{O}_D \rightarrow \mathbb{Z}$

$$N(\alpha) = \alpha\bar{\alpha} = (a + b\sqrt{D})(a - b\sqrt{D})$$

שימו לב שהאינוולוציה $\bar{\alpha}$ 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 6.14. משוואת פל היא כל משוואה דיופנטית מן הצורה

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

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

בעיה 6.15 (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 $\alpha' > \alpha'^{-1} > 0$.

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

6.17. טענה 6.17. 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

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

Irreducible

7.2. טענה 7.2. התנאים הבאים שקולים:

1. a אי פריק.

2. אם $a = xy$, אז $a \sim x$ או $a \sim y$.

3. אם $a = xy$, אז x הפיך או y הפיך.

4. אם $a = xy$, אז $a \sim x$ או x הפיך.

5. אם $x|a$, אז $a \sim x$ 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- $\mathcal{O}_{-5} = \mathbb{Z}[\sqrt{-5}]$ אינו פריק.

פתרו. 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 $p \in R$, $0 \neq p$ 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

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

אבל 3 לא מחלק את $4 \pm \sqrt{10}$ משיקולי נורמה. כלומר אם $(4 \pm \sqrt{10}) = 3\alpha$ 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 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 $\varphi : \mathbb{Z}[x] \rightarrow \mathbb{Z}[\sqrt{-2}]$ 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 האידיאל $\langle x^2 + 2 \rangle$ הוא ראשוני, ולכן $x^2 + 2$ ראשוני.

8 תרגול שמיני

הגדרה 8.1. תחום שלמות R נקרא אטומי אם לכל $0 \neq a \in R$ קיים פירוק לגורמים אי פריקים.

דוגמה 8.2. הנה רשימה של כמה תחומים אטומיים: \mathbb{Z} , כל שדה F (באופן ריק), כל חוג שלמים ריבועיים \mathcal{O}_D , ו- $F[x]$ ו- $\mathbb{Z}[x]$.

הגדרה 8.3. חוג אטומי R יקרא תחום פריקות יחידה (תפ"י) אם בכל שני פירוקים של אותו איבר

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

Unique factorization domain (UFD)

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

דוגמה 8.4. החוג $\mathbb{Z}[\sqrt{10}]$ אינו תחום פריקות יחידה, שכן $(4 + \sqrt{10})(4 - \sqrt{10}) = 6 = 2 \cdot 3$. ראינו כי האיברים בפירוקים הם אי פריקים. נשאר להוכיח שהאיברים מפירוקים שונים לא חברים. זה קל להוכיח מחישוב הנורמות.

משפט 8.5. כל תחום ראשי הוא תחום פריקות יחידה.

מסקנה 8.6. החוג $\mathbb{Z}[\sqrt{10}]$ אינו ראשי.

משפט 8.7. יהי R תחום ראשי. אז $p \in R$ אי פריק אם ורק אם הוא ראשוני.

תרגיל 8.8. יהי p מספר ראשוני אי זוגי, ויהי $D \in \mathbb{Z}$ כך ש- $D \not\equiv 1 \pmod{p}$. הוכיחו שאם למשוואה

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

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

הגדרה 8.9. יהי R תחום שלמות. פונקציה $d : R \rightarrow \mathbb{N} \cup \{0, -\infty\}$ המקיימת $d(0) < d(x)$ לכל $x \neq 0$ נקראת פונקציה אוקלידית אם

Euclidean function

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

2. $d(a) \leq d(b)$ לכל $a|b$.

Euclidean domain

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

דוגמה 8.10. 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.

תרגיל 8.11. הראו שהחוג $\mathbb{Z}[x]$ אינו תחום אוקלידי.

תרגיל 8.12. יהי F שדה. הוכיחו ש- $F[[x]]$ תחום אוקלידי.

תרגיל 8.13. 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).