קורס מתקדם בתורת החוגים

עוזי וישנה

4 בפברואר 2020

קורס מתקדם בתורת החוגים

מהדורה 1.954

הקדמה. חוברת זו מכסה את הקורס "אלגברה קומוטטיבית": קורס המבוא הראשון לתורת החוגים באוניברסיטת בר־אילן.

הקורס באלגברה קומוטטיבית (שמספרו 88-813) מכסה נושאים מרכזיים באלגברה קומוטטיבית לתואר שני. אנו מניחים שהקורא מכיר את החומר הסטנדרטי מקורסי תואר ראשון בתורת החבורות, תורת החוגים ותורת גלואה. כמה מהנושאים היותר אלמנטריים (אידיאלים ראשוניים ומקסימליים, משפט השאריות הסיני, מיקום, חוגים מקומיים, מבוא למודולים) מכוסים בחוברת שלי על תורת החוגים, ולא ראיתי צורך לחזור על הפרטים כאן.

לאלגברה קומוטטיבית, שהיא ביסודו של דבר תורת החוגים הקומוטטיביים, יש שימושים בתחומים מרכזיים במתמטיקה: גאומטריה אלגברית ותורת המספרים האלגברית. תנאי הסופיות הנתרי מתקיים לעתים קרובות, והופך את החוגים הנתריים לתחום מחקר מרכזי גם באלגברה גופא. הקורס הזה עוסק בעיקר בחוגים (קומוטטיביים) נתריים.

הקורס באלגברה לא קומוטטיבית (שמספרו 88-815) כולל פרקים נבחרים בתורת המבנה של חוגים לא קומוטטיביים, ובמיוחד חוגים ארטיניים: משפט ודרברן־ארטין על אלגברות פשוטות ארטיניות, חוגים פרימיטיביים, ומשפט הופקינס־לויצקי הקובע שכל חוג ארטיני הוא נתרי. תכונות של אלגברות פשוטות למחצה בונות את התשתית לתורת ההצגות של חבורות סופיות, שאותה מכסה החלק השני בקורס.

עוזי וישנה, 10.2012

תוכן עניינים

חלק I

אלגברה קומוטטיבית

פרק 1

מודולים נתריים וארטיניים

1.1 מבוא לחוגים ומודולים

1.1.1 חוגים

לכל אורך הדרך נניח ש**חוג** כולל איבר יחידה. בשלב זה לא נניח עדיין שהחוגים קומוטטיביים.

המושגים העיקריים שעל הקורא להכיר: **תת־חוג** (כולל את איבר היחידה); **אידיאל** (שמאלי, ימני, דו־צדדי); **הומומורפיזם** (של חוגים, כלומר - שומר על איבר היחידה); **חוג מנה** (ביחס לאידיאל דו־צדדי).

משפט האיזומורפיזם הראשון קובע שלכל הומומורפיזם $\varphi\colon R\to S$, $\mathrm{Im}(\varphi) \cong R/\mathrm{Ker}(\varphi)$. משפט האיזומורפיזם השני מספק התאמה בין חוגי מנה של תת־חוג $S \subseteq R$ לבין תת־חוגים של חוג המנה R/I: $(S+I)/I \cong S/(I \cap S)$. משפט האיזומורפיזם השלישי מתאר את המנות של חוג מנה: אם $I \subseteq J$ אידיאלים של R, אז $(R/I)/(J/I) \cong R/J$. יחד, המשפטים מספקים איזומורפיזם של סריגים בין סריג האידיאלים של R/I לבין סריג האידיאלים של R המכילים את I.

1.1.2 אידיאלים מקסימליים

אידיאל אמיתי של חוג הוא **מקסימלי** אם אינו מוכל באף אידיאל אמיתי אחר. **חוג פשוט** הוא חוג שאין לו אידיאלים דו־צדדיים אמיתיים שונים מאפס. אידיאל הוא מקסימלי אם ורק אם R/I פשוט. חוג קומוטטיבי הוא פשוט אם ורק אם הוא שדה.

איחוד של שרשרת אידיאלים היא אידיאל. בחוג עם יחידה, איחוד של שרשרת אידיאלים אמיתיים הוא אידיאל אמיתי. לפי הלמה של צורן נובע שבחוג עם יחידה תמיד יש אידיאלים מקסימליים.

תרגיל 1.1.1 בחוג עם יחידה, כל אידיאל מוכל באידיאל מקסימלי.

אידיאלים I, J הם קו־מקסימליים אם $I + J = R$.

משפט 1.1.2 (משפט השאריות הסיני) יהיו $I_1, \dots, I_n$ אידיאלים קו־מקסימליים של חוג R. אז $R/(I_1 \cap \dots \cap I_n) \cong R/I_1 \times \dots \times R/I_n$. ◦

1.1.3 מודולים

מודול הוא חבורה אבלית שהחוג פועל עליה (שמאלי); במלים אחרות, יש פעולת כפל בסקלר המגדירה הומומורפיזם (של חוגים) $R \to \mathrm{End}(M) = \mathrm{Hom}(M, M)$, כשבאגף ימין הפעולה היא הרכבה של פונקציות.

תרגיל 1.1.3 תהי M חבורה אבלית. יש התאמה בין פעולות הכפל בסקלר $R \times M \to M$ ההופכות את M למודול מעל R, לבין הומומורפיזמים $\varphi: R \to \mathrm{End}(M)$, על־פי $a \cdot x = \varphi(a)(x)$.

תת־חבורה של M הסגורה לכפל בסקלר היא **תת־מודול**; אוסף כל תת־המודולים של M הוא סריג, כאשר החיתוך הוא חסם תחתון והסכום הוא חסם עליון. אם $N \leq M$ מודולים, **מודול המנה** הוא חבורת המנה $M/N = \{x + N : x \in M\}$, עם פעולת הכפל בסקלר $a(x + N) = ax + N$.

הומומורפיזם של מודולים הוא העתקה אדיטיבית $\varphi: M \to N$ המקיימת את האקסיומה $\varphi(ax) = a\varphi(x)$.

דוגמא 1.1.4
1. מודולים מעל חוג השלמים $\mathbb{Z}$ אינם אלא חבורות אבליות.
2. כל חוג הוא מודול מעל עצמו, ותת־המודולים שלו הם האידיאלים השמאליים.
3. מודולים מעל שדה F הם המרחבים הוקטוריים מעליו.
4. מודולים מעל חוג הפולינומים $F[x]$ הם מרחבים וקטוריים מעל F, עם העתקה לינארית $T: V \to V$ כך ש־$x \cdot v = T(v)$.
5. המרחב הוקטורי F^n הוא מודול מעל $\mathrm{M}_n(F)$ לפי הפעולה הטבעית של מטריצות על וקטורים.
6. המודולים מעל $\mathbb{Z}/n\mathbb{Z}$ הם החבורות האבליות עם אקספוננט המחלק את n.
7. המודולים מעל $\mathbb{Z}[1/p]$ הם החבורות האבליות שבהן לכל איבר יש שורש־p יחיד.

נזכיר את שלושת משפטי האיזומורפיזם של מודולים:

טענה 1.1.5
1. לכל הומומורפיזם $\varphi: M \to N$ מתקיים $M/\mathrm{Ker}(\varphi) \cong \mathrm{Im}(\varphi)$ (כמודולים);
2. $(N + K)/K \cong N/(N \cap K)$;
3. $(M/K)/(N/K) \cong M/N$.

תרגיל 1.1.6 יש התאמה חד־חד־ערכית ועל בין תת־המודולים של M/N לבין תת־המודולים של M המכילים את N; התאמה זו שומרת על הכלה ומנות.

1.1.4 מודולים ציקליים

מודול שאפשר ליצור על־ידי איבר אחד, כלומר כל מודול מהצורה $Rx = \{ax : a \in R\}$, נקרא **מודול ציקלי**.

תרגיל 1.1.7 מודול ציקלי מעל $\mathbb{Z}$ הוא חבורה ציקלית. מודול ציקלי מעל שדה הוא מרחב וקטורי ממימד 1.

בכל מודול כזה, פעולת החיבור היא $ax + bx = (a + b)x$ והכפל בסקלר הוא $a(bx) = (ab)x$; אבל ההתאמה בין הסקלר a לווקטור ax אינה חד־ערכית, ולא ברור א־פריורי מתי שני איברים שונים זה מזה.

הגדרה 1.1.8 *המאפס של איבר x במודול M הוא הקבוצה* $\operatorname{ann}(x) = \{a \in R : ax = 0\}$.

תרגיל 1.1.9 יהי $M = Rx$ מודול ציקלי מעל R.

1. $\operatorname{ann}(x)$ הוא אידיאל שמאלי של R, ו־$Rx \cong R/\operatorname{ann}(x)$ (כמודולים).
2. כל מודול ציקלי הוא מהצורה R/L כאשר $L \leq_\ell R$.

בסעיף 2.2 נגדיר את המאפס של המודול כולו, שהוא אידיאל דו־צדדי של R.

תרגיל 1.1.10
1. כל מודול מעל חוג מנה R/I הוא גם מודול מעל החוג R עצמו.
2. אם M מודול מעל R ו־$IM = 0$, אז M מודול מעל המנה R/I לפי הפעולה $(r + I)x = rx$.

מודול שאין לו תת־מודולים הוא **מודול פשוט**.

תרגיל 1.1.11 חבורה אבלית היא מודול פשוט (מעל $\mathbb{Z}$) אם ורק אם היא חבורה ציקלית מסדר ראשוני. מרחב וקטורי הוא מודול פשוט אם ורק אם הוא בעל ממד 1. מרחב העמודות F^n הוא מודול פשוט מעל $\mathrm{M}_n(F)$.

תרגיל 1.1.12
1. כל מודול פשוט הוא ציקלי.
2. R/L הוא מודול פשוט אם ורק אם L אידיאל שמאלי מקסימלי.

תרגיל 1.1.13 יהי D חוג עם חילוק. הראה שלכל j, מודול העמודה $L_j = \sum_i De_{ij}$ הוא תת־מודול של $\mathrm{M}_n(D)$ כמודול מעל עצמו. הראה שזהו תת־מודול פשוט.

תרגיל 1.1.14 מודול M מעל חוג R הוא פשוט אם ורק אם R פועל טרנזיטיבית על קבוצת האברים השונים מאפס של M. **הדרכה.** M פשוט אם ורק אם לכל $0 \neq v \in M$, $M = Rv$; אם ורק אם לכל $0 \neq v, w$ קיים $x \in R$ כך ש־$xv = w$.

הגדרה 1.1.15 *קבוצה $B \subseteq M$ **יוצרת את** M אם לכל $x \in M$ קיימים $b_1, \dots, b_n \in B$ וסקלרים $\alpha_1, \dots, \alpha_n \in R$ כך ש־$x = \sum \alpha_i b_i$. **מודול נוצר סופית** הוא מודול שיש לו קבוצת יוצרים סופית.*

תרגיל 1.1.16 אם $B = \{b_1, \dots, b_n\}$ יוצרת מודול M, אז $M = Rb_1 + \cdots + Rb_n$.

1.2 סדרות הרכב

הגדרה 1.2.1 *יהי M מודול מעל חוג R. סדרה*

$$0 = M_t < \cdots < M_2 < M_1 < M_0 = M$$

*נקראת **סדרת הרכב** אם כל המנות M_i/M_{i+1} הן מודולים פשוטים. המנות M_i/M_{i+1} נקראות **גורמי ההרכב**.*

תרגיל 1.2.2 נסמן $M_i = L_1 + \cdots + L_i$, כאשר L_j המודולים מתרגיל 1.1.13. הראה ש־$0 = M_0 < M_1 < \cdots < M_{n-1} < M_n = M$ היא סדרת הרכב של $\mathrm{M}_n(D)$.

תרגיל 1.2.3 מצא לחוג המקומי $R = F[x]/\langle x^n \rangle$ סדרת הרכב באורך n, והראה שכל המנות שלה איזומורפיות לשדה השאריות של R (שהוא F, עם הפעולה $x \cdot \alpha = 0$).

תרגיל 1.2.4 ל־$\mathbb{Z}$ (כמודול מעל עצמו) אין סדרת הרכב.

תרגיל 1.2.5 הוכח את ה**מודולריות** של סריג המודולים: אם $A, B, C \leq M$ תת־מודולים כך ש־$A \leq B$ אז $(A + C) \cap B = A + (C \cap B)$; כלומר, $A + C \cap B$ מוגדר היטב.

תרגיל 1.2.6 אם $K \subseteq K'$, $N \cap K = N \cap K'$ ו־$N + K = N + K'$ אז $K = K'$. **הדרכה.** $K' = (K' + N) \cap K' = (K + N) \cap K' = K + (N \cap K') = K + (N \cap K) = K$.

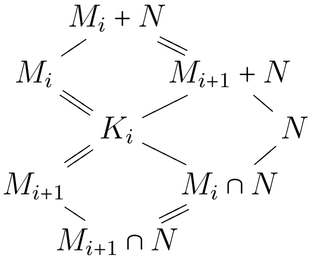
טענה 1.2.7 תהי

$$0 = M_t < \cdots < M_2 < M_1 < M_0 = M \tag{1.1}$$

סדרת הרכב, ויהי $N < M$ תת־מודול כלשהו. אחרי ניכוי השוויונות,

$$0 \leq \cdots \leq M_i \cap N \leq \cdots \leq N \leq \cdots \leq M_i + N \leq \cdots \leq M$$

היא סדרת הרכב, מאותו אורך ועם מנות איזומורפיות למנות בסדרה המקורית.



הוכחה. נסמן $K_i = M_i \cap N + M_{i+1}$, כך שתמיד $M_{i+1} \leq K_i \leq M_i$. מכיוון ש־$N \cap M_0 = N = N + M_t$ משתתף בשני חלקי הסדרה, המנות בסדרה החדשה הן $(M_i + N)/(M_{i+1} + N) \cong M_i/K_i$ ו־$K_i/M_{i+1} \cong (M_i \cap N)/(M_{i+1} \cap N)$. לכל i, בין אם $K_i = M_{i+1}$ ובין אם $K_i = M_i$, אחת המנות האלה היא M_i/M_{i+1}, והשניה שווה לאפס. $\square$

משפט 1.2.8 (משפט ז'ורדן־הולדר־שרייר) *יהי M מודול בעל סדרת הרכב (1.1). אז*

1. *כל סדרה של תת־מודולים $0 = N_\ell < \cdots < N_2 < N_1 < N_0 = M$ **אפשר לעדן לסדרת הרכב**;*
2. *לכל שתי סדרות הרכב יש אותו אורך, ואותם גורמי הרכב עד כדי סדר.*

הוכחה. נאמר ששתי סדרות הרכב הן שקולות אם יש להן אותו אורך ואותם גורמי הרכב, עד כדי סדר. לפי טענה 1.2.7, לכל N, כל סדרת הרכב שקולה לסדרת הרכב העוברת דרך N, כך שרכיבי הסדרה המכילים את N או מוכלים ב־N אינם משתנים. לכן סדרת ההרכב שקולה לסדרת הרכב העוברת דרך N_1, וזו שקולה לסדרת הרכב העוברת דרך $N_2 < N_1$, וכן הלאה עד לסדרת הרכב המעדנת את הסדרה הנתונה. □

לכן אפשר להגדיר:

הגדרה 1.2.9 ***אם יש למודול M סדרת הרכב באורך n אומרים שהאורך שלו הוא n, ומסמנים*** $\ell(M) = n$.

דוגמא 1.2.10 מודול הוא פשוט אם ורק אם האורך שלו הוא 1. האורך של מרחב וקטורי שווה לממד שלו. האורך של $\mathbb{Z}/n\mathbb{Z}$ הוא מספר הגורמים בפירוק של n.

תרגיל 1.2.11 יהיו $N < M$ מודול ותת־מודול. ל־M יש סדרת הרכב אם ורק אם ל־N ו־M/N יש סדרות הרכב. במקרה זה מתקיים ◦

$$\ell(M) = \ell(N) + \ell(M/N). \tag{1.2}$$

הדרכה. אם נתונות סדרות הרכב של N ושל M/N אפשר להרים את האחרונה לסדרת הרכב מ־N ל־M ולקבל סדרת הרכב של M. בכיוון ההפוך יש לעדן את הסדרה $0 < N < M$ כפי שמאפשר לעשות משפט ז'ורדן־הולדר־שרייר.

תרגיל 1.2.12 אם N, N' הם תת־מודולים בעלי אורך סופי של M, אז

$$\ell(N + N') = \ell(N) + \ell(N') - \ell(N \cap N').$$

הדרכה. $\ell(N+N') = \ell((N+N')/N')+\ell(N') = \ell(N/(N\cap N'))+\ell(N') = \ell(N)+\ell(N')-\ell(N\cap N')$.

תרגיל 1.2.13 תהיינה

$$(*) \qquad 0 = N_\ell < \cdots < N_2 < N_1 < N_0 = M,$$

$$(**) \qquad 0 = M_t < \cdots < M_2 < M_1 < M_0 = M$$

סדרות של תת־מודולים. נסמן $K_{ij} = N_{i+1} + M_j \cap N_i$. הראה ש־

$$0 = N_{\ell-1,t} \leq \cdots \leq N_{\ell-1,0} \leq \cdots \leq N_{it} \leq \cdots \leq N_{i0} \leq \cdots \leq N_{0t} \leq \cdots \leq N_{00} = M$$

היא עידון של הסדרה $(*)$, ואם $(**)$ סדרת הרכב אז גם זו סדרת הרכב.

1.2.1 פירוק למרכיבים הומוגניים

בתת־סעיף זה נציג פירוק קנוני של מודול בעל אורך סופי מעל חוג קומוטטיבי R. נאמר שמודול בעל אורך סופי הוא **הומוגני** אם כל גורמי ההרכב שלו איזומורפיים זה לזה (**J־הומוגני** אם כל גורמי ההרכב איזומורפיים ל־R/J, כאשר $J \triangleleft R$ אידיאל מקסימלי).

טענה 1.2.14 יהי M מודול מאורך סופי מעל R (קומוטטיבי), ויהי $J \triangleleft R$ אידיאל מקסימלי. אז M הוא J־הומוגני אם ורק אם קיים n כך ש־$J^n M = 0$.

הוכחה. **אם $0 < M_1 < M_2 < \cdots < M_n = M$ סדרת הרכב שכל גורמיה איזומורפיים ל־R/J, אז באינדוקציה $J^iM \subseteq M_{n-i}$, ולכן $J^nM = 0$. כעת נניח ש־$J^nM = 0$. כל גורם הרכב של M מופיע בצורה N/K כאשר $K < N < M$, וכמובן $J^n(N/K) \subseteq J^n(M/K) = 0$. קיים אידיאל מקסימלי I כך ש־$N/K \cong R/I$, ואז $J^n(R/I) = 0$, כלומר $J^n \subseteq I$. מכיוון ש־I ראשוני, נובע $J \subseteq I$; אבל J** מקסימלי ולכן $I = J$. □

משפט 1.2.15 *מעל חוג קומוטטיבי R, כל מודול בעל אורך סופי הוא סכום ישר של מודולים הומוגניים.*

הוכחה. **כל מודול פשוט מעל R הוא מהצורה R/J כאשר J אידיאל מקסימלי. נסמן את גורמי ההרכב השונים ב־$R/J_1, \dots, R/J_n$; לפי ההנחה יש למודול סדרת הרכב $0 < M_1 < \cdots < M_m = M$; נסמן ב־$n_j$ את מספר הפעמים שמופיע הגורם R/J_j, וניקח $I_j = J_j^{n_j}$. האידיאלים I_j קו־מקסימליים זה לזה, ומתקיים $I_1 \cdots I_n M = 0$. ניקח $I'_j = I_1 \cdots \hat{I}_j \cdots I_n$ ו־$M_j = I'_j M$. אפשר להראות ש־$M = M'_1 \oplus \cdots \oplus M'_n$ (תרגיל 5.2.62 בחוברת תורת החוגים). לכל j מתקיים $I_j M = I_j I'_j M = 0$. לפי טענה 1.2.14, נובע ש־M_j הומוגני.** □

הערה 1.2.16 מודול נקרא **פרימרי** אם מ־$ax = 0$ לאיזשהו $0 \neq x \in M$ נובע n כך ש־$a^nM = 0$; ראה למשל Smith, P.F. "Primary modules over commutative rings", Glasgow Mathematical Journal, **43**(1) (2001), 103–111. מודול הוא הומוגני אם ורק אם הוא פרימרי מאורך סופי.

ממשפט 1.2.15 נובע שמעל חוג קומוטטיבי, למודול מאורך סופי יש סדרות הרכב בכל סדר אפשרי של גורמי ההרכב. מעל חוגים לא קומוטטיביים המצב שונה בתכלית:

דוגמא 1.2.17 יהי $R = \begin{pmatrix} * & * \\ 0 & * \end{pmatrix}$. נתבונן באידיאל השמאלי $M = \begin{pmatrix} 0 & * \\ 0 & * \end{pmatrix}$ כמודול מעל R. סדרת ההרכב היחידה שלו היא $0 < N < M$ כאשר $N = \begin{pmatrix} 0 & * \\ 0 & 0 \end{pmatrix}$. גורמי ההרכב אינם איזומורפיים, משום ש־$e_{22}N = 0$ בעוד ש־$e_{22}(M/N) \neq 0$. מכאן ש־M אינו הומוגני, ולכן גם אינו סכום ישר של מודולים הומוגניים; מאותה סיבה גם אין לו סדרת הרכב שבה הגורמים מופיעים בסדר אחר.

תרגיל 1.2.18 מודול ציקלי בעל אורך סופי (מעל חוג קומוטטיבי R) הוא J־הומוגני אם ורק אם הוא מהצורה R/I כאשר $J^n \subseteq I$. **הדרכה**. לפי טענה 1.2.14, R/I הוא J־הומוגני אם ורק אם יש חזקה n כך ש־$J^n(R/I) = 0$, כלומר $J^n \subseteq I$.

1.2.2 מודולים יוניסריאליים

מודול מאורך סופי הוא **יוניסריאלי** (uniserial) אם יש לו סדרת הרכב יחידה. תת־מודול של מודול יוניסריאלי הוא יוניסריאלי. מודול מנה של מודול יוניסריאלי הוא יוניסריאלי. בסעיף זה נניח ש־R חוג קומוטטיבי.

תרגיל 1.2.19 כל מודול יוניסריאלי הוא הומוגני. **הדרכה**. הפעל את משפט 1.2.15: סכום ישר אינו יכול להיות יוניסריאלי.

העומק $d(M)$ **של מודול J־הומוגני M הוא n המינימלי כך ש־$J^nM = 0$. העומק קיים** לפי טענה 1.2.14, **ותמיד $d(M) \leq \ell(M)$.**

תרגיל 1.2.20 מודול יוניסריאלי M בעל עומק 1 הוא פשוט. **הדרכה**. לפי תרגיל 1.2.19 המודול הוא J־הומוגני, עבור אידיאל מקסימלי J, ומקיים $JM = 0$. לכן M מודול מעל R/J, שהוא שדה, כלומר M הוא מרחב וקטורי. מרחב וקטורי ממימד גדול מ־1 מכיל סכום ישר של תת־מרחבים חד־ממדיים.

תרגיל 1.2.21 התכונות הבאות שקולות עבור מודול מאורך סופי M ואידיאל מקסימלי J:

1. M מודול J־הומוגני המקיים $d(M) = \ell(M)$.
2. M מודול יוניסריאלי, וסדרת ההרכב היחידה שלו היא $M > JM > J^2M > \cdots > 0$.
3. M מודול יוניסריאלי עם מנות הרכב R/J.

הדרכה. $1 \Leftarrow 2$: נניח שיש שתי סדרות הרכב $0 = M_0 < M_1 < M_2 < \cdots < M_n = M$ ו־ $0 = M'_0 < M'_1 < M'_2 < \cdots < M'_n = M$. יהי k המקסימלי כך ש־$M_k = M'_k$. אז $M_{k+1} \cap M'_{k+1} = M_k$, ואם נסמן $N = M_{k+1} + M'_{k+1}$ נקבל ש־$N/M_k = (M_{k+1}/M_k) \oplus (M'_{k+1}/M_k) \cong (R/J) \oplus (R/J)$. האורך של N הוא $k+2$, ולכן $J^{n-k-2}M \subseteq N$. לפי הפירוק $J^{n-k-1}M \subseteq JN \subseteq M_k$, ואז $J^{n-1}M \subseteq J^kM_k = 0$, בסתירה להנחה. כעת נתבונן בשרשרת $M \supseteq JM \supseteq J^2M \supseteq \cdots \supseteq 0$. אם יש שוויון $J^{i+1}M = J^iM$ $(i < n)$, אפשר להוכיח בעזרתו ש־$J^{n-1}M = 0$, בסתירה להנחה. לכן זו שרשרת באורך n, ומכאן שהיא סדרת הרכב. $2 \Leftarrow 3$: ברור. $3 \Leftarrow 1$: נסמן את העומק של M ב־m. לכל $i < m$, נתבונן במנה $J^iM/J^{i+1}M$, שאינה אפס לפי ההנחה. מנה זו היא מודול מעל R/J, שהוא שדה, ולכן היא מרחב וקטורי. לפי תרגיל 1.2.20 האורך של $J^iM/J^{i+1}M$ הוא 1, ולכן $\ell(M) = \sum_{i=0}^{m-1} \ell(J^iM/J^{i+1}M) = m$.

מודול שאי־אפשר לפרק לסכום ישר הוא **מודול אי־פריד**.

תרגיל 1.2.22 תן דוגמא למודול אי־פריד מעל חוג קומוטטיבי R, שהוא הרחבה $0 \longrightarrow (R/J) \longrightarrow M \longrightarrow (R/J)^2 \longrightarrow 0$. (מודול כזה הוא בהכרח הומוגני אבל לא יוניסריאלי).

הומוגני + עומק=אורך
$\parallel$
יוניסריאלי
$\downarrow$
הומוגני + אי־פריד
$\downarrow$
הומוגני

תרגיל 1.2.23 כל מודול יוניסריאלי (מאורך סופי) הוא ציקלי. **הדרכה.** יהי $M_1 < M$ תת־מודול מקסימלי, ויהי $x \in M$, $x \notin M_1$. אז $Rx = M$.

1.2.3 מבוא לאלגברה הומולוגית

הגדרה 1.2.24 *סדרת הומומורפיזמים של מודולים* $A_0 \xrightarrow{f_0} A_1 \xrightarrow{f_1} \cdots \xrightarrow{f_{n-1}} A_n$ *נקראת* ***קומפלקס*** *אם* $f_{i+1} \circ f_i = 0$ *לכל* i. *לכן אפשר להגדיר את* ***חבורות ההומולוגיה*** $H_i = \mathrm{Ker}(f_i)/\mathrm{Im}(f_{i-1})$. *הקומפלקס* ***מדוייק*** *ב־*A_i *אם* $H_i = 0$ *לכל* i.

דוגמא 1.2.25
1. הסדרה $\cdots \longrightarrow B \xrightarrow{f} A \longrightarrow 0$ מדוייקת ב־A אם f חד־חד־ערכית.
2. הסדרה $0 \longrightarrow A \xrightarrow{f} B \longrightarrow \cdots$ מדוייקת ב־A אם f על.
3. הסדרה $0 \longrightarrow B \xrightarrow{f} A \longrightarrow 0$ מדוייקת אם f איזומורפיזם.
4. הסדרה $0 \longrightarrow C \xrightarrow{g} B \xrightarrow{f} A \longrightarrow 0$ מדוייקת אם f שיכון ו־g משרה איזומורפיזם $B/f(A) \cong C$.

הגדרה 1.2.26 *אומרים שהסדרה הקצרה המדוייקת* $0 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 0$ ***מתפצלת*** *אם יש הומומורפיזם* $C \xrightarrow{\theta} B$ *כך ש־*$g\theta = 1_C$.

טענה 1.2.27 הסדרה $0 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 0$ מתפצלת אם ורק אם תמונת A היא מחובר ישר ב־B.

הוכחה. **אם $B = f(A) \oplus C'$, אז $g : C' \to C$ מהווה איזומורפיזם, ואז אפשר לפצל על־ידי** $\theta = (g|_{C'})^{-1}$. **בכיוון ההפוך,** $f(A) \cap \theta(C) = 0$ **כי מ־**$f(a) = \theta(c)$ **נובע** $c = g\theta(c) = fg(a) = 0$, **וכל** $b \in A$ **אפשר להציג** $b = \theta g(b) + (b - \theta g(b)) \in \theta(C) + \mathrm{Ker}(g)$, **שהרי** $g(1-\theta g)(b) = (1-g\theta)g(b) = 0$ $\square$

תרגיל 1.2.28 תהי

$$0 \longrightarrow A_0 \xrightarrow{f_0} A_1 \xrightarrow{f_1} \cdots \xrightarrow{f_{m-1}} A_m \xrightarrow{f_m} \cdots \xrightarrow{f_{n-2}} A_{n-1} \xrightarrow{f_{n-1}} A_n \longrightarrow 0 \,. \tag{1.3}$$

סדרה מדויקת. לכל $0 \leq m \leq n-1$ גם הסדרות שבשורה העליונה והתתונה בדיאגרמה

$$\begin{tikzcd}
0 \arrow[r] & A_0 \arrow[r, "f_0"] & \cdots \arrow[r, "f_{m-1}"] & A_m \arrow[r, "f_m"] \arrow[dr, dotted, "f_m"] & \mathrm{Im}(f_m) \arrow[r] & 0 & & & . \\
& & 0 \arrow[r] & \mathrm{Im}(f_m) \arrow[r, hook] & A_{m+1} \arrow[r, "f_m"] & \cdots \arrow[r, "f_{n-1}"] & A_n \arrow[r] & 0
\end{tikzcd}$$

הן מדויקות.

משפט 1.2.29 *יהי (1.3) קומפלקס של מודולים מאורך סופי. אז*

$$\sum_{i=0}^{n} (-1)^i \ell(A_i) = \sum_{i=0}^{n} (-1)^i \ell(H_i).$$

אגף שמאל אינו תלוי כלל בחיצים, ולכן השוויון מראה שגם אגף ימין אינו תלוי בחיצים. מאידך, יש מצבים שבהם חבורות ההומולוגיה ידועות, וזה מאפשר לומר משהו על האורכים של המודולים בקומפלקס.

הוכחה. **ראשית נבחין כי לכל הומומורפיזם $f : M \to N$ של מודולים בעלי אורך סופי מתקיים** $\ell(\mathrm{Ker}(f)) + \ell(\mathrm{Im}(f)) = \ell(M)$.

לפי ההגדרה $H_0 = \mathrm{Ker}(f_0)$, $H_n = A_n/\mathrm{Im}(f_{n-1})$, **ו־**$H_i = \mathrm{Ker}(f_i)/\mathrm{Im}(f_{i-1})$ **לכל** $i = 1, \ldots, n-1$. **לכן**

$$\begin{aligned}
\sum_{i=0}^{n} (-1)^i \ell(H_i) &= \ell(\mathrm{Ker}(f_0)) + \sum_{i=1}^{n-1} (-1)^i \ell(H_i) + (-1)^n \ell(A_n/\mathrm{Im}(f_{n-1})) \\
&= \ell(\mathrm{Ker}(f_0)) + \sum_{i=1}^{n-1} (-1)^i [\ell(\mathrm{Ker}(f_i)) - \ell(\mathrm{Im}(f_{i-1}))] + (-1)^n \ell(A_n/\mathrm{Im}(f_{n-1})) \\
&= \sum_{i=0}^{n-1} (-1)^i [\ell(\mathrm{Ker}(f_i)) + \ell(\mathrm{Im}(f_i))] + (-1)^n \ell(A_n) \\
&= \sum_{i=0}^{n-1} (-1)^i \ell(A_i) + (-1)^n \ell(A_n) = \sum_{i=0}^{n} \ell(A_i).
\end{aligned}$$

$\square$

תרגיל 1.2.30 אם כל המודולים פרט לאחד בסדרה מדויקת (1.3) הם בעלי אורך סופי, אז כולם בעלי אורך סופי. **הדרכה**. כמו במשפט 1.2.29. אם המודול הסורר אינו A_{n-1}, הטענה נובעת מיד מהנחת האינדוקציה. במקרה האחרון, לפי הנחת האינדוקציה $\mathrm{Im}(f_{n-2})$ בעל אורך סופי, ומכיוון שגם A_n כזה, הרי שגם A_{n-1} בעל אורך סופי.

1.2.4 מודולים פרוייקטיביים

בדיאגרמה משמאל, נאמר ש־f **מתפצל דרך** π אם יש הומומורפיזם $h : P \to N$ כך ש־$f = \pi \circ h$.

$$\begin{tikzcd} & P \arrow[dl, dotted, "h"'] \arrow[d, "f"] \\ M \arrow[r, "\pi"] & Q \end{tikzcd}$$

יהי P מודול חופשי, עם בסיס B, ויהי M מודול כלשהו. לכל פונקציה $f : B \to M$ יש המשכה יחידה להומומורפיזם של מודולים $\hat{f} : P \to M$. בפרט, בדיאגרמה הבאה (כאשר השורה מדוייקת), f מתפצלת דרך π.

$$\begin{tikzcd} & P \arrow[dl, dotted] \arrow[d, "f"] & \\ M \arrow[r, "\pi"] & Q \arrow[r] & 0 \end{tikzcd}$$

הגדרה 1.2.31 *מודול P הוא **פרוייקטיבי** אם כל הומומורפיזם של מודולים $f : P \to Q$ מתפצל דרך כל אפימורפיזם $g : M \to Q$.*

טענה 1.2.32 המודול P הוא פרוייקטיבי אם ורק אם כל סדרה מדוייקת

$$0 \longrightarrow A \longrightarrow B \longrightarrow P \longrightarrow 0$$

מתפצלת.

הוכחה. ראשית נניח ש־P פרוייקטיבי. תהי $0 \longrightarrow A \longrightarrow B \xrightarrow{\ g\ } P \longrightarrow 0$ סדרה קצרה מדוייקת. לפי ההנחה ההומומורפיזם הזהות $P \to P$ מתפצל דרך g, כלומר יש הומומורפיזם $P \xrightarrow{\ \theta\ } B$ כך ש־$g\theta = 1_P$. במלים אחרות, הסדרה מתפצלת.

כעת נניח שכל סדרה קצרה מדוייקת $0 \longrightarrow * \longrightarrow * \longrightarrow P \longrightarrow 0$ מתפצלת. יהי $\varphi : P \to C$ הומומורפיזם, כאשר $g : B \to C$ אפימורפיזם. ניקח $A = \mathrm{Ker}(g)$, ונתבונן בסדרה הקצרה המדוייקת $0 \longrightarrow A \longrightarrow B \xrightarrow{\ g\ } C \longrightarrow 0$. נסמן

$$T = \{(b,p) \in B \oplus P :\ g(b) = \varphi(p)\},$$

ונתבונן בדיאגרמה

$$\begin{tikzcd} 0 \arrow[r] & A \oplus 0 \arrow[r] \arrow[d, "\pi_1"] & T \arrow[r, shift left, "\pi_2"] \arrow[d, "\pi_1"] & P \arrow[r] \arrow[l, shift left, dotted, "\theta"] \arrow[d, "\varphi"] \arrow[dl, dotted] & 0 \\ 0 \arrow[r] & A \arrow[r] & B \arrow[r, "g"] & C \arrow[r] & 0, \end{tikzcd}$$

שבה π_1, π_2 הם ההטלות על הרכיבים. מכיוון ש־g על, גם $\pi_2 : T \to P$ על. הגרעין של $\pi_2 : T \to P$ הוא אכן $A \oplus 0$. לפי ההנחה הסדרה העליונה מתפצלת, כלומר יש הומומורפיזם $P \xrightarrow{\ \theta\ } T$ כך ש־$\pi_2\theta = 1_P$. כלומר, לכל $p \in P$, $\theta(p) = (b,p) \in T$ עבור $b \in B$. לכן $g(\pi_1\theta)(p) = g\pi_1(b,p) = g(b) = \varphi(p)$. מכאן ש־$\varphi$ מתפצל דרך g. □

תרגיל 1.2.33 מחובר ישר של מודול פרוייקטיבי הוא פרוייקטיבי.

הדרכה. העזר בדיאגרמה

$$\begin{tikzcd} P \oplus P' \arrow[r, shift left] \arrow[d, dotted, "(2)"'] \arrow[dr, "(1)"] & P \arrow[l, shift left] \arrow[r] \arrow[d, "f"] \arrow[dl, dotted, "(3)"] & 0 \\ M \arrow[r, "\pi"] & Q \arrow[r] & 0 \end{tikzcd}.$$

טענה 1.2.34 מודול הוא פרוייקטיבי אם ורק אם הוא מחובר ישר במודול חופשי.

הוכחה. כל מודול P אפשר להציג כמנה $P = F/K$ כאשר F חופשי. אם P פרוייקטיבי, נובע מכאן לפי (הכיוון הקל של) טענה 1.2.32 ש־P מחובר ישר של F. הכיוון ההפוך נובע מתרגיל 1.2.33. □

דוגמא 1.2.35 יהי R חוג קומוטטיבי, ויהי $a \in R$ איבר שאינו מחלק אפס (כך ש־$R \cong Ra$ כמודולים מעל R). אם $Ra \neq R$ אז R/Ra אינו פרוייקטיבי.

הוכחה. יש סדרה קצרה מדוייקת $0 \longrightarrow Ra \longrightarrow R \longrightarrow R/Ra \longrightarrow 0$. אם R/Ra פרוייקטיבי אז $R \cong Ra \oplus (R/Ra)$, עם הטלה $\pi : R \to Ra$. נסמן $e = \pi(1)$, אז

$$e^2 = \pi(1) \cdot \pi(1) = \pi(\pi(1)1) = \pi(e) = \pi^2(1) = \pi(1) = e,$$

ולכן $b \in Ra$ מתקיים $be = b\pi(1) = \pi(b1) = \pi(b) = b$. כלומר $b(1-e) = 0$, ובפרט $a(1-e) = 0$. מכאן ש־$e = 1$, ולכן $Ra = R$. □

1.3 תנאֵי השרשרת

1.3.1 תנאי השרשרת בקבוצות סדורות

תהי $(\Lambda, \leq)$ קבוצה סדורה. אומרים ש־Λ מקיימת את **תנאי השרשרת העולה** אם אין שרשרת אינסופית עולה

$$\lambda_0 < \lambda_1 < \lambda_2 < \cdots$$

של אברים של λ. במלים אחרות, לכל שרשרת אינסופית עולה במובן החלש,

$$\lambda_0 \leq \lambda_1 \leq \lambda_2 \leq \cdots$$

יש n כך ש־$\lambda_n = \lambda_{n+1} = \cdots$.

טענה 1.3.1 תנאי השרשרת העולה שקול ל**תנאי המקסימום**, שלפיו בכל תת־קבוצה לא ריקה של Λ יש איבר מקסימלי.

הוכחה. נניח שכל שרשרת עולה ב־Λ מוכרחה להסתיים. תהי $\Lambda_0 \subseteq \Lambda$ תת־קבוצה לא ריקה שאין לה מקסימום. נבחר $\lambda_1 \in \Lambda_0$. לכל n, לאחר שבחרנו $\lambda_1 < \cdots < \lambda_n$ ב־Λ_0, מכיוון ש־λ_n אינו מקסימלי, קיים $\lambda_n < \lambda_{n+1}$ ב־Λ_0; בנינו שרשרת עולה אינסופית, בסתירה להנחה.

בכיוון ההפוך, נניח שלכל קבוצה לא ריקה יש מקסימום. תהי $\lambda_1 \leq \lambda_2 \leq \cdots$ שרשרת עולה; לקבוצה $\{\lambda_1, \lambda_2, \ldots\}$ יש איבר מקסימלי λ_n, ואז $\lambda_n = \lambda_{n+1} = \cdots$. □

הערה 1.3.2 הוכחנו שאם כל שרשרת עולה מוכרחה להסתיים, אז לכל תת־קבוצה לא ריקה יש איבר מקסימלי. **הלמה של צורן** מניחה הרבה פחות: אם לכל שרשרת עולה (לאו דווקא בת־מניה) יש חסם מלעיל, אז יש בקבוצה איבר מקסימלי.

בהיפוך הסדר על Λ, אומרים שקבוצה סדורה מקיימת את **תנאי השרשרת היורדת** אם אין בה שרשרת יורדת אינסופית; תנאי זה שקול ל**עקרון המינימום**: בכל תת־קבוצה לא ריקה יש איבר מינימלי.

דוגמא 1.3.3 $\mathbb{N}$, עם הסדר הרגיל, מקיימת את עקרון המינימום, אבל לא את עקרון המקסימום.

טענה 1.3.4 (**אינדוקציה מוכללת**) נניח ש־Λ מקיימת את עקרון המינימום. נניח ש־$\Lambda_0 \subseteq \Lambda$ היא קבוצה המקיימת את התנאי הבא: לכל $\lambda \in \Lambda$, אם $\lambda' \in \Lambda_0$ לכל $\lambda' < \lambda$, אז גם $\lambda \in \Lambda_0$. אז $\Lambda_0 = \Lambda$.

הוכחה. אחרת קח איבר מינימלי של $\Lambda - \Lambda_0$. □

1.3.2 תנאֵי השרשרת של מודולים

תרגיל 1.3.5 אם $M_1 \leq M_2 \leq \cdots$ מודולים (תת־מודולים של מודול M), אז גם $\bigcup M_i$ הוא מודול (תת־מודול של M).

תרגיל 1.3.6 חיתוך משפחה כלשהי של תת־מודולים הוא תת־מודול.

הגדרה 1.3.7 *אומרים שמודול M הוא **נתרי** (על־שם אמי נתר) אם משפחת תת־המודולים שלו מקיימת את תנאֵי השרשרת העולה, כלומר, אין שרשרת תת־מודולים $M_0 < M_1 < M_2 < \cdots$.*
*אומרים ש־M **ארטיני** (על־שם אמיל ארטין) אם משפחת תת־המודולים שלו מקיימת את תנאֵי השרשרת היורדת, כלומר, אין שרשרת תת־מודולים $M_0 > M_1 > M_2 > \cdots$.*

כפי שראינו, נתריות שקולה לעקרון המקסימום, ואילו ארטיניות שקולה לעקרון המינימום.

תרגיל 1.3.8
1. אם M איזומורפי לתת־מודול אמיתי של עצמו, אז M אינו ארטיני.
2. אם M איזומורפי למודול מנה אמיתי של עצמו, אז M אינו נתרי.

דוגמא 1.3.9 כמודולים מעל $\mathbb{Z}$:

1. כל חבורה אבלית סופית היא נתרית וארטינית.
2. $\mathbb{Z}$ הוא נתרי (כל מנה אמיתית שלו היא סופית) אבל לא ארטיני: $\mathbb{Z} > \cdots > 2^n\mathbb{Z} > \cdots$.
3. $\mathbb{Q}/\mathbb{Z}$ אינו נתרי (הסדרה $2^{-n}\mathbb{Z}/\mathbb{Z}$ עולה) ואינו ארטיני (הסדרה $M_p = \mathbb{Z}[\frac{1}{q}:\ q > p]/\mathbb{Z}$ יורדת).
4. $\mathbb{Z}[\frac{1}{5}]/\mathbb{Z}$ ארטיני (כל תת־מודול אמיתי הוא סופי) ואינו נתרי: $0 < \frac{1}{5}\mathbb{Z}/\mathbb{Z} < \frac{1}{25}\mathbb{Z}/\mathbb{Z} < \cdots$.

תרגיל 1.3.10 קבע האם $\mathbb{Q}$ הוא מודול ארטיני/נתרי מעל $\mathbb{Z}$. **הדרכה.** (דוגמא (1.3.9.(3)) האם הוא ארטיני/נתרי מעל $R = \mathbb{Z}_{\langle 2\rangle} = \left\{\frac{n}{m}:\ 2\not| m\right\}$?

טענה 1.3.11 מודול הוא ארטיני וגם נתרי אם ורק אם יש לו סדרת הרכב.

הוכחה. אם יש סדרת הרכב, הטענה ברורה לפי משפט ז'ורדן־הולדר־שרייר. בכיוון ההפוך, נניח ש־M מקיים את שני תנאֵי השרשרת. נבחר $M_0 = M$, ואחרי שבחרנו את M_i, אם $M_i \neq 0$, נבחר את M_{i+1} להיות מקסימלי מבין התת־מודולים האמיתיים של M_i (זה אפשרי לפי תנאי המקסימום); אבל כך מתקבלת שרשרת יורדת של תת־מודולים, בסתירה לתנאֵי השרשרת היורדת. מכאן שעבור i גדול מספיק, $M_i = 0$, ובנינו סדרת הרכב. □

תרגיל 1.3.12 תת־מודול ומודול מנה של מודול נתרי (ארטיני) הם נתריים (ארטיניים).

טענה 1.3.13 אם $N \leq M$ ו־M/N הם נתריים (ארטיניים) אז גם M כזה.

הוכחה. נוכיח עבור תנאֵי השרשרת העולה. נניח שיש ב־M שרשרת עולה $0 < M_1 < M_2 < \cdots$. אז גם $0 \leq M_1 \cap N \leq M_2 \cap N \leq \cdots$ ו־$0 \leq (M_1 + N)/N \leq (M_2 + N)/N \leq \cdots$ שרשראות עולות, והן מוכרחות לעצור לפי ההנחה. לכן קיים n שממנו והלאה $M_i \cap N = M_{i+1} \cap N$ וגם $M_i + N = M_{i+1} + N$, וסיימנו לפי תרגיל 1.2.6. □

טענה 1.3.14 (**אינדוקציה נתרית**) יהי M מודול נתרי. נניח שלכל תת־מודול A, אם תכונה $\mathcal{P}$ מתקיימת לכל תת־מודול המכיל ממש את A, אז היא מתקיימת גם ל־A. אז $\mathcal{P}$ מתקיימת לכל תת־מודול של M.

הוכחה. אחרת קח דוגמא נגדית מקסימלית: לפי ההנחה היא אינה דוגמא נגדית. (שים לב שמן ההנחה נובע שהתכונה מתקיימת ל־M עצמו באופן ריק.) □

1.3.3 תנאי השרשרת בחוגים

הגדרה 1.3.15 *חוג נקרא **ארטיני** (**נתרי**) אם הוא ארטיני (נתרי) כמודול מעל עצמו, כלומר, אם כל שרשרת יורדת או עולה, בהתאמה, של אידיאלים שמאליים, נעצרת.*

דוגמא 1.3.16 $\mathbb{Z}$ הוא חוג נתרי.

דוגמא 1.3.17 תחום שלמות (שאינו שדה) לעולם אינו ארטיני. **הדרכה.** נבחר $a \in R$ שאינו הפיך, אז $\cdots \supset Ra^2 \supset Ra \supset R$ שרשרת יורדת של אידיאלים.

תרגיל 1.3.18 יהי $\varphi: S \to R$ הומומורפיזם של חוגים.

1. כל מודול מעל R אפשר לראות כמודול מעל S, לפי הפעולה $\alpha \cdot x = \varphi(\alpha)x$.
2. בפרט: מודול מעל חוג R הוא גם מודול מעל כל תת־חוג. מודול מעל חוג מנה R/I הוא גם מודול מעל R.
3. אם M מודול מעל R והוא נתרי (ארטיני) מעל S, אז הוא נתרי (ארטיני) כבר מעל R.

תרגיל 1.3.19 חוג מנה של חוג ארטיני (נתרי) הוא ארטיני (נתרי).

תרגיל 1.3.20 אידיאל שמאלי של חוג ארטיני (נתרי) הוא ארטיני (נתרי) (כחוג בלי יחידה).

תרגיל 1.3.21 הראה שתת־חוג של חוג ארטיני (נתרי) אינו בהכרח ארטיני (נתרי). **הצעה.** שדה הוא נתרי וארטיני, אבל תחום שלמות לעולם אינו ארטיני (טענה 5.1.8 לעיל), וגם אינו חייב להיות נתרי. (הסבר מדוע הנימוק של תרגיל 1.3.20 אינו חל כאן).

1.4 מודולים נוצרים סופית

נתריות וארטיניות, כמו תנאי המינימום ותנאי המקסימום, הם קריטריונים לסופיות. יש מודולים נתריים שאינם ארטיניים, ומודולים ארטיניים שאינם נתריים. למרות הסימטריה המדומה, בסמסטר הבא נוכיח את **משפט הופקינס־לויצקי**: כל חוג ארטיני הוא נתרי.

טענה 1.4.1 אם R ארטיני (נתרי), אז כל מודול נוצר סופית מעל R גם הוא ארטיני (נתרי).

הוכחה. **נניח ש־**$M = Rx_1 + \cdots + Rx_n$. **ההוכחה באינדוקציה על** n. **אם** $n = 1$ **אז** $M \cong R/\mathrm{ann}(x_1)$, **וזהו מודול מנה של** R **שהוא ארטיני או נתרי. במקרה הכללי נסמן** $N = Rx_1 + \cdots + Rx_{n-1}$, **שהוא ארטיני (נתרי) לפי הנחת האינדוקציה.**

אבל גם $M/N = (N + Rx_n)/N \cong Rx_n/(N \cap Rx_n)$ **הוא ארטיני (נתרי) כמודול מנה של מודול ארטיני (נתרי); סיימנו לפי טענה 1.3.13.** □

תכונה נוספת שיש לבחון בהקשר זה היא קיומה של קבוצת יוצרים סופית. מתברר שכל מודול נתרי הוא נוצר סופית, אבל הכיוון ההפוך אינו נכון. אכן, הדוגמא הבאה מספקת תת־מודול שאינו נוצר סופית למודול נוצר סופית.

תרגיל 1.4.2 התבונן בחוג $R = F[x,y]$ (שהוא נתרי, כפי שמיד נוכיח), ובתת־החוג $R_0 = F + Ry$. הראה ש־Ry אינו נוצר סופית כמודול מעל R_0 (למרות ש־$Ry \subseteq R_0 \cdot 1$).
הדרכה. ראשית, $R_0Ry = (F+Ry)Ry = Ry + Ry^2 = Ry$ ולכן $I = Ry$ הוא אידיאל של R_0. נתבונן במודול המנה $M = Ry/Ry^2$, ונבחין ש־$IM = 0$, כך ש־M מודול גם מעל $R_0/I \cong F$. יוצרים של M מעל R_0 יוצרים אותו גם מעל R_0/I, אלא ש־$M = \sum Fx^ny$ בעל ממד אינסופי כמרחב וקטורי.

טענה 1.4.3 מודול הוא נתרי אם ורק אם כל תת־מודול שלו נוצר סופית.

הוכחה. **נניח ש־N אינו נוצר סופית. אז אפשר לבחור $x_0 = 0$ ולכל i לבחור $x_{i+1} \notin N_i = Rx_0 + \cdots + Rx_i$; מתקבלת שרשרת עולה של תת־מודולים, $N_1 < N_2 < \cdots$, כך ש־N אינו נתרי. לכן כל מודול נתרי (וכל תת־מודול של מודול כזה, שגם הוא נתרי לפי תרגיל 1.3.12) הוא נוצר סופית. בכיוון ההפוך, נניח שכל תת־מודול של N נוצר סופית, ותהי $N_1 < N_2 < \cdots$ שרשרת עולה של תת־מודולים; אז $\bar{N} = \bigcup N_i$ הוא תת־מודול, ולפי ההנחה אפשר לכתוב $\bar{N} = Rx_1 + \cdots + Rx_t$; יש n גדול מספיק כך שכל $x_i \in N_n$, ואז גם $N_{n+1} = N_n$, בסתירה להנחה.** □

תרגיל 1.4.4 חוג הוא נתרי אם ורק אם כל אידיאל שמאלי שלו נוצר סופית.

ובפרט:

תרגיל 1.4.5 כל תחום ראשי הוא נתרי.

משפט 1.4.6 (משפט הבסיס של הילברט) *אם R חוג נתרי אז גם חוג הפולינומים $R[x]$ הוא נתרי.*

הוכחה. נניח ש־$R[x]$ אינו נתרי. אז יש לו אידיאל שמאלי $I \leq_\ell R[x]$ שאינו נוצר סופית. נבחר $f_0 = 0$, ולכל $j > 0$ יהי $f_j \in I$ פולינום ממעלה n_j שהיא מינימלית כך ש־$f_j \notin \sum_{i<j} R[x]f_i$. יהי a_j המקדם העליון של f_j. אם $a_j \in \sum_{i<j} Ra_i$ אז אפשר לכתוב $a_j = \sum_{i<j} r_ia_i$ עבור $r_i \in R$, ואז $f_j - \sum_{i<j} r_ix^{n_j-n_i}f_i$ בעל מעלה קטנה משל f_j, והוא שייך ל־I אבל לא ל־$\sum_{i<j} R[x]f_i$, בסתירה. לכן $Ra_1 \subset Ra_1 + Ra_2 \subset \cdots$ שרשרת עולה אינסופית, וגם R אינו נתרי. □

הערה 1.4.7 משפט הבסיס של הילברט תקף גם כאשר R אינו קומוטטיבי, ואפילו (בשינויים קלים של ההוכחה) עבור חוג הפולינומים המעוות $R[x;\sigma,\delta]$ כאשר $\sigma: R \to R$ אוטומורפיזם ו־$\delta: R \to R$ גזירת־σ (כלומר, העתקה המקיימת $\delta(ab) = \sigma(a)\delta(b) + \delta(a)b$); החוג מוגדר לפי היחס $xa = \sigma(a)x + \delta(a)$.

תרגיל 1.4.8 כל חוג קומוטטיבי נוצר סופית מעל חוג נתרי הוא נתרי. **הדרכה**. משפט הבסיס של הילברט ותרגיל 1.3.19. ◦

תרגיל 1.4.9 אם R נתרי אז גם $R[[x]]$ נתרי. **הדרכה**. נסמן ב־$\nu(f)$ את מעלת המונום המוביל של f, וב־$\bar{f}$ את המקדם של $x^{\nu(f)}$ ב־f. יהי $I \triangleleft R[[x]]$. נסמן ב־I_n את האידיאל של R הכולל את המקדמים המובילים של כל $f \in I$ עם $\nu(f) = n$. כך $I_0 \subseteq I_1 \subseteq I_2 \subseteq \cdots$, ולכן השרשרת מתייצבת ב־$I_n$ מתאים. בגלל הנתריות של R, כל I_j נוצר סופית; קבע קבוצות יוצרים לכל I_j, $j \leq n$. לכל יוצר של I_j, בחר $f_{jk} \in I$ עם ערך j, שזה המקדם המוביל שלו; נסמן ב־I' את האידיאל של $R[[x]]$ הנוצר על־ידי כל היוצרים האלה. כעת יהי $f \in I$. נבנה באינדוקציה סדרת אברים $f_i \in I'$ כך ש־$\nu(f - f_i) > i$. נבחר $f_{-1} = 0$. לכל $i \geq 0$ נציג את המקדם של x^i בהפרש $f - f_{i-1}$ כצירוף מעל R של יוצרי I_i, ונרים אותו לצירוף מעל R של אברי I המתאימים; נבחר f_i להיות הסכום של f_{i-1} עם הצירוף הזה. כך המקדם של x^i בהפרש $f - f_i$ שווה לאפס.

תרגיל 1.4.10 החוג $R[x]$ לעולם אינו ארטיני (בגלל השרשרת היורדת $R[x]x^n$).

(ולכן אין גרסה אנלוגית למשפט הבסיס של הילברט עבור תכונת הארטיניות.)

1.4.1 הלמה של נקיימה

תרגיל 1.4.11 יהי $M \neq 0$ מודול. אם אי־אפשר להציג את M כאיחוד על־פני שרשרת עולה של תת־מודולים, אז יש לו תת־מודול מקסימלי. **הדרכה**. ההנחה אומרת שאוסף תת־המודולים האמיתיים מקיים את תנאי צורן.

למודול נתרי יש תת־מודולים מקסימליים לפי עקרון המקסימום. נראה שעובדה זו נכונה לכל מודול נוצר סופית.

תרגיל 1.4.12 למודול נוצר סופית $M = Rx_1 + \cdots + Rx_n$ יש תת־מודול מקסימלי. **הדרכה**. התוצאה נובעת מתרגיל 1.4.11 משום שאם $M = \bigcup M_\lambda$ איחוד על־פני שרשרת עולה, אז יש M_λ המכיל את כל האברים $x_1, \ldots, x_n$, ולכן הוא אינו תת־מודול אמיתי. **הערה**. אין סיבה לחשוב שתת־המודול המקסימלי עצמו נוצר סופית (אלא אם M נתרי).

משפט 1.4.13 (הלמה של נקיימה לחוגים קומוטטיביים) לכל מודול נוצר סופית $M \neq 0$ מעל חוג קומוטטיבי R קיים אידיאל מקסימלי A כך ש־$AM \neq M$.

הוכחה. **לפי תרגיל 1.4.12 יש תת־מודול מקסימלי** $M' < M$. **כעת** M/M' **מודול פשוט, ולכן** $M/M' \cong R/A$ **כאשר** A **אידיאל מקסימלי. כעת** $A(M/M') = 0$ **כי** $A(R/A) = 0$**, ולכן** $AM \subseteq M'$ **ומכאן ש־**$AM \neq M$. $\square$

תרגיל 1.4.14 איחוד שרשרת של תת־מודולים שאינם נוצרים סופית, גם הוא אינו נוצר סופית. **הדרכה**. אחרת $\bigcup M_\alpha = Rx_1 + \cdots + Rx_n$, ואז יש α כך ש־$x_1, \ldots, x_n \in M_\alpha$, בסתירה להנחה.

פרק 2

אידיאלים ראשוניים

2.1 חוגים מקומיים

הגדרה 2.1.1 *חוג קומוטטיבי הוא מקומי אם יש לו אידיאל מקסימלי יחיד.*

טענה 2.1.2 נזכיר ש־$U(R)$ היא חבורת האברים ההפיכים בחוג R. התכונות הבאות שקולות עבור חוג קומוטטיבי:

1. R מקומי,
2. $R - U(R)$ אידיאל,
3. $R - U(R)$ סגור לחיבור,
4. לכל $a \in R$, a או $1 - a$ הפיכים,
5. אין ב־R זוג אידיאלים קו־מקסימליים.

הוכחה. $(1) \Longleftarrow (2)$: כל אידיאל אמיתי זר ל־$U(R)$ ולכן מוכל ב־$R - U(R)$, שהוא לכן מקסימלי. $(2) \Longleftarrow (3)$: נשאר להוכיח שאם a אינו הפיך אז גם ab אינו הפיך; אבל זה נכון בכל חוג קומוטטיבי. $(3) \Longleftarrow (4)$: יהיו $a, b \in R$ אברים לא הפיכים, ונניח בשלילה ש־$a + b$ הפיך. אז $(a+b)^{-1}a + (a+b)^{-1}b = 1$, ולכן אחד המחוברים הפיך, בסתירה להנחה. $(4) \Longleftarrow (5)$: אם גם a וגם $1 - a$ אינם הפיכים, אז Ra ו־$R(1 - a)$ אידיאלים קו־מקסימליים. $(5) \Longleftarrow (1)$: יהי M האידיאל המקסימלי היחיד, אז לכל I, J מתקיים $I + J \subseteq M + M = M < R$. $\square$

מכיוון שלחוג מקומי יש אידיאל מקסימלי יחיד, יש לו מודול פשוט יחיד (עד כדי איזומורפיזם), וממילא כל מודול בעל אורך סופי מעליו הוא הומוגני (ראה תת־סעיף 1.2.1).

בפרק זה נראה כיצד לשכן חוג נתון R בחוג מקומי, כך שאידיאל ראשוני נתון ב־R יהפוך להיות האידיאל המקסימלי היחיד בחוג החדש.

2.2 אידיאלים ראשוניים

אידיאל אמיתי של חוג הוא **ראשוני** אם אינו מכיל מכפלה של אידיאלים בלי להכיל אחד מהם. **חוג ראשוני** הוא חוג שבו אפס אידיאל ראשוני. אידיאל הוא ראשוני אם ורק אם R/I ראשוני.

המושגים קשורים זה לזה: כל אידיאל מקסימלי הוא ראשוני; ולעתים קרובות גם אידיאל שהוא מקסימלי ביחס לתכונה מסויימת הוא ראשוני.

תרגיל 2.2.1 כל אידיאל מקסימלי הוא ראשוני.

תרגיל 2.2.2 אידיאל P הוא ראשוני אם ורק אם לכל $P \subset A, B$, $AB \nsubseteq P$.

תרגיל 2.2.3 $P \triangleleft R$ ראשוני אם ורק אם R/P חוג ראשוני.

תרגיל 2.2.4 אידיאל P בחוג קומוטטיבי R הוא ראשוני אם ורק אם R/P הוא תחום שלמות.

תרגיל 2.2.5 (כאשר R קומוטטיבי) $P \triangleleft R$ ראשוני אם ורק אם לכל $a, b \in R$, אם $ab \in P$ אז $a \in P$ או $b \in P$.

תרגיל 2.2.6 יהי P אידיאל ראשוני. אם $P = A \cap B$ אז $P = A$ או $P = B$. **הדרכה**. $AB \subseteq A \cap B$.

תרגיל 2.2.7 אידיאל מהצורה AB אינו יכול להיות ראשוני, אלא אם הוא שווה ל־A או ל־B.

תרגיל 2.2.8 $n\mathbb{Z}$ הוא אידיאל ראשוני של $\mathbb{Z}$ אם ורק אם n ראשוני או אפס.

תרגיל 2.2.9 בתחום פריקות יחידה: האידיאל $P = Rp$ הוא ראשוני אם ורק אם p אי־פריק, וכל אידיאל ראשוני $\neq 0$ כולל איבר אי־פריק.

תרגיל 2.2.10 יהי R תחום שלמות נתרי. הראה שכל אידיאל ראשוני של R נוצר על־ידי איברים אי־פריקים. **הדרכה**. חוג נתרי הוא בפרט אטומי, כלומר כל איבר הוא מכפלה של איברים אי־פריקים. נניח ש־$P = \langle aa', c_1, \dots, c_n \rangle$; אז $A = \langle a, c_1, \dots, c_n \rangle$ ו־$A' = \{a', c_1, \dots, c_n\}$ מקיימים $AA' = \langle aa', ac_i, a'c_i, c_ic_j \rangle \subseteq P$, ולכן למשל $A \subseteq P$, והרי מצד שני $P \subseteq A$. לכן $P = A$ ואפשר להמשיך באינדוקציה על מספר הגורמים הכולל.

בתרגילים הבאים נניח ש־R קומוטטיבי.

הגדרה 2.2.11 *עבור $I, I' \triangleleft R$, נגדיר $I{:}I' = \{x \in R \colon xI' \subseteq I\}$. זהו האידיאל הגדול ביותר המקיים $(I{:}I')I' \subseteq I$.*

תרגיל 2.2.12 אם I אינו ראשוני, אז יש $a \notin I$ כך ש־$I \subset I{:}a$. **הדרכה**. קח $a, b \in R$ כך ש־$a, b \notin I$ ו־$ab \in I$, אז $b \in I{:}a$.

תרגיל 2.2.13 יהי $J \triangleleft R$, ויהי $a \in R$. אם $I + Ra$ ו־$I{:}a$ נוצרים סופית, אז גם I נוצר סופית. **הדרכה**. כתוב $I{:}a = \sum Rx_i$ ו־$I + Ra = \sum Ry_j$. לפי ההנחה $\sum Rx_ia = (I{:}a)a \subseteq I$, ולכל j יש $t_j \in R$ כך ש־$y_j - t_ja \in I$. נראה שהאברים $\{x_ia, y_j - t_ja\}$ יוצרים את I: לכל $c \in I$, יש $s_j \in R$ כך ש־$c = \sum s_jy_j = \sum s_j(y_j - t_ja) + (\sum s_jt_j)a$, ואז $(\sum s_jt_j)a \in I$ ולכן שייך לאידיאל $\sum Rx_ia$.

המשפט הבא מדגים את העקרון שהוצג בתחילת הסעיף, על כך שאידיאלים מקסימליים ביחס לתכונה מסויימת נוטים להיות ראשוניים.

משפט 2.2.14 חוג קומוטטיבי R שבו כל אידיאל ראשוני נוצר סופית, הוא נתרי.

הוכחה. אם כל האידיאלים נוצרים סופית, סיימנו. נניח שלא, אז לפי תרגיל 1.4.14, מכיוון שהתנאי סגור לשרשראות, אפשר להפעיל את הלמה של צורן ולקבל אידיאל J שהוא מקסימלי בין אלו שאינם נוצרים סופית.

אם J אינו ראשוני אז לפי תרגיל 2.2.12 יש $a \in R$ כך ש־$J \subset J{:}a$ ו־$J \subset Ra + J$, ולפי המקסימליות שני האידיאלים האלה נוצרים סופית. אבל אז, לפי תרגיל 2.2.13, גם J נוצר סופית, בסתירה להנחה. מכאן ש־J ראשוני, אבל אז הוא נוצר סופית לפי ההנחה. $\square$

2.3 מיקום

תהי S תת־קבוצה של חוג R. היינו רוצים לבנות חוג המכיל את R, שבו כל אברי S הפיכים. זה לא תמיד אפשרי (משום שמחלקי אפס אינם הפיכים בשום הרחבה של החוג); בכל זאת, נניח שלקבוצה S יש התכונות הבאות:

1. S סגורה לכפל וכוללת את איבר היחידה.
2. S מוכלת במרכז של R.

נגדיר על $S\times R$ יחס שקילות: $(s,r)\equiv(s',r')$ אם קיים $s_0\in S$ כך ש־$s_0(s'r-sr')=0$ (אם כל אברי S רגולריים, כלומר אינם מחלקי אפס, אז ההגדרה פשוטה יותר: $(s,r)\equiv(s',r')$ אם $s'r=sr'$).

תרגיל 2.3.1 הראה שזהו אכן יחס שקילות. (היכן השתמשנו בהנחה ש־S מרכזית?)

את מחלקת השקילות של (s,r) נסמן $\frac{r}{s}$. נסמן גם $S^{-1}R=\left\{\frac{r}{s}:\ s\in S, r\in R\right\}$. על הקבוצה הזו אפשר להגדיר פעולות: $\frac{r}{s}\cdot\frac{r'}{s'}=\frac{rr'}{ss'}$, $\frac{r}{s}+\frac{r'}{s'}=\frac{s'r+sr'}{ss'}$.

תרגיל 2.3.2 הראה שהפעולות מוגדרות היטב.

תרגיל 2.3.3 הראה ש־$S^{-1}R$, עם הפעולות שהוגדרו לעיל, הוא חוג, שאיבר היחידה שלו $\frac{1}{1}$.

נגדיר העתקה $\iota: R\to S^{-1}R$ לפי $r\mapsto\frac{r}{1}$.

תרגיל 2.3.4 הראה ש־$\mathrm{Ker}(\iota)=\{r\in R:\ (\exists s\in S)sr=0\}$, והסק ש־$\iota$ שיכון אם ורק אם כל אברי S רגולריים (במקרה זה אפשר לזהות את R עם העותק האיזומורפי $\iota R=\left\{\frac{r}{1}:\ r\in R\right\}$ שהוא תת־חוג של $S^{-1}R$).

תרגיל 2.3.5 הראה שאם $0\in S$ אז $S^{-1}R=0$.

תרגיל 2.3.6 תן דוגמא שבה $0\notin S$ ובכל־זאת $\iota: R\to S^{-1}R$ אינו שיכון.

תרגיל 2.3.7 הראה שאברי $\iota S=\left\{\frac{s}{1}:\ s\in S\right\}$ הפיכים ב־$S^{-1}R$. לכן אפשר לכתוב $S^{-1}=\left\{\frac{1}{s}:\ s\in S\right\}$.

תרגיל 2.3.8 נניח שכל אברי S רגולריים. הראה ש־$\iota: R\to S^{-1}R$ היא על, אם ורק אם כל אברי S הפיכים כבר ב־R.

האוניברסליות של חוג השברים

נאמר שהומומורפיזם $R\to R'$ הוא "**הופך** S" אם התמונה של כל איבר של S הפיכה ב־R'.

משפט 2.3.9 *יהי $\varphi: R\to A$ הומומורפיזם הופך S. אז קיים הומומורפיזם יחיד $\varphi': S^{-1}R\to A$ כך ש־$\varphi=\varphi'\circ\iota$.*

$$\begin{tikzcd} S^{-1}R \arrow[dr, dotted, "\varphi'"] & \\ R \arrow[u, "\iota"] \arrow[r, "\varphi"'] & A \end{tikzcd}$$

2.3.1 האידיאלים של $S^{-1}R$

השאלה הטבעית כעת היא מה קורה לאידיאלים של R כשעוברים לחוג $S^{-1}R$. לפני כן, כמה מלים על הקשר בין אידיאלים של חוג לאידיאלים של תת־חוג באופן כללי.

תרגיל 2.3.10 יהיו $S \subseteq R$ הם חוגים קומוטטיביים. כל אידיאל $I \triangleleft S$ משרה אידיאל $\alpha(I) = RI \triangleleft R$, וכל אידיאל $J \triangleleft R$ משרה אידיאל $\beta(J) = S \cap J$ ב־S.

1. שתי ההעתקות שומרות הכלה.
2. תמיד $I \subseteq \beta(\alpha(I))$ ותמיד $\alpha(\beta(J)) \subseteq J$.
3. $\alpha\beta\alpha = \alpha$ ו־$\beta\alpha\beta = \beta$.
4. ההעתקות α, β הופכות זו את זו כאשר מצמצמים אותן לתמונות של β, α בהתאמה.
5. α שומר חיבור, ו־$\alpha(I_1 \cap I_2) \subseteq \alpha(I_1) \cap \alpha(I_2)$.
6. β שומר חיתוך, ו־$\beta(J_1) + \beta(J_2) \subseteq \beta(J_1 + J_2)$.
7. אם מתקיים $\alpha(I_1 \cap I_2) = \alpha(I_1) \cap \alpha(I_2)$ ו־$\beta(J_1) + \beta(J_2) = \beta(J_1 + J_2)$, אז יש איזומורפיזם של סריגים בין האידיאלים של S המושרים על־ידי אידיאלים של R, לבין האידיאלים של R המושרים על־ידי אידיאלים של S.

כעת נראה שעבור הרחבות כמו $R \to S^{-1}R$ המצב משתפר, ובמיוחד כאשר מצטמצמים לאידיאלים ראשוניים.

אם $A \triangleleft R$, נסמן $S^{-1}A = \left\{\frac{a}{s} : a \in A, s \in S\right\}$. כקבוצות ב־$S^{-1}R$, מתקיים $S^{-1}A = S^{-1} \cdot \iota(A)$.

תרגיל 2.3.11 לכל $A \triangleleft R$, $S^{-1}A$ הוא אידיאל של $S^{-1}R$.

בכיוון ההפוך, לכל $T \triangleleft S^{-1}R$, נתבונן ב־$\iota^{-1}(T) = \left\{a \in R : \frac{a}{1} \in T\right\}$. (אם $\iota : R \to S^{-1}R$ שיכון, אז $\iota^{-1}(T) = T \cap R$.)

תרגיל 2.3.12 לכל $T \triangleleft S^{-1}R$, $\iota^{-1}(T)$ הוא אידיאל של R.

תרגיל 2.3.13 1. לכל $T \triangleleft S^{-1}R$, $T = S^{-1}\iota^{-1}(T)$;

2. כל אידיאל של $S^{-1}R$ הוא מהצורה $S^{-1}A$ עבור $A \triangleleft R$ מתאים.

פתרון. יהי $T \triangleleft S^{-1}R$, אז $A = \iota^{-1}(T)$ הוא אידיאל של R, ומכיוון ש־$A \subseteq T$, מתקיים $S^{-1}A = S^{-1}\iota(A) \subseteq S^{-1}T = T$. מאידך, לכל $\frac{x}{s} \in T$, $\frac{x}{1} = \frac{s}{1}\frac{x}{s} \in ST = T$ ולכן $\frac{x}{1} \in \iota(T) = A$; מכאן ש־$\frac{x}{s} = \frac{1}{s}\frac{x}{1} \in S^{-1}A$. אם כך, $T = S^{-1}\iota^{-1}(T)$ הוא מהצורה המבוקשת.

תרגיל זה מראה שההעתקות

$$\{\text{אידיאלים של } R\} \underset{\Psi : T \mapsto \iota^{-1}(T)}{\overset{S^{-1}A \leftarrow A : \Phi}{\rightleftarrows}} \{\text{אידיאלים של } S^{-1}R\}$$

מוגדרות היטב, וגם שההרכבה $\Phi \circ \Psi : T \mapsto S^{-1}\iota^{-1}(T)$ היא הזהות. מכאן ש־Ψ חד־חד־ערכית, וש־Φ על. אינטואיטיבית, פירושו של דבר של־$S^{-1}R$ יש 'פחות' אידיאלים מאשר ל־R. כל אידיאל של $S^{-1}R$ מוגדר על־ידי אידיאל של R, ואידיאלים רבים של R עשויים להגדיר את אותו אידיאל של $S^{-1}R$.

החוג R עצמו עובר תחת Φ אל $S^{-1}R$, בדיוק כפי ש־Ψ מעביר את $S^{-1}R$ ל־R.

תרגיל 2.3.14 1. יהי $A\triangleleft R$. אז $S^{-1}A$ אידיאל אמיתי אם ורק אם $S\cap A=\varnothing$.

2. יהי $T\triangleleft S^{-1}R$. אז T אמיתי אם ורק אם החיתוך של $\iota^{-1}(T)$ עם S ריק.

כלומר, ההעתקות שהוגדרו קודם לכן פועלות גם על הקבוצות המצומצמות

$$\{\text{אידיאלים של } R \text{ הזרים ל-}S\} \underset{\Psi:T\mapsto\iota^{-1}(T)}{\overset{S^{-1}A\leftarrow A:\Phi}{\rightleftarrows}} \{\text{אידיאלים אמיתיים של } S^{-1}R\}$$

וגם כאן $\Phi\circ\Psi$ היא הזהות, כך ש-Ψ חד־חד־ערכית, ו-Φ על.

תרגיל 2.3.15 קח $R=\mathbb{Z}$ ו-$S=\{1,3,9,27,\dots\}$. הראה שהאידיאלים השונים $A=6\mathbb{Z}$ ו-$A'=2\mathbb{Z}$ של R מקיימים $S^{-1}A=S^{-1}A'$, למרות ששניהם זרים ל-S.

תרגיל 2.3.16 יהי $P\triangleleft R$ ראשוני זר ל-S, אז $\iota^{-1}(S^{-1}P)=P$. **פתרון**. ההכלה $P\subseteq\iota^{-1}(S^{-1}P)$ טריוויאלית. נניח ש-$\frac{x}{1}\in\iota^{-1}(S^{-1}P)$, $\frac{a}{s}=\frac{x}{1}$, כאשר $a\in P$ ו-$s\in S$. מכיוון ש-s מרכזי, $(RsR)(RxR)=RsxR=RaR\subseteq P$, אבל $s\notin P$ ולכן $RsR\nsubseteq P$, ולפי הראשוניות נובע מכך ש-$x\in RxR\subseteq P$. מכאן ש-$\frac{x}{1}\in P$.

תרגיל 2.3.17 אם $P\triangleleft R$ ראשוני זר ל-S, אז $S^{-1}P$ ראשוני. **פתרון**. נניח ש-$T_1T_2\subseteq S^{-1}P$ עבור $T_1,T_2\triangleleft R$. נכתוב $T_i=S^{-1}A_i$ עבור $A_i\triangleleft R$, ואז

$$A_1A_2\subseteq\iota^{-1}(S^{-1}A_1\cdot S^{-1}A_2)=\iota^{-1}(T_1T_2)\subseteq\iota^{-1}(S^{-1}P)=P$$

לפי תרגיל 2.3.16. מכיוון ש-P ראשוני, יש i שעבורו $A_i\subseteq P$, ואז $T_i=S^{-1}A_i\subseteq S^{-1}P$.

תרגיל 2.3.18 אם $T\triangleleft S^{-1}R$ ראשוני, אז $\iota^{-1}(T)$ אידיאל ראשוני של R. **פתרון**. נניח ש-$A_1A_2\subseteq\iota^{-1}(T)$ עבור $A_1,A_2\triangleleft R$. אז $S^{-1}A_1\cdot S^{-1}A_2=S^{-1}(A_1A_2)\subseteq S^{-1}\iota^{-1}(T)\subseteq S^{-1}T=T$, ומכיוון ש-$T$ ראשוני נובע מכך ש-$S^{-1}A_i\subseteq T$ ל-i מתאים. לכן $A_i\subseteq\iota^{-1}(S^{-1}A_i)\subseteq\iota^{-1}(T)$.

משני התרגילים האחרונים נובע שההתאמות

$$\left\{\begin{matrix}\text{אידיאלים ראשוניים של } R\\ \text{הזרים ל-}S\end{matrix}\right\} \underset{\Psi:T\mapsto\iota^{-1}(T)}{\overset{S^{-1}A\leftarrow A:\Phi}{\rightleftarrows}} \{\text{אידיאלים ראשוניים של } S^{-1}R\}$$

מוגדרות היטב, ולפי תרגילים 2.3.13 ו-2.3.16, הן הפוכות זו לזו. אם כך, הוכחנו:

משפט 2.3.19 *יש התאמה חד־חד־ערכית ועל בין אידיאלים ראשוניים של R שאינם נחתכים עם S, לבין אידיאלים ראשוניים של $S^{-1}R$, המוגדרת על־ידי $P\mapsto S^{-1}P$, $T\mapsto\iota^{-1}(T)$.*

תרגיל 2.3.20 יהי $A\triangleleft R$ אידיאל זר ל-S. הראה ש-$r+A\mapsto\frac{r}{1}+S^{-1}A$ הוא הומומורפיזם מוגדר היטב $R/A\to S^{-1}R/S^{-1}A$, שהגרעין שלו הוא $\iota^{-1}(S^{-1}A)/A$. לכן הוא מתפצל להטלה ושיכון

$$R/A\twoheadrightarrow R/\iota^{-1}(S^{-1}A)\hookrightarrow S^{-1}R/S^{-1}A.$$

אם A ראשוני, המצב טוב בהרבה:

תרגיל 2.3.21 יהי $P\triangleleft R$ אידיאל ראשוני שהוא זר ל-S. הראה שקיים שיכון $R/P\hookrightarrow S^{-1}R/S^{-1}P$. **הדרכה**. תרגילים 2.3.20 ו-2.3.16.

2.3.2 מיקום באידיאל ראשוני

תרגיל 2.3.22 יהי P אידיאל של חוג קומוטטיבי R. הראה שהמשלים $S = R{-}P$ סגור לכפל אם ורק אם P ראשוני.

אם $P \triangleleft R$ אידיאל ראשוני של חוג קומוטטיבי R, אפשר לפי התרגיל להפעיל את הבניה של הסעיף הקודם ולקבל חוג $(R-P)^{-1}R = \left\{\frac{x}{b} :\ x \in R,\, b \notin P\right\}$, שבו כל איבר מחוץ ל־$P$ הוא הפיך. את החוג הזה מסמנים ב־R_P, והוא נקרא **המיקום** של R ב־P. לכל $A \triangleleft R$ המוכל ב־P, מסמנים $A_P = (R-P)^{-1}A$.

תרגיל 2.3.23 יש התאמה חד־חד־ערכית ועל בין אידיאלים ראשוניים של R המוכלים ב־P, לבין אידיאלים ראשוניים של R_P. **הדרכה.** זהו משפט 2.3.19 עבור $S = R-P$.

תרגיל 2.3.24 יהי P אידיאל ראשוני של חוג קומוטטיבי R. אז R_P מקומי, והאידיאל המקסימלי שלו הוא $P_P = (R-P)^{-1}P$. **הדרכה.** תרגיל 2.3.23.

התרגיל האחרון מציג את התועלת שיש במיקום באידיאל ראשוני P: התוצאה היא חוג מקומי, שבו 'נעלמו' כל האידיאלים שאינם מוכלים ב־P. מיקום כזה מאפשר ללמוד את P ללא הפרעות חיצוניות.

תרגיל 2.3.25 תאר את המיקום $\mathbb{Z}_{\langle 7\rangle}$. מצא איבר $t \in \mathbb{Q}$ כך ש־$\mathbb{Z}_{\langle 7\rangle}[t] = \mathbb{Q}$.

תרגיל 2.3.26 אם R תחום שלמות אז לכל אידיאל ראשוני $P \triangleleft R$ יש שיכון $R_P \hookrightarrow \mathrm{q}(R)$, כאשר $\mathrm{q}(R)$ הוא שדה השברים של R.

משפט 2.3.27 *יהי R תחום שלמות. אז חיתוך כל המיקומים $R_M \subseteq F = \mathrm{q}(R)$, על־פני האידיאלים המקסימליים $M \triangleleft R$, שווה ל־R.*

הוכחה. יהי $b^{-1}a \in F$ איבר השייך לכל המיקומים R_P; כלומר, $a \in bR_P$ לכל אידיאל מקסימלי $P \triangleleft R$. עלינו להראות ש־$a \in Rb$, ואז $b^{-1}a \in R$.

יהי $J = b{:}a = \{x \in R :\ xa \in Rb\}$; ברור שזהו אידיאל של R. אם $J \triangleleft R$ אידיאל אמיתי אז הוא מוכל באידיאל מקסימלי $J \subseteq M$, ואז מ־$b^{-1}a \in R_M$ מסיקים ש־$b^{-1}a = b_1^{-1}a_1$ עבור $a_1 \in R$ ו־$b_1 \notin M$. אבל אז $b_1 a = a_1 b \in Rb$, כך ש־$b_1 \in J \subseteq M$, בסתירה לבחירת b_1. מכאן ש־$1 \in J$ ולכן $a \in Rb$. $\square$

תרגיל 2.3.28 יהי R תחום שלמות. אז חיתוך כל המיקומים $R_P \subseteq F = \mathrm{q}(R)$, על־פני האידיאלים הראשוניים $P \triangleleft R$, שווה ל־R.

מסקנה 2.3.29 (ממשפט 2.3.27) יהי R תחום שלמות עם שדה שברים F. אז חיתוך כל החוגים המקומיים $R \subseteq T \subseteq F$ שווה ל־R.

פרק 3

אלגברות אפיניות

בפרק זה כל החוגים קומוטטיביים, ובדרך כלל נניח שהם תחומי שלמות.

3.1 חוגי פולינומים

הגדרה 3.1.1 *תהי $R \supseteq C$ הרחבה של חוגים. אומרים ש־R **אלגברה אפינית** מעל C אם R נוצר סופית כאלגברה מעל C.*

תרגיל 3.1.2 כל אלגברה אפינית מעל C היא חוג מנה של $C[\lambda_1,\dots,\lambda_n]$ עבור n מתאים. ◦

טענה 3.1.3 אם C חוג נתרי, כל אלגברה אפינית מעל C היא נתרית.

הוכחה. (זהו תרגיל 1.4.8). □

תרגיל 3.1.4 **האוניברסליות של חוגי פולינומים:** נניח ש־$\varphi: C \to R$ הומומורפיזם. לכל $\beta_1,\dots,\beta_n \in R$ יש הומומורפיזם יחיד $\bar{\varphi}: C[\lambda_1,\dots,\lambda_n] \to R$ הממשיך את φ, כך ש־$\bar{\varphi}(\lambda_i) = \beta_i$. ◦

תרגיל 3.1.5 K שדה אינסופי. אם $0 \neq f \in K[\lambda_1,\dots,\lambda_n]$, אז יש $\alpha_1,\dots,\alpha_n \in K$ כך ש־$f(\alpha_1,\dots,\alpha_n) \neq 0$. **הדרכה**. אינדוקציה על n. ◦

תרגיל 3.1.6 הראה שהטענה בתרגיל 3.1.5 אינה נכונה עבור שדה סופי $K = \mathbb{F}_q$.

3.2 ממד גלפנד־קירילוב

בסעיף זה נגדיר ממד של אלגברות נוצרות סופית. במקרה הקומוטטיבי נשתמש בממד הזה על מנת להגדיר את ממד הטרנסצנדנטיות, וכך נראה גם שהם שווים. ממילא נובע שממד גלפנד־קירילוב שימושי יותר במקרה הלא קומוטטיבי.

יהי F שדה, ותהי A אלגברה מעל A. תת־מרחב $V \subseteq A$ הוא **יוצר** אם $A = F[V]$; במלים אחרות $A = \sum_{n=0}^{\infty} V^n$. האלגברה נוצרת סופית אם יש לה מרחב יוצר מממד סופי. כדי לפשט את הסכום, נניח ש־$F \subseteq V$, ואז $F \subseteq V \subseteq V^2 \subseteq \cdots$ ו־$A = \bigcup V^n$.

הגדרה 3.2.1 ***ממד גלפנד קירילוב*** *של A (ביחס למרחב יוצר V מממד סופי כך ש־$F \subseteq V$) הוא הגבול* $\text{GKdim}_V(A) = \limsup_{n\to\infty} \frac{\log\dim(V^n)}{\log(n)}$.

במלים אחרות, אם $\text{GKdim}(A) = \alpha$, אז $\dim(V^n) = O(n^{\alpha+\epsilon})$ לכל $\epsilon > 0$.

טענה 3.2.2 ממד גלפנד־קירילוב אינו תלוי במרחב היוצר V.

הוכחה. אם V, W מרחבים יוצרים, אז יש d כך ש־$V \subseteq W^d$, ואז $\frac{\log\dim(V^n)}{\log(n)} \leq \frac{\log\dim(W^{dn})}{\log(dn)} \frac{\log(dn)}{\log(n)}$ מראה ש־$\text{GKdim}_V(A) \leq \text{GKdim}_W(A)$. □

דוגמא 3.2.3 לחוג הפולינומים $A = F[\lambda_1, \ldots, \lambda_d]$ יש ממד d משום שהמרחב היוצר $V = F + F\lambda_1 + \cdots + F\lambda_d$ הוא בעל גידול $\dim(V^n) = \binom{n+d}{d}$, שהוא פולינום ממעלה d.

לעומת זאת לאלגברה החופשית $F\langle a, b\rangle$ יש ממד ∞, משום שהחזקות של $F = F + Fa + Fb$ גדלות אקספוננציאלית.

תרגיל 3.2.4 $\text{GKdim}(A) = 0$ אם ורק אם $\dim_F(A) < \infty$.

תרגיל 3.2.5 אם $\text{GKdim}(A) < 1$ אז $\text{GKdim}(A) = 0$.

טענה 3.2.6 אם $A \subseteq B$ אז $\text{GKdim}(A) \leq \text{GKdim}(B)$.

הוכחה. קח מרחב יוצר V של A ומרחב יוצר $V \subseteq W$ של B. אז $V^n \subseteq W^n$. □

טענה 3.2.7 יהי $s \in A$ איבר רגולרי. אז $\text{GKdim}(A[s^{-1}]) = \text{GKdim}(A)$.

הוכחה. יהי V מרחב יוצר של A. יש ℓ כך ש־$s \in V^\ell$. המרחב $W = V + Fs^{-1}$ יוצר את $A[s^{-1}]$. אבל $sW = F + sV \subseteq V^{\ell+1}$, ולכן $\dim(W^n) = \dim((sW)^n) \leq \dim((V^{\ell+1})^n)$, כך ש־$\text{GKdim}_W(A[s^{-1}]) \leq \text{GKdim}_{V^{\ell+1}}(A)$. □

טענה 3.2.8 נניח ש־$A \subseteq B$ אלגברות קומוטטיביות, ו־B מודול סופי מעל A. אז $\text{GKdim}(B) = \text{GKdim}(A)$.

הוכחה. נכתוב $B = \sum Ax_i$, וניקח $X = \sum Fx_i$ כך ש־$B = AX$. לכל i, j יש $a_{ij}^k \in A$ כך ש־$x_i x_j = \sum a_{ij}^k x_k$. נבחר מרחב יוצר V של A כך שכל $a_{ij}^j \in V$. אז $XX \subseteq VX$. המרחב $V + X$ יוצר את B, ומכיוון ש־$XV = VX$ בגלל הקומוטטיביות, מתקיים $(V + X)^n = V^n + V^{n-1}X$, כך ש־$\dim((V + X)^n) \leq (\dim(X) + 1)\dim(V^n)$. □

3.3 דרגת הטרנסצנדנטיות

3.3.1 אלגבריות

הגדרה 3.3.1 *תהי $C \subseteq R$ הרחבה של חוגים. איבר $a \in R$ הוא* ***אלגברי*** *מעל C אם יש פולינום $0 \neq f \in C[\lambda]$ כך ש־$f(a) = 0$. הרחבה היא אלגברית אם כל איבריה אלגבריים.*

התוצאה המרכזית של הפרק הזה היא מסקנה 3.5.5, המראה שאם אלגברה אפינית היא שדה אז היא מוכרחה להיות אלגברית (מממד סופי מעל F). מכאן נובע שאם אלגברה אפינית אינה אלגברית, אז יש לה אידיאלים (וזה מאפשר להתחיל תהליכי אינדוקציה).

תרגיל 3.3.2 תהי $F \subseteq R$ הרחבה שבה R תחום שלמות ו־F שדה.

1. לכל $a \in R$, $F[a]$ הוא שדה אם ורק אם a אלגברי מעל F.
2. אם $a_1, \dots, a_n \in R$ אלגבריים מעל F אז $F[a_1, \dots, a_n]$ הוא שדה.

טענה 3.3.3 תהי $C \subseteq R$ הרחבה אלגברית של תחומי שלמות. אז כל אידיאל $0 \neq A \triangleleft R$ נחתך עם C.

הוכחה. **יהי $0 \neq a \in A$. אז קיימים $c_0, \cdots, c_n \in C$ כך ש־$c_n a^n + \cdots + c_1 a + c_0 = 0$; אם $c_0 = 0$ אפשר לצמצם ולקבל פולינום ממעלה נמוכה יותר. כך $0 \neq c_0 = -(c_n a^{n-1} + \cdots + c_1) a \in Ra \subseteq A$.** □

תרגיל 3.3.4 תחום שלמות אלגברי מעל שדה הוא שדה בעצמו. **הדרכה.** טענה 3.3.3.

3.3.2 תלות אלגברית

תהי $C \subseteq R$ הרחבה של תחומי שלמות.

הגדרה 3.3.5 ***אומרים ש־$a_1, \dots, a_n \in R$ תלויים אלגברית אם קיים $0 \neq f \in C[\lambda_1, \dots, \lambda_n]$ כך ש־$f(a_1, \dots, a_n) = 0$.***

תרגיל 3.3.6 תהי $C \subseteq R$ הרחבה. האברים $a_1, \dots, a_t$ בלתי תלויים אלגברית אם ורק אם $C[a_1, \dots, a_t] \cong C[\lambda_1, \dots, \lambda_t]$ על־ידי האיזומורפיזם $\lambda_i \mapsto a_i$.

הרחבה $C \subseteq R$ נקראת **טרנסצנדנטית טהורה** אם $R \cong C[\lambda_1, \dots, \lambda_n]$.

3.3.3 הממד הטרנסצנדנטי

הגדרה 3.3.7 ***מטרואיד הוא אוסף לא ריק M של תת־קבוצות (של קבוצה כלשהי), הסגור כלפי מטה ומקיים את האקסיומה הבאה: לכל $A, B \in M$, אם $|A| < |B|$ אז יש $x \in B \setminus A$ כך ש־$A \cup \{x\} \in M$.***

תרגיל 3.3.8 במטרואיד, לכל שני אברים מקסימליים יש אותו גודל. **הדרכה.** אם $|A| < |B|$ אז לפי האקסיומה, A אינו מקסימלי. לכן כל איבר מקסימלי גדול לפחות כמו כל איבר אחר. לכן כל המקסימליים שווים בגודלם.

טענה 3.3.9 תהי $C \subseteq R$ הרחבה של תחומי שלמות. אוסף הקבוצות הבלתי־תלויות אלגברית הוא מטרואיד.

הוכחה. **הסגירות לתת־קבוצה מיידית. תהיינה $A = \{a_1, \dots, a_n\}$ ו־$B = \{b_1, \dots, b_m\}$ קבוצות בלתי תלויות אלגברית. נניח שלכל i, הקבוצה $a_1, \dots, a_n, b_i$ תלויה אלגברית. עלינו להוכיח ש־$m \leq n$. אפשר להניח ש־$m \geq n$ (אחרת סיימנו). נסמן $E = F(a_1, \dots, a_n, b_1, \dots, b_m)$ ו־$K_0 = F(a_1, \dots, a_n)$. לפי ההנחה, E אלגברי מעל K_0.**

נניח ש־E אלגברי מעל שדה $K_r = F(b_1, \dots, b_r, a_{r+1}, \dots, a_n)$, ו־$r < n$. האיבר $b_{r+1} \in B$ אלגברי מעל K_r; התלות הפולינומית חייבת לכלול יוצר מ־A, למשל a_{r+1}, משום ש־B בלתי תלויה. נסמן $K_{r+1} = F(b_1, \dots, b_{r+1}, a_{r+2}, \dots, a_n)$, אז E אלגברי מעל $K_{r+1}(a_{r+1}) = K_r(b_{r+1})$ משום ש־E אלגברי אפילו מעל K_r, ו־$K_{r+1}(a_{r+1})$ אלגברי מעל K_{r+1}. מכאן ש־E אלגברי מעל K_{r+1}.

בסופו של דבר E אלגברי מעל $K_n = F(b_1, \dots, b_n)$, ומכאן ש־$m \leq n$. □

תרגיל 3.3.10 $C \subseteq R$ תחומי שלמות. תת־קבוצה בלתי תלויה מקסימלית נקראת **בסיס טרנסצנדנטי** של R מעל C. גודלה הוא **הממד הטרנסצנדנטי** או **דרגת הטרנסצנדנטיות** $\operatorname{trdeg}_C(R)$.

תרגיל 3.3.11 אם $R = C[a_1, \dots, a_n]$ אז $\operatorname{trdeg}_C(R) \le n$. מתקיים שוויון אם ורק אם $R \cong F[\lambda_1, \dots, \lambda_n]$ הוא חוג הפולינומים ב־n משתנים.

3.4 הרחבות שלמות

אם $C \subseteq R$ הרחבה (של תחומי שלמות) שבה C אינו שדה, יש צורך גם בהגדרה עדינה יותר מסתם אלגבריות. פולינום הוא **מתוקן** אם המקדם העליון שלו הוא 1.

הגדרה 3.4.1 *אומרים ש־$a \in R$ הוא **שלם** מעל C אם x הוא שורש לפולינום מתוקן $f \in C[\lambda]$.*

איננו דורשים שהפולינום יהיה מינימלי. כל איבר שלם מאפס פולינום אי־פריק מעל שדה השברים של C, ולפי הלמה של גאוס, אם C תחום ראשי, אפשר להניח שהפולינום הזה הוא בעל מקדמים ב־C. אבל איננו רוצים להגביל את עצמנו למקרה של C ראשי, וכאמור אין בזה צורך.

טענה 3.4.2 **תהי $C \subseteq R$ הרחבה של תחומי שלמות. התכונות הבאות שקולות:**

1. $a \in R$ שלם;
2. $C[a]$ מודול נוצר סופית מעל C,
3. קיים תת־מודול נוצר סופית של R הכולל את 1 וסגור לכפל ב־a.

הוכחה. $(1) \Longrightarrow (2)$. **נניח ש־a שלם. אז עבור n מתאים, $a^n \in C + Ca + \cdots Ca^{n-1}$, ולכן לכל j מתקיים $a^j \in C + \cdots + Ca^{n-1}$, ומכאן ש־$C[a] = C + \cdots + Ca^{n-1}$ הוא מודול נוצר סופית.** $(2) \Longrightarrow (3)$. **$C[a]$ הוא המודול הדרוש.** $(3) \Longrightarrow (1)$. **נבחר אברים $x_1, \dots, x_m$ כך ש־$M = \sum Cx_i$ הוא תת־מודול שעבורו $aM \subseteq M$. לכל j נכתוב $ax_j = \sum \alpha_{ij} x_i$; כך $[a] = (\alpha_{ij}) \in \mathrm{M}_m(C)$. לפי משפט קיילי־המילטון (שתקף מעל כל חוג קומוטטיבי), $[a]$ מאפסת את הפולינום האופייני $f(\lambda) = \det(\lambda I - [a]) \in C[\lambda]$, שהוא מתוקן. אינדוקציה מראה ש־$a^k x_j = \sum ([a]^k)_{ij} x_i$ לכל $k \ge 1$; בפרט $f(a)M = 0$, $f(a)1 \in f(a)M$, ולכן $f(a) = 0$.** $\square$

הערה 3.4.3 יהיו $C \subseteq R$, $a \in R$, ו־$J \triangleleft C$. אם יש תת־מודול נוצר סופית $M \le R$ כך $1 \in M$ ו־$aM \subseteq JM$, אז a מקיים פולינום מוני שמקדמיו (פרט לראשון) ב־J.

הוכחה. **נכתוב $M = \sum Cx_i$; לפי ההנחה $ax_i = \sum \alpha_{ij} x_i$ עבור $\alpha_{ij} \in J$, ומקדמי הפולינום האופייני שייכים ל־J כמו בהוכחת $(3) \Longrightarrow (1)$ של טענה 3.4.2.** $\square$

תרגיל 3.4.4 מצא פולינום המאפס את $a^{1/3} + b^{1/3}$ מעל F, כאשר $a, b \in F$.

טענה 3.4.5 **תהי $C \subseteq R$ הרחבה. נניח ש־$a_1, \dots, a_t \in R$ שלמים מעל C. אז כל איבר של $C[a_1, \dots, a_t]$ הוא שלם מעל C.**

הוכחה. **לפי טענה 3.4.2, כל אחד מתת־החוגים $C[a_i] = \sum Ca_i^k$ הוא נוצר סופית, ולכן גם תת־החוג $C[a_1,\dots,a_n] = \sum Ca_1^{k_1}\cdots a_t^{k_t}$ הוא מודול נוצר סופית. שוב לפי הטענה, כל איבר שלו הוא שלם מעל** C. □

מסקנה 3.4.6 תהי $R \supseteq C$ הרחבה, ויהיו $a,b \in R$ שלמים מעל C. אז גם $a+b$ ו־ab הם שלמים.

הוכחה. **לפי טענה 3.4.5, שהרי** $a+b, ab \in C[a,b]$. □

מסקנה 3.4.7 אוסף האברים השלמים ב־R מעל C סגור לחיבור, כפל בסקלר וכפל; לכן זוהי אלגברה, הנקראת **הסגור השלם** של C ב־R (נסמן אותה ב־$\mathrm{Int}_C(R)$).

טענה 3.4.8 אם R שלם מעל R' ו־R' שלם מעל C אז R שלם מעל C.

הוכחה. **יהי** $a \in R$. **לפי ההנחה יש** $b_0,\dots,b_{n-1} \in R'$ **כך ש־**$a^n = \sum b_i a^i$; **לכן** a **שלם מעל** $C[b_1,\dots,b_{n-1}]$, **ומכאן ש־**$C[b_1,\dots,b_{n-1}][a]$ **מודול סופי מעל** $C[b_1,\dots,b_{n-1}]$ **שהוא מודול סופי מעל** C. **לפי הגרירה (3)** $\Longleftarrow$ **(1) של טענה 3.4.2,** a **שלם מעל** C. □

הגדרה 3.4.9 *החוג R נקרא **הרחבה שלמה** של C אם $R = \mathrm{Int}_C(R)$, כלומר כל אברי R שלמים מעל C. אומרים ש־C **סגור בשלמות** בתוך R אם $\mathrm{Int}_C(R) = C$.*

תרגיל 3.4.10 הראה ש־$\mathbb{Z}$ סגור בשלמות בתוך $\mathbb{Q}$, ושכל חוג C סגור בשלמות בתוך חוג הפולינומים $C[\lambda]$.

טענה 3.4.11 לכל הרחבה $R \supseteq C$, $\mathrm{Int}_C(R)$ סגור בשלמות בתוך R.

הוכחה. **כל איבר שלם מעל** $\mathrm{Int}_C(R)$ **הוא שלם מעל** C **לפי טענה 3.4.8.** □

תרגיל 3.4.12 נניח ש־a אלגברי, כלומר מאפס פולינום $f(\lambda) = c_0 + \cdots + c_n\lambda^n \in C[\lambda]$. הראה שבמקרה זה $c_n a$ שלם.

תרגיל 3.4.13 נניח ש־C תחום שלמות, ו־F שדה השברים שלו. תהי R הרחבה של C. אז כל האברים האלגבריים של R נמצאים בתת־האלגברה $F \cdot \mathrm{Int}_C(R)$ של $FR = (C - \{0\})^{-1}R$.

תרגיל 3.4.14 אם a אלגברי והפיך, אז גם a^{-1} אלגברי. **הדרכה**. כתוב $\sum_{i=0}^n \alpha_i a^i = 0$, אז $\sum \alpha_i (a^{-1})^{n-i} = 0$.

תרגיל 3.4.15 אם $a \in R$ הפיך ו־a^{-1} שלם, אז $a^{-1} \in C[a]$. **הדרכה**. כתוב $a^{-n} = \sum_{i=0}^{n-1} \alpha_i a^{-i}$, אז $a^{-1} = \sum_{i=0}^{n-1} \alpha_i a^{n-i-1}$.

3.4.1 אידיאלים בהרחבות שלמות

כאן נלמד את הקשר בין האידיאלים של R ו־C.

תרגיל 3.4.16 תהי $C \subseteq R$ הרחבה. לכל אידיאל $A \triangleleft R$, יש שיכון $C/(C \cap A) \hookrightarrow R/A$.

טענה 3.4.17 תהי $C \subseteq R$ הרחבה כלשהי. לכל אידיאל ראשוני $Q \triangleleft R$ ראשוני, $Q \cap C$ אידיאל ראשוני של C.

הוכחה. **לפי תרגיל 3.4.16, $C/(Q \cap C) \hookrightarrow R/Q$; מכיוון ש־$R/Q$ תחום שלמות, גם $C/(Q \cap C)$ תחום שלמות.** □

תרגיל 3.4.18 נניח ש־R שלם מעל C. לכל אידיאל $A \triangleleft R$, גם R/A הרחבה שלמה של $C/(C \cap A)$.

תרגיל 3.4.19 יהי C' הסגור השלם של C בתוך R. אז לכל מונויד $S \subseteq C$, $S^{-1}C'$ הוא הסגור השלם של $S^{-1}C$ בתוך $S^{-1}R$. **הדרכה.** נניח ש־$s^{-1}a \in S^{-1}R$ שלם מעל $S^{-1}C$; הוכח שקיים s' כך ש־$s'a$ שלם מעל C; אז $s^{-1}a = (s's)^{-1}(s'a) \in S^{-1}C'$.

תרגיל 3.4.20 נניח ש־$C \subseteq R$ הרחבה שלמה, אז לכל מונויד $S \subseteq C$, $S^{-1}C \subseteq S^{-1}R$ הרחבה שלמה. **הדרכה.** מקרה פרטי של תרגיל 3.4.19.

למה 3.4.21 נניח ש־R תחום שלמות, ושלם מעל C. אז R שדה אם ורק אם C שדה.

הוכחה. **נניח ש־R שדה. לכל $c \in C$, $c^{-1} \in R$; מכיוון ש־c^{-1} שלם מעל C לפי ההנחה, $c^{-1} \in C[c] = C$ לפי תרגיל 3.4.15. הכיוון ההפוך הוא מקרה פרטי של תרגיל 3.3.4.** □

תרגיל 3.4.22 הוכח את הכיוון ההפוך של למה 3.4.21 ישירות. **הדרכה.** נניח ש־C שדה, ויהי $r \in R$. מכיוון ש־r שלם אפשר לכתוב $r^n + \sum_{i<n} c_i r^i = 0$ עבור n מינימלי; אם $c_0 = 0$ אפשר היה לצמצם בסתירה למינימליות של n, ולכן $r(r^{n-1} + \sum_{0<i<n} c_i r^i) = -c_0$ הפיך.

תרגיל 3.4.23 $R = F[x \colon x^2 = 0]$ היא דוגמא נגדית ללמה 3.4.21, כאשר מוותרים על ההנחה ש־R תחום שלמות. אכן, $F \subseteq R$ היא הרחבה שלמה, ו־R אינו שדה.

מסקנה 3.4.24 נניח ש־R שלם מעל C, ויהי $M \triangleleft R$ אידיאל ראשוני. אז $M \triangleleft R$ מקסימלי אם ורק אם $N = M \cap C \triangleleft C$ מקסימלי.

הוכחה. **לפי תרגיל 3.4.18, R/M הרחבה שלמה של C/N. לפי למה 3.4.21, R/M שדה אם ורק אם C/N שדה, ולכן M מקסימלי אם ורק אם N מקסימלי.** □

תרגיל 3.4.25 העזר בתרגיל 3.4.23 כדי למצוא הרחבה שלמה $C \subseteq R$ עם אידיאל שאינו ראשוני $M \triangleleft R$, כך ש־$C \cap M \triangleleft C$ מקסימלי (זוהי דוגמא נגדית למסקנה 3.4.24, אם מוותרים על ההנחה ש־M ראשוני). **הדרכה.** C הוא שדה, $M = 0$.

טענה 3.4.17 מראה שהחיתוך של אידיאל ראשוני של R עם C הוא אידיאל ראשוני של C. נוכיח שכל אידיאל ראשוני של C מתקבל באופן כזה.

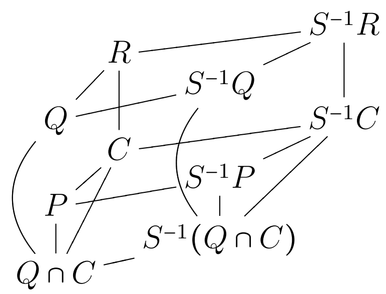
תרגיל 3.4.26 יהי $S \subseteq R$ מונויד כפלי שאינו כולל את אפס. כל אידיאל שאינו נחתך עם S מוכל באידיאל מקסימלי ביחס לאי־החתכות עם S. בפרט יש אידיאלים מקסימליים ביחס לכך שאינם נחתכים עם S. **הדרכה**. קח אידיאל מקסימלי של $S^{-1}R$, או הוכח ישירות בעזרת הלמה של צורן.

טענה 3.4.27 יהי $S \subseteq R$ מונויד כפלי שאינו כולל את אפס. אם $P \triangleleft R$ מקסימלי ביחס לכך ש־$P \cap S = \emptyset$, אז P ראשוני (כאן אין צורך להניח ש־R קומוטטיבי).

הוכחה. נניח ש־$A, B \triangleleft R$ הם אידיאלים המכילים ממש את P. לפי המקסימליות של P, קיימים $s \in S \cap A$ ו־$s' \in S \cap B$; אבל אז $ss' \in S \cap AB$, ומכיוון ש־$S \cap P = \emptyset$, $AB \notin P$. □

משפט 3.4.28 *נניח ש־R שלם מעל C. לכל $P \triangleleft C$ ראשוני קיים $Q \triangleleft R$ ראשוני כך ש־$Q \cap C = P$.*

הוכחה. נסמן $S = C - P$. קח אידיאל מקסימלי $Q' \triangleleft S^{-1}R$. ככל אידיאל ראשוני של $S^{-1}R$, אידיאל זה הוא מהצורה $Q' = S^{-1}Q$ עבור $Q \triangleleft R$ ראשוני. $Q \cap C \subseteq P$ כי $S \cap Q = \emptyset$. מכיוון ש־$S^{-1}R$ היא הרחבה שלמה של החוג (המקומי) $S^{-1}C$, גם שדה המנה $S^{-1}R/S^{-1}Q$ הוא הרחבה שלמה של $S^{-1}C/S^{-1}(Q \cap C)$, ולכן גם $S^{-1}C/S^{-1}(Q \cap C)$ הוא שדה (למה 3.4.21). מכאן ש־$S^{-1}(Q \cap C)$ מקסימלי ב־$S^{-1}C$, ולכן



$$S^{-1}P = S^{-1}(Q \cap C)$$

ו־$P = Q \cap C$ כי שניהם ראשוניים.

□

הערה 3.4.29 תהי $C \subseteq R$ הרחבה שלמה, ויהי $P \triangleleft C$ אידיאל ראשוני. אז לכל $a \in P$ מתקיים $Ra \cap C \subseteq P$.

הוכחה. יהי $r \in R$ כך ש־$ra \in C$. לפי ההנחה יש $c_0, \dots, c_{n-1} \in C$ כך ש־$r^n = \sum c_i r^i$, ואז $(ra)^n = (\sum c_i (ra)^i a^{n-1-i})a \in Ca \subseteq P$, ומכיוון ש־$P$ ראשוני נובע מזה $ra \in P$. □

תרגיל 3.4.30 תן דוגמא נגדית לגרסה החזקה הבאה של הערה 3.4.29: "תהי $C \subseteq R$ הרחבה שלמה, ויהי $a \in C$. אז $Ra \cap C \subseteq Ca$" (שאפשר לנסח גם כך: אם $a, b \in C$ ו־$a | b$ בחוג R, אז $a | b$ בחוג C). **הדרכה**. $\mathbb{Z}[2\sqrt{2}] \subseteq \mathbb{Z}[\sqrt{2}]$ היא הרחבה שלמה.

3.5 יישומים לאלגברות אפיניות

3.5.1 פירוק ההרחבה

יהיו F שדה, ו־$R = F[a_1, \dots, a_n]$ אלגברה אפינית מעל F. נסמן $t = \mathrm{trdeg}_F(R)$, אז יש בסיס טרנסצנדנטי בין היוצרים, שאפשר לסמן $a_1, \dots, a_t \in R$. נסמן $R_0 = F[a_1, \dots, a_t] \subseteq R$; זהו חוג פולינומים, ובפרט תחום שלמות. כעת $F \subseteq R_0 \subseteq R$ כאשר ההרחבה הראשונה טרנסצנדנטית טהורה והשניה אלגברית. אפשר לשפר את המצב:

טענה 3.5.1 תהי R אלגברה אפינית מעל שדה F, שהיא תחום שלמות. אז יש תת־חוג $R_0 \subseteq R$ ואיבר $0 \neq s \in R_0$ כך שעבור $S = \{s^i : i \geq 0\}$, בשרשרת

$$F \subseteq R_0 \hookrightarrow S^{-1}R_0 \subseteq S^{-1}R,$$

ההרחבה הראשונה טרנסצנדנטית, השניה מיקוס, והשלישית היא הרחבה שלמה.

הוכחה. כמקודם נבחר קבוצה בלתי־תלויה אלגברית מקסימלית (שאחרי מספור מחדש אפשר להניח שהיא $(a_1, \ldots, a_t)$, ונסמן $R_0 = F[a_1, \ldots, a_t]$. האברים $a_{t+1}, \ldots, a_n$ אלגבריים מעל R_0. נסמן ב־s את מכפלת המקדמים המובילים של הפולינומים המינימליים שלהם, אז לאחר המיקוס כל הפולינומים מתוקנים. □

משפט הנורמליזציה של נתר משפר את המצב עוד יותר, בכך שהוא מראה שאין צורך במיקום.

משפט 3.5.2 (משפט הנורמליזציה של נתר) תהי $R = F[a_1, \ldots, a_n]$ אלגברה אפינית מעל שדה F. אז קיימים $b_1, \ldots, b_n \in R$ כך ש־$R = F[b_1, \ldots, b_n]$, ו־R שלם מעל תת־החוג $R_0 = F[b_1, \ldots, b_t]$ שהוא טרנסצנדנטי טהור.

הוכחה. נסמן ב־t את גודל הקבוצה הבלתי־תלויה אלגברית המקסימלית בין היוצרים $a_1, \ldots, a_n$, ונסדר את היוצרים כך ש־$a_1, \ldots, a_t$ בלתי תלויים אלגברית. אפשר להניח $t < n$. ההוכחה באינדוקציה על n.

נראה שאפשר למצוא $c_1, \ldots, c_{n-1} \in R$ כך שעבור $R_1 = F[c_1, \ldots, c_{n-1}]$, $R = R_1[a_n]$ שלם מעל R_1, ואז, לפי הנחת האינדוקציה יש תת־חוג טרנסצנדנטי טהור $R_0 \subseteq R_1$ כך ש־R_1 שלם מעל R_0, ואז R שלם מעל R_0 לפי תרגיל 3.4.8.

מכיוון ש־a_n אלגברי מעל $F[a_1, \ldots, a_{n-1}]$, יש פולינום $f(\lambda_1, \ldots, \lambda_n) = \sum \alpha_{i_1 \ldots i_n} \lambda_1^{i_1} \cdots \lambda_n^{i_n} \in F[\lambda_1, \ldots, \lambda_n]$, שאינו טריוויאלי במשתנה λ_n, כך ש־$f(a_1, \ldots, a_n) = 0$. נבחר מספר טבעי m הגדול מהמעלה של f לפי כל λ_i, וניקח $c_i = a_i - a_n^{m^{n-i}}$ $(i < n)$. נתבונן בתת־החוג $R_1 = F[c_1, \ldots, c_{n-1}]$ ובפולינום $h(\lambda) = f(c_1 + \lambda^{m^{n-1}}, \ldots, c_{n-1} + \lambda^m, \lambda) \in R_1[\lambda]$, שהוא סכום הפולינומים

$$\alpha_{i_1 \ldots i_n} (c_1 + \lambda^{m^{n-1}})^{i_1} (c_2 + \lambda^{m^{n-2}})^{i_2} \cdots (c_{n-1} + \lambda^m)^{i_{n-1}} \lambda^{i_n};$$

כל אחד מאלו הוא בעל מקדם מוביל מ־F ומעלה $m^{n-1}i_1 + m^{n-2}i_2 + \cdots + mi_{n-1} + i_n$, ולכן המעלות שונות זו מזו. לכן המונום המוביל של הפולינום בעל המעלה הגדולה ביותר הוא גם המונום המוביל של h, שהוא לפיכך פולינום מוני. מאידך ברור ש־$h(a_n) = 0$, ולכן $R_1[a_n]$ שלם מעל R_1. □

דוגמא 3.5.3 החוג $R = F[x, y, z \mid x^2y + y^2z + z^2x = 0]$ הוא אלגברה אפינית מעל F. בהתאם לסימוני ההוכחה, ניקח $m = 3$, $f(\lambda_1, \lambda_2, \lambda_3) = \lambda_1^2\lambda_2 + \lambda_2^2\lambda_3 + \lambda_3^2\lambda_1$, ואז $c_1 = x - z^9$ ו־$c_2 = y - z^3$. כעת R הרחבה שלמה של $F[x - z^9, y - z^3]$, עם הפולינום המאפס המתוקן $h(\lambda) = f(x - z^9 + \lambda^9, y - z^3 + \lambda^3, \lambda) = \lambda^{21} + \cdots$.

3.5.2 שדות אינם אפיניים

טענה 3.5.4 תהי $R = F[a_1, \ldots, a_n]$ אלגברה אפינית שהיא שדה. אז R אלגברי מעל F.

הוכחה. לפי משפט 3.5.2, R הרחבה שלמה של חוג פולינומים $R_0 = F[a_1, \ldots, a_t]$, כאשר $t = \mathrm{trdeg}(R)$. לפי משפט 3.4.28 כל אידיאל ראשוני של R_0 מתקבל כחיתוך $R_0 \cap Q$ עם אידיאל $Q \triangleleft R$, אבל R שדה, ומכאן שגם R_0 שדה. לכן $t = 0$, ו־R אלגברי. □

מסקנה 3.5.5 יהי F שדה סגור אלגברית. אלגברה אפינית $R = F[a_1, \ldots, a_n]$ המכילה ממש את F אינה יכולה להיות שדה.

הוכחה. אחרת R אלגברי מעל F לפי מסקנה 3.5.4, ואז $R = F$ שהרי F סגור אלגברית. □

3.5.3 המשכת הומומורפיזמים

בתת־סעיף זה נשתמש במשפט הנורמליזציה כדי להוכיח את מסקנה 3.5.8, שנזדקק לה לצורך משפט האפסים של הילברט (משפט 4.2.37). הגישה של המשכת הומומורפיזמים מאפשרת גם לעקוף את הנורמליזציה בהוכחה שאלגברה אפינית אינה שדה (מסקנה 3.5.5).

משפט 3.5.6 *תהי $C \subseteq R$ הרחבה שלמה, ויהי K שדה. לכל הומומורפיזם $\varphi : C \to K$ קיימת המשכה $\bar{\varphi} : R \to \hat{K}$ כאשר $\hat{K}$ הסגור האלגברי של K.* ∘

$$\begin{tikzcd}
R \arrow[rrrr, dotted, "\bar{\varphi}"] \arrow[dr, two heads] & & & & \hat{K} \\
& \bar{R} \arrow[r, hook] & S^{-1}\bar{R} \arrow[r, hook] & \hat{F} \arrow[ur, hook] & \\
C \arrow[uu, hook] \arrow[rrrr, "\varphi"] \arrow[dr, two heads] & & & & K \arrow[uu, hook] \\
& \bar{C} \arrow[r, hook] \arrow[uu, hook] & F \arrow[r, equal] \arrow[uu, hook] & F \arrow[uu, hook] \arrow[ur, hook] &
\end{tikzcd}$$

הוכחה. נסמן $P = \mathrm{Ker}(\varphi)$, אז $C/P \cong \varphi(C) \subseteq K$ ולכן P ראשוני. לפי משפט 3.4.28, יש אידיאל ראשוני $Q \triangleleft R$ כך ש־$Q \cap C = P$. לפי תרגיל 3.4.18, $\bar{R} = R/Q$ שלם מעל $\bar{C} = (C+Q)/Q \cong C/P$. נסמן $S = \bar{C} - \{0\}$, אז $S^{-1}\bar{R}$ הרחבה שלמה של שדה השברים $F = \mathrm{q}(\bar{C}) = S^{-1}\bar{C}$ לפי תרגיל 3.4.20, כלומר, $S^{-1}\bar{R}$ תחום שלמות אלגברי מעל F. לפי תרגיל 3.3.4 נובע מכך ש־$S^{-1}\bar{R}$ שדה, ומכיוון שהוא אלגברי מעל F, הוא משוכן בסגור האלגברי $\hat{F}$. אבל $F \subseteq K$ ולכן יש שיכון $\hat{F} \hookrightarrow \hat{K}$. הרכבת החצים בפאה העליונה של הדיאגרמה נותנת את $\bar{\varphi}$. □

משפט 3.5.7 *$K \subseteq F$ שדות. יהי $R = F[a_1, \dots, a_n]$ תחום שלמות אפיני. אז יש הומומורפיזם של F־אלגברות $R \to \hat{K}$, כאשר $\hat{K}$ אלגברי מעל K.* ∘

הוכחה. לפי משפט הנורמליזציה של נתר, יש תת־חוג $R_0 \subseteq R$, איזומורפי לחוג פולינומים, כך ש־R שלם מעל R_0. לפי משפט 3.5.6, אפשר להמשיך ל־$R \to \hat{K}$ כל הומומורפיזם $R_0 \to K$. □

מסקנה 3.5.8 יהי $R = F[a_1, \dots, a_n]$ תחום שלמות אפיני מעל השדה F. אז יש הומומורפיזם $R \to \hat{F}$ הממשיך את הזהות על F. ∘

מסקנה 3.5.9 יהי $R = F[a_1, \dots, a_n]$ תחום שלמות אפיני מעל שדה סגור אלגברית F. אז יש הומומורפיזם $R \to F$ הממשיך את הזהות על F. ∘

תרגיל 3.5.10 השתמש במסקנה 3.5.8 כדי לתת הוכחה אחרת לטענה 3.5.4. **הדרכה**. לפי מסקנה 3.5.8 יש הומומורפיזם מ־R להרחבה אלגברית של F, וכל הומומורפיזם של שדות הוא שיכון.

כעת נציג הוכחה של מסקנה 3.5.5 שאינה זקוקה לנורמליזציה.

תרגיל 3.5.11 הומומורפיזם $\varphi : R \to K$ עם $\varphi(s) \neq 0$, אז יש $\varphi : S^{-1}R \to K$ הממשיך את φ, כאשר $S = \{s^i : i \geq 0\}$. **הדרכה**. הגדר $\bar{\varphi}(s^{-i}r) = \varphi(s)^{-i}\varphi(r)$; קל לאשר ש־$\bar{\varphi}$ מוגדר היטב וממשיך את φ. ∘

תרגיל 3.5.12 תן הוכחה למשפט 3.5.7, בהנחה ש־K אינסופי, שאינה משתמשת במשפט הנורמליזציה של נתר. **הדרכה**. לפי טענה 3.5.1, יש תת־חוג $R_0 \subseteq R$ ואיבר $0 \neq s \in R_0$ כך שבשרשרת

$$F \subseteq R_0 \hookrightarrow \langle s \rangle^{-1} R_0 \subseteq \langle s \rangle^{-1} R,$$

ההרחבה הראשונה טרנסצנדנטית, השניה מיקום, והשלישית היא הרחבה שלמה. לפי תרגיל 3.1.5 יש הומומורפיזם $\varphi' : R_0 \to K$ כך ש־$\varphi'(s) \neq 0$. לפי תרגיל 3.5.11 יש המשכה $\varphi'' : \langle s \rangle^{-1} R_0 \to K$. מסיימים בעזרת משפט 3.5.6.

פרק 4

מבוא לגאומטריה אלגברית

בפרק זה נקבע שדה F ונתבונן בעיקר באידיאלים של חוג הפולינומים $F[\lambda_1, \ldots, \lambda_n]$. החוג הזה הוא **חוג הפונקציות** (הפולינומיות) של המרחב האפיני F^n.

4.1 קבוצות אלגבריות ואידיאלים גאומטריים

הגדרה 4.1.1 *תהי $A \subseteq F[\lambda_1, \ldots, \lambda_n]$ קבוצה של פולינומים.* ***קבוצת האפסים*** *$Z(A)$ היא קבוצת* ***הנקודות*** *$v \in F^n$ כך ש־$f(v) = 0$ לכל $f \in A$.*

תרגיל 4.1.2 לכל קבוצה A, $\mathcal{Z}(A) = \mathcal{Z}(\langle A \rangle)$.

לכן אפשר לדבר על קבוצות האפסים של אידיאלים ב־R. קבוצה מהצורה $\mathcal{Z}(A)$ נקראת **קבוצה אלגברית**. גאומטריה אלגברית לומדת את קבוצות האפסים האלה, כלומר את המקומות הגאומטריים שאפשר להגדיר על־ידי תנאים פולינומיים.

הגדרה 4.1.3 *לכל קבוצה $S \subseteq F^n$, $\mathcal{I}(S) = \{f \in R : (\forall s \in S) f(s) = 0\}$ -* ***קבוצת הפולינומים המאפסים את כל אברי*** *S.*

תרגיל 4.1.4 האופרטורים $\mathcal{I}, \mathcal{Z}$ מקיימים את התכונות הבאות:

1. אם $A_1 \subseteq A_2$ אז $\mathcal{Z}(A_1) \supseteq \mathcal{Z}(A_2)$.
2. אם $S_1 \subseteq S_2$ אז $\mathcal{I}(S_1) \supseteq \mathcal{I}(S_2)$.
3. לכל A, $A \subseteq \mathcal{I}(\mathcal{Z}(A))$.
4. לכל S, $S \subseteq \mathcal{Z}(\mathcal{I}(S))$.

תרגיל 4.1.5 הוכח מן התכונות בתרגיל 4.1.4 ש־S קבוצה אלגברית אם ורק אם $S = \mathcal{Z}(\mathcal{I}(S))$, ו־$A$ אידיאל מהצורה $\mathcal{I}(S)$ אם ורק אם $A = \mathcal{I}(\mathcal{Z}(A))$.

4.2 רדיקלים

השאלה המדריכה אותנו בסעיף זה: אילו אידיאלים הם מהצורה $\mathcal{I}(S)$?

הגדרה 4.2.1 *יהי $A \triangleleft R$ אידיאל בחוג קומוטטיבי. אז* $\sqrt{A} = \{f \in A\colon (\exists n) f^n \in A\}$ ***הוא הרדיקל*** *של A.*

תרגיל 4.2.2 $\sqrt{A}$ הוא אידיאל (אמיתי) של R, המכיל את A.

תרגיל 4.2.3 אם $A \subseteq A'$ אז $\sqrt{A} \subseteq \sqrt{A'}$.

הגדרה 4.2.4 *אידיאל A* ***נקרא רדיקלי*** *אם $A = \sqrt{A}$.*

תרגיל 4.2.5 כל רדיקל $\sqrt{A}$ הוא אידיאל רדיקלי. (כלומר $\sqrt{\sqrt{A}} = \sqrt{A}$.)

תרגיל 4.2.6 $\sqrt{\sqrt{A}+\sqrt{B}} = \sqrt{A+B}$. **פתרון**. ראשית, $A, B \subseteq A+B$ ולכן $\sqrt{A}+\sqrt{B} \subseteq \sqrt{A+B}$. אבל, $A+B \subseteq \sqrt{A}+\sqrt{B}$, ולכן $\sqrt{A+B} \subseteq \sqrt{\sqrt{A}+\sqrt{B}} \subseteq \sqrt{\sqrt{A+B}} = \sqrt{A+B}$ לפי תרגיל 4.2.5.

תרגיל 4.2.7 תן דוגמא נגדית לטענה $\sqrt{A+B} = \sqrt{A}+\sqrt{B}$, עבור $A, B \triangleleft F[\lambda_1, \lambda_2]$.
הדרכה. קח $A = \langle \lambda_1 \rangle$, $B = \langle \lambda^2 - \lambda_1 \rangle$; כך $A+B = \langle \lambda_1, \lambda_2^2 \rangle$.

תרגיל 4.2.8
1. $\sqrt{\bigcap A_\lambda} \subseteq \bigcap \sqrt{A_\lambda}$, אבל במקרה הכללי לא חייב להתקיים שוויון.
2. $\sqrt{A \cap B} = \sqrt{A} \cap \sqrt{B}$. **פתרון**. ההכלה $\subseteq$ ברורה. נניח $x \in \sqrt{A} \cap \sqrt{B}$, אז קיים n כך ש-$x^n \in A$, וקיים n' כך ש-$x^{n'} \in B$. לכן $x^{\max\{n,n'\}} \in A \cap B$.

טענה 4.2.9 חיתוך של אידיאלים רדיקליים הוא רדיקלי.

הוכחה. יהיו A_i אידיאלים רדיקליים ($i \in I$, I קבוצת אינדקסים כלשהי), ויהי $A = \cap A_i$. אם $r \in \sqrt{A}$ אז $r^m \in A$ עבור m מתאים, ואז $r^m \in P_i$ לכל i, ו-$r \in P_i$ לפי הרדיקליות של כל אחד מהאידיאלים. לכן $r \in \cap A_i = A$. □

תרגיל 4.2.10 נניח ש-$A \subseteq B$, אז $\sqrt{B/A} = \sqrt{B}/A$.

תרגיל 4.2.11 יהי R תחום פריקות יחידה. נניח ש-$a = p_1^{n_1} \cdots p_k^{n_k}$ כאשר p_i ראשוניים זרים. הראה ש-$\sqrt{Ra} = Rp_1 \cdots p_k$.

תרגיל 4.2.12 הראה ש-$\sqrt{A} = \sqrt{A^n}$.

תרגיל 4.2.13 הראה ש-$\sqrt{AB} \subseteq \sqrt{A}\sqrt{B}$.

תרגיל 4.2.14 הראה שבתחום ראשי מתקיים $\sqrt{A}+\sqrt{B} = \sqrt{A+B}$.

תרגיל 4.2.15 אם R תחום ראשי, אז $\sqrt{AB}\sqrt{A+B} = \sqrt{A}\sqrt{B}$. האם השוויון הזה נכון בכל חוג קומוטטיבי?

4.2.1 חוג ראשוני למחצה

חוגים ראשוניים למחצה מאפשרים לזהות רדיקליות דרך מעבר לחוג המנה.

הגדרה 4.2.16 *איבר $a \in R$ הוא נילפוטנטי אם $a^m = 0$ ל־m גדול מספיק. חוג (קומוטטיבי) R נקרא ראשוני למחצה אם אין בו איברים נילפוטנטים.*

תרגיל 4.2.17 הראה ש־R ראשוני למחצה אם ורק אם $0 \triangleleft R$ אידיאל רדיקלי.

תרגיל 4.2.18 החוג הקומוטטיבי R הוא ראשוני למחצה אם ורק אם $x^2 = 0$ גורר $x = 0$, אם ורק אם $J^2 = 0$ גורר $J = 0$. **הדרכה**. אם מ־$x^2 = 0$ נובע $x = 0$, אז לכל $n \geq 2$, אם $x^n = 0$ גם $x^{2(n-1)} = 0$ ולכן $x^{n-1} = 0$.

תרגיל 4.2.19 החוג R ראשוני למחצה אם ורק אם אין בו אידיאלים נילפוטנטיים.

טענה 4.2.20 יהי R חוג קומוטטיבי. אז $A \triangleleft R$ רדיקלי אם ורק אם R/A ראשוני למחצה.

הוכחה. נניח ש־A רדיקלי, ויהי $r + A \in R/A$; אם $(r+A)^m = r^m + A = 0$ אז $r^m = A$ ולכן $A = \sqrt{A} \ni r$, כלומר $r + A = \bar{0} \in R/A$. מאידך נניח ש־R/A ראשוני למחצה, ויהי $r \in \sqrt{A}$; אז $r^m \in A$ עבור m מתאים, ולכן $(r+A)^m = r^m + A = \bar{0} \in R/A$; לפי ההנחה נובע מכאן $r + A = 0$, כלומר $r \in A$, והוכחנו $A = \sqrt{A}$. □

תרגיל 4.2.21 כל תחום שלמות הוא ראשוני למחצה.

תרגיל 4.2.22 החוג $\mathbb{Z} \times \mathbb{Z}$ הוא ראשוני למחצה ואינו תחום שלמות.

תרגיל 4.2.23 מכפלה ישרה (לאו דווקא סופית) של שדות היא ראשונית למחצה.

תרגיל 4.2.24 אם $A \triangleleft R$ הוא ראשוני למחצה גם כאידיאל וגם כחוג (בלי יחידה), אז R ראשוני למחצה. **הדרכה**. יהי $I \triangleleft R$ ונניח $I^2 = 0 \subseteq A$, אז $I \subseteq A$ ולכן $I \triangleleft A$.

תרגיל 4.2.25 נניח ש־R ראשוני למחצה כחוג, ו־$A \triangleleft R$ הוא אידיאל ראשוני למחצה. אז גם A ראשוני למחצה כחוג. **הדרכה**. אם $I \triangleleft A$ ו־$I^2 = 0$ אז $(AIA)^2 = AIAIA \subseteq AI^2A = 0$ ולכן $AIA = 0$.

4.2.2 הרדיקל הראשוני

תרגיל 4.2.26 כל אידיאל ראשוני הוא רדיקלי. **הדרכה**. טענה 4.2.20 ותרגיל 4.2.21.

מסקנה 4.2.27 יהי R חוג כלשהו. לכל $a \in R$ שאינו נילפוטנטי (הגדרה 5.2.1) יש אידיאל ראשוני P כך ש־$a \notin P$.

הוכחה. לפי ההנחה המונויד $S = \langle a \rangle$ אינו כולל את 0. קח P מקסימלי ביחס לתכונה $S \cap P = \emptyset$ (השקולה ל־$a \notin P$ אם R קומוטטיבי); אידיאל כזה קיים לפי תרגיל 3.4.26, והוא ראשוני לפי טענה 3.4.27. □

מסקנה 4.2.28 נניח ש־R ראשוני למחצה. לכל $0 \neq a \in R$ יש אידיאל ראשוני P כך ש־$a \notin P$.

הוכחה. זו מסקנה 4.2.27 כי כאשר R ראשוני למחצה, אם $a \neq 0$ אז $a^n \neq 0$ לכל n. □

הגדרה 4.2.29 *חיתוך כל האידיאלים הראשוניים בחוג R נקרא* ***הרדיקל הראשוני*** *של R, ומסמנים אותו ב־$\operatorname{rad}(R)$. (באופן כללי יותר, אם $I \triangleleft R$ אז חיתוך כל הראשוניים המכילים את I נקרא* ***הרדיקל של*** *I).*

מסקנה 4.2.30 הרדיקל של כל חוג הוא נילי (ולכן הרדיקל הראשוני נקרא גם **הרדיקל הנילי התחתון**).

מסקנה 4.2.31 בחוג (קומוטטיבי) ראשוני למחצה, $\operatorname{rad}(R) = 0$.

כעת אפשר להוכיח את התוצאה המרכזית על אידיאלים רדיקליים:

מסקנה 4.2.32 אידיאל רדיקלי שווה לחיתוך כל האידיאלים הראשוניים המכילים אותו.

הוכחה. יהי A אידיאל רדיקלי, ויהי A' חיתוך האידיאלים הראשוניים המכילים את A. ברור ש־$A \subseteq A'$. יהי $a \notin A$. נתבונן בחוג הראשוני למחצה R/A, שבו $\bar{a} = a + A \neq 0$. לפי מסקנה 4.2.28 יש אידיאל ראשוני $\bar{P} = P/A \triangleleft R/A$ כך ש־$\bar{a} \notin \bar{P}$, אבל אז $a \notin P$ ומכיוון שגם P ראשוני, $a \notin A'$. לכן $A' = A$, כדרוש. □

בפרט, אידיאל הוא רדיקלי אם ורק אם הוא חיתוך של ראשוניים. (במשפט 5.3.3 נראה שבחוג נתרי, החיתוך של מסקנה 4.2.32 הוא תמיד סופי.)

מסקנה 4.2.33 בכל חוג קומוטטיבי R, $\operatorname{rad}(R) = \sqrt{0}$.

4.2.3 משפט האפסים של הילברט

תרגיל 4.2.34 כל אידיאל מהצורה $\mathcal{I}(S)$ הוא רדיקלי. **פתרון**. נסמן $A = \mathcal{I}(S)$. עלינו להוכיח ש־$\sqrt{A} = A$. יהי $f \in \sqrt{A}$, אז קיים k כך ש־$f^k \in A$, כלומר $f(a_1,\dots,a_n)^k = 0$ לכל $(a_1,\dots,a_n) \in S$; אבל F שדה ולכן גם $f(a_1,\dots,a_n) = 0$, כך ש־$f \in \mathcal{I}(S) = A$.

תרגיל 4.2.35 לכל $A \triangleleft F[\lambda_1,\dots,\lambda_n]$ מתקיים $\sqrt{A} \subseteq \mathcal{I}(\mathcal{Z}(A))$. **פתרון**. ברור ש־$A \subseteq \mathcal{I}(\mathcal{Z}(A))$, ולפי תרגיל 4.2.34, גם $\sqrt{A} \subseteq \sqrt{\mathcal{I}(\mathcal{Z}(A))} = \mathcal{I}(\mathcal{Z}(A))$.

תרגיל 4.2.36 $\mathcal{Z}(\sqrt{A}) = \mathcal{Z}(A)$. **פתרון**. מכיוון ש־$A \subseteq \sqrt{A}$, ברור ש־$\mathcal{Z}(\sqrt{A}) \subseteq \mathcal{Z}(A)$. בכיוון ההפוך נניח ש־$s = (s_1,\dots,s_n) \in \mathcal{Z}(A)$, ויהי $f \in \sqrt{A}$. אז קיים k כך ש־$f^k \in A$, כך ש־$f(s)^k = 0$; לכן גם $f(s) = 0$, ו־$s \in \mathcal{Z}(\sqrt{A})$.

משפט 4.2.37 (Hilbert's Nullstellensatz) *נניח ש־F סגור אלגברית. לכל אידיאל $A \triangleleft F[\lambda_1,\dots,\lambda_n]$ מתקיים $\mathcal{I}(\mathcal{Z}(A)) = \sqrt{A}$.*

הוכחה. הכיוון $\sqrt{A} \subseteq \mathcal{I}(\mathcal{Z}(A))$ הוא תרגיל 4.2.35. נותר להוכיח את ההכלה ההפוכה, $\mathcal{I}(\mathcal{Z}(A)) \subseteq \sqrt{A}$, וזאת נעשה בדרך השלילה. נניח ש־$f \in \mathcal{I}(\mathcal{Z}(A))$, ו־$f \notin \sqrt{A}$. לפי מסקנה 4.2.32, יש אידיאל ראשוני $P \triangleleft F[\lambda_1,\dots,\lambda_n]$, כך ש־$A \subseteq P$ ו־$f \notin P$. נתבונן בתחום השלמות האפיני $R = F[\lambda_1,\dots,\lambda_n]/P$, שבו $\bar{f} \neq 0$. נסמן ב־K את שדה השברים של R, ונתבונן ב־$R' = R[\bar{f}^{-1}] \subseteq K$. מכיוון ש־$F$ סגור אלגברית, לפי מסקנה 3.5.9 יש המשכה $\varphi\colon R' \to F$ של הזהות. כך מתקבלת ההרכבה $\psi\colon F[\lambda_1 \dots,\lambda_n] \twoheadrightarrow R \hookrightarrow R' \xrightarrow{\varphi} F$, המקיימת $\psi(f) = \varphi(f) \neq 0$.

נתבונן בווקטור $x = (\psi(\lambda_1),\dots,\psi(\lambda_n)) \in F^n$. לכל $g = \sum \alpha_{\vec{i}} \lambda_1^{i_1} \dots \lambda_n^{i_n}$ מתקיים

$$g(\psi(\lambda_1),\dots,\psi(\lambda_n)) = \sum \alpha_{\vec{i}} \psi(\lambda_1)^{i_1} \dots \psi(\lambda_n)^{i_n} = \psi(g);$$

אם $g \in A$ אז $g + A = \bar{0} \in R$ וממילא $\psi(g) = 0$, ומכאן ש־$x \in \mathcal{Z}(A)$. אבל לפי ההנחה $f \in \mathcal{I}(\mathcal{Z}(A))$, ולכן $0 = f(x) = \psi(f) \neq 0$, וזו סתירה. □

במלים אחרות, כל יחס המתקיים בקבוצת הפתרונות המשותפים של הפולינומים $f_1 = \cdots = f_k = 0$, אפשר להסיק מן הזהויות $f_i = 0$ על־ידי פעולות חיבור וחיסור, כפל בפולינום כלשהו, והוצאת שורש.

משפט האפסים של הילברט משלים סוף־סוף את ההתאמה בין קבוצות אלגבריות לאידיאלים רדיקליים:

מסקנה 4.2.38 ההתאמה בין קבוצות אלגבריות לאידיאלים רדיקליים, הנתונה על־ידי $\mathcal{I}$ ו־$\mathcal{Z}$, היא חד־חד־ערכית ועל. אכן, לפי המשפט $A = \sqrt{A} = \mathcal{I}(\mathcal{Z}(A))$ לכל A רדיקלי, ואם S קבוצה אלגברית אז $S = \mathcal{Z}(\mathcal{I}(S))$ לפי תרגיל 4.1.5.

מסקנה 4.2.39 (מעל שדה סגור אלגברית) אידיאל הוא מהצורה $\mathcal{I}(S)$ אם ורק אם הוא רדיקלי.

הוכחה. תרגיל **4.2.34** ומשפט **4.2.37**. $\square$

תרגיל 4.2.40 נניח ש־F סגור אלגברית. אם $\mathcal{Z}(f) \subseteq \mathcal{Z}(A)$ אז $f \in \sqrt{A}$. **פתרון**. לפי משפט האפסים, $f \in \mathcal{I}(\mathcal{Z}(f)) \subseteq \mathcal{I}(\mathcal{Z}(A)) = \sqrt{A}$.

מכאן נובעת מסקנה חשובה:

מסקנה 4.2.41 נניח ש־F סגור אלגברית. לכל אידיאל אמיתי $A \triangleleft F[\lambda_1, \ldots, \lambda_n]$, $\mathcal{Z}(A) \neq \varnothing$. ◦

הוכחה. **אחרת** $F[\lambda_1, \ldots, \lambda_n] = \mathcal{I}(\varnothing) = \mathcal{I}(\mathcal{Z}(A)) = \sqrt{A}$. $\square$

תרגיל 4.2.42 תן דוגמא נגדית למשפט האפסים של הילברט מעל שדה שאינו סגור אלגברית. היכן בדיוק נכשלת ההוכחה?

(לגרסה מעל הממשיים, ראה תרגיל 3.4.28 בספר על Model Theory של David Marker.)

תרגיל 4.2.43 $f(x,y) \in F[x,y]$ כאשר F שדה אינסופי, ו־$f(\alpha,\alpha) = 0$ לכל $\alpha \in F$. הוכח ש־$(x-y) \mid f(x,y)$.

הדרכה. מכיוון ש־$x^n y^m = (x^n - y^n)y^m + y^{n+m}$, אפשר לחלק ב־$F[x,y]$ ולהציג $f(x,y) = (x-y)g(x,y) + h(y)$. כעת, לפי ההנחה, $h(\alpha) = f(\alpha,\alpha) = 0$ לכל α, ולכן $h(y) = 0$ ו־$(x-y) \mid f(x,y)$.

תרגיל 4.2.44 $f(x,y) \in F[x,y]$ כאשר F סגור אלגברית, ו־$f(\alpha,\alpha^{-1}) = 0$ לכל $\alpha \in F^{\times}$. הוכח ש־$(xy-1) \mid f(x,y)$.

הדרכה. לפי הנתון $\mathcal{Z}(\langle xy-1\rangle) \subseteq \mathcal{Z}(\langle f\rangle)$ ולכן

$$\langle f\rangle \subseteq \sqrt{\langle f\rangle} = \mathcal{I}(\mathcal{Z}(\langle f\rangle)) \subseteq \mathcal{I}(\mathcal{Z}(\langle xy-1\rangle)) = \sqrt{\langle xy-1\rangle} = \langle xy-1\rangle.$$

4.2.4 האידיאלים המקסימליים של חוג הפולינומים

עבור $s = (s_1, \ldots, s_n) \in F^n$, נסמן $P_s = \langle \lambda_1 - s_1, \ldots, \lambda_n - s_n \rangle \triangleleft R = F[\lambda_1, \ldots, \lambda_n]$.

טענה 4.2.45 1. P_s הוא אידיאל מקסימלי.

2. $\mathcal{Z}(P_s) = \{s\}$.

3. $\mathcal{I}(\{s\}) = P_s$.

הוכחה. **1. המנה $F[\lambda_1, \ldots, \lambda_n]/P_s \cong F$ על־ידי ההצבה $\lambda_i \mapsto s_i$.**

2. לכל נקודה $s' = (s'_1, \ldots, s'_n)$, הצבת $\lambda_i \mapsto s'_i$ מאפסת את $\lambda_i - s_i$ אם ורק אם $s'_i = s_i$.

3. בזכות האוטומורפיזם של חוג הפולינומים המוגדר על־ידי $\lambda_i \mapsto \lambda_i + s_i$, מספיק להוכיח את הטענה עבור $s = 0$. נכתוב $R = F[\lambda_1, \ldots, \lambda_n]$, אז $R = \sum R\lambda_i \oplus F$, וההטלה על הרכיב האחרון היא ההצבה.

□

לכן כל נקודה היא קבוצה אלגברית.

טענה 4.2.46 נניח ש־F סגור אלגברית. אז כל אידיאל מקסימלי הוא מהצורה P_s.

הוכחה. יהי P אידיאל מקסימלי. **אז $\mathcal{Z}(P) \neq \varnothing$ לפי מסקנה 4.2.41. נבחר $s \in \mathcal{Z}(P)$, אז $P = \sqrt{P} = \mathcal{I}(\mathcal{Z}(P)) \subseteq \mathcal{I}(\{s\}) = P_s$ לפי משפט האפסים.** □

תרגיל 4.2.47 מצא אידיאל מקסימלי של $\mathbb{R}[\lambda_1, \lambda_2]$ שאינו מהצורה $\langle \lambda_1 - a_1, \lambda_2 - a_2 \rangle$.

תרגיל 4.2.48 מצא את כל האידיאלים המקסימליים של $\mathbb{C}[x, y]/\langle y^2 - x^3 + x \rangle$.

4.3 קבוצות אלגבריות אי־פריקות

טענה 4.2.46 מראה שההתאמה בין אידיאלים רדיקליים לבין קבוצות אלגבריות משייכת אידיאלים מקסימליים לנקודות ב־F^n. בסעיף זה נברר אילו קבוצות מתאימות לאידיאלים ראשוניים.

הגדרה 4.3.1 *קבוצה אלגברית S היא **אי־פריקה** אם אי־אפשר לכתוב אותה בצורה $S = S_1 \cup S_2$ כאשר $S_1, S_2 \subset S$ קבוצות אלגבריות.*

טענה 4.3.2 לכל שני אידיאלים $A_1, A_2 \triangleleft F[\lambda_1, \ldots, \lambda_n]$,

1. $\mathcal{Z}(A_1) \cup \mathcal{Z}(A_2) = \mathcal{Z}(A_1 \cap A_2)$,

2. $\mathcal{Z}(A_1) \cap \mathcal{Z}(A_2) = \mathcal{Z}(A_1 + A_2)$.

הוכחה. **1. מכיוון ש־$A_1 \cap A_2 \subseteq A_1, A_2$, ההכלה $\mathcal{Z}(A_1) \cup \mathcal{Z}(A_2) \subseteq \mathcal{Z}(A_1 \cap A_2)$ ברורה. בכיוון ההפוך נניח ש־$v \notin \mathcal{Z}(A_1), \mathcal{Z}(A_2)$; אז יש $f_i \in A_i$ כך ש־$f_i(v) \neq 0$, וממילא $(f_1 f_2)(v) \neq 0$, כך ש־$v \notin \mathcal{Z}(\langle f_1 f_2 \rangle)$. אבל $f_1 f_2 \in A_1 \cap A_2$, ולכן $v \notin \mathcal{Z}(A_1 \cap A_2)$.**

2. ברור ש־$\mathcal{Z}(A_1+A_2) \supseteq \mathcal{Z}(A_1)\cap\mathcal{Z}(A_2)$. נניח ש־$v \in \mathcal{Z}(A_1)\cap\mathcal{Z}(A_2)$. לכל $f \in A_1+A_2$ נכתוב $f = f_1 + f_2$ עבור $f_i \in A_i$, אז $f(v) = f_1(v) + f_2(v) = 0$, ולכן $v \in \mathcal{Z}(A_1 + A_2)$.
□

תרגיל 4.3.3 $BC \subseteq B \cap C \subseteq \sqrt{BC}$. **פתרון.** אם $d \in B \cap C$ אז $d^2 \in BC$ ולכן $d \in \sqrt{BC}$.

תרגיל 4.3.4 אם $BC \subseteq A$ אז $B \cap C \subseteq \sqrt{A}$. **פתרון.** $B \cap C \subseteq \sqrt{BC} \subseteq \sqrt{A}$ לפי תרגיל 4.3.3.

טענה 4.3.5 יהי F שדה סגור אלגברית. נניח ש־A רדיקלי. אז A אידיאל ראשוני אם ורק אם $\mathcal{Z}(A)$ קבוצה אלגברית אי־פריקה.

הוכחה. נניח ש־A ראשוני, ובכל זאת $\mathcal{Z}(A) = S_1 \cup S_2$ כאשר $S_i \subset \mathcal{Z}(A)$ קבוצות אלגבריות. לפי תרגיל 4.2.36 כל קבוצה אלגברית היא מהצורה $S_i = \mathcal{Z}(A_1)$ עבור A_i רדיקלי. לפי משפט האפסים

$$\begin{aligned} A &= \sqrt{A} \\ &= \mathcal{I}(\mathcal{Z}(A)) \\ &= \mathcal{I}(\mathcal{Z}(A_1) \cup \mathcal{Z}(A_2)) \\ &= \mathcal{I}(\mathcal{Z}(A_1 \cap A_2)) \\ &= \sqrt{A_1 \cap A_2} \\ &= \sqrt{A_1} \cap \sqrt{A_2} \\ &= A_1 \cap A_2, \end{aligned}$$

אבל מתרגיל 2.2.6 נובע ש־$A = A_1$ או $A = A_2$, בסתירה להנחה $\mathcal{Z}(A_i) \subset \mathcal{Z}(A)$.

בכיוון ההפוך, נניח ש־$\mathcal{Z}(A)$ אי־פריקה. נניח ש־A אינו ראשוני, אז יש אידיאלים $A_1, A_2 \supset A$ כך ש־$A_1A_2 \subseteq A$, ולפי תרגיל 4.3.4, $A_1 \cap A_2 \subseteq \sqrt{A}$. לכן

$$\mathcal{Z}(A) \supseteq \mathcal{Z}(A_1) \cup \mathcal{Z}(A_2) = \mathcal{Z}(A_1 \cap A_2) \supseteq \mathcal{Z}(\sqrt{A}) = \mathcal{Z}(A),$$

וזה פירוק של $\mathcal{Z}(A)$ אלא אם $\mathcal{Z}(A_i) = \mathcal{Z}(A)$ לאיזשהו i; אלא שאז

$$A = \sqrt{A} = \mathcal{I}(\mathcal{Z}(A)) = \mathcal{I}(\mathcal{Z}(A_i)) = \sqrt{A_i} \supseteq A_i \supset A,$$

וזו סתירה.
□

לסיכום, יש התאמות כדלהלן, שמהן הראשונה משרה את האחרות:

אידיאלים רדיקליים	$\Longleftrightarrow$	קבוצות אלגבריות
אידיאלים ראשוניים	$\Longleftrightarrow$	קבוצות אי־פריקות
אידיאלים מקסימליים	$\Longleftrightarrow$	נקודות

התאמה זו מתרגמת איחוד וחיתוך של קבוצות אלגבריות לחיתוך וסכום של אידיאלי היחסים.

תרגיל 4.3.6 הוכח את הגרסה החזקה של טענה 4.3.2.(2): $\bigcap \mathcal{Z}(A_i) = \mathcal{Z}(\sum A_i)$ לכל משפחה של אידיאלים A_i.

תרגיל 4.3.7 (דוגמא נגדית לכיוון $\Longrightarrow$ של טענה 4.3.5 מעל שדה שאינו סגור אלגברית) נניח ש־$F = \mathbb{R}$. הראה ש־$A = \langle \lambda_1(\lambda_2^2 + 1)\rangle$ הוא אידיאל רדיקלי שאינו ראשוני, אבל $\mathcal{Z}(A)$ אי־פריקה.

4.4 טופולוגיות זריצקי

4.4.1 הטופולוגיה על המרחב האפיני

יהי F שדה סגור אלגברית. **טופולוגיית זריצקי** על המרחב F^n מוגדרת כך שהקבוצות הסגורות הן הקבוצות מהצורה $\mathcal{Z}(A)$ (עבור $A \triangleleft F[\lambda_1, \ldots, \lambda_n]$).

טענה 4.4.1 טופולוגיית זריצקי היא אכן טופולוגיה.

הוכחה. **יש להוכיח שהקבוצה הריקה $\mathcal{Z}(\langle 1 \rangle) = \varnothing$ והמרחב כולו $F^n = \mathcal{Z}(0)$ סגורים, ושאיחוד של שתי קבוצות סגורות או חיתוך כלשהו של קבוצות כאלה, הם קבוצות סגורות. עובדות אלו נובעות מטענה 4.3.2 ותרגיל 4.3.6.** □

תרגיל 4.4.2 טופולוגיית זריצקי של F (כלומר, המקרה החד־ממדי) היא הטופולוגיה הקו־סופית.

תרגיל 4.4.3 טופולוגיית זריצקי על F^n היא הטופולוגיה הקטנה ביותר שעבורה כל הפונקציות הפולינומיות $f\colon F^n \to F$ רציפות, כאשר F מצויידת בטופולוגיה הקו־סופית.

תרגיל 4.4.4 המרחב F^n קומפקטי ביחס טופולוגיית זריצקי (ומכאן שכל תת־קבוצה סגורה היא קומפקטית). **הדרכה.** כל אידיאל של $F[\lambda_1, \ldots, \lambda_n]$ נוצר סופית.

תרגיל 4.4.5 הראה שכל קבוצה פתוחה לא ריקה בטופולוגיית זריצקי היא צפופה. **הדרכה.** אם $\mathcal{Z}(A)^{\mathrm{c}} \subseteq \mathcal{Z}(B)$ אז $\mathcal{Z}(0) = F^n = \mathcal{Z}(A) \cup \mathcal{Z}(B) = \mathcal{Z}(A \cap B)$ ולכן $AB \subseteq A \cap B = 0$, אבל אם $\mathcal{Z}(A)^{\mathrm{c}} \neq \varnothing$ הרי ש־$A \neq 0$ ולכן $B = 0$ ו־$\mathcal{Z}(B) = F^n$.

הגדרה 4.4.6 ***מרחב טופולוגי מקיים את תכונת ההפרדה T_0 אם אפשר להפריד אחת מכל שתי נקודות מן השניה על־ידי קבוצה פתוחה; את תכונת ההפרדה T_1 אם אפשר להפריד כל שתי נקודות על־ידי קבוצות פתוחות; ואת תכונת ההפרדה T_2 אם אפשר להפריד כל שתי נקודות על־ידי קבוצות פתוחות וזרות.***

התכונה T_2 נקראת **תכונת האוסדורף**. התכונה T_1 שקולה לכך שכל נקודה היא סגורה.

תרגיל 4.4.7 טופולוגיית זריצקי של המרחב האפיני מקיימת את אקסיומת ההפרדה T_1, אבל לא את אקסיומת ההפרדה T_2.

4.4.2 הספקטרום

יהי R חוג קומוטטיבי. **הספקטרום** של R הוא האוסף $\operatorname{spec}(R)$ של אידיאלים ראשוניים של R.

הגדרה 4.4.8 *לכל אידיאל $I \triangleleft R$, נסמן* $\mathcal{V}(I) = \{P \in \operatorname{spec}(R) : I \subseteq P\}$.

אפשר לראות באברי החוג פונקציות מן הספקטרום אל איחוד חוגי המנה הראשוניים של R, המוגדרות לפי $a(P) = a + P \in R/P$, ואז

$$\mathcal{V}(I) = \{P \in \operatorname{spec}(R) : (\forall a \in I)\ a(P) = 0\},$$

בדומה להגדרה של קבוצת האפסים $\mathcal{Z}(I)$.

תרגיל 4.4.9 $\mathcal{V}(I)=\mathcal{V}(\sqrt{I})$.

תרגיל 4.4.10 הקבוצות $\mathcal{V}(I)$ $(I\triangleleft R)$ מהוות אוסף הקבוצות הסגורות בטופולוגיה על $\operatorname{spec}(R)$. **הדרכה.**

1. $\mathcal{V}(0)=\operatorname{spec}(R)$;
2. $\mathcal{V}(R)=\varnothing$;
3. $\bigcap\mathcal{V}(I_i)=\mathcal{V}(\sum I_i)$;
4. $\mathcal{V}(I_1)\cup\mathcal{V}(I_2)=\mathcal{V}(I_1I_2)$.

הטופולוגיה המוגדרת באופן הזה נקראת **טופולוגיית זריצקי של הספקטרום** (בניגוד לטופולוגיית זריצקי של המרחב האפיני, מתת־הסעיף הקודם)

תרגיל 4.4.11 לכל אידיאל $I\triangleleft R$, $\operatorname{spec}(R/I)$ הומיאומורפי ל־$\mathcal{V}(I)$.

תרגיל 4.4.12 הקבוצות הפתוחות $S_a=\{P\in\operatorname{spec}(R):\ a\notin P\}$ מהוות בסיס לטופולוגיה על $\operatorname{spec}(R)$.

תרגיל 4.4.13 אם $\mathcal{V}(A)=\varnothing$ אז $A=R$.

טענה 4.4.14 הספקטרום קומפקטי תחת טופולוגיית זריצקי.

הוכחה. $\operatorname{spec}(R)=\cup\mathcal{V}(A_\alpha)^c$ **אם ורק אם** $\varnothing=(\cup\mathcal{V}(A_\alpha)^c)^c=\cap\mathcal{V}(A_\alpha)=\mathcal{V}(\sum A_\alpha)$, **אם ורק אם** $R=\sum A_\alpha$. **אבל אם** $1\in\sum A_\alpha$ **אז יש סכום סופי המכיל את** 1. □

תרגיל 4.4.15 טופולוגיית זריצקי של הספקטרום מקיימת את אקסיומת ההפרדה T_0.

תרגיל 4.4.16 $\operatorname{spec}(R_1\times R_2)=\operatorname{spec}(R_1)\cup\operatorname{spec}(R_2)$.

תרגיל 4.4.17 הספקטרום הוא מרחב קשיר אם ורק אם אין ב־R אידמפוטנטים.

הנקודה $\{P\}$ סגורה בספקטרום אם ורק אם P אידיאל מקסימלי. אוסף הנקודות הסגורות, עם הטופולוגיה המושרית מן הספקטרום, נקרא **הספקטרום המקסימלי** של R, ומסמנים אותו ב־$\operatorname{mspec}R$.

תרגיל 4.4.18 $\operatorname{mspec}\mathbb{Z}$ הוא המרחב של הראשוניים עם הטופולוגיה הקו־סופית.

הקשר בין שתי הטופולוגיות שהגדרנו מוסבר על־ידי הטענה הבאה.

טענה 4.4.19 המרחב האפיני F^n הומיאומורפי לספקטרום המקסימלי של $R=F[\lambda_1,\dots,\lambda_n]$.

הוכחה. **נגדיר** $\varphi\colon F^n\to\operatorname{spec}R$ **לפי** $\varphi(s)=P_s$. **לפי טענה 4.2.46, תמונת** φ **היא הספקטרום המקסימלי. לכל אידיאל רדיקלי** A,

$$\varphi(\mathcal{Z}(A))=\{P_s:\ s\in\mathcal{Z}(A)\}=\{P_s:\ \mathcal{I}(\mathcal{Z}(A))\subseteq\mathcal{I}(\{s\})\}=\{P_s:\ A\subseteq P_s\},$$

כלומר, φ **מעתיקה את הקבוצות הסגורות במרחב האפיני אל הקבוצות** $\mathcal{V}(A)\cap\operatorname{mspec}R$, **שהן הקבוצות הסגורות בספקטרום המקסימלי. לכן זהו הומיאומורפיזם.** □

הרעיון היסודי בטענה 4.4.19 הוא שאפשר לזהות את המרחב האפיני עם הספקטרום המקסימלי של מרחב הפונקציות המוגדרות עליו. למרות שטענה זו, בניסוח המוצג לעיל, נכונה רק עבור המרחב האפיני וכאשר השדה סגור אלגברית, אפשר להשתמש בה כמודל עבור יריעות אלגבריות כלליות.

תרגיל 4.4.20 יהי K מרחב האוסדורף קומפקטי. נסמן ב־$C(K)$ את חוג הפונקציות הרציפות $K \to \mathbb{C}$. הראה ש־$M_x \mapsfrom x$ הוא הומיאומורפיזם $K \to \mathrm{mspec} C(K)$, כאשר $M_x = \{f : f(x) = 0\}$.

תרגיל 4.4.21 יהי $f : R \to S$ הומומורפיזם של חוגים. אז $f^* : \mathrm{spec} S \to \mathrm{spec} R$ המוגדר לפי $Q \mapsto f^{-1}(Q)$ הוא הומיאומורפיזם.

תרגיל זה הופך את הספקטרום לפונקטור קונטרווריאנטי מקטגוריית החוגים הקומוטטיביים אל הקטגוריה של מרחבים טופולוגיים.

פרק 5

ממד קרול של חוגים

הממד של יריעה תלת־ממדית אי־פריקה הוא 3, משום שהיא מכילה יריעות דו־ממדיות, המכילות עקומים המכילים נקודות. ההתאמה בין יריעות אי־פריקות לאידיאלים ארשוניים מאפשרת להגדיר את ה'ממד' של אידיאל ראשוני לפי שרשראות יורדות של אידיאלים שיורדים ממנו. האידיאל $I = \langle \lambda_1 - a_1, \dots, \lambda_t - a_t \rangle$ של חוג הפולינומים $F[\lambda_1, \dots, \lambda_n]$ מתאים לקבוצה $\mathcal{Z}(I)$, שהיא הזזה של מרחב וקטורי ממימד $n - t$. באופן כללי יותר, אנו מעוניינים לבנות התאמה בין הממד של קבוצה אלגברית S, לממד של האלגברה האפינית $F[\lambda_1, \dots, \lambda_n]/\mathcal{I}(S)$. רעיון זה מוביל לפיתוח של מושג הממד עבור חוגים כלליים.

5.1 ממד קרול

הגדרה 5.1.1 *יהי R חוג. **ממד קרול של החוג** הוא n המקסימלי כך שקיימת שרשרת של אידיאלים ראשוניים $P_0 \subset P_1 \subset \cdots \subset P_n$ ב־R.*

תרגיל 5.1.2 נניח ש־$P \subset Q$ אידיאלים ראשוניים של R. אפשר לעדן את השרשרת $P \subset Q$ אם ורק אם האידיאל Q/P אינו אידיאל ראשוני מינימלי בחוג המנה R/P.

תרגיל 5.1.3 $\dim(F[\lambda_1, \dots, \lambda_n]) \geq n$ כי $0 \subset \langle \lambda_1 \rangle \subset \cdots \subset \langle \lambda_1, \dots, \lambda_n \rangle$ שרשרת של אידיאלים ראשוניים. ◦

תרגיל 5.1.4 לכל אידיאל $I \triangleleft R$, $\dim(R/I) \leq \dim(R)$. **הדרכה**. כל שרשרת של אידיאלים ראשוניים ב־R/I אפשר להרים לשרשרת ב־R. ◦

תרגיל 5.1.5 אם F שדה אז $\dim(F) = 0$.

תרגיל 5.1.6 $\dim(R) = 0$ אם ורק אם כל אידיאל ראשוני הוא מקסימלי.

תרגיל 5.1.7 אם R תחום שלמות ממימד אפס אז הוא שדה. **הדרכה**. 0 אידיאל ראשוני.

טענה 5.1.8 כל תחום שלמות ארטיני הוא שדה. ◦

הוכחה. יהי R תחום שלמות ארטיני, ויהי $0 \neq a \in R$. אם a אינו הפיך אז $a^n \notin Ra^{n+1}$, ומכאן ש־$Ra^{n+1} \subset Ra^n$, וכך מתקבלת שרשרת $\cdots \subset Ra^3 \subset Ra^2 \subset Ra$, בסתירה לארטיניות. □

טענה 5.1.9 לכל חוג ארטיני (קומוטטיבי) R יש ממד 0. ◦

הוכחה. יהי $P \triangleleft R$ אידיאל ראשוני, אז R/P תחום שלמות ארטיני (תרגיל **1.3.19**), ולפי טענה **5.1.8** הוא שדה, ולכן P מקסימלי. □

5.2 אידיאלים ניליים ונילפוטנטיים

הגדרה 5.2.1 ***איבר $a \in R$ הוא איבר נילפוטנטי אם יש $n \geq 1$ כך ש־$a^n = 0$. אידיאל $I \triangleleft R$ הוא נילי אם כל איבריו נילפוטנטיים. אידיאל הוא נילפוטנטי אם יש n כך ש־$I^n = 0$.***

תרגיל 5.2.2 כל אידיאל נילפוטנטי הוא נילי.

תרגיל 5.2.3 אידיאל נילי ראשי הוא נילפוטנטי.

טענה 5.2.4 יהיו $A \subseteq B$ אידיאלים של חוג R. אם A ו־B/A ניליים (נילפוטנטיים), אז B נילי (נילפוטנטי).

הוכחה. נניח ש־$A, B/A$ ניליים, ויהי $b \in B$. אז קיים n כך ש־$b^n + A = (b + A)^n = 0 + A$, ולכן $b^n \in A$, וקיים m כך ש־$(b^n)^m = 0$. נניח ש־$A, B/A$ נילפוטנטים. אז קיים n כך ש־$(B^n + A)/A = (B/A)^n = 0$, ולכן $B^n \subseteq A$; קיים m כך ש־$A^m = 0$, ואז $B^{nm} \subseteq A^m = 0$. □

תרגיל 5.2.5 אם A, B ניליים (נילפוטנטים) אז $A+B$ נילי (נילפוטנטי). **הדרכה**. טענה 5.2.4. לטענה על נילפוטנטיות אפשר לתת גם הוכחה ישירה: נניח ש־$A^n = 0$ ו־$B^m = 0$, אז $(A+B)^{n+m-1} = 0$ כי אפשר לפרק את החזקה לסכום של מכפלות שבכל אחת מהן יש לפחות $n-1$ הופעות של A, או לפחות $m-1$ הופעות של B.

תרגיל 5.2.6 כל אידיאל נילי נוצר סופית הוא נילפוטנטי. **הדרכה**. תרגיל 5.2.5.

תרגיל 5.2.7 בחוג קומוטטיבי נתרי, כל אידיאל נילי הוא נילפוטנטי. **הדרכה**. תרגיל 5.2.6

תרגיל 5.2.8 סכום של מספר כלשהו של אידיאלים ניליים הוא נילי. **הדרכה**. מספיק להוכיח את הטענה עבור סכום סופי, וזה תרגיל 5.2.5. **הערה**. בתרגיל זה נשבר הדמיון בין אידיאלים ניליים לנילפוטנטים: למרות שסכום של אידיאלים ניליים הוא נילי, סכום של מספר כלשהו של אידיאלים נילפוטנטיים הוא נילי, אבל אינו בהכרח נילפוטנטי. כתוצאה מכך אי אפשר להגדיר את "הרדיקל הנילפוטנטי", אלא בחוגים מיוחדים.

תרגיל 5.2.9 תן דוגמא לחוג (קומוטטיבי) עם אידיאל נילי שאינו נילפוטנטי. **הדרכה**. למשל, קח $I = \langle a_1, a_2, \dots \rangle$ בחוג $R = F[a_1, a_2, \dots]/\sum \langle a_1, \dots, a_n \rangle^n$.

הגדרה 5.2.10 ***סכום האידיאלים הניליים בחוג, שהוא נילי לפי תרגיל 5.2.8, הוא כמובן האידיאל הנילי הגדול ביותר של R. אידיאל זה נקרא הרדיקל הנילי העליון, ומסמנים אותו ב־$\mathrm{Nil}(R)$.***

טענה 5.2.11 כאשר R חוג קומוטטיבי, $\mathrm{Nil}(R) = \sqrt{0}$ (השווה ל־$\mathrm{rad}(R)$ לפי מסקנה 4.2.33).

הוכחה. איבר הוא נילפוטנטי אם ורק אם הוא שייך ל־$\sqrt{0}$, המהווה משום כך אידיאל נילי. □

5.3 חוגים מממד אפס

כבר ראינו שאידיאל רדיקלי הוא תמיד חיתוך של ראשוניים (מסקנה 4.2.32). כדי להוכיח את המשפט המרכזי של הסעיף הזה אנו צריכים להוכיח שבחוג נתרי $\sqrt{0}$ הוא חיתוך מספר סופי של אידיאלים ראשוניים. בהזדמנות זו, נוכיח עוד כמה תוצאות יסוד בעלות אופי דומה על חוגים נתריים.

ראשית, הגדרה: אידיאל נקרא **אי־פריק** אם אי אפשר להציג אותו כחיתוך אמיתי $I = A \cap B$ (אלא אם $A = I$ או $B = I$). כל אידיאל ראשוני הוא אי־פריק, משום שאם $P = A \cap B \supseteq AB$ אז $A \subseteq P$ ובהכרח $A = P$, או $B \subseteq P$ ובהכרח $B = P$.

למה 5.3.1 אם $N \triangleleft R$ רדיקלי ומתקיים $N \subset A, B$ ו־$AB \subseteq N$, אז $\sqrt{A} \cap \sqrt{B} = N$.

הוכחה. לפי תרגיל **4.3.4**, $N \subseteq A \cap B \subseteq \sqrt{N} = N$, ולכן (תרגיל **4.2.8**) $\sqrt{A} \cap \sqrt{B} = \sqrt{A \cap B} = \sqrt{N} = N$. □

מסקנה 5.3.2 אידיאל רדיקלי הוא אי־פריק אם ורק אם הוא ראשוני.

הוכחה. נניח ש־N רדיקלי. אם $N \subseteq A, B$ ו־$AB \subseteq N$ אז $N = \sqrt{A} \cap \sqrt{B}$ לפי למה **5.3.1**, ולכן $N = \sqrt{A} \supseteq A$ או $N = \sqrt{B} \supseteq B$. □

משפט 5.3.3 *יהי R חוג נתרי.*

1. *כל אידיאל הוא חיתוך סופי של אידיאלים אי־פריקים.*
2. *כל אידיאל מכיל מכפלה סופית של ראשוניים.*
3. *כל אידיאל רדיקלי הוא חיתוך סופי של ראשוניים.*
4. *כל אידיאל מוכל במספר סופי של אידיאלים ראשוניים מינימליים (ביחס לכך שהם מכילים אותו).*

הוכחה. **ההוכחה בארבעת המקרים מבוססת על אינדוקציה נתרית.**

1. **יהי N דוגמא נגדית מקסימלית, כלומר אידיאל שאינו חיתוך מספר סופי של אידיאלים אי־פריקים, והוא מקסימלי ככזה. בפרט, N פריק, ואפשר לכתוב אותו כחיתוך $N = A \cap B$ כאשר $N \subset A, B$. לפי המקסימליות כל אחד מן האידיאלים A, B הוא חיתוך סופי של אידיאלים אי־פריקים, ולכן גם N כזה, בסתירה להנחה.**
2. **יהי N דוגמא נגדית מקסימלית, כלומר אידיאל שאינו מכיל מכפלה סופית של ראשוניים, והוא מקסימלי ככזה. בפרט, N אינו ראשוני, והוא מכיל מכפלה AB של אידיאלים $N \subset A, B$. לפי המקסימליות, כל אחד מן האידיאלים A, B מכיל מכפלה סופית של ראשוניים, ו־N מכיל את המכפלה של המכפלות האלה, בסתירה.**
3. **יהי N דוגמא נגדית מקסימלית, כלומר אידיאל רדיקלי שאינו חיתוך מספר סופי של ראשוניים, והוא מקסימלי ככזה. בפרט N אינו ראשוני, והוא מכיל מכפלה AB של אידיאלים $N \subset A, B$. לפי המקסימליות של N, כל אחד מהאידיאלים הרדיקליים $\sqrt{A}, \sqrt{B}$ הוא חיתוך מספר סופי של אידיאלים ראשוניים, ולכן גם $\sqrt{A} \cap \sqrt{B}$, השווה ל־N לפי למה 5.3.1, הוא חיתוך כזה.**

4. יהי N דוגמא נגדית מקסימלית, כלומר אידיאל המוכל באינסוף ראשוניים מינימליים. בפרט N אינו ראשוני, והוא מכיל מכפלה AB של אידיאלים $A, B \supset N$. כל אידיאל ראשוני המכיל את N מכיל את A או את B, ולכן כל אידיאל ראשוני מינימלי ביחס להכלת N הוא ראשוני מינימלי ביחס להכלת A או ביחס להכלת B. אבל לפי המקסימליות יש רק מספר סופי של ראשוניים מינימליים מעל A ומעל B, בסתירה להנחה.

□

הערה 5.3.4 בחוג נתרי קומוטטיבי כל אידיאל אי־פריק הוא פרימרי (=אם $ab \in P$ ו־$a \notin P$ אז יש חזקה $b^n \in P$); ולאידיאל פרימרי יש רדיקל ראשוני. לפי זה, החלק השלישי של המשפט נובע מן הראשון.

לכן כל אידיאל הוא חיתוך מספר סופי של אידיאלים פרימריים. זהו משפט לסקר־נתר, הקובע גם כי בהצגה המינימלית של אידיאל כחיתוך של אידיאלים פרימריים, הרדיקלים של הגורמים בחיתוך יחידים עד־כדי סדר.

טענה 5.3.5 לחוג ארטיני (קומוטטיבי) יש מספר סופי של אידיאלים ראשוניים.

הוכחה. אחרת, יהיו $P_1, P_2, \dots$ אידיאלים ראשוניים שונים בחוג הארטיני R. נסמן $I_n = P_1 \cap \cdots \cap P_n$, אז $I_1 \supseteq I_2 \supseteq I_3 \supseteq \cdots$ היא שרשרת יורדת, המוכרחה לעצור לפי הארטיניות. כלומר, קיים n כך ש־$I_n = I_{n+1}$, היינו $P_1 \cdots P_n \subseteq P_1 \cap \cdots \cap P_n \subseteq P_1 \cap \cdots \cap P_n \cap P_{n+1} \subseteq P_{n+1}$. מכיוון ש־$P_{n+1}$ ראשוני, יש $i \leq n$ כך ש־$P_i \subseteq P_{n+1}$; אבל לפי טענה 5.1.9, P_i מקסימלי, כך ש־$P_i = P_{n+1}$, בסתירה להנחה.

(עובדה זו נכונה גם עבור חוגים ארטיניים לא קומוטטיביים.) □

טענה 5.3.6 יהי R חוג קומוטטיבי ראשוני למחצה. התנאים הבאים שקולים:

1. R נתרי בעל ממד אפס.
2. R ארטיני.
3. R הוא מכפלה ישרה של מספר סופי של שדות.

הוכחה. $(2,1) \Longrightarrow (3)$: אם R נתרי יש בו מספר סופי של ראשוניים שחיתוכם $\sqrt{0}$ (משפט 5.3.3), ואם R ארטיני יש לו מספר סופי של ראשוניים, לפי טענה 5.3.5, וחיתוכם הוא $\sqrt{0}$ לפי מסקנה 4.2.33. בכל מקרה אפשר לכתוב $0 = \sqrt{0} = P_1 \cap \cdots \cap P_t$ כאשר $P_i \triangleleft R$ ראשוניים. הממד של R הוא אפס לפי ההנחה עבור המקרה הנתרי, ולפי טענה 5.1.9 אם R ארטיני; לכן האידיאלים P_i מקסימליים. לפי משפט השאריות הסיני, $R = R/0 = R/(P_1 \cap \cdots \cap P_t) \cong R/P_1 \times \cdots \times R/P_t$, כאשר R/P_i הם שדות.
$(3) \Longrightarrow (2,1)$: החוג ארטיני ונתרי משום שלמכפלה של t שדות יש בדיוק 2^t אידיאלים. □

הערה 5.3.7 כל מכפלה ישרה של שדות היא ראשונית למחצה; זהו תרגיל 4.2.23.

משפט 5.3.8 *יהי R חוג נתרי מממד 0. אז R ארטיני.*

הוכחה. נסמן $N = \sqrt{0}$. זהו אידיאל רדיקלי, ולכן R/N ראשוני למחצה (טענה 4.2.20), נתרי כחוג מנה של R, ובעל ממד אפס (תרגיל 5.1.4). לפי משפט 5.3.6, R/N ארטיני.

לפי טענה 5.2.11 ותרגיל 5.2.7, N אידיאל נילפוטנטי, ולכן קיים n כך ש־$N^n = 0$. בגלל הנתריות, N נוצר סופית כמודול מעל R. מכאן שלכל i, $N^i \triangleleft R$ נוצר סופית כמודול. מכאן שגם המנה N^i/N^{i+1} נוצרת סופית כמודול מעל R, ו־N מאפס אותה. לפי תרגיל 1.1.10, N^i/N^{i+1} מודול נוצר סופית מעל R/N, שהוא ארטיני ונתרי, ולכן גם N^i/N^{i+1} ארטיני ונתרי, כלומר (טענה 1.3.11) בעל סדרת הרכב. כך אפשר לעדן את הסדרה $R > N > \cdots > N^{n-2} > N^{n-1} > 0$ לסדרת הרכב של R (כמודול מעל עצמו), ומכאן ש־R בעל אורך סופי כמודול מעל עצמו. שוב לפי טענה 1.3.11, R ארטיני. □

מסקנה 5.3.9 תהי R אלגברה אפינית. אז R ארטיני אם ורק אם יש לו ממד אפס. במקרה זה, לכל מודול נוצר סופית מעל R יש סדרת הרכב (כי R ארטיני ונתרי).

5.4 גובה של אידיאלים

הגדרה 5.4.1 *יהי R תחום שלמות. אידיאל ראשוני $P \triangleleft R$ נקרא **מינימלי** אם הוא אינו מכיל אף אידיאל ראשוני $\neq 0$.*
*יהי $0 \neq I \triangleleft R$. אידיאל ראשוני P המכיל את I הוא **מינימלי מעל** I אם אין ראשוני $P \subset P_0 \subseteq I$. אם $I = Ra$, אומרים ש־P **מינימלי מעל** a.*

תרגיל 5.4.2 בכל חוג, לכל $0 \neq I \triangleleft R$ יש אידיאל ראשוני מינימלי המכיל את I. **הדרכה**. I מוכל באידיאל מקסימלי, שהוא ראשוני, והאידיאלים הראשוניים המכילים את I מקיימים את תנאי המינימום כי החיתוך של שרשרת ראשוניים הוא אידיאל ראשוני.

טענה 5.4.3 בחוג נתרי, מעל כל אידיאל יש מספר סופי של ראשוניים מינימליים.

הוכחה. משפט **5.3.3**(4). □

תרגיל 5.4.4 לכל $k \geq 1$, ראשוני P הוא מינימלי מעל a אם ורק אם הוא מינימלי מעל a^k. ◦

תרגיל 5.4.5 כל אידיאל ראשוני ראשי הוא מינימלי מעל איבר מתאים.

תרגיל 5.4.6 נניח ש־R תחום פריקות יחידה. אידיאל ראשוני הוא מינימלי אם ורק אם הוא ראשי. **הדרכה**. יהי P אידיאל ראשוני מינימלי, ויהי $p \in P$ איבר אי־פריק (תרגיל 2.2.9). אז $0 \neq Rp \subseteq P$, ומכאן ש־$P = Rp$ הוא אידיאל ראשי. בכיוון ההפוך, יהי $P = R\pi$ אידיאל ראשוני ראשי, ונניח ש־$0 \neq Q \subseteq P$; שוב יש ב־Q איבר אי־פריק p; מכיוון ש־$\pi | p$, בהכרח $P = R\pi = Rp \subseteq Q$ ולכן $Q = P$.

תרגיל 5.4.7 (גרסת צעצוע של משפט האידיאל הראשי) בתחום שלמות נתרי, כל אידיאל ראשוני מהצורה Rp הוא מינימלי. **הדרכה**. אחרת יש ראשוני $0 \neq Q \subset Rp$. לכל $b \in Q$ אפשר לכתוב $b = pb'$, ואז $b' \in Q$ כי $p \notin Q$; כלומר, $p|b$. לכן $p^n | b$ לכל n. נתבונן בשרשרת $Rb \subseteq Rp^{-1}b \subseteq Rp^{-2}b \subseteq \cdots$; היא מוכרחה לעצור בגלל הנתריות, אבל אז $p^{-n-1}b \in Rp^{-n}b$ ו־$1 \in Rp$.
הערה. תכונה זו נכונה בכל תחום שלמות אטומי.

תרגיל 5.4.8 יהי R תחום שלמות, ויהיו $N < M$ תת־מודולים חסרי פיתול של R. אז לכל $0 \neq a \in R$, $M/N \cong aM/aN$. **הדרכה**. הגרעין של $\ell_a : M \to Ma/Na$ המוגדר על־ידי $\ell_a(x) = ax$ כולל את האברים x כך ש־$ax \in aN$, ועל־ידי צמצום ב־a נובע שהגרעין הוא N. ◦

משפט 5.4.9 (*משפט האידיאל הראשי, קרול*) *יהי R תחום שלמות נתרי. אם $P \triangleleft R$ ראשוני מינימלי מעל איבר $a \in R$ אז הוא מינימלי.* ◦

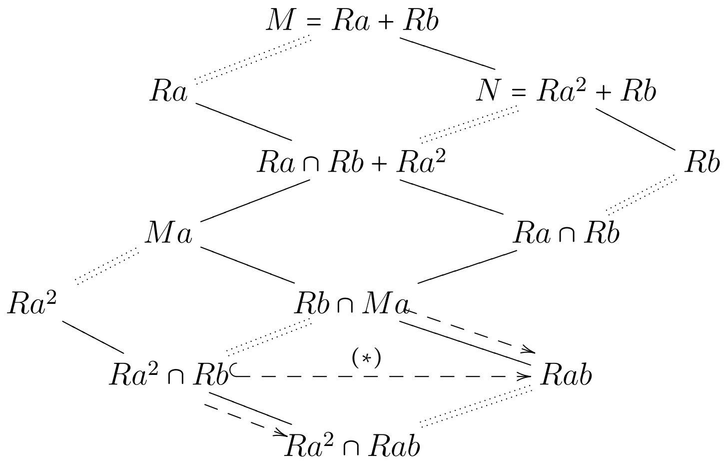
הוכחה. **נניח שלא. אז קיים אידיאל ראשוני $0 \subset P_1 \subset P$. רדוקציה ראשונה. נבצע מיקום ב־P, כלומר, ניקח $S = R - P$, ונעבור לשרשרת $0 \subset P_1' \subset P' \triangleleft R'$, כאשר $P_1' = S^{-1}P_1$, $P' = S^{-1}P$, ו־$R' = S^{-1}R$. האידיאל P' עדיין מינימלי מעל a, משום שכל אידיאל ראשוני של R' מתאים לאידיאל של R שהוא זר ל־S (כלומר מוכל ב־P). אלא שכעת R' מקומי, ו־P' אידיאל מקסימלי יחיד. נחזור לסימון המקורי, תחת הנחות אלו.**

נתבונן בחוג המנה R/Ra^2, שהוא נתרי. כל אידיאל ראשוני ב־R/Ra^2 הוא מהצורה $\tilde{P}/Ra^2$ כאשר $\tilde{P} \triangleleft R$ ראשוני המכיל את a^2, ולכן גם את a. בנוסף, $\tilde{P} \subseteq P$ מכיוון ש־P מקסימלי יחיד. לא יתכן ש־$\tilde{P} \subset P$, כי P מינימלי מעל a, ומכאן ש־$\tilde{P} = P$. הראינו שאין ב־R/Ra^2 אידיאלים ראשוניים פרט ל־P/Ra^2, ולכן $\dim(R/Ra^2) = 0$. לפי משפט 5.3.8, R/Ra^2 ארטיני.

יהי $0 \neq b \in P_1$ איבר כלשהו. **רדוקציה שניה.** נסמן $A_i = \{x \in R \colon xa^i \in Rb\}$; זהו אידיאל של R, ו־$A_1 \subseteq A_2 \subseteq \cdots$. מכיוון ש־$R$ נתרי, השרשרת נעצרת ויש j כך ש־$A_j = A_{j+1} = \cdots$. נסמן $a' = a^j$, ונבחין שאם $xa'^2 = xa^{2j} \in Rb$ אז $x \in A_{2j} = A_j$ ולכן $xa' = xa^j \in Rb$. לפי תרגיל 5.4.4, P מינימלי מעל a', ולכן אפשר להחליף a ב־a' ולקבל את התנאי

$$(*) \qquad xa^2 \in Rb \implies xa \in Rb.$$

פירושו של התנאי הזה הוא שאם $xa^2 \in Rb$ אז $xa^2 \in Rab$, כלומר $Ra^2 \cap Rb \subseteq Rab$, ולכן $Rb \cap Ma = Rb \cap (Ra^2 + Rab) = (Rb \cap Ra^2) + Rab = Rab$, כאשר $M = Ra + Rb$.



איור 5.1: תת־מודולים של R, א־פריורי. החצים המקווקווים מתארים את התנאי $(*)$.

נסמן $N = Rb + Ma = Ra^2 + Rb$. לפי תרגיל 5.4.8 (פעמיים),

$$Ra/Ra^2 \cong R/Ra \cong Rb/Rab = Rb/(Rb \cap Ma) \cong (Rb + Ma)/Ma = N/Ma,$$

וגם $Ma/Ra^2 \cong M/Ra$. כעת, M/Ra^2 הוא מודול מעל R/Ra^2, שהוא ארטיני ונתרי, ולכן יש ל־M/Ra^2 סדרות הרכב. לפי תרגיל 1.2.11,

$$\ell(M/Ra) + \ell(Ra/Ra^2) = \ell(M/Ra^2) = \ell(M/N) + \ell(N/Ma) + \ell(Ma/Ra^2),$$

ומאחר שהוכחנו $\ell(M/Ra) = \ell(aM/Ra^2)$ ו־$\ell(N/Ma) = \ell(Ra/Ra^2)$ נובע ש־$\ell(M/N) = 0$, ובהכרח $M = N$. אם כך, $a \in M = N = Ra^2 + Rb$, ואפשר לכתוב $a = xa^2 + yb$; אבל R מקומי, ולכן $(1 - xa)$ הפיך ואפשר לכתוב $a = (1 - xa)^{-1}yb \in Rb \subseteq P_1$, בסתירה למינימליות של P. □

הערה. למשפט חשוב זה יש גרסה לא קומוטטיבית. ראה למשל Dimensions of Ring Theory, Nastasesecu and van Oyestaeyen, Sec. 6.6.

הגדרה 5.4.10 *הגובה של אידיאל ראשוני P הוא t המקסימלי כך שקיימת שרשרת*

$$P_0 \subset \cdots \subset P_{t-1} \subset P_t = P$$

של אידיאלים ראשוניים. את הגובה מסמנים ב־$\mathrm{ht}(P) = t$.

אפשר לנסח מחדש את משפט האידיאל הראשי:

מסקנה 5.4.11 יהי R קומוטטיבי נתרי. לכל אידיאל ראשוני P שהוא מינימלי מעל איבר $a \neq 0$, מתקיים $\mathrm{ht}(P) \leq 1$.

תרגיל 5.4.12 הממד $\dim(R)$ שווה לסופרימום הגבהים של האידיאלים המקסימליים. ◦
הדרכה. כל שרשרת של אידיאלים ראשוניים אפשר להמשיך כך שהיא מסתיימת באידיאל מקסימלי.

למה 5.4.13 יהי R חוג נתרי קומוטטיבי. תהי $P_t \subset P_{t-1} \subset \cdots \subset P_1 \subset P_0 = P$ שרשרת של אידיאלים ראשוניים, ויהי $b \in P$. אז יש שרשרת $P'_t \subset P'_{t-1} \subset \cdots \subset P'_1 \subset P_0 = P$, כך ש־$b \in P'_{t-1}$. ◦

הוכחה. באינדוקציה. נניח ש־$b \in P_k$, כאשר $k \leq t-2$, ונתבונן ב־$P_{k+2} \subset P_{k+1} \subset P_k$. נעבור לחוג המנה R/P_{k+2}, שם $0 \subset P_{k+1}/P_{k+2} \subset P_k/P_{k+2}$. מכיוון ש־$P_k/P_{k+2}$ אינו ראשוני מינימלי, לפי משפט האידיאל הראשי הוא אינו ראשוני מינימלי מעל $b + P_{k+2}$, ולכן קיים אידיאל ראשוני $P_{k+2} \subset P'_{k+1} \subset P_k$ כך ש־$b \in P'_{k+1}$. □

את מושג המינימליות מעל איבר אפשר לנסח גם כמינימליות מעל האידיאל שאותו איבר יוצר. משפט האידיאל הראשי המוכלל עוסק במינימליות מעל כל אידיאל נוצר סופית.

משפט 5.4.14 (*משפט האידיאל הראשי המוכלל*) *יהי R קומוטטיבי נתרי. אם ראשוני P הוא מינימלי מעל $B = Ra_1 + \cdots + Ra_t$, אז* $\mathrm{ht}(P) \leq t$. ◦

הוכחה. באינדוקציה על t, כאשר המקרה $t = 1$ הוא משפט האידיאל הראשי, 5.4.9. נניח שקיימת שרשרת ראשוניים $P_{t+1} \subset P_t \subset \cdots \subset P_1 \subset P_0 = P$. לפי למה 5.4.13 אפשר להניח ש־$a_t \in P_t$. נעבור לחוג המנה $\bar{R} = R/Ra_t$, שבו $\bar{P} = P/Ra_t$ מינימלי מעל $\bar{B} = B/Ra_t = Ra_1 + \cdots + Ra_{t-1}$. לפי הנחת האינדוקציה $\mathrm{ht}(\bar{P}) \leq t-1$, אבל $P_t/Ra_t \subset \cdots \subset P_1/Ra_t \subset P/Ra_t$ היא שרשרת של ראשוניים מאורך t, וזו סתירה. □

מסקנה 5.4.15 בחוג קומוטטיבי נתרי, אם $P = Ra_1 + \cdots + Ra_t$ הוא ראשוני, אז $\mathrm{ht}(P) \leq t$.

מסקנה 5.4.16 הגובה של כל אידיאל ראשוני P בחוג קומוטטיבי נתרי הוא סופי. ◦

הוכחה. מכיוון שהחוג נתרי אפשר לכתוב $P = Ra_1 + \cdots + Ra_t$, ומכיוון ש־P מינימלי מעל עצמו, $\mathrm{ht}(P) \leq t$. □

מסקנה 5.4.17 בחוג נתרי קומוטטיבי אין שרשרת יורדת אינסופית של אידיאלים ראשוניים.
הדרכה. מסקנה 5.4.16.

מסקנה 5.4.18 יהי R חוג נתרי מקומי, אז יש לו ממד סופי.

הוכחה. ממד החוג שווה לגובה של האידיאל המקסימלי שלו. □

מסקנה 5.4.19 אידיאל מגובה t אי אפשר ליצור בפחות מ־t איברים.

מסקנה 5.4.20 יהי F שדה סגור אלגברית. אז $\dim(F[\lambda_1,\dots,\lambda_n]) = n$.

הוכחה. לפי טענה 4.2.46, האידיאלים המקסימליים של R נוצרים על־ידי n איברים, וממשפט 5.4.14 נובע שגובהם אינו עולה על n. מאידך בתרגיל 5.1.3 בנינו שרשרת אידיאלים ראשוניים באורך n. המסקנה נובעת לפי תרגיל 5.4.12. □

הערה 5.4.21 מסקנה 5.4.20 נכונה לכל שדה. ראה הוכחה קצרה ב־*A Short Proof for the Krull Dimension of a Polynomial Ring*, Thierry Coquand and Henri Lombardi.

הערה 5.4.22 Nagata מצא ב־1962 חוג נתרי קומוטטיבי ממימד אינסופי: יהי $A = k[x_1,\dots]$; נקבע סדרה עולה $m_1 < m_2 < \cdots$, וניקח $n_i = m_1 + \cdots + m_i$. יהיו $P_i = \langle x_{n_i},\dots,x_{n_{i+1}-1}\rangle$. ניקח $S = (\bigcup P_i)^c$. אז $S^{-1}A$ נתרי ממימד אינסופי.

הערה 5.4.23 הממד של החוג אינו חוסם את מספר היוצרים של אידיאל לא ראשוני. למשל, הראה שאת האידיאל $I = \langle\lambda_1^n,\lambda_1^{n-1}\lambda_2,\dots,\lambda_2^n\rangle \triangleleft F[\lambda_1,\lambda_2]$ אי אפשר ליצור בפחות מ־$n+1$ איברים. מהו $\sqrt{I}$? מצא אידיאל ראשוני מינימלי מעל I.

את מושג המינימליות אפשר לתאר בהקשר רחב יותר. נאמר שאידיאלים ראשוניים $P \subset Q$ הם **שכנים** אם אין ראשוני $P \subset P' \subset Q$. (כך, ראשוני מינימלי הוא שכן של אפס.)

משפט 5.4.24 *(קפלנסקי) בחוג קומוטטיבי, בין כל שני אידיאלים ראשוניים יש ראשוניים שכנים.*

הוכחה. נתונים $P \subseteq Q$ ראשוניים. לפי עקרון המקסימום של האוסדורף (השקול ללמה של צורן), יש שרשרת מקסימלית של ראשוניים $\{P_\alpha\}$ בין P ל־Q. נקבע $x \in Q - P$. אז $P' = \bigcup_{x\notin P_\alpha} P_\alpha$ ו־$Q' = \bigcap_{x\in P_\alpha} P_\alpha$ הם ראשוניים (משום שחיתוך שרשרת של ראשוניים הוא תמיד ראשוני, ואיחוד שרשרת של ראשוניים הוא ראשוני בחוג קומוטטיבי). בנוסף $P' \subset Q'$, ולו היה ראשוני ביניהם, אפשר היה לעדן בעזרתו את השרשרת. □

5.5 אידיאלים ראשוניים בהרחבות

תהי $C \subseteq R$ הרחבה של חוגים. אומרים שראשוני $Q \triangleleft R$ **נמצא מעל** $P \triangleleft C$ אם $P = Q \cap C$. בטענה 3.4.17 הראינו שבמקרה זה גם P ראשוני.

הגדרה 5.5.1 *ההרחבה $C \subseteq R$ מקיימת את התכונה LO (Lying Over) אם לכל אידיאל ראשוני $P \triangleleft C$ יש ראשוני $Q \triangleleft R$ הנמצא מעליו.*
ההרחבה מקיימת את התכונה GU (Going Up) אם לכל ראשוני Q מעל P ולכל $P \subset P_1$ יש Q_1 מעל P_1 המכיל את Q.
ההרחבה מקיימת את התכונה INC (Incomparable) אם אין $Q \subset Q_1$ הנמצאים שניהם מעל אותו ראשוני P.

5.5.1 ראשוניים בהרחבות וממד קרול

טענה 5.5.2 אם $R \subseteq C$ קומוטטיביים וההרחבה מקיימת INC, אז $\mathrm{ht}(Q) \leq \mathrm{ht}(P)$ לכל Q שמעל P.

הוכחה. נניח שיש שרשרת ראשוניים $Q = Q_0 \supset Q_1 \supset \cdots \supset Q_t$. נחתוך עם C ונקבל שרשרת ראשוניים $P = P_0 \supseteq P_1 \supseteq \cdots \supseteq P_t$ כאשר $P_i = Q_i \cap C$, אבל כל ההכלות אמיתיות לפי INC, ולכן $\mathrm{ht}(P) \geq t$. □

טענה 5.5.3 בהרחבה $R \subseteq C$ המקיימת LO ו־GU, לכל $P \triangleleft C$ יש Q מעליו כך ש־$\mathrm{ht}(P) \leq \mathrm{ht}(Q)$.

הוכחה. נתונה שרשרת של ראשוניים $P = P_0 \supset P_1 \supset \cdots \supset P_t$. יש ראשוני $Q_t \triangleleft R$ הנמצא מעל P_t לפי LO, ולכל $i = t-1, \ldots, 1, 0$ יש ראשוני Q_i מעל P_i המכיל את Q_{i+1} לפי GU. □

טענה 5.5.4 אם ההרחבה $R \subseteq C$ מקיימת GU, LO ו־INC אז לכל $P \triangleleft C$ יש Q מעליו כך ש־$\mathrm{ht}(Q) = \mathrm{ht}(P)$.

הוכחה. טענות 5.5.2 ו־5.5.3. □

טענה 5.5.5 אם ההרחבה $R \subseteq C$ מקיימת GU, LO ו־INC אז $\dim(C) = \dim(R)$.

הוכחה. $\dim(R) = \sup \mathrm{ht}(Q) \geq \sup \mathrm{ht}(P) = \dim(C)$ לפי טענה 5.5.4, והכיוון ההפוך נובע מטענה 5.5.2. □

הערה 5.5.6 אם $R \subseteq C$ תחומי שלמות, אז מהתכונה GU נובע LO (ראה טענה 5.5.7).

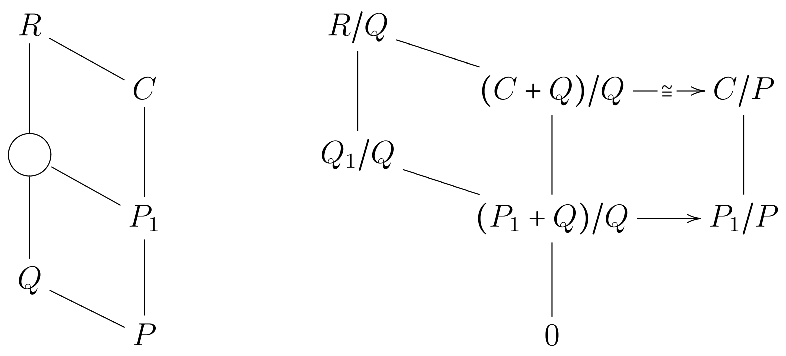
הוכחה. יהי P אידיאל ראשוני של C, אז הוא מכיל את $0 \triangleleft C$ שמעליו נמצא $0 \triangleleft R$. לפי GU יש אידיאל $Q \triangleleft R$ (המכיל את 0) הנמצא מעל P. □

טענה 5.5.7 בכל הרחבה $R \subseteq C$ של חוגים קומוטטיביים, מהתכונה GU נובע LO.

הוכחה. יהי $P \triangleleft C$. נסמן $S = C - P$. ניקח אידיאל מקסימלי ב־$S^{-1}R$, אז הוא מהצורה $S^{-1}Q_0$ עבור אידיאל ראשוני $Q_0 \triangleleft R$ שאינו חותך את S; מכאן ש־$P_0 = Q_0 \cap C \subseteq P$. לפי GU, יש אידיאל ראשוני $Q_0 \subseteq Q$ הנמצא מעל P. □

הערה 5.5.8 יהי $S \subseteq R$ מונויד, $P \triangleleft R$ אידיאל שאינו נחתך עם S. אז $\mathrm{ht}(S^{-1}P) = \mathrm{ht}(P)$.

הוכחה. יש התאמה שומרת סדר בין האידיאלים הראשוניים של $S^{-1}R$ לאידיאלים הראשוניים של R שאינם חותכים את S. □



איור 5.2: הוכחת GU בהרחבה שלמה.

5.5.2 שרשראות של ראשוניים בהרחבות שלמות

הערה 5.5.9 כל הרחבה שלמה $C \subseteq R$ מקיימת את התכונה LO (משפט 3.4.28).

טענה 5.5.10 כל הרחבה שלמה $C \subseteq R$ מקיימת את התכונה GU.

הוכחה. (ראה איור 5.2). יהי Q ראשוני מעל P, ויהי $P \subseteq P_1$. לפי תרגיל 3.4.18, $\bar{R} = R/Q$ הרחבה שלמה של $\bar{C} = (C+Q)/Q \cong C/P$, ולפי LO בהרחבה זו, יש ראשוני $Q' \triangleleft R/Q$ שנמצא מעל $P_1' = (P_1+Q)/Q$; נכתוב $Q' = Q_1/Q$, כאשר Q_1 ראשוני המכיל את Q; מן העובדה ש־Q_1' מעל P_1' נובע ש־

$$(P_1+Q)/Q = Q' \cap \bar{C} = Q_1/Q \cap (C+Q)/Q = (Q_1 \cap (C+Q))/Q = ((Q_1 \cap C)+Q)/Q,$$

ולכן $Q + P_1 = Q_1 \cap C + Q$. אבל

$$P_1 = P + P_1 = (C \cap Q) + P_1 = C \cap (Q + P_1) = C \cap (Q_1 \cap (C+Q)) = C \cap Q_1.$$

□

הערה 5.5.11 כל הרחבה שלמה $C \subseteq R$ מקיימת את התכונה INC.

הוכחה. אחרת יש אידיאלים ראשוניים $Q \subset Q'$ של R הנמצאים מעל $P \triangleleft C$. לפי תרגיל 3.4.18, R/Q שלם (ובפרט אלגברי) מעל $(C+Q)/Q \cong C/P$, ולפי טענה 3.3.3, $0 \neq Q'/Q \triangleleft R/Q$ נחתך עם $(C+Q)/Q$, בסתירה להנחה ש־$Q' \cap C = P$. □

מסקנה 5.5.12 אם $C \subseteq R$ הרחבה שלמה אז $\dim(R) = \dim(C)$.

מסקנה 5.5.13 יהי R תחום שלמות אפיני מעל F. אז $\dim(R) = \mathrm{trdeg}_F(R)$.

הוכחה. לפי משפט הנורמליזציה של נתר, משפט 3.5.2, יש תת־חוג $R_0 \subseteq R$ ש־R שלם מעליו, וכך ש־$R_0 \cong F[\lambda_1, \dots, \lambda_t]$ כאשר $t = \mathrm{trdeg}(R)$. לפי טענה 5.4.20, $\dim(R) = \dim(R_0) = \mathrm{trdeg}_F(R)$, כשהשוויון האחרון הוא מסקנה 5.4.20. □

כלומר, ממד קרול שווה לדרגת הטרנסצנדנטיות!

5.5.3 תחומי שלמות נורמליים

הגדרה 5.5.14 *תחום שלמות C הוא* ***נורמלי*** *אם הוא שווה לסגור השלם של עצמו בשדה השברים.*

הערה 5.5.15 כל תחום פריקות יחידה הוא נורמלי. בפרט, חוג פולינומים הוא נורמלי.

טענה 5.5.16 תהי $C \subseteq R$ הרחבה שלמה של תחומי שלמות, כאשר C נורמלי. אז הפולינום מן המעלה המינימלית של $a \in R$ מעל C מתחלק (מעל C) במקדם העליון שלו.

הוכחה. נסמן ב־f את הפולינום הנתון. יהיו F שדה השברים של C, K שדה השברים של R, ו־E שדה פיצול של f, מעל K. אפשר לכתוב $f(\lambda) = \alpha \prod(\lambda - a_i)$ כאשר $\alpha \in C$ ו־a_i מאפסים אותו פולינום מוני מעל C שאותו מאפס a, ולכן כולם שלמים אלגבריים. מכאן שגם מקדמי $\frac{1}{\alpha}f$, השייכים ל־F, הם שלמים אלגבריים, ולפי ההנחה הם שייכים ל־C. □

למה 5.5.17 (הלמה של גאוס עבור תחומים נורמליים) יהי C תחום שלמות נורמלי ו־F שדה השברים שלו. אם $f, g \in C[\lambda]$ מתוקנים ו־$f \,|\, g$ מעל F, אז $f \,|\, g$ מעל C.

הוכחה. נניח ש־$g = fh$ עבור $h \in F[\lambda]$, ונכתוב $h = a^{-1}h_0$ כאשר $c \in C$ ו־$h_0 \in C[\lambda]$; כך $cg = fh_0$. נפרק $g(\lambda) = \prod(\lambda - a_i)$ כאשר a_i הם השורשים בשדה פיצול מעל F. מכיוון ש־h_0 מחלק את g שם, אפשר לכתוב $h_0 = c'h_0'$ כאשר h_0' מכפלה של גורמים מהצורה $\lambda - a_i$, ומקדמיו הם שלמים אלגבריים השייכים ל־F, ולכן שייכים ל־C. לכן $g = fh_0'$. □

תרגיל 5.5.18 תן דוגמא נגדית לטענה 5.5.16 כאשר R אינו תחום שלמות, כדלקמן. מצא הרחבה שלמה $C \subseteq R$ של חוגים קומוטטיביים, שבה C תחום שלמות נורמלי, עם איבר $a \in R$ המאפס פולינום ממעלה ראשונה, אבל אינו מאפס אף פולינום מוני ממעלה זו. **הדרכה.** למשל $C = \mathbb{Z}$ עם $R = \mathbb{Z}[a \,|\, a^2 = 0, 2a = 0]$.

הגדרה 5.5.19 *הרחבה $C \subseteq R$ מקיימת את התכונה* GD (Going Down) *אם לכל ראשוני Q_1 מעל P_1 ולכל $P \subseteq P_1$ יש Q מעל P המוכל ב־Q_1.*

משפט 5.5.20 *נניח ש־C תחום שלמות נורמלי. כל R שלם מעל C מקיים* GD.

הוכחה. ניקח $S' = C - P$, $S_1 = R - Q_1$ ו־$S = S'S_1$. מספיק להראות ש־$S \cap PR = \emptyset$, משום שאז, אם $PR \subseteq Q \triangleleft R$ הוא מקסימלי ביחס לכך שהוא זר ל־S, אז Q ראשוני לפי תרגיל 3.4.27, ו־$Q \cap C = P$.

נניח, בשלילה, ש־$s = cr \in PR$ עבור $c \in S'$ ו־$r \in S_1$. יש פולינום מתוקן $f(\lambda) = \lambda^n + \sum d_i\lambda^i \in C[\lambda]$, בעל מעלה מינימלית, המאפס את s. מאידך אם נכתוב $s = \sum_{j=1}^{\ell} p_jr_j$ עבור $p_j \in P$ ו־$r_j \in R$, נוכל לבחור $M = C[r_1, \dots, r_\ell]$, ואז $sM \subseteq \sum p_jr_jM \subseteq \sum p_jM \subseteq PM$. מכאן נובע, לפי הערה 3.4.3, שיש פולינום מתוקן $g(\lambda) = \lambda^m + \sum c_i\lambda^i$ המאפס את s, כך ש־$c_0, \dots, c_{m-1} \in P$. מכיוון ש־$f \,|\, g$ מעל שדה השברים F, זה נכון גם ב־$C[\lambda]$ לפי למה 5.5.17, ולכן גם בחוג המנה C/P, שם $\bar{f} \,|\, \bar{g} = \lambda^m$, כלומר $\bar{f} = \lambda^n$. לפיכך, $d_i \in P$.

כעת, מעלות הפולינומים המינימליים של s, r מעל F שוות, ולפי טענה 5.5.16, r מאפס פולינום מתוקן $h(\lambda) = \lambda^n + \sum_i d_i'\lambda^i \in C[\lambda]$. אבל אז $0 = f(s) = f(cr) = c^nr^n + \sum d_ic^ir^i$, ולכן r שורש של $c^n\lambda^n + \sum d_ic^i\lambda^i$, וגם של $c^nh(\lambda)$. על־ידי השוואת מקדמים, מקבלים ש־$c^{n-i}d_i' = d_i \in P$ לכל $i < n$. אבל $c \notin P$, ולכן $d_i' \in P$, ומכאן ש־$r^n = -\sum d_i'r^i \in PR \subseteq Q_1$, בסתירה להנחה. □

5.5.4 קטנריות

שרשרת של אידיאלים ראשוניים נקראת **רוויה** אם אי־אפשר לעדן אותה.

משפט 5.5.21 (*קטנריות*) *יהי R תחום שלמות אפיני. אז לכל שתי שרשראות רוויות שקצותיהן $P' \subset P$ יש אותו אורך. בפרט, לכל שרשרת רוויה מ־0 ל־P יש אורך $\mathrm{ht}(P)$, ולכל האידיאלים המקסימליים אותו גובה.*

הוכחה. על־ידי מעבר לחוג המנה אפשר להניח ש־$P' = 0$. לפי משפט הנורמליזציה של נתר, R הרחבה שלמה של חוג פולינומים R_0, שהוא נורמלי, ולכן ההרחבה מקיימת GD; יחד עם GU ו־INC, נובע שיש התאמה בין שרשראות רוויות ב־R לשרשראות רוויות ב־R_0. כאן אפשר להוכיח את הטענה באינדוקציה, בעזרת תרגיל 2.2.9. □

משפט 5.5.22 *לכל ראשוני $P \triangleleft R$ מתקיים* $\dim(R) = \dim(R/P) + \mathrm{ht}(P)$.

הוכחה. בחר אידיאל מקסימלי $P \subseteq M$, עדן את השרשרת $0 \subset P \subset M$ עד לרוויה, והפעל את משפט 5.5.21. □

מסקנה 5.5.23 תהי R אלגברה אפינית. אז $\dim(R[\lambda]) = \dim(R) + 1$.

הוכחה. קח $P = \langle \lambda \rangle$ במשפט 5.5.21. □

פרק 6

ערכים מוחלטים והערכות של שדות

הפרק האחרון מספק מבוא לתורת המספרים האלגברית.

6.1 הגדרה ודוגמאות

הגדרה 6.1.1 ***ערך מוחלט על שדה F הוא פונקציה*** $\mathbb{R} \supseteq [0,\infty) \leftarrow F$ ***,*** $a \mapsto |a|$***, המקיימת***

(*1*) $|a| = 0$ ***אם ורק אם*** $a = 0$;

(*2*) $|ab| = |a| \cdot |b|$;

(*3*) ***קיים קבוע*** $C \geq 1$ ***כך ש־*** $|a+b| \leq C \cdot \max\{|a|,|b|\}$.

(התנאי $C \geq 1$ בהגדרה - הכרחי: בחר $a = 1$, $b = 0$.)

תרגיל 6.1.2 תנאי (3) שקול לתנאי

(*3′*) ***קיים קבוע*** $C \geq 1$ ***כך שאם*** $|a| \leq 1$ ***אז*** $|a+1| \leq C$.

הדרכה. בתנאי (3) אפשר לקחת $b = 1$; בתנאי (3′) קח ab^{-1} במקום a.

דוגמא 6.1.3 **הערך המוחלט הטריוויאלי** $|a| = 1$ לכל $a \neq 0$.

תרגיל 6.1.4 בכל ערך מוחלט מתקיים $|1| = 1$; הערך המוחלט של כל שורש יחידה הוא 1 ולכן גם $|a| = |-a|$ לכל a. הראה שכל ערך מוחלט על שדה סופי הוא טריוויאלי.

דוגמא 6.1.5 הערכים המוחלטים הסטנדרטיים על $\mathbb{R}$ ועל $\mathbb{C}$ הם אכן ערכים מוחלטים.

תרגיל 6.1.6 אם ערך מוחלט מקיים $|a+b| \leq 2 \cdot \max\{|a|,|b|\}$, אז $|a_1 + \cdots + a_n| \leq 2n\max\{|a_i|\}$. **הדרכה.** באינדוקציה, $|a_1 + \cdots + a_{2^{m+1}}| \leq 2^{m+1} \cdot \max\{|a_i|\}$; אם $2^m \leq n < 2^{m+1}$ אז $|a_1 + \cdots + a_n| \leq 2^{m+1}\max\{|a_i|\} \leq 2 \cdot n\max\{|a_i|\}$. **הערה.** אם $|a+b| \leq C \cdot \max\{|a|,|b|\}$, אז $|a_1 + \cdots + a_n| \leq C \cdot n^{\frac{\log(C)}{\log(2)}}\max\{|a_i|\}$ לפי אותה הוכחה.

טענה 6.1.7 תנאי (3) עם $C = 2$ שקול לאי־שוויון המשולש

(*3″*) $|a+b| \leq |a| + |b|$.

הוכחה. **אם מתקיים** $|a+b| \le |a| + |b|$ **אז בוודאי** $|a+b| \le 2\max\{|a|,|b|\}$. **נניח ש־**$|a+b| \le 2\max\{|a|,|b|\}$**, אז לפי תרגיל 6.1.6, לכל** n **מתקיים**

$$\begin{aligned} |a+b|^n &= \left|\sum_{k=0}^{n}\binom{n}{k}a^k b^{n-k}\right| \\ &\le 2(n+1)\max\left\{\left|\binom{n}{i}a^i b^{n-i}\right|\right\} \\ &\le 4(n+1)\sum_{k=0}^{n}\binom{n}{k}|a|^k|b|^{n-k} \\ &= 4(n+1)(|a|+|b|)^n, \end{aligned}$$

ולכן $|a+b| \le \sqrt[n]{4(n+1)}(|a|+|b|)$**. התוצאה נובעת ממעבר לגבול** $n\to\infty$. □

6.2 שקילות של ערכים מוחלטים

הגדרה 6.2.1 ***אם*** $|\cdot|$ ***ערך מוחלט, אז לכל*** $p>0$***,*** $|a|' = |a|^\alpha$ ***גם הוא ערך מוחלט, עם הקבוע*** C^α***. ערכים כאלה הם שקולים.***

תרגיל 6.2.2 כל ערך מוחלט שקול לערך מוחלט המקיים את אי־שוויון המשולש.

הגדרה 6.2.3 ***ערך מוחלט מגדיר טופולוגיה שבה הקבוצות*** $B_a(\epsilon) = \{b \in F : |a-b| < \epsilon\}$ ***מהוות בסיס.***

הערה 6.2.4 ערכים מוחלטים שקולים מגדירים את אותה טופולוגיה. (**הדרכה**. אם $|\cdot|' = |\cdot|^\alpha$ אז $B'_a(\epsilon) = B_a(\epsilon^\alpha)$.) לפי תרגיל 6.2.2, זוהי טופולוגיה מטרית.

משפט 6.2.5 ***התכונות הבאות שקולות עבור ערכים מוחלטים לא טריוויאליים*** $|\cdot|, |\cdot|'$:

1. ***הערכים המוחלטים שקולים זה לזה.***
2. ***הערכים משרים את אותה טופולוגיה.***
3. ***אם*** $|a| < 1$ ***אז*** $|a|' < 1$.
4. ***אם*** $|a| \le 1$ ***אז*** $|a|' \le 1$.
5. ***אם*** $|a| < 1$ ***אז*** $|a|' < 1$***, ואם*** $|a| = 1$ ***אז*** $|a|' = 1$.
6. $|a|', |a|$ ***קטנים, שווים או גדולים מ־***1 ***יחד.***

הוכחה. **נסמן ב־**τ **את הטופולוגיה המושרית על־ידי** $|\cdot|$**, וב־**τ' **את זו המושרית על־ידי** $|\cdot|'$. $(1) \Longrightarrow (2)$: **הערה 6.2.4.** $(2) \Longrightarrow (3)$: **נניח ש־**$|a| < 1$**, אז הסדרה** a^n **מתכנסת ל־**0 **לפי** τ**, ולפי ההנחה גם לפי** τ'**. לכן לא יתכן** $|a|' \ge 1$. $(3) \Longrightarrow (5)$: **נבחר** $b \in F$ **כך ש־**$|b| < 1$**, ואז גם** $|b|' < 1$**. נניח ש־**$|a| = 1$**. לכל** n **מתקיים** $|a^n b| < 1$**, ולפי ההנחה גם** $|a^n b|' < 1$**. מכאן ש־**$|a|' < |b|'^{-1/n}$**, ולכן** $|a|' \le 1$**. אותו נימוק תקף גם ל־**a^{-1}**, ולכן** $|a|' = 1$. $(5) \Longrightarrow (4)$: **טריוויאלי.** $(4) \Longrightarrow (3)$: **יש** $c \in F^\times$ **כך ש־**$|c|' < 1$**, ואז לכל** a**, אם** $|a| < 1$ **אז** $|a^n c^{-1}| \le 1$ **עבור** n **גדול מספיק, ולפי ההנחה גם** $|a^n c^{-1}|' \le 1$**, כך ש־**$|a|'^n \le |c|' < 1$**, ואז** $|a|' < 1$. $(5) \Longrightarrow (6)$: **אם** $|a| > 1$ **אז** $|a^{-1}| < 1$ **ו־**$|a^{-1}|' < 1$**, כך ש־**$|a|' > 1$. $(6) \Longrightarrow (1)$: **יהי** $b \in F$ **כך ש־**$|b| > 1$**; אז גם** $|b|' > 1$**, וקיים** $\alpha > 0$ **כך ש־**$|b|' = |b|^\alpha$**. לכל** a **עם** $|a| > 1$**, כתוב** $|a| = |b|^s$ **ו־**$|a|' = |b|'^t$**. לכל** $\frac{m}{n} \in \mathbb{Q}$ **מתקיים** $s < \frac{m}{n}$ **אם ורק אם** $1 < |b|^{m-sn} = |b|^m|a|^{-n} = |a^{-n}b^m|$**, אם ורק אם** $1 < |a^{-n}b^m|' = |b|'^m|a|'^{-n} = |b|'^{m-tn}$**, אם ורק אם** $t < \frac{m}{n}$**. לכן** $s = t$ **ו־**$|a|' = |b|'^s = |b|^{\alpha s} = |a|^\alpha$. □

6.3 ערכים לא ארכימדיים

ערך מוחלט נקרא **לא ארכימדי** אם $|a+b| \leq \max\{|a|,|b|\}$, **וארכימדי** אחרת. ערכים שקולים זה לזה הם ארכימדיים או לא ארכימדיים יחדיו.

תרגיל 6.3.1 אם $|\cdot|$ ערך מוחלט לא ארכימדי אז $|a+b| = |a|$ לכל $|b| < |a|$.

טענה 6.3.2 התנאים הבאים שקולים:

1. $|\cdot|$ לא ארכימדי;
2. $|n| \leq 1$ לכל n;
3. הקבוצה $\{|n| = |1+\cdots+1|\}$ חסומה.

הוכחה. ברור ש־$(1) \Longrightarrow (2) \Longrightarrow (3)$. נניח שקיים M כך ש־$|n| \leq M$ לכל n. לכל a,b,

$$\begin{aligned} |a+b|^n &= |(a+b)^n| = \left|\sum \binom{n}{k} a^k b^{n-k}\right| \\ &\leq 2(n+1)\max\left\{\left|\binom{n}{k} a^k b^{n-k}\right|\right\} \\ &\leq 2(n+1)M\max\left\{|a|^k|b|^{n-k}\right\} \\ &\leq 2(n+1)M\max\{|a|,|b|\}^n; \end{aligned}$$

על־ידי הוצאת שורש n־י מתקבל התנאי (1). □

משפט 6.3.3 *(אוסטרובסקי) כל ערך מוחלט ארכימדי של $\mathbb{Q}$ שקול לערך המוחלט הסטנדרטי.*

הוכחה. יהי $|\cdot|$ ערך מוחלט ארכימדי; נניח, על־ידי העלאה בחזקה מתאימה, שהוא מקיים את אי־שוויון המשולש. לפי טענה 6.3.2, יש $m \in \mathbb{N}$ כך ש־$1 < |m|$. נקבע $n \in \mathbb{N}$, ונכתוב את m בבסיס n: $m = a_k n^k + \cdots + a_1 n + a_0$, כאשר $0 \leq a_i < n-1$, ו־$a_k \neq 0$. כך $|m| = |\sum a_i n^i| \leq \sum a_i |n|^i \leq n(k+1)\max\left\{1,|n|^k\right\}$. מכיוון ש־$n^k \leq m$, $k \leq \log_n m$ ולכן $|m| \leq n(1+\log_n m)\max\left\{1,|n|^{\log_n m}\right\}$. אפשר להציב m^r $(r>0)$ במקום m, ולקבל $|m|^r \leq n(1+r\log_n m)\max\left\{1,|n|^{r\log_n m}\right\}$, כלומר $|m| \leq n^{1/r}(1+r\log_n m)^{1/r}\max\left\{1,|n|^{\log_n m}\right\}$. כאשר $r\to\infty$ מקבלים $|m| \leq |n|^{\log_n m}$, כלומר $\frac{\log|m|}{\log m} \leq \frac{\log|n|}{\log n}$, ולכן $|m| = m^\gamma$ לכל $m \in \mathbb{N}$ עבור γ קבוע. □

תרגיל 6.3.4 יהי F שדה עם ערך מוחלט לא ארכימדי. לכל $b \in F$ ו־$r > 0$ ממשי, אפשר להמשיך את הערך המוחלט מ־F ל־$F(t)$ לפי $|\sum \alpha_i (x-b)^i|_{b,r} = \max|\alpha_i| r^i$. הראה שזה אכן ערך מוחלט. הראה שאם $|b'| = |b|$, אז $|\cdot|_{b,r} = |\cdot|_{b',r}$ אם ורק אם $|b| \leq r$.

6.4 הערכות

הגדרה 6.4.1 *חבורה אבלית סדורה היא חבורה אבלית עם יחס סדר $<$, כך שאם $\alpha < \beta$ אז $\alpha+\gamma < \beta+\gamma$.*

הגדרה 6.4.2 *תהי Γ חבורה אבלית סדורה. פונקציה $\nu : F \to \Gamma \cup \{-\infty\}$ נקראת **הערכה** של השדה F אם:*

(*1*) $\nu(a) = -\infty$ *אם ורק אם* $a = 0$;

(*2*) $\nu(ab) = \nu(a) + \nu(b)$;

(*3*) *קיים קבוע* $c \geq 0$ *כך ש־*$\nu(a+b) \geq -c + \min\{\nu(a), \nu(b)\}$.

*נאמר שההערכה **לא ארכימדית** אם אפשר לבחור $c = 0$, כלומר $\nu(a+b) \geq \min\{\nu(a), \nu(b)\}$.*

מושג ההערכה מכליל את מושג הערך המוחלט, באופן הבא:

תרגיל 6.4.3 לכל ערך מוחלט לא ארכימדי $|\cdot|$, $\nu(a) = -\log(|a|)$ היא הערכה של אותו שדה (המקבלת ערכים ממשיים). בכיוון ההפוך, אם ν הערכה המקבלת ערכים ממשיים, אז $|a| = e^{-\nu(a)}$ הוא ערך מוחלט. (**הדרכה**. העזר בתרגיל 6.1.2 ובטענה אנלוגית עבור הערכות.)
יתרה מזו, הערך המוחלט הצמוד להערכה הוא ארכימדי אם ורק אם ההערכה ארכימדית.

תרגיל 6.4.4 תהי ν הערכה לא ארכימדית. אם $\nu(a_1), \dots, \nu(a_n)$ שונים זה מזה אז $\nu(a_1 + \cdots + a_n) = \min\{\nu(a_1), \dots, \nu(a_n)\}$.

הגדרה 6.4.5 *תחום שלמות R נקרא **חוג הערכה** אם לכל $a \neq 0$ בשדה השברים $F = \mathrm{q}(F)$, $a \in R$ או $a^{-1} \in R$.*

טענה 6.4.6 תהי $\nu : F \to \Gamma \cup \{-\infty\}$ הערכה לא ארכימדית. אז $\mathcal{O}_\nu = \{a \in F : \nu(a) \geq 0\}$ הוא תת־חוג של F, שהוא חוג הערכה.
חוג זה נקרא **חוג ההערכה** (או **חוג השלמים**) של ההערכה, והאידיאל המקסימלי היחיד שלו, $M_\nu = \{a \in F : \nu(a) > 0\}$, נקרא **אידיאל ההערכה**. המנה $\mathcal{O}_\nu / M_\nu$ היא **שדה השאריות** של ההערכה.

הוכחה. $\mathcal{O}_\nu$ סגור לחיבור ולכפל לפי ההנחות על ההערכה. לכל $0 \neq a \in F$, $\nu(a) \geq 0$ או ש־$\nu(a^{-1}) \geq 0$, ו־$a \in \mathcal{O}_\nu$ או $a^{-1} \in R$ בהתאמה. כל איבר מחוץ ל־M_ν הוא בעל $\nu(a) = 0$ ולכן הפיך ב־R. $\square$

תחום שלמות מקיים את **תכונת בזו** אם כל אידיאל נוצר סופית הוא ראשי (לכן חוג הוא ראשי אם ורק אם הוא נתרי ומקיים את תכונת בזו).

משפט 6.4.7 *התכונות הבאות של תחום שלמות R שקולות זו לזו:*

1. *R הוא חוג הערכה.*

2. *קבוצת האידיאלים הראשיים של R סדורה לינארית ביחס להכלה.*

3. *קבוצת האידיאלים של R סדורה ביחס להכלה.*

4. R *מקומי ומקיים את תכונת בזו.*

5. ***יש הערכה לא ארכימדית ν של שדה השברים** $F = \mathrm{q}(R)$, **כך ש־**$R = \mathcal{O}_\nu$.*

הוכחה. $(1) \Longrightarrow (2)$: לכל $0 \neq a, b \in R$, או ש־$\frac{a}{b} \in R$ ואז $Ra \subseteq Rb$, או ש־$\frac{b}{a} \in R$ ואז $Rb \subseteq Ra$.
$(2) \Longrightarrow (3)$: יהיו $I, J \lhd R$ אידיאלים כך ש־$I \nsubseteq J$. אז יש $a \in I$ כך ש־$a \notin J$. לכל $b \in J$, $a \notin Rb$ כי $a \notin J$, ולכן $Rb \subseteq Ra \subseteq I$. מכאן ש־$J \subseteq I$.
$(3) \Longrightarrow (4)$: לפי ההנחה יש אידיאל מקסימלי יחיד. מבין כל קבוצה סופית אידיאלים ראשיים, אחד מהם מכיל את כל האחרים, ולכן סכומם שווה לו.
$(4) \Longrightarrow (1)$: יהיו $a, b \in R$, ויהי $M \lhd R$. נסמן $I = Ra + Rb$. מכיוון ש־I ראשי, I/MI הוא מרחב וקטורי חד־ממדי מעל השדה $\bar{R} = R/M$, ולכן התמונות של a, b תלויות לינארית. לכן יש $u, v \in R$, לא שניהם ב־M, כך ש־$ua + vb \in MI = Ma + Mb$. נכתוב $ua + vb = xa + yb$ עבור $x, y \in M$, אז $a(u - x) = b(y - v)$. אם למשל u הפיך, גם $u - x$ הפיך ולכן $\frac{a}{b} = (u - x)^{-1}(y - v) \in R$.
$(1) \Longleftarrow (5)$: זו טענה **6.4.6**.
$(5) \Longleftarrow (2)$: נסמן $\Gamma = F^\times/R^\times$, ונסדר את החבורה כך ש־$aR^\times > bR^\times$ אם $a \in Rb$. לפי ההנחה, Γ היא חבורה אבלית סדורה לינארית. הפונקציה $\nu(a) = aR^\times$ מהווה הערכה לא ארכימדית של F, שעבורה חוג ההערכה הוא $R = \{a\colon aR^\times \supseteq R^\times\}$. □

דוגמא 6.4.8 **ההערכה ה־p־אדית** על $\mathbb{Q}$ מוגדרת לפי $\nu_p(p^i \frac{n}{m}) = i$ כאשר n, m זרים ל־p.

אפשר להגדיר שקילות של הערכות באותו אופן שבו הגדרנו שקילות של ערכים מוחלטים; למשל אם $\Gamma \subseteq \mathbb{R}$, אז $\nu'(a) = t \cdot \nu(a)$ היא הערכה שקולה ל־ν, לכל $t > 0$.

משפט 6.4.9 (*אוסטרובסקי*) *כל הערכה לא ארכימדית על $\mathbb{Q}$ שקולה להערכה p־אדית עבור ראשוני p.*

הוכחה. תהי ν הערכה לא ארכימדית של $\mathbb{Q}$. נתבונן בחיתוך $P = \{n \in \mathbb{Z}\colon \nu(n) > 0\}$ של אידיאל ההערכה עם חוג השלמים; לפי טענה **3.4.17**, $P \lhd \mathbb{Z}$ ראשוני. אם $P = 0$ אז $\nu(n) = 0$ לכל $n \in \mathbb{Z}$, וההערכה טריוויאלית. לכן יש מספר ראשוני p כך ש־$P = p\mathbb{Z}$. נסמן $\kappa = \nu(p)$, אז לכל n, m זרים ל־p מתקיים $\nu(n) = \nu(m) = 0$ משום ש־$n, m \notin P$, ו־$\nu(p^i \frac{n}{m}) = \kappa i$, כלומר $\nu(\cdot) \sim \nu_p(\cdot)$. □

מסקנה 6.4.10 שדה המספרים הרציונליים מקיים את **נוסחת המכפלה:** אפשר לבחור ערך מוחלט אחד מכל מחלקת שקילות, כך ש־$\prod |a| = 1$ לכל $a \in \mathbb{Q}$. **הדרכה.** $\left|\prod_i p_i^{n_i}\right|_p = p_i^{-n_i}$ אם $p = p_i$.

שדה המקיים תכונה זו נקרא **שדה גלובלי.**

תרגיל 6.4.11 הוכח את ההכללה הבאה של משפט אוסטרובסקי: יהי R תחום ראשי. כל הערכה לא־ארכימדית של $F = \mathrm{q}(R)$ שעבורה $R \subseteq \mathcal{O}_\nu$, היא הערכה p־אדית עבור ראשוני $p \in R$ (המוגדרת בדומה לדוגמא 6.4.8).

תרגיל 6.4.12 יהי F שדה. הראה שכל הערכה לא ארכימדית של $F(t)$, המשרה את ההערכה הטריוויאלית על F, היא או הערכה p־אדית עבור פולינום אי־פריק $p \in F[\lambda]$, או שקולה להערכה ν_∞ המוגדרת על $F[t]$ לפי $\nu_\infty(f) = -\deg(f)$. **הדרכה.** אם $\nu(t) \geq 0$ אז $F[t] \subseteq \mathcal{O}_\nu$, והתוצאה נובעת מתרגיל 6.4.11; אחרת $\nu(t^n) = n\nu(t)$ ו־$\nu(f) = \nu(t)\deg(f)$ לפי תרגיל 6.4.4.

6.5 שדות שלמים והשלמות

יהי F שדה עם הערכה. ההערכה משרה על F טופולוגיה מטרית. השדה **שלם** אם כל סדרת קושי מתכנסת. אם $F \subseteq K$ הרחבה של שדות כך שלהערכה של F יש המשכה יחידה אל K, וביחס אליה התמונה של F ב־K צפופה, אז K נקרא **השלמה** של F.

משפט 6.5.1 *לכל שדה עם הערכה יש השלמה יחידה (עד כדי איזומורפיזם של שדות עם הערכה).*

אפשר לבנות את ההשלמה כחוג מנה של החוג של סדרות קושי מעל F, מודולו האידיאל הכולל סדרות המתכנסות לאפס. ההערכה מומשכת אל השדה הזה באופן יחיד, והשיכון האלכסוני הוא צפוף.

דוגמא 6.5.2 ההשלמה של $\mathbb{Q}$ עם הערך המוחלט הארכימדי היא שדה המספרים הממשיים $\mathbb{R}$.

דוגמא 6.5.3 ההשלמה של $\mathbb{Q}$ ביחס להערכה ה־p־אדית היא שדה המספרים ה־p־אדיים, $\mathbb{Q}_p$.

טענה 6.5.4 שדה עם הערכה לא־ארכימדית הוא קומפקטי מקומית (במרחב טופולוגי) אם ורק אם הוא שלם, ושדה השאריות שלו סופי.

משפט 6.5.5 *השדות היחידים שהם שלמים ביחס לערך מוחלט ארכימדי הם $\mathbb{R}$ ו־$\mathbb{C}$. השדות היחידים שהם שלמים ביחס להערכות לא ארכימדיות הם השדות $\mathbb{Q}_p$ ו־$\mathbb{F}_p((x))$ (לכל p ראשוני), והרחבות סופיות שלהם.*

// חלק שני - אלגברה לא קומוטטיבית - אינו מוצג.