תורת החוגים

עוזי וישנה

זוהי חוברת תרגילים[1] המלווה את הקורסים "תורת החוגים" ו-"אלגברה מו-פשטת 2" בבר-אילן. החומר חולק למספר גדול של נושאים, וכל אחד מהם מוצג (במידת האפשר) בשלמותו - כולל ההגדרות והמשפטים היסודיים. טענות העזר והשיטות הסטנדרטיות נוסחו כתרגילים, ולחלקם ניתנת הדרכה או רמז. כל סעיף מחולק לכמה נושאים, ובכל נושא השאלות מסודרות כך שהתרגילים התאורטיים יותר קודמים.

התרגילים (כולל הטענות והמשפטים) מלווים בציון רמת הקושי שלהם: תר-גילים 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. למשל, סעיף 4.4 (על חוגים עם נורמה). לעומת זאת, החוברת אינה נוגעת במודולים.

גרסה מוקדמת של החוברת נכתבה (במאי 2000) עם אלי בגנו. החומר תורגם באופן אוטומטי-למחצה מקובץ Oren, ואני תולה בתוכנת התרגום את כל השגיאות (גם אלו שהכנסתי במו-ידי). בשאר הבעיות אשמים השגעונות של LaTeXבעברית.

[1] June 2006, Version 4.1

תוכן עניינים

פרק 1

מבוא

1.1 חוגים

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 (**) הוכח את הזהויות הבאות: א. $-0 = 0$.
ב. $0 \cdot a = 0 = a \cdot 0$.
ג. $(-a) \cdot b = -(a \cdot b)$ ובפרט $-b = (-1) \cdot b$.
ד. $(-a) \cdot (-b) = a \cdot b$.

תרגיל 1.1.2 (**) 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 $\{\begin{pmatrix} 0 & a \\ b & c \end{pmatrix} : a, b, c \in \mathbb{R}\}$.

תרגיל 1.1.3 (**) 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 $x \odot y = xy - 1$.

1.1.1 איברי 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 1.1.4 (*) 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 1.1.5 (**) הוכח את הקומוטטיביות של החיבור $(a+b = b+a)$ מתוך האקסיומות האחרות של חוג עם יחידה. רמז. העזר בדיסטריבוטיביות.

תרגיל 1.1.6 (**) הוכח ש- $\mathbb{Z}_{12}$ עם החיבור הרגיל והכפל $x * y = 5xy$ הוא חוג עם יחידה.

תרגיל 1.1.7 (-**) 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.

1.1.2 איברים 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 1.1.8 (-**) אם x הפיך מימין והפיך משמאל, אז הוא הפיך.
אם R חוג, מסמנים ב- $R^\times$ את אוסף האברים ההפיכים.

תרגיל 1.1.9 (*) $R^\times$ חבורה (ביחס לכפל של החוג).

תרגיל 1.1.10 (+**) אם $R^\times$ קבוצה סופית, אז סכום אבריה הוא 0 או 1.

תרגיל 1.1.11 (**) אם $1 - ab$ הפיך בחוג אז $1 - ba$ הפיך. [רמז: חישבו על $1 + b(1 - ab)^{-1}a$].
חוג עם יחידה שבו כל איבר הפיך נקרא **חוג עם חילוק**.

תרגיל 1.1.12 (**) אם כל איבר $x \neq 0$ בחוג R הפיך משמאל, אז R הוא חוג עם חילוק.

1.1.3 קומוטטיביות

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

תרגיל 1.1.13 (**) אם החבורה החיבורית של חוג היא ציקלית, אז החוג הוא קומוטטיבי.

הגדרה 1.1.14 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.

1.1.4 המרכז

הגדרה 1.1.15 יהי $S \subseteq R$ תת-חוג. **המרכז** (ריש קמוצה) של S ב- R הוא

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

תרגיל 1.1.16 (*) $C_R(S)$ הוא תת-חוג של R.

תרגיל 1.1.17 (+*) $S \subseteq C_R(C_R(S))$.

תרגיל 1.1.18 (***) תן דוגמא לחוג R עם תת-חוג S, כך ש- $S \subset C_R(C_R(S))$.

תרגיל 1.1.19 (+**) $C_R(C_R(C_R(S))) = C_R(S)$.
אחד המשפטים היסודיים עבור אלגברות פשוטות קובע שאם S תת-אלגברה פשוטה של אלגברה פשוטה R, אז $C_R(C_R(S)) = S$.

1.1.5 זהויות

תרגיל 1.1.20 (**) יהי R חוג המקיים $x^2 = x$ לכל $x \in R$. הוכח:
א. $x + x = 0$ לכל $x \in R$.
ב. R קומוטטיבי.

תרגיל 1.1.21 (-***) 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 1.1.22 (**) נניח ש- $a, b \in R$ מקיימים $ab = a$, $ba = b$. הוכח ש- $a^2 = a$ ו- $b^2 = b$.

1.1.6 בניות סטנדרטיות של חוגים

יהי R חוג. חוג המטריצות מעל R הוא החוג $M_n(R)$ שאיבריו מטריצות $n \times n$ עם רכיבים ב- R.

תרגיל 1.1.23 (**) הראה שכפל מטריצות $(AB)_{ij} = \sum A_{ik} B_{kj}$ הוא אסוציאטיבי, ולכן $M_n(R)$ חוג.

תרגיל 1.1.24 (*) אם R חוג עם יחידה, אז גם $M_n(R)$ חוג עם יחידה.
את הגדרת הדטרמיננטה $\det : M_n(R) \to R$ המוכרת משדות אפשר להכליל לכל חוג קומוטטיבי R.

תרגיל 1.1.25 (+**) העזר בנוסחת $Cramer$ כדי להראות שאם $|A|$ הפיך ב- R, אז A הפיך ב- $M_n(R)$.

תרגיל 1.1.26 (**) R חוג עם יחידה. מצא ב- $M_n(R)$ 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 1.1.27 (+**) יהי R חוג כלשהו. מצא את $Z(M_n(R))$. יהיו R,S חוגים. המכפלה הקרטזית של R,S היא החוג $R \times S$ עם הפעולות לפי רכיבים.

תרגיל 1.1.28 (*) אם R,S חוגים עם יחידה אז גם $R \times S$ חוג עם יחידה, ו- $1_{R\times S} = (1_R, 1_S)$.

תרגיל 1.1.29 (+*) הוכח ש- $Z(R \times S) = Z(R) \times Z(S)$.

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

תרגיל 1.1.30 (+*) הוכח ש- R^{op} חוג; אם R חוג עם יחידה, גם R^{op} חוג עם יחידה.

תרגיל 1.1.31 (**) $(R^{op})^{op} = R$. אם R קומוטטיבי, $R^{op} = R$.

1.2 תת-חוגים ואידיאלים

1.2.1 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 1.2.1 (**) נסמן $S = \{\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} : a \in \mathbb{Q}\}$, $D = \{\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} : a,b \in \mathbb{Q}\}$, $U = \{\begin{pmatrix} a & c \\ 0 & b \end{pmatrix} : a,b,c \in \mathbb{Q}\}$, $T = \{\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} : a,b \in \mathbb{Q}\}$, $R = M_2(\mathbb{Q})$.

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 1.2.2 (**) הראה ש- $A_2 = \{n + m\sqrt{2} : n,m \in \mathbb{Z}\}$ ו- $A_7 = n + m\sqrt{7} : n,m \in \mathbb{Z}$ הם תת-חוגים של $\mathbb{R}$. מצא את $A_7 \cap A_2$. האם $A_2 \cap A_7$ תת-חוג של A_2?

1.2.2 אידיאלים חד-צדדיים

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

תרגיל 1.2.3 (*) לכל $x \in R$, $Rx = \{rx : r \in R\}$ הוא אידיאל שמאלי של R.

תרגיל 1.2.4 (+*) אם $L \leq_l$ אידיאל שמאלי, ו- $x \in L$, אז $Rx \subseteq L$.

תרגיל 1.2.5 (**) אם $L \leq_l R$ ו- $x \in L$ הפיך משמאל, אז $L = R$.

תרגיל 1.2.6 (-**) $L \leq_l R$ אידיאל שמאלי, $x \in R$. הוכח שגם Lx אידיאל שמאלי.

תרגיל 1.2.7 (**) R חוג. הראה ש- $I = \{\begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix} : a, b \in R\}$ אידיאל חד-צדדי של חוג המטריצות $M_2(R)$.

תרגיל 1.2.8 (+**) 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.

תרגיל 1.2.9 (**) I א ידאל שמאלי של R. הוכח שהקבוצה $\{1 - a : a \in I\}$ סגורה לכפל.

תרגיל 1.2.10 (**) הראה, על-ידי דוגמא נגדית, שבדרך-כלל $R(a+b) \neq Ra + Rb$.

1.2.3 אידיאלים (דו-צדדיים)

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

תרגיל 1.2.11 (*) 0 הוא אידיאל של R (ושמו: אידיאל האפס).

תרגיל 1.2.12 (**) יהי $\{U_\lambda : \lambda \in \Lambda\}$ אוסף אידיאלים של R. הוכח: $\bigcap_{\lambda \in \Lambda} U_\lambda$ אידיאל של R.

הגדרה 1.2.13 האידיאל הנוצר על-ידי $x \in R$ הוא $\langle x \rangle = \{\, \sum a_i x b_i \,\}$.

תרגיל 1.2.14 (**) הוכח ש- $\langle x \rangle$ אידיאל של R.

תרגיל 1.2.15 (**) בחוג קומוטטיבי, $\langle x \rangle = Rx = \{rx : r \in R\}$.
דוגמא. $2\mathbb{Z} = \{2n : n \in \mathbb{Z}\}$ הוא האידיאל הנוצר על-ידי 2 בחוג $\mathbb{Z}$.

תרגיל 1.2.16 (+**) 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- $I^{++} = I^+$.

תרגיל 1.2.17 (-***) האידיאל הנוצר על-ידי $\begin{pmatrix} n & 0 \\ 0 & m \end{pmatrix}$ ב- $M_2(\mathbb{Z})$ מכיל את $\begin{pmatrix} 0 & d \\ 0 & 0 \end{pmatrix}$, כאשר $d = (n, m)$.

תרגיל 1.2.18 (**) 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 1.2.19 (+**) 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. $\phi \neq \tau \subseteq P(X)$ הוא אידיאל אם ורק אם τ סגור לאיחוד ולהקטנה ($A, B \in \tau \rightarrow A \cup B \in \tau$ ו- $A \subseteq B \in \tau \rightarrow A \in \tau$).
ג. אם X סופי, $\tau \subseteq P(X)$ אידיאל אם ורק אם קיים $C \subseteq X$ כך ש- $\tau = P(C)$.
ד. מצא אידיאל של $P(\mathbb{Z})$ שאינו מהצורה $P(C)$.

1.2.4 חוגים פשוטים

הגדרה 1.2.20 חוג פשוט הוא חוג שאין לו אידיאלים למעט 0.

תרגיל 1.2.21 (*) שדה הוא חוג פשוט.

תרגיל 1.2.22 (**) חוג פשוט קומוטטיבי עם יחידה הוא שדה.

תרגיל 1.2.23 (+**) אם F שדה, אז $M_2(F)$ חוג פשוט.

תרגיל 1.2.24 (***) אם F שדה, $M_n(F)$ חוג פשוט.

תרגיל 1.2.25 (-**) לחוג R אין אידיאלים משמאל, אם ורק אם R הוא חוג עם חילוק.

1.2.5 פעולות באידיאלים

הגדרה 1.2.26 (**חיבור אידיאלים**) אם $I, J \triangleleft R$, $I + J = \{a + b : a \in I, b \in J\}$.

תרגיל 1.2.27 (*) $I + J$ הוא אידיאל של R.

תרגיל 1.2.28 (*) $I + J = J + I$.

תרגיל 1.2.29 (*) $(I + J) + K = I + (J + K)$.

תרגיל 1.2.30 (**) הוכח או הפרך: $Ra + Rb = R(a + b)$

הגדרה 1.2.31 ((**כפל אידיאלים**)) אם $I \leq_l R, J \leq_r R$, המכפלה $I \cdot J$ מוגדרת לפי $I \cdot J = \{\sum a_i b_i : a_i \in I, b_i \in J\}$

תרגיל 1.2.32 (**) $IJ \lhd R$.

תרגיל 1.2.33 (***) תן דוגמא לחוג R עם אידיאלים I, J, כך ש- $\{ab : a \in I, b \in J\}$ אינו אידיאל.

הצעה. $R = [x, y]$ (חוג הפולינומים בשני משתנים), $I = J =< x, y >$.

תרגיל 1.2.34 (**) $IJ \subseteq I \cap J$.

תרגיל 1.2.35 (**) אסוציאטיביות של כפל אידיאלים: $I(JK) = (IJ)K$ ($I, J, K \lhd R$).

תרגיל 1.2.36 (**) דיסטריבוטיביות של פעולות באידיאלים: $I(J + K) = IJ + IK$ ($I, J, K \lhd R$).

תרגיל 1.2.37 (-***) מצא אידיאלים I, J של $M_2(\mathbb{Z})$ כך ש- $IJ \neq JI$.

תרגיל 1.2.38 (**) R חוג קומוטטיבי עם יחידה. הוכח ש- $(Ra)(Rb) = Rab$.

1.2.6 פירוק לסכום ישר ואידמפוטנטים

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 1.2.39 (**) 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 1.2.40 (**) אם e אידמפוטנט, אז $1 - e$ אידמפוטנט אורתוגונלי אליו.

תרגיל 1.2.41 (**) 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 1.2.42 (**) הוכח שזהו אכן יחס סדר, וש- $0 \leq x \leq 1$ לכל $x \in E_C$.

תרגיל 1.2.43 (**) אם $x, y \in E$ אורתוגונליים, $x, y \leq x + y \in E$.

תרגיל 1.2.44 (**) אם $x \leq y$ אז $y - x \in E$, אורתוגונלי ל- x, ו- $x \leq y - x$.

תרגיל 1.2.45 (**) אם $x, y \in E$, אז $xy \leq x, y \leq x + y - xy$ (ולכן E הוא סריג).

תרגיל 1.2.46 (***) 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- $eh = h = he$.

1.3 דוגמאות לחוגים

תרגיל 1.3.1 (**) 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.

1.3.1 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 1.3.2 (*) הראה ש- $ji = -k$.

נגדיר העתקה $x \mapsto \bar{x}$ לפי $\overline{a + bi + cj + dk} = a - bi - cj - dk$.

תרגיל 1.3.3 (**) חשב: $\overline{x + y} = \bar{x} + \bar{y}$; $\bar{\bar{x}} = x$; $\overline{xy} = \bar{y} \cdot \bar{x}$.

נגדיר $N : \mathbb{H} \to \mathbb{R}$ לפי $N(a + bi + cj + dk) = a^2 + b^2 + c^2 + d^2$.

תרגיל 1.3.4 (**) חשב: $N(x) = xx$.

תרגיל 1.3.5 (**) (בלי לחשב): $N(x) = xx$; $N(xy) = N(x)N(y)$.

תרגיל 1.3.6 (**) הסק: $\mathbb{H}$ חוג עם חילוק.

תרגיל 1.3.7 (+**) מצא איברים לא הפיכים בחוג

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

1.3.2 אלגברת חבורה

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 1.3.8 (**) הראה ש- $F[G]$ חוג.

תרגיל 1.3.9 (+***) הראה שאם $2 \neq 0$ בשדה F, אז $F[\mathbb{Z}_4] \simeq F[\mathbb{Z}_2 \times \mathbb{Z}_2]$.

1.3.3 חוג האנדומורפיזמים

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 1.3.10 (+**) הוכח ש- $End(G)$ חוג עם יחידה.

תרגיל 1.3.11 (**) כתוב דוגמא מפורשת המראה ש- $End(G)$ אינו בהכרח קומוטטיבי.

תרגיל 1.3.12 (***) חשב את חוג האנדומורפיזמים של $R = \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/25\mathbb{Z}$.

פרק 2

משפטי איזומורפיזם

2.1 הומומורפיזמים של חוגים

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

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

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

תרגיל 2.1.2 (**) $I \lhd S$. הוכח ש- $\varphi^{-1}(I) \lhd R$.

תרגיל 2.1.3 (-**) הגרעין $Ker(\varphi) = \varphi^{-1}(0) = \{r : \varphi(r) = 0\}$ הוא אידיאל של R.

תרגיל 2.1.4 (+**) נניח ש- φ על. הוכח שתמונה של אידיאל ב- R היא אידיאל ב- S.

תרגיל 2.1.5 (**) אם D חוג פשוט (לדוגמא: שדה) ו- $\varphi : D \to R$ הומומורפיזם של חוגים, $\varphi \neq 0$, אז φ מונומורפיזם.

תרגיל 2.1.6 (**) תאר הומומורפיזם $\varphi : \mathbb{Z}[\lambda] \to \mathbb{Z}_p$, שהגרעין שלו הוא אוסף הפולינומים שסכום מקדמיהם מתחלק ב- p.

תרגיל 2.1.7 (**) הראה שהפונקציות $\varphi_0, \varphi_1 : M_n(F) \to M_{2n}(F)$ המוגדרות לפי $\varphi_0(A) = \begin{pmatrix} A & 0 \\ 0 & 0 \end{pmatrix}$ ו- $\varphi_1(A) = \begin{pmatrix} A & 0 \\ 0 & A \end{pmatrix}$ הן מונומורפיזמים של חוגים. φ_1 הוא הומומורפיזם של חוגים עם יחידה, אבל φ_0 אינו כזה.

תרגיל 2.1.8 (**) אם R חוג עם יחידה ו- $\varphi : R \to S$ אפימורפיזם, אז S חוג עם יחידה ו- $\varphi(1_R) = 1_S$.

תרגיל 2.1.9 (-***) 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- $\varphi(1_R)^2 x = \varphi(1_R) x$ לכל $x \in S$].

2.1.1 מאפסים

הגדרה 2.1.10 אם $I \subseteq R$, המאפס השמאלי של I הוא $Ann_l(I) = \{x \in R : Ix = 0\}$. המאפס הימני הוא $Ann_r(I) = \{x \in R : xI = 0\}$, והמאפס הוא החיתוך $Ann(I) = Ann_l(I) \cap Ann_r(I)$.

תרגיל 2.1.11 (+*) אם $I \leq_r R$, אז $Ann_l(I) \lhd R$ (ואם $I \leq_l R$ אז $Ann_r(I) \lhd R$).

תרגיל 2.1.12 (*) אם $I \lhd R$ אז $Ann(I) \lhd R$.

תרגיל 2.1.13 (*) הראה שאם $J \subseteq I$ אז $Ann_l(J) \subseteq Ann_l(I)$ ו- $Ann(J) \subseteq Ann_(I)$.

תרגיל 2.1.14 (**) הראה ש- $I \subseteq Ann_r(Ann_l(I))$.

תרגיל 2.1.15 (**) $Ann_l(I + J) = Ann_l(I) \cap Ann_l(J)$.

תרגיל 2.1.16 (**) $Ann_l(I \cap J) \supseteq Ann_l(I) + Ann_l(J)$.

2.1.2 איזומורפיזמים

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

תרגיל 2.1.17 (**) א. הראה שאוסף המטריצות $K = \{\begin{pmatrix} x & y \\ -y & x \end{pmatrix} : x, y \in \mathbb{R}\}$ הוא חוג.
ב. K איזומורפי לשדה המספרים המרוכבים $\mathbb{C}$.

תרגיל 2.1.18 (+**) הראה שאוסף המטריצות $U = \{\begin{pmatrix} x & y \\ -\bar{y} & \bar{x} \end{pmatrix} : x, y \in \mathbb{R}\}$ איזומורפי לחוג הקווטרניונים $\mathbb{H}$.

תרגיל 2.1.19 (+**) הראה שאוסף המטריצות

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

איזומורפי ל- $\mathbb{H}$.

תרגיל 2.1.20 (+**) 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 2.1.21 (**) הוכח שחוג האנדומורפיזמים של $\mathbb{Z}_n$ מקיים $End(\mathbb{Z}_n) \simeq \mathbb{Z}_n$. הדרכה. הגדר $\varphi \mapsto \varphi(1)$.

תרגיל 2.1.22 (-***) יהי V מרחב וקטורי ממימד n מעל שדה F. הוכח ש- $End(V) \simeq M_n(F)$.

תרגיל 2.1.23 (**) הוכח ש- $M_n(R \times S) \simeq M_n(R) \times M_n(S)$.

תרגיל 2.1.24 (-***) הוכח ש- $M_n(M_m(R)) \simeq M_{mn}(R)$.

2.2 חוגי מנה

תהי $R \supset I$ 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 2.2.1 (**) הוכח שהפעולה מוגדרת היטב אם ורק אם $I \lhd R$.

תרגיל 2.2.2 (**) נניח ש- $I \lhd R$. הוכח ש- R/I, ביחס לחיבור והכפל שהגדרנו, הוא חוג.

תרגיל 2.2.3 (*) 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 האי-דיאלים של R/I מצורה זו.

תרגיל 2.2.4 (**) נסמן $R = [x]$, $I = \langle x^n \rangle$, $J = \langle x \rangle$. חשב את $(J/I)^n$.

2.3 משפטי נתר

יהי $\varphi : R \to S$ איזומורפיזם.

תרגיל 2.3.1 (**) $Ker(\varphi) = \{a \in R : \varphi(a) = 0\}$ הוא אידיאל של R.

תרגיל 2.3.2 (+**) $Im(\varphi) = \{\varphi(a) : a \in R\}$ הוא תת-חוג של S, אבל אינו בהכרח אידיאל.

משפט 2.3.3 (**משפט האיזומורפיזם הראשון** (**)) : $R/Ker(\varphi) \cong Im(\varphi)$.

תרגיל 2.3.4 (-**) $\varphi : R \to S$, $\psi : S \to T$ אפימורפיזמים. הוכח ש- T איזומורפי לחוג מנה של R.

תרגיל 2.3.5 (**) $\varphi : R \to S$ על, $I \lhd S$. הוכח ש- $R/\varphi^{-1}(I) \simeq S/I$.

תרגיל 2.3.6 (**+) $I \lhd R$. הוכח ש- $M_n(R/I) \simeq M_n(R)/M_n(I)$. הדרכה. הגדר $\varphi : M_n(R) \to M_n(R/I)$ לפי $\varphi((a_{ij})_{ij}) = (\theta(a_{ij}))_{ij}$ כאשר $\theta : R \to R/I$ ההיטל הטבעי.

תרגיל 2.3.7 (***) כל אידיאל של $M_n(R)$ הוא מהצורה $M_n(I)$ עבור $I \lhd R$.

תרגיל 2.3.8 (**) $I \subseteq J$ אידיאלים של R. הראה שקיים אפימורפיזם $R/I \to R/J$.

משפט 2.3.9 (**משפט האיזומורפיזם השני** (**)) אם $I \subseteq J$ אידיאלים של R, אז $(R/I)/(J/I) \cong R/J$.

2.3.1 חוגי פולינומים

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

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

עם החיבור והכפל המתאימים.

תרגיל 2.3.10 (**) הראה ש- $R[\lambda]$ הוא חוג.

תרגיל 2.3.11 (**) הראה שקיים שיכון $R \to R[\lambda]$.

תרגיל 2.3.12 (**-) $a \in R[\lambda]$ הפיך אם ורק אם $a \in R$ והפיך שם.

תרגיל 2.3.13 (**) $M_n(R[\lambda]) \simeq (M_n(R))[\lambda]$.

תרגיל 2.3.14 (**) $(R \times S)[\lambda] \simeq R[\lambda] \times S[\lambda]$.

תרגיל 2.3.15 (**+) $Z(R[\lambda]) = (Z(R))[\lambda]$.

תרגיל 2.3.16 (**) יהי R חוג, $I = \langle\lambda\rangle \lhd R[\lambda]$. הוכח ש- $R[\lambda]/\langle\lambda\rangle \simeq R$.

תרגיל 2.3.17 (**) 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: $R[s] = \{a_0 + ... + a_ns^n : a_i \in R\}$. אם חושבים על λ כעל איבר של חוג הפולינומים, אז שתי המשמעויות מתלכדות בביטוי $R[\lambda]$.

תרגיל 2.3.18 (**) הסבר מדוע $R[x_1] \simeq R[x_2]$ והסק שגם $(R[x_1])[x_2] \simeq (R[x_3])[x_4]$.

תרגיל 2.3.19 (**) נסמן $R[x,y] = (R[x])[y]$. הוכח ש- $R[x,y] = (R[y])[x]$ (מה התפקיד של כל '[ ]' ?).

2.3.2 משפט השאריות הסיני

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

תרגיל 2.3.20 (**) $I, J \lhd R$ אידיאלים המקיימים $I+J=R$. הראה ש- $I\cap J = IJ+JI$.

משפט 2.3.21 (**משפט השאריות הסיני** (***)) יהיו $I_1, ..., I_t \lhd R$ אידיאלים כך ש- $I_i + I_j = R$ לכל $i \neq j$ (במקרה זה אומרים ש- $I_1, \dots, I_t$ קו-מקסימליים). אז $R/(I_1 \cap \ldots \cap I_t) \simeq (R/I_1) \times \cdots \times (R/I_t)$.[ניסוח אחר. לכל $a_1, \dots, a_t$, קיים $x \in R/(I_1 \cap \ldots \cap I_t)$ יחיד כך ש- $\forall i : x - a_i \in I_i$.]

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

תרגיל 2.3.22 (+*) 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 2.3.23 (**) נניח ש- $(n, m) = 1$ מספרים שלמים זרים. כתוב $\alpha n + \beta m = 1$. הראה ש- $x = \alpha nb + \beta ma$ הוא פתרון למערכת המשוואות $x \equiv a \pmod n$, $x \equiv b \pmod m$.

תרגיל 2.3.24 (**) פתור את המשוואה $x \equiv 2 \pmod{37}, x \equiv 2 \pmod{101}, x \equiv 2 \pmod{197}$.

תרגיל 2.3.25 (+**) פתור את המשוואה $x \equiv 2 \pmod 3, x \equiv 4 \pmod 8, x \equiv 11 \pmod{25}$.

תרגיל 2.3.26 (+**) 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 $\frac{x-a}{b-a} - \frac{x-b}{b-a} = 1$].

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

תרגיל 2.3.27 (-***) הכלל את השאלה האחרונה, והראה שלכל $a_1, ..., a_t$ שונים ולכל $b_1, ..., b_t, c_1, ..., c_t$, קיימת פונקציה $f : \mathbb{R} \to \mathbb{R}$ גזירה ברציפות, כך ש- $f(a_i) = b_i$, ו- $f'(a_i) = b_i$.

תרגיל 2.3.28 (***) העזר בחוג R שהוגדר להלן כדי להראות שהטענה הבאה אינה נכונה: "יהיו $I_1, I_2, ... \lhd R$ אידיאלים קו-מקסימליים. אז לכל $a_1, a_2, ... \subseteq R$ קיים $x \in R$ כך ש- $x - a_i \in I_i$."

פרק 3

תחומי שלמות

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

תרגיל 3.0.30 (**) תאר במפורש את כל מחלקי-אפס הימניים בחוג $M_2(\mathbb{R})$.

תרגיל 3.0.31 (-***) 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- $a \in Ra^2$.

3.0.3 איברים נילפוטנטיים

הגדרה 3.0.32 $a \in R$ נקרא איבר נילפוטנטי אם $a^n = 0$ לאיזשהו $1 \leq n$.

תרגיל 3.0.33 (+*) כל איבר נילפוטנטי הוא מחלק אפס.

תרגיל 3.0.34 (**) יהי $a \in R$ איבר נילפוטנטי. הוכח ש- $(1-a)$ הפיך. הדרכה. חשב את $(1-a)^{-1}$.

הגדרה 3.0.35 אידיאל (חד-צדדי) של R הוא אידיאל נילי אם כל איבריו נילפוטנטיים.

תרגיל 3.0.36 (**) אם $L \leq_l$ אידיאל נילי, אז $1 - a : a \in L$ חבורה כפלית.

תרגיל 3.0.37 (+**) קיימים ב- $_n$ איברים נילפוטנטיים $0 \neq$ אם ורק אם קיים ראשוני p כך ש- $p^2|n$.

תרגיל 3.0.38 (**) מצא את כל האברים הנילפוטנטיים ב- $\mathbb{Z}_{180}$.

3.0.4 תחומי שלמות

הגדרה 3.0.39 חוג קומוטטיבי D ללא מחלקי אפס (פרט ל- 0) נקרא תחום שלמות.

תרגיל 3.0.40 (+*) יהיו $0 \neq I_1, ..., I_t$ אידיאלים של תחום שלמות D. הוכח ש- $I_1 \cap .... \cap I_t \neq 0$.

תרגיל 3.0.41 (**) D תחום שלמות, $a, b \in D$ מקיימים $a^{40} = b^{40}$, $a^{27} = b^{27}$. הוכח ש- $a = b$.

תרגיל 3.0.42 (**) $\mathbb{Z}_n$ הוא תחום שלמות אם ורק אם n ראשוני.

תרגיל 3.0.43 (+**) כל תחום שלמות סופי הוא שדה (אפילו כאשר לא נתון שקיימת יחידה).

תרגיל 3.0.44 (**) הוכח או הפרך: אם D_1, D_2 תחומי שלמות, אז $D_1 \times D_2$ תחום שלמות.

תרגיל 3.0.45 (**) אם D תחום שלמות אז גם חוג הפולינומים $D[\lambda]$ תחום שלמות.

תרגיל 3.0.46 (**) תן דוגמא לחוג מנה של תחום שלמות שאינו תחום שלמות.

3.1 אידיאלים של $\mathbb{Z}$

משפט 3.1.1 (**) כל אידיאל של $\mathbb{Z}$ הוא מהצורה $n\mathbb{Z} = \langle n \rangle$.

תרגיל 3.1.2 (**) הוכח: $n \subseteq m$ אם ורק אם $m|n$.

תרגיל 3.1.3 (**) 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 3.1.4 (**) מצא את כל האידיאלים של $\mathbb{Z}/12$.

תרגיל 3.1.5 (**) מצא את כל האידיאלים של $\mathbb{Z}/60$.

תרגיל 3.1.6 (**) אם קיים אפימורפיזם $/J \to /I$, אז $I \subseteq J$.

תרגיל 3.1.7 (+**) מצא את כל האידיאלים של החוג $R \times R$ כאשר $R = \mathbb{Z}/4\mathbb{Z}$.

תרגיל 3.1.8 (+**) 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 3.1.9 (+**) החיתוך של כל שרשרת יורדת של אידיאלים של הוא אידיאל האפס.

3.2 שדה שברים

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

תרגיל 3.2.1 (**) הוכח שהיחס הנ"ל הוא יחס שקילות.
על אוסף מחלקות השקילות נגדיר פעולות: $[(a,b)] \cdot [(c,d)] = [(ac,bd)]$, $[(a,b)] + [(c,d)] = [(ad+bc,bd)]$.

תרגיל 3.2.2 (**) הראה שהפעולות מוגדרות היטב.

תרגיל 3.2.3 (**) הראה שאוסף מחלקות השקילות הוא חוג ביחס לפעולות שהגדרנו.
הגדרה. החוג שהוגדר להלן נקרא המיקום של D ב- S, ומסומן ב- S^{-1}.

תרגיל 3.2.4 (**) 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 3.2.5 (**) הראה שהאברים של S בחוג $S^{-1}D$ הם הפיכים.

תרגיל 3.2.6 (-***) (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 3.2.7 (+**) 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 3.2.8 (**) הראה ש- $q(D)$ הוא שדה.

תרגיל 3.2.9 (**) נניח ש- $t \in R$ מחלק אפס. בדוק את שלבי הבניה של $q(R)$, ומצא מה השיבוש הראשון.

תרגיל 3.2.10 (**) אם F שדה, אז $F \simeq q(F)$. הציגו במפורש את האיזומורפיזם.

תרגיל 3.2.11 (**) יהיו $D_1 \subseteq D_2$ תחומי שלמות. הראה ש- $q(D_1) \subseteq q(D_2)$.

תרגיל 3.2.12 (-***) 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: $q(D_1) \simeq q(D_2$).

תרגיל 3.2.13 (+**) אם D תחום שלמות, אז $D[x]$ (חוג הפולינומים) גם הוא תחום שלמות. תאר את שדה השברים של $D[x]$. הדרכה. ס מן $F = q(D)$. $D[x] \subseteq F[x]$, ומספיק לתאר את $q(F[x])$ (מדוע ?).

תרגיל 3.2.14 (+**) יהי $D \in \mathbb{Z}$. הראה ש-

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

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

3.3 אידיאלים מקסימליים

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

משפט 3.3.1 (***-) יהי R חוג קומוטטיבי עם יחידה. $I \lhd R$ הוא מקסימלי אם ורק אם R/I שדה.

תרגיל 3.3.2 (**) R ק ומוטטיבי. $I \lhd R$ מקסימלי אם ורק אם לכל $x \in R$, $I + Rx = R$.

תרגיל 3.3.3 (+**) $\varphi : R \to S$ על. אם $P \lhd S$ מקסימלי, הוכח שגם $\varphi^{-1}(P) \lhd R$ מקסימלי.

תרגיל 3.3.4 (+**) $\varphi : R \to \mathbb{Z}$ על. הוכח שיש ב- R אינסוף אידיאלים מקסימליים שונים.

תרגיל 3.3.5 (**) האידיאלים המקסימליים של $\mathbb{Z}$ הם $p\mathbb{Z}$ עבור p ראשוני.

תרגיל 3.3.6 (**) יהיו $F_1, ..., F_t$ שדות. מצא את האידיאלים המקסימליים של $R = F_1 \times ... \times F_t$.

תרגיל 3.3.7 (**) 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.

משפט 3.3.8 (**הלמה של צורן** (***)) בהנחה שמקבלים את אקסיומת הבחירה, כל אי-דיאל של חוג R עם יחידה מוכל באידיאל מקסימלי.

תרגיל 3.3.9 (**) R קומוטטיבי. $a \in R$ הפיך אם"ם $a + M$ הפיך ב- R/M לכל אידיאל מקסימלי M.

תרגיל 3.3.10 (***) 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 $A + B = R$. $AC \subseteq A \cap C \subseteq A, C \Leftarrow AC = 0$. בדומה $BC = 0$. כעת $C = RC = (A+B)C = AC + BC = 0 + 0 = 0$.

3.3.1 רדיקלים

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

תרגיל 3.3.11 (**) $x \in Jac(R)$ אם ורק אם $1-xy$ הפיך לכל $y \in R$.

תרגיל 3.3.12 (**+) אם $I + Jac(R) = R$ אז $I = R$.

תרגיל 3.3.13 (**) חשב את $Jac(\mathbb{Z}/24\mathbb{Z})$, $Jac(\mathbb{Z}/9\mathbb{Z})$.

תרגיל 3.3.14 (**) חשב את $Jac(\mathbb{Z}/6\mathbb{Z})$, $Jac(\mathbb{Z}/36\mathbb{Z})$.

הגדרה 3.3.15 אם R חוג קומוטטיבי, נסמן $Nil(R) = \{a \in R : \exists n a^n = 0\}$ - "הרדיקל של 0".

תרגיל 3.3.16 (*+) אם $x \in Nil(R)$, אז $x^n \in Nil(R)$ לכל n.

תרגיל 3.3.17 (*) אם D תחום שלמות אז $Nil(D) = 0$.

תרגיל 3.3.18 (*+) אם $z \in Nil(R)$ אז $1 - z$ הפיך.

תרגיל 3.3.19 (**) $Nil(R) \lhd R$.

תרגיל 3.3.20 (**+) $Nil(R/Nil(R)) = 0$.

הגדרה 3.3.21 אם $I \lhd R$, נסמן $\sqrt{I} = \{a \in R : \exists n : a^n \in I\}$ (הרדיקל של I).

תרגיל 3.3.22 (**+) הראה ש- $\sqrt{I}$ אידיאל של R [הדרכה: אם $a^n, b^m \in I$ חשוב על $(a+b)^{n+m}$].

תרגיל 3.3.23 (*) הראה ש- $\sqrt{0} = Nil(R)$.

תרגיל 3.3.24 (*) הראה ש- $I \subseteq \sqrt{I} \lhd R$.

תרגיל 3.3.25 (*) אם $J \subseteq I$ אז $\sqrt{J} \subseteq \sqrt{I}$. אידיאל המקיים $\sqrt{I} = I$ נקרא אידיאל רדיקלי.

תרגיל 3.3.26 (**) הראה ש- $\sqrt{\sqrt{I}} = \sqrt{I}$, כלומר $\sqrt{I}$ אידיאל רדיקלי.

תרגיל 3.3.27 (**) אם $I \subseteq J \lhd R$ אז $\sqrt{J/I} = \sqrt{J}/I$.

תרגיל 3.3.28 (**) כל אידיאל ראשוני הוא רדיקלי.

תרגיל 3.3.29 (**) מצא את כל האידיאלים הרדיקליים של $\mathbb{Z}$.

תרגיל 3.3.30 (**) 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- $\sqrt{I+J} \neq \sqrt{I} + \sqrt{J}$.

3.3.2 חוגים מקומיים

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

תרגיל 3.3.31 (+*) הוכח שהחוג $/256$ הוא חוג מקומי.

תרגיל 3.3.32 (+**) R מקומי אם ורק אם אוסף האברים הלא-הפיכים הוא אידיאל.

תרגיל 3.3.33 (**) F שדה. $R = \left\{ \begin{pmatrix} c & * & * \\ 0 & c & * \\ 0 & 0 & c \end{pmatrix} : c \in F^\times \right\}$ הוא חוג מקומי.

תרגיל 3.3.34 (**) R מקומי אם ורק אם $a+b=1$ גורר ש- a הפיך או b הפיך.

תרגיל 3.3.35 (-***) מצא את כל מחלקי האפס של $\mathbb{Z}_p[\lambda]/\langle \lambda^n \rangle$. הראה שזהו חוג מקומי.

3.4 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 3.4.1 (**) יהי R חוג קומוטטיבי. אם 0 הוא אידיאל ראשוני של R אז R תחום שלמות.

משפט 3.4.2 (-***) יהי R חוג קומוטטיבי. $P \lhd R$ אידיאל ראשוני אם ורק אם R/P תחום שלמות.

תרגיל 3.4.3 (**) כל אידיאל מקסימלי הוא ראשוני.

תרגיל 3.4.4 (**) האידיאלים הראשוניים של $\mathbb{Z}$ הם $p\mathbb{Z}$ (p ראשוני) ו- 0.

תרגיל 3.4.5 (+**) $\varphi : R \to S$ על. אם $P \lhd S$ ראשוני, הוכח שגם $\varphi^{-1}(P) \lhd R$ ראשוני.

תרגיל 3.4.6 (**) R חוג קומוטטיבי סופי עם יחידה. הוכח שכל אידיאל ראשוני הוא מקסימלי.

תרגיל 3.4.7 (**) 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 3.4.8 (**) נגדיר $\varphi : \mathbb{Z}[\lambda] \to \mathbb{Z}_p$ לפי $\varphi(f) = f(1)$ (כאשר p ראשוני). חשב את $I = Ker(\varphi)$. האם זהו אידיאל ראשוני? האם הוא מקסימלי?

תרגיל 3.4.9 (+**) הוכח ש- $Nil(R)$ הוא חיתוך כל האידיאלים הראשוניים של R.

תרגיל 3.4.10 (+**) תהי $\{P_\lambda : \lambda \in \Lambda\}$, $\Lambda \neq \phi$, קבוצת אידיאלים ראשוניים של חוג R, כך שלכל $\lambda, \lambda' \in \Lambda$ מתקיים $A_\lambda \subseteq A_{\lambda'}$ או $A_{\lambda'} \subseteq A_\lambda$. הוכח ש- $A = \bigcup A_\lambda$ הוא אידיאל ראשוני.

תרגיל 3.4.11 (+**) R קומוטטיבי, $A, B \lhd R$. אם $A \cap B$ אידיאל ראשוני אז $A \subseteq B$ או $B \subseteq A$.

תרגיל 3.4.12 (**) תן דוגמא מפורשת לחוג עם אידיאלים ראשוניים A_1, A_2 כך ש- $A_1 \cap A_2$ אינו ראשוני.

תרגיל 3.4.13 (+**) $\langle 3 \rangle = 3R$ הוא אידיאל ראשוני של החוג

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

תרגיל 3.4.14 (**) $\langle \lambda \rangle \lhd F[\lambda, \mu]$ ראשוני אבל לא מקסימלי.

תרגיל 3.4.15 (+**) $\langle 2\lambda - 1 \rangle \lhd \mathbb{Z}[\lambda]$ ראשוני אבל לא מקסימלי.

תרגיל 3.4.16 (+**) $I =< 5 >$ אידיאל של $\mathbb{Z}[i]$. הוכח:

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

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

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

פרק 4

תחומי שלמות מיוחדים

יהי R חוג קומוטטיבי עם יחידה.

הגדרה 4.0.17 $a,b \in R$. נאמר ש- a מחלק את b אם קיים $c \in R$ כך ש- $b = ac$. במקרה זה נסמן $a|b$.

תרגיל 4.0.18 (-**) $a|b$ אם ורק אם $Rb \subseteq Ra$.

תרגיל 4.0.19 (**) היחס "מחלק" הוא יחס רפלקסיבי וטרנזיטיבי (קדם-סדר חלקי חלש).

תרגיל 4.0.20 (*) 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 $a \approx b$.

תרגיל 4.0.21 (**) $a \approx b$ אם ורק אם קיים $u \in R$ הפיך כך ש- $b = ua$.

תרגיל 4.0.22 (**) $a \approx b$ אם ורק אם $Ra = Rb$.

תרגיל 4.0.23 (*) יחס החברות הוא יחס שקילות.

תרגיל 4.0.24 (**) יחס החילוק מוגדר על מחלקות השקילות ביחס לחברות (כלומר - אם $a_1 \approx a$ ו- $b_1 \approx b$, אז $a|b \Rightarrow a_1|b_1$).

תרגיל 4.0.25 (***) 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- $n = -2, -4, -18$.

תרגיל 4.0.26 (-***) הראה שהאידיאל $I = \langle 96, 5n, 2n-7 \rangle$ טריוויאלי לכל $n \in \mathbb{Z}$. הדרכה. חשב את $\mathbb{Z}/I$.

4.1 חוגים אוקלידיים

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

תרגיל 4.1.1 (*) $\mathbb{Z}^\times = \{+1,-1\}$. אם R תחום שלמות, מסמנים $R^* = R-0$ - המונויד הכפלי של החוג.

תרגיל 4.1.2 (*) 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 4.1.3 (**) כל שדה הוא חוג אוקלידי (ביחס לפונקציה d מתאימה).

תרגיל 4.1.4 (**) $u \in R$ הפיך אם ורק אם $d(u) = d(1)$.

תרגיל 4.1.5 (**) $0 \neq a \in R$. אם b הפיך אז $d(a) = d(ab)$, ואם b אינו הפיך אז $d(a) < d(ab)$.

תרגיל 4.1.6 (-***) 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 $d\left(\frac{x}{y}\right) = \frac{\{d(x)}{d(y)\}}$. הוכח ש- d מוגדרת היטב על F.
ב. נניח ש- $a = bq+r$, $a,b,q,r \in R$. 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 4.1.7 (-***) יהי $R = \mathbb{Z}[i]$ עם הפונקציה $d(a+bi) = a^2+b^2$. הראה ש- (R,d) חוג אוקלידי.

תרגיל 4.1.8 (***) מצא את ארבעת הפתרונות $q,r \in \mathbb{Z}[i]$ כך ש- $(14+5i) = (3+7i)\cdot q + r$ ו- $|r| < |3+7i|$.

תרגיל 4.1.9 (**) חשב את השארית מחילוק $145-71i$ ב- $13-6i$.

4.2 תחומי פריקות יחידה

4.2.1 איברים פריקים

יהי R תחום שלמות.

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

תרגיל 4.2.1 (*) $a \in R$ איפריק אם $b|1 \leftarrow b|a$ או $a|b$.

תרגיל 4.2.2 (**+) הראה כי $t \in \mathbb{Z}_n$ הוא איפריק אם ורק אם (t,n) מספר ראשוני (במובן הרגיל).

משפט 4.2.3 (**) יהי R חוג אוקלידי. אז כל $a \in R$ הוא מכפלה $a = q_1 \cdots q_t$ של איברים איפריקים.

4.2.2 אברים ראשוניים

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

תרגיל 4.2.4 (**) $p \in R$ ראשוני $p \Leftarrow$ איפריק.

תרגיל 4.2.5 (**) $p \in R$ ראשוני אם ורק אם R/Rp תחום שלמות (כלומר, אם ורק אם Rp אידיאל ראשוני).

משפט 4.2.6 (**) פירוק לראשוניים, אם הוא קיים, הוא יחיד (בכל תחום שלמות): יהיו $p_1,...,p_n$, $q_1,...,q_m$ ראשוניים, כך ש- $p_1...p_n = q_1...q_m$. אז $n = m$ ויש התאמה $q_j \leftrightarrow p_i$ כך ש- $p_i \approx q_j$.

משפט 4.2.7 (***) בחוג אוקלידי, כל איבר איפריק הוא ראשוני.

הגדרה. **תחום שלמות שבו לכל איבר קיים פירוק יחיד ,סעד-כדי סדר ותברות כמכפלה של איפריקים, נקרא תחום פריקות יחידה, ובאנגלית** UFD = Unique Factorization Domain.

משפט 4.2.8 (***-) בתחום פריקות יחידה כל איבר איפריק הוא ראשוני.

משפט 4.2.9 (**+) כל חוג אוקלידי הוא תחום פריקות יחידה.

תרגיל 4.2.10 (***) 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 $\delta(fg) = 0$) אז f,g מונומים.

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

(החוג אינו נותרי)

תרגיל 4.2.11 (**) 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.

4.3 תחומים ראשיים

4.3.1 אידיאלים ראשיים

הגדרה. אידיאל מהצורה Ra של חוג (קומוטטיבי) R נקרא אידיאל ראשי.

תרגיל 4.3.1 (**) אם $R \neq I \supset 0$ אידיאל ראשי בתחום שלמות, אז $I \supset I^2 \supset I^3 \supset \dots \supset$.

תרגיל 4.3.2 (***) מצא דוגמא לאידיאל ראשי $I \supset 0$ כך ש- $I = I^2$, כאשר R אינו תחום שלמות.

תרגיל 4.3.3 (**) 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 4.3.4 (***) אם $I \subset J$, I ראשי, ו- J ראשוני, אז $IJ = J$. הדרכה. כתוב $J = I \cdot J_1$, והראה ש- $J_1 \subseteq J$.

תרגיל 4.3.5 (**) האידיאל $\langle 3, x^3 - x \rangle \lhd \mathbb{Z}[x]$ אינו ראשי.

4.3.2 תחומים ראשיים

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 4.3.6 (**) אם Ra מקסימלי, אז a אי־פריק.

משפט (^{3}): בתחום ראשי, אם a איבר אי־פריק אז Ra הוא אידיאל מקסימלי.

משפט ($^{3-}$): כל חוג אוקלידי הוא ראשי.

משפט (^{3h}): כל תחום ראשי הוא תחום פריקות יחידה.

תרגיל 4.3.7 (**) בתחום ראשי a אי־פריק 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 אי־פריק (זה נכון בכל תחום). לכן Rp מקסימלי.

תרגיל 4.3.8 (**) F שדה. הוכח ש- $F[x, y]$ אינו תחום ראשי (ולכן לא אוקלידי). הערה. $F[x, y]$ הוא תחום פריקות יחידה.

תרגיל 4.3.9 (**) הראה ש- $\mathbb{Z}[\lambda]$ אינו תחום ראשי.

תרגיל 4.3.10 (-***) מצא סדרה יורדת של אידיאלים של $\mathbb{Z}[\lambda]$, שחיתוכה אינו אידיאל האפס.

4.3.3 מחלק משותף מקסימלי

הגדרה. בתחום ראשי: המחלק המשותף המקסימלי של a, b הוא יוצר של האידיאל $\langle a, b\rangle = Ra + Rb$. את המחלק המשותף המקסימלי נסמן ב- (a, b) (הוא מוגדר עד-כדי חברות).

בתחום פריקות יחידה, המחלק המשותף המקסימלי של $u\pi_1^{\alpha_1}\dots\pi_n^{\alpha_n}$ ו- $v\pi_1^{\beta_1}\dots\pi_n^{\beta_n}$, כאשר הגורמים π_i הם ראשוניים שאינם חברים זה לזה ו- u, v הפיכים, מוגדר להיות $\pi_1^{\min\{\alpha_1,\beta_1\}}\dots\pi_n^{\min\{\alpha_n,\beta_n\}}$.

תרגיל 4.3.11 (***) בתחום ראשי, שתי ההגדרות מתלכדות.

תרגיל 4.3.12 (**) קיימים $\alpha, \beta \in R$ כך ש- $(a, b) = \alpha a + \beta b$.

תרגיל 4.3.13 (**) $c = (a, b)$ הוא המחלק המשותף המקסימלי במובן הרגיל; כלומר - $c|a, c|b$, ואם $e|a, b$ אז גם $e|c$.

תרגיל 4.3.14 (**) חשב את המחלק המשותף המקסימלי ב- $\mathbb{Z}$: $(320, 56), (100, -26), (16, 4)$.

תרגיל 4.3.15 (**) נניח ש- $a = up_1^{\alpha_1}...p_n^{\alpha_n}$, $b = vp_1^{\beta_1}...p_n^{\beta_n}$ הפירוק למכפלת אברים איפריקים של a, b (כאשר u, v הפיכים). מצא את (a, b).

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

תרגיל 4.3.16 (+*) הראה ש- $a, b \in R$ זרים אם ורק אם a הפיך ב- R, או $b + Ra$ הפיך ב- R/Ra.

תרגיל 4.3.17 (+**) $C \subseteq D$ תחומים ראשיים. הוכח: אם $a, b \in C$ זרים ב- C, אז a, b זרים ב- D.

תרגיל 4.3.18 (**) $(ad, bd) = (a, b)d$. בפרט, אם $c = (a, b)$ ו- $a = ca_1, b = cb_1$, אז a_1, b_1 זרים.

תרגיל 4.3.19 (+**) בחוג $R = \mathbb{Q}[x, y]$, האברים $a = x + y - 6$ ו- $b = xy$ אינם זרים.
הדרכה. חוג מנה.

תרגיל 4.3.20 (+**) בחוג $R = \mathbb{Q}[x, y]$, האברים $a = x + y - 6$ ו- $b = xy - 1$ הם זרים.

תרגיל 4.3.21 (***) 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 4.3.22 (***) הראה שבתחום ראשי, $Ann_l(I \cap J) = Ann_l(I) + Ann_l(J)$. (ראה 2.1.1).

4.3.4 האלגוריתם של אוקלידס

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** $c_{i-1}=q_ic_i+c_{i+1}$ **כאשר** $d(c_{i-1})<d(c_i)$**. התהליך נעצר כאשר** 0=c_{n+1}**, ואז** $c_n=(a,b)$.

תרגיל 4.3.23 (*) הוכח שהתהליך סופי, וחסום את מספר הצעדים n.

דוגמא. נחשב את $(52,14)$ ב- . נסמן 25=c_0, 41= c_1. 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 4.3.24 (***) הוכח שהאלגוריתם ממלא את יעודו, כלומר, כאשר 0=c_{n+1} מתקיים $c_n=(a,b)$. הדרכה. הראה ש- $(c_{i-1},c_i)=(c_i,c_{i+1})$ לכל $0<i\leq n$.

נניח 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 $c_{i-1}=q_ic_i+c_{i+1}$ 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 $A_0=(\ 1\quad 00\quad 1\ )$, ובאינדוקציה $A_i=(\ 0\quad 11\quad -q_i\ )\,A_{i-1}$. בסופו של דבר (כאשר $c_{n+1}=0$), $(\ c_n0\ )=A_n\,(\ c_0c_1\ )$ ולכן $(c_0,c_1)=c_n=(A_n)_{11}c_0+(A_n)_{12}c_1$.

תרגיל 4.3.25 (**) הוכח ש- $\begin{pmatrix} c_n \\ 0 \end{pmatrix} = A_n \begin{pmatrix} c_0 \\ c_1 \end{pmatrix}$.

תרגיל 4.3.26 (**) חשב את המחלק המשותף המקסימלי של $\lambda^2 + 5\lambda + 6$ ושל $\lambda^4 + \lambda^3 - \lambda^2 + \lambda - 2$ בחוג $\mathbb{Z}[\lambda]$.

4.4 חוגים עם נורמה

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

4.4.1 נורמה בחוגים $\mathbb{Z}[\sqrt{D}]$

יהי R **חוג קומוטטיבי, המכיל (עותק של)** .

יהי $\sigma : R \to R$ **אוטומורפיזם, המקיים** $\sigma^2(x) = x$, **ובנוסף** $\sigma(x) = x$ **אם ורק אם** $x \in$.

נסמן $N(x) = x \cdot \sigma(x)$.

תרגיל 4.4.1 (**) $N : R \to$ פונקציה שומרת כפל.

יהי $D \in$. נתבונן בחוג $R = [\sqrt{D}] = \{m + n\sqrt{D} : m, n \in \mathbb{Z}\}$.

תרגיל 4.4.2 (**) א. הראה ש- R חוג. ב. $\sigma(n + m\sqrt{D}) = n - m\sqrt{D}$ הומומורפיזם, המקיים $\sigma^2 = Id$, ו- $\sigma(x) = x \to x \in ?$.

תרגיל 4.4.3 (**) הראה ש- $\mathbb{Z}[\sqrt{D}] \cong \{\begin{pmatrix} a & bD \\ b & a \end{pmatrix} : a, b \in \mathbb{Z}\}$.

תרגיל 4.4.4 (**) יהי $R = \{n + m\sqrt{-3} : 2m, 2n, n + m \in y\}$. הוכח: R תת-חוג של $\mathbb{C}$.

תרגיל 4.4.5 (**) פתור את המשוואה $(3 + 2\sqrt{2})^n - \sqrt{2}(\sqrt{2} + 1)^n + \sqrt{2} = 0$ עבור $n \in \mathbb{Z}$.

4.4.2 איברים הפיכים

תרגיל 4.4.6 (*+) $u \in R$ הפיך אם ורק אם $N(u) = \pm 1$.

תרגיל 4.4.7 (**) נניח ש- $D < 0$. מצא את כל האברים ההפיכים ב- $\mathbb{Z}[\sqrt{D}]$.

תרגיל 4.4.8 (**) מצא את $(3 + 2\sqrt{2})^{-1}$ בחוג $\mathbb{Z}[\sqrt{2}]$.

תרגיל 4.4.9 (-***) מצא את כל האברים ההפיכים בחוג

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

תרגיל 4.4.10 (***) 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 4.4.11 (**) הראה ש- $7-4\sqrt{2}, 5+2\sqrt{2}$ חברים בחוג $\mathbb{Z}[\sqrt{2}]$.

4.4.3 פירוק של איברים

תרגיל 4.4.12 (**) אם $N(x)$ מספר ראשוני ב- , אז x איפריק ב- R.

תרגיל 4.4.13 (***+) 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 4.4.14 (**) יתכן ש- $x \in \mathbb{Z}[\sqrt{-1}]$ איפריק למרות ש- $N(x)$ פריק. הצעה: $x = 3$.

תרגיל 4.4.15 (-***) 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 $n = p_1^{\alpha_1}...p_t^{\alpha_t}$, לכל $p_i \equiv -1 \pmod 4$ החזקה α_i זוגית.

תרגיל 4.4.16 (-***) 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 4.4.17 (***) 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 4.4.18 (**) 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 4.4.19 (**) אם $p \equiv \pm 3 \pmod 8$, אז p איפריק ב- $\mathbb{Z}[\sqrt{2}]$.

תרגיל 4.4.20 (-***) 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- $\alpha,\beta,\gamma,\delta \equiv 0 \pmod p$, וש- $\alpha\gamma \equiv -D\beta\delta, \alpha\delta \equiv -\beta\gamma$. מצא a, b שעליהם אפשר להפעיל את ההנחה.

תרגיל 4.4.21 (**) (ניסוח אחר). p ראשוני בחוג $\mathbb{Z}[\sqrt{D}]$ אם ורק אם D אינו שארית ריבועית מודולו p.

תרגיל 4.4.22 (**) הראה ש- $p = 11$ הוא איפריק בחוג $\mathbb{Z}[\sqrt{-6}]$, אבל אינו ראשוני שם.

תרגיל 4.4.23 (**) הוכח ש- $7 + 10\sqrt{-1}$ ראשוני ב- $\mathbb{Z}[\sqrt{-1}]$.

תרגיל 4.4.24 (**) פרק לגורמים ראשוניים ב- $\mathbb{Z}[\sqrt{-1}]$ את 2 ואת 5.

תרגיל 4.4.25 (**) פרק לגורמים ראשוניים ב- $\mathbb{Z}[\sqrt{-1}]$ את $11 + 13i$ ואת $13 + 11i$.

תרגיל 4.4.26 (**) פרק לגורמים אי-פריקים את $48 - 31\sqrt{6}$ בחוג $\mathbb{Z}[\sqrt{6}]$.

תרגיל 4.4.27 (**) מצא פירוק של $15 - 7\sqrt{-5}$ לגורמים איפריקים ב- $\mathbb{Z}[\sqrt{-5}]$.

תרגיל 4.4.28 (**) פרק לגורמים אי-פריקים את $145 + 62\sqrt{-11}$ בחוג $\mathbb{Z}[\sqrt{-11}]$.

תרגיל 4.4.29 (**-) יהיו $\alpha, \beta \in \mathbb{Z}[\sqrt{D}]$, $\gamma = (\alpha, \beta)$ המחלק המשותף המקסימלי. אז $N(\gamma)|(N(\alpha), N(\beta))$.

תרגיל 4.4.30 (**) מצא מחלק משותף מקסימלי ב- $\mathbb{Z}[i]$ של $3 + 4i, 4 - 3i$, ושל $11 + 7i, 18 - i$.

תרגיל 4.4.31 (**) מצא את כל המחלקים המשותפים המקסימליים ב- $\mathbb{Z}[i]$ של $7+4i, 11+10i$.

תרגיל 4.4.32 (**) חשב את המחלק המשותף המקסימלי של $23 - 9\sqrt{3}, 9 - 3\sqrt{3}$ בחוג $\mathbb{Z}[\sqrt{3}]$.

תרגיל 4.4.33 (***) 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 4.4.34 (***-) תן תנאי הכרחי ומספיק לכך ש- $x \in \mathbb{H}_0$ הפיך ב- $\mathbb{H}_0$, ומצא את כל האברים ההפיכים.

תרגיל 4.4.35 (***-) הוכח: $9 + 2i + 3j + 3k$ הוא איבר איפריק של $\mathbb{H}_0$.

תרגיל 4.4.36 (***) פרק לגורמים אי-פריקים את 2 ב- $\mathbb{Z}[\rho_8]$, כאשר $\rho_8 = e^{\frac{2\pi i}{8}}$.

תרגיל 4.4.37 (***-) 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.

4.4.4 אידיאלים

תרגיל 4.4.38 (**+) הוכח שכל אידיאל $I\lhd[\sqrt{D}]$ מכיל מספר טבעי, והסק שחוג המנה $\mathbb{Z}[\sqrt{D}]/I$ סופי. הסק מכאן ש- I אידיאל ראשוני אם ורק אם הוא מקסימלי. יהי $\alpha = a+b\sqrt{D}\in[\sqrt{D}]$.

תרגיל 4.4.39 (**+) 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 4.4.40 (***) אם $(a,b)=1$ אז $N(\alpha)=\left|\mathbb{Z}[\sqrt{D}]/\langle\alpha\rangle\right|$. 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 4.4.41 (**+) הוכח ש- $4\pm\sqrt{10},2,3$ הם איפריקים בחוג $\mathbb{Z}[\sqrt{10}]$. הסק ש- $\mathbb{Z}[\sqrt{10}]$ אינו תפ"י ולכן גם אינו אוקלידי.

תרגיל 4.4.42 (**) 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 4.4.43 (-***) הוכח שהאידיאל $\left\langle 3,1+2\sqrt{-5}\right\rangle$ אינו אידיאל ראשי בחוג $\mathbb{Z}[\sqrt{-5}]$.

תרגיל 4.4.44 (**+) 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 4.4.45 (***) 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 4.4.46 (***) 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. $R/3R\simeq\mathbb{Z}_3\times\mathbb{Z}_3$ (הדרכה. הגדר $(x\mapsto(2-\sqrt{7})x,(2+\sqrt{7})x)+3R$), אבל $R/aR\simeq\mathbb{Z}_9$.
ח. הראה ש- $3R+I^2=I$.
ט. הסק ש- $3R+I^n=I$ לכל $1\leq n$.

4.4.5 אוקלידיות

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 $\left|N(\frac{r+s\sqrt{D}}{N(b)})\right|=\left|\frac{N(r+s\sqrt{D})}{N(b)^2}\right|=\frac{\left|r^2-s^2D\right|}{|N(b)|^2}\leq\frac{1+|D|}{4}<1$.

תרגיל 4.4.47 (**) מצא את השארית מחילוק $15+11\sqrt{2}$ ב- $4-3\sqrt{2}$ בחוג $\mathbb{Z}[\sqrt{2}]$.

תרגיל 4.4.48 (**+) מצא את המחלק המשותף המקסימלי של $14+3\sqrt{3}$ ו- $2-9\sqrt{3}$ בחוג $\mathbb{Z}[\sqrt{3}]$.

תרגיל 4.4.49 (**+) הסבר מדוע הפירוק $6=2\cdot3=(1+\sqrt{7})(-1+\sqrt{7})$ אינו סותר את העובדה ש- $\mathbb{Z}[\sqrt{7}]$ חוג אוקלידי (ולכן גם תחום פריקות יחידה).

4.4.6 היחידות של $\mathbb{Z}[\sqrt{D}]$, $0<D$

יהי $0<D$ **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- $0<x$ **אם** $0<x',x''$; $x<y$ **אם** $0<x-y$.

תרגיל 4.4.50 (**) א. אם $0<x,y$, אז גם $0<x+y$ ו- $0<xy$.
ב. אם $0<x,y$, אז $x'\leq(xy)'$. אם $x''\neq0$ ו- $y\neq1$, אז $x'<(xy)'$.

"משוואת $Pell$" היא המשוואה $x^2-Dy^2=1$, כאשר $x,y\in$.

תרגיל 4.4.51 (**) יהיו $(x',x''),(y',y'')$ פתרונות למשוואת $Pell$. הוכח שגם $(x'y'+Dx''y'',x'y''+x''y')$ פתרון למשוואה. הדרכה. x,y הפיכים.

משפט דיריכלה ([3]). קיים $z\in R$ כך שכל איבר הפיך הוא מהצורה $\pm z^n$ עבור $n\in\mathbb{Z}$.
הוכחת המשפט. יהיו x,y הפיכים, כך ש- $0<x,y$. א. $y'<x'\Leftarrow y<x$.
ב. נניח $x<y$. הוכח $0<xy$.
ג. הוכח ש- $(xy)'<x'$. הדרכה: העלה בריבוע והצב את $x'^2=1+Dx''^2$ באגף שמאל. ד. סיים את הוכחת המשפט. הדרכה. בחר $0<y<x$ שאינם חזקות של אותו z, עם x' מינימלי. השתמש בסעיף ג' כדי להראות ש- x' אינו מינימלי.

תרגיל 4.4.52 (***) מצא את כל היחידות של $\mathbb{Z}[\sqrt{3}]$.
פתרון. הפתרון המינימלי של המשוואה $a^2-3b^2=\pm1$ הוא $a=2,b=1$. נסמן $\eta=2+\sqrt{3}$. האיברים ההפיכים ב- $\mathbb{Z}[\sqrt{3}]$ הם $\pm\eta^n$, $n\in$; ואין בלתם.

תרגיל 4.4.53 (***) מצא חמישה איברים הפיכים בחוג $\mathbb{Z}[\sqrt{6}]$.

תרגיל 4.4.54 (***) מצא חמישה איברים הפיכים בחוג $\mathbb{Z}[\sqrt{5}]$.

4.5 פולינומים מעל שדה

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

תרגיל 4.5.1 (*) אם $c \in F$ אז $deg(c) = 0$.

תרגיל 4.5.2 (*) הוכח ש- $deg(fg) = deg(f) + deg(g)$, והסק ש- $F[x]$ תחום שלמות.

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

תרגיל 4.5.4 (-***) נתון ש- $(x^2 + 2)|(x^6 + 30x + 48)$ בחוג $_p[x]$, מצא את p.

4.5.1 מחלק משותף מקסימלי

תרגיל 4.5.5 (**) 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 4.5.6 (**) 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 4.5.7 (**) 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 4.5.8 (**) מצא את $x^4 - x^3 - 12x^2 + x + 3$, $2x^3 + 9x^2 + 3x - 18$ מעל $\mathbb{Z}$.

תרגיל 4.5.9 (+**) 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- $(2x+3)\alpha(x) + (x^2 - 2)\beta(x) = 1$.

4.5.2 שורשים של פולינום

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

תרגיל 4.5.10 (-**) יהי F שדה, ויהיו $a, b \in F$ אברים שונים. הוכח כי $x-a, x-b \in F[x]$ זרים.

תרגיל 4.5.11 (**) יהיF שדה ויהי $f(x) \in F[x]$. הוכח כי $(x-a)|f(x)$ אם ורק אם $f(a) = 0$.

תרגיל 4.5.12 (**) מספר השורשים של $f(x) \in F[x]$ בשדה F אינו עולה על $deg(f)$.

תרגיל 4.5.13 (+*) כל פולינום ממעלה ≤ 2 שיש לו שורשים בשדה הוא פריק (בחוג הפולינומים).

תרגיל 4.5.14 (**) מצא פולינום פריק מעל שאין לו שרשים ב- .

תרגיל 4.5.15 (**) אם $f(x) \in F[x]$ פולינום ללא שורשים, ו- $3 \leq deg(f)$, אז $f(x)$ איפריק מעל F.

תרגיל (^{t2}). הוכח כי הפולינום x^3-2 איפריק מעל .

תרגיל (^{t2}). הוכח כי x^2+x+1 אי פריק מעל $\mathbb{Z}_2$.

תרגיל 4.5.16 (**) הוכח כי x^2+1 אי פריק מעל $\mathbb{Z}_7$.

תרגיל 4.5.17 (+**) פרק את הפולינום x^4+1 למכפלת פולינומים אי פריקים ב $\mathbb{Z}_{13}$.

תרגיל 4.5.18 (**) x^3-2 פריק מעל $\mathbb{Z}_{113}$ (אין צורך למצוא פירוק).

תרגיל 4.5.19 (**) 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.

4.5.3 שורשים מעל $\mathbb{Q}$

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

תרגיל 4.5.20 (**) הוכח שלפולינום x^n-נ אין שורשים ב- כאשר p ראשוני.

תרגיל 4.5.21 (**) הוכח כי הפולינום $8x^3-6x-1$ איפריק מעל .

תרגיל 4.5.22 (**) הוכח כי הפולינום x^3-x^2-2x-1 איפריק מעל .

תרגיל 4.5.23 (+**) הפולינום $3x^3+2x-12$ איפריק מעל . רמז. $0 < f'(x)$ תמיד, ובקטע $(1,2)$ יש שורש.

4.5.4 הקריטריון של אייזנשטיין

תרגיל 4.5.24 (**) יהי $I\lhd R$. הוכח ש- $I[x]+\lhd R[x]$, וש- $R[x]/I[x]\simeq (R/I)[x]]$.

הקריטריון של אייזנשטיין. יהיו R תחום שלמות, $f(x)=a_0+a_1x+\dots+a_nx^n\in$ $R[x]$. נניח שקיים ראשוני $P\lhd R$ כך ש- a_0, ...,ב$\in P_{n-1}$, אבל $a_nn\in P$, ו- $a_0\in P^2$. אז $f(x)$ איפריק ב- $R[x]$.

תרגיל 4.5.25 (***) 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 4.5.26 (**) הוכח שהפולינום $x^5+12x^3-36x^2+21$ איפריק ב- $\mathbb{Z}[x]$.

תרגיל 4.5.27 (**) יהי $p\in R$ ראשוני, R תחום פריקות יחידה. הוכח ש- x^n-נ איפריק ב- $R[x]$.

תרגיל 4.5.28 (**+) 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 4.5.29 (**+) 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 4.5.30 (**+) הוכח כי $x^3y+x^3-x^2y+xy-x^2+y^2+x+2y+2$ אי-פריק ב- $\mathbb{Z}[x,y]$.

4.5.5 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 $f(x)=a_0+a_1x+\dots+a_nx^n\in D[x]$ מוגדרת כמחלק המשותף המקסימלי של המקדמים $a_0,\dots,a_n$. פולינום נקרא פרימיטיבי אם $c(f)=1$ (כלומר, $c(f)$ הפיך).

משפט 4.5.31 (**הלמה של גאוס** (***)) אם $f(x)\in D[x]$ פרימיטיבי ואיפריק מעל D, אז הוא איפריק מעל F.

תרגיל 4.5.32 (**+) הוכח כי הפולינום x^6+x^3+1 איפריק מעל.

תרגיל 4.5.33 (**+) האם הפולינום $2x^5+36x^3+60x^2-24$ פריק מעל $\mathbb{Q}$? מעל $\mathbb{Z}$?

משפט 4.5.34 (***) אם R תחום פריקות יחידה, אז גם $R[x]$ תחום פריקות יחידה.

פרק 5

שדות

5.1 בניית שדה הרחבה

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

תרגיל 5.1.2 (**) נסמן: $u = x + \langle f \rangle = [x]$. הוכח כי $\{1, u, u^2, ..., u^{n-1}\}$ בסיס של $F[x]/I$: א. כל איבר של $F[x]/I$ הוא צירוף לינארי של איברי $1, u, u^2, ..., u^{n-1}$ עם מקדמים מ- F.

ב. הצגה זו היא יחידה.

תרגיל 5.1.3 (*) 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 5.1.4 (**) 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, $\mathbb{R}[x]/\langle x^2+1 \rangle \simeq \mathbb{C}$.

דוגמא. נתבונן בפולינום $f(x) = x^3 + x + 1$ מעל השדה $\mathbb{F}_2$. $f(x)$ אי־פריק 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 ליניארי 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 $_2$. 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 5.1.5 (*) הראה ש- $a + a = 0$ ב- K. פתרון. $a + a = (1+1)\cdot a = 0\cdot a = 0$.

תרגיל 5.1.6 (+*) 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 5.1.7 (+**) בנה שדה בעל 27 איברים ומצא בסיס עבורו מעל $\mathbb{Z}_3$.

תרגיל 5.1.8 (+**) בנה שדה בעל 121 איברים ומצא בסיס עבורו מעל $\mathbb{Z}_{11}$.

תרגיל 5.1.9 (**) יהי $S = \mathbb{R}[x]/\left\langle x^2 + x + 2\right\rangle$.

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 אי־פריקים: $x^2 - 2$ ו- $x^2 - 3$. נסמן $L_2 = \mathbb{Q}[x]/\left\langle x^2 - 2\right\rangle$ ו- $L_3 = \mathbb{Q}[x]/\left\langle x^2 - 3\right\rangle$.

תרגיל 5.1.10 (**) הוכח שלפולינום x^2-2 אין שורשים ב- L_3, ול- x^2-3 אין שורשים ב- L_2.

תרגיל 5.1.11 (**) $K_{23} = L_2[y]/\left\langle y^2 - 3\right\rangle$ ו - $K_{32} = L_3[y]/\left\langle y^2 - 2\right\rangle$ הם שדות הרחבה של $\mathbb{Q}$.

תרגיל 5.1.12 (+**) הוכח ש- $K_{32} \simeq K_{23}$.

5.2 שדות ותת-שדות

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 5.2.1 (-**) הוכח כי $F(a)$ הוא חיתוך כל תת-השדות של K המכילים את F ואת a.

תרגיל 5.2.2 (*) אם $F \subseteq F_1 \subseteq K$, F_1 שדה, ו- $a \in F_1$, אז $F(a) \subseteq F_1$.

תרגיל 5.2.3 (**) הוכח ש- $\mathbb{Q}(\sqrt{2}) = \{\alpha + \beta\sqrt{2} : \alpha, \beta \in \mathbb{Q}\}$ (כלומר, ש-

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

שדה).

תרגיל 5.2.4 (+**) הוכח ש- $\alpha + \beta\sqrt{3} + \gamma\sqrt{5} + \delta\sqrt{15} : \alpha, \beta, \gamma, \delta \in \mathbb{Q}$ שדה.

תרגיל 5.2.5 (-***) הוכח ש- $\{\alpha + \beta \cdot 2^{1/3} + \gamma \cdot 2^{2/3} : \alpha, \beta, \gamma \in \mathbb{Q}\}$ שדה.

5.2.1 הומומורפיזם ההצבה

תרגיל 5.2.6 (**) 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- $b = \varphi(\lambda)$. הדרכה. הראה ש- $\varphi(a_0 + ... + a_n\lambda^n) = a_0 + ... + a_nb^n$

תרגיל 5.2.7 (**) 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 $Ker(\varphi)$.

5.2.2 איברים אלגבריים

נקבע איבר $a \in K$.

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

תרגיל 5.2.8 (*) הוכח כי φ הוא הומומורפיזם של חוגים עם יחידה.

הגדרה. נסמן $F[a] = Im\varphi = \{b_0 + b_1a + b_2a^2 + \cdots + b_na^n\}$.

מכיוון ש- $F[x]$ תחום ראשי, $Ker\varphi \lhd F[x]$ אידיאל ראשי. לפי משפט האיזומורפיזם הראשון, $F[x]/Ker\varphi \simeq F[a]$. דוגמא. $\mathbb{Z}[x]/\langle x^2 - 2\rangle \simeq \mathbb{Z}(\sqrt{2})$.

תרגיל 5.2.9 (**) אם $Ker\varphi = 0$, אז המימד של $F[a]$ (כמרחב וקטורי) מעל F אינו סופי.

משפט (^{2}). נניח ש- $Ker\varphi = \langle f\rangle \neq 0$. אז הפולינום f איפריק (ולכן $Ker\varphi$ מקסימלי).

הגדרה. היוצר המתוקן של $Ker\varphi$ נקרא הפולינום המינימלי של a.

תרגיל 5.2.10 (*) יהי $g(x)$ הפולינום המינימלי של a מעל F. הראה ש- $g(a) = 0$.

תרגיל 5.2.11 (**) המימד של $F[a]$ מעל F שווה ל- $deg(g)$.

תרגיל (^{t2}). חשב את המימד של $\mathbb{Q}[\sqrt{-1}]/\mathbb{Q}$ ושל $\mathbb{Q}(\sqrt{-1}, \sqrt{2})/\mathbb{Q}(\sqrt{2})$.

תרגיל 5.2.12 (**) 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.

5.2.3 סיפוח של קבוצת אברים

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

תרגיל 5.2.13 (*) הוכח כי אם $T=\{a_1,...,a_n\}$ אז $F(T)=F(a_1,...,a_n)=F(a_1)(a_2)\cdots(a_n)$.

הגדרה. הרחבה $F\subseteq K$ נקראת הרחבה פשוטה שלF אם $K=F(a)$ עבור איזשהוא $a\in K$. דוגמאות. $(\sqrt{5})$ הרחבה פשוטה של . הרחבה פשוטה של $\mathbb{R}$ כי $\mathbb{R}[i]=$.

תרגיל 5.2.14 (**) $\mathbb{Q}(\sqrt{2},\sqrt{3})=\mathbb{Q}(\sqrt{2}+\sqrt{3})$ (ולכן) $\sqrt{2},\sqrt{3}$ הרחבה פשוטה של .
פתרון. מספיק להוכיח הכלה בשני הכיוונים, כלומר, $\sqrt{2+\sqrt{3}}\in(\sqrt{2},\sqrt{3})$ ו-$\in\sqrt{2},\sqrt{3}$ $\sqrt{2+\sqrt{3}}$. 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 $\sqrt{2}=\frac{1}{2}\left(a^3-9a\right)\in(a)$.

תרגיל 5.2.15 (**) יהיו $p,q\in$ ראשוניים. הוכח ש- $(\sqrt{p},\sqrt{q})=(\sqrt{p}+\sqrt{q})$.

תרגיל 5.2.16 (**+) הראה ש- $(\sqrt{2}\cdot 5^{1/3})=(\sqrt{2},5^{1/3})$. רמז. $(\sqrt{2}\cdot 5^{1/3})^4=20\cdot 5^{1/3}$.

5.2.4 הרחבות אלגבריות והרחבות סופיות

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 $1,a,a^2,...$ תלויה ליניארית מעל F ולכן קיים פולינום המאפס את a.

תרגיל 5.2.17 (**) אם $a\in K$ אלגברי מעל F אז $F(a)$ הרחבה אלגברית של F.

תרגיל 5.2.18 (**) הרחבה אלגברית פשוטה היא סופית.

תרגיל 5.2.19 (-**) נניח ש- $F \subseteq L \subseteq K$, $a \in K$, a אלגברי מעל F. הוכח ש- a אלגברי מעל L.

5.2.5 הרכבה של הרחבות סופיות

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

תרגיל 5.2.20 (*) 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 5.2.21 (**) מצא בסיס ל- $\mathbb{Q}(\sqrt{3}, \sqrt{5}, i)$ מעל $\mathbb{Q}$. מה מימד ההרחבה ?

תרגיל 5.2.22 (***) יהיו $p_1, ..., p_t \in \mathbb{Z}$ מספרים זרים בזוגות. הוכח כי $[\mathbb{Q}(\sqrt{p_1}, ..., \sqrt{p_t}) : \mathbb{Q}] = 2^t$. פתרון. נניח, באינדוקציה, שהטענה נכונה לכל $p_1, ..., p_t$ זרים. (השלם את המקרה $t = 1$). נסמן $K_i = (\sqrt{p_1}, ..., \sqrt{p_i})$, 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 $\sqrt{p_{t+1}} \in K_{t-1} = \mathbb{Q}(\sqrt{p_1}, ..., \sqrt{p_{t-1}})$, ואם $\alpha = 0$ אז $\sqrt{p_{t+1}p_t} = \beta p_t \in K_{t-1}$, בשני המקרים סתירה להנחת האינדוקציה.

5.2.6 הסגור האלגברי

תרגיל 5.2.23 (+**) אם $F \subseteq L \subseteq K$, $a \in K$ אלגברי, אז $[L[a] : L] \leq [F[a] : F]$.

תרגיל 5.2.24 (**) אם $a_1, ..., a_n \in K$ אלגבריים, אז $F \subseteq F[a_1, ..., a_n]$ 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 $f(x) = b_0 + ... + b_n x^n \in L[x]$ כך ש- $f(a) = 0$. נסמן $L_0 = F(b_0, b_1, ..., b_n)$. 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 5.2.25 (**) 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 5.2.26 (*) הסגור האלגברי הוא תת-שדה של K.

תרגיל 5.2.27 (**) מצא הרחבות אלגבריות של שאינן סופיות.

5.3 שדות פיצול

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 $f(x)$, $\mathbb{Q}[\sqrt{2}]$, 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 5.3.1 (**) $\mathbb{Q}(\sqrt{-2}) \subset \mathbb{Q}(\sqrt{-1}, \sqrt{2})$.

תרגיל 5.3.2 (-**) 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 5.3.3 (**) יהיו $F \subseteq K$ שדות, $f(x) \in F[x]$ פולינום, ו- $\alpha_1, ..., \alpha_n \in K$ השורשים של f. אז תת-השדה $F[\alpha_1, ..., \alpha_n]$ של K הוא שדה פיצול של f.

תרגיל 5.3.4 (**) מצא את שדה הפיצול של $(x^2-1)(x^2+1)$ מעל $\mathbb{Q}$.

תרגיל 5.3.5 (**) מצא את שדה הפיצול של x^4+1 מעל $\mathbb{Q}$.

תרגיל 5.3.6 (-***) מצא את שדה הפיצול של $x^4 - 2$ מעל $\mathbb{Q}$. מה מימדו?

תרגיל 5.3.7 (**) 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 $[E : F] \leq n!$.

5.4 שדות סופיים

5.4.1 המאפיין של חוג

הגדרה. יהי R חוג קומוטטיבי עם יחידה. המספר הטבעי הקטן ביותר n המקיים $\underbrace{1+1+\cdots+1} = 0$ (n פעמים) 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 5.4.1 (*) אם R תחום שלמות אז $charR = p$ (p ראשוני) או $charR = 0$.

תרגיל 5.4.2 (+*) אם F שדה סופי אז $charF = p$ (p ראשוני).

תרגיל 5.4.3 (-**) בשדה ממאפיין p מתקיים $(a+b)^p = a^p + b^p$.

תרגיל 5.4.4 (**) יהי D תחום ממאפיין p. הוכח ש- $\varphi : a \mapsto a^p$ הוא מונומורפיזם של D.

5.4.2 ספרביליות

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

תרגיל 5.4.6 (-***) $f(\lambda) = a_n\lambda^n + ... + a_0 \in F[\lambda]$ איפריק. הוכח שאם $a_i^{1/p} \in F$ לכל i, $p = charF$, אז f ספרבילי.

5.4.3 מספר האברים של שדה סופי

תרגיל 5.4.7 (**) 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 5.4.8 (**) 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.

5.4.4 החבורה הכפלית של שדה

תרגיל 5.4.9 (*) 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 5.4.10 (**) 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 5.4.11 (+**) בנה שדה F מסדר 9 ומצא $u \in F$ כך שכל $v \neq 0$ ב- F הוא חזקה של u.

5.4.5 פולינומים מעל שדה סופי

תרגיל 5.4.12 (**) פרק לגורמים איפריקים מעל $\mathbb{Z}_3$, $\mathbb{Z}_7$ את x^3+2 ואת x^2+2x-1.

תרגיל 5.4.13 (+**) 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 5.4.14 (+**) x^3-9 איפריק מעל $\mathbb{Z}_{31}$, אבל מתפצל לגורמים ליניאריים מעל $\mathbb{Z}_{11}$.

תרגיל 5.4.15 (-***) 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 5.4.16 (+**) לחוג $\mathbb{Z}_4[\alpha]/\left\langle\alpha^2+\alpha+1\right\rangle$ יש אידיאל יחיד, שהוא $\langle 2\rangle$. הוכח ש- $R/\langle 2\rangle$ שדה בן ארבעה אברים. מה הכפל באידיאל (כחוג) ?

תרגיל 5.4.17 (-***) מצא כמה פולינומים מתוקנים איפריקים ממעלה 2 יש מעל שדה סופי F.