תורת החוגים: חוברת תרגילים

עוזי וישנה

מהדורה 5.1

חוברת תרגילים זו מלווה את הקורס 'מבנים אלגבריים 2' (88-212) באוניברסיטת בר־אילן. החומר התאורטי מכוסה בחוברת אחרת ("מבוא לחוגים ומודולים"), וסדר הנושאים שם, לרבות מספרי הסעיפים ותת־הסעיפים, נשמר. למרות שחוברת זו נועדה בעיקר לספק אפשרויות לתרגול עצמי, המשפטים היסודיים, טענות עזר ושיטות סטנדרטיות, מופיעות כאן כשהן מחופשות לתרגילים, עם הדרכה או רמז המהווים לפעמים פתרון מלא.

התרגילים (כולל הטענות והמשפטים) מלווים בציון רמת הקושי: תרגילים קלים (1) דורשים בדרך־כלל שליטה בהגדרות ותו לא. תרגילים טכניים מורכבים, לא רגילים או סתם קשים סומנו ב־ (3). שאר התרגילים קיבלו את הציון (2), (2+) או (2−). מספר התרגילים מספיק כדי לפתור חלק מן התרגילים בכיתה, חלק כתרגילי בית, ואת השאר לקראת המבחן. במספר מקומות הרחבנו מעבר לרמה הנדרשת בקורס. לעומת זאת, החוברת אינה נוגעת במודולים.

אודה למי שיביא לתשומת ליבי שגיאות מתמטיות, דקדוקיות או טיפוגרפיות, לרבות מיקום שגוי של תרגילים, ובפרט למי שיציע דרך להתגבר על ההיפוך המוזר ש־LaTeX כופה על שמות הפרקים.

עוזי וישנה, אדר תשע"א.

תוכן עניינים

1 חוגים ואידיאלים **7**

1.1 מבוא ־ מושגי יסוד ודוגמאות 7

1.1.1 איברים של חוגים 7

אברי יחידה 8

אברים הפיכים 8

מחלקי אפס 9

המאפיין 10

1.1.2 תת־חוגים 10

המרְכָּז והמרכֵּז 10

יוצרים של תת־חוג 11

1.1.3 דוגמאות ובניה של חוגים 11

מטריצות 11

פולינומים 12

אלגברות 13

אלגברת הקווטרניונים 13

טורי לורן 14

מכפלה ישרה של חוגים 14

1.2 אידיאלים וחוגי מנה 14

1.2.1 אידיאלים חד־צדדיים ודו־צדדיים 14

איחוד וחיתוך 15

אידיאלים אמיתיים 16

אידיאלים של חוגים מיוחדים 16

1.2.2 סכום ומכפלה של אידיאלים 16

סכומים סופיים וכלליים 16

מכפלה 16

סריג האידיאלים 17

מאפסים 17

1.2.3 חוגי מנה 18

1.2.4 הומומורפיזמים 18

הומומורפיזמים של חוגים בלי יחידה 18
הגרעין והתמונה 19
הומומורפיזמים ומכפלה פנימית 19
1.2.5 משפטי האיזומורפיזמים 19
תת־החוג היסודי 20
הומומורפיזם ויוצרים 20

2 אידיאלים ראשוניים ומקסימליים **21**
2.1 אידיאלים מקסימליים 22
אידיאלים מינימליים 23
2.1.1 הלמה של צורן 23
2.1.2 חוגים פשוטים 23
2.1.3 אידיאלים ראשוניים 23
חוגים ראשוניים 23
אידיאלים ראשוניים 24
2.1.4 פירוק למכפלה ישרה 25
אידיאלים קו־מקסימליים 25
משפט השאריות הסיני 25
אידמפוטנטים 27

3 תחומי שלמות **29**
3.1 מיקום ושדה השברים 29
3.1.1 מיקום מרכזי 29
3.1.2 שדה השברים 29
חוג השברים הטוטאלי 31
3.1.3 חוגים מקומיים 31
3.2 חוגי שלמים 31
3.2.1 איברים הפיכים 34
3.3 איברים ראשוניים ואי־פריקים 35
3.3.1 יחס החלוקה 35
תאור לפי אידיאלים 35
3.3.2 איברים הפיכים 36
3.3.3 איברים אי־פריקים 36
3.3.4 איברים ראשוניים 36
3.4 פירוק לגורמים 36
3.4.1 חוגים אטומיים 38
3.4.2 תחומי פריקות יחידה 38
3.4.3 חוגים נותריים 39
3.4.4 תחומים ראשיים 39
מחלק משותף מקסימלי 41

תחומי Bezout 43
כפולה משותפת מינימלית 43
3.4.5 חוגים אוקלידיים 43
אוקלידיות של חוגי שלמים 45
הקשר בין האקסיומות $(E1)$ ו־$(E2)$ 46
תנאי הכרחי לאוקלידיות 46

4 פולינומים ושדות **47**
4.1 מבוא לתורת השדות 47
4.1.1 ממד של אלגברות 47
4.1.2 הפולינום המינימלי 48
4.1.3 שורשים ושדה מפצל 50
סיפוח שורשים 52
4.2 פירוק של פולינומים 54
4.2.1 שורשים רציונליים 54
4.2.2 קריטריון אייזנשטיין 55
4.2.3 הלמה של גאוס 55
תכולה של פולינום 56
הלמה של גאוס 56
פירוק פולינומים מעל תחום פריקות יחידה 56

פרק 1

חוגים ואידיאלים

1.1 מבוא - מושגי יסוד ודוגמאות

חוג (בלי יחידה) הוא קבוצה R, עם פעולות בינאריות $+, *$ ואיבר מיוחד $0 \in R$, כך ש- $\langle R; +; 0\rangle$ חבורה קומוטטיבית, והפעולה $*$ אסוציאטיבית, ודיסטריבוטיבית ביחס ל- $+$ (דוגמא: $\mathbb{Z}$).

תרגיל 1.1.1 (**) איזה מן המבנים הבאים הוא חוג? מצא את איבר האפס שלו, והראה שהאחרים אינם חוגים:

א. $\mathbb{Z}$ עם החיבור הרגיל והכפל $a * b = 2ab - a^2 - b^2$.

ב. אוסף הפולינומים ממעלה 4 מעל הרציונליים.

ג. המספרים הרציונליים, עם הפעולות $a \oplus b = a + b - 1$, $a \odot b = a + b - ab$.

ד. אוסף המטריצות $\left\{ \begin{pmatrix} 0 & a \\ b & c \end{pmatrix} : a, b, c \in \mathbb{R} \right\}$.

תרגיל 1.1.2 (**) הראה שהקבוצות הבאות אינן חוגים.

א. $\mathbb{R}^+ = \{x : x > 0\}$ עם החיבור $x \oplus y = xy$ והכפל $x \odot y = xy$.

ב. עם החיבור $x \oplus y = xy$ והכפל $x \odot y = x + y$.

ג. עם החיבור $x \oplus y = x + y - 1$ והכפל $x \odot y = xy - 1$.

תרגיל 1.1.3 (-)** יהי C אוסף הפונקציות הרציפות $\mathbb{R} \to \mathbb{R}$. חיבור וכפל של פונקציות מוגדר כרגיל לפי $(f + g)(x) = f(x) + g(x)$, $(f \cdot g)(x) = f(x)g(x)$. הוכח ש-$C$ חוג עם יחידה.

1.1.1 איברים של חוגים

תרגיל 1.1.4 (**) הוכח את הזהויות הבאות: א. $0 = -0$.

ב. $0 \cdot a = 0 = a \cdot 0$.

ג. $(-a) \cdot b = -(a \cdot b)$ ובפרט $(-1) \cdot b = -b$.

ד. $(-a)\cdot(-b)=a\cdot b$.

חוג קומוטטיבי הוא חוג שבו פעולת הכפל קומוטטיבית. חוג קומוטטיבי עם חילוק נקרא **שדה**.

תרגיל 1.1.5 (**) אם החבורה החיבורית של חוג היא ציקלית, אז החוג הוא קומוטטיבי.

תרגיל 1.1.6 (**) יהי R חוג המקיים $x^2=x$ לכל $x\in R$. הוכח:
א. $x+x=0$ לכל $x\in R$.
ב. R קומוטטיבי.

תרגיל 1.1.7 (־*)** יהי R חוג (בלי יחידה) המקיים $x^2=0$ לכל $x\in R$. הוכח:
א. $ab+ba=0$.
ב. $aba=0$.
ג. $abc+cba=0$.
ד. $abc+abc=0$.

תרגיל 1.1.8 (**) נניח ש־ $a,b\in R$ מקיימים $ab=a$, $ba=b$. הוכח ש־ $a^2=a$ ו־ $b^2=b$.

אברי יחידה

איבר $e\in R$ נקרא **יחידה מימין** אם $xe=x$ לכל $x\in R$, ויחידה **משמאל** אם $ex=x$ לכל $x\in R$. איבר המקיים $\forall x: ex=x=xe$ נקרא **יחידה**.

תרגיל 1.1.9 (*) אם e_1 יחידה מימין ו־ e_2 יחידה משמאל, אז $e_1=e_2$ וזהו איבר יחידה.
חוג שבו קיים איבר יחידה נקרא חוג עם יחידה.

תרגיל 1.1.10 (**) הוכח את הקומוטטיביות של החיבור $(a+b=b+a)$ מתוך האקסיומות האחרות של חוג עם יחידה. רמז. העזר בדיסטריבוטיביות.

תרגיל 1.1.11 (**) הוכח ש־ $\mathbb{Z}_{12}$ עם החיבור הרגיל והכפל $x*y=5xy$ הוא חוג עם יחידה.

אברים הפיכים

יהי R חוג עם יחידה, ויהי $x\in R$. אם קיים $y\in R$ כך ש־ $yx=1$, אומרים ש־ x **הפיך משמאל**. אם קיים $z\in R$ כך ש־ $xz=1$, אומרים ש־ x **הפיך מימין**. אם קיים $u\in R$ כך ש־ $xu=ux=1$, אז x **הפיך**.

תרגיל 1.1.12 (־)** אם x הפיך מימין והפיך משמאל, אז הוא הפיך.

אם R חוג, מסמנים ב־ $R^\times$ את אוסף האברים ההפיכים

תרגיל 1.1.13 (*) $R^\times$ חבורה (ביחס לכפל של החוג).

תרגיל 1.1.14 (**) אם $1-ab$ הפיך בחוג אז $1-ba$ הפיך. רמז: חישבו על האיבר

$$1+b(1-ab)^{-1}a.$$

חוג עם יחידה שבו כל איבר הפיך נקרא **חוג עם חילוק**.

תרגיל 1.1.15 (**) אם כל איבר $x \neq 0$ בחוג R הפיך משמאל, אז R הוא חוג עם חילוק.

תרגיל 1.1.16 (***) יהי R חוג שבו $R^\times$ קבוצה סופית; נסמן את סכום האיברים ב־ $R^\times$ ב־ x.

א. הוכח ש־ $x^2 = x$ או $x^2 = 0$. (הדרכה: לכל u הפיך, $ux = x$.)

ב. אם $2 \neq 0$ בחוג אז $x = 0$.

ג. חשב את x בחוגים $\mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}/4\mathbb{Z}$ ו־ $\mathbb{F}_2[\epsilon \mid \epsilon^2 = 0]$.

מחלקי אפס

איבר $x \in R$ הוא מחלק אפס ימני אם קיים $a \neq 0$ כך ש־ $ax = 0$, ומחלק אפס שמאלי אם קיים $a \neq 0$ כך ש־ $xa = 0$.

תרגיל 1.1.17 (+*) $a \neq 0$, ו־ $xax = 0$. הוכח ש־ x מחלק אפס ימני או שמאלי.

תרגיל 1.1.18 (**) תאר במפורש את כל מחלקי־אפס הימניים בחוג $\mathrm{M}_2(\mathbb{R})$.

הגדרה 1.1.19 **$a \in R$ נקרא איבר נילפוטנטי אם $a^n = 0$ לאיזשהו $n \geq 1$.**

תרגיל 1.1.20 (+*) כל איבר נילפוטנטי הוא מחלק אפס.

תרגיל 1.1.21 (**) יהי $a \in R$ איבר נילפוטנטי. הוכח ש־ $(1-a)$ הפיך. הדרכה. הסכום האינסופי $\sum_{i=0}^{\infty} a^i$ מוגדר.

תרגיל 1.1.22 (**) מצא את כל האברים הנילפוטנטיים ב־ $\mathbb{Z}_{180}$.

המאפיין

הגדרה. יהי R חוג קומוטטיבי עם יחידה. המספר הטבעי הקטן ביותר n המקיים $\underbrace{1+1+\cdots+1}_{n \text{ פעמים}} = 0$ נקרא המאפיין של R. אם אין כזה, נאמר ש R בעל מאפיין 0. את המאפיין מסמנים ב־ $charR$.
דוגמא. $char\mathbb{Q} = 0$. דוגמא. $char\mathbb{Z}_n = n$.

תרגיל 1.1.23 (*) אם R תחום שלמות אז $charR = p$ (p ראשוני) או $charR = 0$.

תרגיל 1.1.24 (+*) אם F שדה סופי אז $charF = p$ (p ראשוני).

תרגיל 1.1.25 (־)** בשדה ממאפיין p מתקיים $(a+b)^p = a^p + b^p$.

תרגיל 1.1.26 (**) יהי D תחום ממאפיין p. הוכח ש־ $\varphi : a \mapsto a^p$ הוא מונומורפיזם של D.

1.1.2 תת־חוגים

$S \subseteq R$ הוא תת־חוג אם S תת־חבורה חיבורית, ו־ S סגור לכפל.
אם R הוא חוג עם יחידה, אז $S \subseteq R$ הוא תת־חוג־עם יחידה אם $1_R \in S$ (במקרה זה $1_R = 1_S$).

תרגיל 1.1.27 (**) נסמן $S = \left\{ \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} : a \in \mathbb{Q} \right\}$, $D = \left\{ \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} : a, b \in \mathbb{Q} \right\}$, $U = \left\{ \begin{pmatrix} a & c \\ 0 & b \end{pmatrix} : a, b, c \in \mathbb{Q} \right\}$, $T = \left\{ \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} : a, b \in \mathbb{Q} \right\}$, $R = \mathrm{M}_2(\mathbb{Q})$.
D הוא תת־חוג־עם יחידה של U, ו־ U תת־חוג עם יחידה של R; S הוא חוג עם יחידה, אבל אינו תת־חוג־עם־יחידה של D; T הוא חוג בלי יחידה.

תרגיל 1.1.28 (**) הראה ש־ $A_d = \left\{ n + m\sqrt{d} : n, m \in \mathbb{Z} \right\}$ הוא תת־חוג של $\mathbb{R}$. מצא את $A_2 \cap A_7$. האם $A_{12} \cap A_8$ תת־חוג של A_2?

המרְכָּז והמרכֵּז

הגדרה 1.1.29 ה**מרכז** של חוג R הוא $Z(R) = \{z \in R : (\forall x) zx = xz\}$.

טענה [2]. המרכז $Z(R)$ הוא תת־חוג קומוטטיבי של R.

הגדרה 1.1.30 יהי $S \subseteq R$ תת־חוג. ה**מרכז** (ריש קמוצה) של S ב־ R הוא

$$C_R(S) = \{z \in R : (\forall x \in S) xz = zx\}$$

תרגיל 1.1.31 (*) $C_R(S)$ הוא תת־חוג של R.

תרגיל 1.1.32 (+*) $S \subseteq C_R(C_R(S))$.

תרגיל 1.1.33 (***) תן דוגמא לחוג R עם תת־חוג S, כך ש־ $S \subset C_R(C_R(S))$.

תרגיל 1.1.34 (+)** $C_R(C_R(C_R(S))) = C_R(S)$.
אחד המשפטים היסודיים עבור אלגברות פשוטות קובע שאם S תת־אלגברה פשוטה של אלגברה פשוטה R, אז $C_R(C_R(S)) = S$.

יוצרים של תת־חוג

1.1.3 דוגמאות ובניה של חוגים

תרגיל 1.1.35 (*) יהי R חוג. נגדיר חוג R^{op} עם אותה חבורה חיבורית, וכפל $a * b = ba$.

תרגיל 1.1.36 (+*) הוכח ש־ R^{op} חוג; אם R חוג עם יחידה, גם R^{op} חוג עם יחידה.

תרגיל 1.1.37 (**) $(R^{op})^{op} = R$. אם R קומוטטיבי, $R^{op} = R$.

תרגיל 1.1.38 (**) יהי R חוג עם יחידה, כך ש־ תת־חוג עם יחידה שלו, וכך שכחבורה חיבורית, R איזומורפי ל־ $\mathbb{Z} \oplus \mathbb{Z}_p$ (p הוא מספר ראשוני).
א. הוכח שעד־כדי איזומורפיזם, יש לכל היותר שני חוגים R כנ"ל.
ב. חשב בכל אחד מהם את הקבוצה $\{z : z^2 = 0\}$, והסק שהם אינם איזומורפיים.

מטריצות

יהי R חוג. חוג המטריצות מעל R הוא החוג $\mathrm{M}_n(R)$ שאיבריו מטריצות $n \times n$ עם רכיבים ב־ R.

תרגיל 1.1.39 (**) הראה שכפל מטריצות $(AB)_{ij} = \sum A_{ik}B_{kj}$ הוא אסוציאטיבי, ולכן $\mathrm{M}_n(R)$ חוג.

תרגיל 1.1.40 (*) אם R חוג עם יחידה, אז גם $\mathrm{M}_n(R)$ חוג עם יחידה.
את הגדרת הדטרמיננטה $\det : \mathrm{M}_n(R) \to R$ המוכרת משדות אפשר להכליל לכל חוג קומוטטיבי R.

תרגיל 1.1.41 (+)** העזר בנוסחת Cramer כדי להראות שאם $|A|$ הפיך ב־ R, אז A הפיך ב־ $M_n(R)$.

תרגיל 1.1.42 (**) R חוג עם יחידה. מצא ב־ $\mathrm{M}_n(R)$ אברים $e_{ij} : 1 \leq i, j \leq n$ כך ש־ $e_{ij}e_{kl} = \delta_{jk}e_{il}$. הוכח ש־ $(I + re_{ij})^{-1} = (I - re_{ij})$ לכל $i \neq j$.

תרגיל 1.1.43 (+)** יהי R חוג כלשהו. מצא את $Z(\mathrm{M}_n(R))$.

תהי G חבורה אבלית. על אוסף ההומומורפיזמים

$$End(G) = \{\varphi : G \to G : \varphi(x+y) = \varphi(x) + \varphi(y)\}$$

מוגדרות פעולות של חיבור (לפי רכיבים) וכפל פונקציות (דהיינו הרכבה).

תרגיל 1.1.44 (+)** הוכח ש־ $End(G)$ חוג עם יחידה.

תרגיל 1.1.45 (**) כתוב דוגמא מפורשת המראה ש־ $End(G)$ אינו בהכרח קומוטטיבי.

תרגיל 1.1.46 (***) חשב את חוג האנדומורפיזמים של $R = \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/25\mathbb{Z}$.

פולינומים

יהי R חוג. חוג הפולינומים במשתנה אחד מעל R הוא החוג

$$R[\lambda] = \left\{a_0 + a_1\lambda + a_2\lambda^2 + \cdots + a_n\lambda^n : a_i \in R\right\}$$

עם החיבור והכפל המתאימים.

תרגיל 1.1.47 (**) הראה ש־ $R[\lambda]$ הוא חוג.

תרגיל 1.1.48 (**) הראה שקיים שיכון $R \to R[\lambda]$.

תרגיל 1.1.49 (־)** $a \in R[\lambda]$ הפיך אם ורק אם $a \in R$ והפיך שם.

תרגיל 1.1.50 (**) $\mathrm{M}_n(R[\lambda]) \cong (\mathrm{M}_n(R))[\lambda]$.

תרגיל 1.1.51 (**) $(R \times S)[\lambda] \cong R[\lambda] \times S[\lambda]$.

תרגיל 1.1.52 (+)** $Z(R[\lambda]) = (Z(R))[\lambda]$.

תרגיל 1.1.53 (**) יהי R חוג, $I = \langle\lambda\rangle \lhd R[\lambda]$. הוכח ש־ $R[\lambda]/\langle\lambda\rangle \cong R$.

תרגיל 1.1.54 (**) מצא עבור אילו איברים $a \in R$ קיים אוטומורפיזם $R[\lambda] \to R[\lambda]$ המקיים $\lambda \mapsto a\lambda$.

הערה. הסוגריים "[ ]" משמשות בשני תפקידים דומים. האחד, בניה של חוגי פולינומים: λ הוא משתנה חדש, ו־ $R[\lambda]$ הוא חוג הפולינומים. השני, בניה של תת־חוגים. אם $R \subseteq S$ ו־ $s \in S$, אז $R[s]$ הוא תת־החוג של S הכולל את כל הפולינומים ב־ s: $R[s] = \{a_0 + \cdots + a_n s^n : a_i \in R\}$. אם חושבים על λ כעל איבר של חוג הפולינומים, אז שתי המשמעויות מתלכדות בביטוי $R[\lambda]$.

תרגיל 1.1.55 (**) הסבר מדוע $R[x_1] \cong R[x_2]$ והסק שגם $(R[x_1])[x_2] \cong (R[x_3])[x_4]$.

תרגיל 1.1.56 (**) נסמן $R[x,y] = (R[x])[y]$. הוכח ש־ $(R[y])[x] = R[x,y]$ (מה התפקיד של כל '[ ]'?).

יהי F שדה. נגדיר פונקצית מעלה **לפי** $deg : F[x] \to \mathbb{R}$ $\deg(a_0 + a_1x + \cdots + a_nx^n) = \max i : a_i \neq 0$ (כלומר, החזקה הגבוהה ביותר של x המופיע בפולינום). $deg(0) = 0$.

תרגיל 1.1.57 (*) אם $c \in F$ אז $deg(c) = 0$.

תרגיל 1.1.58 (*) הוכח ש־ $deg(fg) = deg(f) + deg(g)$, והסק ש־ $F[x]$ תחום שלמות.

אלגברות

יהיו F שדה ו־ G חבורה.
על המרחב הוקטורי $F[G] = sp_F(G)$ נגדיר פעולת כפל:

$$\left(\sum_{g\in G} \alpha_g g\right)\left(\sum_{h\in G} \beta_h h\right) = \sum_{k\in G}\left(\sum_{g} \alpha_g \beta_{g^{-1}k}\right)k.$$

תרגיל 1.1.59 (**) הראה ש־ $F[G]$ חוג.

תרגיל 1.1.60 (****) הראה שאם $2 \neq 0$ בשדה F, אז $F[\mathbb{Z}_4] \cong F[\mathbb{Z}_2 \times \mathbb{Z}_2]$.

אלגברת הקווטרניונים

נסמן $\mathbb{H} = \{a + bi + cj + dk : a,b,c,d \in \mathbb{R}\}$, חוג הקווטרניונים, עם כפל המוגדר לפי הכללים $i^2 = j^2 = k^2 = -1$, $ij = k$, $jk = i$, $ki = j$.

תרגיל 1.1.61 (*) הראה ש־ $ji = -k$.
נגדיר העתקה $x \mapsto \bar{x}$ לפי $a + bi + cj + dk = a - bi - cj - dk$.

תרגיל 1.1.62 (**) חשב: $\overline{\overline{x}} = x$; $\overline{x+y} = \overline{x} + \overline{y}$; $\overline{xy} = \overline{y} \cdot \overline{x}$.
נגדיר $N : \mathbb{H} \to \mathbb{R}$ לפי $N(a + bi + cj + dk) = a^2 + b^2 + c^2 + d^2$.

תרגיל 1.1.63 (**) חשב: $N(x) = xx$.

תרגיל 1.1.64 (**) (בלי לחשב): $N(x) = xx$; $N(xy) = N(x)N(y)$.

תרגיל 1.1.65 (**) הסק: $\mathbb{H}$ חוג עם חילוק.

תרגיל 1.1.66 (+)** מצא איברים לא הפיכים בחוג

$$\mathbb{H}' = \{a + bi + cj + dk : a, b, c, d \in \mathbb{Z}\}.$$

טורי לורן

תרגיל 1.1.67 (+)** מצא נוסחה למקדמים של $(1 - x - x^2)^{-1} \in \mathbb{Z}[[x]]$.

אם $f \in R((x))$, מסמנים ב־$\bar{f}$ את המקדם המוביל (הנמוך ביותר) של f.

תרגיל 1.1.68 (+)** מצא איבר הפיך של $\mathbb{Z}_4((x))$ כך ש־$\bar{f} = 2$.

תרגיל 1.1.69 (***) הוכח את ההכלות $\mathbb{Q}[[x]][[y]] \subseteq \mathbb{Q}[y][[x]] \subseteq [[y]][[x]] \subseteq [[x]][y]$ $\mathbb{Q}[[y]]((x)) \subseteq \mathbb{Q}((x))[[y]]$, והראה שאף אחת מהן אינה שוויון.

תרגיל 1.1.70 (***) יהי F שדה. קבע את כל יחסה הכלה בין 18 החוגים $F\alpha\beta$ ו־$F\beta\alpha$ כאשר $\alpha \in \{[x], [[x]], ((x))\}$, $\beta \in \{[y], [[y]], ((y))\}$.

מכפלה ישרה של חוגים

תרגיל 1.1.71 (**) יהיו R, S חוגים. המכפלה הקרטזית של R, S היא החוג $R \times S$ עם הפעולות לפי רכיבים.

תרגיל 1.1.72 (*) אם R, S חוגים עם יחידה אז גם $R \times S$ חוג עם יחידה, ו־$1_{R\times S} = (1_R, 1_S)$.

תרגיל 1.1.73 (*+) הוכח ש־$Z(R \times S) = Z(R) \times Z(S)$.

1.2 אידיאלים וחוגי מנה

1.2.1 אידיאלים חד־צדדיים ודו־צדדיים

תהי $I \subseteq R$ תת־חבורה ביחס לחיבור. I הוא אידיאל שמאלי $(I \leq_l R)$ אם לכל $x \in R, a \in I$, $xa \in I$; אידיאל ימני $(I \leq_r R)$ אם לכל $x \in R, a \in I$, $ax \in I$.

תרגיל 1.2.1 (*) לכל $x \in R$, $Rx = \{rx : r \in R\}$ הוא אידיאל שמאלי של R.

תרגיל 1.2.2 (*+) אם $L \leq_l R$ אידיאל שמאלי, ו־$x \in L$, אז $Rx \subseteq L$.

תרגיל 1.2.3 (**) אם $L \leq_l R$ ו־ $x \in L$ הפיך משמאל, אז $L = R$.

תרגיל 1.2.4 (־)** $L \leq_l R$ אידיאל שמאלי, $x \in R$. הוכח שגם Lx אידיאל שמאלי.

תרגיל 1.2.5 (**) R חוג. הראה ש־ $I = \left\{ \begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix} : a, b \in R \right\}$ אידיאל חד־צדדי של חוג המטריצות $\mathrm{M}_2(R)$.

תרגיל 1.2.6 (**) I אידאל שמאלי של R. הוכח שהקבוצה $\{1 - a : a \in I\}$ סגורה לכפל.

תרגיל 1.2.7 (**) הראה, על־ידי דוגמא נגדית, שבדרך־כלל $R(a+b) \neq Ra + Rb$.

I הוא אידיאל ($I \lhd R$) אם הוא אידיאל ימני וגם אידיאל שמאלי.

תרגיל 1.2.8 (*) 0 הוא אידיאל של R (ושמו: אידיאל האפס).

איחוד וחיתוך

תרגיל 1.2.9 (**) מצא חוג עם אידיאל שמאלי L ואידיאל ימני P כך ש־ $L \cap P$ אינו אידיאל.

תרגיל 1.2.10 (**) יהי $\{U_\lambda : \lambda \in \Lambda\}$ אוסף אידיאלים של R. הוכח: $\bigcap_{\lambda\in\Lambda} U_\lambda$ אידיאל של R.

הגדרה 1.2.11 האידיאל הנוצר על־ידי $x \in R$ הוא $\langle x \rangle = \{\sum a_i x b_i\}$.

תרגיל 1.2.12 (**) הוכח ש־ $\langle x \rangle$ אידיאל של R.

תרגיל 1.2.13 (**) בחוג קומוטטיבי, $\langle x \rangle = Rx = \{rx : r \in R\}$.

דוגמא 1.2.14 $2\mathbb{Z} = \{2n : n \in \mathbb{Z}\}$ הוא האידיאל הנוצר על־ידי 2 בחוג $\mathbb{Z}$.

תרגיל 1.2.15 (+)** אם $I \leq_l$, נגדיר $I^+ = \{x \in R : xR \subseteq I\}$.

א. הוכח ש־ $I^+ \lhd R$.

ב. אם $I \lhd R$ אז $I \subseteq I^+$.

ג. נניח ש־ R חוג עם יחידה. הוכח ש־ $I^{++} = I^+$.

אידיאלים אמיתיים

אידיאלים של חוגים מיוחדים

תרגיל 1.2.16 (־*)** האידיאל הנוצר על־ידי $\begin{pmatrix} n & 0 \\ 0 & m \end{pmatrix}$ ב־ $\mathrm{M}_2(\mathbb{Z})$ מכיל את $\begin{pmatrix} 0 & d \\ 0 & 0 \end{pmatrix}$, כאשר $d = (n, m)$.

תרגיל 1.2.17 (**) א. הוכח ש־ $\mathbb{Z}[\sqrt{5}] = \{n + m\sqrt{5} : n, m \in \mathbb{Z}\}$ תת־חוג של $\mathbb{R}$.

ב. הוכח ש־ $5\mathbb{Z}+\sqrt{5}\mathbb{Z} = \{n + m\sqrt{5} : n, m \in \mathbb{Z}, 5|n\}$ הוא אידיאל של $\mathbb{Z}[\sqrt{5}]$.

תרגיל 1.2.18 (+)** תהי X קבוצה. עבור $A, B \subseteq X$, נסמן $A\Delta B = (A \cup B) - (A \cap B)$.

א. הוכח ש־ $\langle P(X); \Delta, \cap \rangle$ הוא חוג, ומצא את איבר האפס ואת איבר היחידה שלו.

ב. $P(X) \supseteq \tau \neq \phi$ הוא אידיאל אם ורק אם τ סגור לאיחוד ולהקטנה ($A, B \in \tau \to A \cup B \in \tau$ ו־ $A \subseteq B \in \tau \to A \in \tau$).

ג. אם X סופי, $P(X) \supseteq \tau$ אידיאל אם ורק אם קיים $C \subseteq X$ כך ש־ $\tau = P(C)$.

ד. מצא אידיאל של $P(\mathbb{Z})$ שאינו מהצורה $P(C)$.

1.2.2 סכום ומכפלה של אידיאלים

סכומים סופיים וכלליים

הגדרה 1.2.19 (חיבור אידיאלים) אם $I, J \lhd R$, $I + J = \{a + b : a \in I, b \in J\}$.

תרגיל 1.2.20 (*) $I + J$ הוא אידיאל של R.

תרגיל 1.2.21 (*) $I + J = J + I$.

תרגיל 1.2.22 (*) $(I + J) + K = I + (J + K)$.

תרגיל 1.2.23 (**) הוכח או הפרך: $Ra + Rb = R(a + b)$

מכפלה

הגדרה 1.2.24 (כפל אידיאלים) אם $A, B \subseteq R$ תת־קבוצות כלשהן, המכפלה $A \cdot B$ מוגדרת לפי $A \cdot B = \{\sum a_i b_i : a_i \in A, b_i \in B\}$, כלומר אוסף הסכומים הסופיים של מכפלות.

תרגיל 1.2.25 (**) אם $R \geq_r J, R \geq_l I$, אז $IJ \lhd R$.

תרגיל 1.2.26 (***) תן דוגמא לחוג R עם אידיאלים I, J, כך ש־ $\{ab : a \in I, b \in J\}$ אינו אידיאל.

הצעה. $R = \mathbb{Q}[x, y]$ (חוג הפולינומים בשני משתנים), $I = J = \langle x, y \rangle$.

תרגיל 1.2.27 (**) $IJ \subseteq I \cap J$.

תרגיל 1.2.28 (**) R חוג קומוטטיבי עם יחידה. הוכח ש־ $(Ra)(Rb) = Rab$.

תרגיל 1.2.29 (**) אסוציאטיביות של כפל אידיאלים: $I(JK) = (IJ)K$ $(I, J, K \lhd R)$.

תרגיל 1.2.30 (**) דיסטריבוטיביות של פעולות באידיאלים: $I(J+K) = IJ+IK$ $(I, J, K \lhd R)$.

תרגיל 1.2.31 (־*)** הראה שלכל שני אידיאלים I, J של $\mathrm{M}_2(\mathbb{Z})$, $IJ = JI$.

תרגיל 1.2.32 (־*)** מצא אידיאלים $I, J \lhd \left\{ \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \right\} \subseteq \mathrm{M}_2(\mathbb{Z})$, כך ש־ $IJ \neq JI$.

סריג האידיאלים

מאפסים

הגדרה 1.2.33 אם $B \subseteq R$ תת־קבוצה כלשהי, המאפס השמאלי של B הוא $\mathrm{Ann}_l(B) = \{x \in R : xB = 0\}$. המאפס הימני הוא $\mathrm{Ann}_r(B) = \{x \in R : Bx = 0\}$, והמאפס הוא החיתוך $\mathrm{Ann}(B) = \mathrm{Ann}_l(B) \cap Ann_r(B)$.

תרגיל 1.2.34 (+*) לכל תת־קבוצה B, המאפס השמאלי $\mathrm{Ann}_l(B)$ הוא אידיאל שמאלי של R; המאפס הימני $\mathrm{Ann}_r(B)$ הוא אידיאל ימני; והמאפס הדו־צדדי הוא אידיאל.

תרגיל 1.2.35 (+*) אם $I \leq_l R$ אידיאל שמאלי, אז $\mathrm{Ann}_l(I) \lhd R$.

תרגיל 1.2.36 (*) אם $I \lhd R$ אז $\mathrm{Ann}(I) \lhd R$.

תרגיל 1.2.37 (*) הראה שאם $I \subseteq J$ אז $\mathrm{Ann}_l(J) \subseteq \mathrm{Ann}_l(I)$ ו־ $\mathrm{Ann}(J) \subseteq Ann(I)$.

תרגיל 1.2.38 (**) הראה ש־ $I \subseteq \mathrm{Ann}_r(\mathrm{Ann}_l(I))$.

תרגיל 1.2.39 (**) $\mathrm{Ann}_l(I + J) = Ann_l(I) \cap Ann_l(J)$.

תרגיל 1.2.40 (**) $\mathrm{Ann}_l(I \cap J) \supseteq Ann_l(I) + Ann_l(J)$.

תרגיל 1.2.41 (**) מצא דוגמא המראה שלפעמים $\mathrm{Ann}_l(I \cap J) \neq \mathrm{Ann}_l(I) + \mathrm{Ann}_l(J)$. ראה תרגיל 3.4.75.

1.2.3 חוגי מנה

תהי $I \supset R$ תת־חבורה חיבורית. נגדיר יחס שקילות על R: $x \equiv y$ אם"ם $x - y \in I$.
נגדיר פעולת כפל בחבורת המנה R/I: $(x+I)(y+I) = xy + I$.

תרגיל 1.2.42 (**) הוכח שהפעולה מוגדרת היטב אם ורק אם $I \lhd R$.

תרגיל 1.2.43 (**) נניח ש־ $I \lhd R$. הוכח ש־ R/I, ביחס לחיבור והכפל שהגדרנו, הוא חוג.

תרגיל 1.2.44 (*) אם R חוג עם יחידה, אז כך גם R/I, ו־ $1_{R/I} = 1_R + I$.
משפט $(^{-3})$: יהי $I \lhd R$. אם $J \lhd R$ אידיאל המכיל את I, אז $J/I \lhd R/I$; וכל האידיאלים של R/I מצורה זו.

תרגיל 1.2.45 (**) נסמן $R = \mathbb{Z}[x]$, $I = \langle x^n \rangle$, $J = \langle x \rangle$. חשב את $(J/I)^n$.

1.2.4 הומומורפיזמים

יהיו R, S חוגים. העתקה $\varphi : R \to S$ השומרת על החיבור והכפל (כלומר: $\varphi(a+b) = \varphi(a)+\varphi(b)$, $\varphi(ab) = \varphi(a)\varphi(b)$) נקראת הומומורפיזם (של חוגים). אם R, S חוגים עם יחידה, ו־ $\varphi(1_R) = 1_S$, אז φ הומומורפיזם של חוגים עם יחידה (או הומומורפיזם אוניטרי).

תרגיל 1.2.46 (*) ההעתקה $r \mapsto 0$ היא הומומורפיזם (הנקרא הומומורפיזם האפס).

הומומורפיזם שהוא על נקרא אפימורפיזם; הומומורפיזם שהוא חד־חד־ערכי נקרא מונומורפיזם.

תרגיל 1.2.47 (**) אם D חוג פשוט (לדוגמא: שדה) ו־ $\varphi : D \to R$ הומומורפיזם של חוגים, $\varphi \neq 0$, אז φ מונומורפיזם.

תרגיל 1.2.48 (**) תאר הומומורפיזם $\varphi : \mathbb{Z}[\lambda] \to \mathbb{Z}_p$, שהגרעין שלו הוא אוסף הפולינומים שסכום מקדמיהם מתחלק ב־ p.

הומומורפיזמים של חוגים בלי יחידה

תרגיל 1.2.49 (**) הראה שהפונקציות $\varphi_0, \varphi_1 : \mathrm{M}_n(F) \to \mathrm{M}_{2n}(F)$ המוגדרות לפי $\varphi_1(A) = \begin{pmatrix} A & 0 \\ 0 & A \end{pmatrix}$ ו־ $\varphi_0(A) = \begin{pmatrix} A & 0 \\ 0 & 0 \end{pmatrix}$ הן מונומורפיזמים של חוגים. φ_1 הוא הומומורפיזם של חוגים עם יחידה, אבל φ_0 אינו כזה.

תרגיל 1.2.50 (**) אם R חוג עם יחידה ו־ $\varphi : R \to S$ אפימורפיזם, אז S חוג עם יחידה ו־ $\varphi(1_R) = 1_S$.

תרגיל 1.2.51 (־*)** אם R חוג עם יחידה ו־ $\varphi : R \to S$ הומומורפיזם, $\varphi \neq 0$, ובנוסף S תחום שלמות (כלומר: $ab \neq 0$ לכל $0 \neq a, b \in S$), אז S חוג עם יחידה ו־ $\varphi(1_R) = 1_S$. [הדרכה. הראה ש־ $x\varphi(1_R) = \varphi(1_R)^2 x$ לכל $x \in S$].

הגרעין והתמונה

יהי $\varphi : R \to S$ הומומורפיזם של חוגים.
יהי $\varphi : R \to S$ איזומורפיזם.

תרגיל 1.2.52 (**) $Ker(\varphi) = \{a \in R : \varphi(a) = 0\}$ הוא אידיאל של R.

תרגיל 1.2.53 (+)** $Im(\varphi) = \{\varphi(a) : a \in R\}$ הוא תת־חוג של S, אבל אינו בהכרח אידיאל.

תרגיל 1.2.54 (**) $I \lhd S$. הוכח ש־ $\varphi^{-1}(I) \lhd R$.

תרגיל 1.2.55 (־)** הגרעין $Ker(\varphi) = \varphi^{-1}(0) = \{r : \varphi(r) = 0\}$ הוא אידיאל של R.

תרגיל 1.2.56 (+)** נניח ש־ φ על. הוכח שתמונה של אידיאל ב־ R היא אידיאל ב־ S.

הומומורפיזמים ומכפלה פנימית

תרגיל 1.2.57 (+)** R, S חוגים עם יחידה, K אידיאל שמאלי של $R \times S$. הוכח ש־ $K = I \times J$ כאשר I, J אידיאלים שמאליים של R, S, בהתאמה.

1.2.5 משפטי האיזומורפיזמים

משפט 1.2.58 (משפט האיזומורפיזם הראשון (**)) : $R/\operatorname{Ker}(\varphi) \cong \operatorname{Im}(\varphi)$.

תרגיל 1.2.59 (־)** $\varphi : R \to S$, $\psi : S \to T$ אפימורפיזמים. הוכח ש־ T איזומורפי לחוג מנה של R.

תרגיל 1.2.60 (**) $\varphi : R \to S$ על, $I \lhd S$. הוכח ש־ $R/\varphi^{-1}(I) \cong S/I$.

תרגיל 1.2.61 (+)** $I \lhd R$. הוכח ש־ $\mathrm{M}_n(R/I) \cong M_n(R)/\mathrm{M}_n(I)$. הדרכה. הגדר $\varphi : \mathrm{M}_n(R) \to \mathrm{M}_n(R/I)$ לפי $\varphi((a_{ij})_{ij}) = (\theta(a_{ij}))_{ij}$ כאשר $\theta : R \to R/I$ ההיטל הטבעי.

תרגיל 1.2.62 (***) כל אידיאל של $\mathrm{M}_n(R)$ הוא מהצורה $\mathrm{M}_n(I)$ עבור $I \lhd R$.

תרגיל 1.2.63 (**) $I \subseteq J$ אידיאלים של R. הראה שקיים אפימורפיזם $R/I \to R/J$.

משפט 1.2.64 (משפט האיזומורפיזם השני (**)) אם $I \subseteq J$ אידיאלים של R, אז $R/J \cong (R/I)/(J/I)$.

הומומורפיזם $\varphi : R \to S$ שהוא חד־חד־ערכי ועל, נקרא **איזומורפיזם**. אם קיים כזה, אומרים שהחוגים R, S איזומורפיים.

תרגיל 1.2.65 (**) א. הראה שאוסף המטריצות $K = \left\{ \begin{pmatrix} x & y \\ -y & x \end{pmatrix} : x, y \in \mathbb{R} \right\}$ הוא חוג.

ב. K איזומורפי לשדה המספרים המרוכבים $\mathbb{C}$.

תרגיל 1.2.66 (+)** הראה שאוסף המטריצות $U = \left\{ \begin{pmatrix} x & y \\ -\bar{y} & \bar{x} \end{pmatrix} : x, y \in \mathbb{R} \right\}$ איזומורפי לחוג הקווטרניונים $\mathbb{H}$.

תרגיל 1.2.67 (+)** הראה שאוסף המטריצות

$$U_2 = \left\{ \begin{pmatrix} a & b & c & d \\ -b & a & -d & c \\ -c & d & a & -b \\ -d & -c & b & a \end{pmatrix} : a, b, c, d \in \mathbb{R} \right\}$$

איזומורפי ל־ $\mathbb{H}$.

תרגיל 1.2.68 (+)** על אוסף המספרים החיוביים הממשיים $\mathbb{R}^+$ נגדיר פעולות $r \oplus s = rs$, $r \otimes s = r^{log(s)}$. הוכח ש־ $\vartheta = (\mathbb{R}^+; \oplus, \otimes)$ חוג עם יחידה. הדרכה. מצא איזומורפיזם $\vartheta \to (\mathbb{R}; +, \cdot)$.

תרגיל 1.2.69 (**) הוכח שחוג האנדומורפיזמים של $\mathbb{Z}_n$ מקיים $End(\mathbb{Z}_n) \cong \mathbb{Z}_n$. הדרכה. הגדר $\varphi \mapsto \varphi(1)$.

תרגיל 1.2.70 (־*)** יהי V מרחב וקטורי ממימד n מעל שדה F. הוכח ש־ $End(V) \cong \mathrm{M}_n(F)$.

תרגיל 1.2.71 (**) הוכח ש־ $\mathrm{M}_n(R \times S) \cong \mathrm{M}_n(R) \times \mathrm{M}_n(S)$.

תרגיל 1.2.72 (־*)** הוכח ש־ $\mathrm{M}_n(\mathrm{M}_m(R)) \cong \mathrm{M}_{mn}(R)$.

תת־החוג היסודי

הומומורפיזם ויוצרים

פרק 2

אידיאלים ראשוניים ומקסימליים

נסמן ב־ $\mathrm{Jac}(R)$ את חיתוך כל האידיאלים המקסימליים של R.

תרגיל 2.0.73 (**) $x \in \mathrm{Jac}(R)$ אם ורק אם $1 - xy$ הפיך לכל $y \in R$.

תרגיל 2.0.74 (*+)** אם $I + \mathrm{Jac}(R) = R$ אז $I = R$.

תרגיל 2.0.75 (**) חשב את $\mathrm{Jac}(\mathbb{Z}/24\mathbb{Z})$, $\mathrm{Jac}(\mathbb{Z}/9\mathbb{Z})$.

תרגיל 2.0.76 (**) חשב את $\mathrm{Jac}(\mathbb{Z}/6\mathbb{Z})$, $\mathrm{Jac}(\mathbb{Z}/36\mathbb{Z})$.

הגדרה 2.0.77 אם R חוג קומוטטיבי, נסמן $Nil(R) = \{a \in R : \exists n a^n = 0\}$ ־ "הרדיקל של 0".

תרגיל 2.0.78 (*+) אם $x \in Nil(R)$, אז $x^n \in Nil(R)$ לכל n.

תרגיל 2.0.79 (*) אם D תחום שלמות אז $Nil(D) = 0$.

תרגיל 2.0.80 (*+) אם $z \in Nil(R)$ אז $1 - z$ הפיך.

תרגיל 2.0.81 (**) $Nil(R) \lhd R$.

תרגיל 2.0.82 (*+)** $Nil(R/Nil(R)) = 0$.

הגדרה 2.0.83 אם $I \lhd R$, נסמן $\sqrt{I} = \{a \in R : \exists n : a^n \in I\}$ (הרדיקל של I).

תרגיל 2.0.84 (*+)** הראה ש־ $\sqrt{I}$ אידיאל של R [הדרכה: אם $a^n, b^m \in I$ חשוב על $(a+b)^{n+m}$].

תרגיל 2.0.85 (*) הראה ש־ $\sqrt{0} = Nil(R)$.

תרגיל 2.0.86 (*) הראה ש־ $I \subseteq \sqrt{I} \lhd R$.

תרגיל 2.0.87 (*) אם $I \subseteq J$ אז $\sqrt{I} \subseteq \sqrt{J}$. אידיאל המקיים $\sqrt{I} = I$ נקרא אידיאל רדיקלי.

תרגיל 2.0.88 (**) הראה ש־ $\sqrt{\sqrt{I}} = \sqrt{I}$, כלומר $\sqrt{I}$ אידיאל רדיקלי.

תרגיל 2.0.89 (**) אם $I \subseteq J \lhd R$ אז $\sqrt{J/I} = \sqrt{J}/I$.

תרגיל 2.0.90 (**) כל אידיאל ראשוני הוא רדיקלי.

תרגיל 2.0.91 (**) מצא את כל האידיאלים הרדיקליים של $\mathbb{Z}$.

תרגיל 2.0.92 (**) חשב את $\sqrt{\langle x, 4\rangle}, \sqrt{\langle x\rangle}, \sqrt{\langle x-4\rangle}$ (אידיאלים של $\mathbb{Z}[x]$). הראה שבאופן כללי, יתכן ש־ $\sqrt{I+J} \neq \sqrt{I} + \sqrt{J}$.

2.1 אידיאלים מקסימליים

הגדרה. אידיאל $I \lhd R$ **הוא מקסימלי אם לא קיים אידיאל** $J \lhd R$ **כך ש־** $I \subset J \subset R$.

משפט 2.1.1 (*־)** יהי R חוג קומוטטיבי עם יחידה. $I \lhd R$ הוא מקסימלי אם ורק אם R/I שדה.

תרגיל 2.1.2 (**) R קומוטטיבי. $I \lhd R$ מקסימלי אם ורק אם לכל $x \in R$, $I + Rx = R$.

תרגיל 2.1.3 (+)** $\varphi : R \to S$ על. אם $P \lhd S$ מקסימלי, הוכח שגם $\varphi^{-1}(P) \lhd R$ מקסימלי.

תרגיל 2.1.4 (+)** $\varphi : R \to \mathbb{Z}$ על. הוכח שיש ב־ R אינסוף אידיאלים מקסימליים שונים.

תרגיל 2.1.5 (**) האידיאלים המקסימליים של $\mathbb{Z}$ הם $p\mathbb{Z}$ עבור p ראשוני.

תרגיל 2.1.6 (**) יהיו $F_1, \ldots, F_t$ שדות. מצא את האידיאלים המקסימליים של $R = F_1 \times \cdots \times F_t$.

תרגיל 2.1.7 (**) יהיו $S \neq \phi$ קבוצה, F שדה. על $F^S = \{f : S \to F\}$ מגדירים פעולות לפי רכיבים. הוכח ש־ $F_a = \{f : f(a) = 0\}$ הוא אידיאל מקסימלי של F^S.

הלמה של צורן קובעת שבכל קבוצה סדורה, אם לכל שרשרת עולה יש חסם מלעיל, אז יש איברים מקסימליים.

משפט 2.1.8 מן הלמה של צורן נובע שכל אידיאל של חוג R עם יחידה מוכל באידיאל מקסימלי.

תרגיל 2.1.9 (**) R קומוטטיבי. $a \in R$ הפיך אם"ם $a+M$ הפיך ב־ R/M לכל אידיאל מקסימלי M.

תרגיל 2.1.10 (***) בחוג עם יחידה R, כל האידיאלים פרט ל־ 0 הם מקסימליים. הוכח: אין ל־ R יותר משני אידיאלים פרט ל־ 0. פתרון. יהיו $A, B, C \lhd R$ אידיאלים שונים, $A, B \neq 0$. $A \subseteq A+B \subseteq R$, ואם $A = A+B$ אז $B \subset A$; לכן $A+B = R$. $AC = 0 \Leftarrow AC \subseteq A \cap C \subseteq A, C$. בדומה $BC = 0$. כעת $C = RC = (A+B)C = AC + BC = 0 + 0 = 0$.

אידיאלים מינימליים

תרגיל 2.1.11 (־*)** יהי $H < R$ אידיאל שמאלי מינימלי (כלומר: אם $T \subset H$ אידיאל שמאלי, אז $T = 0$). הוכח שכל איבר $a \in H$ הוא מחלק אפס שמאלי. הדרכה. הראה ש־ $a \in Ra^2$.

2.1.1 הלמה של צורן

2.1.2 חוגים פשוטים

הגדרה 2.1.12 חוג פשוט הוא חוג שאין לו אידיאלים למעט 0.

תרגיל 2.1.13 (*) שדה הוא חוג פשוט.

תרגיל 2.1.14 (**) חוג פשוט קומוטטיבי עם יחידה הוא שדה.

תרגיל 2.1.15 (+)** אם F שדה, אז $\mathrm{M}_2(F)$ חוג פשוט.

תרגיל 2.1.16 (***) אם F שדה, $\mathrm{M}_n(F)$ חוג פשוט.

תרגיל 2.1.17 (־)** לחוג R אין אידיאלים שמאליים, אם ורק אם R הוא חוג עם חילוק.

2.1.3 אידיאלים ראשוניים

חוגים ראשוניים

הגדרה 2.1.18 אידיאל (חד־צדדי) של R הוא אידיאל נילי אם כל איבריו נילפוטנטיים.

תרגיל 2.1.19 (**) אם $L \leq_l$ אידיאל נילי, אז $\{1-a : a \in L\}$ חבורה כפלית.

תרגיל 2.1.20 (+)** קיימים ב־ $\mathbb{Z}_n$ איברים נילפוטנטיים $0 \neq$ אם ורק אם קיים ראשוני p כך ש־ $p^2|n$.

תרגיל 2.1.21 (+)** נניח ש־ J אידיאל נילי של חוג R. הראה ש־ $a \in R$ הפיך אם ורק אם $a+J$ הפיך בחוג המנה R/J.

תרגיל 2.1.22 (־*)** תן דוגמא לתת־חוג של חוג פשוט, שאינו ראשוני.

תרגיל 2.1.23 (***) נאמר ש־ R הוא **הרחבה מרכזית** של תת־חוג S, אם $\mathrm{Z}(R)S = R$. הוכח שאם ל־ S יש הרחבה מרכזית שהיא חוג פשוט, אז S חוג ראשוני.

אידיאלים ראשוניים

הגדרה. אידיאל $P \lhd R$ **הוא אידיאל ראשוני אם לכל** $A, B \lhd R$ **המקיימים** $AB \subseteq P$, **מתקיים** $A \subseteq P$ **או** $B \subseteq P$. **דוגמא.** 6 **אינו אידיאל ראשוני של כי** $(4) \cdot (9) \subseteq 6$, **למרות ש־** $4, 9 \subseteq 6$.

תרגיל 2.1.24 (**) יהי R חוג קומוטטיבי. אם 0 הוא אידיאל ראשוני של R אז R תחום שלמות.

משפט 2.1.25 (*־)** **יהי R חוג קומוטטיבי. $P \lhd R$ אידיאל ראשוני אם ורק אם R/P תחום שלמות.**

תרגיל 2.1.26 (**) כל אידיאל מקסימלי הוא ראשוני.

תרגיל 2.1.27 (**) האידיאלים הראשוניים של $\mathbb{Z}$ הם $p\mathbb{Z}$ (p ראשוני) ו־ 0.

תרגיל 2.1.28 (+)** $\varphi : R \to S$ על. אם $P \lhd S$ ראשוני, הוכח שגם $\varphi^{-1}(P) \lhd R$ ראשוני.

תרגיל 2.1.29 (**) R חוג קומוטטיבי סופי עם יחידה. הוכח שכל אידיאל ראשוני הוא מקסימלי.

תרגיל 2.1.30 (**) יהי R חוג קומוטטיבי עם יחידה. הראה שקיים הומומורפיזם $\Phi :\to R$ המוגדר לפי $1 \mapsto 1_R$. בנוסף, אם R תחום שלמות, אז $Ker\Phi$ אידיאל ראשוני של (ולכן מהצורה p, p ראשוני).

תרגיל 2.1.31 (**) נגדיר $\varphi : \mathbb{Z}[\lambda] \to \mathbb{Z}/p\mathbb{Z}$ לפי $\varphi(f) = f(1)$ (כאשר p ראשוני). חשב את $I = Ker(\varphi)$. האם זהו אידיאל ראשוני? האם הוא מקסימלי?

תרגיל 2.1.32 (+)** הוכח ש־ $Nil(R)$ הוא חיתוך כל האידיאלים הראשוניים של R.

תרגיל 2.1.33 (+)** תהי $\{P_\lambda : \lambda \in \Lambda\}$, $\Lambda \neq \phi$, שרשרת של אידיאלים ראשוניים של חוג R, כלומר, לכל $\lambda, \lambda' \in \Lambda$ מתקיים $P_\lambda \subseteq P_{\lambda'}$ או $P_{\lambda'} \subseteq P_\lambda$. הוכח ש־ $M = \bigcup P_\lambda$ ו־ $N = \bigcap P_\lambda$ הם אידיאלים ראשוניים.

תרגיל 2.1.34 (־*)** יהיו $I \subseteq A$ אידיאלים של חוג R. הוכח שבקבוצת האידיאלים הראשוניים $I \subseteq P \subseteq A$ יש אידיאלים מינימליים ומקסימליים.

תרגיל 2.1.35 (***) יהי A אידיאל של חוג R. אם A אינו ראשוני, או שהוא נוצר סופית, אז יש ראשוני מקסימלי בקבוצת האידיאלים $P \subset A$.

תרגיל 2.1.36 (+)** R קומוטטיבי, $A, B \lhd R$. אם $A \cap B$ אידיאל ראשוני אז $A \subseteq B$ או $B \subseteq A$.

תרגיל 2.1.37 (**) תן דוגמא מפורשת לחוג עם אידיאלים ראשוניים A_1, A_2 כך ש־ $A_1 \cap A_2$ אינו ראשוני.

תרגיל 2.1.38 (+)** $3R = \langle 3 \rangle$ הוא אידיאל ראשוני של החוג

$$R = \mathbb{Z}[i] = \{n + mi : n, m \in \mathbb{Z}\} \subseteq \mathbb{C}.$$

תרגיל 2.1.39 (**) $\langle \lambda \rangle \lhd F[\lambda, \mu]$ ראשוני אבל לא מקסימלי.

תרגיל 2.1.40 (+)** $\langle 2\lambda - 1 \rangle \lhd \mathbb{Z}[\lambda]$ ראשוני אבל לא מקסימלי.

תרגיל 2.1.41 (+)** $I = \langle 5 \rangle$ אידיאל של $\mathbb{Z}[i]$. הוכח:

א. $I \cap \mathbb{Z}$ אידיאל ראשוני של, אך I אינו ראשוני ב־ $\mathbb{Z}[i]$.

ב. מצא אידיאל ראשוני J של $\mathbb{Z}[i]$ כך ש־ $J \cap \mathbb{Z} = \mathbb{Z} \cap I$.

ג. $I = \langle 7 \rangle$ אידיאל ראשוני ב־ $\mathbb{Z}[i]$.

2.1.4 פירוק למכפלה ישרה

אידיאלים קו־מקסימליים

משפט השאריות הסיני

יהי R חוג (לאו־דוקא קומוטטיבי) עם יחידה.

הגדרה 2.1.42 I, J **קו־מקסימליים אם** $I + J = R$.

תרגיל 2.1.43 (***) אם $I, J \lhd R$ קומקסימליים, אז לכל $n, m \geq 0$, גם I^n ו־ J^m קו־מקסימליים. (הדרכה: ראשית הנח ש־ $m = 1$).

תרגיל 2.1.44 (**) $I, J \lhd R$ אידיאלים קו־מקסימליים. הראה ש־ $I \cap J = IJ + JI$.

משפט 2.1.45 (משפט השאריות הסיני (***)) יהיו $I_1, \ldots, I_t \lhd R$ אידיאלים קו־מקסימליים בזוגות. אז $R/(I_1 \cap \cdots \cap I_t) \cong (R/I_1) \times \cdots \times (R/I_t)$ (ניסוח אחר: לכל $a_1, \ldots, a_t$, קיים $x \in R/(I_1 \cap \cdots \cap I_t)$ יחיד כך ש־ $(\forall i : x - a_i \in I_i$).

הדרכה. הגדר $\varphi : R \to (R/I_1) \times \cdots \times (R/I_t)$ לפי $\varphi(a) = (a + I_1, \ldots, a + I_t)$. כדי להוכיח ש־ φ על, מספיק להראות שלכל i קיים $a \in R$ כך ש־ $a \in I_1 \cap \cdots \cap (1 + I_i)$. כתוב $1 = b_j + c_j \in I_i + I_j$, וחשב את $1 = (b_1 + c_1) \cdots (b_t + c_t)$.

תרגיל 2.1.46 (+*) F שדה. בחוג $R = F \times F \times F$ ישנם אידיאלים $I_1 = 0 \times F \times F$, $I_2 = F \times 0 \times F$, $I_3 = F \times F \times 0$. א. הראה שהאידיאלים קו־מקסימליים.

ב. מצא $\alpha \in R$ כך ש־ $\alpha - (6, 2, 3) \in I_1$, $\alpha \in (4, 5, 6) + I_2$, ו־ $\alpha \equiv (-1, -2, -2)$ בחוג המנה R/I_3.

תרגיל 2.1.47 (**) נניח ש־ $(n, m) = 1$ מספרים שלמים זרים. כתוב $\alpha n + \beta m = 1$. הראה ש־ $x = \alpha n b + \beta m a$ הוא פתרון למערכת המשוואות $x \equiv a \pmod{n}$, $x \equiv b \pmod{m}$.

תרגיל 2.1.48 (**) פתור את המשוואה $x \equiv 2 \pmod{37}, x \equiv 2 \pmod{101}, x \equiv 2 \pmod{197}$.

תרגיל 2.1.49 (+)** פתור את המשוואה $x \equiv 2 \pmod{3}, x \equiv 4 \pmod{8}, x \equiv 11 \pmod{25}$.

תרגיל 2.1.50 (+)** א. הראה שאוסף הפונקציות הרציפות $R = \{f : \mathbb{R} \to \mathbb{R}\}$ הוא חוג.

ב. הראה שלכל $a \in \mathbb{R}$, האוסף $I_a = \{f \in R | f(a) = 0\}$ הוא אידיאל של R.

ג. הראה שכל שני אידיאלים כאלה הם קו־מקסימליים [הדרכה. חשוב על $1 = \frac{x-a}{b-a} - \frac{x-b}{b-a}$].

ד. הוכח שלכל $a_1, \ldots, a_t$ שונים, ולכל $b_1, \ldots, b_t$, קיימת פונקציה רציפה $f : \mathbb{R} \to \mathbb{R}$ כך ש־ $f(a_i) = b_i$.

תרגיל 2.1.51 (־*)** הכלל את השאלה האחרונה, והראה שלכל $a_1, \ldots, a_t$ שונים ולכל $b_1, \ldots, b_t, c_1, \ldots, c_t$, קיימת פונקציה $f : \mathbb{R} \to \mathbb{R}$ גזירה ברציפות, כך ש־ $f(a_i) = b_i$, ו־ $f'(a_i) = b_i$.

תרגיל 2.1.52 (***) העזר בחוג R שהוגדר להלן כדי להראות שהטענה הבאה אינה נכונה: "יהיו $I_1, I_2, \ldots \lhd R$ אידיאלים קו־מקסימליים. אז לכל $a_1, a_2, \ldots \subseteq R$ קיים $x \in R$ כך ש־ $x - a_i \in I_i$".

תרגיל 2.1.53 (**) בחוג $R = \begin{pmatrix} * & * \\ 0 & * \end{pmatrix}$, נסח את התוצאה של משפט השאריות הסיני עבור $I_1 = \begin{pmatrix} * & * \\ 0 & 0 \end{pmatrix}$ ו־ $I_2 = \begin{pmatrix} 0 & * \\ 0 & * \end{pmatrix}$.

תרגיל 2.1.54 (**) בחוג $R = \begin{pmatrix} * & * & * \\ 0 & * & * \\ 0 & 0 & * \end{pmatrix}$, נסח את התוצאה של משפט השאריות הסיני עבור $I_1 = \begin{pmatrix} 0 & * & * \\ 0 & * & * \\ 0 & 0 & * \end{pmatrix}$, $I_2 = \begin{pmatrix} * & * & * \\ 0 & 0 & * \\ 0 & 0 & * \end{pmatrix}$ ו־ $I_3 = \begin{pmatrix} * & * & * \\ 0 & * & * \\ 0 & 0 & 0 \end{pmatrix}$.

אידמפוטנטים

אם L_1, L_2 אידיאלים שמאליים כך ש־ $L_1 \cap L_2 = 0$, מסמנים את סכומם ב־ $L_1 \oplus L_2$, וקוראים לו סכום ישר. ההגדרה דומה עבור אידיאלים ימניים או דו־צדדיים. בסכום ישר $R \oplus S$ של חוגים, אנו דורשים בנוסף ש־ $RS = SR = 0$.
איבר $e \in R$ נקרא אידמפוטנט אם $e^2 = e$.

תרגיל 2.1.55 (*) אם $aba = a$ אז ab ו־ ba הם אידמפוטנטים.

אידמפוטנטים e_1, e_2 נקראים אורתוגונליים אם $e_1e_2 = e_2e_1 = 0$.

תרגיל 2.1.56 (**) אם e אידמפוטנט, אז $1 - e$ אידמפוטנט אורתוגונלי אליו.

תרגיל 2.1.57 (**) כאשר $e \in R$ אידמפוטנט, אז

$$A = eAe \oplus (1-e)Ae \oplus eA(1-e) \oplus (1-e)A(1-e)$$

הוא פירוק לסכום ישר של חוגים.

נסמן ב־ E את אוסף האידמפוטנטים של החוג. נגדיר עליו יחס סדר, $x \leq y$ אם $xy = x = yx$.

תרגיל 2.1.58 (**) הוכח שזהו אכן יחס סדר, וש־ $0 \leq x \leq 1$ לכל $x \in E_C$.

תרגיל 2.1.59 (**) אם $x, y \in E$ אורתוגונליים, $x, y \leq x + y \in E$.

תרגיל 2.1.60 (**) אם $y \leq x$ אז $y - x \in E$, אורתוגונלי ל־ x, ו־ $y - x \leq x$.

תרגיל 2.1.61 (**) אם $x, y \in E$, אז $xy \leq x, y \leq x + y - xy$ (ולכן E הוא סריג).

תרגיל 2.1.62 (***) יהי $e \in R$ אידמפוטנט. הוכח שהאידיאל השמאלי Re מתפרק לסכום ישר $Re = M \oplus N$ של אידיאלים שמאליים אם ורק אם קיימים אידמפוטנטים אורתוגונליים g, h כך ש־ $e = g + h$, $eg = g = ge$ ו־ $eh = h = he$.

פרק 3

תחומי שלמות

הגדרה 3.0.63 חוג קומוטטיבי D ללא מחלקי אפס (פרט ל־ 0) נקרא **תחום שלמות**.

תרגיל 3.0.64 (+*) יהיו $0 \neq I_1, \ldots, I_t$ אידיאלים של תחום שלמות D. הוכח ש־ $I_1 \cap \cdots \cap I_t \neq 0$.

תרגיל 3.0.65 (**) D תחום שלמות, $a, b \in D$ מקיימים $a^{40} = b^{40}$, $a^{27} = b^{27}$. הוכח ש־ $a = b$.

תרגיל 3.0.66 (**) $\mathbb{Z}_n$ הוא תחום שלמות אם ורק אם n ראשוני.

תרגיל 3.0.67 (+)** כל תחום שלמות סופי הוא שדה (אפילו כאשר לא נתון שקיימת יחידה).

תרגיל 3.0.68 (**) הוכח או הפרך: אם D_1, D_2 תחומי שלמות, אז $D_1 \times D_2$ תחום שלמות.

תרגיל 3.0.69 (**) אם D תחום שלמות אז גם חוג הפולינומים $D[\lambda]$ תחום שלמות.

תרגיל 3.0.70 (**) תן דוגמא לחוג מנה של תחום שלמות שאינו תחום שלמות.

3.1 מיקום ושדה השברים

3.1.1 מיקום מרכזי

3.1.2 שדה השברים

יהי D תחום שלמות. תהי $S \subseteq D - 0$ קבוצה סגורה לכפל.
נגדיר יחס על $D \times S$ לפי $(a, b) \sim (c, d)$ אם"ם $ad = bc$.

תרגיל 3.1.1 (**) הוכח שהיחס הנ"ל הוא יחס שקילות (שים לב לתפקידה של האסוציאטיביות).

על אוסף מחלקות השקילות נגדיר פעולות: $[(a,b)]+,[(a,b)]\cdot[(c,d)]=[(ac,bd)]$ $[(c,d)]=[(ad+bc,bd)]$.

תרגיל 3.1.2 (**) הראה שהפעולות מוגדרות היטב.

תרגיל 3.1.3 (**) הראה שאוסף מחלקות השקילות הוא חוג ביחס לפעולות שהגדרנו.
הגדרה. החוג שהוגדר להלן נקרא המיקום של D ב־ S, ומסומן ב־ $S^{-1}D$.

תרגיל 3.1.4 (**) נגדיר $\varphi : D \to S^{-1}D$ לפי $\varphi : d \mapsto [(d,1)]$. הוכח ש־ φ מונומורפיזם.
מסקנה. $S^{-1}D$ מכיל תת־חוג איזומורפי ל־ D. כאשר אין סכנה לבלבול, אפשר לכתוב $D \subseteq S^{-1}D$.

תרגיל 3.1.5 (**) הראה שהאברים של S בחוג $S^{-1}D$ הם הפיכים.

תרגיל 3.1.6 (־*)** (אוניברסליות של המיקום). הראה שאם $\varphi : D \to R$ שיכון, כך שהתמונות של אברי S הם אברים הפיכים בחוג R, אז קיים שיכון $S^{-1}D \hookrightarrow R$.

תרגיל 3.1.7 (+)** אם $S_1 \subseteq S_2 \subseteq D-0$ מונוידים, אז קיים שיכון $S_1^{-1}D \hookrightarrow S_2^{-1}D$.

הגדרה. במקרה המיוחד $S = D-0$, נסמן את החוג $S^{-1}D$ ב־ $q(D)$ ־ חוג השברים של D.

תרגיל 3.1.8 (**) הראה ש־ $q(D)$ הוא שדה.

תרגיל 3.1.9 (**) נניח ש־ $t \in R$ מחלק אפס. בדוק את שלבי הבניה של $q(R)$, ומצא מה השיבוש הראשון.

תרגיל 3.1.10 (**) אם F שדה, אז $q(F) \cong F$. הציגו במפורש את האיזומורפיזם.

תרגיל 3.1.11 (**) יהיו $D_1 \subseteq D_2$ תחומי שלמות. הראה ש־ $q(D_1) \subseteq q(D_2)$.

תרגיל 3.1.12 (־*)** יהיו $D_1 \subseteq D_2$ תחומי שלמות, ולכל $d \in D_2$ קיים $c \in D_1$ כך ש־ $cd \in D_1$. הוכח: $q(D_1) \cong q(D_2)$.

תרגיל 3.1.13 (+)** אם D תחום שלמות, אז $D[x]$ (חוג הפולינומים) גם הוא תחום שלמות. תאר את שדה השברים של $D[x]$. הדרכה. סמן $F = q(D)$. $F[x] \supseteq D[x]$, ומספיק לתאר את $q(F[x])$ (מדוע?).

תרגיל 3.1.14 (+)** יהי $D \in \mathbb{Z}$. הראה ש־

$$\mathbb{Z}[\sqrt{D}] = \left\{a + b\sqrt{D} : a, b \in \mathbb{Z}\right\} \cong \left\{\begin{pmatrix} a & b \\ Db & a \end{pmatrix} : a, b \in \mathbb{Z}\right\}.$$

הוכח ששדה השברים של $\mathbb{Z}[\sqrt{D}]$ הוא $\mathbb{Q}[\sqrt{-d}] = \left\{a + b\sqrt{D} : a, b \in \mathbb{Q}\right\}$.

תרגיל 3.1.15 (***) יהי R חוג למחצה (כלומר, אין מניחים נגדי ביחס לחיבור), קומוטטיבי וללא יחידה, שאין לו מחלקי אפס. הראה שקיים לו 'שדה שברים' $q(R)$ שהוא שדה למחצה.

שים לב: בחוג למחצה אין צמצום, ולכן יש להגדיר את יחס השקילות לפי $b_2^{-1}a_2 \equiv b_1^{-1}a_1$ אם ורק אם $\exists c \neq 0 : ca_1b_2 = ca_2b_1$.

חוג השברים הטוטאלי

3.1.3 חוגים מקומיים

הגדרה. חוג שבו יש אידיאל מקסימלי יחיד, נקרא **חוג מקומי**.

תרגיל 3.1.16 (+*) הוכח שהחוג $\mathbb{Z}/256\mathbb{Z}$ הוא חוג מקומי.

תרגיל 3.1.17 (+)** R מקומי אם ורק אם אוסף האברים הלא־הפיכים הוא אידיאל.

תרגיל 3.1.18 (**) F שדה. $R = \left\{\begin{pmatrix} c & * & * \\ 0 & c & * \\ 0 & 0 & c \end{pmatrix} : c \in F^\times\right\}$ הוא חוג מקומי.

תרגיל 3.1.19 (**) R מקומי אם ורק אם $a + b = 1$ גורר ש־ a הפיך או b הפיך.

תרגיל 3.1.20 (־*)** הוכח שבחוג מקומי, אם $a_1 + \cdots + a_n = 1$, אז אחד ה־ a_i הפוך.

תרגיל 3.1.21 (־*)** מצא את כל מחלקי האפס של $\mathbb{Z}_p[\lambda]/\langle\lambda^n\rangle$. הראה שזהו חוג מקומי.

3.2 חוגי שלמים

בסעיף זה נבנה כמה דוגמאות לחוגים שפגשנו בפרק, כולן מהטיפוס $\mathbb{Z}[\sqrt{d}]$ עבור $d \in \mathbb{Z}$. נטפל בחוגים אלה כשבידינו כלי רב עוצמה: נורמה של חוגים.

תרגיל 3.2.1 (־*)** יהי R תחום שלמות.

1. הראה שלכל $a \in R$ ולכל $I \lhd R$, $aI \lhd R$ הוא אידיאל;

2. בתנאים אלה, $|R/aI| = |R/Ra| \cdot |R/I|$.

3. ההעתקה $N : R \to \mathbb{N} \cup \{\infty\}$ המוגדרת לפי $N(a) = |R/Ra|$ היא כפלית.

יהי R חוג קומוטטיבי, המכיל (עותק של) $\mathbb{Z}$. יהי $\sigma : R \to R$ אוטומורפיזם, המקיים $\sigma^2(x) = x$, ובנוסף $\sigma(x) = x$ אם ורק אם $x \in \mathbb{Z}$.
נסמן $N(x) = x \cdot \sigma(x)$.

תרגיל 3.2.2 (**) $N : R \to \mathbb{Z}$ פונקציה שומרת כפל.
יהי $D \in \mathbb{Z}$. נתבונן בחוג $R = [\sqrt{D}] = \left\{m + n\sqrt{D} : m, n \in \mathbb{Z}\right\}$.

תרגיל 3.2.3 (**) א. הראה ש־ R חוג. ב. $\sigma(n + m\sqrt{D}) = n - m\sqrt{D}$ הומומורפיזם, המקיים $\sigma^2 = Id$, ו־ $\sigma(x) = x \to x \in \mathbb{Z}$.

תרגיל 3.2.4 (**) הראה ש־ $\mathbb{Z}[\sqrt{D}] \cong \left\{\begin{pmatrix} a & bD \\ b & a \end{pmatrix} : a, b \in \mathbb{Z}\right\}$.

תרגיל 3.2.5 (**) יהי $R = \left\{n + m\sqrt{-3} : 2m, 2n, n + m \in y\right\}$. הוכח: R תת־חוג של $\mathbb{C}$.

תרגיל 3.2.6 (**) פתור את המשוואה $(3 + 2\sqrt{2})^n - \sqrt{2}(\sqrt{2} + 1)^n + \sqrt{2} = 0$ עבור $n \in \mathbb{Z}$.

תרגיל 3.2.7 (+)** הוכח שכל אידיאל $I \triangleleft [\sqrt{D}]$ מכיל מספר טבעי, והסק שחוג המנה $\mathbb{Z}[\sqrt{D}]/I$ סופי. הסק מכאן ש־ I אידיאל ראשוני אם ורק אם הוא מקסימלי.

יהי $\alpha = a + b\sqrt{D} \in \mathbb{Z}[\sqrt{D}]$.

תרגיל 3.2.8 (+)** א. אם $\alpha | n$, $n \in \mathbb{Z}$, אז $N(\alpha) | n$. הדרכה. התחל במקרה $(a, b) = 1$.
ב. $\langle \alpha \rangle \cap \mathbb{Z} = \langle N(\alpha) \rangle$.

תרגיל 3.2.9 (***) אם $\alpha = a + b\sqrt{D}$ כאשר $(a, b) = 1$ אז $\left|\mathbb{Z}[\sqrt{D}]/\langle\alpha\rangle\right| = N(\alpha)$. במקרה הכללי, $\left|\mathbb{Z}[\sqrt{D}]/\langle\alpha\rangle\right| = \frac{N(\alpha)}{(a,b)}$. הדרכה. אם $(a, b) = 1$ אז גם $(b, N(\alpha)) = 1$. לכן התנאי $a + b\sqrt{D} \equiv 0$ שקול לתנאי מהצורה $\sqrt{D} \equiv k$.

תרגיל 3.2.10 (+)** הוכח ש־ $2, 3, 4 \pm \sqrt{10}$ הם איפריקים בחוג $\mathbb{Z}[\sqrt{10}]$. הסק ש־ $\mathbb{Z}[\sqrt{10}]$ אינו תפ"י ולכן גם אינו אוקלידי.

תרגיל 3.2.11 (**) הראה ש־ $2 \cdot 11 = 22 = (3 + \sqrt{-13})(3 - \sqrt{-13})$ הם שני פירוקים של 22 לגורמים איפריקים, והסק ש־ $\mathbb{Z}[\sqrt{-13}]$ אינו תחום פריקות יחידה.

תרגיל 3.2.12 (־*)** הוכח שהאידיאל $\left\langle 3, 1+2\sqrt{-5} \right\rangle$ אינו אידיאל ראשי בחוג $\mathbb{Z}[\sqrt{-5}]$.

תרגיל 3.2.13 (+)** הוכח שהאידיאל $I = \left\langle 2, 1+\sqrt{5} \right\rangle$ של $\mathbb{Z}[\sqrt{5}]$ מקיים $I^2 = I\langle 2\rangle$, למרות ש־$I \neq \langle 2\rangle$. הראה ש־ $J = \left\langle 4, 1+3\sqrt{5} \right\rangle$ מקיים $J^3 = \langle 2\rangle^3$. חשב את חוגי המנה $\mathbb{Z}[\sqrt{5}]/I$ ו־ $\mathbb{Z}[\sqrt{5}]/J$.

תרגיל 3.2.14 (־*)** הוכח שהאידיאל $\left\langle 7, 5-2\sqrt{11} \right\rangle$ אינו אידיאל ראשי בחוג $\mathbb{Z}[\sqrt{11}]$.

תרגיל 3.2.15 (+)** הוכח שהאידיאל $I = \left\langle 21, 9+3\sqrt{-5}, -2+4\sqrt{-5} \right\rangle$ של $R = \mathbb{Z}[\sqrt{-5}]$ הוא ראשי. הדרכה. העזר בשיקולי נורמה כדי למצוא את היוצר של I.

תרגיל 3.2.16 (***) נתבונן באיבר $7 \in R = \mathbb{Z}[\sqrt{-13}]$.

א. נסמן $I = \left\langle 7, 1+\sqrt{-13} \right\rangle$, $I' = \left\langle 7, 1-\sqrt{-13} \right\rangle$. הוכח ש־ $\langle 7\rangle = I \cdot I'$, אבל 7 איפריק בחוג.

ב. הראה ש־ 7 אינו ראשוני ב־ R.

ג. הוכח ש־ $R/\langle 7\rangle \cong \mathbb{Z}_7 \times \mathbb{Z}_7$ (ולכן $\langle 7\rangle$ אינו אידיאל ראשוני), ו־ $R/I \cong \mathbb{Z}_7$ (ולכן I ראשוני).

תרגיל 3.2.17 (***) יהי $R = \mathbb{Z}[\sqrt{7}]$.

א. הראה שאין $a \in R$ עם $N(a) = 3$.

ב. האידיאל $I = \left\langle 3, \sqrt{7}-1 \right\rangle$ אינו ראשי; בפרט, $3R \subset I$.

ג. האידיאל $J = \left\langle 2, \sqrt{7}-1 \right\rangle$ הוא ראשי.

ד. הראה ש־ $I^2 = Ra$ לאיזשהו $a \in R$.

ה. $N(a) = 9 = N(3)$.

ו. הוכח ש־ $I^2 \cap \mathbb{Z} = 9\mathbb{Z}$.

ז. $R/3R \cong \mathbb{Z}_3 \times \mathbb{Z}_3$ (הדרכה. הגדר $(x \mapsto (2-\sqrt{7})x, (2+\sqrt{7})x) + 3R$), אבל $R/aR \cong \mathbb{Z}_9$.

ח. הראה ש־ $3R + I^2 = I$.

ט. הסק ש־ $3R + I^n = I$ לכל $1 \leq n$.

יהי $D > 0$ שלם שאין לו מחלקים מהצורה p^2 $(1 < p)$. נסמן $R = \mathbb{Z}[\sqrt{D}]$. אם $x \in R$, $x = n + \sqrt{D}m$, נסמן $x' = n$ ו־ $x'' = m$.
נאמר ש־ $x > 0$ אם $0 < x', x''$; $x < y$ אם $0 < y - x$. (יחס זה אינו הופך את החוג ל"חוג סדור", משום שהוא לא יניארי).

תרגיל 3.2.18 (**) א. אם $0 < x, y$, אז גם $0 < x + y$ ו־ $0 < xy$.

ב. אם $0 < x, y$, אז $x' \leq (xy)'$. זהו אי־שוויון חזק, כלומר, $x' < (xy)'$, אלא אם $x'' = 0$ ו־ $y' = 1$.

"משוואת Pell" היא המשוואה $a^2 - Db^2 = 1$, כאשר $a, b \in \mathbb{Z}$. אומרים ש־(a, b) הוא פתרון למשוואת פל, וגם ש־$x = a + b\sqrt{D}$ הוא פתרון.

תרגיל 3.2.19 (־)** $x = x' + x''\sqrt{D} \in \mathbb{Z}[\sqrt{D}]$ הוא הפיך אם ורק אם $x'^2 - Dx''^2 = \pm 1$.

תרגיל 3.2.20 (**) יהי $x = x' + x''\sqrt{D} \in \mathbb{Z}[\sqrt{D}]$ איבר שאינו שייך ל־$\mathbb{Z}$ וגם לא ל־$\mathbb{Z}\sqrt{D}$. הראה שבדיוק אחד מבין ארבעת האברים $\pm x, \pm\overline{x}$ הוא חיובי. הסק: אם $x \in \mathbb{Z}[\sqrt{D}]$ הפיך, אז בדיוק אחד מבין ארבעת האברים $\pm x, \pm x^{-1}$ הוא חיובי.

תרגיל 3.2.21 (**) יהיו $(x', x''), (y', y'')$ פתרונות למשוואת Pell. הוכח שגם הזוג הסדור $(x'y' + Dx''y'', x'y'' + x''y')$ פתרון למשוואה. **הדרכה.** x, y הפיכים.

תרגיל 3.2.22 (***) הוכח: קיים $z \in R$ כך שכל איבר הפיך הוא מהצורה $\pm z^n$ עבור $n \in \mathbb{Z}$ (זהו **משפט דיריכלה** למקרה של שדות ריבועיים עם דיסקרימיננטה חיובית). הדרכה:

1. נניח ש־$x, y > 0$ הפיכים. הוכח ש־$x' > y'$ אם ורק אם $x'' > y''$, אם ורק אם $x > y$.
2. נניח ש־ $y > x > 0$ פתרונות למשוואת פל. הראה ש־$y > yx^{-1} > 0$.
3. הוכח שקיים $z > 0$ כך שכל פתרון למשוואת פל הוא מהצורה $\pm z^m$ עבור $m \in \mathbb{N}$: בחר פתרון $z > 0$ מינימלי, והנח בדרך השלילה שיש פתרון $x > 0$ שאינו חזקה של z.
4. סיים את הוכחת המשפט.

תרגיל 3.2.23 (***) מצא את כל היחידות של $\mathbb{Z}[\sqrt{3}]$.
פתרון. הפתרון המינימלי של המשוואה $a^2 - 3b^2 = \pm 1$ הוא $a = 2, b = 1$. נסמן $\eta = 2 + \sqrt{3}$. האברים ההפיכים ב־ $\mathbb{Z}[\sqrt{3}]$ הם $\pm\eta^n$, $n \in \mathbb{Z}$; ואין בלתם.

תרגיל 3.2.24 (***) מצא חמישה אברים הפיכים בחוג $\mathbb{Z}[\sqrt{6}]$.

תרגיל 3.2.25 (***) מצא חמישה אברים הפיכים בחוג $\mathbb{Z}[\sqrt{5}]$.

3.2.1 איברים הפיכים

תרגיל 3.2.26 (+*) $u \in R$ הפיך אם ורק אם $N(u) = \pm 1$.

תרגיל 3.2.27 (**) נניח ש־ $D < 0$. מצא את כל האברים ההפיכים ב־ $\mathbb{Z}[\sqrt{D}]$.

תרגיל 3.2.28 (**) מצא את $(3 + 2\sqrt{2})^{-1}$ בחוג $\mathbb{Z}[\sqrt{2}]$.

תרגיל 3.2.29 (־*)** מצא את כל האברים ההפיכים בחוג

$$\mathbb{Z}[\frac{1+\sqrt{-3}}{2}] = \left\{ n + m\frac{1+\sqrt{-3}}{2} : n, m \in \mathbb{Z} \right\}.$$

תרגיל 3.2.30 (***) הראה שהמשוואה $a_n + b_n\sqrt{3} = (1+\sqrt{3})^n$ מגדירה היטב $a_n, b_n \in \mathbb{Z}$. חשב את $\lim \frac{a_n}{b_n}$.

תרגיל 3.2.31 (**) הראה ש־ $7 - 4\sqrt{2}, 5 + 2\sqrt{2}$ חברים בחוג $\mathbb{Z}[\sqrt{2}]$.

3.3 איברים ראשוניים ואי־פריקים

3.3.1 יחס החלוקה

יהי R חוג קומוטטיבי עם יחידה.

הגדרה 3.3.1 $a, b \in R$. נאמר ש־ a מחלק את b אם קיים $c \in R$ כך ש־ $b = ac$. במקרה זה נסמן $a|b$.

תרגיל 3.3.2 (**) היחס "מחלק" הוא יחס רפלקסיבי וטרנזיטיבי (קדם־סדר חלקי חלש).

תרגיל 3.3.3 (*) לכל $a \in R$, $a|0$ ו־ $1|a$.

הגדרה. יהיו $a, b \in R$ אברים לא הפיכים. אם $a|b$ וגם $b|a$ נאמר ש־ a, b חברים, ונסמן $a \sim b$.

תרגיל 3.3.4 (**) $a \sim b$ אם ורק אם קיים $u \in R$ הפיך כך ש־ $b = ua$.

תרגיל 3.3.5 (*) יחס החברות הוא יחס שקילות.

תרגיל 3.3.6 (**) יחס החילוק מוגדר היטב על מחלקות השקילות ביחס לחברות (כלומר ־ אם $a_1 \sim a$ ו־ $b_1 \sim b$, אז $a|b \Rightarrow a_1|b_1$).

תרגיל 3.3.7 (+)** יחס החילוק הוא יחס סדר חלש על אוסף מחלקות החברות.

תרגיל 3.3.8 (**) הראה שבחוג $\mathbb{Z}/n\mathbb{Z}$, אם $t \in \mathbb{Z}$ אז t חבר של (t, n); כלומר, בכל מחלקת־חברות יש נציג המחלק את n. הוכח שנציג זה הוא יחיד.

תרגיל 3.3.9 (***) פתור את המשוואה $(3n+5)|(2n^2-11)$ עבור $n \in \mathbb{Z}$. פתרון. הראה ש־ $49 \in \langle 3n+5, 2n^2-11 \rangle$ ולכן $3n+5|49$ ו־ $n = -2, -4, -18$.

תאור לפי אידיאלים

תרגיל 3.3.10 (־)** $a|b$ אם ורק אם $Rb \subseteq Ra$.

תרגיל 3.3.11 (**) $a \sim b$ אם ורק אם $Ra = Rb$.

3.3.2 איברים הפיכים

3.3.3 איברים אי־פריקים

יהי R תחום שלמות.
הגדרה. איבר $0 \neq a \in R$ הוא איבר איפריק אם לכל פירוק $a = bc$, b או c הפיכים.

תרגיל 3.3.12 (*) $a \in R$ איפריק אם $b|a \leftarrow b|1$ או $a|b$.

תרגיל 3.3.13 (+)** הראה כי $\bar{t} \in \mathbb{Z}/n\mathbb{Z}$ הוא איפריק אם ורק אם (t, n) מספר ראשוני (במובן הרגיל). [ראה תרגיל 3.3.1]

3.3.4 איברים ראשוניים

הגדרה. איבר $p \in R$ הוא ראשוני אם $p|a \leftarrow p|ab$ או $p|b$.

תרגיל 3.3.14 (**) כל איבר ראשוני הוא איפריק.

תרגיל 3.3.15 (**) $p \in R$ ראשוני אם ורק אם R/Rp תחום שלמות (כלומר, אם ורק אם Rp אידיאל ראשוני).

לסיכום, Rx מקסימלי $\Leftarrow$ Rx ראשוני $\Leftrightarrow$ x ראשוני $\Leftarrow$ x איפריק.

3.4 פירוק לגורמים

תרגיל 3.4.1 (**) אם $N(x)$ מספר ראשוני ב־ $\mathbb{Z}$, אז x איפריק ב־ R.

תרגיל 3.4.2 (***) א. אם $x \in R$ ראשוני ואינו חבר של איבר ב־ $\mathbb{Z}$, אז $N(x)$ ראשוני. ב. אם $x \in R$ ראשוני חבר של איבר ב־ $\mathbb{Z}$, אז $N(x)$ ריבוע של מספר ראשוני בשלמים.

תרגיל 3.4.3 (+*)** יהי $S = \mathbb{Z}[\sqrt{D}]$ כאשר $D \in \mathbb{Z}$. אם $N(x) \in \mathbb{Z}$ ראשוני, אז x ראשוני ב־ S. הוכחה. S מוכל בחוג דדקינד R, עם אותה נורמה. $N(x) = |R/Rx|$ ראשוני, לכן R/Rx שדה ו־ Rx אידיאל מקסימלי. מכאן ש־ x ראשוני ב־ R, ולכן ב־ S.

תרגיל 3.4.4 (**) יתכן ש־ $x \in \mathbb{Z}[\sqrt{-1}]$ איפריק למרות ש־ $N(x)$ פריק. הצעה: $x = 3$.

תרגיל 3.4.5 (־*)** נניח ש־ $D < 0$. מספר האברים עם נורמה n בחוג $\mathbb{Z}[\sqrt{D}]$ הוא סופי לכל n. משפט ($^{3+}$). $n \in$. קיים $x \in [\sqrt{-1}]$ כך ש־ $n = N(x)$ אם ורק אם בפירוק $n = p_1^{\alpha_1} \dots p_t^{\alpha_t}$, לכל $p_i \equiv -1 \pmod 4$ החזקה α_i זוגית.

תרגיל 3.4.6 (־*)** א. הראה שאם $2|N(x)$ אז קיים מחלק $v|x$ עם $N(v)=2$.
ב. הראה שאם $3|N(x)$ אז $3|x$.

תרגיל 3.4.7 (***) הראה שאם $m|N(x)$ וקיים y כך ש־ $m=N(y)$, אז קיים z כך ש־ $m=N(z)$ ו־ $z|x$. הדרכה. פירוק לגורמים ראשוניים.
יהי $p\in\mathbb{Z}$ ראשוני.

תרגיל 3.4.8 (**) p אי־פריק בחוג $\mathbb{Z}[\sqrt{D}]$ אם ורק אם לא קיימים $a,b\in\mathbb{Z}$ כך ש־ $a^2-Db^2=\pm p$.

תרגיל 3.4.9 (**) אם $p\equiv\pm3 \pmod 8$, אז p איפריק ב־ $\mathbb{Z}[\sqrt{2}]$.

תרגיל 3.4.10 (־*)** p ראשוני בחוג $\mathbb{Z}[\sqrt{D}]$ אם ורק אם הפתרון היחיד למשוואה $a^2\equiv Db^2 \pmod p$ הוא $a\equiv b\equiv 0$. הדרכה (לכיוון הקשה). נניח ש־ $p|(\alpha+\beta\sqrt{D})(\gamma+\delta\sqrt{D})$, אבל p אינו מחלק את $\alpha+\beta\sqrt{D},\gamma+\delta\sqrt{D}$. הראה ש־ $\alpha,\beta,\gamma,\delta\equiv 0 \pmod p$, ושי $\alpha\gamma\equiv -D\beta\delta, \alpha\delta\equiv-\beta\gamma$. מצא a,b שעליהם אפשר להפעיל את ההנחה.

תרגיל 3.4.11 (**) (ניסוח אחר). p ראשוני בחוג $\mathbb{Z}[\sqrt{D}]$ אם ורק אם D אינו שארית ריבועית מודולו p.

תרגיל 3.4.12 (**) הראה ש־ $p=11$ הוא איפריק בחוג $\mathbb{Z}[\sqrt{-6}]$, אבל אינו ראשוני שם.

תרגיל 3.4.13 (**) הוכח ש־ $7+10\sqrt{-1}$ ראשוני ב־ $\mathbb{Z}[\sqrt{-1}]$.

תרגיל 3.4.14 (**) פרק לגורמים ראשוניים ב־ $\mathbb{Z}[\sqrt{-1}]$ את 2 ואת 5.

תרגיל 3.4.15 (**) פרק לגורמים ראשוניים ב־ $\mathbb{Z}[\sqrt{-1}]$ את $13+11i$ ואת $11+13i$.

תרגיל 3.4.16 (**) פרק לגורמים אי־פריקים את $48-31\sqrt{6}$ בחוג $\mathbb{Z}[\sqrt{6}]$.

תרגיל 3.4.17 (**) מצא פירוק של $15-7\sqrt{-5}$ לגורמים איפריקים ב־ $\mathbb{Z}[\sqrt{-5}]$.

תרגיל 3.4.18 (**) פרק לגורמים אי־פריקים את $145+62\sqrt{-11}$ בחוג $\mathbb{Z}[\sqrt{-11}]$.

תרגיל 3.4.19 (־)** יהיו $\alpha,\beta\in\mathbb{Z}[\sqrt{D}]$. אם קיים להם מחלק משותף מקסימלי $\gamma=(\alpha,\beta)$, אז $N(\gamma)|(N(\alpha),N(\beta))$.

תרגיל 3.4.20 (**) מצא מחלק משותף מקסימלי ב־ $\mathbb{Z}[i]$ של $3+4i, 4-3i$, ושל $11+7i, 18-i$.

תרגיל 3.4.21 (**) מצא את כל המחלקים המשותפים המקסימליים ב־ $\mathbb{Z}[i]$ של $7+4i, 11+10i$.

תרגיל 3.4.22 (**) חשב את המחלק המשותף המקסימלי של $23-9\sqrt{3}, 9-3\sqrt{3}$ בחוג $\mathbb{Z}[\sqrt{3}]$.

תרגיל 3.4.23 (־*)** הסבר מדוע השוויון $6 = \sqrt{6}\cdot\sqrt{6} = 2\cdot 3$ אינו סותר את העובדה ש־ $\mathbb{Z}[\sqrt{6}]$ הוא אוקלידי. הדרכה: מצא איברים בעלי נורמה $-2, 3$.

תרגיל 3.4.24 (***) הראה ש־ $\mathbb{H}_0 = \{a+bi+cj+dk : a,b,c,d \in \mathbb{Z}\}$ הוא תת־חוג של חוג הקווטרניונים $\mathbb{H}$. הוכח שגם $\mathbb{H}_1 = \mathbb{H}_0 + \mathbb{Z}\frac{1+i+j+ij}{2}$ הוא תת־חוג. חשב את חוגי המנה $\mathbb{H}_0/\langle 2\rangle$ ו־ $\mathbb{H}_1/\langle 2\rangle$ (שים לב שהחוג השני אינו קומוטטיבי).

תרגיל 3.4.25 (־*)** תן תנאי הכרחי ומספיק לכך ש־ $x \in \mathbb{H}_0$ הפיך ב־ $\mathbb{H}_0$, ומצא את כל האברים ההפיכים.

תרגיל 3.4.26 (־*)** הוכח: $9+2i+3j+3k$ הוא איבר איפריק של $\mathbb{H}_0$.

תרגיל 3.4.27 (***) פרק לגורמים אי־פריקים את 2 ב־ $\mathbb{Z}[\rho_8]$, כאשר $\rho_8 = e^{\frac{2\pi i}{8}}$.

תרגיל 3.4.28 (־*)** אם $d \equiv 1 \pmod 4$, אז $R = \mathbb{Z}[\sqrt{d}]$ אינו תחום־פריקות־יחידה. הדרכה. קח $\alpha = 1+\sqrt{d}$. הראה ש־ $2|\alpha^2$, והסק ש־ 2 אינו ראשוני ב־ R. הראה שהוא אי־פריק.

3.4.1 חוגים אטומיים

3.4.2 תחומי פריקות יחידה

משפט 3.4.29 (**) יהי R חוג אוקלידי. אז כל $a \in R$ הוא מכפלה $a = q_1\cdots q_t$ של איברים איפריקים.

משפט 3.4.30 (**) פירוק לראשוניים, אם הוא קיים, הוא יחיד (בכל תחום שלמות): יהיו $p_1,\ldots,p_n$, $q_1,\ldots,q_m$ ראשוניים, כך ש־ $p_1\ldots p_n = q_1\ldots q_m$. אז $n=m$ ויש התאמה $p_i \leftrightarrow q_j$ כך ש־ $p_i \sim q_j$.

משפט 3.4.31 (***) בחוג אוקלידי, כל איבר איפריק הוא ראשוני.

הגדרה. תחום שלמות שבו לכל איבר קיים פירוק יחיד (עד־כדי סדר וחברות) כמכפלה של איפריקים, נקרא תחום פריקות יחידה, ובאנגלית UFD = Unique Factorization Domain.

משפט 3.4.32 (*־)** בתחום פריקות יחידה כל איבר איפריק הוא ראשוני.

משפט 3.4.33 (*+)** כל חוג אוקלידי הוא תחום פריקות יחידה.

תרגיל 3.4.34 (***) חוג שבו אין פירוק לאי־פריקים. יהי F שדה, ויהי $R = F[\lambda^r : 0 < r \in \mathbb{Q}]$ חוג הפולינומים במשתנה λ בחזקות רציונליות־חיוביות מעל F.

א. לכל $0 < r$, λ^r פריק.

ב. נגדיר פונקציות מעלה $deg(f)$ ־ המעלה המקסימלית של מונום ב־ f, ו־ $deg(f)$ המינימלית.

הוכח ש־ $deg(fg) = deg(f) + deg(g)$ ו־ $deg(fg) = deg(f) + deg(g)$.

ג. נגדיר $\delta(f) = deg(f) - deg(f)$. הוכח ש־ $\delta(fg) = \delta(f) + \delta(g)$ ולכן $\delta(fg) \geq \delta(f)$.

ד. אם fg הוא מונום (כלומר δ) $(fg) = 0$ אז f, g מונומים.

ה. הסק: לא קיים פירוק $\lambda = \pi_1 \dots \pi_n$ כאשר π_i איפריקים.

(החוג אינו נותרי)

תרגיל 3.4.35 (**) יהיו $S \subseteq R$ תחומי שלמות. אם $a \in S$ הוא ראשוני ב־ R, אז הוא ראשוני ב־ S. אם הוא איפריק ב־ R, אז הוא איפריק ב־ S. הראה שההיפך אינו בהכרח נכון, לשתי התכונות.

3.4.3 חוגים נותריים

3.4.4 תחומים ראשיים

משפט 3.4.36 (**) כל אידיאל של $\mathbb{Z}$ הוא מהצורה $n\mathbb{Z} = \langle n \rangle$.

תרגיל 3.4.37 (**) הוכח: $n \subseteq m$ אם ורק אם $m|n$.

תרגיל 3.4.38 (**) הוכח את היחסים הבאים: א. $n\mathbb{Z} + m\mathbb{Z} = (n, m)\mathbb{Z}$

ב. $n\mathbb{Z} \cap m\mathbb{Z} = [n, m]\mathbb{Z}$

ג. $n\mathbb{Z} \cdot m\mathbb{Z} = (nm)\mathbb{Z}$

תרגיל 3.4.39 (**) מצא את כל האידיאלים של $\mathbb{Z}/12$.

תרגיל 3.4.40 (**) מצא את כל האידיאלים של $\mathbb{Z}/60$.

תרגיל 3.4.41 (**) אם קיים אפימורפיזם $J \to I/$, אז $I \subseteq J$.

תרגיל 3.4.42 (+*)** מצא את כל האידיאלים של החוג $R \times R$ כאשר $R = \mathbb{Z}/4\mathbb{Z}$.

תרגיל 3.4.43 (+*)** מצא שרשרת יורדת $I_1 \supseteq I_2 \supseteq I_3 \supseteq \dots$ של אידיאלים של $\mathbb{Z}$, כך ש־ $(I_k)^2 \subseteq I_{k+1}$.

תרגיל 3.4.44 (+*)** החיתוך של כל שרשרת יורדת של אידיאלים של $\mathbb{Z}$ הוא אידיאל האפס.

הגדרה. תחום שלמות שבו כל אידיאל הוא ראשי נקרא תחום ראשי, ובאנגלית PID=Principal ideal domain.
תזכורת: (בכל תחום) האידיאל $Ra \lhd R$ הוא אידיאל ראשוני אם ורק אם a איבר ראשוני.

תרגיל 3.4.45 (**) אם Ra מקסימלי, אז a איפריק.
משפט $(^3)$: בתחום ראשי, אם a איבר איפריק אז Ra הוא אידיאל מקסימלי.
משפט $(^{3-})$: כל חוג אוקלידי הוא ראשי.
משפט $(^{3h})$: כל תחום ראשי הוא תחום פריקות יחידה.

תרגיל 3.4.46 (**) בתחום ראשי a איפריק אם ורק אם a ראשוני. הדרכה. כל אידיאל מקסימלי הוא ראשוני.
משפט $(^{2+})$: (בתחום ראשי) כל אידיאל ראשוני הוא מקסימלי. פתרון. יהי $P = Rp$ ראשוני, אז p איבר ראשוני ולכן איפריק (זה נכון בכל תחום). לכן Rp מקסימלי.

תרגיל 3.4.47 (**) F שדה. הוכח ש־ $F[x,y]$ אינו תחום ראשי (ולכן לא אוקלידי).
הערה. $F[x,y]$ הוא תחום פריקות יחידה.

תרגיל 3.4.48 (**) הראה ש־ $\mathbb{Z}[\lambda]$ אינו תחום ראשי.

תרגיל 3.4.49 (־*)** מצא סדרה יורדת של אידיאלים של $\mathbb{Z}[\lambda]$, שחיתוכה אינו אידיאל האפס.

יש דוגמא מפורסמת לחוג ראשי שאינו אוקלידי: $\mathbb{Z}[\frac{\sqrt{-19}+1}{2}]$. כדי להוכיח תכונות אלה, נעזרים בתכונה הבאה.

הגדרה 3.4.50 תחום שלמות R הוא **כמעט אוקלידי** אם קיימת עבורו פונקציה $d: R \to \mathbb{N}$ כך ש־ $d(ab) \geq d(a)$ לכל $b \neq 0$, ולכל a, b, אם b אינו מחלק את a, אז קיימים $q, q' \in R$ כך ש־ $0 < d(qa + q'b) < d(b)$.

תרגיל 3.4.51 (**) כל חוג אוקלידי הוא כמעט אוקלידי

תרגיל 3.4.52 (־*)** כל חוג כמעט אוקלידי הוא תחום ראשי

תרגיל 3.4.53 (***) כל חוג ראשי הוא כמעט אוקלידי [הדרכה: הראה שהפונקציה

$$d(p_1 \dots p_n) = 2^n$$

מקיימת את הדרישות; ראה John Greene, *Principal Ideal Domains Are Almost Euclidean*, AMS Notices, Feb. 1997, 154–157].

תרגיל 3.4.54 (***) בחוגי שלמים של שדות מספרים, כאשר מוגדרת נורמה כפלית, כל חוג ראשי הוא כמעט אוקלידי ביחס לנורמה.

זאת בניגוד לאוקלידיות: $\mathbb{Z}[\frac{\sqrt{69}+1}{2}]$ ו־ $\mathbb{Z}[\sqrt{14}]$ הם אוקלידיים, אבל לא ביחס לנורמה (דוגמאות מ־ 1994 ו־ 2004, בהתאמה).

תרגיל 3.4.55 (**) אם $0 \subset I \neq R$ אידיאל ראשי בתחום שלמות, אז $I \supset I^2 \supset I^3 \supset \dots$.

תרגיל 3.4.56 (***) מצא דוגמא לאידיאל ראשי $0 \subset I$ כך ש־ $I^2 = I$, כאשר R אינו תחום שלמות.

תרגיל 3.4.57 (**) אם $J \subseteq I$ ו־ $I = Ra$ ראשי, אז קיים אידיאל J_1 כך ש־ $J = I \cdot J_1$. הדרכה. לכל $x \in J$, $a|x$.

תרגיל 3.4.58 (***) אם $J \subset I$, I ראשי, ו־ J ראשוני, אז $J = IJ$. הדרכה. כתוב $J = I \cdot J_1$, והראה ש־ $J_1 \subseteq J$.

תרגיל 3.4.59 (**) האידיאל $\langle 3, x^3 - x \rangle \lhd \mathbb{Z}[x]$ אינו ראשי.

מחלק משותף מקסימלי

הגדרה 3.4.60 יהיו $a, b \in R$. נאמר ש־ $d \in R$ הוא מחלק משותף מקסימלי של a, b אם הוא איבר מקסימלי בין המחלקים המשותפים, כלומר, $d \,|\, a, b$, ואם $c \,|\, a, b$ אז $c \,|\, d$.

לא תמיד קיים מחלק משותף מקסימלי.

תרגיל 3.4.61 (**) אם קיים מחלק משותף מקסימלי של a, b, אז הוא יחיד עד כדי חברות.

תרגיל 3.4.62 (־*)** הראה שהאידיאל $I = \langle 96, 5n, 2n - 7 \rangle$ טריוויאלי לכל $n \in$. הדרכה. חשב את $\mathbb{Z}/I$.

הזכר בהגדרה הכללית שבסעיף **??**, ובכך שהמחלק המשותף המקסימלי, כאשר הוא קיים, מוגדר היטב עד־כדי חברות.

תרגיל 3.4.63 (**) אם $Ra + Rb$ אידיאל ראשי, אז היוצר של אותו אידיאל הוא המחלק המשותף המקסימלי של a, b.

תרגיל 3.4.64 (**) בחוג ראשי, לכל שני איברים שאינם שניהם 0 קיים מחלק משותף מקסימלי.

תרגיל 3.4.65 (***) בתחום פריקות יחידה, כל שני איברים לא הפיכים a, b אפשר להציג בצורה $a = u\pi_1^{\alpha_1} \dots \pi_n^{\alpha_n}$ ו־ $b = v\pi_1^{\beta_1} \dots \pi_n^{\beta_n}$, כאשר הגורמים π_i הם ראשוניים שאינם חברים זה לזה ו־ u, v הפיכים.

תרגיל 3.4.66 (+)** בהמשך לתרגיל הקודם, המחלק המשותף המקסימלי של a, b (איברים לא הפיכים של תחום פריקות יחידה) הוא $\pi_1^{\min\{\alpha_1,\beta_1\}} \dots \pi_n^{\min\{\alpha_n,\beta_n\}}$.

תרגיל 3.4.67 (**) בתחום ראשי, קיימים $\alpha, \beta \in R$ כך ש־ $(a, b) = \alpha a + \beta b$.

תרגיל 3.4.68 (**) חשב את המחלק המשותף המקסימלי ב־ $\mathbb{Z}$: $(320, 56)$, $(100, -26)$, $(16, 4)$.

הגדרה. $a, b \in R$ זרים אם $(a, b) = 1$, כלומר, $Ra + Rb = R$.

תרגיל 3.4.69 (+*) הראה ש־ $a, b \in R$ זרים אם ורק אם a הפיך ב־ R, או $b + Ra$ הפיך ב־ R/Ra.

תרגיל 3.4.70 (+)** $C \subseteq D$ תחומים ראשיים. הוכח: אם $a, b \in C$ זרים ב־ C, אז a, b זרים ב־ D.

תרגיל 3.4.71 (**) $(ad, bd) = (a, b)d$. בפרט, אם $c = (a, b)$ ו־ $a = ca_1, b = cb_1$, אז a_1, b_1 זרים.

תרגיל 3.4.72 (+)** בחוג $R = \mathbb{Q}[x, y]$, האברים $a = x + y - 6$ ו־ $b = xy - \alpha$ אינם זרים, לכל $\alpha \in \mathbb{Q}$. הדרכה. חוג מנה.

תרגיל 3.4.73 (+)** בחוג $R = \mathbb{Q}[x, y]$, האברים $a = x + y - 6$, $b = xy + 1$ ו־ $c = y^2 - x$ הם זרים.

תרגיל 3.4.74 (***) בתחום ראשי, נסמן ב־ $[a, b]$ איבר המקיים $Ra \cap Rb = R[a, b]$. הוכח ש־ $ab = (a, b) \cdot [a, b]$. הדרכה. כתוב $a = ca', b = cb'$ כאשר $c = (a, b)$, ו־ $\alpha a_1 + \beta b_1 = 1$. הראה שאם $x \in Ra \cap Rb$ אז $x \in Rca'b'$.

תרגיל 3.4.75 (***) הראה שבתחום ראשי, $\mathrm{Ann}_l(I \cap J) = \mathrm{Ann}_l(I) + \mathrm{Ann}_l(J)$. (ראה תרגיל 1.2.40).

תרגיל 3.4.76 (***) נניח ש־ R תחום ראשי. הוכח שכל תת־חוג נוצר סופית $S = R[\alpha_1, \dots, \alpha_n] \subseteq \mathrm{q}(R)$ הוא מהצורה $S = R[\frac{1}{a}]$ עבור a מתאים.

לעומת זאת, הראה שההרחבה $S = R[\frac{x}{y}, \frac{x^2}{y^3}]$ של $R = F[x, y]$ אינה נוצרת על־ידי איבר אחד.

מצא תת־חוג (אמיתי) של $\mathbb{Q}$, שאינו נוצר סופית מעל $\mathbb{Z}$.

תחומי Bezout

כפולה משותפת מינימלית

3.4.5 חוגים אוקלידיים

נזכיר שאם R חוג, מסמנים ב־ $R^\times$ את אוסף האברים ההפיכים.

תרגיל 3.4.77 (*) $\mathbb{Z}^\times = \{+1,-1\}$. אם R תחום שלמות, מסמנים $R^* = R - 0$ ־ המונויד הכפלי של החוג.

תרגיל 3.4.78 (*) אם F שדה, אז $F^\times = F^*$.

הגדרה: תחום שלמות R הוא חוג אוקלידי אם קיימת פונקציה $d : R^\times \to \mathbb{N}$ כך ש: אם $a|b$ אז $d(a) \le d(b)$; וכן לכל $a, b \in R$, $b \neq 0$, קיימים $q, r \in R$ כך ש־ $a = qb + r$, וכן $r = 0$ או $d(r) < d(b)$.

תרגיל 3.4.79 (**) כל שדה הוא חוג אוקלידי (ביחס לפונקציה d מתאימה).

תרגיל 3.4.80 (**) $u \in R$ הפיך אם ורק אם $d(u) = d(1)$.

תרגיל 3.4.81 (**) $0 \neq a \in R$. אם b הפיך אז $d(a) = d(ab)$, ואם b אינו הפיך אז $d(a) < d(ab)$.

תרגיל 3.4.82 (־*)** יהיו R תחום שלמות, $d : R^\cdot \to \mathbb{N} - 0$ פונקציה שומרת כפל, $d(0) = 0$. יהי $F = q(R)$ שדה השברים של R. א. נרחיב את d ל־ F לפי $d\frac{x}{y} = \left\{ \frac{d(x)}{d(y)} \right\}$. הוכח ש־ d מוגדרת היטב על F.
ב. נניח ש־ $a, b, q, r \in R$, $a = bq + r$. הוכח: $d(r) < d(b)$ אם ורק אם $d(q - a/b) < 1$. ג. עבור $y \in F$ נסמן $B(y) = \{x \in F : d(x - y) < 1\}$. הוכח: אם (R, d) חוג אוקלידי, אז $F = \bigcup_{y \in R^*} B(y)$.
ד. השתמש בסעיף ב' כדי לנסח אלגוריתם לחילוק עם שארית בחוג R.

תרגיל 3.4.83 (־*)** יהי $R = \mathbb{Z}[i]$ עם הפונקציה $d(a + bi) = a^2 + b^2$. הראה ש־ (R, d) חוג אוקלידי.

תרגיל 3.4.84 (***) מצא את ארבעת הפתרונות $q, r \in \mathbb{Z}[i]$ כך ש־ $(14 + 5i) = (3 + 7i) \cdot q + r$ ו־ $|r| < |3 + 7i|$.

תרגיל 3.4.85 (**) חשב את השארית מחילוק $145 - 71i$ ב־ $13 - 6i$.

האלגוריתם של אוקלידס (Euclid) מחשב, עבור איברים a, b בחוג אוקלידי R, את היוצר של האידיאל $Ra + Rb$, דהיינו את המחלק המשותף המקסימלי.
האלגוריתם של אוקלידס. יהיו R חוג אוקלידי, $a, b \in R$. נגדיר $c_0 = a$, $c_1 = b$, ובאינדוקציה $c_{i-1} = q_i c_i + c_{i+1}$ כאשר $d(c_i) < d(c_{i-1})$. התהליך נעצר כאשר $c_{n+1} = 0$, ואז $c_n = (a, b)$.

תרגיל 3.4.86 (*) הוכח שהתהליך סופי, וחסום את מספר הצעדים n.

דוגמא. נחשב את $(52,14)$ ב־ . נסמן c_0=25, c_1= 41. לפי ההגדרה,

$$52 = 3 \cdot 14 + 10 \Rightarrow c_2\text{=}10$$
$$14 = 1 \cdot 10 + 4 \Rightarrow c_3 = 4$$
$$10 = 2 \cdot 4 + 2 \Rightarrow c_4 = 2$$
$$4 = 2 \cdot 2 + 0 \Rightarrow c_5 = 0$$

ואכן $(52,14) = 2$.

תרגיל 3.4.87 (***) הוכח שהאלגוריתם ממלא את יעודו, כלומר, כאשר $c_{n+1} = 0$ מתקיים $c_n = (a,b)$. הדרכה. הראה ש־ $(c_{i-1}, c_i) = (c_i, c_{i+1})$ לכל $0 < i \leq n$.

ננית ש־ c מחלק משותף מקסימלי של $a, b \in R$. לפי ההגדרה, $Ra + Rb = Rc$, ובפרט $c \in Ra + Rb$. לכן קיימים $\alpha, \beta \in R$ כך ש־ $\alpha a + \beta b = c$. שכלול קל של האלגוריתם מאפשר למצוא את α, β בד בבד עם מציאת c.

דוגמא. בדוגמא הקודמת,

$$\begin{aligned}(52,14) &= 2 = 10 - 2 \cdot 4 \\ &= 10 - 2 \cdot (14 - 1 \cdot 10) \\ &= 3 \cdot 10 - 2 \cdot 14 \\ &= 3 \cdot (52 - 3 \cdot 14) - 2 \cdot 14 = 3 \cdot 52 - 11 \cdot 14.\end{aligned}$$

אלגוריתם אוקלידס הכללי. את המשוואה $c_{i-1} = q_i c_i + c_{i+1}$ המגדירה את c_{i-1} אפשר לכתוב בצורה מטריציאלית: $\begin{pmatrix} c_i \\ c_{i+1} \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & -q_i \end{pmatrix} \begin{pmatrix} c_{i-1} \\ c_i \end{pmatrix}$. באינדוקציה, אפשר לחשב

$$\begin{pmatrix} c_n \\ 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & -q_n \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -q_{n-1} \end{pmatrix} \cdots \begin{pmatrix} 0 & 1 \\ 1 & -q_2 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -q_1 \end{pmatrix} \begin{pmatrix} c_0 \\ c_1 \end{pmatrix}$$

כדי לחשב את המכפלות תוך־כדי התהליך, נגדיר $A_0 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, ובאינדוקציה $A_i = \begin{pmatrix} 0 & 1 \\ 1 & -q_i \end{pmatrix} A_{i-1}$. בסופו של דבר (כאשר $c_{n+1} = 0$), $\begin{pmatrix} c_n \\ 0 \end{pmatrix} = A_n \begin{pmatrix} c_0 \\ c_1 \end{pmatrix}$ ולכן $(c_0, c_1) = c_n = (A_n)_{11} c_0 + (A_n)_{12} c_1$.

תרגיל 3.4.88 (**) הוכח ש־ $\begin{pmatrix} c_n \\ 0 \end{pmatrix} = A_n \begin{pmatrix} c_0 \\ c_1 \end{pmatrix}$.

תרגיל 3.4.89 (**) חשב את המחלק המשותף המקסימלי של $\lambda^2 + 5\lambda + 6$ ושל $\lambda^4 + \lambda^3 - \lambda^2 + \lambda - 2$ בחוג $\mathbb{Z}[\lambda]$.

משפט ($^{2+}$). אם F שדה, אז $F[x]$ חוג אוקלידי ביחס לפונקציה deg, כלומר: לכל $f,g \in F[x]$ כך ש־ $g \neq 0$ ואינו הפיך, קיימים $q,r \in F[x]$ כך ש־ $f(x) = q(x)g(x) + r(x)$, ו־ $deg(r) < deg(g)$.

תרגיל 3.4.90 (**) מצא את המנה והשארית בחלוקת $x^4 - 2$ ב־ $x^2 - 1$ בחוג $\mathbb{Z}[x]$.

תרגיל 3.4.91 (־*)** נתון ש־ $(x^2+2)|(x^6+30x+48)$ בחוג $\mathbb{Z}_p[x]$. מצא את p.

תרגיל 3.4.92 (+)** התנהגות פתולוגית מעל חוג שאינו תחום שלמות: הוכח שהפולינום x^4-x^2-56 פריק מעל $\mathbb{Z}_3$ ומעל $\mathbb{Z}_5$, אבל אי־פריק מעל $\mathbb{Z}_3 \times \mathbb{Z}_5 \cong \mathbb{Z}_{15}$.

תרגיל 3.4.93 (**) מצא מחלק משותף מקסימלי של $x^3 - 6x^2 + 11x - 6$ ושל $2x^4 + 2x^3 - 14x^2 - 26x - 12$ בחוג $\mathbb{Z}[x]$.

תרגיל 3.4.94 (**) בצע את אלגוריתם אוקלידס על הפולינומים $f_0(x) = x^9 + x^7 + x^2 + 1$ ו־ $f_1(x) = x^6 + x^4 + x + 1$, בחוג $\mathbb{Z}_2[x]$.

תרגיל 3.4.95 (**) מצא $f \in \mathbb{Z}_3[x]$ כך ש־

$$\langle f \rangle = \left\langle x^6 + 2x^2 + 1, x^9 + x^5 + 2x + 2, x^8 + 2x^7 + x^3 + x^2 + 2 \right\rangle.$$

תרגיל 3.4.96 (**) מצא את $x^4 - x^3 - 12x^2 + x + 3$, $2x^3 + 9x^2 + 3x - 18$ מעל $\mathbb{Z}$.

תרגיל 3.4.97 (+)** חשב את $(2x+3)^{-1} \pmod{x^2-2}$, כלומר, מצא את ההופכי של $2x+3$ בחוג $\mathbb{Z}[x]/\langle x^2-2 \rangle$. הדרכה. מצא $\alpha(x), \beta(x)$ כך ש־ $(2x+3)\alpha(x) + (x^2-2)\beta(x) = 1$.

אוקלידיות של חוגי שלמים

ישנם חוגים אוקלידיים שבהם פונקציית המעלה N היא, בנוסף לשאר תכונותיה הטובות, כפלית. חלק מן החוגים $\mathbb{Z}[\sqrt{D}]$ הם כאלה. אחרים הם אוקלידיים, למרות שלא ביחס לפונקציה $a + b\sqrt{D} \mapsto a^2 - Db^2$.

משפט (^{3}): אם $D = -2, -1, 2, 3$, אז $R = \mathbb{Z}[\sqrt{D}]$ חוג אוקלידי.

הדרכה. העזר בקריטריון על כיסוי $q(R)$ בכדורים. עבור $\frac{a}{b} \in q(R)$, כתוב $\frac{a}{b} = \frac{ab}{N(b)} = q + \frac{r+s\sqrt{D}}{N(b)}$, כאשר $\left|\frac{r}{N(b)}\right|, \left|\frac{s}{N(b)}\right| \leq \frac{1}{2}$. אז $\left|N(\frac{r+s\sqrt{D}}{N(b)})\right| = \left|\frac{N(r+s\sqrt{D})}{N(b)^2}\right| = \frac{|r^2-s^2D|}{|N(b)|^2} \leq \frac{1+|D|}{4} < 1$.

תרגיל 3.4.98 (**) מצא את השארית מחילוק $15+11\sqrt{2}$ ב־ $4-3\sqrt{2}$ בחוג $\mathbb{Z}[\sqrt{2}]$.

תרגיל 3.4.99 (+)** מצא את המחלק המשותף המקסימלי של $14+3\sqrt{3}$ ו־ $2-9\sqrt{3}$ בחוג $\mathbb{Z}[\sqrt{3}]$.

תרגיל 3.4.100 (+)** הסבר מדוע הפירוק $6=2\cdot 3=(1+\sqrt{7})(-1+\sqrt{7})$ אינו סותר את העובדה ש־ $\mathbb{Z}[\sqrt{7}]$ חוג אוקלידי (ולכן גם תחום פריקות יחידה).

הקשר בין האקסיומות $(E1)$ ו־$(E2)$

תנאי הכרחי לאוקלידיות

פרק 4

פולינומים ושדות

4.1 מבוא לתורת השדות

תרגיל 4.1.1 (*) אם F שדה, אז $F^* = F - 0$ חבורה ביחס לכפל. תזכורת. חבורה מסדר n ואקספוננט n היא ציקלית.

משפט $(^2)$. כל תת־חבורה סופית G של החבורה הכפלית של שדה היא ציקלית. הדרכה. אם $e = exp(G)$ אז כל אברי G הם שורשים של הפולינום $x^e - 1$.

תרגיל 4.1.2 (**) יהי K שדה הרחבה של $\mathbb{Z}_2$ הנוצר על־ידי איבר אלגברי α מדרגה 3. תאר את מבנה החבורות $(K, +)$ ו־ $(K - 0, \cdot)$.

תרגיל 4.1.3 (+)** בנה שדה F מסדר 9 ומצא $u \in F$ כך שכל $v \neq 0$ ב־ F הוא חזקה של u.

4.1.1 ממד של אלגברות

הגדרה. הרחבה K/F נקראת הרחבה סופית אם K מרחב וקטורי ממימד סופי מעל F. את המימד מסמנים $dim_F(K) = [K : F]$.

הגדרה. הרחבה K/F נקראת אלגברית מעל F אם כל איבר $a \in K$ הוא אלגברי מעל F.

משפט $(^2)$. כל הרחבה סופית היא אלגברית. הוכחה. יהי $a \in K$. מכיוון שהמימד של $F[a] \subseteq K$ סופי, הקבוצה $1, a, a^2, \ldots$ תלויה ליניארית מעל F ולכן קיים פולינום המאפס את a.

תרגיל 4.1.4 (**) אם $a \in K$ אלגברי מעל F אז $F(a)$ הרחבה אלגברית של F.

תרגיל 4.1.5 (**) הרחבה אלגברית פשוטה היא סופית.

תרגיל 4.1.6 (־)** נניח ש־ $F \subseteq L \subseteq K$, $a \in K$, a אלגברי מעל F. הוכח ש־ a אלגברי מעל L.

משפט ($^{-3}$). אם $F \subseteq L \subseteq K$ הרחבות סופיות, אז $[K:F] = [K:L] \cdot [L:F]$.

תרגיל 4.1.7 (*) אם ההרחבות $F \subseteq L, L \subseteq K$ סופיות, אז גם $F \subseteq K$ סופית.
דוגמא. $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ מרחב וקטורי ממימד 2, עם בסיס $1, \sqrt{2}$. $\mathbb{Q}(\sqrt{2})(\sqrt{3})/\mathbb{Q}(\sqrt{2})$ ממימד 2 עם בסיס $1, \sqrt{3}$. לכן, $\mathbb{Q}(\sqrt{2})(\sqrt{3}) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ מרחב וקטורי ממימד 4 מעל $\mathbb{Q}$, עם בסיס $1, \sqrt{2}, \sqrt{3}, \sqrt{6}$.

תרגיל 4.1.8 (**) מצא בסיס ל־ $\mathbb{Q}(\sqrt{3}, \sqrt{5}, i)$ מעל $\mathbb{Q}$. מה מימד ההרחבה?

תרגיל 4.1.9 (***) יהיו $p_1, \ldots, p_t \in \mathbb{Z}$ מספרים זרים בזוגות. הוכח כי המימד $[\mathbb{Q}(\sqrt{p_1}, \ldots, \sqrt{p_t}) : \mathbb{Q}] = 2^t$. פתרון. נניח, באינדוקציה, שהטענה נכונה לכל $p_1, \ldots, p_t$ זרים. (השלם את המקרה $t = 1$). נסמן $K_i = (\sqrt{p_1}, \ldots, \sqrt{p_i})$, אז לפי ההנחה $[K_t : \mathbb{Q}] = 2^t$. לכן $[K_{t+1} : \mathbb{Q}] = [K_{t+1} : K_t] \cdot [K_t : \mathbb{Q}] = [K_t(\sqrt{p_{t+1}}) : K_t] \cdot 2^t \leq 2^{t+1}$, ומספיק להוכיח ש־ $\sqrt{p_{t+1}} \in K_t = K_{t-1}(\sqrt{p_t})$. נניח, בשלילה, ש־ $\sqrt{p_{t+1}} = \alpha + \beta\sqrt{p_t}$ עבור $\alpha, \beta \in K_{t-1}$, אז $2\alpha\beta\sqrt{p_t} = p_{t+1} - \alpha^2 - \beta^2 p_t \in K_{t-1}$. אבל $\sqrt{p_t} \in K_{t-1}$ לפי ההנחה, ולכן $\alpha\beta = 0$. אם $\beta = 0$ אז $\sqrt{p_{t+1}} \in K_{t-1} = (\sqrt{p_1}, \ldots, \sqrt{p_{t-1}})$, ואם $\alpha = 0$ אז $\sqrt{p_{t+1}p_t} = \beta p_t \in K_{t-1}$, בשני המקרים סתירה להנחת האינדוקציה.

4.1.2 הפולינום המינימלי

בסעיף הקודם בנינו הרחבות של F יש מאין. בסעיף זה נתבונן בהרחבות של F שהן תת־שדות של שדה גדול יותר. יהיו $F \subseteq K$ שדות. נאמר ש־ K הרחבה של F. את ההרחבה נסמן ב־ K/F.
הגדרה. יהי $a \in K$. $F(a)$ מוגדר להיות השדה הקטן ביותר המכיל את F ואת a (כלומר: השדה המורכב מאיברי K המתקבלים על ידי מספר סופי של פעולות חיבור, חיסור, כפל וחילוק באיברי F ובאיבר a). המעבר מהשדה F לשדה $F(a)$ נקרא סיפוח האיבר a לשדה F.

תרגיל 4.1.10 (־)** הוכח כי $F(a)$ הוא חיתוך כל תת־השדות של K המכילים את F ואת a.

תרגיל 4.1.11 (*) אם $F \subseteq F_1 \subseteq K$, F_1 שדה, ו־ $a \in F_1$, אז $F(a) \subseteq F_1$.

תרגיל 4.1.12 (**) הוכח ש־ $\mathbb{Q}(\sqrt{2}) = \left\{\alpha + \beta\sqrt{2} : \alpha, \beta \in \mathbb{Q}\right\}$ (כלומר, ש־

$$\left\{\alpha + \beta\sqrt{2} : \alpha, \beta \in \mathbb{Q}\right\}$$

שדה).

תרגיל 4.1.13 (+)** הוכח ש־ $\alpha+\beta\sqrt{3}+\gamma\sqrt{5}+\delta\sqrt{15}:\alpha,\beta,\gamma,\delta\in\mathbb{Q}$ שדה.

תרגיל 4.1.14 (־*)** הוכח ש־ $\left\{\alpha+\beta\cdot 2^{1/3}+\gamma\cdot 2^{2/3}:\alpha,\beta,\gamma\in\mathbb{Q}\right\}$ שדה.

נקבע איבר $a\in K$.
הגדרה. ההעתקה $\varphi:F[x]\to K$ המוגדרת לפי $\varphi(f(x))=f(a)$ נקראת **הומומורפיזם ההצבה**.

תרגיל 4.1.15 (*) הוכח כי φ הוא הומומורפיזם של חוגים עם יחידה.
הגדרה. נסמן $F[a]=Im\varphi=\left\{b_0+b_1a+b_2a^2+\cdots+b_na^n\right\}$.
מכיוון ש־ $F[x]$ תחום ראשי, $\operatorname{Ker}\varphi\lhd F[x]$ אידיאל ראשי. לפי משפט האיזומורפיזם הראשון, $F[a]\cong F[x]/\operatorname{Ker}\varphi$. דוגמא. $\mathbb{Z}[x]/\left\langle x^2-2\right\rangle\cong\mathbb{Z}(\sqrt{2})$.

תרגיל 4.1.16 (**) אם $Ker\varphi=0$, אז המימד של $F[a]$ (כמרחב וקטורי) מעל F אינו סופי.
משפט (^{2}). נניח ש־ $\operatorname{Ker}\varphi=\langle f\rangle\neq 0$. אז הפולינום f איפריק (ולכן $\operatorname{Ker}\varphi$ מקסימלי). הגדרה. היוצר המתוקן של $\operatorname{Ker}\varphi$ נקרא הפולינום המינימלי של a.

תרגיל 4.1.17 (*) יהי $g(x)$ הפולינום המינימלי של a מעל F. הראה ש־ $g(a)=0$.

תרגיל 4.1.18 (**) המימד של $F[a]$ מעל F שווה ל־ $deg(g)$.

תרגיל (^{2}). **חשב את המימד של** $\mathbb{Q}[\sqrt{-1}]/\mathbb{Q}$ **ושל** $\mathbb{Q}(\sqrt{-1},\sqrt{2})/\mathbb{Q}(\sqrt{2})$.

תרגיל 4.1.19 (**) הבאים שקולים: $F[a]$ שדה.

$F[a]=F(a)$.

$Ker\varphi\neq 0$ (כלומר ־ קיים פולינום מעל F המאפס את a).

$Ker\varphi$ אידיאל מקסימלי.

אם תנאים אלה מתקיימים, אומרים ש־ a איבר אלגברי מעל F.

תרגיל 4.1.20 (**) יהיו $R\subseteq S$ חוגים, $b\in S$. הראה שקיים הומומורפיזם יחיד $\varphi:R[\lambda]\to S$ המקיים $\varphi(r)=r$ לכל $r\in R$, ו־ $\varphi(\lambda)=b$. הדרכה. הראה ש־ $\varphi(a_0+\cdots+a_n\lambda^n)=a_0+\cdots+a_nb^n$.

תרגיל 4.1.21 (**) יהי R חוג, $b\in R$. נסמן ב־ φ את ההצבה $\varphi:R[\lambda]\to R$ המוגדרת לפי $\varphi(f)=f(b)$. הראה ש־ φ אפימורפיזם, ומצא יוצר של האידיאל $\operatorname{Ker}(\varphi)$.

הגדרה. פולינום אי־פריק $f(\lambda) \in F[\lambda]$ נקרא פולינום ספרבילי אם בכל הרחבה $F \subseteq K$, השורשים של f שונים זה מזה.
משפט [3]. $f(\lambda) \in F[\lambda]$ אינו ספרבילי אם ורק אם $f' = 0$.

תרגיל 4.1.22 (**) $f' = 0$ אם ורק אם $f(\lambda) = g(\lambda^p)$ לאיזשהו פולינום g.

תרגיל 4.1.23 (־*)** $f(\lambda) = a_n\lambda^n + \cdots + a_0 \in F[\lambda]$ איפריק. הוכח שאם $a_i^{1/p} \in F$ לכל i, $p = charF$, אז f ספרבילי.

4.1.3 שורשים ושדה מפצל

אם $f(x) = a_0+a_1x+\cdots+a_nx^n \in F[x]$ ו־ $b \in F$, אז $f(b) = a_0+a_1b+\cdots+a_nb^n$. אומרים ש־ b שורש של f אם $f(b) = 0$.

תרגיל 4.1.24 (־)** יהי F שדה, ויהיו $a, b \in F$ אברים שונים. הוכח כי $x-a, x-b \in F[x]$ זרים.

תרגיל 4.1.25 (**) יהי F שדה ויהי $f(x) \in F[x]$. הוכח כי $(x-a)|f(x)$ אם ורק אם $f(a) = 0$.

תרגיל 4.1.26 (**) מספר השורשים של $f(x) \in F[x]$ בשדה F אינו עולה על $deg(f)$.

תרגיל 4.1.27 (+*) כל פולינום ממעלה ≤ 2 שיש לו שורשים בשדה הוא פריק (בחוג הפולינומים).

תרגיל 4.1.28 (**) מצא פולינום פריק מעל $\mathbb{Q}$ שאין לו שרשים ב־$\mathbb{R}$.

תרגיל 4.1.29 (**) אם $f(x) \in F[x]$ פולינום ללא שורשים, ו־ $deg(f) \leq 3$, אז $f(x)$ איפריק מעל F.
תרגיל [2]. הוכח כי הפולינום x^3-2 איפריק מעל .
תרגיל [2]. הוכח כי $x^2 + x + 1$ אי פריק מעל $\mathbb{Z}_2$.

תרגיל 4.1.30 (**) הוכח כי $x^2 + 1$ אי פריק מעל $\mathbb{Z}_7$.

תרגיל 4.1.31 (+)** פרק את הפולינום $x^4 + 1$ למכפלת פולינומים אי פריקים ב $\mathbb{Z}_{13}$.

תרגיל 4.1.32 (**) $x^3 - 2$ פריק מעל $\mathbb{Z}_{113}$ (אין צורך למצוא פירוק).

תרגיל 4.1.33 (**) אם $f(z) \in \mathbb{R}[z]$ ו־ $\alpha \in \mathbb{C}$ שורש של f, אז גם $\bar{\alpha}$ (הצמוד המרוכב) הוא שורש של f.

תרגיל 4.1.34 (+)** אם $F \subseteq L \subseteq K$, $a \in K$ אלגברי, אז $[L[a] : L] \leq [F[a] : F]$.

תרגיל 4.1.35 (**) אם $a_1, \ldots, a_n \in K$ אלגבריים, אז $F \subseteq F[a_1, \ldots, a_n]$ הרחבה סופית. משפט (^{3}). אם ההרחבות $F \subseteq L$ ו־ $L \subseteq K$ הן אלגבריות, אז גם $F \subseteq K$ אלגברית.

הוכחה. יהי $a \in K$. לפי ההנחה קיים פולינום $f(x) = b_0 + \cdots + b_n x^n \in L[x]$ כך ש־ $f(a) = 0$. נסמן $L_0 = F(b_0, b_1, \ldots, b_n)$. לפי ההנחה על L/F, b_i אלגבריים ולכן $F \subseteq L_0$ הרחבה סופית. לבסוף, $[L_0[a] : L_0] \leq n$, לכן ההרחבה $L_0[a]/F$ סופית, ולכן גם $F[a]/F$ סופית, ו־ a אלגברי.

תרגיל 4.1.36 (**) הוכח שאם $a, b \in K$ אלגברים מעל F אז $a+b$, $a-b$, ab, a/b אלגבריים מעל F. הדרכה. חשוב על ההרחבה $F(a, b)$. הגדרה. קבוצת האיברים של Kשהם אלגבריים מעל F נקראת הסגור האלגברי של F ב־ K.

תרגיל 4.1.37 (*) הסגור האלגברי הוא תת־שדה של K.

תרגיל 4.1.38 (**) מצא הרחבות אלגבריות של שאינן סופיות.

הגדרה. יהיו $F \subseteq K$ שדות ו־ $f(x) \in F[x]$. נאמר ש־ K שדה פיצול של $f(x)$ מעל F אם

א. כל שרשי $f(x)$ נמצאים ב K.

ב. K הוא הקטן ביותר ביחס לתכונה זו, כלומר: אם קיים שדה המכיל את כל שורשי$f(x)$ וכן $F \subseteq E \subseteq K$ אז $E = K$.

דוגמא. $F = \mathbb{Q}$, $f(x) = x^2 - 2$. שדה הפיצול הוא $\mathbb{Q}(\sqrt{2})$ שכן שרשי $f(x)$, $\pm\sqrt{2}$, נמצאים ב־ $\mathbb{Q}(\sqrt{2})$.

דוגמא. $F =$, $f(x) = x^2 + 2$. שני השרשים הם $\pm\sqrt{-2}$, ולכן שדה הפיצול הוא $\mathbb{Q}(\sqrt{-2})$.

תרגיל 4.1.39 (**) $\mathbb{Q}(\sqrt{-2}) \subset \mathbb{Q}(\sqrt{-1}, \sqrt{2})$.

תרגיל 4.1.40 (־)** אם E הוא שדה הפיצול של הפולינום $f(x) \in F[x]$ אז $f(x)$ מתפצל ב $E[x]$ לגורמים לינאריים, מהצורה $x - \alpha_i$.

תרגיל 4.1.41 (**) יהיו $F \subseteq K$ שדות, $f(x) \in F[x]$ פולינום, ו־ $\alpha_1, \ldots, \alpha_n \in K$ השורשים של f. אז תת־השדה $F[\alpha_1, \ldots, \alpha_n]$ של K הוא שדה פיצול של f.

תרגיל 4.1.42 (**) מצא את שדה הפיצול של $(x^2 - 1)(x^2 + 1)$ מעל $\mathbb{Q}$.

תרגיל 4.1.43 (**) מצא את שדה הפיצול של $1+x^4$ מעל $\mathbb{Q}$.

תרגיל 4.1.44 (־*)** מצא את שדה הפיצול של $x^4 - 2$ מעל $\mathbb{Q}$. מה מימדו?

תרגיל 4.1.45 (**) מצא את שדה הפיצול E של $x^4 - 8x^2 + 15$ מעל $\mathbb{Q}$. מצא $d \in E$ כך ש־ $E = \mathbb{Q}[d]$.

משפט (^{3}). לכל פולינום קיים שדה פיצול, והוא יחיד עד־כדי איזומורפיזם.

משפט ($^{2+}$). אם $f \in F[x]$ פולינום ממעלה n עם שדה פיצול E, אז $[E : F] \leq n!$.

סיפוח שורשים

יהי F שדה, ויהי $f(x) \in F[x]$ פולינום איפריק. בסעיף זה נראה כיצד לבנות שדה K המכיל את F, כך שלפולינום $f(x)$ יש שורש ב־ K.

$F[x]$ הוא חוג אוקלידי, ובפרט תחום ראשי. מכיוון ש־ $f(x)$ איפריק, $I = \langle f \rangle$ אידאל מקסימלי ואז $K = F[x]/I$ שדה. לדוגמא, $\mathbb{R}[x]/\langle x^2+1 \rangle$ הוא שדה. בהמשך נראה שזהו שם אחר לשדה המרוכבים.

תרגיל 4.1.46 (*) בכל מחלקת שקילות ב־ $F[x]/I$ יש נציג שהוא פולינום ממעלה קטנה מ־ $deg(f)$. הדרכה. השתמש באלגוריתם של אוקלידס.

תרגיל 4.1.47 (**) נסמן: $u = x + \langle f \rangle = [x]$. הוכח כי $\{1, u, u^2, \ldots, u^{n-1}\}$ בסיס של $F[x]/I$: א. כל איבר של $F[x]/I$ הוא צירוף לינארי של איברי $1, u, u^2, \ldots, u^{n-1}$ עם מקדמים מ־ F.

ב. הצגה זו היא יחידה.

תרגיל 4.1.48 (*) הוכח כי ההעתקה $F \to F[x]/I$ המוגדרת ע"י $a \mapsto a + I$ היא מונומורפיזם.

הוכחנו, אם כן, שיש ל־ F עותק איזומורפי בתוך $F[x]/I$. מעתה נאמר ש־ F תת־שדה של $F[x]/I$.

תרגיל 4.1.49 (**) הפולינום f מוגדר גם מעל השדה הגדול יותר, $F[x]/I$. הוכח כי $u = x + I$ הוא שורש של הפולינום f.

דוגמא. נתבונן בשדה הממשיים $\mathbb{R}$. נסמן $f(x) = x^2 + 1$. איברי חוג המנה $\mathbb{R}[x]/\langle x^2+1 \rangle$ הם ביטויים מהצורה $au + b$ כאשר $u = x + \langle x^2+1 \rangle$, $a, b \in \mathbb{R}$, ו־ $u^2 + 1 = 0$. לכן, $\mathbb{R}[x]/\langle x^2+1 \rangle \cong \mathbb{C}$.

דוגמא. נתבונן בפולינום $f(x) = x^3 + x + 1$ מעל השדה $\mathbb{F}_2$. $f(x)$ איפריק מעל $\mathbb{Z}_2$, מכיוון שאין לו שורשים (והוא ממעלה 3). לכן $K = \mathbb{Z}_2[x]/\langle f(x) \rangle$ שדה, ממימד 3 מעל $\mathbb{Z}_2$.

כל איבר של $\mathbb{Z}_2/\langle f \rangle$ הוא צירוף לינארי של שלושת אברי הבסיס, עם מקדמים מ־ $\mathbb{Z}_2$, ולכן מספר האברים הוא $2^3 = 8$.

אם נסמן $a = x + \langle f(x) \rangle \in K$, אז $1, a, a^2$ הוא בסיס ל־ K מעל $\mathbb{Z}_2$. איברי K הם $0, 1, a, a+1, a^2, a^2+1, a^2+a, a^2+a+1$. שים לב שאפשר לבחור לתפקיד a כל שורש של f ב־ K (יש שלושה כאלה: a, a^2, a^2+a).

תרגיל 4.1.50 (*) הראה ש־ $a+a=0$ ב־ K. פתרון. $a+a = (1+1)\cdot a = 0 \cdot a = 0$.

תרגיל 4.1.51 (+*) כתוב את לוח הכפל של K.

דוגמא. $(a+a^2)(a+1) = a^2 + a + a^3 + a^2 = a^3 + 2a^2 + a = a^3 + a = (-a-1) + a = 1$.

תרגיל 4.1.52 (+)** בנה שדה בעל 27 איברים ומצא בסיס עבורו מעל $\mathbb{Z}_3$.

תרגיל 4.1.53 (+)** בנה שדה בעל 121 איברים ומצא בסיס עבורו מעל $\mathbb{Z}_{11}$.

תרגיל 4.1.54 (**) יהי $S = \mathbb{R}[x]/\langle x^2+x+2\rangle$.
א. הוכח כי S הוא שדה הרחבה של $\mathbb{R}$ (כלומר, הוכח כי S הוא שדה והוכח שיש מונומורפיזם $\mathbb{R} \to S$). ב. מצא את כל הפתרונות של המשוואה $x^2+1=0$ ב־ S.

דוגמא. נבנה הרחבה של $\mathbb{Q}$ המכילה שורשים לשני פולינומים איפריקים: x^2-2 ו־ x^2-3. נסמן $L_2 = \mathbb{Q}[x]/\langle x^2-2\rangle$ ו־ $L_3 = \mathbb{Q}[x]/\langle x^2-3\rangle$.

תרגיל 4.1.55 (**) הוכח שלפולינום x^2-2 אין שורשים ב־ L_3, ולי־ x^2-3 אין שורשים ב־ L_2.

תרגיל 4.1.56 (**) $K_{23} = L_2[y]/\langle y^2-3\rangle$ ו־ $K_{32} = L_3[y]/\langle y^2-2\rangle$ הם שדות הרחבה של $\mathbb{Q}$.

תרגיל 4.1.57 (+)** בתרגיל הקודם, הוכח ש־ $K_{23} \cong K_{32}$.

תהי $T \subseteq K$ קבוצה כלשהיא. נסמן ב $F(T)$ את השדה הקטן ביותר המכיל את F ואת T.

תרגיל 4.1.58 (*) הוכח כי אם $T = \{a_1, \ldots, a_n\}$ אז $F(T) = F(a_1, \ldots, a_n) = F(a_1)(a_2)\cdots(a_n)$.
הגדרה. הרחבה $K \supseteq F$ נקראת הרחבה פשוטה של F אם $K = F(a)$ עבור איזשהוא $a \in K$. דוגמאות. $\mathbb{Q}(\sqrt{5})$ הרחבה פשוטה של $\mathbb{Q}$. $\mathbb{C}$ הרחבה פשוטה של $\mathbb{R}$ כי $\mathbb{C} = \mathbb{R}[i]$.

תרגיל 4.1.59 (**) $\mathbb{Q}(\sqrt{2},\sqrt{3}) = \mathbb{Q}(\sqrt{2}+\sqrt{3})$ (ולכן) הרחבה פשוטה של $\sqrt{2},\sqrt{3}$. פתרון. מספיק להוכיח הכלה בשני הכיוונים, כלומר, $\sqrt{2}+\sqrt{3} \in (\sqrt{2},\sqrt{3})$ ו־ $\sqrt{2},\sqrt{3} \in \sqrt{2}+\sqrt{3}$. הטענה הראשונה מיידית. כדי להוכיח ש־ $\sqrt{2} \in (\sqrt{2}+\sqrt{3})$ נסמן $a = \sqrt{2}+\sqrt{3}$, ונבחין כי $a^3 = 11\sqrt{2}+9\sqrt{3} = 9a+2\sqrt{2}$ ולכן $\sqrt{2} = \frac{1}{2}(a^3-9a) \in (a)$.

תרגיל 4.1.60 (**) יהיו p,q ראשוניים. הוכח ש־ $(\sqrt{p},\sqrt{q}) = (\sqrt{p}+\sqrt{q})$.

תרגיל 4.1.61 (+)** הראה ש־ $(\sqrt{2}\cdot 5^{1/3}) = (\sqrt{2},5^{1/3})$. רמז. $(\sqrt{2}\cdot 5^{1/3})^4 = 20\cdot 5^{1/3}$.

תרגיל 4.1.62 (**) יהי F שדה סופי ממאפיין $p = charF$.
א. F מכיל בתוכו את $\mathbb{Z}_p$ (עד כדי איזומורפיזם), או במילים אחרות, יש מונומורפיזם מ $\mathbb{Z}_p$ ל F. ב. F הוא מרחב וקטורי מעל $\mathbb{Z}_p$. ג. הסק: מספר האברים של F הוא חזקה של מספר ראשוני.

תרגיל 4.1.63 (**) כל שדה בגודל p^n הוא שדה פיצול של $x^{p^n}-x$, ולכן כולם איזומורפיים (אם הם קיימים).
משפט ([3]). שדה הפיצול של הפולינום $x^{p^n}-x$ מעל השדה $\mathbb{Z}_p$ הוא שדה בן p^n אברים.

תרגיל 4.1.64 (**) פרק לגורמים איפריקים מעל $\mathbb{Z}_3$, $\mathbb{Z}_7$ את x^3+2 ואת x^2+2x-1.

תרגיל 4.1.65 (+)** יהי $F=\mathbb{Z}_2[\alpha]$ כאשר $\alpha^3+\alpha+1=0$. פרק את x^3+x+1 ואת x^3+x^2+1 לגורמים איפריקים מעל $\mathbb{Z}_2$.

תרגיל 4.1.66 (+)** x^3-9 איפריק מעל $\mathbb{Z}_{31}$, אבל מתפצל לגורמים ליניאריים מעל $\mathbb{Z}_{11}$.

תרגיל 4.1.67 (־*)** הוכח ש־ x^4+1 אי פריק מעל $\mathbb{Q}$, אבל הוא פריק מעל כל שדה $\mathbb{Z}_p$. רמז. אם $p\neq 2$, אז בחבורה הכפלית של השדה מסדר p^2 קיים איבר מסדר 8.

תרגיל 4.1.68 (+)** לחוג $\mathbb{Z}_4[\alpha]/\langle\alpha^2+\alpha+1\rangle$ יש אידיאל יחיד, שהוא $\langle 2\rangle$. הוכח ש־ $R/\langle 2\rangle$ שדה בן ארבעה אברים. מה הכפל באידיאל (כחוג) ?

תרגיל 4.1.69 (־*)** מצא כמה פולינומים מתוקנים איפריקים ממעלה 2 יש מעל שדה סופי F.

4.2 פירוק של פולינומים

4.2.1 שורשים רציונליים

משפט ([2]). **יהי** $f(x)=a_0+a_1x+\cdots+a_nx^n\in[x]$. **אם** $u/v\in$ **שורש של** f**, אז** $u|a_0$ **ו־** $v|a_n$.

תרגיל 4.2.1 (**) הוכח שלפולינום x^n־ אין שורשים ב־ כאשר p ראשוני.

תרגיל 4.2.2 (**) הוכח כי הפולינום $8x^3-6x-1$ איפריק מעל .

תרגיל 4.2.3 (**) הוכח כי הפולינום x^3-x^2-2x-1 איפריק מעל .

תרגיל 4.2.4 (+)** הפולינום $3x^3+2x-12$ איפריק מעל . רמז. $f'(x)>0$ תמיד, ובקטע $(1,2)$ יש שורש.

4.2.2 קריטריון אייזנשטיין

תרגיל 4.2.5 (**) יהי $I \lhd R$. הוכח ש־ $R[x]/I[x] \cong (R/I)[x]$, וש־ $I[x] + \lhd R[x]$.

הקריטריון של אייזנשטיין. יהיו R תחום שלמות, $f(x) = a_0 + a_1 x + \cdots + a_n x^n \in R[x]$. נניח שקיים ראשוני $P \lhd R$ כך ש־ $a_0, \ldots, P_{n-1} \in$, אבל $a_n n \in P$, ו־ $a_0 \in P^2$. אז $f(x)$ איפריק ב־ $R[x]$.

תרגיל 4.2.6 (***) הוכח את הקריטריון.

הדרכה. הנח ש־ $f(x) = g(x)h(x)$, וחשב את התמונה ב־ $R[x]/P[x]$, שהוא תחום שלמות. הבחן שלפולינום x^n יש פירוק יחיד מעל כל תחום שלמות.

תרגיל 4.2.7 (**) הוכח שהפולינום $x^5 + 12x^3 - 36x^2 + 21$ איפריק ב־ $\mathbb{Z}[x]$.

תרגיל 4.2.8 (**) יהי $p \in R$ ראשוני, R תחום פריקות יחידה. הוכח ש־ x^n־ איפריק ב־ $R[x]$.

תרגיל 4.2.9 (+)** הוכח ש־ $f(x) = x^4 + x^3 + x^2 + x + 1$ איפריק מעל . הדרכה. חשב את $f(x+1)$. הראה שאם $f(x+1)$ איפריק אז גם $f(x)$ איפריק.

תרגיל 4.2.10 (+)** הוכח ש־ $4x^6 - 121x^3 + 110$ איפריק בחוג $\mathbb{Z}[\sqrt{-1}][x]$.

דוגמא. $p(x,y) = y^2 + (x^2+2)y + (x^2+2)(x^3+2)$ איפריק מעל $\mathbb{Z}[x,y]$ לפי הקריטריון של אייזנשטיין, עם הראשוני $x^2 + 2$ בחוג $\mathbb{Z}[x]$.

תרגיל 4.2.11 (+)** הוכח כי $x^3y + x^3 - x^2y + xy - x^2 + y^2 + x + 2y + 2$ אי־פריק ב־ $\mathbb{Z}[x,y]$.

תרגיל 4.2.12 (**) הוכח שאם $p \nmid a_n$, $p^{n+1-i} \mid a_i$ ו־ $p^{n+2} \nmid a_0$, אז הפולינום $f(x) = a_n x^n + \cdots + a_0$ אי־פריק.

4.2.3 הלמה של גאוס

סעיף זה מאפשר ליישם משפטים על איפריקות מעל $\mathbb{Q}$ לאיפריקות מעל $\mathbb{Z}$.

יהיו D תחום פריקות יחידה ו־ $F = q(D)$ שדה השברים.

הגדרה. מעל תחום פריקות יחידה (ובפרט, תחום ראשי), התכולה של פולינום $f(x) = a_0 + a_1 x + \cdots + a_n x^n \in D[x]$ מוגדרת כמחלק המשותף המקסימלי של המקדמים $a_0, \ldots, a_n$. . פולינום נקרא פרימיטיבי אם $c(f) = 1$ (כלומר, $c(f)$ הפיד).

משפט 4.2.13 (הלמה של גאוס (***)) אם $f(x) \in D[x]$ פרימיטיבי ואיפריק מעל D, אז הוא איפריק מעל F.

תרגיל 4.2.14 (+)** הוכח כי הפולינום $x^6 + x^3 + 1$ איפריק מעל.

תרגיל 4.2.15 (+)** האם הפולינום $2x^5 + 36x^3 + 60x^2 - 24$ פריק מעל $\mathbb{Q}$? מעל $\mathbb{Z}$?

משפט 4.2.16 (***) אם R תחום פריקות יחידה, אז גם $R[x]$ תחום פריקות יחידה.

תכולה של פולינום

הלמה של גאוס

פירוק פולינומים מעל תחום פריקות יחידה