אלגברה מתקדמת

עוזי וישנה

22 באפריל 2015

אלגברה מתקדמת

מהדורה 1.936

הקדמה. חוברת זו מכסה, בשני חלקיה, את הקורסים "אלגברה קומוטטיבית" ו"אלגברה לא קומוטטיבית".

הקורס הראשון (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 השני (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

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 מודולים

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

תרגיל 1.1.1 תהי M חבורה אבלית. יש התאמה בין פעולות הכפל בסקלר $R\times M\to M$ ההופכות את M למודול מעל R, לבין הומומורפיזמים $\varphi\colon R\to\mathrm{End}(M,M)$, 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 $\varphi\colon M\to N$ מקיים את האקסיומה $\varphi(ax) = a\varphi(x)$.

דוגמא 1.1.2 1. מודולים מעל חוג השלמים $\mathbb{Z}$ אינם אלא חבורות אבליות.

2. כל חוג הוא מודול מעל עצמו, ותת־המודולים 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.

נזכיר את שלושת משפטי האיזומורפיזם של מודולים:

טענה 1.1.3 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 1.1.4 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.

1.1.3 מודולים ציקליים

∘ מודול שיש לו יוצר אחד, כלומר כל מודול מהצורה $Rx = \{ax : a \in R\}$, נקרא **מודול ציקלי**.

תרגיל 1.1.5 מודול ציקלי מעל $\mathbb{Z}$ הוא חבורה ציקלית.

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 אברים שונים זה מזה.

∘ **הגדרה 1.1.6** *יהי M מודול, ו־$x \in M$. אז $\mathrm{Ann}(x) = \{a \in R : ax = 0\}$ נקרא* ***המאפס*** *של x.*

תרגיל 1.1.7 יהי $M = Rx$ מודול ציקלי מעל R.
1. $\mathrm{Ann}(x)$ הוא אידיאל שמאלי של R, ו־$Rx \cong R/\mathrm{Ann}(x)$ (כמודולים).
2. כל מודול ציקלי הוא מהצורה R/L כאשר $L \leq_\ell R$.

בסעיף 8.2 נגדיר את המאפס של המודול כולו, שהוא אידיאל דו־צדדי של R.

∘ **תרגיל 1.1.8** 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 $(r + I)x = rx$(השווה לתרגיל 8.2.2).

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

תרגיל 1.1.9 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 1.1.10 1. כל מודול פשוט הוא ציקלי.

2. R/L הוא מודול פשוט אם ורק אם L אידיאל שמאלי מקסימלי.

תרגיל 1.1.11 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 1.1.12 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 1.1.13 *קבוצה $M \subseteq B$ **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 1.1.14 אם $B = \{b_1, \dots, b_n\}$ יוצרת מודול M, אז $M = Rb_1 + \dots + Rb_n$.

1.2 סדרות הרכב

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

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

*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 $M_i = L_1 + \dots + L_i$, כאשר L_j המודולים מתרגיל 1.1.11. הראה ש־$0 = M_0 < M_1 < \dots < M_{n-1} \leq M_n = M$ היא סדרת הרכב של $\mathrm{M}_n(D)$.

תרגיל 1.2.3 ל־$\mathbb{Z}$ (כמודול מעל עצמו) אין סדרת הרכב.

תרגיל 1.2.4 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 1.2.5 אם $K \subseteq K'$, $N \cap K = N \cap K'$ ו־$N + K = N + K'$ אז $K = K'$. **הדרכה.** $K' = (K' + N) \cap K' = (K + N) \cap K' = K + (N \cap K') = K + (N \cap K) = K$.

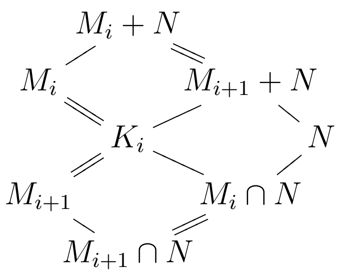
טענה 1.2.6 תהי

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

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

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

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



הוכחה. **נסמן $K_i = M_i \cap N + M_{i+1}$, כך שתמיד $M_{i+1} \le K_i \le M_i$. 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־$(M_i \cap N)/(M_{i+1} \cap N) \cong K_i/M_{i+1}$. 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.** □

משפט 1.2.7 (משפט ז'ורדן־הולדר־שרייר) ***יהי M מודול בעל סדרת הרכב (1.1). אז***

1. ***כל סדרה של תת־מודולים $0 = N_\ell < \cdots < N_2 < N_1 < M$ 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 1.2.6, 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 1.2.8 ***אם יש למודול M סדרת הרכב באורך n אומרים שהאורך שלו הוא n, ומסמנים $\ell(M) = n$.***

תרגיל 1.2.9 יהי M מודול בעל אורך סופי; אז לכל תת־מודול N, יש ל־N ול־M/N סדרות הרכב, ומתקיים $\ell(M) = \ell(N) + \ell(M/N)$. **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 1.2.10 אם N, N' הם תת־מודולים בעלי אורך סופי של M, אז $\ell(N+N') \le \ell(N) + \ell(N')$. **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 1.2.11 הראה שסדרת ההרכב המתקבלת בהוכחה של משפט ז'ורדן־הולדר־שרייר היא

$$0 \le \cdots \le N_{j+2} + M_i \cap N_{j+1} \le \cdots \le N_{j+1} + M_i \cap N_j \le \cdots \le M,$$

עם סדר לקסיקוגרפי של האינדקסים (קודם j ואחר־כך i).

1.3 תנאי השרשרת

תרגיל 1.3.1 אם $M_1 \leq M_2 \leq \cdots$ מודולים (תת־מודולים של מודול M), אז גם $\cup M_i$ הוא מודול (תת־מודול של M).

תרגיל 1.3.2 חיתוך משפחה כלשהי של תת־מודולים הוא תת־מודול.

הגדרה 1.3.3 *אומרים שמודול M מקיים את **תנאי השרשרת העולה** אם כל שרשרת עולה של תת־מודולים מוכרחה להסתיים: לא יתכן ש־ $M_0 < M_1 < \cdots$ כשאלו תת־מודולים של M. מודול כזה נקרא **נתרי** (על־שם אמי נתר).*
*אומרים ש־M מקיים את **תנאי השרשרת היורדת** אם כל שרשרת יורדת של תת־מודולים מוכרחה להסתיים: לא יתכן ש־ $M_0 > M_1 > \cdots$. מודול כזה נקרא **ארטיני** (על־שם אמיל ארטין).*

תרגיל 1.3.4 תנאי השרשרת העולה שקול ל**תנאי המקסימום**, שלפיו בכל משפחה של תת־מודולים יש איבר מקסימלי. בדומה לזה, תנאי השרשרת היורדת שקול ל**תנאי המינימום** (בכל משפחה של תת־מודולים יש איבר מינימלי).

דוגמא 1.3.5 כמודולים מעל $\mathbb{Z}$:

1. $\mathbb{Z}$ הוא נתרי (כל מנה אמיתית שלו היא סופית) אבל לא ארטיני: $\mathbb{Z} > \cdots > 2^n\mathbb{Z} > \cdots$.
2. $\mathbb{Q}/\mathbb{Z}$ אינו נתרי (הסדרה $2^{-n}\mathbb{Z}/\mathbb{Z}$ עולה) ואינו ארטיני (הסדרה $M_p = \mathbb{Z}[\frac{1}{q}:\ q > p]$ יורדת).
3. $\mathbb{Z}[\frac{1}{5}]/\mathbb{Z}$ 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 1.3.6 קבע האם $\mathbb{Q}$ הוא מודול ארטיני/נתרי מעל $\mathbb{Z}$. **הדרכה.** (דוגמא (2).1.3.5) האם הוא ארטיני/נתרי מעל $R = \mathbb{Z}_{\langle 2\rangle} = \left\{\frac{n}{m}:\ 2 \nmid m\right\}$?

תרגיל 1.3.7
1. אם M איזומורפי לתת־מודול אמיתי של M, אז M אינו ארטיני.
2. אם M איזומורפי למודול מנה אמיתי של M, אז M אינו נתרי.

טענה 1.3.8 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 תנאי 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 לתנאי השרשרת היורדת. מכאן שעבור i גדול מספיק, $M_i = 0$, ובנינו סדרת הרכב. $\square$

תרגיל 1.3.9 תת־מודול ומודול מנה של מודול נתרי (ארטיני) הם נתריים (ארטיניים).

טענה 1.3.10 אם $N \leq M$ ו־M/N הם נתריים (ארטיניים) אז גם M כזה.

הוכחה. נוכיח עבור תנאי השרשרת העולה. נניח שיש ב־M שרשרת עולה $0 < M_1 < M_2 < \cdots$. אז גם $0 < M_1 \cap N < M_2 \cap N < \cdots$ ו־ $0 < (M_1+N)/N < (M_2+N)/N < \cdots$ 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 1.2.5. $\square$

טענה 1.3.11 (**אינדוקציה נתרית**) יהי M מודול נתרי. נניח שאם תכונה $\mathcal{P}$ מתקיימת לכל תת־מודול המכיל ממש את $A \leq M$, 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. □

1.3.1 תנאי השרשרת בחוגים

הגדרה 1.3.12 *חוג נקרא **ארטיני** או **נתרי** אם הוא ארטיני או נתרי כמודול מעל עצמו.*

דוגמא 1.3.13 $\mathbb{Z}$ הוא חוג ארטיני שאינו נתרי.

תרגיל 1.3.14 חוג מנה של חוג נתרי (ארטיני) הוא נתרי (ארטיני).

תרגיל 1.3.15 הראה שתת־חוג של חוג נתרי (ארטיני) אינו בהכרח נתרי (ארטיני). **הצעה.** שדה הוא נתרי וארטיני, אבל תחום שלמות לעולם אינו ארטיני (טענה 5.1.8 לעיל), וגם אינו חייב להיות נתרי.

1.4 מודולים נוצרים סופית

נתריות וארטיניות, כמו תנאי המינימום ותנאי המקסימום, הם קריטריונים לסופיות. למרות הסימטריה המדומה, יש מודולים נתריים שאינם ארטיניים, ומודולים ארטיניים שאינם נתריים. בסמסטר הבא נוכיח את **משפט הופקינס־לויצקי** (משפט 8.5.4): כל חוג ארטיני הוא נתרי.

טענה 1.4.1 אם R ארטיני או נתרי, אז כל מודול נוצר סופית מעל R גם הוא ארטיני או 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 $M/N \cong N/(N \cap Rx_n)$ הוא ארטיני (נתרי) כתת־מודול של מודול ארטיני (נתרי); סיימנו לפי טענה 1.3.10.** □

תכונה נוספת שיש לבחון בהקשר זה היא קיומה של קבוצת יוצרים סופית. מתברר שכל מודול נתרי הוא נוצר סופית, אבל הכיוון ההפוך אינו נכון:

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/I, אלא ש־$M = \sum x^n y$ בעל מימד 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 $x_{i+1} \not\in N_i = Rx_0 + \cdots + Rx_i$; 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 1.3.9) 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 $\bar{N} = \cup N_i$ 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־$f_j \not\in \sum_{i<j} R[x]f_i$. יהי a_j המקדם העליון של f_j. אם $a_j \in \sum_{i<j} Ra_i$ אז אפשר לכתוב $a_j = \sum_{i<j} r_i a_i$ עבור $r_i \in R$, ואז $f_j - \sum_{i<j} r_i x^{n_j - n_i} f_i$ 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 $\sigma\colon R \to R$ אוטומורפיזם ו־$\delta\colon R \to R$ 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 1.3.14. ◦

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 $I \lhd R[[x]]$. נסמן ב־I_n את האידיאל של R הכולל את המקדמים המובילים של כל אברי $I \cap x^n R[[x]]$. כך $I_0 \subseteq I_1 \subseteq I_2 \cdots$, 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 יהי F שדה, אז $F[x]$ אינו ארטיני.

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

תרגיל 1.4.11 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

אידיאל אמיתי של חוג הוא **מקסימלי** אם אינו מוכל באף אידיאל אמיתי אחר, **וראשוני** אם אינו מכיל מכפלה של אידיאלים אלא אם הוא מכיל אחד מהם. **חוג פשוט** הוא חוג שאין לו אידיאלים שונים מאפס, **וחוג ראשוני** הוא חוג שבו אפס אידיאל ראשוני. אידיאל הוא מקסימלי אם ורק אם R/I פשוט, וראשוני אם ורק אם R/I ראשוני.

המושגים קשורים זה לזה באופן הדוק: כל אידיאל ראשוני הוא מקסימלי, ואידיאל מקסימלי ביחס לתכונה מסויימת הוא לעתים קרובות ראשוני.

2.1 אידיאלים ראשוניים ומקסימליים

תרגיל 2.1.1 אידיאל P בחוג קומוטטיבי R הוא ראשוני אם ורק אם R/P הוא תחום שלמות.

תרגיל 2.1.2 (כאשר R קומוטטיבי) $P \lhd R$ ראשוני אם ורק אם לכל $a, b \in R$, אם $ab \in P$ אז $a \in P$ או $b \in P$.

תרגיל 2.1.3 יהי P אידיאל ראשוני. אם $P = A \cap B$ אז $P = A$ או $P = B$. **הדרכה**. $AB \subseteq A \cap B$. ◦

תרגיל 2.1.4 $n\mathbb{Z}$ הוא אידיאל ראשוני של $\mathbb{Z}$ אם ורק אם n ראשוני.

תרגיל 2.1.5 בתחום פריקות יחידה: האידיאל $P = Rp$ הוא ראשוני אם ורק אם p אי־פריק, וכל אידיאל ראשוני $\neq 0$ כולל איבר אי־פריק. ◦

תרגיל 2.1.6 יהי R תחום שלמות נתרי (חוג נתרי הוא בפרט אטומי, כלומר כל איבר הוא מכפלה של איברים אי־פריקים). הראה שכל אידיאל ראשוני של R נוצר על־ידי איברים אי־פריקים. **הדרכה**. 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.

משפט 2.1.7 (משפט השאריות הסיני) יהיו $I_1, \dots, I_n$ אידיאלים קו־מקסימליים של חוג R. אז $R/(I_1 \cap \dots \cap I_n) \cong R/I_1 \times \dots \times R/I_n$. ◦

הגדרה 2.1.8 *עבור $I, I' \lhd R$, נגדיר $I{:}I' = \{x \in R : xI' \subseteq I\}$. זהו האידיאל הגדול ביותר המקיים $(I{:}I')I' \subseteq I$.*

תרגיל 2.1.9 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 2.1.10 יהי $J \lhd R$, 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 $\sum Rx_i a = (I{:}a)a \subseteq I$, ולכל j יש $t_j \in R$ כך ש־$y_j - t_j a \in I$. נראה שהאברים $\{x_i a, y_j - t_j a\}$ יוצרים את I: לכל $c \in I$, יש $s_j \in R$ כך ש־$c = \sum s_j y_j = \sum s_j(y_j - t_j a) + (\sum s_j t_j)a$, ואז $(\sum s_j t_j)a \in I$ ולכן שייך לאידיאל $\sum Rx_i a$.

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

משפט 2.1.11 חוג קומוטטיבי R שבו כל אידיאל ראשוני נוצר סופית, הוא נתרי.

הוכחה. אם כל האידיאלים נוצרים סופית, סיימנו. נניח שלא, אז לפי תרגיל 1.4.11, 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 2.1.9 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 2.1.10, גם J נוצר סופית, בסתירה להנחה. מכאן ש־J ראשוני, אבל אז הוא נוצר סופית לפי ההנחה. $\square$

2.2 חוגים מקומיים

מן הלמה של צורן נובע שכל אידיאל בחוג (עם יחידה) מוכל באידיאל מקסימלי.

הגדרה 2.2.1 *חוג קומוטטיבי הוא מקומי אם יש לו אידיאל מקסימלי יחיד.*

טענה 2.2.2 R מקומי אם ורק אם $R - U(R)$ אידיאל, אם ורק אם $R - U(R)$ סגור לחיבור, אם ורק אם לכל $a \in R$, a או $1 - a$ הפיכים.

משפט 2.2.3 (הלמה של נקיימה לחוגים מקומיים) יהי R חוג מקומי. לכל אידיאל $A \lhd R$ ולכל מודול נוצר סופית M, מתקיים $AM < M$.

הוכחה. נכתוב $M = Rx_1 + \cdots + Rx_n$ עבור n מינימלי, ונניח בשלילה ש־$AM = M$. בפרט אפשר לכתוב את $x_n \in M = AM$ בצורה $x_n = a_1x_1 + \cdots + a_nx_n$ עבור $a_i \in A$; ואז $(1 - a_n)x_n \in \sum_{i<n} Ax_i \subseteq \sum_{i<n} Rx_i$. אבל $1 - a_n$ הפיך, ולכן $x_n \in \sum_{i<n} Rx_i$, בסתירה להנחה. $\square$

מסקנה 2.2.4 (הלמה של נקיימה לחוגים קומוטטיביים) לכל מודול נוצר סופית M מעל חוג קומוטטיבי R קיים אידיאל מקסימלי A כך ש־$AM \neq M$.

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?) $\circ$

את מחלקת השקילות של (s,r) נסמן $\frac{r}{s}$. נסמן גם $S^{-1}R = \left\{\frac{r}{s} \colon\ s \in S, r \in R\right\}$. 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. $\circ$

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

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

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

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

תרגיל 2.3.8 נניח שכל אברי S רגולריים. הראה ש־$\iota \colon R \to S^{-1}R$ 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 $\varphi \colon R \to A$ הומומורפיזם הופך S. **אז קיים הומומורפיזם יחיד** $\varphi' \colon S^{-1}R \to A$ כך ש־$\varphi = \varphi' \circ \iota$.* $\circ$

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

2.3.1 האידיאלים של $S^{-1}R$

השאלה הטבעית כעת היא מה קורה לאידיאלים של R כשעוברים לחוג $S^{-1}R$. אם $A \lhd R$, 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 2.3.10 לכל $A \lhd R$, $S^{-1}A$ הוא אידיאל של $S^{-1}R$.

בכיוון ההפוך, לכל $T \lhd S^{-1}R$, 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 2.3.11 לכל $T \lhd S^{-1}R$, $\iota^{-1}(T)$ הוא אידיאל של R.

תרגיל 2.3.12
1. לכל $T \lhd S^{-1}R$, $T = S^{-1}\iota^{-1}(T)$;
2. כל אידיאל של $S^{-1}R$ הוא מהצורה $S^{-1}A$ עבור $A \lhd R$ מתאים.

פתרון. *יהי $T \lhd S^{-1}R$, אז $A = \iota^{-1}(T)$ הוא אידיאל של R, ומכיוון ש־$T \subseteq A$, מתקיים $T = S^{-1}T \subseteq S^{-1}\iota(A) = S^{-1}A$. 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

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

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 2.3.13
1. יהי $A \lhd R$. אז $S^{-1}A$ אידיאל אמיתי אם ורק אם $S \cap A = \emptyset$.
2. יהי $T \lhd S^{-1}R$. אז T אמיתי אם ורק אם החיתוך של $\iota^{-1}(T)$ עם S ריק.

כלומר, ההעתקות שהוגדרו קודם לכן פועלות גם על הקבוצות המצומצמות

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

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

תרגיל 2.3.14 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 2.3.15 יהי $P \lhd R$ ראשוני זר ל־S, אז $\iota^{-1}(S^{-1}P) = P$. ***פתרון.*** *ההכלה $P \subseteq \iota^{-1}(S^{-1}P)$ טריוויאלית. נניח ש־$\frac{x}{1} \in \iota^{-1}(S^{-1}P)$, $\frac{a}{s} =$ כאשר $a \in P$ ו־$s \in S$. מכיוון ש־s מרכזי, $(RsR)(RxR) = RsxR = RaR \subseteq P$, אבל $s \notin P$ ולכן $RsR \not\subseteq P$, ולפי הראשוניות נובע מכך ש־$RxR \subseteq P$. מכאן ש־$x \in P$.*

תרגיל 2.3.16 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* $T_i = S^{-1}A$ *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 2.3.15. מכיוון ש־P *ראשוני, יש* i *שעבורו* $A_i \subseteq P$, *ואז* $T_i = S^{-1}A_i \subseteq S^{-1}P$.

תרגיל 2.3.17 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

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

מוגדרות היטב, ולפי תרגילים 2.3.12 ו־2.3.15, הן הפוכות זו לזו. אם כך, הוכחנו:

משפט 2.3.18 *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* $P \longleftarrow S^{-1}P$*,* $T \mapsto \iota^{-1}(T)$. ◦

תרגיל 2.3.19 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 ◦

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

לעומת זאת:

תרגיל 2.3.20 יהי $P \triangleleft R$ אידיאל ראשוני שהוא זר ל־S. הראה שקיים שיכון $R/P \hookrightarrow S^{-1}R/S^{-1}P$. **הדרכה**. תרגילים 2.3.19 ו־2.3.15.

2.3.2 מיקום באידיאל ראשוני

תרגיל 2.3.21 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 2.3.22 יש התאמה חד־חד־ערכית ועל בין אידיאלים ראשוניים של R המוכלים ב־P, לבין אידיאלים ראשוניים של R_P. **הדרכה**. זהו משפט 2.3.18 עבור $S = R - P$. ◦

תרגיל 2.3.23 יהי P אידיאל ראשוני של חוג קומוטטיבי R. אז R_P מקומי, והאידיאל המקסימלי שלו הוא $P_P = (R-P)^{-1}P$. **הדרכה**. תרגיל 2.3.22.

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

תרגיל 2.3.25 אם R תחום שלמות אז לכל אידיאל ראשוני $P \lhd R$ יש שיכון $R_P \hookrightarrow \mathrm{q}(R)$, כאשר $\mathrm{q}(R)$ הוא שדה השברים של R.

משפט 2.3.26 *יהי R תחום שלמות. אז חיתוך כל המיקומים $R_M \subseteq F = \mathrm{q}(R)$, על־פני האידיאלים המקסימליים $M \lhd R$, שווה ל־R.*

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

יהי $J = b{:}a = \{x \in R\colon\ xa \in Rb\}$; ברור שזהו אידיאל של R. אם $J \lhd R$ 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־$b_1 \not\in M$. 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 2.3.27 יהי R תחום שלמות. אז חיתוך כל המיקומים $R_P \subseteq F = \mathrm{q}(R)$, על־פני האידיאלים הראשוניים $P \lhd R$, שווה ל־R.

מסקנה 2.3.28 (ממשפט 2.3.26) 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.

הגדרה 3.0.29 *תהי $R \supseteq C$ הרחבה של חוגים. אומרים ש־R* ***אלגברה אפינית מעל*** *C אם R נוצר סופית כאלגברה מעל C.*

3.1 חוגי פולינומים

תרגיל 3.1.1 כל אלגברה אפינית מעל C היא חוג מנה של $C[\lambda_1, \ldots, \lambda_n]$ עבור n מתאים. ∘

טענה 3.1.2 אם C חוג נתרי, כל אלגברה אפינית מעל C היא נתרית.

הוכחה. (זהו תרגיל **1.4.8**). □

תרגיל 3.1.3 **האוניברסליות של חוגי פולינומים:** נניח ש־$\varphi : C \rightarrow R$ הומומורפיזם. לכל $\beta_1, \ldots, \beta_n \in R$ יש הומומורפיזם $\bar{\varphi} : C[\lambda_1, \ldots, \lambda_n] \rightarrow K$ יחיד הממשיך את φ, כך ש־$\bar{\varphi}(\lambda_i) = \beta_i$. ∘

תרגיל 3.1.4 K שדה אינסופי. אם $0 \neq f \in K[\lambda_1, \ldots, \lambda_n]$, אז יש $\alpha_1, \ldots, \alpha_n \in K$ כך ש־$f(\alpha_1, \ldots, \alpha_n) \neq 0$. **הדרכה**. אינדוקציה על n. ∘

תרגיל 3.1.5 הראה שהטענה בתרגיל 3.1.4 אינה נכונה עבור שדה סופי $K = \mathbb{F}_q$.

3.2 אלגבריות

הגדרה 3.2.1 *תהי $R \supseteq C$ 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 3.4.4, המראה שאם אלגברה אפינית היא שדה אז היא מוכרחה להיות אלגברית (וממימד סופי מעל F). מכאן נובע שאם אלגברה אפינית אינה אלגברית, אז יש לה אידיאלים (וזה מאפשר להתחיל תהליכי אינדוקציה).

תרגיל 3.2.2 תהי $R \supseteq F$ 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 3.2.3 **תהי $R \subseteq C$ הרחבה אלגברית של תחומי שלמות. אז כל אידיאל $0 \neq A \lhd R$ נחתך עם C.**

הוכחה. **יהי $0 \in a \in A$. 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 3.2.4 תחום שלמות אלגברי מעל שדה הוא שדה בעצמו. **הדרכה.** טענה 3.2.3.

3.2.1 מימד טרנסצנדנטי

הגדרה 3.2.5 ***יהי $\leadsto$ יחס בין תת־קבוצות ואברים של קבוצה X (כלומר, לכל תת־קבוצה $S \subseteq X$ ולכל איבר $s \in X$, יכול להתקיים או לא להתקיים היחס $S \leadsto s$.) עבור תת־קבוצה S' נסמן $S \leadsto S'$ אם לכל $x \in S'$ מתקיים $S \leadsto x$. היחס נקרא תלות פורמלית אם***

1. אם $s \in S$ אז $S \leadsto s$;

2. אם $S \leadsto s$ אז קיימת $S_0 \subseteq S$ סופית כך ש־$S_0 \leadsto s$;

3. אם $S \leadsto a$ ו־$S \leadsto S'$ אז $S' \leadsto a$;

4. אם $S \cup \{a\} \leadsto b$ אבל $S \not\leadsto b$ אז $S \cup \{b\} \leadsto a$ ("למת ההחלפה של שטייניץ").

קבוצה S נקראת בלתי תלויה אם לכל $a \notin S$, $a \not\leadsto S - \{a\}$.

תרגיל 3.2.6 יהי V מרחב וקטורי. היחס "$S \leadsto s$ אם s הוא צירוף לינארי של אברי S" הוא תלות פורמלית על V.

תרגיל 3.2.7 הסבר היכן נכשלת ההוכחה בתרגיל 3.2.6 אם מחליפים את V במודול כלשהו, ותן דוגמא נגדית מתאימה.

תרגיל 3.2.8 הראה שכל תלות פורמלית מקיימת את התנאי

$4'$. אם $a \not\leadsto S$ ו־S בלתי תלויה, אז $S \cup \{a\}$ בלתי תלויה.

פתרון. *אחרת יש $s \in S$ כך ש־$(S - \{s\}) \cup \{a\} \leadsto s$, אבל $S - \{s\} \not\leadsto s$, ולפי תכונה 4 $S \leadsto a$, בסתירה להנחה.*

תרגיל 3.2.9 אם S בלתי תלויה מקסימלית אז לכל a, $S \leadsto a$. **הדרכה.** אם $a \in S$ המסקנה נובעת מתנאי 1. אחרת $S \cup \{a\}$ בלתי תלויה לפי $4'$.

תרגיל 3.2.10 נניח ש־$\leadsto$ תלות פורמלית. אז כל תת־קבוצה בלתי תלויה אפשר להרחיב לתת־קבוצה בלתי תלויה מקסימלית (ביחס להכלה). **הדרכה.** הלמה של צורן.

משפט 3.2.11 ***נניח ש־$\leadsto$ תלות פורמלית. אז לכל הקבוצות הבלתי־תלויות המקסימליות יש אותה עוצמה.***

הוכחה. (נסתפק בהוכחה כאשר הקבוצות סופיות). תהיינה B, B' קבוצות בלתי תלויות מקסימליות. נכתוב $B = \{b_1, \dots, b_n\}$, ונראה שלכל $k \leq n$ קיימים $b'_1, \dots, b'_k \in B'$ כך ש־$\{b'_1, \dots, b'_k, b_{k+1}, \dots, b_n\}$ בלתי תלויה. בפרט, עבור $k = n$, יוצא ש־$n = |B| \leq |B'|$. ההוכחה באינדוקציה על k. עבור $k = 0$ אין מה להוכיח. נניח שהטענה נכונה עבור $k - 1$; אם $b_k \in B'$, גמרנו. אחרת, לפי תרגיל 3.2.9, $b_k \rightsquigarrow B'$; אבל $b_k \not\rightsquigarrow B_k = \left\{b'_1, \dots, b'_{k-1}, b_{k+1}, \dots, b_n\right\}$ לפי הנחת האינדוקציה, ומתכונה 3 נובע שקיים $b'_k \in B'$ כך ש־$b'_k \not\rightsquigarrow B_k$. □

הגדרה 3.2.12 *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־$f(a_1, \dots, a_n) = 0$.*

הגדרה 3.2.13 *יהיו $F \subseteq R$ חוגים. עבור קבוצה $S \subseteq R$ ו־$a \in R$, a תלוי אלגברית ב־S אם a אלגברי מעל $F[S]$. במלים אחרות אם יש $f \in F[\lambda_1, \dots, \lambda_n, \lambda_{n+1}]$ שאינו שייך ל־$F[\lambda_1, \dots, \lambda_n]$, ואברים $a_1, \dots, a_n \in S$, כך ש־$f(a_1, \dots, a_n, a) = 0$.*

תרגיל 3.2.14 הראה שיחס התלות האלגברית היא יחס תלות פורמלית.

תרגיל 3.2.15 $C \subseteq R$ חוגים. תת־קבוצה בלתי תלויה מקסימלית נקראת **בסיס טרנסצנדנטי** של R מעל C. גודלה הוא **המימד הטרנסצנדנטי** או **דרגת הטרנסצנדנטיות** $\mathrm{trdeg}_C(R)$.

תרגיל 3.2.16 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 $\lambda_i \mapsto a_i$.

תרגיל 3.2.17 אם $R = C[a_1, \dots, a_n]$ אז $\mathrm{trdeg}_C(R) \leq n$. מתקיים שוויון אם ורק אם $R \cong F[\lambda_1, \dots, \lambda_n]$ הוא חוג הפולינומים ב־n משתנים.

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

תרגיל 3.2.18 נסח את כל הנ"ל בשפה של מטרואידים. מטרואיד הוא אוסף לא ריק M של תת־קבוצות, הסגור כלפי מטה ומקיים את האקסיומה הבאה: לכל $A, B \in M$, אם $|B| > |A|$ אז יש $x \in B \setminus A$ כך ש־$A \cup \{x\} \in M$.

3.3 הרחבות שלמות

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

הגדרה 3.3.1 *אומרים ש־$a \in R$ הוא **שלם** מעל C אם x הוא שורש לפולינום מתוקן $f \in C[\lambda]$.*

טענה 3.3.2 תהי $C \subseteq R$ הרחבה. התכונות הבאות שקולות:

א. $a \in R$ שלם;

ב. $C[a]$ מודול נוצר סופית מעל C,

ג. קיים תת־מודול נוצר סופית של R הכולל את 1 וסגור לכפל ב־a.

הוכחה. **(1) $\Longleftarrow$ (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) $\Longleftarrow$ (3). $C[a]$ הוא המודול הדרוש. (3) $\Longleftarrow$ (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־$a^kx_j = \sum([a]^k)_{ij}x_i$ לכל $k \geq 1$; בפרט $f(a)1 \in f(a)M = 0$, ולכן $f(a) = 0$.** □

הערה 3.3.3 יהיו $C \subseteq R$, $a \in R$, ו־$J \lhd C$. אם יש תת־מודול נוצר סופית $M \leq R$ כך ש־$1 \in M$ 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) $\Longleftarrow$ (1) של טענה 3.3.2.** □

תרגיל 3.3.4 מצא פולינום המאפס את $a^{1/3} + b^{1/3}$ מעל F, כאשר $a, b \in F$.

טענה 3.3.5 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 3.3.2, 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 3.3.6 תהי $C \subseteq R$ הרחבה, ויהיו $a, b \in R$ שלמים מעל C. אז גם $a + b$ ו־ab הם שלמים.

הוכחה. **לפי טענה 3.3.5, שהרי $a + b, ab \in C[a, b]$.** □

מסקנה 3.3.7 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 3.3.8 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 3.3.2, a שלם מעל C.** □

הגדרה 3.3.9 ***החוג R נקרא הרחבה שלמה של C אם $\mathrm{Int}_C(R) = R$, כלומר כל אברי R שלמים מעל C. אומרים ש־C סגור בשלמות בתוך R אם $\mathrm{Int}_C(R) = C$.***

תרגיל 3.3.10 הראה ש־$\mathbb{Z}$ סגור בשלמות בתוך $\mathbb{Q}$, ושכל חוג C סגור בשלמות בתוך חוג הפולינומים $C[\lambda]$.

טענה 3.3.11 לכל הרחבה $C \subseteq R$, $\mathrm{Int}_C(R)$ סגור בשלמות בתוך R.

הוכחה. **כל איבר שלם מעל $\mathrm{Int}_C(R)$ הוא שלם מעל C לפי טענה 3.3.8.** □

תרגיל 3.3.12 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 3.3.13 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 3.3.14 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 3.3.15 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 $a^{-1} = \sum_{i=0}^{n-1} \alpha_i a^{n-i-1}$.

3.3.1 אידיאלים בהרחבות שלמות

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

תרגיל 3.3.16 תהי $C \subseteq R$ הרחבה. לכל אידיאל $A \triangleleft R$, יש שיכון $C/(C \cap A) \hookrightarrow R/A$.

טענה 3.3.17 תהי $C \subseteq R$ הרחבה כלשהי. לכל אידיאל ראשוני $Q \triangleleft R$ ראשוני, $Q \cap C$ אידיאל ראשוני של C.

הוכחה. לפי תרגיל 3.3.16, $C/(Q \cap C) \hookrightarrow R/Q$; מכיוון ש־$R/Q$ תחום שלמות, גם $C/(Q \cap C)$ תחום שלמות. $\square$

תרגיל 3.3.18 נניח ש־R שלם מעל C. לכל אידיאל $A \triangleleft R$, גם R/A הרחבה שלמה של $C/(C \cap A)$.

תרגיל 3.3.19 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 3.3.20 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 3.3.19.

למה 3.3.21 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 3.3.15. הכיוון ההפוך הוא מקרה פרטי של תרגיל 3.2.4. $\square$

תרגיל 3.3.22 הוכח את הכיוון ההפוך של למה 3.3.21 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 3.3.23 $R = F[x\colon\ x^2 = 0]$ היא דוגמא נגדית ללמה 3.3.21, כאשר מוותרים על ההנחה ש־R תחום שלמות. אכן, $F \subseteq R$ היא הרחבה שלמה, ו־R אינו שדה.

מסקנה 3.3.24 נניח ש־R שלם מעל C, ויהי $M \lhd R$ אידיאל ראשוני. אז $M \lhd R$ מקסימלי אם ורק אם $N = M \cap C \lhd C$ מקסימלי.

הוכחה. לפי תרגיל 3.3.18, R/M הרחבה שלמה של C/N. לפי למה 3.3.21, R/M שדה אם ורק אם C/N שדה, ולכן M מקסימלי אם ורק אם N מקסימלי. □

תרגיל 3.3.25 העזר בתרגיל 3.3.23 כדי למצוא הרחבה שלמה $C \subseteq R$ עם אידיאל שאינו ראשוני $M \lhd R$, כך ש־$M \cap C \lhd C$ מקסימלי (זוהי דוגמא נגדית למסקנה 3.3.24, אם מוותרים על ההנחה ש־M ראשוני). **הדרכה.** C הוא שדה, $M = 0$.

טענה 3.3.17 מראה שהחיתוך של אידיאל ראשוני של R עם C הוא לאידיאל ראשוני של C. נוכיח שכל אידיאל ראשוני של C מתקבל באופן כזה.

תרגיל 3.3.26 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.** הלמה של צורן.

טענה 3.3.27 יהי $S \subseteq R$ מונויד כפלי שאינו כולל את אפס. אם $P \lhd R$ מקסימלי ביחס לכך ש־$P \cap S = \emptyset$, אז P ראשוני.

הוכחה. נניח ש־$A, B \lhd R$ 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־$S \cap P = \emptyset$, $AB \not\subseteq P$. □

הערה 3.3.28 תהי $C \subseteq R$ הרחבה שלמה, ויהי $P \lhd C$ 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 3.3.29 תן דוגמא נגדית לגרסה החזקה הבאה של הערה 3.3.28: "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).

משפט 3.3.30 *נניח ש־R שלם מעל C. לכל $P \lhd C$ ראשוני קיים $Q \lhd R$ ראשוני כך ש־$Q \cap C = P$.*

הוכחה. נסמן $S = C - P$. קח אידיאל מקסימלי $S^{-1}Q$ של $S^{-1}R$. 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 3.3.21). 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.

□

3.4 שדות אינם אפיניים

3.4.1 פירוק ההרחבה

יהיו F שדה, ו־$R = F[a_1, \dots, a_n]$ אלגברה אפינית מעל F. נסמן $t = \operatorname{trdeg}_F(R)$, 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 3.4.1 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 $a_1, \dots, a_t$, ונסמן $R_0 = F[a_1, \dots, a_t]$. האברים $a_{t+1}, \dots, a_n$ אלגבריים מעל R_0. נסמן ב־s את מכפלת המקדמים המובילים של הפולינומים המינימליים שלהם, אז לאחר המיקום כל הפולינומים מתוקנים. □

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

משפט 3.4.2 (משפט הנורמליזציה של נתר) תהי $R = F[a_1, \dots, a_n]$ אלגברה אפינית מעל שדה F. אז קיימים $b_1, \dots, b_n \in R$ כך ש־$R = F[b_1, \dots, b_n]$, ו־R שלם מעל תת־החוג $R_0 = F[b_1, \dots, b_t]$ שהוא איזומורפי לחוג הפולינומים ב־t משתנים מעל F.

הוכחה. נסמן ב־t את גודל הקבוצה הבלתי־תלויה אלגברית המקסימלית בין היוצרים $a_1, \dots, a_n$. אפשר להניח $t < n$. ההוכחה באינדוקציה על n.

נראה שאפשר למצוא $c_1, \dots, c_{n-1} \in R$ כך שעבור $R_1 = F[c_1, \dots, c_{n-1}]$, $R = R_1[a_n]$ שלם מעל R_1, ואז, לפי הנחת האינדוקציה יש תת־חוג חופשי $R_0 \subseteq R_1$ כך ש־R_1 שלם מעל R_0, ואז R שלם מעל R_0 לפי תרגיל 3.3.8.

מכיוון ש־a_n אלגברי מעל $F[a_1, \dots, a_{n-1}]$, יש פולינום $f(\lambda_1, \dots, \lambda_n) = \sum \alpha_{i_1 \dots i_n} \lambda_1^{i_1} \cdots \lambda_n^{i_n} \in F[\lambda_1, \dots, \lambda_n]$, שאינו טריוויאלי במשתנה האחרון, כך ש־$f(a_1, \dots, a_n) = 0$. נבחר m גדול מהמעלה של f לפי כל λ_i, וניקח $c_i = a_i - a_n^{m^{n-i}}$. נתבונן בתת־החוג $R_1 = F[c_1, \dots, c_{n-1}]$ ובפולינום $h(\lambda) = f(c_1 + \lambda^{m^{n-1}}, \dots, c_{n-1} + \lambda^m, \lambda) \in R_1[\lambda]$, שהוא סכום הפולינומים $\alpha_{i_1 \dots i_n}(c_1 + \lambda^{m^{n-1}})^{i_1}(c_2 + \lambda^{m^{n-2}})^{i_2} \cdots (c_{n-1} + \lambda^m)^{i_{n-1}} \lambda^{i_n}$; כל אחד מאלו הוא 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. □

טענה 3.4.3 תהי $R = F[a_1, \dots, a_n]$ אלגברה אפינית שהיא שדה. אז R אלגברי מעל F.

הוכחה. לפי משפט 3.4.2, R הרחבה שלמה של חוג פולינומים $R_0 = F[a_1, \dots, a_t]$, כאשר $t = \operatorname{trdeg}(R)$. לפי משפט 3.3.30 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 3.4.4 ("משפט A") יהי F שדה סגור אלגברית. אלגברה אפינית $R = F[a_1, \dots, a_n]$ המכילה ממש את F אינה יכולה להיות שדה.

הוכחה. אחרת R אלגברי מעל F לפי מסקנה 3.4.3, ואז $R = F$ שהרי F סגור אלגברית. □

3.4.2 המשכת הומומורפיזמים

משפט 3.4.5 *תהי $R \subseteq C$ 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.*

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

הוכחה. נסמן $P = \mathrm{Ker}(\varphi)$, אז $C/P \cong \varphi(C) \subseteq K$ ולכן P ראשוני. לפי משפט 3.3.30, יש אידיאל ראשוני $Q \lhd R$ כך ש־$P = Q \cap C$. לפי תרגיל 3.3.18, $\bar{R} = R/Q$ 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 3.3.20, כלומר, $S^{-1}\bar{R}$ תחום שלמות אלגברי מעל F. לפי תרגיל 3.2.4 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 3.4.6 *יהי $F \subseteq K$ 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 3.4.5, אפשר להמשיך ל־$R \to \hat{K}$ כל הומומורפיזם $R_0 \to K$. □

מסקנה 3.4.7 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.

תרגיל 3.4.8 השתמש במסקנה 3.4.7 כדי לתת הוכחה אחרת למסקנה 3.4.3. **הדרכה**. לפי מסקנה 3.4.7 יש הומומורפיזם מ־R להרחבה אלגברית של F, וכל הומומורפיזם של שדות הוא שיכון.

כעת נציג הוכחה של משפט A (משפט 3.4.4) שאינה זקוקה לנורמליזציה.

תרגיל 3.4.9 $\varphi : R \to K$ הומומורפיזם עם $\varphi(s) \neq 0$, אז יש $\varphi : S^{-1}R \to K$ הממשיך את φ, כאשר $S = \langle s \rangle$. **הדרכה**. הגדר $\bar{\varphi}(s^{-i}r) = \varphi(s)^{-i}\varphi(r)$; קל לאשר ש־$\bar{\varphi}$ מוגדר היטב וממשיך את φ.

תרגיל 3.4.10 תן הוכחה למשפט 3.4.6, בהנחה ש־K אינסופי, שאינה משתמשת במשפט הנורמליזציה של נתר. **הדרכה**. לפי טענה 3.4.1, 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 3.1.4 יש הומומורפיזם $\varphi' : R_0 \to K$ כך ש־$\varphi'(s) \neq 0$. לפי תרגיל 3.4.9 יש המשכה $\varphi'' : \langle s \rangle^{-1} R_0 \to K$. מסיימים בעזרת משפט 3.4.5.

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*** $S \subseteq F^n$, $\mathcal{I}(S) = \{f \in R \colon (\forall s \in S) f(s) = 0\}$ ***- 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 $A \lhd R$ 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 $\sqrt{A} = A$.*

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 $A, B \lhd F[\lambda_1, \lambda_2]$.
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 $\sqrt{A \cap B} = \sqrt{A} \cap \sqrt{B}$. ***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 $x^{\max\{n,n'\}} \in A \cap B$.*

תרגיל 4.2.9 נניח ש־$A \subseteq B$, אז $\sqrt{B/A} = \sqrt{B}/A$.

תרגיל 4.2.10 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 4.2.11 הראה ש־$\sqrt{A} = \sqrt{A^n}$.

תרגיל 4.2.12 הראה ש־$\sqrt{AB} \subseteq \sqrt{A}\sqrt{B}$.

תרגיל 4.2.13 הראה שבתחום ראשי מתקיים $\sqrt{A+B} = \sqrt{A}+\sqrt{B}$.

תרגיל 4.2.14 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

הגדרה 4.2.15 *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 4.2.16 הראה ש־R ראשוני למחצה אם ורק אם $0 \lhd R$ אידיאל רדיקלי.

תרגיל 4.2.17 החוג R ראשוני למחצה אם ורק אם $x^2 = 0$ גורר $x = 0$. **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 $x^{n-1} = 0$.

טענה 4.2.18 יהי R חוג קומוטטיבי. אז $A \lhd R$ רדיקלי אם ורק אם R/A ראשוני למחצה.

הוכחה. נניח ש־A רדיקלי, ויהי $r + A \in R/A$; אם $(r+A)^m = 0$ אז $r^m + A = (r+A)^m = 0$ ולכן $r^m = A$ ולכן $r \in \sqrt{A} = A$, 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 $A = \sqrt{A}$. $\square$

תרגיל 4.2.19 כל תחום שלמות הוא ראשוני למחצה.

תרגיל 4.2.20 החוג $\mathbb{Z} \times \mathbb{Z}$ הוא ראשוני למחצה ואינו תחום שלמות.

תרגיל 4.2.21 מכפלה ישרה (לאו דווקא סופית) של שדות היא ראשונית למחצה.

תרגיל 4.2.22 אם $A \lhd R$ הוא ראשוני למחצה גם כאידיאל וגם כחוג (בלי יחידה), אז R ראשוני למחצה. **הדרכה**. יהי $I \lhd R$ ונניח $I^2 = 0 \subseteq A$, אז $I \subseteq A$ ולכן $I \lhd A$.

תרגיל 4.2.23 נניח ש־R ראשוני למחצה כחוג, ו־$A \lhd R$ הוא אידיאל ראשוני למחצה. אז גם A ראשוני למחצה כחוג. **הדרכה**. אם $I \lhd A$ ו־$I^2 = 0$ אז $(AIA)^2 = AIAIA \subseteq AI^2A = 0$ ולכן $AIA = 0$.

4.2.2 הרדיקל הראשוני

תרגיל 4.2.24 כל אידיאל ראשוני הוא רדיקלי. **הדרכה**. טענה 4.2.18 ותרגיל 4.2.19.

טענה 4.2.25 החיתוך של אידיאלים ראשוניים הוא רדיקלי.

הוכחה. יהיו P_i אידיאלים ראשוניים ($i \in I$, I קבוצת אינדקסים כלשהי), ויהי $A = \cap P_i$. 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 תרגיל 4.2.24. לכן $r \in \cap P_i = A$. $\square$

מסקנה 4.2.26 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 3.3.26, והוא ראשוני לפי טענה 3.3.27. $\square$

מסקנה 4.2.27 נניח ש־R ראשוני למחצה. לכל $0 \neq a \in R$ יש אידיאל ראשוני P כך ש־$a \notin P$.

הוכחה. זו מסקנה 4.2.26 כי כאשר R ראשוני למחצה, אם $a \neq 0$ אז $a^n \neq 0$ לכל n. □

הגדרה 4.2.28 *חיתוך כל האידיאלים הראשוניים בחוג R נקרא **הרדיקל הראשוני** של R, ומסמנים אותו ב־*$\mathrm{rad}(R)$. *(באופן כללי יותר, אם $I \lhd R$ אז חיתוך כל הראשוניים המכילים את I נקרא **הרדיקל של** I).*

מסקנה 4.2.29 הרדיקל של כל חוג הוא נילי (ולכן הרדיקל הראשוני נקרא גם **הרדיקל הנילי התחתון**).

מסקנה 4.2.30 בחוג (קומוטטיבי) ראשוני למחצה, $\mathrm{rad}(R) = 0$.

מסקנה 4.2.31 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 4.2.27 יש אידיאל ראשוני $\bar{P} = P/A \lhd R/A$ כך ש־$\bar{a} \notin \bar{P}$, אבל אז $a \notin P$ ומכיוון שגם P ראשוני, $a \notin A'$. לכן $A' = A$, כדרוש. □

מסקנה 4.2.32 בכל חוג קומוטטיבי R, $\mathrm{rad}(R) = \sqrt{0}$.

4.2.3 משפט האפסים של הילברט

תרגיל 4.2.33 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 4.2.34 לכל $A \lhd F[\lambda_1, \dots, \lambda_n]$ מתקיים $\sqrt{A} \subseteq \mathcal{I}(\mathcal{Z}(A))$. ***פתרון.*** *ברור ש־*$A \subseteq \mathcal{I}(\mathcal{Z}(A))$, *ולפי תרגיל 4.2.33, גם* $\sqrt{A} \subseteq \sqrt{\mathcal{I}(\mathcal{Z}(A))} = \mathcal{I}(\mathcal{Z}(A))$.

תרגיל 4.2.35 $\mathcal{Z}(A) = \mathcal{Z}(\sqrt{A})$. ***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 4.2.36 (Hilbert's Nullstellensatz) *נניח ש־F סגור אלגברית. לכל אידיאל* $A \lhd F[\lambda_1, \dots, \lambda_n]$ *מתקיים* $\sqrt{A} = \mathcal{I}(\mathcal{Z}(A))$.

הוכחה. הכיוון $\sqrt{A} \subseteq \mathcal{I}(\mathcal{Z}(A))$ הוא תרגיל 4.2.34. 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 4.2.31, יש אידיאל ראשוני $P \lhd F[\lambda_1, \dots, \lambda_n]$ כך ש־$f \notin P$. 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 3.4.7 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 בוקטור $x = (\psi(\lambda_1), \dots, \psi(\lambda_n)) \in F^n$. 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, אם נתונה מערכת משוואות, אפשר לקבל את כל המסקנות ממנה על־ידי פעולות חיבור וחיסור, כפל בפולינום כלשהו, והוצאת שורש.

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

כבר בתרגיל 4.1.5 ראינו שיש התאמה חד־חד־ערכית בין קבוצות אלגבריות לאידיאלים מהצורה $\mathcal{I}(S)$; אלא שתאור זה של האידיאלים אינו מספק, משום שהוא אינו מתייחס ישירות לאידיאל. משפט האפסים של הילברט משלים סוף־סוף את ההתאמה בין קבוצות אלגבריות לאידיאלים רדיקליים:

מסקנה 4.2.37 (מעל שדה סגור אלגברית) אידיאל הוא מהצורה $\mathcal{I}(S)$ אם ורק אם הוא רדיקלי.

הוכחה. תרגיל **4.2.33** ומשפט **4.2.36**. $\square$

תרגיל 4.2.38 נניח ש־F סגור אלגברית. אם $\mathcal{Z}(A) \subseteq \mathcal{Z}(f)$ אז $f \in \sqrt{A}$. ***פתרון***. לפי *משפט האפסים*, $f \in \mathcal{I}(\mathcal{Z}(f)) \subseteq \mathcal{I}(\mathcal{Z}(A)) = \sqrt{A}$.

מסקנה 4.2.39 נניח ש־F סגור אלגברית. אז לכל אידיאל $A \lhd F[\lambda_1,\dots,\lambda_n]$, $\mathcal{Z}(A) \neq \emptyset$. ◦

הוכחה. אחרת $1 \in F[\lambda_1,\dots,\lambda_n] = \mathcal{I}(\emptyset) = \mathcal{I}(\mathcal{Z}(A)) = \sqrt{A}$. $\square$

תרגיל 4.2.40 תן דוגמא נגדית למשפט האפסים של הילברט מעל שדה שאינו סגור אלגברית. היכן בדיוק נכשלת ההוכחה?

4.2.4 האידיאלים המקסימליים של חוג הפולינומים

עבור $a = (a_1,\dots,a_n) \in F^n$, נסמן $P_a = \langle \lambda_1 - a_1,\dots,\lambda_n - a_n\rangle \lhd R = F[\lambda_1,\dots,\lambda_n]$.

טענה 4.2.41 P_a הוא אידיאל מקסימלי, ו־$\mathcal{Z}(P_s) = \{s\}$.

הוכחה. המנה $F[\lambda_1,\dots,\lambda_n]/P_s \cong F$ על־ידי ההצבה $\lambda_i \mapsto s_i$. לכל נקודה $s' = (s'_1,\dots,s'_n)$, הצבת $\lambda_i \mapsto s'_i$ מאפסת את $\lambda_i - s_i$ אם ורק אם $s'_i = s_i$. $\square$

לכן כל נקודה היא קבוצה אלגברית.

טענה 4.2.42 נניח ש־F סגור אלגברית. אז כל אידיאל מקסימלי הוא מהצורה P_s. ◦

הוכחה. יהי P אידיאל מקסימלי. אז $S = \mathcal{Z}(P) \neq \emptyset$ לפי מסקנה **4.2.39**. נבחר $s \in S$, אז $P_s = \mathcal{I}(\{s\}) \subseteq \mathcal{I}(S) = \sqrt{P} = P$ לפי משפט האפסים, מש"ל. $\square$

תרגיל 4.2.43 מצא אידיאל מקסימלי של $\mathbb{R}[\lambda_1,\lambda_2]$ שאינו מהצורה $\langle \lambda_1 - a_1, \lambda_2 - a_2\rangle$.

4.3 קבוצות אלגבריות אי־פריקות

טענה 4.2.42 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 $A_1, A_2 \lhd F[\lambda_1, \dots, \lambda_n]$,

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

טענה 4.3.4 נניח ש־A רדיקלי. אז A אידיאל ראשוני אם ורק אם $\mathcal{Z}(A)$ 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 4.2.35 כל קבוצה אלגברית היא מהצורה $S_i = \mathcal{Z}(A_i)$ עבור A_i רדיקלי. לפי משפט האפסים $A = \sqrt{A} = \mathcal{I}(\mathcal{Z}(A)) = \mathcal{I}(\mathcal{Z}(A_1) \cup \mathcal{Z}(A_2)) = \mathcal{I}(\mathcal{Z}(A_1 \cap A_2)) = \sqrt{A_1 \cap A_2} = \sqrt{A_1} \cap \sqrt{A_2} = A_1 \cap A_2$, אבל מתרגיל 2.1.3 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־$A_1 A_2 \subseteq A$, ולפי תרגיל 4.3.3, $A_1 \cap A_2 \subseteq \sqrt{A}$. 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

תרגיל 4.3.5 הוכח את הגרסה החזקה של טענה 4.3.2.(2): $\cap \mathcal{Z}(A_i) = \mathcal{Z}(\sum A_i)$ לכל משפחה של אידיאלים A_i.

תרגיל 4.3.6 (דוגמא נגדית לכיוון $\Longrightarrow$ של טענה 4.3.4 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 טופולוגיית זריצקי

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

טענה 4.4.1 טופולוגיית זריצקי היא אכן טופולוגיה.

הוכחה. **יש להוכיח שהקבוצה הריקה $\mathcal{Z}(\langle 1\rangle) = \emptyset$ 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 4.3.5.** □

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

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

תרגיל 4.4.4 כל תת־קבוצה סגורה של F^n (עם טופולוגיית זריצקי) היא קומפקטית. **הדרכה.** כל אידיאל של $F[\lambda_1,\dots,\lambda_n]$ נוצר סופית.

תרגיל 4.4.5 טופולוגיית זריצקי מקיימת את אקסיומת ההפרדה T_1 (כל נקודה היא קבוצה סגורה), אבל לא את אקסיומת ההפרדה T_2 (כל שתי נקודות אפשר להפריד בקבוצות פתוחות זרות).

4.4.1 הספקטרום

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

הגדרה 4.4.6 *לכל אידיאל $I \lhd R$, נסמן* $\mathcal{V}(I) = \{P \in \operatorname{spec}(R) :\ I \subseteq P\}$.

תרגיל 4.4.7 $\mathcal{V}(I) = \mathcal{V}(\sqrt{I})$.

תרגיל 4.4.8
1. $\mathcal{V}(0) = \operatorname{spec}(R)$;
2. $\mathcal{V}(R) = \emptyset$;
3. $\cap \mathcal{V}(I_i) = \mathcal{V}(\sum I_i)$;
4. $\mathcal{V}(I_1) \cup \mathcal{V}(I_2) = \mathcal{V}(I_1 I_2)$.

תרגיל 4.4.9 הקבוצות $\mathcal{V}(I)$ $(I \lhd R)$ מהוות אוסף הקבוצות הסגורות בטופולוגיה על $\operatorname{spec}(R)$. הטופולוגיה נקראת **טופולוגיית זריצקי** של הספקטרום (בניגוד לטופולוגיית זריצקי של המרחב האפיני, מתת־הסעיף הקודם). **הדרכה.** זהו תרגיל 4.4.8.

תרגיל 4.4.10 הקבוצות $S_a = \{P \in \operatorname{spec}(R) :\ a \notin P\}$ מהוות בסיס לטופולוגיה על $\operatorname{spec}(R)$.

תרגיל 4.4.11 אם $\mathcal{V}(A) = \emptyset$ אז $A = R$.

טענה 4.4.12 הספקטרום קומפקטי תחת טופולוגיית זריצקי.

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

תרגיל 4.4.13 טופולוגיית זריצקי של הספקטרום מקיימת את אקסיומת ההפרדה T_0 (מכל שתי נקודות, אפשר להפריד אחת מהן מן השניה על־ידי קבוצה פתוחה).

תרגיל 4.4.14 לכל אידיאל $I \lhd R$, $\mathrm{spec}(R/I)$ הומיאומורפי ל־$\mathcal{V}(I)$.

פרק 5

מימד 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 מממד $n-t$. באופן כללי יותר, אנו מעוניינים לבנות התאמה בין המימד של קבוצה אלגברית S, למימד של האלגברה האפינית $F[\lambda_1, \dots, \lambda_n]/\mathcal{I}(S)$. רעיון זה מוביל לפיתוח של מושג המימד עבור חוגים כלליים.

5.1 מימד קרול

הגדרה 5.1.1 ***יהי R חוג. מימד קרול של החוג הוא n המקסימלי כך שקיימת שרשרת של אידיאלים ראשוניים $P_0 \subset P_1 \subset \dots \subset P_n$ 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 $0 \subset \langle \lambda_1 \rangle \subset \dots \subset \langle \lambda_1, \dots, \lambda_n \rangle$ שרשרת של אידיאלים ראשוניים. ◦

תרגיל 5.1.4 לכל אידיאל $I \lhd R$, $\dim(R/I) \leq \dim(R)$. **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 $\dots \subset Ra^3 \subset Ra^2 \subset Ra$, בסתירה לארטיניות. □

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

הוכחה. *יהי* $P \lhd R$ אידיאל ראשוני, אז R/P תחום שלמות ארטיני (תרגיל 1.3.14), 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 $I \lhd R$ 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.

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 4.2.32).

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

5.3 חוגים ממימד אפס

למה 5.3.1 $N \lhd R$ רדיקלי, $N \subset A, B$, $AB \subseteq N$. אז $\sqrt{A} \cap \sqrt{B} = N$.

הוכחה. לפי תרגיל 4.3.3, $N \subseteq A \cap B \subseteq \sqrt{A} \cap \sqrt{B} \subseteq \sqrt{N} = N$. □

משפט 5.3.2 *נניח ש־R נתרי. כל אידיאל רדיקלי של R הוא חיתוך מספר סופי של אידיאלים ראשוניים.*

הוכחה. יהי N אידיאל רדיקלי מקסימלי שאינו חיתוך של מספר סופי של ראשוניים. בפרט N אינו ראשוני, ולכן יש $A, B \supset N$ כך ש־$AB \subseteq N$. לפי המקסימליות של N, כל אחד מהאידיאלים $\sqrt{A}, \sqrt{B}$ 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. □

טענה 5.3.3 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.

(בטענה 8.4.10 נוכיח טענה זו עבור חוגים לא קומוטטיביים.) □

טענה 5.3.4 יהי R חוג קומוטטיבי ראשוני למחצה. התנאים הבאים שקולים:

1. R נתרי בעל מימד 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 5.3.2), ואם R ארטיני יש לו מספר סופי של ראשוניים, לפי טענה 5.3.3, וחיתוכם הוא $\sqrt{0}$ לפי מסקנה 4.2.32. בכל מקרה אפשר לכתוב $0 = \sqrt{0} = P_1 \cap \cdots \cap P_t$ כאשר $P_i \lhd R$ ראשוניים. המימד 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, וראשוני למחצה לפי תרגיל 4.2.21. □

משפט 5.3.5 *יהי R חוג נתרי ממימד 0. אז R ארטיני.*

הוכחה. נסמן $N = \sqrt{0}$. זהו אידיאל רדיקלי, ולכן R/N ראשוני למחצה (טענה 4.2.18), נתרי כחוג מנה של R, ובעל מימד אפס (תרגיל 5.1.4). לפי משפט 5.3.4, R/N ארטיני.

לפי טענה 5.2.11 ותרגיל 5.2.7, N אידיאל נילפוטנטי, ולכן קיים n כך ש־$N^n = 0$. לכל $i < n$, $N^i \lhd R$ נוצר סופית כאידיאל, ולכן גם כמודול מעל R. מכאן שגם המנה N^i/N^{i+1} נוצרת סופית כמודול מעל R, ו־N מאפס אותה. לפי תרגיל 1.1.8, 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 1.3.8) 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 1.3.8, R ארטיני. □

מסקנה 5.3.6 יהי R חוג אפיני. אז R ארטיני אם ורק אם יש לו מימד 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 $P \lhd R$ נקרא **מינימלי** אם הוא אינו מכיל אף אידיאל ראשוני $\neq 0$.*
*יהי $0 \neq I \lhd R$. אידיאל ראשוני P המכיל את I הוא **מינימלי מעל** I אם אין ראשוני $P_0 \subseteq P$ כך ש־$I \subseteq P_0$. אם $I = Ra$, אומרים ש־P **מינימלי מעל** a.*

תרגיל 5.4.2 בכל חוג, לכל $I \lhd R$ יש אידיאל ראשוני מינימלי המכיל את I. **הדרכה.** I מוכל באידיאל מקסימלי, שהוא ראשוני, והאידיאלים הראשוניים המכילים את I מקיימים את תנאי המינימום.

תרגיל 5.4.3 לכל $k \geq 1$, ראשוני P הוא מינימלי מעל a אם ורק אם הוא מינימלי מעל a^k.

תרגיל 5.4.4 כל אידיאל ראשוני ראשי הוא מינימלי מעל איבר מתאים.

תרגיל 5.4.5 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 2.1.5). 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־$\pi \mid p$, בהכרח $P = R\pi = Rp \subseteq Q$ ולכן $Q = P$.

תרגיל 5.4.6 יהי R תחום שלמות, ויהיו $N < M$ תת־מודולים 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 5.4.7 *(משפט האידיאל הראשי) יהי R תחום שלמות נתרי. אם P מינימלי מעל a אז הוא מינימלי.*

הוכחה. *נניח שלא. אז קיים אידיאל ראשוני $0 \subset P_1 \subset P$. נבצע מיקום ב־P, כלומר, ניקח $S = R - P$, ונעבור לשרשרת $0 \subset P_1' \subset P' \lhd R'$, כאשר $P_1' = S^{-1}P_1$, $P' = S^{-1}P$, ו־$R' = S^{-1}R$. האידאל 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.*

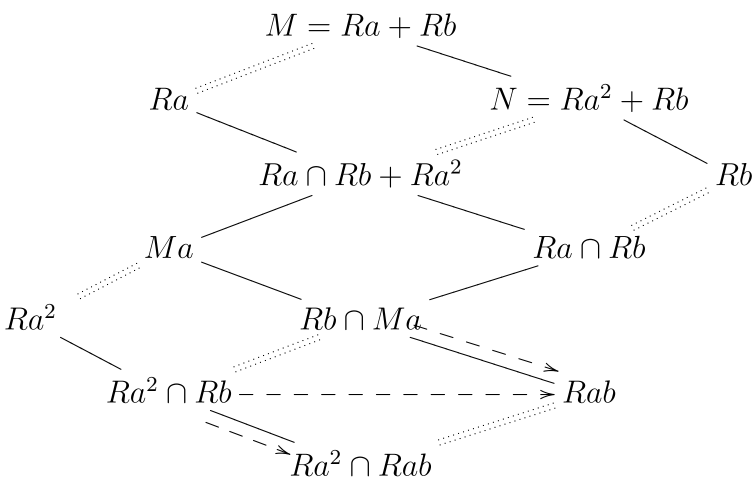
נתבונן בחוג המנה R/Ra^2, שהוא נתרי. כל אידיאל ראשוני ב־R/Ra^2 הוא מהצורה $\tilde{P}/Ra^2$ כאשר $\tilde{P} \lhd R$ ראשוני המכיל את a^2, ולכן גם את a. בנוסף, $\tilde{P} \subseteq P$ מכיוון ש־P מקסימלי יחיד. לא יתכן ש־$\tilde{P} \subset P$, כי P מינימלי מעל a, ומכאן ש־$\tilde{P} = P$. הראינו שאין ב־R/Ra^2 אידיאלים ראשוניים פרט ל־P/Ra^2, ולכן $\dim(R/Ra^2) = 0$. לפי משפט 5.3.5, R/Ra^2 ארטיני.

יהי $0 \neq b \in P_1$ איבר כלשהו. 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 5.4.3, P מינימלי מעל a', ולכן אפשר להחליף a ב־a' ולקבל את התנאי

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

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 $M = Ra + Rb$.
נסמן $N = Rb + Ma = Ra^2 + Rb$. לפי תרגיל 5.4.6 (פעמיים),

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



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

וגם $M/Ra \cong Ma/Ra^2$. **כעת,** M/Ra^2 **הוא מודול מעל** R/Ra^2**, שהוא ארטיני ונתרי, ולכן יש ל־**M/Ra^2 **סדרות הרכב. לפי תרגיל 1.2.9,**

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

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 5.4.8 ***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 5.4.9 *יהי* R *קומוטטיבי נתרי. לכל אידיאל ראשוני* P *שהוא מינימלי מעל איבר* $a \neq 0$*, מתקיים* $\mathrm{ht}(P) \leq 1$.

תרגיל 5.4.10 המימד $\dim(R)$ שווה לסופרימום הגבהים של האידיאלים המקסימליים. ∘
הדרכה. כל שרשרת של אידיאלים ראשוניים אפשר להמשיך כך שהיא מסתיימת באידיאל מקסימלי.

למה 5.4.11 יהי R חוג נתרי קומוטטיבי. תהי $P = P_0 \supset P_1 \supset \cdots \supset P_{t-1} \supset P_t$ שרשרת של אידיאלים ראשוניים, ויהי $b \in P$. אז יש שרשרת $P = P_0 \supset P_1' \supset \cdots \supset P_{t-1}' \supset P_t'$, 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 5.4.12 (*משפט האידיאל הראשי המוכלל*) *יהי R קומוטטיבי נתרי. אם ראשוני P הוא מינימלי מעל $B = Ra_1 + \cdots + Ra_t$, אז $\operatorname{ht}(P) \leq t$.*

הוכחה. באינדוקציה על t, כאשר המקרה $t = 1$ הוא משפט האידיאל הראשי, 5.4.7. נניח שקיימת שרשרת ראשוניים $P = P_0 \supset P_1 \supset \cdots \supset P_t \supset P_{t+1}$. לפי למה 5.4.11 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 $\operatorname{ht}(\bar{P}) \leq t-1$, אבל $P/Ra_t \supset P_1/Ra_t \supset \cdots \supset P_t/Ra_t$ היא שרשרת של ראשוניים מאורך t, וזו סתירה. □

מסקנה 5.4.13 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, $\operatorname{ht}(P) \leq t$. □

מסקנה 5.4.14 בחוג נתרי קומוטטיבי אין שרשרת יורדת אינסופית של אידיאלים ראשוניים.
הדרכה. מסקנה 5.4.13.

מסקנה 5.4.15 יהי R חוג נתרי מקומי, אז יש לו מימד סופי.

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

מסקנה 5.4.16 יהי F שדה סגור אלגברית. אז $\dim(F[\lambda_1, \ldots, \lambda_n]) = n$.

הוכחה. לפי טענה 4.2.42, האידיאלים המקסימליים של R נוצרים על־ידי n איברים, וממשפט 5.4.12 נובע שגובהם אינו עולה על n. מאידך בתרגיל 5.1.3 בנינו שרשרת אידיאלים ראשוניים באורך n. המסקנה נובעת לפי תרגיל 5.4.10. □

הערה 5.4.17 מסקנה 5.4.16 נכונה לכל שדה. ראה הוכחה קצרה ב־`A Short Proof for the Krull Dimension of a Polynomial Ring`, *Thierry Coquand and Henri Lombardi*.

הערה 5.4.18 *Nagata* מצא ב־*1962* חוג נתרי ממימד אינסופי.

הערה 5.4.19 בדרך כלל אין קשר בין מספר היוצרים למימד. למשל, הראה שאת האידיאל $I = \left\langle \lambda_1^n, \lambda_1^{n-1}\lambda_2, \ldots, \lambda_2^n \right\rangle \triangleleft F[\lambda_1, \lambda_2]$ אי אפשר ליצור בפחות מ־$n+1$ איברים. מהו $\sqrt{I}$? מצא אידיאל ראשוני מינימלי מעל I.

5.5 אידיאלים ראשוניים בהרחבות

תהי $C \subseteq R$ הרחבה של שדות. אומרים שראשוני $Q \lhd R$ **נמצא מעל** $P \lhd C$ אם $P = Q \cap C$. בטענה 3.3.17 הראינו שבמקרה זה גם P ראשוני.

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

הערה 5.5.2 כל הרחבה שלמה $C \subseteq R$ מקיימת את התכונה LO (משפט 3.3.30).

טענה 5.5.3 כל הרחבה שלמה $C \subseteq R$ מקיימת את התכונה GU.

הוכחה. יהי Q ראשוני מעל P, ויהי $P \subseteq P_1$. לפי תרגיל 3.3.18, $\bar{R} = R/Q$ הרחבה שלמה של $\bar{C} = (C+Q)/Q \cong C/P$, ולפי LO בהרחבה זו, יש ראשוני $Q' \lhd R/Q$ שנמצא מעל $P_1' = P_1/P$; נכתוב $Q' = Q_1/Q$, אז Q_1 ראשוני המכיל את Q; אידיאל זה נמצא מעל P_1 משום ש־$P_1/Q = P_1' = Q' \cap \bar{C} = Q_1/Q \cap (C+Q)/Q = (Q_1 \cap C + Q)/Q = (Q_1 \cap C)/Q$, ולכן $P_1 = Q_1 \cap C$. □

הערה 5.5.4 אם $C \subseteq R$ תחומי שלמות, אז מהתכונה GU נובע LO (ראה טענה 5.5.5).

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

טענה 5.5.5 בכל הרחבה $C \subseteq R$ של חוגים קומוטטיביים, מהתכונה GU נובע LO.

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

טענה 5.5.6 אם $C \subseteq R$ קומוטטיביים וההרחבה מקיימת INC, אז $\operatorname{ht}(Q) \leq \operatorname{ht}(P)$ לכל Q שמעל P.

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

הערה 5.5.7 יהי $S \subseteq R$ מונויד, $P \lhd R$ אידיאל שאינו נחתך עם S. אז $\operatorname{ht}(S^{-1}P) = \operatorname{ht}(P)$.

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

הערה 5.5.8 כל הרחבה שלמה $C \subseteq R$ מקיימת את התכונה INC.

הוכחה. אחרת יש אידיאלים ראשוניים $Q \subset Q'$ של R הנמצאים מעל $P \lhd C$. לפי תרגיל 3.3.18, R/Q שלם (ובפרט אלגברי) מעל $(C+Q)/Q \cong C/P$, ולפי טענה 3.2.3, $0 \neq Q'/Q \lhd R/Q$ נחתך עם $(C+Q)/Q$, בסתירה להנחה ש־$Q' \cap C = P$. □

טענה 5.5.9 בהרחבה $R \subseteq C$ המקיימת LO ו־GU, לכל $P \lhd C$ 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 $Q_t \lhd R$ הנמצא מעל P_t לפי LO, ולכל $i = t-1, \dots, 1, 0$ יש ראשוני Q_i מעל P_i המכיל את Q_{i+1} לפי GU. □

טענה 5.5.10 אם ההרחבה $R \subseteq C$ מקיימת GU, LO ו־INC אז לכל $P \lhd C$ יש Q מעליו כך ש־$\mathrm{ht}(P) = \mathrm{ht}(Q)$.

הוכחה. טענות 5.5.6 ו־5.5.9. □

טענה 5.5.11 אם ההרחבה $R \subseteq C$ מקיימת GU, LO ו־INC אז $\dim(R) = \dim(C)$.

הוכחה. $\dim(C) = \sup \mathrm{ht}(P) \leq \sup \mathrm{ht}(Q) = \dim(R)$ לפי טענה 5.5.10, והכיוון ההפוך נובע מטענה 5.5.6. □

מסקנה 5.5.12 אם $R \subseteq C$ 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 3.4.2, 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 5.4.16, $\dim(R) = \dim(R_0) = \mathrm{trdeg}_F(R)$, כשהשוויון האחרון הוא מסקנה 5.4.16. □

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 $R \subseteq C$ הרחבה שלמה של תחומי שלמות, כאשר C נורמלי. אז הפולינום המינימלי 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־$f \mid g$ מעל F, אז $f \mid g$ 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 $g = f h_0'$. □

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 $R = \mathbb{Z}[a \mid a^2 = 0, 2a = 0]$.

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 **3.3.27**, 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 $s = \sum_{j=1}^{\ell} p_j r_j$ עבור $p_j \in P$ ו־$r_j \in R$, נוכל לבחור $M = C[r_1, \dots, r_\ell]$, ואז $sM \subseteq \sum p_j r_j M \subseteq \sum p_j M \subseteq PM$. מכאן נובע, לפי הערה **3.3.3**, 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־$f \mid g$ מעל שדה השברים F, זה נכון גם ב־$C[\lambda]$ לפי למה **5.5.17**, ולכן גם בחוג המנה C/P, שם $\bar{f} \mid \bar{g} = \lambda^m$, 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 $0 = f(s) = f(cr) = c^n r^n + \sum d_i c^i r^i$, ולכן r שורש של $c^n \lambda^n + \sum d_i c^i \lambda^i$, וגם של $c^n h(\lambda)$. 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. $\square$

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 **2.1.5**. $\square$

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

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

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**. $\square$

פרק 6

ערכים מוחלטים

6.1 הגדרה ודוגמאות

הגדרה 6.1.1 *ערך מוחלט על שדה F הוא פונקציה $F \to [0,\infty] \subseteq \mathbb{R}$, $a \mapsto |a|$, 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**

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

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** $|\cdot|'$**.** $(\mathbf{1}) \Longrightarrow (\mathbf{2})$**: הערה 6.2.4.** $(\mathbf{2}) \Longrightarrow (\mathbf{3})$**: נניח ש־**$|a| < 1$**, אז הסדרה** a^n **מתכנסת ל־0 לפי** τ**, ולפי ההנחה גם לפי** τ'**. לכן לא יתכן** $|a|' \ge 1$**.** $(\mathbf{3}) \Longrightarrow (\mathbf{5})$**: נבחר** $b \in F$ **כך ש־**$|b| < 1$**, ואז גם** $|b|' < 1$**. נניח ש־**$|a| = 1$**. לכל** n **מתקיים** $|a^nb| < 1$**, ולפי ההנחה גם** $|a^nb|' < 1$**. מכאן ש־**$|a|' < |b|'^{-1/n}$**, ולכן** $|a|' \le 1$**. אותו נימוק תקף גם ל־**a^{-1}**, ולכן** $|a|' = 1$**.** $(\mathbf{5}) \Longrightarrow (\mathbf{4})$**: טריוויאלי.** $(\mathbf{4}) \Longrightarrow (\mathbf{3})$**: יש** $c \in F^\times$ **כך ש־**$|c|' < 1$**, ואז לכל** a**, אם** $|a| < 1$ **אז** $|a^nc^{-1}| \le 1$ **עבור** n **גדול מספיק, ולפי ההנחה גם** $|a^nc^{-1}|' \le 1$**, כך ש־**$|a|'^n \le |c|' < 1$**, ואז** $|a|' < 1$**.** $(\mathbf{5}) \Longrightarrow (\mathbf{6})$**: אם** $|a| > 1$ **אז** $|a^{-1}| < 1$ **ו־**$|a^{-1}|' < 1$**, כך ש־**$|a|' > 1$**.** $(\mathbf{6}) \Longrightarrow (\mathbf{1})$**: 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** $|a^{-n}b^m| = |a|^{-n}|b|^m = |b|^{m-sn} > 1$**, אם ורק אם** $|a^{-n}b^m|' = |a|'^{-n}|b|'^m = |b|'^{m-tn} > 1$**, 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־$(3) \Longleftarrow (2) \Longleftarrow (1)$. נניח שקיים M כך ש־$|n| \leq C$ 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. □

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 $\nu(a_1+\dots+a_n)=\min\{\nu(a_1),\dots,\nu(a_n)\}$.

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 $\nu\colon F\to\Gamma\cup\{-\infty\}$ 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 $0\neq a\in F$, $0\geq\nu(a)$ 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. □

תחום שלמות מקיים את **תכונת בזו** אם כל אידיאל נוצר סופית הוא ראשי.

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)) $\Longleftarrow$ ((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)) $\Longleftarrow$ ((3)): יהיו $I,J \lhd R$ אידאלים כך ש־$I \not\subseteq J$. 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)) $\Longleftarrow$ ((4)): לפי ההנחה יש אידיאל מקסימלי יחיד. מבין כל קבוצה סופית אידיאלים ראשיים, אחד מהם מכיל את כל האחרים, ולכן סכומם שווה לו.

((4)) $\Longleftarrow$ ((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 $R = \{a\colon aR^\times \supseteq R^\times\}$. $\square$

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 3.3.17, $P \lhd \mathbb{Z}$ 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 $\nu(\cdot) \sim \nu_p(\cdot)$. $\square$

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.** $|\prod_i p_i^{n_i}|_p = p_i^{-n_i}$ 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.

חלק II

אלגברה לא קומוטטיבית

החלק הזה מכסה את יסודות תורת המבנה של חוגים לא קומוטטיביים, בהיקף הנדרש לפיתוח מלא של תורת ההצגות לחבורות סופיות. נפתח תורה של מודולים פריקים לחלוטין באופן שיאפשר להוכיח את משפט הצפיפות הכללי. משפט זה מאפשר לשכן חוג שיש לו מודול פריק לחלוטין, באופן צפוף, בחוג אנדומורפיזמים של המודול. מכאן נוכל להוכיח שחוג ארטיני פרימיטיבי הוא חוג מטריצות מעל חוג חילוק. בין החוגים הארטיניים (בפרט, בין האלגברות ממימד סופי), כל חוג ראשוני הוא פשוט, וכך מתקבל משפט המבנה של ודרברן־ארטין: חוג ארטיני ראשוני הוא חוג מטריצות על מחוג עם חילוק.

לחוג ארטיני יש מספר סופי של אידיאלים ראשוניים, החיתוך שלהם (שהוא הרדיקל של החוג) הוא נילפוטנטי, והמנה ביחס אליו היא חוג פשוט למחצה. תכונות אלו מאפשרות להוכיח את משפט הופקינס־לויצקי: כל חוג ארטיני הוא נתרי, ולכן למודולים מעליו יש אורך סופי. כעת תהי G חבורה סופית, ויהי F שדה ממאפיין זר ל־$|G|$. אז אלגברת החבורה $F[G]$ היא פשוטה למחצה וארטינית, ולכן מתפרקת לסכום ישר של חוגי מטריצות. הפירוק הזה מתניע את תורת ההצגות, ומאפשר להוכיח למשל את המשפט של ברנסייד, שלסדר של חבורה פשוטה יש לפחות שלושה גורמים ראשוניים.

פרק 7

מבנה של מודולים

7.1 מושגי יסוד בתורת המודולים

7.1.1 חוגי מטריצות

במהלך הקורס נראה שאלגברות פשוטות מסויימות אפשר להציג כאלגברות מטריצות מעל חוגים עם חילוק. משום כך חשוב להכיר את התכונות של אלגברת המטריצות באופן כללי.

טענה 7.1.1 יהי R חוג. המרְכָּז של $\mathrm{M}_n(R)$ הוא אוסף המטריצות הסקלריות עם מקדמים ב־$\mathrm{Z}(R)$.

טענה 7.1.2 יש התאמה בין אידיאלים של $\mathrm{M}_n(R)$ לבין אידיאלים של R: לכל $A \lhd R$, $\mathrm{M}_n(A) \lhd \mathrm{M}_n(R)$, וכל אידיאל של $\mathrm{M}_n(R)$ הוא מהצורה $\mathrm{M}_n(A)$ עבור $A \lhd R$ מתאים.

מסקנה 7.1.3 כל חוג מטריצות מעל חוג פשוט, הוא פשוט בעצמו.

תרגיל 7.1.4 קבע לגבי החוג $S = \begin{pmatrix} \mathbb{Z} & \mathbb{Q} \\ 0 & \mathbb{Z} \end{pmatrix}$ האם הוא ארטיני שמאלי; האם הוא ארטיני ימני. כך גם עבור $S' = \begin{pmatrix} \mathbb{Q} & \mathbb{Q} \\ 0 & \mathbb{Z} \end{pmatrix}$ (ראה גם תרגיל 7.3.2).

איך מזהים חוג מטריצות, באופן כללי? יהי T חוג. אברים $e_{ij} \in T$ $(i, j = 1, \dots, n)$ נקראים מערכת של **יחידות מטריצות** אם $e_{ij}e_{k\ell} = \delta_{jk}e_{i\ell}$, ו־$e_{11} + \cdots + e_{nn} = 1$. יחידות המטריצות הסטנדרטיות בחוג $T = \mathrm{M}_n(R)$ הן אכן מערכת כזו, ושם אפשר לכתוב $T = \sum Re_{ij} = \sum e_{ij}R$.

טענה 7.1.5 יהי T חוג שיש בו מערכת של יחידות מטריצות, $\{\epsilon_{ij}\}$. אז $R = \epsilon_{11}T\epsilon_{11}$ הוא תת־חוג, ו־$T \cong \mathrm{M}_n(R)$. ◦

הוכחה. R סגור לכפל משום ש־$R^2 = (\epsilon_{11}T\epsilon_{11})^2 = \epsilon_{11}T\epsilon_{11}^2T\epsilon_{11} \subseteq \epsilon_{11}T\epsilon_{11}$. נסמן ב־$e_{ij}$ את יחידות המטריצות הסטנדרטיות של $\mathrm{M}_n(R) = \sum Re_{ij} = \sum e_{ij}R$, ונגדיר העתקה $\psi : T \rightarrow \mathrm{M}_n(R)$

לפי $t \mapsto \sum_{ij} (\epsilon_{1i} t \epsilon_{j1}) e_{ij}$**. זו פונקציה כפלית כי**

$$\begin{aligned}\psi(t)\psi(s) &= \sum_{ij} (\epsilon_{1i} t \epsilon_{j1}) e_{ij} \cdot \sum_{i'j'} (\epsilon_{1i'} s \epsilon_{j'1}) e_{i'j'} \\ &= \sum_{i,k} \left(\sum_j \epsilon_{1i} t \epsilon_{j1} \epsilon_{1j} s \epsilon_{k1} \right) e_{ik} \\ &= \sum_{i,k} (\epsilon_{1i} t s \epsilon_{k1})\, e_{ik} = \psi(ts).\end{aligned}$$

כעת, לכל קבוצת איברים $t_{ij} \in T$,

$$\psi(\sum_{ij} \epsilon_{i1} t_{ij} \epsilon_{1j}) = \sum_{i,j,i',j'} (\epsilon_{1i'} \epsilon_{i1} t_{ij} \epsilon_{1j} \epsilon_{j'1}) e_{i'j'} = \sum_{i,j} (\epsilon_{11} t_{ij} \epsilon_{11}) e_{ij},$$

וזהו האיבר הכללי של $\mathrm{M}_n(R)$**. לכן הפונקציה על. לבסוף, אם** $\psi(t) = 0$ **אז** $\epsilon_{i1} t \epsilon_{1j} = 0$ **לכל** i, j**, ואז גם** $t = (\sum_i \epsilon_{ii}) t (\sum_j \epsilon_{jj}) = \sum_{ij} \epsilon_{i1} (\epsilon_{1i} t \epsilon_{j1}) \epsilon_{1j} = 0$**. לכן** $\psi : T \to \mathrm{M}_n(R)$ **איזומורפיזם.**$\Box$

תרגיל 7.1.6 נניח ש־$a, b \in R$ מקיימים $ab = 1$ אבל $e = ba \neq 1$ (חוג שאין בו זוג כזה נקרא **דדקינד־סופי**, בשל ההגדרה של דדקינד לקבוצות סופיות.) הראה ש־$e_{ij} = b^i(1-e)a^j$ היא מערכת אינסופית של יחידות מטריצות ושכולם שונים מאפס. בפרט, R מכיל סכום ישר אינסופי של אידיאלים שמאליים, $\oplus R e_{ii}$.

7.1.2 חוגי אנדומורפיזמים

בחלק הקודם של הקורס הגדרנו **מודול** כחבורה אבלית שהחוג פועל עליה על־ידי כפל $r : x \mapsto rx$. כלומר, הפעולה $(r, x) \mapsto rx$ אדיטיבית בשני הרכיבים, ובנוסף $1x = x$ ו־$(rr')x = r(r'x)$. מכיוון שהחוגים היו בדרך כלל קומוטטיביים, לא הרגשנו שזו למעשה ההגדרה של **מודול שמאלי**. אפשר להגדיר **מודול ימני** באותו אופן, אלא שהפעם הפעולה היא $r : x \mapsto xr$, והתנאי הוא $x(rr') = (xr)r'$, במקום $(rr')x = r(r'x)$. כדי להבדיל בין שתי ההגדרות, נסמן ב־${}_RM$ מודול שמאלי, וב־M_R מודול ימני.

הגדרה 7.1.7 *יהיו* ${}_RM, {}_RN$ *מודולים מעל חוג* R*. אז* $\mathrm{Hom}_R(M, N)$ *הוא אוסף ההומומורפיזמים* $f : M \to N$*, כלומר פונקציות אדיטיביות המקיימות* $f(rx) = rf(x)$ *לכל* $r \in R$ *ו־*$x \in M$*. זוהי חבורה אבלית עם הפעולה* $(f+g)(x) = f(x) + g(x)$.

אותה הגדרה תקפה גם עבור מודולים ימניים M_R, N_R*: אז* $\mathrm{Hom}_R(M, N)$ *הוא אוסף ההומומורפיזמים* $f : M \to N$*, כלומר פונקציות אדיטיביות המקיימות* $f(xr) = f(x)r$ *לכל* $r \in R$ *ו־*$x \in M$.

נעיר שכאשר R אינו קומוטטיבי, אין דרך טבעית להפוך את $\mathrm{Hom}(M, N)$ למודול מעל R, משום ש־$x \mapsto af(x)$ אינו הומומורפיזם של מודולים (ו־$f(x)a$ אינו מוגדר).

הגדרה 7.1.8 *יהי* ${}_RM$ *מודול שמאלי מעל* R*, מסמנים* $\mathrm{End}({}_RM) = \mathrm{Hom}_R(M, M)$*. זהו חוג, כאשר* $fg = g \circ f$ *היא פעולת ההרכבה ההפוכה.*

בדומה לזה, אם M_R *מודול ימני, אז* $\mathrm{End}(M_R) = \mathrm{Hom}_R(M, M)$*. כאן פעולת הכפל היא ההרכבה הרגילה* $fg = f \circ g$.

הסיבה להגדרת הכפל דווקא באופן הזה תתברר בתת־סעיף 7.3.1.

תרגיל 7.1.9 בדוק ש־$\operatorname{End}(M)$ סגור לכפל כאשר M מודול שמאלי או ימני.

תרגיל 7.1.10 לכל חוג (עם יחידה) R, $R \cong \operatorname{End}(R_R) \cong \operatorname{End}({}_RR)$.

הגדרה 7.1.11 *יהי R חוג.* ***החוג המנוגד*** *R^{op} הוא החוג עם אותה קבוצת אברים ואותה פעולת חיבור, וכפל בסדר הפוך: $x^{\mathrm{op}}y^{\mathrm{op}} = (yx)^{\mathrm{op}}$.*

הערה 7.1.12 $(R^{op})^{op} = R$, ואם R קומוטטיבי אז $R = R^{op}$. אבל בדרך כלל החוגים R, R^{op} אינם איזומורפיים. למשל, נתבונן בחוג $R = \begin{pmatrix} \mathbb{Q} & \mathbb{Q} \\ 0 & \mathbb{Z} \end{pmatrix}$. לכל איבר נילפוטנטי t, האידיאל השמאלי Rt איזומורפי, כחבורה חיבורית, ל־$\mathbb{Q}$, ואילו האידיאל הימני tR איזומורפי ל־$\mathbb{Z}$. ב־R^{op} המצב הפוך, כמובן, ולכן $R \not\cong R^{op}$.

החוג המנוגד מספק דרך טכנית לעבור בין מודולים שמאליים וימניים ומראה שהתאוריות סימטריות זו לזו, משום שכל מודול ימני מעל R אפשר לראות כמודול שמאלי מעל R^{op} (על־ידי הפעולה $x \cdot r = r^{\mathrm{op}}x$, שהרי $x(rr') = (rr')^{\mathrm{op}}x = r'^{\mathrm{op}}(r^{\mathrm{op}}x) = r'^{\mathrm{op}}(xr) = (xr)r'$), ולהיפך.

תרגיל 7.1.13 יהי M מודול שמאלי מעל החוג R. אז $\operatorname{End}({}_RM)^{\mathrm{op}} = \operatorname{End}(M_{R^{\mathrm{op}}})$.

7.1.3 מטריצות ודרגה של מודול

אחד הכלים היסודיים באלגברה לינארית, שאינה אלא תורת המודולים מעל שדה כללי, הוא קיומו של בסיס לכל מרחב וקטורי. קבוצה $X \subseteq M$ היא **בסיס** אם לכל איבר $v \in M$ יש הצגה יחידה כסכום $\alpha_1x_1 + \cdots + \alpha_nx_n$ עבור $\alpha_i \in R$ ו־$x_i \in X$. מודול שיש לו בסיס נקרא **מודול חופשי**, ו**הדרגה** שלו היא גודל הבסיס (הדרגה לא תמיד מוגדרת היטב).

טענה 7.1.14 אם ${}_RM$ מודול חופשי מדרגה n, אז $\operatorname{End}_R(M) \cong \mathrm{M}_n(R)$.

טענה 7.1.15 מעל חוג עם חילוק, כל מודול הוא חופשי.

תרגיל 7.1.16 הוכח את הטענה, בעזרת תלות מופשטת (שהגדרנו בקורס הקודם).

לחוג יש התכונה **IBN** (Invariant Base Number, **מספר בסיס קבוע**) אם $R^n \cong R^m$ רק כאשר $n = m$.

טענה 7.1.17 לחוג יש IBN אם ורק אם עבור $A \in \mathrm{M}_{n\times m}(R)$ ו־$B \in \mathrm{M}_{m\times n}(R)$, מהתכונות $AB = I_n$ ו־$BA = I_m$ נובע $m = n$.

טענה 7.1.18 הדרגה מוגדרת היטב מעל חוג קומוטטיבי (העזר בקיום הדטרמיננטה הכפלית).

טענה 7.1.19 הדרגה מוגדרת היטב מעל כל חוג עם חילוק. (לכל קבוצה בלתי תלויה מקסימלית יש אותו גודל, לפי משפט 3.2.11 על גודלה של קבוצה בלתי תלויה מקסימלית לגבי תלות פורמלית).

תרגיל 7.1.20 נניח ש־$R = \operatorname{End}_F(V)$ כאשר V מרחב וקטורי ממימד אינסופי מעל F. הראה ש־$R \cong R \oplus R$ כמודולים, ולכן R אינו בעל IBN.

7.1.4 סכום וסכום ישר

תהי N_α משפחה (לאו דווקא סופית) של מודולים כלשהם. **הסכום הישר** (החיצוני) של המשפחה הוא המודול $\oplus N_\alpha$ שאבריו הם וקטורים (x_α) השווים לאפס כמעט בכל רכיב, עם הפעולה $r(x_\alpha) = (rx_\alpha)$. במקביל להגדרה זו, אנו זקוקים גם לסכום הישר הפנימי של תת־מודולים. ראשית נזכיר כיצד מגדירים סכום של תת־מודולים.

יהי M מודול, ותהי N_α משפחה של תת־מודולים. הסכום $M' = \sum_\alpha N_\alpha$ כולל, בהגדרה, את כל הסכומים הסופיים $x_1 + \cdots + x_n$ כאשר $x_i \in N_{\alpha_i}$. זהו תמיד תת־מודול של M. כל וקטור ב־M' אפשר להציג כסכום שבו כל מחובר מגיע מתת־מודול אחר (משום שאפשר לקבץ מחוברים השייכים לאותו תת־מודול ולהחליף אותם בסכומם). יש אפימורפיזם מן הסכום הישר החיצוני אל הפנימי, $\pi : \oplus N_\alpha \to \sum N_\alpha$, לפי $\pi((x_\alpha)) = \sum x_\alpha$ (בכל וקטור של הסכום הישר יש מספר סופי של רכיבים שונים מאפס).

הסכום הוא **סכום ישר** (פנימי) אם ההצגה של כל וקטור ב־M' באופן הזה היא יחידה.

טענה 7.1.21 התנאים הבאים שקולים:

1. הסכום $\sum N_\alpha$ הוא סכום ישר;
2. אם $x_1 + \cdots + x_n = 0$ כאשר $x_i \in N_{\alpha_i}$, $\alpha_1, \dots, \alpha_n$ שונים, אז $x_i = 0$ לכל i;
3. לכל α_0, $N_{\alpha_0} \cap \sum_{\alpha \neq \alpha_0} N_\alpha = 0$;
4. הפונקציה $\pi : \oplus N_\alpha \to \sum N_\alpha$ שהוגדרה לעיל היא איזומורפיזם.

הוכחה. $(1) \implies (2)$ משום שהצגת הוקטור 0 היא יחידה. $(2) \implies (3)$: אם $x_0 = x_1 + \cdots + x_n$ כאשר $x_0 \in N_{\alpha_0}$ ו־$x_i \in N_{\alpha_i}$ עבור $\alpha_i \neq \alpha_0$ שונים, אז $-x_0 + x_1 + \cdots + x_n = 0$ ו־$x_0 = 0$ לפי ההנחה. $(3) \implies (1)$: אם $x_1 + \cdots + x_n = y_1 + \cdots + y_n$, אפשר למחוק מחוברים השווים לאפס ולצמצם מחוברים עד שכל מחובר מגיע מתת־מודול אחר; נניח שהסכומים עדיין אינם אפס אז מתקבלת הצגה של $x_1 \in N_{\alpha_1}$, ל־α_1 מתאים, כסכום של מחוברים מתת־מודולים אחרים, ולכן $x_1 = 0$, בסתירה להנחה. $(1) \iff (4)$ משום שהסכום הפנימי ישר אם ורק אם π חד־חד־ערכית. $\square$

כעת נוכיח שחוג אנדומורפיזמים מסויים הוא חוג מטריצות. התוצאה הבאה תאפשר לנו לעבור בין מודול נתון לסכום ישר של כמה עותקים שלו. יהי M מודול מעל חוג R. נסמן ב־$M^{(n)} = M \oplus \cdots \oplus M$ את הסכום הישר של n עותקים של M; לשם נוחות נכתוב את אברי $M^{(n)}$ כעמודות בגובה n שרכיביהן ב־M; גם זה מודול מעל R.

טענה 7.1.22 נסמן $T = \mathrm{End}({}_R M)$, אז $T_n = \mathrm{End}({}_R M^{(n)}) \cong \mathrm{M}_n(T)$.

הוכחה. נגדיר הומומורפיזמים $\mu_i : M \to M^{(n)}$ על־ידי מיקום האיבר הנתון בקואורדינטה ה־i, ו־$\pi_i : M^{(n)} \to M$ לפי שליפת הרכיב בקואורדינטה ה־i. כך $\pi_i \mu_j = \delta_{ij} \mathrm{id}_M$, ו־$\sum_i \mu_i \pi_i$ היא הזהות של $M^{(n)}$. מכאן ש־$e_{ij} = \mu_i \pi_j \in T_n$ הן יחידות מטריצות. לפי טענה 7.1.5, $T_n \cong \mathrm{M}_n(T')$ כאשר $T' = e_{11} T_n e_{11} = \mu_1 \pi_1 T_n \mu_1 \pi_1$.

נגדיר $\Psi : T \to T'$ לפי $\Psi(\varphi) = \mu_1 \varphi \pi_1 = e_{11} \mu_1 \varphi \pi_1 e_{11}$, ו־$\Psi' : T' \to T$ לפי $\Psi'(e_{11} \varphi' e_{11}) = \pi_1 e_{11} \varphi' e_{11} \mu_1 = \pi_1 \varphi' \mu_1$; אלו הומומורפיזמים של חוגים, המקיימים $\Psi \Psi'(e_{11} \varphi' e_{11}) = \mu_1 \pi_1 e_{11} \varphi' e_{11} \mu_1 \pi_1 = e_{11} \varphi' e_{11}$ ו־$\Psi' \Psi(\varphi) = \pi_1 \mu_1 \varphi \pi_1 \mu_1 = \varphi$; כלומר, Ψ ו־Ψ' הופכים זה את זה, ו־$T \cong T'$. $\square$

7.2 מודולים פריקים לחלוטין

בסעיף זה נעסוק במודולים שאפשר לתאר באמצעות תת־המודולים הפשוטים שלהם, ונאסוף כמה הגדרות שקולות למשפחה החשובה של חוגים פשוטים למחצה.

7.2.1 מודולים פריקים לחלוטין

נזכיר ש**מודול פשוט** הוא מודול שאין לו תת־מודולים. בתרגיל 1.1.10 ראינו שכל מודול פשוט מעל R איזומורפי למנה R/L כאשר L אידיאל שמאלי מקסימלי. תת־מודול פשוט נקרא גם **תת־מודול מינימלי**.

הגדרה 7.2.1 *יהי M מודול מעל חוג R.* ***התשתית*** *$\operatorname{soc}(M)$ מוגדרת כסכום כל תת־המודולים הפשוטים של M. אם אין תת־מודולים פשוטים, אז $\operatorname{soc}(M) = 0$.*

הגדרה 7.2.2 *מודול M נקרא* ***פריק לחלוטין*** *אם $M = \operatorname{soc}(M)$.*

דוגמא 7.2.3 $\mathrm{M}_n(F)$ פריק לחלוטין (כמודול מעל עצמו). עם זאת, לא כל איבר של $\mathrm{M}_n(F)$ שייך למודול פשוט, ולכן $\operatorname{soc}(M)$ אינו בהכרח איחוד של תת־מודולים פשוטים.

הערה 7.2.4 לכל מודול M, $\operatorname{soc}(\operatorname{soc}(M)) = \operatorname{soc}(M)$. לכן התשתית של כל מודול היא מודול פריק לחלוטין.

דוגמא 7.2.5 כל מרחב וקטורי הוא פריק לחלוטין (כסכום של תת־המרחבים החד־ממדיים).

הערה 7.2.6
1. סכום ישר של מודולים פריקים לחלוטין הוא פריק לחלוטין.
2. סכום של תת־מודולים פריקים לחלוטין הוא תת־מודול פריק לחלוטין.
3. תמונה הומומורפית של מודול פריק לחלוטין היא פריקה לחלוטין.

תרגיל 7.2.7 יהיו $K \leq M$ מודול ותת־מודול. הראה ש־$(\operatorname{soc}(M)+K)/K \leq \operatorname{soc}(M/K)$, ותן דוגמא לכך שההכלה אמיתית.

למה 7.2.8 נניח שהסכום $\sum N_i \leq M$ הוא סכום ישר (המושג מוגדר בתת־סעיף 7.1.4), ו־$S \leq M$ תת־מודול פשוט שאינו מוכל בו. אז גם הסכום $S + \sum N_i$ הוא ישר.

הוכחה. **אחרת יש סכום לא טריוויאלי המסתכם לאפס. הרכיב של S אינו אפס משום ש־$\sum N_i$ סכום ישר, אבל אז הרכיב הזה שייך ל־$S \cap \sum N_i$, שהוא תת־מודול אמיתי של S ולכן אפס.** □

טענה 7.2.9 לכל מודול M, $\operatorname{soc}(M)$ הוא סכום ישר של תת־מודולים פשוטים (לא בהכרח כולם!).

הוכחה. **לפי הלמה של צורן יש מערכת מקסימלית של תת־מודולים N_i כך ש־$N = \sum N_i$ הוא סכום ישר. אם $N = \sum N_i < \operatorname{soc}(M)$ אז קיים $S \leq M$ פשוט שאינו מוכל ב־$\sum N_i$, ואז לפי למה 7.2.8 $S + \sum N_i$ הוא סכום ישר, בסתירה למקסימליות של $\{N_i\}$.** □

תרגיל 7.2.10 הוכח בעזרת טענה 7.2.9 את משפט הבסיס של האמל: לכל מרחב וקטורי יש בסיס. **הדרכה**. מרחב וקטורי מעל השדה F הוא מודול פריק לחלוטין, ואם V הוא סכום ישר של תת־המודולים הפשוטים Fb_λ אז $\{b_\lambda\}$ הוא בסיס של V.

7.2.2 תת־מודולים גדולים

הגדרה 7.2.11 *יהי M מודול. תת־מודול $N \leq M$ הוא **תת־מודול גדול** אם $N \cap K \neq 0$ לכל תת־מודול $K \neq 0$.*

תרגיל 7.2.12 בתחום שלמות, כל אידיאל הוא תת־מודול גדול.

הערה 7.2.13 כל תת־מודול גדול N מכיל כל תת־מודול פשוט S.

הוכחה. לפי ההנחה $0 \neq N \cap S \leq S$ ולכן $N \cap S = S$. □

מסקנה 7.2.14 למודול פריק לחלוטין M אין תת־מודולים גדולים פרט ל־M.

הגדרה 7.2.15 *יהי $N < M$ תת־מודול. $N' \leq M$ **נקרא משלים עקרונית** אם $N' \cap N = 0$ ו־$N + N'$ תת־מודול גדול של M.*

תרגיל 7.2.16 לכל שלושה תת־מודולים $A, B, C \leq M$:

1. אם $A \cap (B + C) = 0$ אז $B \cap C = B \cap (A + C)$. **הדרכה.** אם $b = a + c$ אז $A \ni a = b - c \in B + C$, ולכן $a = b - c \in A \cap (B + C) = 0$, ואז $b = c$.
2. אם $A \cap (B + C) = B \cap C = 0$ אז $B \cap (A + C) = 0$. **הדרכה.** לפי הסעיף הקודם $B \cap (A + C) = B \cap C = 0$.

תרגיל 7.2.17 הוכח את למה 7.2.8 בעזרת תרגיל 7.2.16. **הדרכה.** $S \cap \sum N_i = 0$; ולכל j, $N_j \cap (S + \sum_{i \neq j} N_i) = 0$, כי $S \cap \sum N_i = N_j \cap \sum_{i \neq j} N_i = 0$ לפי מתרגיל 7.2.16.

טענה 7.2.18 לכל תת־מודול $N < M$ יש משלים עקרונית.

הוכחה. ניקח תת־מודול $N' < M$ שהוא מקסימלי ביחס לתנאי $N' \cap N = 0$ (קיים לפי הלמה של צורן). יהי $K \leq M$ תת־מודול כלשהו; אם $K \cap (N' + N) = 0$ אז גם $(K + N') \cap N = 0$ לפי תרגיל 7.2.16, ולפי המקסימליות של N' בהכרח $K \subseteq N'$, אבל אז $K \subseteq N + N'$ ו־$K = K \cap (N + N') = 0$.□

7.2.3 משלימים של תת־מודול

הגדרה 7.2.19 *יהי $N < M$ תת־מודול. תת־מודול $K \leq M$ **נקרא משלים של** N אם $M = N \oplus K$ (כלומר $K + N = M$ ו־$K \cap N = 0$).*

הערה 7.2.20 יהי M מודול מעל חוג R. לתת־מודול $N < M$ יש משלים אם ורק אם יש אידמפוטנט $e \in \mathrm{End}(_RM)$ כך ש־$N = \mathrm{Im}(e)$.

הוכחה. אם יש לתת־המודול משלים, אפשר לכתוב $M = N \oplus N'$ ולקחת $e(x, x') = (x, 0)$. בכיוון ההפוך אם $N = \mathrm{Im}(e)$ ניקח $N' = \mathrm{Im}(1 - e)$, אז מ־$e(x) = (1 - e)(y)$ נובע $e(x) = e^2(x) = e(1 - e)(y) = 0$ ולכן $N \cap N' = 0$, וכל $x \in M$ אפשר לכתוב בצורה $x = e(x) + (1 - e)(x)$, כך ש־$M = \mathrm{Im}(e) + \mathrm{Im}(1 - e)$. □

מודול הוא **בעל משלימים** אם לכל תת־מודול יש משלים.

למה 7.2.21 יהיו $K \leq N \leq M$. אם K' משלים של K בתוך M, אז $K'' = K' \cap N$ משלים של K בתוך N.

הוכחה. $K'' = K' \cap N \leq N$ מקיים $K'' \cap K \subseteq K' \cap K = 0$ ו־$K'' + K = (N \cap K') + K = N \cap (K' + K) = N \cap M = N$ לפי המודולריות. $\square$

טענה 7.2.22 (תורשתיות קיום המשלימים) נניח ש־M בעל משלימים; אז כל תת־מודול $N < M$ גם הוא בעל משלימים.

הוכחה. יהי $K \leq N$. לפי ההנחה יש לו משלים K' בתוך M, ואז $K'' = K' \cap N$ משלים שלו בתוך N לפי למה 7.2.21. $\square$

למה 7.2.23 לכל מודול $M \neq 0$ בעל משלימים יש תת־מודול פשוט.

הוכחה. נבחר $0 \neq x \in M$. נתבונן בתת־מודול $N < M$ שהוא מקסימלי ביחס לתכונה $x \notin N$. לפי ההנחה יש משלים N' של N בתוך M. נניח ש־$0 < K < N'$, אז לפי התורשתיות יש משלים $0 < K' < N'$ בתוך N', ואז $N < N + K, N + K'$. לפי המקסימליות של N נובע מכאן ש־$x \in (N + K) \cap (N + K')$. נכתוב $x = n + k = n' + k'$ עבור $n, n' \in N$, $k \in K$ ו־$k' \in K'$; אז $n - n' = k' - k \in N \cap (K + K') = N \cap N' = 0$, כלומר $k' = k \in K' \cap K = 0$, אבל אז $x \in N$, בסתירה להנחה ש־K תת־מודול אמיתי של N'. מכאן ש־N' פשוט. $\square$

משפט 7.2.24 *התנאים הבאים שקולים עבור מודול M:*

1. *M פריק לחלוטין.*
2. *אין ל־M תת־מודול גדול אמיתי.*
3. *M הוא בעל משלימים.*

הוכחה. הוכחנו $(1) \implies (2)$ במסקנה 7.2.14.

$(2) \implies (3)$: יהי M מודול שאין בו תת־מודולים גדולים פרט לעצמו, ויהי $N \leq M$ תת־מודול. לפי טענה 7.2.18 קיים N' כך ש־$N \cap N' = 0$ ו־$N + N' \leq M$ גדול, ולפי ההנחה $N + N' = M$ ולכן N' משלים של N.

נותר אם כך להוכיח $(3) \implies (1)$. יהי M מודול בעל משלימים. נסמן $S = \operatorname{soc}(M)$. יהי S' משלים של S, ונניח בשלילה ש־$S' \neq 0$. התורשתיות מאפשרת להפעיל את למה 7.2.23 ולהסיק שיש תת־מודול פשוט $N' \leq S'$. אבל אז $N' \leq S$ לפי ההגדרה, ולכן $N' \leq S \cap S' = 0$, וזו סתירה להנחה ש־$S' \neq 0$. מכאן ש־$M = S$ פריק לחלוטין. $\square$

משפט 7.2.25 *$\operatorname{soc}(M)$ שווה לחיתוך תת־המודולים הגדולים של M.*

הוכחה. נסמן ב־$S = \operatorname{soc}(M)$ ונסמן ב־J את חיתוך תת־המודולים הגדולים. לפי הערה 7.2.13, $J \leq S$. נוכיח ש־J הוא בעל משלימים. יהי $N < J$. לפי טענה 7.2.18, יש ל־N משלים עקרונית N' בתוך M; לכן $N + N'$ תת־מודול גדול והוא מכיל את J לפי ההגדרה. אבל N' משלים של N ב־$N + N'$, ולפי למה 7.2.21, $N' \cap J$ משלים של N בתוך J.

כעת J פריק לחלוטין לפי משפט 7.2.24, ולכן שווה לסכום תת־המודולים הפשוטים שלו, שכולם תת־מודולים פשוטים של M, ולכן סכומם מוכל ב־S; כלומר $J \leq S$ ומכאן נובע השוויון הדרוש. $\square$

7.2.4 חוגים פשוטים למחצה

הגדרה 7.2.26 *חוג R הוא **חוג פשוט למחצה** אם הוא פריק לחלוטין כמודול מעל עצמו (כלומר, הוא שווה לסכום של אידיאלים שמאליים מינימליים).*

הערה 7.2.27 נניח ש־R פשוט למחצה. אז הוא שווה לסכום של מספר סופי של אידיאלים מינימליים.

הוכחה. כתוב את $1 \in R$ בתור סכום $\sum a_i = 1$ עבור $a_i \in A_i$ כאשר A_i אידיאלים מינימליים; אז לכל $r \in R$, $r = \sum ra_i \in \sum A_i$. □

טענה 7.2.28 כל מודול מעל חוג פשוט למחצה R הוא פריק לחלוטין.

הוכחה. כתוב $R = \sum L_i$ כאשר L_i אידיאלים שמאליים מינימליים. יהי M מודול מעל R. אפשר לכתוב $M = \sum_{x \in M} Rx = \sum_{x \in M} \sum_i L_i x$, אבל לכל i ולכל x, אם $L_i x \neq 0$ אז הוא מינימלי כי $L_i \cong L_i x$. □

תרגיל 7.2.29 חוג R פשוט למחצה אם ורק אם כל מודול מעליו הוא פריק לחלוטין.

טענה 7.2.30 כל אידיאל שמאלי $A \leq_\ell R$ בחוג פשוט למחצה הוא מהצורה $L = Re$ כאשר e אידמפוטנט.

הוכחה. לפי ההגדרה יש מודול משלים, כלומר $R =: \oplus L'$. נפרק $1 = e + e'$ עבור $e \in A$, אז $e = e^2 + ee'$, ומצד שני $e = e + 0$. לכן $e^2 = e$ ו־$ee' = 0$. לכל $a \in L$, $a + 0 = a = ae + ae'$, ושוב מהשוואת רכיבים מקבלים $a = ae \in Re$; לכן $L = Re$. □

7.3 משפט הצפיפות הכללי

7.3.1 בי־מודולים

הגדרה 7.3.1 *יהיו R, T חוגים. נניח ש־M הוא מודול שמאלי מעל R, וגם מודול ימני מעל T. אומרים שהוא **בי־מודול** מעל R, T אם $r(xt) = (rx)t$ לכל $r \in R$, $t \in T$ ולכל $x \in M$. מציינים ש־M הוא בי־מודול בסימון ${}_RM_T$.*

לדוגמא, כל מודול ${}_RM$ מעל חוג קומוטטיבי הוא גם מודול ימני לפי $x \cdot a = ax$, ולמעשה הוא בימודול ${}_RM_R$, מכיוון ש־$(ax)b = b(ax) = (ba)x = (ab)x = a(bx) = a(xb)$.

כעת נוכל להסביר את הגדרה 7.1.8. יהיו R חוג ו־${}_RM$ מודול שמאלי מעל R. נסמן $T = \mathrm{End}({}_RM)$. הפעולה $x \cdot f = f(x)$ הופכת את M למודול ימני מעל T (אכן, $x \cdot (fg) = (fg)(x) = g(f(x)) = g(x \cdot f) = (x \cdot f) \cdot g$ לפי הגדרת הכפל ב־T). לו היינו מגדירים את הכפל על־ידי שינוי הסדר, כלומר לו היינו מתבוננים ב־T^{op} במקום ב־T, M היה מודול שמאלי במקום ימני. היתרון בחילופי הצדדים הוא ש־M הוא בימודול, ${}_RM_T$: $(rx)f = f(rx) = rf(x) = r(xf)$.

דוגמא נוספת: כל חוג R מהווה מודול שמאלי וגם ימני מעל עצמו, לפי הפעולה המושרית מן הכפל של החוג (כלומר, $a \cdot x = ax$, $x \cdot a = xa$). ביחס לפעולות אלו, R הוא בימודול מעל R, R, משום ש־$(ax)b = a(xb)$ בחוג.

תרגיל 7.3.2 יהיו R, R' חוגים.

1. הראה ש־$S = \begin{pmatrix} R & M \\ 0 & R' \end{pmatrix}$ הוא חוג (אסוציאטיבי) ביחס לפעולת הכפל הרגילה של מטריצות, אם ורק אם ${}_RM_{R'}$ הוא בי־מודול. נניח שזה אכן כך.

2. $\begin{pmatrix} 0 & N \\ 0 & 0 \end{pmatrix}$ הוא אידיאל שמאלי אם $N \leq {}_RM$; ואידיאל ימני אם $N \leq M_{R'}$. הראה שאם החוג S נתרי/ארטיני משמאל, אז M נתרי/ארטיני כמודול שמאלי מעל R, ואם S נתרי/ארטיני מימין, אז M נתרי/ארטיני כמודול ימני מעל R'.

3. נניח ש־$M = R' = K$ כאשר K שדה, ו־$R \subseteq K$.

(א) S נתרי/ארטיני ימני אם ורק אם R נתרי/ארטיני. **הדרכה.** האידיאלים הימניים של S הם מהצורה $\left\{\begin{pmatrix} 0 & v_1 \\ 0 & v_2 \end{pmatrix} : \begin{pmatrix} v_1 \\ v_2 \end{pmatrix} \in V\right\}$ עבור תת־מרחבים וקטוריים $V \subseteq K^2$, או מהצורה $\begin{pmatrix} I & K \\ 0 & K \end{pmatrix}$ כאשר $I \lhd R$.

(ב) S נתרי/ארטיני שמאלי אם ורק אם R חוג נתרי/ארטיני, וגם K נתרי/ארטיני כמודול מעל R. **הדרכה.** האידיאלים השמאליים של S הם מהצורה $\left\{\begin{pmatrix} a & v \\ 0 & 0 \end{pmatrix} : (a,v) \in N\right\}$ עבור תת־מודולים $N \leq R \times K$ מעל R, או מהצורה $\begin{pmatrix} I & K \\ 0 & K \end{pmatrix}$ כאשר $I \lhd R$.

(ג) $\begin{pmatrix} \mathbb{Z} & \mathbb{Q} \\ 0 & \mathbb{Q} \end{pmatrix}$ נתרי ימני אבל לא נתרי שמאלי.

(ד) $\begin{pmatrix} \mathbb{Q} & \mathbb{R} \\ 0 & \mathbb{R} \end{pmatrix}$ ארטיני ימני אבל לא ארטיני שמאלי.

7.3.2 ההצגה הרגולרית

הצגה של חוג היא הומומורפיזם ממנו אל אובייקט קונקרטי, כמו חוג אנדומורפיזמים. תהי M חבורה אבלית. כידוע, כל חבורה אבלית היא מודול ימני מעל חוג השלמים $\mathbb{Z}$, ולכן יש לה חוג אנדומורפיזמים $\operatorname{End}(M_{\mathbb{Z}})$ (ראה תרגיל **1.1.1**).

מתברר שהצגה של R לתוך החוג $\operatorname{End}(M_{\mathbb{Z}})$ אינה אלא שכלול של M לכדי מודול שמאלי מעל R.

טענה 7.3.3 לכל הומומורפיזם של חוגים $\psi : R \to \operatorname{End}(M_{\mathbb{Z}})$ אפשר לראות את M כמודול מעל R לפי הפעולה $r \cdot x = \psi(r)(x)$. ◦

בכיוון ההפוך, אם M מודול שמאלי מעל R, אז לכל $r \in R$ הפונקציה $\psi(r) : x \mapsto rx$ היא אנדומורפיזם של M, והפונקציה $r \mapsto \psi(r)$ היא הומומורפיזם של חוגים, $R \to \operatorname{End}(M_{\mathbb{Z}})$.

הוכחה. בכיוון הראשון, מכיוון ש־$\psi(rr') = \psi(r)\psi(r')$, לכל x מתקיים

$$(rr') \cdot x = \psi(rr')(x) = (\psi(r) \circ \psi(r'))(x) = r \cdot (r' \cdot x).$$

□

כדי לשפר את ההצגה, נניח ש־M הוא כבר מודול שמאלי מעל R, ויש לו בנוסף לזה מבנה של מודול ימני מעל חוג S, ההופך את M לבימודול. נסמן $\hat{R} = \mathrm{End}(M_S)$. זהו תת־חוג $\hat{R} \subseteq \mathrm{End}(M_{\mathbb{Z}})$, שהוא קטן יותר ככל ש־$S$ גדול יותר.

המבנה של M כמודול מעל R הופך את M למודול שמאלי מעל $\hat{R}$, על־ידי הפעולה $f \cdot x = f(x)$. למעשה M הוא בי־מודול מעל $\hat{R}, S$, משום ש־

$$(f \cdot x)t = f(x)t = f(xt) = f \cdot (xt)$$

לפי הגדרת $\hat{R}$.

אם מעוניינים בהצגה של R לתוך חוג קונקרטי, כדאי שזה יהיה חוג קטן ככל האפשר. המבנה של M כמודול מעל $\hat{R}$ מאפשר להגדיר הומומורפיזם $R \to \hat{R}$ לפי $\psi : r \mapsto \hat{r}$, כאשר $\hat{r} \cdot x = rx$.

כעת נניח רק ש־M מודול שמאלי מעל חוג R. כדי להגדיר על M מבנה של בימודול, ניקח $T = \mathrm{End}({}_RM)$, ונגדיר $x \cdot f = f(x)$. כפי שראינו לפני כן, M הוא אכן בימודול מעל R, T, ואפשר לקחת $\hat{R} = \mathrm{End}(M_T)$. ($T = \mathrm{End}({}_RM)$ הוא החוג הגדול ביותר כך ש־M הוא R, T־בימודול, ולכן $\hat{R}$ הזה הוא החוג הקטן ביותר האפשרי מהצורה $\mathrm{End}(M_S)$.)

טענה 7.3.4 יהיו M מודול שמאלי מעל חוג R, $T = \mathrm{End}({}_RM)$, ו־$\hat{R} = \mathrm{End}(M_T)$. אז $\hat{R}$ הוא המרכז של T^{op} בחוג האנדומורפיזמים הכללי $\mathrm{End}(M_{\mathbb{Z}})$.

הוכחה. נחשב. כדי ש־$\varphi \in \mathrm{End}(M_{\mathbb{Z}})$ יהיה שייך ל־$\hat{R}$ נדרש שלכל $f \in T$ ולכל $x \in M$, $\varphi(f(x)) = \varphi(x \cdot f) = \varphi(x) \cdot f = f(\varphi(x))$, כלומר $\varphi \circ f = f \circ \varphi$. $\square$

מסקנה 7.3.5 עם $M, R, \hat{R}$ כמו בטענה 7.3.4, $\hat{R} \cap T = \mathrm{Z}(T)$.

במקרה המיוחד שבו R קומוטטיבי המבנה הדוק עוד יותר.

הערה 7.3.6 אם R קומוטטיבי, אז $\mathrm{Im}(\psi) \subseteq \mathrm{Z}(T)$. נוכיח ש־$\mathrm{Im}(\psi) \subseteq T = \mathrm{End}({}_RM)$. אכן, לכל $r \in R$, מתקיים $\hat{r} \in T$, שהרי $\hat{r}(ax) = r(ax) = (ra)x = (ar)x = a(rx) = a\hat{r}x$. הטענה נובעת ממסקנה 7.3.5.

7.3.3 חוגים צפופים

שוב יהי ${}_RM$ מודול מעל החוג R. כמקודם, נבחר $T = \mathrm{End}({}_RM)$, ונגדיר $\hat{R} = \mathrm{End}(M_T)$.

הגדרה 7.3.7 תת־חוג $R_0 \subseteq \hat{R}$ הוא n**־צפוף** אם לכל $f \in \hat{R}$ ולכל $x_1, \dots, x_n \in M$ קיים $f_0 \in R_0$ כך ש־$f(x) = f_0(x)$; תת־החוג **צפוף** אם הוא n־צפוף לכל n.

(יכולנו להגדיר צפיפות ב־$\mathrm{End}(M_T)$ לכל T שעבורו ${}_RM_T$ הוא בימודול. אפשר גם להגדיר צפיפות ב־$\mathrm{End}({}_RM)$ בדיוק כפי שהגדרנו צפיפות ב־$\mathrm{End}(M_T)$; אין לנו צורך בהכללות האלה.)

מה נדרש על־מנת ש־R יהיה 1־צפוף? נאמר ש־f **שומר** על תת־מודול N אם $f(N) \subseteq N$. לפי ההגדרה, $R \subseteq \hat{R}$ הוא 1־צפוף אם לכל $f \in \hat{R}$ ולכל $x \in M$, $f(Rx) \subseteq Rx$; כלומר, אם כל $f \in \hat{R}$ שומר על כל תת־מודול ציקלי.

תרגיל 7.3.8 אנדומורפיזם $f \in \mathrm{End}(M_T)$ שומר על כל תת־מודול ציקלי, אם ורק אם הוא שומר על כל תת־מודול.

ומתי מובטח שתת־מודול N נשמר?

למה 7.3.9 נניח של־M $N<$ יש משלים. אז לכל $f\in\operatorname{End}(M_T)$ מתקיים $f(N)\subseteq N$.

הוכחה. לפי הערה 7.2.20 יש אידמפוטנט $\pi\in T$ המקיים $N=\pi(M)$, ואז לכל $x\in M$ מתקיים $N \ni f(\pi(x))=f(x\cdot\pi)=f(x)\cdot\pi=\pi(f(x))$, ולכן $f(N)\subseteq N$. □

משפט 7.3.10 (משפט הצפיפות הכללי) *יהי M מודול פריק לחלוטין מעל חוג R. אז תמונת R ב־$\hat{R}$ צפופה שם.*

הוכחת משפט הצפיפות. ראשית נוכיח שהתמונה היא 1־צפופה: יהיו $f\in\hat{R}$ ו־$x_1\in M$. ניקח $N=Rx_1\leq M$. מכיוון שיש ל־N משלים ב־M, למה 7.3.9 קובעת ש־$f(x_1)\in N$, ולכן קיים $r\in R$ כך ש־$f(x_1)=rx_1$.

נעבור למקרה הכללי. נחליף את M במודול $\tilde{M}=M^{(n)}$, שגם הוא פריק לחלוטין לפי הערה 7.2.6. בהתאם לזה יש להחליף את T ב־$\tilde{T}=\operatorname{End}({}_R\tilde{M})=\operatorname{M}_n(T)$ לפי טענה 7.1.22, את $x_1,\dots,x_n\in M$ הנתונים בוקטור $\tilde{x}=(x_1,\dots,x_n)^{\mathrm{t}}=\sum\nu_i(x_i)\in\tilde{M}$, ואת $f\in\hat{R}=\operatorname{End}(M_T)$ באנדומורפיזם $\tilde{f}$ הפועל אלכסונית על רכיבי $M^{(n)}$. כפעולה אלכסונית, $\tilde{f}\in\operatorname{End}(\tilde{M}_{\tilde{T}})$ לפי משפט 7.3.4.

כפי שהוכחנו לעיל, תמונת R 1־צפופה ב־$\operatorname{End}(\tilde{M}_{\tilde{T}})$, ולכן קיים $r\in R$ כך ש־$(f(x_1),\dots,f(x_n))^{\mathrm{t}}=\tilde{f}(\tilde{x})=r\tilde{x}=(rx_1,\dots,rx_n)^{\mathrm{t}}$, כלומר $f(x_i)=rx_i$ לכל $i=1,\dots,n$. □

מסקנה 7.3.11 יהי ${}_RM$ מודול פריק לחלוטין, ונניח ש־M נוצר סופית מעל $T=\operatorname{End}({}_RM)$. אז ההומומורפיזם $R{\rightarrow}\hat{R}$ הוא על. (משום שאיבר ב־$\hat{R}$ נקבע לפי פעולתו על קבוצה פורשת.)

המשפט נקרא כך בשל הפירוש הטופולוגי שלו. נגדיר טופולוגיה על $\hat{R}=\operatorname{End}(M_T)$, שהבסיס שלה הוא הקבוצות $U_{f;x_1,\dots,x_n}=\{g\in\operatorname{End}(M_T):\ g(x_i)=f(x_i), i=1,\dots,n\}$.

תרגיל 7.3.12 הראה שזה אכן בסיס לטופולוגיה (משפחה של קבוצות היא בסיס לטופולוגיה אם לכל A,B במשפחה ולכל $x\in A\cap B$ יש C במשפחה כך ש־$x\in C\subseteq A\cap B$; הטופולוגיה הנוצרת על־ידי הבסיס כוללת את כל האיחודים של קבוצות ממנו.)

משפט הצפיפות טוען שתמונת R ב־$\hat{R}$ תחת השיכון הרגולרי, צפופה שם במובן הטופולוגי.

תרגיל 7.3.13 תת־מודול N של ${}_RM$ נקרא **צפוף** אם לכל $x,y\in M$ כך ש־$x\neq 0$, יש $a\in R$ כך ש־$ax\neq 0$ ו־$ay\in N$.

1. כל תת־מודול צפוף הוא גדול.
2. אם תת־מודול הוא צפוף, אז כל תת־מודול המכיל אותו הוא צפוף.
3. חיתוך של תת־מודולים צפופים הוא צפוף.
4. בחוג קומוטטיבי, אידיאל הוא צפוף (בחוג כמודול מעל עצמו) אם ורק אם הוא נאמן (כמודול).
5. הראה ש־N צפוף ב־M אם ורק אם $\operatorname{Hom}(N'/N,M)\neq 0$ לכל $N\leq N'\leq M$.

פרק 8

המבנה של חוגים ארטיניים

8.1 חוגים פשוטים

בסעיף הראשון נתן כמה דוגמאות לחוגים פשוטים, ארטיניים ולא ארטיניים. **חוג פשוט** הוא חוג (עם יחידה) שאין לו אידיאלים אמיתיים. נתחיל בדוגמא קיצונית לחוגים פשוטים.

הערה 8.1.1 התכונות הבאות של חוג D שקולות זו לזו:

1. D **חוג עם חילוק** (כלומר, כל האברים השונים מאפס הפיכים),
2. כל האברים השונים מאפס ב־D הפיכים משמאל.
3. אין ל־D אידיאלים שמאליים לא־טריוויאליים.
4. D פשוט כמודול מעל עצמו.

הוכחה. **ברור שהתכונה הראשונה גוררת את השניה, ושתכונות 2, 3 שקולות זו לזו. ברור גם שתכונות 4,3 שקולות זו לזו. כדי להוכיח ש־2 גורר את 1, נניח שב־D כל האברים הפיכים משמאל; יהי $0 \neq a \in D$, אז יש $b \in D$ כך ש־$ba = 1$, ויש $c \in D$ כך ש־$cb = 1$. לכן $c = cba = a$, כלומר $ab = ba = 1$ ו־a הפיך.** $\square$

בפרט, כל חוג עם חילוק הוא פשוט, אבל ההיפך אינו נכון: לפי טענה 7.1.2, חוג מטריצות מעל חוג פשוט גם הוא חוג פשוט. כלומר, כל החוגים מהצורה $\mathrm{M}_n(D)$, כאשר D חוג עם חילוק, הם פשוטים. בדוגמאות האלה נעסוק בתת־סעיף 8.1.2. חוג פשוט מהצורה $\mathrm{M}_n(D)$ שהוא **תחום** (ללא מחלקי אפס), הוא בהכרח חוג עם חילוק. בסעיף 8.1.3 נציג דוגמא לחוג פשוט שהוא תחום, אבל אינו חוג עם חילוק.

בין החוגים הקומוטטיביים, חוגים פשוטים אינם אלא שדות. יתרה מזו:

טענה 8.1.2 המרכז של חוג פשוט הוא שדה.

הוכחה. **יהי $0 \neq a Z(R)$, כאשר R חוג שפוט. אז Ra הוא אידיאל (דו־צדדי), השונה ואפס, ולכן שווה לכל החוג. בפרט $1 \in aR = Ra$, ולכן a הפיך בחוג. אבל לכל $x \in R$, מ־ $xa = ax$ נובע $a^{-1}x = xa^{-1}$ ו־$a^{-1} \in R$.** $\square$

בעקבות טענה זו, כל חוג פשוט הוא אלגברה מעל שדה כלשהו. אחת הגישות בתאוריה של אלגברות פשוטות היא למיין את כל האלגברות הפשוטות (ממימד סופי) שהמרכז שלהן הוא שדה נתון.

הערה 8.1.3 יהי F שדה סגור אלגברית. אין אלגברת חילוק ממימד סופי מעל F (פרט כמובן ל־F עצמו). ◦

הוכחה. נניח ש־D אלגברת חילוק שהמרכז שלה K מכיל את F, וכך ש־$[D:F] < \infty$. אז $[K:F] < \infty$ ולכן $K = F$. בנוסף, לכל $d \in D$, $F[d]$ הוא תת־חוג אלגברי של D, ולכן הוא חוג עם חילוק, ומכיוון ש־$F[d]$ קומוטטיבי, הוא שדה. לכן $F[d] = F$ ו־$d \in F$. □

אלגברת החילוק היחידה שהמרכז שלה הוא $\mathbb{R}$ היא אלגברת הקווטרניונים.

8.1.1 אלגברות ציקליות

נציג בניה מעניינת וכללית למדי לחוגים פשוטים.

תהי K/F הרחבת גלואה של שדות, עם חבורת גלואה ציקלית $\mathbb{Z}/n\mathbb{Z} \cong \langle\sigma\rangle$. יהי $b \in F^\times$. נתבונן בחוג

$$A = K \oplus Kz \oplus \cdots \oplus Kz^{n-1},$$

עם פעולת הכפל המוגדרת לפי $(az^i)(a'z^{i'}) = a\sigma^i(a')z^{i+i'}$, ו־$z^n = b$. בפרט z הפיך, ו־$zkz^{-1} = \sigma(k)$ לכל $k \in K$. היחס $z^n = b$ נשמר תחת ההצמדה ב־z, מכיוון ש־$zbz^{-1} = \sigma(b) = b = z^n = (zzz^{-1})^n = z^n$. את האלגברה הזו, שהממד שלה מעל F הוא n^2, מסמנים ב־$(K/F, \sigma, b)$. אלגברה מצורה זו נקראת **אלגברה ציקלית**.

טענה 8.1.4 האלגברה $(K/F, \sigma, b)$ פשוטה.

הוכחה. כל איבר של A אפשר להציג באופן יחיד בצורה $\sum a_i z^i$, כאשר $a_i \in K$. ה'אורך' של האיבר הוא מספר המונומים השונים מאפס בסכום הזה. נניח ש־$0 \neq I \lhd A$, ויהי $0 \neq f \in I$ איבר בעל אורך מינימלי. נכתוב $f = \sum a_i z^i$. על־ידי כפל מימין בחזקה מתאימה של z, אפשר להניח ש־$a_0 \neq 0$. אם $f \in K$, הוא הפיך וסיימנו. אחרת, יש $i_0 \neq 0$ כך ש־$a_{i_0} \neq 0$. נבחר $k \notin K^{\sigma^{i_0}}$ כלשהו. אז הקומוטטור החיבורי $[f,k] = \sum a_i[z^i,k] = \sum a_i(\sigma^i(k) - k)$ שייך ל־I, והוא קצר מ־f, בסתירה להנחה. □

טענה 8.1.5 המרכז של $(K/F, \sigma, b)$ הוא F.

הוכחה. נניח ש־$f = \sum a_i z^i$ שייך למרכז. לכל $k \in K$ מתקיים $0 = [f,k] = \sum a_i(\sigma^i(k) - k)$, ולכן לכל $i \neq 0$ בהכרח $a_i = 0$. כלומר, $f \in K$. אבל כעת $[z,f] = \sigma(a_0) - a_0$, ולכן $a_0 \in K^\sigma = F$. □

אלגברה ציקלית ממימד $n^2 = 4$ נקראת **אלגברת קווטרניונים**. לשם פשטות, נתאר את האלגברות האלה בהנחה ש־$\mathrm{char}F \neq 2$.

דוגמא 8.1.6 (אלגברת קווטרניונים במאפיין שונה מ־2) תהי K/F הרחבה ריבועית. כידוע, הרחבה כזו היא תמיד מהצורה $K = F[x]$ כאשר $x^2 = a$. האוטומורפיזם $\sigma\colon K \to K$ מוגדר על־ידי $\sigma(x) = -x$, ולכן אפשר לתאר את האלגברה $(a,b)_{2,F} = (F[a]/F, \sigma, b)$ כמרחב וקטורי

$$Q = K \oplus Kz = F \oplus Fx \oplus Fz \oplus Fxz,$$

עם הכפל המוגדר לפי היחסים $x^2 = a$, $z^2 = b$, $zx = -xz$.

על Q מוגדרת אינוולוציה (כלומר אנטי־אוטומורפיזם מסדר 2), לפי

$$\overline{\alpha + \beta x + \gamma z + \delta xz} = \alpha - \beta x - \gamma z - \delta xz.$$

האינוולוציה מאפשרת להגדיר העתקה אדיטיבית $t\colon Q\to F$ לפי $t(w) = w + \bar{w}$, והעתקה כפלית $n\colon Q\to F$ לפי $n(w) = w\bar{w} = \bar{w}w$, כך שמתקיים $w^2 - t(w)w + n(w) = 0$ לכל $w \in Q$. אפשר לחשב ש־

$$n(\alpha + \beta x + \gamma z + \delta xz) = \alpha^2 - a\beta^2 - b\gamma^2 + ab\delta^2.$$

כעת יש שתי אפשרויות. נאמר שהתבנית הריבועית $n(w)$ היא **איזוטרופית** אם יש פתרון שונה מאפס למשוואה $n(w) = 0$, ואנאיזוטרופית אחרת.

1. אם תבנית הנורמה אנאיזוטרופית, $w^{-1} = n(w)^{-1}\bar{w}$ לכל $w \neq 0$. במקרה זה Q היא אלגברת חילוק.

2. אם התבנית איזוטרופית, $Q \cong \mathrm{M}_2(F)$. **הדרכה.** הראה שאפשר להציג את b בצורה $b = \alpha^2 - \beta^2 a$; העזר באברים $z - \alpha \pm \beta x$.

דוגמא 8.1.7 **אלגברת הקווטרניונים של המילטון** היא האלגברה

$$\mathbb{H} = \mathbb{R} \oplus \mathbb{R}i \oplus \mathbb{R}j \oplus \mathbb{R}ij$$

עם פעולת הכפל המוגדרת לפי $i^2 = j^2 = -1$, $ji = -ij$, המתקבלת מן הדוגמא הקודמת כשנבחר $a = b = -1$ מעל השדה $F = \mathbb{R}$. מכיוון שתבנית הנורמה $n(a + bi + cj + dij) = a^2 + b^2 + c^2 + d^2$ היא חיובית לחלוטין, זו אלגברת חילוק.

התרגיל הבא מכליל את הבניה של אלגברות ציקליות, מהרחבת שדות ציקלית להרחבת גלואה כלשהי.

תרגיל 8.1.8 נניח ש־D היא אלגברה עם חילוק מעל המרכז $F = \mathrm{Z}(D)$. נניח ש־$K \subseteq D$ הוא תת־שדה מקסימלי, וש־K/F היא הרחבת גלואה, עם חבורת גלואה G. אלגברת חילוק כזו נקראת **מכפלה משולבת**. הראה ש־D הוא מודול שמאלי מעל K, ושיש לו בסיס $\{z_g :\ g \in G\}$ כך ש־$z_g k = g(k) z_g$ לכל $g \in G$ ו־$k \in K$. הראה שהסקלרים $c_{g,h} = z_g z_h z_{gh}^{-1}$ שייכים ל־$K^{\times}$, ומקיימים את הזהות $c_{pq,r}c_{p,q} = p(c_{q,r})c_{p,qr}$.

8.1.2 מטריצות מעל חוג עם חילוק

כידוע, **חוג ארטיני** (שמאלי) הוא חוג המקיים את תנאי השרשרת היורדת על אידיאלים שמאליים, ובאופן שקול לזה, בכל קבוצת אידיאלים שמאליים שלו יש איבר מינימלי.

אלגברה לינארית היא התאוריה של מרחבים וקטוריים מעל שדה. אפשר לפתח תורה דומה גם מעל חוגים עם חילוק, אם מקפידים לקבוע את הצד שבו פועלים הסקלרים. כך למשל, כל אלגברה המכילה חוג עם חילוק D מהווה מודול (שמאלי) מעליו. כל מודול מעל חוג עם חילוק הוא חופשי, ולכן קיים לו מימד (שמאלי).

תרגיל 8.1.9 אם לאלגברה יש ממד סופי מעל חוג עם חילוק, אז היא ארטינית. (כל אידיאל שמאלי הוא תת־מודול, והממד חוסם את האורך של שרשראות.)

תרגיל 8.1.10 יהי D חוג עם חילוק. נסמן $L_v = \mathrm{M}_n(D)v$, כאשר $v \in D^n$. זהו אידיאל שמאלי של $\mathrm{M}_n(D)$. הראה שכל אידיאל שמאלי הוא סכום של אידיאלים מהצורה L_v.

טענה 8.1.11 האורך של $\mathrm{M}_n(D)$, כמודול מעל עצמו, הוא n.

הוכחה. אפשר להציג את החוג כסכום ישר של אידיאלים שמאליים,

$$\mathrm{M}_n(D) = \mathrm{M}_n(D)e_{11} \oplus \cdots \oplus \mathrm{M}_n(D)e_{1n}.$$

□

בפרט, לכל חוג עם חילוק D, חוג המטריצות $\mathrm{M}_n(D)$ הוא פשוט וארטיני. המשפט המרכזי שנוכיח בהמשך (משפט 8.2.16) קובע שגם ההיפך נכון: כל חוג פשוט ארטיני הוא חוג מטריצות מעל חוג עם חילוק.

טענה 8.1.12 כל חוג מהצורה $R = \mathrm{M}_{n_1}(D_1) \oplus \cdots \oplus \mathrm{M}_{n_t}(D_t)$, כאשר $D_1, \dots, D_t$ הם חוגים עם חילוק, הוא פשוט למחצה.

הוכחה. כל חוג עם חילוק הוא פשוט למחצה (כי האידיאל השמאלי המינימלי היחיד הוא החוג עצמו). חוג המטריצות $\mathrm{M}_n(D)$ פשוט למחצה לפי תרגיל 8.1.10. אם $R_1, \dots, R_n$ פשוטים למחצה אז R_i פריק לחלוטין כמודול מעל עצמו, ולכן גם מעל הסכום הישר $R = R_1 \oplus \cdots \oplus R_n$, הפועלת על R_i לפי הרכיב ה־i. זה מספק הצגה של R כסכום ישר של מודולים פריקים לחלוטין מעל עצמו. □

את הכיוון ההפוך (כל חוג פשוט למחצה הוא מכפלה של חוגי מטריצות מעל חוגים עם חילוק) נראה במשפט 8.4.11.

8.1.3 אלגברת וייל

אלגברת וייל, שנבנה בתת־הסעיף הזה, היא אלגברה פשוטה שאינה ארטינית.

דוגמא 8.1.13 נגדיר את **אלגברת וייל** $\mathbb{A}_1$ כחוג הנוצר על ידי היוצרים x, y עם יחס אחד:

$$\mathbb{A}_1 = F\langle x, y \mid yx - xy = 1\rangle;$$

לכן $\mathbb{A}_1 = \sum Fx^iy^j = \sum F[x]y^j$.

תרגיל 8.1.14
1. $[y, f] = \frac{d}{dx}f$ לכל $f \in F[x]$, ו־$[g, x] = \frac{d}{dy}g$ לכל $g \in F[y]$. **הדרכה.** מדובר בנגזרת הפורמלית $\frac{d}{dx}x^n = nx^{n-1}$; $[y, x^n] = nx^{n-1}$ באינדוקציה.
2. $\mathbb{A}_1$ הוא תחום (היינו, אין בו מחלקי אפס). **הדרכה.** נסמן $\overline{\sum_{i=0,\dots,n} f_iy^i} = f_n$, כלומר המקדם העליון ביחס ל־y; אז $\overline{fg} = \overline{f}\overline{g}$.
3. $\mathbb{A}_1$ אינו ארטיני. **הדרכה.** הראה ש־$\mathbb{A}_1 \supset \mathbb{A}_1y \supset \mathbb{A}_1y^2 \supset \cdots$.
4. ל־$\mathbb{A}_1$ אין אידיאלים שמאליים מינימליים.
5. אם $\mathrm{char}F = 0$ אז $\mathbb{A}_1$ אלגברה פשוטה. **הדרכה.** אם $0 \neq \sum f_iy^i \in I \lhd \mathbb{A}_1$, אז גזירה חוזרת לפי x מספקת ערך $0 \neq g \in I \cap F[y]$, וגזירה לפי y מספקת סקלר שונה מאפס ב־I. **הערה.** במאפיין p, $\langle x^p - x - a, y^p - b\rangle \lhd \mathbb{A}_1$ לכל $a, b \in F$.
6. אין שיכון של $\mathbb{A}_1$ לאלגברת מטריצות מעל חוג קומוטטיבי ממאפיין אפס. **הדרכה.** העקבה.

תרגיל 8.1.15 יהי R חוג כלשהו. יהי $\sigma : R \to R$ אוטומורפיזם. העתקה אדיטיבית $\delta : R \to R$ המקיימת $\delta(ab) = \sigma(a)b + a\delta(b)$ נקראת σ־גזירה (כאשר $\sigma = \mathrm{id}_R$, σ־גזירה נקראת סתם גזירה). נסמן ב־$R[x; \sigma, \delta]$ את חוג הפולינומים ב־$R[x]$ עם החיבור הרגיל והכפל $xa = \sigma(a)x + \delta(a)$ לכל $a \in R$. חוג זה נקרא **הרחבת** Ore של R.

1. הצג את אלגברת וייל כמקרה פרטי של הבניה הזו.
2. הראה שאם הגזירה אינה פנימית (גזירה מהצורה $\delta(a) = ba - ab$) ו־R שדה אז $R[x; \sigma, \delta]$ פשוט (למעשה די להניח ש־R פשוט).
3. נניח ש־R חוג עם חילוק. הראה שעל־ידי החלפת משתנים מתאימה אפשר להניח ש־$\sigma = \mathrm{id}$ או ש־$\delta = 0$. **הדרכה.** נסמן $F = \mathrm{Z}(R)$. אם יש $a \in F$ כך ש־$\sigma(a) \neq a$, כך $x' = x + (a - \sigma(a))^{-1}\delta(a)$ והראה ש־$R[x; \sigma, \delta] \cong R[x'; \sigma, 0]$. אחרת σ הוא הזהות על F; לפי משפט סקולם־נתר (תרגיל 8.3.9), יש u כך ש־$\sigma(c) = ucu^{-1}$ לכל $c \in R$, ואז $R[x; \sigma, \delta] \cong R[u^{-1}x; 1; u^{-1}\delta]$.

8.2 חוגים פרימיטיביים

בסעיף זה נעסוק בחוגים פרימיטיביים, שהם החוגים המתאימים ביותר להפעלת משפט הצפיפות.

8.2.1 מודולים נאמנים

הגדרה 8.2.1 *יהי M מודול מעל חוג R. **המאפס של M הוא אוסף האברים** $\mathrm{Ann}(M) = \{a \colon aM = 0\} \subseteq R$.*

תרגיל 8.2.2 יהי M מודול מעל חוג R.

1. $\mathrm{Ann}(M) \lhd R$; זהו אידיאל אמיתי אלא אם $M = 0$.
2. M הוא מודול מעל חוג המנה R/I, ביחס לפעולה $(a + I)x = ax$, אם ורק אם $I \subseteq \mathrm{Ann}(M)$.
3. $R/\mathrm{Ann}(M)$ היא המנה המינימלית של R ש־M מודול מעליה.

הגדרה 8.2.3 *מודול M מעל חוג R **הוא נאמן אם** $\mathrm{Ann}(M) = 0$.*

(כל מודול מעל חוג מנה של R אפשר לראות גם כמודול מעל החוג, אבל רק מודולים נאמנים משקפים את המבנה האמיתי של החוג עצמו, ולא של חוגי המנה שלו.)

את המאפס של מודול יש להשוות למאפס של איבר במודול: אם M מודול מעל R, אז לכל $x \in M$, $\mathrm{Ann}(x) = \{a \in R \colon ax = 0\}$; זהו אידיאל שמאלי של R, שאינו בהכרח דו־צדדי.

במשפט הצפיפות הכללי עסקנו בתמונה של R בתוך $\hat{R} = \mathrm{End}(M_T)$, כאשר $_RM$ מודול שמאלי מעל R ו־$T = \mathrm{End}(_RM)$.

טענה 8.2.4 **הגרעין של $R \to \hat{R}$ הוא המאפס $\mathrm{Ann}(M) = \{a \in R \colon aM = 0\}$. בפרט, $R \hookrightarrow \hat{R}$ אם ורק אם $_RM$ נאמן.**

8.2.2 מודולים פשוטים

לפני שנפעיל את משפט הצפיפות עבור מודולים פשוטים, נציין כמה תכונות של מודולים כאלה.

תרגיל 8.2.5 1. כל מודול פשוט הוא ציקלי.

2. מודול ציקלי איזומורפי למודול מהצורה R/L כאשר L אידיאל שמאלי של R.

3. מודול המנה R/L הוא פשוט אם ורק אם L אידיאל שמאלי מקסימלי.

תרגיל 8.2.6 (חוג האנדומורפיזמים של מודול ציקלי) יהי $L \leq_\ell R$ אידיאל שמאלי. נסמן $L^* = \{a \in R\colon\ La \subseteq L\}$. הוכח ש־$L^*$ הוא תת־החוג המקסימלי של R שבו L הוא אידיאל דו־צדדי.

הראה שכל אנדומורפיזם של המודול הציקלי $M = R/L$ הוא מהצורה $r_a\colon x + L \mapsto xa + L$ עבור $x \in L^*$, והסק ש־$\operatorname{End}(_RM) = (L^*/L)^{\text{op}}$. נסמן $La^{-1} = \{x \in R\colon\ xa \in L\}$; זהו אידיאל שמאלי, המכיל את L אם $a \in L^*$. האנדומורפיזם r_a $(a \in L^*)$ הוא חד־חד־ערכי אם ורק אם $La^{-1} = L$; ו־r_a על אם ורק אם Ra קו־מקסימלי ביחס ל־L.

מצא קשר בין האידיאלים השמאליים של L^*/L לבין האידיאלים השמאליים של R/L (לפי הלמה של שור, 8.2.12, אם ב־R/L אין אידיאלים מקסימליים אז גם ב־L^*/L אין אידיאלים מקסימליים).

8.2.3 פרימיטיביות

הגדרה 8.2.7 ***חוג שיש לו מודול פשוט נאמן נקרא חוג פרימיטיבי.***

תרגיל 8.2.8 המאפס של מודול פשוט R/L, היינו $\operatorname{Ann}(R/L) = \{a\colon\ aR \subseteq L\}$, הוא האידיאל הדו־צדדי המקסימלי המוכל ב־L.

בפרט, מודול מהצורה R/L הוא נאמן אם ורק אם L אינו מכיל אף אידיאל דו־צדדי (שונה מאפס).

מסקנה 8.2.9 חוג הוא פרימיטיבי אם ורק אם יש לו אידיאל שמאלי מקסימלי שאינו מכיל אף אידיאל דו־צדדי.

טענה 8.2.10 כל חוג פשוט הוא פרימיטיבי.

הוכחה. יהי L אידיאל שמאלי מקסימלי (קיים לפי הלמה של צורן); המנה R/L היא מודול פשוט, שהוא נאמן כי המאפס שלו, שהוא אידיאל, מוכרח להיות שווה לאפס. □

טענה 8.2.11 חוג פרימיטיבי קומוטטיבי הוא שדה.

הוכחה. לפי מסקנה 8.2.9. □

משפט הצפיפות הכללי חל כאשר M מודול פריק לחלוטין; כלומר, סכום של תת־מודולים פשוטים. אם נניח ש־M פשוט, נקבל במשפט הצפיפות תכונות נוספות ובלתי צפויות. המפתח לכך הוא הלמה הבאה.

למה 8.2.12 (הלמה של שור) יהי ${}_RM$ מודול פשוט. אז $T = \mathrm{End}({}_RM)$ הוא חוג עם חילוק.

הוכחה. יהי $0 \neq f \in \mathrm{End}({}_RM)$, כלומר $f : M \to M$ הומומורפיזם שאינו אפס. לכן $0 \neq \mathrm{Im}(f) \leq M$ ומכיוון ש־M פשוט, f על; ו־$\mathrm{Ker}(f) < M$, ומאותה סיבה $\mathrm{Ker}(f) = 0$, כך ש־f חד־חד־ערכי. מכאן ש־f הפיך. □

מסקנה 8.2.13 כל חוג פרימיטיבי אפשר לשכן בחוג אנדומורפיזמים של מרחב וקטורי מעל חוג עם חילוק.

הוכחה. יהי M מודול פשוט ונאמן מעל R. לפי טענה 8.2.4, $R \hookrightarrow \hat{R} = \mathrm{End}(M_D)$ כאשר $D = \mathrm{End}({}_RM)$ הוא חוג עם חילוק לפי הלמה של שור. □

משפט 8.2.14 (משפט הצפיפות של ג'ייקובסון) *יהי ${}_RM$ מודול פשוט ונאמן מעל חוג R. יהיו $x_1, \dots, x_n \in M$ בלתי תלויים מעל $D = \mathrm{End}({}_RM)$, ו־$y_1, \dots, y_n \in M$; אז קיים $r \in R$ כך ש־$rx_i = y_i$.* ◦

הוכחה. נתונים $x_1, \dots, x_n \in M$ בלתי תלויים מעל D, שהוא חוג עם חילוק לפי הלמה של שור. לכן אפשר להשלים את הקבוצה לבסיס של M מעל T, ולהגדיר $f \in \mathrm{End}(M_D)$ לפי $f(x_i) = y_i$ ו־$f(x) = 0$ לשאר אברי הבסיס. מכיוון ש־M פשוט, הוא פריק לחלוטין. לפי משפט הצפיפות הכללי, יש $r \in R$ כך ש־$rx_i = f(x_i) = y_i$, כדרוש. □

להלן גרסה חזקה של משפט 8.2.14:

מסקנה 8.2.15 יהי ${}_RM$ מודול פשוט ונאמן מעל חוג R, $D = \mathrm{End}({}_RM)$. אם $[M:D] = n$, אז $R \cong \hat{R} \cong \mathrm{M}_n(D)$. ◦

הוכחה. יהי $x_1, \dots, x_n$ בסיס של M מעל D, ויהי $h \in \hat{R}$. נבחר $y_i = h(x_i)$, אז לפי משפט הצפיפות יש $r \in R$ כך ש־$\hat{r}(x_i) = rx_i = y_i = h(x_i)$ לכל i. לכן $\hat{r} = h$ על אברי הבסיס, ומכאן ש־$h = \hat{r}$. □

משפט 8.2.16 (משפט ודרברן־ארטין) *יהי R חוג פרימיטיבי ארטיני. אז $R \cong \mathrm{M}_n(D)$.* ◦

הוכחה. לפי טענה 8.2.10, R פרימיטיבי, ולכן יש לו מודול פשוט נאמן. לפי הלמה של שור $D = \mathrm{End}({}_RM)$ הוא חוג עם חילוק, ו־$R \subseteq \hat{R} = \mathrm{End}(M_D)$; לפי משפט הצפיפות, R צפוף שם. כדי ליישם את המסקנה, מספיק להראות ש־$[M:D] < \infty$. אחרת, יש קבוצה בלתי תלויה $x_1, x_2, \dots$ ב־M מעל D, ואם ניקח $L_m = \mathrm{Ann}(\{x_1, \dots, x_m\})$ נקבל שרשרת יורדת $L_1 \supseteq L_2 \supseteq \cdots$. לכל m יש $r \in R$ כך ש־$rx_1 = \cdots = rx_m = 0$ ו־$rx_{m+1} = x_{m+1} \neq 0$, ובפרט $r \in L_m$, $r \notin L_{m+1}$. לכן השרשרת יורדת ממש, וזו סתירה לארטיניות של R. □

המקרה הכללי אינו רחוק ממשפט 8.2.16:

משפט 8.2.17 *יהי R חוג פרימיטיבי שמרכזו השדה F. או שקיים חוג עם חילוק D (עם אותו מרכז) כך ש־$R = \mathrm{M}_n(D)$, או שלכל n יש ל־R תת־חוג ש־$\mathrm{M}_n(F)$ הוא תמונה הומומורפית שלו.*

הוכחה. כמו במשפט 8.2.16, יש ל־R מודול פשוט ונאמן M, ו־$D = \mathrm{End}({}_RM)$ הוא חוג עם חילוק, ש־M הוא מודול ימני מעליו. אם M סופי מעל D, סיימנו. יהי n כלשהו. מכיוון ש־M אינו סופי מעל D, יש קבוצה בלתי תלויה $x_1, \dots, x_n \in M_D$. נסמן $M_n = \sum x_iD \subseteq M$. נתבונן ב־$R_n = \{r \in R : rM_n \subseteq M_n\}$. זה תת־חוג של R, ו־M_n מודול מעליו. לכן מוגדר הומומורפיזם $R \to \mathrm{End}((M_n)_D) = \mathrm{M}_n(D)$. ההומומורפיזם הזה הוא על, משום שכל פעולה על M_n אפשר לממש על־ידי איבר של R, השייך ל־R_n לפי ההגדרה. כדי לסיים אפשר לקחת את התמונה ההפוכה של $\mathrm{M}_n(F)$ ב־$\mathrm{M}_n(D)$, שהיא תת־חוג של R_n. □

8.2.4 דוגמאות לחוגים פרימיטיביים

היפוך של משפט הצפיפות, על־ידי זיהוי תת־חוגים צפופים של חוג אנדומורפיזמים, מספק דרך קלה לבנות חוגים פרימיטיביים. יהיו F שדה, $_FV$ מרחב וקטורי. נקבע טרנספורמציות $r_i\colon V\to V$, ונגדיר $R = F\{r_1,\dots,r_n\}$, כלומר תת־האלגברה של $\operatorname{End}(V_F)$ הנוצרת על־ידי האברים r_i. הפעולה היא זו המושרית מפעולת $\operatorname{End}(V_F)$, היינו הרכבה בסדר הרגיל.

טענה 8.2.18 אם $R \subseteq \operatorname{End}(V)$ פועל טרנזיטיבית על $V-\{0\}$ אז R פרימיטיבי.

הוכחה. **מכיוון ש־$R \subseteq \operatorname{End}(V)$, המודול V נאמן כעניין של הגדרה; אם הפעולה טרנזיטיבית אז המודול פשוט לפי תרגיל 1.1.12.** $\square$

תרגיל 8.2.19 יהי V מרחב וקטורי ממימד אינסופי α.

1. הראה ש־V מודול פשוט ונאמן מעל $\operatorname{End}(V)$, ולכן $\operatorname{End}(V)$ פרימיטיבי.
2. הראה ש־$\operatorname{End}(V)$ אינו פשוט. **הדרכה**. תהי $\beta < \alpha$ עוצמה אינסופית כלשהי; הראה ש־$I_\beta = \{x \in \operatorname{End}(V)\colon\ \dim \operatorname{Im}(x) < \beta\}$ הוא אידיאל אמיתי.
3. ל־$\operatorname{End}(V)$ יש אידיאל שמאלי מינימלי. **הדרכה**. לכל תת־מרחב $V_0 \leq V$, $L_{V_0} = \{x \in \operatorname{End}(V)\colon\ x(V_0) = 0\}$ הוא אידיאל שמאלי. אם $\dim(V/V_0) = 1$, זהו אידיאל שמאלי מינימלי.
4. $\operatorname{End}(V)$ אינו נתרי ואינו ארטיני.

כדי לראות את אלגברת וייל $\mathbb{A}_1$ מתת־סעיף 8.1.3 בהקשר של הבניה הכללית, נסמן $V = F[x]$ ונגדיר את ההעתקות $X, Y \in \operatorname{End}(V)$ לפי $Xf = xf$ ו־$Yf = \frac{d}{dx}f$. העתקות אלו מקיימות $(YX - XY)f = (xf)' - xf' = f$, כלומר $YX - XY = 1$.

תרגיל 8.2.20 $\mathbb{A}_1 \cong F[X,Y] \subseteq \operatorname{End}(F[x])$. **הדרכה**. ההעתקה $X \mapsto x$, $Y \mapsto y$ מראה ש־$F[X,Y]$ היא מנה של $\mathbb{A}_1$. נראה שזהו למעשה איזומורפיזם. במאפיין אפס אין מה להוכיח (כי הגרעין מוכרח להיות אפס). מעל כל שדה, אם $\sum \alpha_{ij}X^iY^j = 0 \mapsfrom \sum \alpha_{ij}x^iy^j$ אז $\sum_j(\sum_i \alpha_{ij}x^i)(\frac{d}{dx})^j g = 0$ לכל $g \in F[x]$; בחר $g = x^j$ עבור j המינימלי עם $\sum \alpha_{ij}x^i \neq 0$, וקבל סתירה.

תרגיל 8.2.21 הוכח שבמאפיין אפס, $F[X,Y]$ פועלת טרנזיטיבית על $F[x]$, והיא פרימיטיבית לפי טענה 8.2.18. **הערה**. הראה שבמאפיין p הפעולה אינה טרנזיטיבית.

תרגיל 8.2.22 נגדיר $\mathbb{A}_n(F) = F[x_1,\dots,x_n,y_1,\dots,y_n]$ להיות האלגברה הכפופה ליחסים $[y_i,x_i] = 1$ כאשר כל שני יוצרים אחרים מתחלפים (זוהי **אלגברת וייל** ה־n־ית). הראה ש־$\mathbb{A}_n$ פשוטה.

8.3 חוגים ארטיניים ראשוניים

הגדרה 8.3.1 *חוג R הוא **ראשוני** אם לכל שני אידיאלים $A, B \neq 0$, גם $AB \neq 0$.*

טענה 8.3.2 כל חוג פרימיטיבי הוא ראשוני.

הוכחה. יהי M מודול פשוט ונאמן מעל R, ויהיו $A, B \neq 0$ אידיאלים של R. יש $0 \neq b \in B$, ומכיוון ש־M נאמן, $0 \neq bM \subseteq BM$, ולכן $0 \neq BM \leq M$; אבל M פשוט, ולכן $BM = M$. באותו אופן גם $ABM = AM \neq 0$, ולכן $AB \neq 0$. □

מתברר שלאידיאלים שמאליים מינימליים יש תפקיד חשוב ביותר, אם הם קיימים. נזכיר ש־$\operatorname{soc}({}_RR)$ הוא סכום תת־המודולים הפשוטים, כלומר סכום האידיאלים השמאליים המינימליים; לכן יש לחוג R אידיאל שמאלי מינימלי, אם ורק אם $\operatorname{soc}(R) \neq 0$.

תרגיל 8.3.3 לכל אידיאל שמאלי מינימלי L ולכל $a \in R$, או ש־$La = 0$ או ש־La מינימלי. **הדרכה**. יש הומומורפיזם של מודולים $L \to La$ המוגדר לפי $x \mapsto xa$, שהוא או אפס או איזומורפיזם.

טענה 8.3.4 יהי R חוג ראשוני שיש לו אידיאל שמאלי מינימלי $L \neq 0$. °

1. R פרימיטיבי.
2. L הוא המודול הפשוט והנאמן היחיד של R.

הוכחה. לפי המינימליות, L מודול פשוט. נסמן $A = \operatorname{Ann}(L)$, אז $A(LR) = (AL)R = 0$ ולכן $A = 0$, כלומר L נאמן. מכאן ש־R פרימיטיבי. כעת יהי M מודול פשוט ונאמן כלשהו. אז $LM \neq 0$ כי M נאמן, ולכן קיים $x \in M$ כך ש־$Lx = M$, שהרי M פשוט. לפי תרגיל 8.3.3, $L \cong M$. □

מסקנה 8.3.5 יהי R חוג ראשוני ארטיני. אז $R \cong \mathrm{M}_n(D)$. בפרט, בין החוגים הארטיניים, ראשוני = פרימיטיבי = פשוט.

הוכחה. מכיוון ש־R ארטיני יש לו אידיאל שמאלי מינימלי. לפי טענה 8.3.4 R פרימיטיבי, ולכן חל משפט 8.2.16. □

מסקנה 8.3.6 יהי R חוג ארטיני. כל אידיאל ראשוני של R הוא מקסימלי. (השווה לטענה 5.1.9 מהקורס הקומוטטיבי.) °

טענה 8.3.7 לכל חוג R, $\operatorname{soc}(R)$ הוא אידיאל דו־צדדי (או R כולו).

הוכחה. לפי תרגיל 8.3.3, לכל אידיאל שמאלי מינימלי L ולכל $a \in R$, אם $La \neq 0$ אז הוא מינימלי, ולכן לכל $a \in R$, $\operatorname{soc}(R)a = \sum La = \sum L = \operatorname{soc}(R)$, כאשר הסכום על־פני האידיאלים השמאליים המינימליים. לכן $\operatorname{soc}(R) \lhd R$. □

טענה 8.3.8 כל חוג פשוט עם אידיאל שמאלי מינימלי הוא ארטיני.

הוכחה. לפי טענה 8.3.7, $\operatorname{soc}(R) \neq 0$ ולכן $\operatorname{soc}(R) = R$ ו־R פשוט למחצה. □

אם לסכם, קיבלנו את ההיררכיה הבאה למחלקות של חוגים:

$$\begin{tikzcd}
 & \mathrm{M}_n(D) = \text{פשוט ארטיני} \arrow[dl, Rightarrow] \arrow[d, Rightarrow] \\
\text{ראשוני עם שמאלי מינימלי} \arrow[dr, Rightarrow] & \text{פשוט} \arrow[d, Rightarrow] \\
 & \text{פרימיטיבי} \arrow[d, Rightarrow] \\
 & \text{ראשוני}
\end{tikzcd}$$

דוגמאות נגדיות לגרירות בכיוון ההפוך: $\mathrm{End}(V)$ מתרגיל 8.2.19 הוא פרימיטיבי עם אידיאל שמאלי מינימלי, אבל אינו פשוט ואינו ארטיני. אלגברת וייל היא פשוטה אבל לא ארטינית (ואף אין לה אידיאל שמאלי מינימלי).

תרגיל 8.3.9 הוכח את **משפט סקולם־נתר**: כל אוטומורפיזם של חוג פשוט ארטיני, המשרה את אוטומורפיזם הזהות על המרכז, הוא פנימי (כלומר מהווה הצמדה באיבר קבוע). **הדרכה**. טענה 8.3.4 והעובדה שחוג עם חילוק פשוט כמודול מעל עצמו.

תרגיל 8.3.10 הוכח את **הלמה של בראואר**: יהי L אידיאל שמאלי מינימלי בחוג R כך ש־$L^2 \neq 0$. אז קיים אידמפוטנט e כך ש־$L = Re$; ואז eRe הוא חוג עם חילוק.

הדרכה. לפי ההנחה קיים $a \in L$ כך ש־$La \neq 0$, ואז $0 \neq La \subseteq L^2 \subseteq L$, ולפי המינימליות $L = La$. לכן $a \in L = La$ ויש $e \in L$ כך ש־$a = ea$. נתבונן ב־$Q = \{x \in L\colon\ xa = 0\}$. ברור ש־$Q \subseteq L$ הוא אידיאל שמאלי, אבל $e \notin Q$ ולכן $Q \subset L$, ולפי המינימליות $Q = 0$. אבל $(e^2 - e)a = 0$, ומכאן ש־$e^2 - e \in Q = 0$, כלומר e אידמפוטנט. כעת $0 \neq e = e^2 \in Re \subseteq L$, ושוב לפי המינימליות $L = Re$, כפי שרצינו.

יהי $0 \neq ebe \in eRe$ איבר כלשהו. אם $Lb = 0$ אז $ebe \in Lbe = 0$, בסתירה להנחה, ולכן $Lb = L$. כעת $eRe \cdot ebe = eRebe = eLbe = eLe = e(Re)e = eRe$, כלומר, ל־$eRe$ אין אידיאלים שמאליים אמיתיים, ולכן כל איבר הפיך משמאל. מכאן ש־eRe חוג עם חילוק.

8.4 חוגים ראשוניים למחצה

נזכיר שהרדיקל הראשוני $\mathrm{rad}(R)$ של חוג R שווה לחיתוך כל האידיאלים הראשוניים שלו. בהגדרה 4.2.15 קראנו לחוג קומוטטיבי "ראשוני למחצה" אם אין בו איברים נילפוטנטיים, ואז ראינו שהרדיקל הראשוני של חוג כזה הוא אפס. נאמץ תכונה זו כהגדרה למקרה הכללי.

הגדרה 8.4.1 *חוג R נקרא **ראשוני למחצה** אם* $\mathrm{rad}(R) = 0$.

ברור שכל חוג ראשוני הוא ראשוני למחצה. אומרים שחוג R הוא **מכפלה תת־ישרה** של החוגים S_λ אם יש שיכון $R \hookrightarrow \prod_\lambda S_\lambda$, כך שהטלת התמונה על כל רכיב בנפרד היא על.

הערה 8.4.2 R הוא ראשוני למחצה אם ורק אם הוא מכפלה תת־ישרה של המנות הראשוניות שלו.

8.4.1 הרדיקל הוא נילי

למה 8.4.3 בכל חוג R, $\mathrm{rad}(R)$ הוא אידיאל נילי.

הוכחה. **זוהי מסקנה 4.2.29, הנכונה גם כשהחוג לא קומוטטיבי. (תמצית ההוכחה: אם a אינו נילפוטנטי, קח P מקסימלי ביחס לכך ש־$a^n \notin P$ לכל n; אידיאל כזה הוא ראשוני משום שאם $A, B \supset P$ אז AB נחתך עם S ולכן אינו מוכל ב־P. מכיוון ש־$a \notin P$ כאשר P ראשוני, $a \notin \mathrm{rad}(R)$.)** □

בפרט, חוג שאין לו אידיאלים ניליים הוא ראשוני למחצה.

8.4.2 ראשוני למחצה = אין אידיאלים נילפוטנטיים

תרגיל 8.4.4 בחוג אין אידיאלים נילפוטנטיים אם ורק אם $A^2 = 0$ גורר $A = 0$, אם ורק אם $xRx \neq 0$ לכל $x \neq 0$. **הדרכה**. אם $xRx = 0$ אז $(RxR)^2 = RxRxR = 0$.

למה 8.4.5 **תהי $x_1, x_2, \ldots$ סדרת אברים בחוג R, כך ש־$0 \neq x_{n+1} \in (Rx_nR)^2$ לכל n. אז יש אידיאל ראשוני שאינו מכיל אף x_n.**

הוכחה. **כמו במסקנה 4.2.26: יהי P אידיאל מקסימלי ביחס לתכונה $x_i \notin P$ לכל i (יש אידיאל כזה כי 0 מקיים את התנאי); נניח ש־$A, B \supset P$, אז מכיוון ש־$Rx_{i+1}R \subseteq Rx_iR$ לכל i, קיים n כך ש־$x_n \in A, B$, ואז $x_{n+1} \in x_nRx_n \subseteq ARB = AB \subseteq P$, בסתירה להנחה. לכן P ראשוני.** □

משפט 8.4.6 ***חוג הוא ראשוני למחצה אם ורק אם אין לו אידיאלים נילפוטנטיים.***

הוכחה. **ברור שכל אידיאל נילפוטנטי מוכל בכל אידיאל ראשוני, ולכן ב־$\mathrm{rad}(A) = 0$. מצד שני נניח שלכל $x \neq 0$ גם $xRx \neq 0$, ונראה שהחוג ראשוני למחצה. יהי $x_0 \neq 0$. נניח שבחרנו את $x_i \neq 0$; לפי ההנחה יש $0 \neq x_{i+1} \in x_iRx_i$. לפי למה 8.4.5, יש ראשוני P כך ש־$x_0 \notin P$, ואז $x_0 \notin \mathrm{rad}(A)$. לכן $\mathrm{rad}(R) = 0$.** □

תרגיל 8.4.7 חוג הוא ראשוני למחצה אם ורק אם $L^2 \neq 0$ לכל אידיאל שמאלי $0 \neq L \leq R$. **הדרכה**. אם $(Rx)^2 = 0$ אז $(RxR)^2 = RxRxR = (Rx)^2R = 0$.

תרגיל 8.4.8 בחוג ראשוני למחצה, אם $AB = 0$ (כאשר $A \leq_r R$, $B \leq_\ell R$) אז $BA = 0$.
פתרון. $(BA)^2 = BABA = 0$ ***לפי ההנחה, ולכן*** $BA = 0$.

תרגיל 8.4.9 בהמשך לתרגיל 8.3.10, נניח ש־R ראשוני למחצה, ויהי $L = Re$ אידיאל שמאלי מינימלי (כאשר e אידמפוטנט). אז eR אידיאל ימני מינימלי.

8.4.3 חוג ראשוני למחצה ארטיני

הערה 8.4.10 בטענה 5.3.3 הראינו שלחוג ארטיני קומוטטיבי יש מספר סופי של אידיאלים ראשוניים. טענה זו נכונה גם עבור חוגים לא קומוטטיביים. ההוכחה חלה במקרה הזה מלה במלה, פרט להחלפת טענה 5.1.9 במסקנה 8.3.6:

אחרת, יהיו $P_1, P_2, \ldots$ 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 מסקנה 8.3.6, P_i מקסימלי, כך ש־$P_i = P_{n+1}$, בסתירה להנחה.

המשפט החשוב הבא הוא גרסה לא קומוטטיבית של טענה 5.3.4.

משפט 8.4.11 *התנאים הבאים שקולים:*

(1) R *פשוט למחצה.*

(2) R *ראשוני למחצה ארטיני (שמאלי).*

(3) R *הוא מכפלה ישרה של מספר סופי של חוגי מטריצות מעל חוגים עם חילוק.*

הוכחה. $(1) \Longleftarrow (2)$: נניח ש־R פשוט למחצה; לפי הערה 7.2.27, יש אידיאלים שמאליים מינימליים $L_1, \dots, L_n$ כך ש־$R = L_1 + \cdots + L_n$. מכאן ש־$\ell(R) \leq \ell(L_1) + \cdots + \ell(L_t) = t$, כלומר R בעל אורך סופי ולכן ארטיני. נסמן $P_i = \mathrm{Ann}(L_i)$, אז L_i הוא מודול פשוט ונאמן מעל R/P_i. מכאן ש־R/P_i פרימיטיבי, ולכן ראשוני. מאידך אם $a \in \cap P_i = \cap \mathrm{Ann}(L_i)$ אז $a \in aR \subseteq aL_1 + \cdots + aL_n = 0$, ולכן $\cap P_i = 0$. $(2) \Longleftarrow (3)$: לפי טענה 8.4.10 יש לחוג מספר סופי של אידיאלים ראשוניים. לכל אידיאל ראשוני P_i, R/P_i הוא ארטיני ראשוני, ולכן איזומורפי לחוג מטריצות מעל חוג עם חילוק, ובפרט הוא פשוט; כלומר P_i מקסימלי. לפי משפט השאריות הסיני, $R \cong R/P_1 \times \cdots \times R/P_t$, כנדרש.

טענה 8.1.12 מוכיחה את $(3) \Longleftarrow (1)$. □

הערה 8.4.12 תנאי (3) במשפט 8.4.11 הוא סימטרי להחלפת ימין־שמאל, ולכן התנאים המופיעים בו שקולים גם ל־

(1′) R הוא סכום האידיאלים הימניים המינימליים שלו.

(2′) R ארטיני ימני וראשוני למחצה.

בפרט, עבור חוגים ראשוניים למחצה, ארטיניות שמאלית שקולה לארטיניות ימנית. זה לא נכון בדרך כלל, ראה תרגיל 7.3.2.

הערה 8.4.13 בספרים אחדים מוגדר חוג פשוט למחצה כחוג שחיתוך האידיאלים המקסימליים שלו הוא אפס; נאמר שזה "המובן החלש" של המונח. חוג הוא פשוט למחצה במובן שלנו, אם ורק אם הוא פשוט למחצה במובן החלש, וארטיני.

8.4.4 מהמקרה הכללי לחוג ראשוני למחצה

טענה 8.4.14 לכל חוג R, המנה $R/\mathrm{rad}(R)$ ראשונית למחצה (כלומר $\mathrm{rad}(R/\mathrm{rad}(R)) = 0$).

הוכחה. נסמן $N = \mathrm{rad}(R)$. לכל אידיאל ראשוני $P \lhd R$ מתקיים $N \subseteq P$ ולכן $P/N \lhd R/N$ הוא ראשוני. לכן חיתוך כל האידיאלים הראשוניים של R/N שווה לחיתוך כל האידיאלים הראשוניים של R, מודולו N, והמנה הזו היא אפס. □

מסקנה 8.4.15 יהי R חוג ארטיני. אז $R/\mathrm{rad}(R)$ פשוט למחצה.

הוכחה. לפי טענה 8.4.14 $R/\mathrm{rad}(R)$ ראשוני למחצה, ולפי משפט 8.4.11 (ותרגיל 1.3.14), $R/\mathrm{rad}(R)$ פשוט למחצה. □

8.5 משפט הופקינס־לויצקי

טענה 8.5.1 בחוג ארטיני R, כל אידיאל שמאלי נילי הוא נילפוטנטי. (השווה לטענה 5.2.7.)

הוכחה. **יהי N אידיאל שמאלי נילי. מכיוון שהחוג ארטיני, השרשרת היורדת $N \supseteq N^2 \supseteq N^3 \supseteq \cdots$ נעצרת, וקיים t כך ש־$N^t = N^{t+1}$. נסמן $N' = N^t$, אז $N'^2 = N'$. נניח בשלילה ש־$N' \neq 0$. לפי הארטיניות קיים אידיאל שמאלי $0 \neq L \subseteq N$ שהוא מינימלי ביחס לתכונה $N'L = L$. לכל $a \in L$ מתקיים $N'(N'a) = N'^2a = N'a$, אבל $N'a \subseteq L$; אם $N'a \neq 0$ אז לפי המינימליות $L = N'a$, ולכן $a \in L = N'a$. מכאן שקיים $x \in N'$ כך ש־$a = xa$, אבל x נילי, ולכן $1-x$ הפיך ו־$a = 0$, בסתירה להנחה ש־$N'a \neq 0$. מכאן ש־$N'L = 0$, ואז $L = 0$, בסתירה להנחה ש־$L \neq 0$.** □

(גם בחוג נתרי, כל אידיאל חד־צדדי נילי הוא נילפוטנטי. לא נוכיח זאת כאן.)

תרגיל 8.5.2 מודול ארטיני אינו יכול להכיל סכום ישר אינסופי של תת־מודולים. **הדרכה**. אחרת $\sum_{i\geq 1} N_i > \sum_{i\geq 2} N_i > \sum_{i\geq 3} N_i > \cdots$ היא שרשרת יורדת אינסופית.

מסקנה 8.5.3 יהי M מודול ארטיני פריק לחלוטין. אז $\ell(M) < \infty$.

הוכחה. **כתוב את $M = \operatorname{soc}(M)$ כסכום ישר של תת־מודולים פשוטים, לפי טענה 7.2.9. הסכום מוכרח להיות סופי לפי תרגיל 8.5.2, ואז $\ell(M) = \ell(N_1) + \cdots + \ell(N_t) = t$.** □

משפט 8.5.4 (משפט הופקינס־לויצקי) *כל חוג ארטיני הוא נתרי.*

הוכחה. **יהי R חוג ארטיני. נסמן $N = \operatorname{rad}(R)$. לפי למה 8.4.3, N נילי, ומכאן שהוא נילפוטנטי לפי טענה 8.5.1. נניח ש־$N^n = 0$. נסמן $N^0 = R$. לכל $i \geq 0$, N מאפס את מודול המנה N^i/N^{i+1}, ולכן N^i/N^{i+1} הוא מודול מעל R/N, שהוא חוג פשוט למחצה לפי מסקנה 8.4.15. לפי טענה 7.2.28** (כל מודול מעל חוג פשוט למחצה R הוא פריק לחלוטין)**, נובע מכך שכל N^i/N^{i+1} הוא פריק לחלוטין. מכיוון ש־N^i ארטיני (כתת־מודול של R), גם N^i/N^{i+1} ארטיני ולפי מסקנה 8.5.3 האורך של N^i/N^{i+1} סופי. מכאן נובע שגם $\ell(R) = \ell(R/N) + \ell(N/N^2) + \cdots + \ell(N^{n-1}/N^n) < \infty$. מכיוון שהאורך של R סופי, הוא נתרי לפי טענה 1.3.8.** □

8.6 הרדיקל של ג'ייקובסון

יהי R חוג כלשהו. מגדירים את **רדיקל ג'ייקובסון** של החוג, $\operatorname{Jac}(R)$, להיות החיתוך של כל האידיאלים השמאליים המקסימליים. הרדיקל הזה מכיל את הרדיקל הראשוני $\operatorname{rad}(R)$, ולא מובטח שהוא נילי. עם זאת, בכמה מקרים חשובים $\operatorname{Jac}(R)$ נילי, ואף נילפוטנטי.

טענה 8.6.1 התכונות הבאות שקולות (ומגדירות את P כ**אידיאל פרימיטיבי**):

1. חוג המנה R/P פרימיטיבי.
2. P מאפס מודול פשוט ${}_RM$.
3. P הוא האידיאל הדו־צדדי המקסימלי המוכל באידיאל מקסימלי L.

הוכחה. אם P מאפס מודול פשוט ${}_RM$, אז M מודול פשוט ונאמן מעל R/P. בכיוון ההפוך, נניח ש־R/P פרימיטיבי, אז יש מודול פשוט ונאמן ${}_{R/P}M$. לפי ההנחה, המאפס של M מעל R/P הוא אפס, ולכן המאפס שלו כמודול מעל R שווה ל־P. אם $N < M$ תת־מודול, אז $PN \subseteq PM = 0$, ולכן N מודול מעל R/P, אבל מכיוון ש־M פשוט כמודול מעל R/P, בהכרח $N = 0$. לכן M פשוט מעל R, ו־P המאפס שלו. השקילות של (2) ו־(3) נובעת מתרגיל 8.2.8: המאפס של מודול פשוט R/L, כאשר $L \leq_\ell R$ אידיאל שמאלי מקסימלי, הוא האידיאל הדו־צדדי המקסימלי המוכל ב־L. □

מסקנה 8.6.2 כל אידיאל מקסימלי הוא פרימיטיבי וכל אידיאל פרימיטיבי הוא ראשוני (בגלל הטענה המקבילה על חוג המנה).

טענה 8.6.3 $\mathrm{Jac}(R)$ שווה לחיתוך האידיאלים הפרימיטיביים של R.

הוכחה. מחד, כל אידיאל פרימיטיבי מוכל באיזשהו אידיאל שמאלי מקסימלי לפי טענה 8.6.1. מאידך, יהי P אידיאל פרימיטיבי, אז הוא המאפס של איזשהו מודול $M = R/L$ עבור L שמאלי מקסימלי, ולכן $\mathrm{Jac}(R)M \subseteq LM = 0$, ומכאן ש־$\mathrm{Jac}(R) \subseteq \mathrm{Ann}(M) = P$. □

מסקנה 8.6.4 לכל חוג R, $\mathrm{rad}(R) \subseteq \mathrm{Jac}(R)$, כי כל האידיאלים הפרימיטיביים משתתפים בחיתוך היוצר את הרדיקל.

מסקנה 8.6.5 בחוג ארטיני, $\mathrm{Jac}(R) = \mathrm{rad}(R)$, משום שכל אידיאל ראשוני הוא פרימיטיבי לפי מסקנה 8.3.6.

תרגיל 8.6.6 לכל חוג R, $\mathrm{Jac}(R/\mathrm{Jac}(R)) = 0$.

כדי ללמוד את הסדרה היורדת של החזקות של $\mathrm{Jac}(R)$, נצטרך את הגרסה הבאה ללמה של נקיימה (משפט 2.2.3).

תרגיל 8.6.7 למודול נוצר סופית יש תת־מודול מקסימלי. **הדרכה.** נכתוב $M = Rx_1 + \cdots + Rx_n$ עבור n מינימלי. לפי הלמה של צורן קיים תת־מודול $N \supseteq Rx_1 + \cdots + Rx_{n-1}$, שהוא מקסימלי ביחס ל־$x_n \notin N$. ברור ש־$N < M$ תת־מודול מקסימלי. **הערה.** אם איננו יודעים ש־M נוצר סופית, ההוכחה נכשלת משום שאין דרך למנוע מהאיחוד של שרשרת תת־מודולים אמיתיים להיות המודול כולו.

הגרסה הקומוטטיבית של הלמה של נקיימה (מסקנה 2.2.4) קבעה שלכל מודול נוצר סופית M מעל חוג קומוטטיבי R, קיים אידיאל מקסימלי A כך ש־$AM \subset M$. מכיוון שבמקרה הקומוטטיבי אין הבדל בין אידיאל קומוטטיבי למקסימלי, טענה זו שקולה לכך ש־$J(R)M \subset M$.

למה 8.6.8 (הלמה של נקיימה, המקרה הכללי) לכל מודול נוצר סופית $0 \neq {}_RM$ מתקיים $J(R)M \subset M$.

הוכחה. יהי $N < M$ תת־מודול מקסימלי (תרגיל 8.6.7), אז M/N פשוט, ו־$P = \mathrm{Ann}(M/N)$ פרימיטיבי. אבל $PM \subseteq N \neq M$ לפי הגדרת P, ולכן $J(R)M \subseteq PM \neq M$. □

טענה 8.6.9 יהי R חוג נתרי. אם השרשרת

$$\cdots \subseteq J(R)^3 \subseteq J(R)^2 \subseteq J(R)$$

עוצרת, אז היא עוצרת באפס ו־$J(R)$ נילפוטנטי.

הוכחה. נסמן $J = J(R)$. נניח ש־$J^n = J^{n+1}$. לפי הנתריות J נוצר סופית כמודול מעל R, ולכן גם J^n נוצר סופית; אם $J^n \neq 0$ אז $J^{n+1} = JJ^n < J^{n+1}$, בסתירה להנחה. מכאן ש־$J^n = 0$. □

השערת ג'ייקובסון, שאם R נתרי ימני ושמאלי אז $\bigcap J(R)^n = 0$, עודנה פתוחה.

8.6.1 המשפט העיקרי של ודרברן

8.6.2 חוגים פרימיטיביים למחצה

הגדרה 8.6.10 *חוג R הוא **פרימיטיבי למחצה** אם* $\mathrm{Jac}(R) = 0$.

הערה 8.6.11 חוג R הוא פרימיטיבי למחצה אם ורק אם הוא מכפלה תת־ישרה של המנות הפרימיטיביות שלו (השווה להערה 8.4.2: חוג הוא ראשוני למחצה אם ורק אם הוא מכפלה תת־ישרה של המנות הראשוניות שלו).

טענה 8.6.12
1. כל חוג פרימיטיבי הוא פרימיטיבי למחצה.
2. כל חוג פשוט למחצה (אפילו במובן החלש של הערה 8.4.13) הוא פרימיטיבי למחצה.
3. כל חוג פרימיטיבי למחצה הוא ראשוני למחצה.

הוכחה.
1. **אידיאל האפס משתתף בחיתוך היוצר את** $\mathrm{Jac}(R)$.
2. **לפי ההנחה חיתוך האידיאלים המקסימליים הוא אפס, וכל אידיאל פרימיטיבי הוא מקסימלי.**
3. $\mathrm{rad}(R) \subseteq \mathrm{Jac}(R)$.

□

כעת נוכל להרחיב את הדיאגרמה שהצגנו קודם לכן:

$$\begin{tikzcd}
 & \text{פשוט ארטיני} = \mathrm{M}_n(D) \arrow[dl, Rightarrow] \arrow[d, Rightarrow] \arrow[dr, Rightarrow] & \\
\text{ראשוני עם שמאלי מינימלי} \arrow[dr, Rightarrow] & \text{פשוט} \arrow[d, Rightarrow] \arrow[dr, Rightarrow] & \text{פשוט למחצה ארטיני} = \prod_{i=1}^{t} \mathrm{M}_{n_i}(D_i) \arrow[d, Rightarrow] \\
 & \text{פרימיטיבי} \arrow[d, Rightarrow] \arrow[dr, Rightarrow] & \text{פשוט למחצה (במובן החלש)} \arrow[d, Rightarrow] \\
 & \text{ראשוני} \arrow[dr, Rightarrow] & \text{פרימיטיבי למחצה} \arrow[d, Rightarrow] \\
 & & \text{ראשוני למחצה}
\end{tikzcd}$$

תרגיל 8.6.13 יהי F שדה. הראה ש־$F[x]$ ראשוני ופרימיטיבי למחצה, אבל לא פרימיטיבי.

תרגיל 8.6.14 הצג בדיאגרמה את המחלקות המופיעות לעיל, במקרה הקומוטטיבי.

פרק 9

הצגות של חבורות

9.1 אלגברת החבורה

הגדרה 9.1.1 *תהי G חבורה, ויהי V מרחב וקטורי מעל שדה F.* ***הצגה*** *של G על V היא הומומורפיזם $G \to \operatorname{Aut}(V) = \operatorname{End}(V)^\times$. הממד של V נקרא* ***ממד ההצגה****. בחירת בסיס של V מאפשרת לזהות $\operatorname{Aut}(V) = \operatorname{GL}_n(F)$, ואז מתקבלת הצגה באמצעות מטריצות. הצגה* ***נאמנה*** *אם היא חד־חד־ערכית.*

כדי לחקור הצגות של חבורה נתונה, נפרש אותן כמודולים מעל חוג מתאים.

הגדרה 9.1.2 ***אלגברת החבורה*** *$F[G]$ היא המרחב הוקטורי ש־G הוא בסיס שלו מעל F, עם פעולת הכפל של החבורה, המומשכת על־ידי אסוציאטיביות. כלומר, $\sum_{g\in G} \alpha_g g \cdot \sum_{g'\in G} b_{g'} g' = \sum_{g''\in G} (\sum_{gg'=g''} \alpha_g b_{g'}) g''$.*

תרגיל 9.1.3 הסק ממשפט קיילי שלכל חבורה סופית יש הצגה נאמנה מממד סופי. (ההצגה המתקבלת, $\rho : G \to \operatorname{End}(F[G])$ לפי $\rho(g)(x) = gx$, נקראת **ההצגה הרגולרית** של G.)

תרגיל 9.1.4 הראה שאלגברת החבורה $F[\mathbb{Z}]$ היא חוג הפולינומים $F[t, t^{-1}]$.

הערה 9.1.5 כל הצגה $\rho : G \to \operatorname{GL}_n(F)$ אפשר להמשיך להומומורפיזם של אלגברות $\hat{\rho} : F[G] \to \operatorname{M}_n(F)$, לפי $\hat{\rho}(\sum \alpha_g g) = \sum \alpha_g \rho(g)$. גם להיפך, כל הומומורפיזם של אלגברות $F[G] \to \operatorname{M}_n(F)$ משרה הומומורפיזם של חבורות $G \to \operatorname{GL}_n(F)$ ($\hat{\rho}(g)\hat{\rho}(g^{-1}) = \hat{\rho}(1) = 1$, ולכן $\hat{\rho}(g)$ היא מטריצה הפיכה לכל $g \in G$).

טענה 9.1.6 יש התאמה בין הצגות של G על המרחב הוקטורי F^n, הומומורפיזמים של חוגים $F[G] \to \operatorname{End}(F^n)$, ומודולים מעל $F[G]$ בעלי ממד n כמרחבים וקטוריים מעל F (זוהי חזרה על טענה 7.3.3.)

הערה 9.1.7 מודול מעל $F[G]$ שהוא נוצר סופית מעל F, נוצר סופית גם מעל $F[G]$ (על־ידי אותו בסיס). לחבורה אינסופית יכולות להיות הצגות נוצרות סופית מממד אינסופי, אבל כאשר G סופית כל הצגה נוצרת סופית היא מממד סופי.

הגדרה 9.1.8 *נניח ש־$\rho : G \to \operatorname{GL}_n(F)$ הצגה, ו־$a \in \operatorname{GL}_n(F)$ איבר קבוע. אז $\gamma_a \circ \rho : G \to \operatorname{GL}_n(F)$ המוגדרת לפי $(\gamma_a \circ \rho)(g) = a\rho(g)a^{-1}$ היא* ***הצגה צמודה*** *ל־ρ. שתי הצגות ρ, ρ' נקראות* ***צמודות*** *אם $\rho' = \gamma_a \circ \rho$ לאיזשהו $a \in \operatorname{GL}_n(F)$ (זהו יחס שקילות).*

תרגיל 9.1.9 שתי הצגות הן שקולות אם ורק אם המודולים המתאימים להן איזומורפיים זה לזה.

תרגיל 9.1.10 לחבורה הדיהדרלית $\langle x, y \mid x^2 = y^2 = (xy)^4 = 1\rangle$ יש ההצגה $x \mapsto \begin{pmatrix} 0 & i \\ -i & 0 \end{pmatrix}$ ו־$y \mapsto \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. הראה שהצגה זו צמודה להצגה המוגדרת מעל $\mathbb{Q}$.

9.2 הצגות אי־פריקות ואי־פרידות

משתי הצגות אפשר לבנות בקלות הצגה חדשה:

הגדרה 9.2.1 *נניח ש־$\rho_1 : G \to \mathrm{Aut}(V_1)$ ו־$\rho_2 : G \to \mathrm{Aut}(V_2)$ הן שתי הצגות של חבורה G.* ***הסכום הישר*** *$\rho_1 \oplus \rho_2$ הוא ההצגה $g \mapsto \mathrm{Aut}(V_1 \oplus V_2)$, המוגדרת לפי $\rho(g)(v_1, v_2) = (\rho_1(g)v_1, \rho_2(g)v_2)$; בכתיב מטריצות, $g \mapsto \begin{pmatrix} \rho_1(g) & 0 \\ 0 & \rho_2(g) \end{pmatrix}$.*

הסכום הישר של ההצגות, $\rho_1 \oplus \rho_2$, מתאים לסכום הישר של המודולים $V_1 \oplus V_2$. מודול שאפשר לפרק לסכום ישר של תת־מודולים נקרא **מודול פריד** (decomposable). ההצגה המתאימה למודול כזה נקראת הצגה פרידה.

נתבונן כעת במקרה כללי יותר. נניח שמודול ההצגה V אינו פשוט, ויש לו תת־מודול $U \leq V$. במקרה זה V/U גם הוא מודול, ולכן ההצגה $\rho G \to \mathrm{Aut}(V)$ מגדירה הצגות $G \to \mathrm{Aut}(U)$ ו־$G \to \mathrm{Aut}(V/U)$. בחירת בסיס של U והשלמתו לבסיס של V מאפשרת לכתוב בכתיב מטריצות, $g \mapsto \begin{pmatrix} \rho_1(g) & * \\ 0 & \rho_2(g) \end{pmatrix}$. במקרה כזה ההצגה **פריקה** (reducible).

הגדרה 9.2.2 *הצגה נקראת* ***אי־פריקה*** *אם היא אינה פריקה (המודול המתאים הוא פשוט);* ***ואי־פרידה*** *אם היא אינה פרידה (המודול המתאים אינו ניתן להפרדה לסכום ישר של תת־מודולים).*

כל מודול פריד הוא פריק, כלומר, כל מודול אי־פריק הוא אי־פריד. ההיפך אינו בהכרח נכון: יתכן שמודול יהיה פריק אבל אי־פריד.

כל מודול של הצגה ממימד סופי הוא נוצר סופית, ולכן בעל אורך סופי וסדרת הרכב מתאימה. במלים אחרות, כל הצגה ניתן לפירוק עם מרכיבים אי־פריקים. הבעיה היא שממרכיבים אי־פריקים קשה לבנות את ההצגה בחזרה (משום שמתת־המודול ומודול המנה אי אפשר לשחזר את המודול עצמו): חסר המידע על המרכיב הנוסף שמעל לאלכסון, המסומן לעיל ב־$*$. למרבה המזל, לפעמים הבעיה הזו נפתרת מעצמה:

הערה 9.2.3 מעל חוג פשוט למחצה, כל מודול אי־פריד הוא אי־פריק (כך שהמושגים מתלכדים): אם $U \leq V$ אז יש משלים $V = U \oplus U'$, והמודול פריד.

בסעיף הבא נראה שבמקרים רבים הערה 9.2.3 חלה על אלגברת החבורה $F[G]$.

9.3 משפט משקה

9.3.1 אידיאל האוגמנטציה

הגדרה 9.3.1 ***ההצגה הטריוויאלית*** *של חבורה G היא ההומומורפיזם $g \mapsto 1 \in \mathrm{GL}_1(F) = F^{\times}$.*

הגדרה 9.3.2 ***אידיאל האוגמנטציה*** *של אלגברת חבורה $F[G]$ הוא הגרעין I_G של ההטלה $F[G]\to F$ שמשרה ההצגה הטריוויאלית.*

טענה 9.3.3 האיבר $\sum_g \alpha_g g \in F[G]$ שייך ל־I_G אם ורק אם $\sum \alpha_g = 0$.

תרגיל 9.3.4 $I_G = \sum_{g\in G} F(g-1)$ (ובפרט $\dim(I_G) = |G|-1$). אם $G = \langle g_1,\dots,g_t\rangle$ אז I_G נוצר, כאידיאל, על־ידי $g_1-1,\dots,g_t-1$.

תרגיל 9.3.5 תהי $N\triangleleft G$ תת־חבורה נורמלית; אז יש הטלה $\theta_N : F[G]\to F[G/N]$ המוגדרת לפי $g\mapsto gN$. הראה ש־$\mathrm{Ker}(\theta) = I_N$, כאשר $I_N\triangleleft F[G]$ הוא האידיאל הנוצר על־ידי האברים $n-1$, $n\in N$. **הדרכה**. התנאי לכך ש־$\theta(\sum \alpha_g g) = 0$ הוא שלכל $g'\in G$, $\sum_{x\in N}\alpha_{g'x}x = 0$. ◦

9.3.2 המקרה המודולרי

לפני שנציג את המשפט הבסיסי של תורת ההצגות, נתבונן במקרה המודולרי, שבו G היא חבורת־p ו־$\mathrm{char}F = p$.

טענה 9.3.6 אם G חבורת־p סופית ומאפיין השדה הוא p, אז אידיאל האוגמנטציה נילפוטנטי.

הוכחה. **אם $G=1$ אין מה להוכיח כי $I_G=0$. נניח ש־G אינה טריוויאלית, ויהי x איבר מסדר p במרכז של G; נסמן $Z=\langle x\rangle$. לפי תרגיל 9.3.5, $F[G]/\langle x-1\rangle \cong F[G/Z]$, כאשר $I_G/\langle x-1\rangle$ עובר אל $I_{G/Z}$. על־פי הנחת האינדוקציה יש n כך ש־$(I_G/\langle x-1\rangle)^n = I_{G/Z}^n = 0$, ואז $I_G^n \subseteq \langle x-1\rangle$. אבל $(x-1)^p = x^p-1 = 0$, ולכן $I_G^{np}\subseteq \langle x-1\rangle^p = 0$.** □

תרגיל 9.3.7 תהי G חבורת־p אבלית כלשהי (לאו דווקא סופית). הראה ש־I_G נילי. **הדרכה**. כל $x\in I_G$ אפשר לכתוב כסכום סופי $\sum \alpha_g(g-1)$, וקיים q כך ש־$g^q=1$ לכל g המשתתף בסכום. מכיוון ש־G אבלית אפשר להפעיל את אוטומורפיזם פרובניוס ולקבל $x^q = \sum \alpha_g^q(g-1)^q = \sum \alpha_g^q(g^q-1) = 0$.

9.3.3 משפט משקה

משפט 9.3.8 (*משפט משקה*) *תהי G חבורה סופית מסדר זר למאפיין של F, אז $F[G]$ פשוט למחצה.*

הוכחה. **לפי משפט 7.2.24, די להוכיח שלכל תת־מודול N של מודול M יש משלים. נבחר הטלה כלשהי $\pi : M\to N$ של מרחבים וקטוריים, ונגדיר $\pi'(x) = \frac{1}{|G|}\sum_{g\in G} g^{-1}\pi(gx)$. זהו הומומורפיזם של G־מודולים לפי חישוב; תמונתו היא N והוא שווה לזהות על N. לכן $M = N\oplus\ker(\pi')$.** □

הערה 9.3.9 הגרסה הבאה של משפט משקה נכונה גם כאשר G אינסופית: אם $\mathrm{char}F = 0$ אז ל־$F[G]$ אין אידיאלים ניליים.

מסקנה מכרעת אחת היא שעכשיו אפשר ליישם את טענה 7.2.28: בתנאי משפט משקה, כל מודול מעל $F[G]$ הוא פריק לחלוטין. הוכחנו מסקנה חשובה:

מסקנה 9.3.10 (במאפיין זר ל־$|G|$) כל הצגה של G מתפרקת באופן יחיד לסכום של הצגות אי־פריקות. ◦

לפי משפט 8.4.11, הוכחנו:

מסקנה 9.3.11 תהי G חבורה סופית, ו־F שדה ממאפיין זר ל־$|G|$. אז יש פירוק $F[G] \cong \mathrm{M}_{n_1}(D_1) \oplus \cdots \oplus \mathrm{M}_{n_t}(D_t)$, כאשר D_i הן אלגברות עם חילוק שהמרכז שלהן מכיל את F.

הגדרה 9.3.12 *אם $F[G]$ איזומורפי לסכום ישר של אלגברות מטריצות מעל F, אומרים ש־F **מפצל את** G (או ש־G **מתפצלת מעל** F).*

אם שדה F מפצל את G, אז כל שדה המכיל את F מפצל גם הוא. לפי הערה 8.1.3, $\mathbb{C}$ מפצל כל חבורה סופית. אחת התוצאות הראשונות בקומבינטוריקה אלגברית קובעת ש־S_n מתפצלת כבר מעל $\mathbb{Q}$, ולכן מעל כל שדה ממאפיין אפס.

גרסה חלשה, ללא מודולים משלימים

נוכיח גרסה חלשה למשפט משקה, ללא צורך במשפט 7.2.24 על מודולים פריקים לחלוטין.

הגדרה 9.3.13 *יהי R חוג. **אינוולוציה** של R היא פונקציה אדיטיבית $x \mapsto x^*$ המקיימת $x^{**} = x$ ו־$(xy)^* = y^*x^*$.*

תרגיל 9.3.14 אינוולוציה היא איזומורפיזם $R \to R^{\mathrm{op}}$.

תהי G חבורה כלשהי.
על אלגברת החבורה $\mathbb{C}[G]$ מוגדרת אינוולוציה לפי $(\sum \alpha_g g)^* = \sum \bar{\alpha_g} g^{-1}$.

למה 9.3.15 אם $a \in \mathbb{C}[G]$ מקיים $aa^* = 0$ אז $a = 0$.

הוכחה. נכתוב $a = \sum \alpha_g g$, ונחשב: $aa^* = \sum \alpha_g g \bar{\alpha_h} h^{-1} = \sum_x (\sum_h \alpha_{xh} \bar{\alpha_h}) x$, ולכן המקדם של 1 במכפלה aa^* שווה ל־$\sum |\alpha_h|^2$; אם זה שווה לאפס אז כל $\alpha_h = 0$ ולכן $a = 0$. $\square$

טענה 9.3.16 לכל חבורה G, $\mathbb{C}[G]$ ראשוני למחצה.

הוכחה. לפי טענה 8.4.6 מספיק להראות שאם $A \triangleleft \mathbb{C}[G]$ מקיים $A^2 = 0$, אז $A = 0$. יהי $a \in A$, אז $(aa^*)(aa^*)^* = (aa^*)^2 \in A^2 = 0$; לפי למה 9.3.15 $aa^* = 0$, ומאותה סיבה $a = 0$. $\square$

משפט 9.3.17 (גרסה חלשה של משפט משקה) *יהי $F \subseteq \mathbb{C}$ תת־שדה כלשהו, אז לכל חבורה G, $F[G]$ ראשוני למחצה.*

הוכחה. כמו בטענה 9.3.16, נניח ש־$A \triangleleft F[G]$ מקיים $A^2 = 0$, אז $\mathbb{C}A \triangleleft \mathbb{C}[G]$ ומקיים $(\mathbb{C}A)^2 = \mathbb{C}A^2 = 0$; לפי הטענה נובע מזה ש־$A \subseteq \mathbb{C}A = 0$. $\square$

מסקנה 9.3.18 יהי $F \subseteq \mathbb{C}$ תת־שדה כלשהו. לכל חבורה סופית G, $F[G]$ פשוט למחצה.

הוכחה. לפי משפט 8.4.11, משום ש־$F[G]$ ארטיני. $\square$

9.4 ההצגות האי־פריקות של חבורה סופית

9.4.1 מודולים מעל מכפלה ישרה

הלמה הבאה מתארת את תורת המודולים של חוג שהוא מכפלה ישרה של חוגים.

למה 9.4.1 יהי $R = R_1 \times \cdots \times R_t$ מכפלה של חוגים R_i. נכתוב $e_i = (0, \dots, 0, 1, 0, \dots, 0)$ ו־$R'_i = e_iR = Re_i$, כך ש־$e_1 + \cdots + e_t = 1$, $e_ie_j = \delta_{ij}e_i$ ו־$R'_i \cong R_i$.

1. יהי M מודול מעל R. אז $M_i = e_iM$ הם תת־מודולים, ו־$M = \oplus M_i$.
2. תת־קבוצה של M_j היא תת־מודול מעל R אם ורק אם היא תת־מודול מעל R'_j.
3. תת־מודול של M הוא פשוט אם ורק אם הוא תת־מודול פשוט של אחד ה־M_j.
4. $\operatorname{soc}(M) = \sum \operatorname{soc}(M_i)$.
5. כל הומומורפיזם $\varphi\colon M \to N$ של מודולים מעל R משרה הומומורפיזמים $\varphi_i\colon M_i \to N_i$ לפי $\varphi_i(e_ix) = e_i\varphi(x)$; φ חד־חד־ערכי אם ורק אם כל φ_i הוא חד־חד־ערכי, ועל אם ורק אם כל φ_i הוא על.
6. $M \cong N$ אם ורק אם $M_i \cong N_i$ לכל i.

הוכחה. **1.** ברור ש־$M = (\sum e_i)M \subseteq \sum(e_iM) \subseteq M$. כדי להראות שמדובר בסכום ישר, נניח ש־$\sum x_i = 0$ כאשר $x_i \in e_iM$; אז $e_jx_i = \delta_{ij}x_i$ ולכן לכל j, $0 = e_j\sum_i x_i = \sum e_jx_i = e_jx_j = x_j$.

2. אם $N \subseteq e_jM$ ו־$RN \subseteq N$ אז בוודאי גם $e_jN = e_jRN \subseteq e_jN$, ובכיוון ההפוך אם $e_jN \subseteq N$ אז $RN = \sum_i Re_iN = \sum_i Re_ie_jN = Re_jN = e_jN \subseteq N$.

3. אם $N \leq M$ פשוט אז $N = \sum e_iN$ ורק אחד המרכיבים שונה מאפס, לכן $N = e_jN$ לאיזשהו j, והוא פשוט כי כל תת־מודול הוא גם תת־מודול של N.

4. לפי סעיף 3.

5. φ_i הומומורפיזם כי $\varphi_i(xe_iv) = \varphi_i(e_ixv) = e_i\varphi(xv) = e_ix\varphi(v) = xe_i\varphi(v) = x\varphi_i(v)$. אם φ חד־חד־ערכי ו־$\varphi_i(e_iv) = 0$ אז $0 = \varphi_i(e_iv) = e_i\varphi(v) = \varphi(e_iv)$ ולכן $e_iv = 0$; הכיוון ההפוך מיידי. באותו אופן φ על אם ורק אם כל φ_i כזה.

6. לפי סעיף 5.

□

תרגיל 9.4.2 הוכח, ישירות, שהאידיאלים $F \times 0$ ו־$0 \times F$ של $F \times F$ אינם איזומורפיים כמודולים.

9.4.2 מספר ההצגות

תהי G חבורה סופית, ויהי F שדה המפצל את G. נכתוב $F[G] = \mathrm{M}_{n_1}(F) \times \cdots \times \mathrm{M}_{n_t}(F)$, ונסמן ב־$S_i = \mathrm{M}_{n_i}(F)$ את המרכיב ה־i.

הערה 9.4.3 מהשוואת מימדים מקבלים מיד $|G| = n_1^2 + \cdots + n_t^2$.

תרגיל 9.4.4 ל־$\mathrm{M}_n(F)$ יש מודול פשוט אחד עד כדי איזומורפיים, והוא המרחב הוקטורי F^n עם הפעולה הטבעית. חוג המטריצות, כמודול מעל עצמו, איזומורפי לסכום ישר של n עותקים של המודול הפשוט.

לפי למה 9.4.1, המודולים של $F[G]$ מתוארים על־ידי המודולים של המרכיבים S_i. נסמן ב־$V_i = F^{n_i}$ את המודול הפשוט של $S_i = \mathrm{M}_{n_i}(F)$; פעולת S_i על המודול היא לפי כפל מטריצה בווקטור. ההטלה $\rho_i : F[G] \to S_i$ שולחת כל איבר $g \in G$ למטריצה בגודל $n_i \times n_i$, והיא ההצגה המאתימה למודול V_i.

מסקנה 9.4.5 ל־$F[G]$ יש בדיוק t מודולים עד־כדי איזומורפיזם.

מסקנה 9.4.6 כל מודול מעל $F[G]$ אפשר לפרק לסכום ישר (לאו דווקא סופי) של מרכיבים שכל אחד מהם איזומורפי לאחד ה־V_i.

מודול נוצר סופית איזומורפי למודול מהצורה $V_1^{(n_1)} \oplus \cdots \oplus V_t^{(n_t)}$ כאשר n_i סופיים.

הערה 9.4.7 $F[G]$, כמודול מעל עצמו, איזומורפי לסכום ישר של n_i עותקים של V_i, $i = 1, \dots, t$. בפרט, כל מודול אי־פריק הוא תת־מודול של $F[G]$.

תרגיל 9.4.8 $\mathrm{Z}(F[G]) = F \times \cdots \times F$, t עותקים, ולכן מספר ההצגות האי־פריקות של G הוא המימד $[\mathrm{Z}(F[G]) : F]$. **הדרכה**. המרכז של מכפלה ישרה של חוגים שווה למכפלת המרכזים, והמרכז של אלגברת מטריצות מעל שדה שווה לשדה עצמו.

מאידך, את המרכז של $F[G]$ אפשר לחשב ישירות. לכל מחלקת צמידות $C \subseteq G$, נסמן $\hat{C} = \sum_{g \in C} g$.

טענה 9.4.9 המרכז של $F[G]$ נפרש, כמרחב וקטורי, על־ידי האברים $\hat{C}$.

הוכחה. **ראשית, $\sum \alpha_g g \in \mathrm{Z}(F[G])$ אם ורק אם $\alpha_g = \alpha_{g'}$ לכל g, g' צמודים בחבורה. אכן, איבר a הוא מרכזי באלגברת החבורה אם ורק אם הוא מתחלף עם כל $x \in G$, וזה קורה אם ורק אם $\sum \alpha_g g = a = xax^{-1} = \sum \alpha_g (xgx^{-1}) = \sum \alpha_{x^{-1}gx} g$ לכל x, אם ורק אם $\alpha_g = \alpha_{x^{-1}gx}$ לכל $x, g \in G$. לכן $\hat{C}$ הם מרכזיים, וכל איבר מרכזי הוא צירוף לינארי שלהם.** □

מסקנה 9.4.10 מכיוון שהאברים $\hat{C}$, על־פני מחלקות הצמידות השונות, הם בלתי תלויים מעל F, $[\mathrm{Z}(F[G]) : F]$ שווה למספר מחלקות הצמידות של G.

מסקנה 9.4.11 מספר המרכיבים t בפירוק של $F[G]$ לרכיבי מטריצות שווה למספר ההצגות האי־פריקות השונות של G, ושווה למספר מחלקות הצמידות של החבורה.

9.4.3 הצגות חד־ממדיות והשראה מחבורת מנה

מסקנה 9.4.11, יחד עם הערה 9.4.3, מאפשרות למצוא את ממדי ההצגות האי־פריקות של חבורות קטנות.

דוגמא 9.4.12 תהי G חבורה אבלית. אז יש לה $|G|$ מחלקות צמידות, ולכן גם $|G|$ הצגות אי־פריקות, שכולן חד־ממדיות. אכן, $F[G] = F \times \cdots \times F$ כי רכיבי מטריצות גדולים יותר אינם אבליים.

תרגיל 9.4.13 תהי G חבורה עם תת־חבורה נורמלית $N \lhd G$. כל הצגה של G/N משרה הצגה של G, על־ידי הרכבה עם פונקציית ההטלה. אומרים שהצגה כזו **מתפצלת** דרך G/N. הצגה אי־פריקה של G/N משרה הצגה אי־פריקה של G.

טענה 9.4.14 מספר ההצגות ממימד 1 של G שווה לסדר של האבליניזציה G/G'.

דוגמא 9.4.15 לחבורה הסימטרית S_3 יש שלוש מחלקות צמידות, ולכן ממדי ההצגות האי־פריקות הם $6 = 1^2 + 1^2 + 2^2$; כלומר, יש לחבורה שתי הצגות חד־ממדיות, ועוד הצגה דו־ממדית (וכל הצגה אי־פריקה היא סכום של אלו). את ההצגות החד־ממדיות קל לנחש: זו ההצגה הטריוויאלית $g \mapsto (1)$, **והצגת הסימן** $g \mapsto (\operatorname{sgn}(g))$. הוכח ש־$(12) \mapsto \begin{pmatrix} -1 & 1 \\ 0 & 1 \end{pmatrix}$, $(23) \mapsto \begin{pmatrix} 1 & 0 \\ 1 & -1 \end{pmatrix}$ מגדיר הצגה דו־ממדית אי־פריקה.

תרגיל 9.4.16 הראה שלחבורה הסימטרית S_4 יש חמש הצגות אי־פריקות: שתיים ממד 1, שתיים ממימד 3, ושתיים ממימד 2. **הדרכה**. העזר במנה $S_4/K \cong S_3$.

הערה 9.4.17 חבורת האוטומורפיזמים של G פועלת על ההצגות האי־פריקות: אם $\pi \in \operatorname{Aut}(G)$, אז לכל הצגה ρ גם $\rho \circ \pi$ היא הצגה. אבל אם π אוטומורפיזם פנימי אז ההצגות צמודות, ולכן חבורת האוטומורפיזמים החיצוניים $\operatorname{Out}(G) = \operatorname{Aut}(G)/Inn(G)$ פועלת על מחלקות האיזומורפיזם של ההצגות האי־פריקות.

9.5 קרקטרים

9.5.1 יחסי שור

יהי $F[G] \cong S_1 \times \cdots \times S_t$ הפירוק של אלגברת החבורה של חבורה סופית G מעל שדה המפצל אותו, F, למכפלה ישרה של מרכיבים פשוטים $S_i = \mathrm{M}_{n_i}(F)$. ההצגות האי־פריקות של G מושרות על־ידי ההטלות $\rho_i : F[G] \to \mathrm{M}_{n_i}(F)$, ומתאימות למודולים האי־פריקים $V_i = F^{(n_i)}$. כל V_i הוא מודול מעל $F[G]$ לפי $g \cdot v = \rho_i(g)v$. אפשר להניח שההצגה הראשונה היא ההצגה הטריוויאלית, $\rho_1(g) = 1$ לכל g.

למה 9.5.1 תהי $A \in \mathrm{M}_{n_v \times n_u}(F)$ מטריצה כלשהי. אז $\eta(A) = \sum_g \rho_v(g) A \rho_u(g^{-1})$ מגדיר הומומורפיזם של מודולים $\eta(A) : V_u \to V_v$.

הוכחה. נבחין ש־$\rho_v(g) \in \mathrm{M}_{n_v}(F)$ ו־$\rho_u(g) \in \mathrm{M}_{n_u}(F)$, כך ש־$\eta(A) \in \mathrm{M}_{n_v \times n_u}(F)$. לכל $h \in G$ ולכל $x \in V_u$ מתקיים

$$\begin{aligned}
\eta(A)(h \cdot x) &= \eta(A)\rho_u(h)x = \sum_g \rho_v(g)A\rho_u(g^{-1}h)x \\
&= \sum_g \rho_v(hg)A\rho_u(g^{-1})x = \rho_v(h)\eta(A)x = h \cdot \eta(A)x.
\end{aligned}$$

□

מסקנה 9.5.2 לכל מטריצה A, אם $u \neq v$ אז $\eta(A) = 0$, ואם $u = v$ אז $\eta(A)$ סקלרית.

הוכחה. כאשר $u \neq v$, $\eta(A) : V_u \to V_v$ הוא הומומורפיזם של מודולים פשוטים שאינם איזומורפיים. כאשר $u = v$, $\eta(A) : V_u \to V_u$ הומומורפיזם, כלומר לכל $s \in \mathrm{M}_{n_u}(F)$ ולכל $x \in V_u$ מתקיים $\eta(A)(sx) = s\eta(A)x$, כלומר $\eta(A)s = s\eta(A)$ ו־$\eta(A) \in \mathrm{Z}(\mathrm{M}_{n_u}(F))$. □

כדי שלא לסרבל את הסימון עבור רכיבים של מטריצות ההצגה, נסמן $\rho^{(u)}$ במקום ρ_u.

משפט 9.5.3 (שור) לכל $u, v = 1, \dots, t$ ולכל $1 \leq i, j \leq n_u$ ו־$1 \leq k, \ell \leq n_v$ מתקיים

$$\sum_{g \in G} \rho_{ij}^{(u)}(g)\rho_{k\ell}^{(v)}(g^{-1}) = \delta_{uv}\delta_{jk}\delta_{i\ell}\frac{|G|}{n_u}.$$

הוכחה. נתבונן במטריצה $A = e_{jk} \in \mathrm{M}_{n_u \times n_v}(F)$, ונחשב:

$$\begin{aligned}
\eta(A) &= \eta(e_{jk}) = \sum_g \rho^{(u)}(g)e_{jk}\rho^{(v)}(g^{-1}) \\
&= \sum_g \sum_{i,j',k',\ell} \rho_{ij'}^{(u)}(g)e_{ij'}e_{jk}e_{k'\ell}\rho_{k'\ell}^{(v)}(g^{-1}) \\
&= \sum_{i,\ell} \left(\sum_g \rho_{ij}^{(u)}(g)\rho_{k\ell}^{(v)}(g^{-1}) \right) e_{i\ell},
\end{aligned}$$

כלומר $\eta(A)_{i\ell} = \sum_g \rho_{ij}^{(u)}(g)\rho_{k\ell}^{(v)}(g^{-1})$. כאשר $u \neq v$, $\eta(A) = 0$ לפי מסקנה 9.5.2, ואז מתקבלת הזהות המבוקשת מהשוואת מקדמים. כאשר $u = v$, לפי המסקנה יש קבוע $\gamma \in F$ כך ש־$\eta(A)_{i\ell} = \delta_{i\ell}\gamma$, וסיימנו כמקודם אם $i \neq \ell$. נשאר המקרה $i = \ell$. נסכם את אברי האלכסון של $\eta(A)$:

$$\begin{aligned}
n_u\gamma &= \mathrm{tr}(\eta(A)) = \sum_i \eta(A)_{ii} \\
&= \sum_i \sum_g \rho_{ij}^{(u)}(g)\rho_{ki}^{(u)}(g^{-1}) \\
&= \sum_g \sum_i \rho_{ki}^{(u)}(g^{-1})\rho_{ij}^{(u)}(g) \\
&= \sum_g \left(\rho^{(u)}(g^{-1})\rho^{(u)}(g)\right)_{kj} = \sum_g \delta_{kj} = \delta_{kj}|G|,
\end{aligned}$$

כלומר $\eta(A)_{ii} = \delta_{kj}\frac{|G|}{n_u}$, כדרוש. □

9.5.2 קרקטרים

תהי $\rho\colon G\to\mathrm{GL}_n(F)$ הצגה. נסמן $\chi(g)=\mathrm{tr}(\rho(g))$; זוהי פונקציה $\chi\colon G\to\mathbb{C}$ הנקראת **הקרקטר של ההצגה** (character of the representation). למרות שהיא אינה כפלית (אין קשר פשוט בין העקבה של AB לעקבות של A,B), הקרקטר נושא אינפורמציה חשובה על ההצגה, וכפי שנראה בהמשך, אפשר לפתח את תורת ההצגות במידה רבה דרך הקרקטרים, בלי להתייחס להצגות באופן ישיר.

תפקידם המרכזי של הקרקטרים נעוץ בהבחנה הבאה:

הערה 9.5.4 אם ρ,ρ' הצגות שקולות, אז יש להן אותו קרקטר (משום שהעקבה אינה משתנה בהצמדה).

הערה 9.5.5 $\chi_{\rho\oplus\rho'}=\chi_\rho+\chi_{\rho'}$ (משום שעקבה של מטריצת בלוקים היא סכום העקבות של הבלוקים). ◦

אומרים שקרקטר הוא **אי־פריק** אם הוא מתאים להצגה אי־פריקה. ממד ההצגה נקרא גם הממד של הקרקטר.

טענה 9.5.6 יש t קרקטרים אי־פריקים, וכל קרקטר הוא צירוף לינארי שלהם, עם מקדמים טבעיים.

הוכחה. **הקרקטרים האי־פריקים הם אלו המתאימים להצגות האי־פריקות. כל הצגה ρ אפשר לפרק לסכום ישר של הצגות אי־פריקות לפי מסקנה 9.3.10, ואז χ_ρ הוא סכום הקרקטרים המתאימים.** □

9.5.3 אורתוגונליות הקרקטרים

מיחסי שור אפשר להסיק יחסים שימושיים ביותר, המנוסחים בשפה של הקרקטרים. נזכיר ש־$\chi_u(g)=\sum_i\rho_{ii}^{(u)}(g)$. אם ניקח $j=i$ ו־$\ell=k$ ביחסי שור (משפט 9.5.3), נקבל

$$\sum_{g\in G}\rho_{ii}^{(u)}(g)\rho_{kk}^{(v)}(g^{-1})=\delta_{uv}\delta_{ik}\frac{|G|}{n_u},$$

ואם נסכם לכל i ולכל k נקבל

$$\begin{aligned}\sum_{g\in G}\chi_u(g)\chi_v(g^{-1}) &= \sum_{g\in G}\left(\sum_i\rho_{ii}^{(u)}(g)\right)\left(\sum_k\rho_{kk}^{(v)}(g^{-1})\right)\\ &= \sum_i\delta_{uv}\frac{|G|}{n_u}=\delta_{uv}|G|.\end{aligned}$$

מסקנה 9.5.7 לכל שני קרקטרים אי־פריקים χ_u,χ_v, מתקיים **יחס שור הראשון**

$$\frac{1}{|G|}\sum_{g\in G}\chi_u(g)\chi_v(g^{-1})=\delta_{uv}. \tag{9.1}$$

9.5.4 הערכים של קרקטר

הערה 9.5.8 יהי χ קרקטר המתאים להצגה ρ. לכל $g \in G$, $\rho(g)^N = \rho(g^N) = 1$ כאשר $N = |G|$, ולכן הערכים העצמיים של $\rho(g)$ הם שורשי יחידה. הערך $\chi(g)$ הוא סכום הערכים העצמיים של $\rho(g)$, ולכן הוא שלם אלגברי, השייך לחוג $\mathbb{Z}[\omega_N]$, כאשר ω_N הוא שורש יחידה פרימיטיבי מסדר N.

תרגיל 9.5.9 כל מטריצה $A \in \mathrm{M}_n(\mathbb{C})$ המקיימת שוויון מהצורה $A^N = 1$ היא לכסינה.
הדרכה. התבונן בצורת ז'ורדן של A.

הערה 9.5.10 לכל קרקטר ממימד n, $|\chi(g)| \leq n$, עם שוויון אם ורק אם $\rho(g)$ סקלרית.

הוכחה. הטענה הראשונה נובעת מכך ש־$\chi(g)$ הוא סכום של n שורשי יחידה; אם יש שוויון אז כל המחוברים האלה שווים לשורש יחידה ω, וזהו הערך העצמי היחיד של $\rho(g)$. לפי תרגיל 9.5.9, $\rho(g) = \omega I$. □

9.5.5 הקרקטר הצמוד

יהי χ קרקטר המתאים להצגה ρ.

טענה 9.5.11 לכל $g \in G$, $\chi(g^{-1}) = \overline{\chi(g)}$.

הוכחה. $\chi_\rho(g)$ הוא סכום הערכים העצמיים של $\rho(g)$, שהם הפוכים לערכים העצמיים של $\rho(g^{-1}) = \rho(g)^{-1}$; אלא ששורשי יחידה מקיימים $\bar{\omega} = \omega^{-1}$, ולכן $\mathrm{tr}(\rho(g^{-1})) = \overline{\mathrm{tr}(\rho(g))}$. □

הגדרה 9.5.12 *תהי* $\rho\colon G \to \mathrm{GL}_n(F)$ *הצגה. ההצגה הצמודה היא ההצגה מאותו ממד המוגדרת לפי* $\rho^*(g) = \rho(g^{-1})^{\mathrm{t}}$. *את העקבה שלה מסמנים* $\bar{\chi}(g) = \mathrm{tr}(\rho^*(g))$.

טענה 9.5.13 לכל $g \in G$, $\bar{\chi}(g) = \overline{\chi(g)}$.

הוכחה. $\bar{\chi}(g) = \mathrm{tr}(\rho^*(g)) = \mathrm{tr}(\rho(g^{-1})) = \chi(g^{-1}) = \overline{\chi(g)}$. □

שוויון זה מאפשר לנסח מחדש את יחס שור הראשון:

$$\frac{1}{|G|}\sum_{g\in G}\chi_u(g)\overline{\chi_v(g)} = \delta_{uv}. \tag{9.2}$$

הערה 9.5.14 ההצמדה פועלת על קבוצת ההצגות האי־פריקות, בדומה לפעולה של $\mathrm{Out}(G)$ מהערה 9.5.14.

9.5.6 המכפלה הפנימית

כעת מתבקש להגדיר מכפלה פנימית על $F[G]$, לפי $\langle g, h\rangle = \frac{1}{|G|}\delta_{gh}$, כלומר

$$\left\langle \sum_g a_g g, \sum_h b_h h\right\rangle = \frac{1}{|G|}\sum_g a_g\overline{b_g}.$$

עד כדי כפל בסקלר, זוהי המכפלה הפנימית הסטנדרטית של המרחב הוקטורי $F[G] \cong \{f\colon G \to F\} \cong F^{|G|}$ המוכל ב־$\mathbb{C}^{|G|}$. נזכיר שהמכפלה הפנימית היא תבנית סמי־ליניארית, כלומר, $\langle b, a\rangle = \overline{\langle a, b\rangle}$ ולכל $\alpha \in F$ מתקיים $\langle \alpha a, b\rangle = \alpha\langle a, b\rangle$ ו־$\langle a, \alpha b\rangle = \bar{\alpha}\langle a, b\rangle$.

9.5.7 בסיס הקרקטרים

לכל קרקטר אי־פריק χ, נסמן $\hat{\chi} = \sum_{g\in G} \chi(g)g$.
מיחס שור הראשון מתקבל השוויון

$$\left\langle \hat{\chi}, \hat{\chi}' \right\rangle = \sum_g \sum_h \chi(g)\overline{\chi'(h)}\langle g, h\rangle = \frac{1}{|G|}\sum_g \chi(g)\overline{\chi'(g)} = \delta_{\chi,\chi'}.$$

מסקנה 9.5.15 האברים $\hat{\chi} = \sum_g \chi(g)g$, עבור הקרקטרים האי־פריקים, מהווים קבוצה אורתונורמלית. °

בפרט,

מסקנה 9.5.16 האברים $\hat{\chi}$ השייכים להצגות אי־פריקות שונות הם שונים זה מזה.

כלומר, כפי שההצגה מגדירה את הקרקטר, הקרקטר (בינתיים, האי־פריק) קובע את ההצגה.

תרגיל 9.5.17 לכל קרקטר χ, האיבר $\hat{\chi}$ שייך למרכז של אלגברת החבורה. **הדרכה.** טענה 9.4.9: אם g, g' אברים צמודים, אז $\rho(g), \rho(g')$ הן מטריצות צמודות, ולכן יש להן אותה עקבה.

כלומר, אלו t וקטורים אורתוגונליים במרחב מממד t.

מסקנה 9.5.18 האברים $\hat{\chi}$ מהווים בסיס למרכז של אלגברת החבורה.

ביתר פירוט, לכל איבר מרכזי $f \in \mathrm{Z}(F[G])$ יש הצגה יחידה בצורה $f = \sum_\chi t_\chi \hat{\chi}$, כאשר הסכום הוא על הקרקטרים האי־פריקים, ולכל χ' מתקיים

$$\left\langle f, \hat{\chi}' \right\rangle = \left\langle \sum_\chi t_\chi \hat{\chi}, \hat{\chi}' \right\rangle = \sum t_\chi \left\langle \hat{\chi}, \hat{\chi}' \right\rangle = t_{\chi'},$$

כלומר, לכל $f \in \mathrm{Z}(F[G])$,

$$f = \sum_\chi \langle f, \hat{\chi}\rangle \hat{\chi}. \tag{9.3}$$

9.5.8 פונקציות המחלקה

כל פונקציה $f : G \to F$ אפשר לראות כאיבר $\sum_g f(g)g$ באלגברת החבורה, ולהיפך. למשל, הקרקטר χ, כפונקציה $G \to F$, מתאים לאיבר $\hat{\chi}$ של אלגברת החבורה. פונקציה $f : G \to F$ המקבלת אותו ערך בכל האברים של אותה מחלקת צמידות נקראת **פונקציית מחלקה**. כעת אפשר לפרש את מסקנה 9.5.18:

מסקנה 9.5.19 הקרקטרים האי־פריקים מהווים בסיס למרחב של פונקציות המחלקה.

לאור הפירוש של איברי המרכז כפונקציות מחלקה, נוסחת המקדמים (9.3) מספקת מסקנה מבנית חשובה. תהי ρ הצגה כלשהי. כפי שראינו כבר, אפשר לפרק $\rho = \sum m_u \rho_u$, סכום ישר של הצגות אי־פריקות, עם מקדמים $m_u \in \mathbb{N}$. לפי הערה 9.5.5 הקרקטרים מתפרקים באותו אופן: $\chi_\rho = \sum m_u \chi_u$. לפי החישוב לעיל, הקרקטר χ קובע את מקדמי הפירוק של ρ, $m_u = \langle \chi_\rho, \chi \rangle$.

מסקנה 9.5.20 הקרקטר קובע את ההצגה: אם לשתי הצגות יש אותם קרקטרים, אז הן איזומורפיות.

ועוד מסקנה שימושית: $\langle\chi_\rho,\chi_\rho\rangle = \sum m_u^2$, ובפרט:

מסקנה 9.5.21 הצגה ρ היא אי־פריקה אם ורק אם הקרקטר שלה הוא בעל נורמה 1.

9.5.9 האידמפוטנטים האורתוגונליים

כדי להעמיק את תפקידם של אברי המרכז $\hat{\chi} = \sum \chi(g)g$, נכליל את החישוב שבתת־סעיף 9.5.3. ניקח ביחסי שור $j = i$, ונכפיל את היחס בסקלר $\rho^{(v)}_{\ell k}(h)$, כאשר $h \in G$ קבוע:

$$\sum_{g\in G} \rho^{(u)}_{ii}(g)\rho^{(v)}_{k\ell}(g^{-1})\rho^{(v)}_{\ell k}(h) = \delta_{uv}\delta_{ik}\delta_{i\ell}\frac{|G|}{n_u}\rho^{(v)}_{\ell k}(h).$$

סיכום על כל הערכים של i,k,ℓ נותן

$$\begin{aligned}
\sum_{g\in G}\chi_u(g)\chi_v(g^{-1}h) &= \sum_{g\in G}\chi_u(g)\sum_k \rho^{(v)}_{kk}(g^{-1}h) \\
&= \sum_{g\in G}\chi_u(g)\sum_k (\rho^{(v)}(g^{-1})\rho^{(v)}(h))_{kk} \\
&= \sum_{g\in G}\left(\sum_i \rho^{(u)}_{ii}(g)\right)\left(\sum_k\left(\sum_\ell \rho^{(v)}_{k\ell}(g^{-1})\rho^{(v)}_{\ell k}(h)\right)\right) \\
&= \delta_{uv}\frac{|G|}{n_v}\sum_i\sum_k\sum_\ell \delta_{ik}\delta_{i\ell}\rho^{(v)}_{\ell k}(h) \\
&= \delta_{uv}\frac{|G|}{n_v}\sum_i \rho^{(v)}_{ii}(h) = \delta_{uv}\frac{|G|}{n_v}\chi_v(h).
\end{aligned}$$

לכל קרקטר אי־פריק χ, נסמן $e_\chi = \frac{\chi(1)}{|G|}\hat{\chi}$.

טענה 9.5.22 האברים e_χ הם אידמפוטנטים (מרכזיים).

הוכחה.

$$\begin{aligned}
e_{\chi_u}e_{\chi_v} &= \frac{n_u n_v}{|G|^2}\sum_{h\in G}\left(\sum_g \chi_u(g)\chi_v(g^{-1}h)\right)h \\
&= \delta_{uv}\frac{n_v}{|G|}\sum_{h\in G}\chi_v(h)h \\
&= \delta_{uv}e_{\chi_v}
\end{aligned}$$

□

אבל באלגברה $\prod_{i=1}^t \mathrm{M}_{n_i}(F)$ יש רק מערכת אחת של אידמפוטנטים מרכזיים אורתוגונליים, הלוא היא המערכת של המטריצות הסקלריות ברכיבים השונים. מכאן שהאיזומורפיזם $F[G]{\rightarrow}\prod_{u=1}^t \mathrm{M}_{n_u}(F)$ שולח את האידמפוטנטים e_χ למטריצות היחידה ברכיבים השונים. למעשה, כפל ב־e_{χ_u} משרה אפימורפיזם $F[G]{\rightarrow}F[G]e_{\chi_u}\cong \mathrm{M}_{n_u}(F)$.

כדי לחשב את ההצגה במרכיב המתאים ל־e_{χ_u}, בחר איבר גנרי $a\in F[G]$; בהסתברות 1, המטריצה $e_{\chi_u}a$ בעלת n_u ערכים עצמיים שונים $\lambda_1,\dots,\lambda_{n_u}$, ועל־ידי הצבה בפולינומי האינטרפולציה $\prod(\lambda-\lambda_i)/(\lambda_j-\lambda_i)$, מקבלים אידמפטונטים e_{ii} השייכים למרכיב $F[G]e_{\chi_u}$. פתור את המשוואות $e_{ii}x=xe_{jj}=x$ כדי למצוא את יחידות המטריצות עד כדי סקלרים. קבע את x_{1i}; מכאן קבל את x_{i1} ככפולות של e_{i1} כך ש־$x_{1i}x_{i1}=e_{11}$; ואז קבע $x_{ij}=x_{i1}x_{1j}$; יחד, זו מערכת של יחידות מטריצות, וההצגה ρ מתקבלת במפורש כך: לכל $g\in G$, הבע את ge_χ כצירוף לינארי של ה־x_{ij}; המקדמים מרכיבים את המטריצה $\rho(g)$.

9.5.10 טבלת הקרקטרים

לפי תרגיל 9.5.17, לכן אפשר לקודד את כל הערכים של הקרקטרים על אברי החבורה באמצעות הערכים שלהם על נציגים ממחלקות הצמידות.

הגדרה 9.5.23 *המטריצה $X_{ij}=\chi_i(g_j)$, כאשר $g_j\in C_j$ איברים כלשהם (הערכים אינם תלויים בבחירת הנציגים) נקראת מטריצת הקרקטרים של G. זוהי מטריצה ריבועית: $X\in \mathrm{M}_t(\mathbb{C})$.*

נוסף לסימונים בראש תת־סעיף 9.5.1, נסמן ב־$h_i=|C_i|$ את הגדלים של מחלקות הצמידות. אפשר להניח שהמחלקות של אברים במרכז מופיעות ראשונות, כשהמחלקה של איבר היחידה בראש. בפרט $h_1=1$, ו־$X_{i1}=\chi_i(1)=\mathrm{tr}(\rho_i(1))=n_i$. נסמן גם $H=\mathrm{diag}(h_1,h_2,\dots,h_t)$. נפרש את היחס (9.1) בשפה החדשה:

$$\sum_i h_i\chi_u(g_i)\overline{\chi_v(g_i)}=\sum_i\sum_{g\in C_i}\chi_u(g_i)\overline{\chi_v(g_i)}=\sum_{g\in G}\chi_u(g)\overline{\chi_v(g)}=\delta_{uv}|G|, \tag{9.4}$$

ולכן

$$(XH\overline{X^{\mathrm{t}}})_{uv}=\sum_{j=1}^t h_jX_{uj}\overline{X_{vj}}=\delta_{uv}|G|.$$

כלומר, $XH\overline{X^{\mathrm{t}}}=|G|\cdot I$, כאשר I היא מטריצת היחידה.

תרגיל 9.5.24 הראה ש־$|\det(X)|^2=|G|^t\prod_j h_j^{-1}$. בפרט, X הפיכה.

תרגיל 9.5.25 תהי X טבלת הקרקטרים של חבורה אבלית G. הראה ש־$|\det(X)|=|G|^{|G|/2}$.

תרגיל 9.5.26 תהי $A\in \mathrm{M}_n(\mathbb{C})$ המטריצה הסיבובית המוגדרת לפי $A_{ij}=\rho^{ij}$ כאשר ρ שורש יחידה מסדר n. חשב את $\det(A)$.

טענה 9.5.27 (יחס שור השני) לכל i,j, $\sum_u\chi_u(g_i)\overline{\chi_u(g_j)}=\delta_{ij}\frac{|G|}{h_i}$.

הוכחה. הוכחנו ש־$XH\overline{X^{\mathrm{t}}}=|G|\cdot I$. נצמיד ב־$X$ ונקבל $\overline{X^{\mathrm{t}}}X=|G|\cdot H^{-1}$. מהשוואת רכיבים מתקבל $\sum_u\overline{\chi_u(g_i)}\chi_u(g_j)=\sum_u\overline{X^{\mathrm{t}}}_{iu}X_{uj}=(\overline{X^{\mathrm{t}}}X)_{ij}=|G|(H^{-1})_{ij}=\delta_{ij}\frac{|G|}{h_i}$. □

כלומר, כאשר מתבוננים בשתי עמודות $u\neq v$ של טבלת הקרקטרים, הן אורתוגונליות כווקטורים במרחב $\mathbb{C}^t$; ואילו הנורמה־בריבוע של העמודה ה־u שווה ל־$\frac{|G|}{h_u}$.

9.5.11 דוגמאות

נציג את טבלאות הקרקטרים של כמה חבורות. לצד כל שורה נכתוב את שם הקרקטר, ומעל לעמודה נכתוב את שם מחלקת השקילות ומספר האברים במחלקה (לפעמים שימושי גם לדעת מיהם האברים במחלקה, ומה הסדר שלהם).

דוגמא 9.5.28 $G = \mathbb{Z}/3\mathbb{Z} = \{0,1,2\}$. זוהי חבורה אבלית, ולכן כל ההצגות חד־ממדיות:

	$\{0\}$	$\{1\}$	$\{2\}$
χ_1	1	1	1
χ_2	1	ω	ω^{-1}
χ_3	1	ω^{-1}	ω

דוגמא 9.5.29 $G = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} = \langle x,y \mid x^2 = y^2 = [x,y] = 1\rangle$. גם כאן כל ההצגות חד־ממדיות:

	1	x	y	xy
χ_0	1	1	1	1
χ_1	1	1	-1	-1
χ_2	1	-1	1	-1
χ_3	1	-1	-1	1

דוגמא 9.5.30 $G = S_3$. יש שלוש מחלקות צמידות ולכן שלוש הצגות, שמצאנו בתרגיל 9.4.15. נראה כיצד למצוא את הטבלה ישירות. את ההצגות הלינאריות קל לחשב, והן מותירות הצגה דו־ממדית אחת, עם ערכים a,b שאותם נמצא בעזרת חוקי האורתוגונליות:

	1	$(\cdot\cdot)$	$(\cdot\cdot\cdot)$
χ_1	1	1	1
sgn	1	-1	1
χ	2	a	b

מחישוב המכפלות הפנימיות מקבלים $0 = \langle \chi_1, \chi\rangle = 2+3a+2b$ ו־$0 = \langle \mathrm{sgn}, \chi\rangle = 2-3a+2b$, ולכן $a = 0$ ו־$b = -1$.

דוגמא 9.5.31 $G = D_4$: חמש מחלקות צמידות, עם $G/G' \cong \mathbb{Z}_2 \times \mathbb{Z}_2$. הרמת ההצגות מספקת את ארבע השורות הראשונות, והאורתוגונליות את השורה החמישית. הראה שהאוטומורפיזם החיצוני $\sigma \mapsto \sigma$, $\tau \mapsto \sigma\tau$ מחליף (בפעולה של הערה 9.5.14) את χ_3, χ_4, ומשאיר את שאר ההצגות במקומן.

	1	1	2	2	2
	1	σ^2	τ	$\sigma\tau$	σ
χ_1	1	1	1	1	1
χ_2	1	1	-1	-1	1
χ_3	1	1	1	-1	-1
χ_4	1	1	-1	1	-1
χ	2	-2	0	0	0

דוגמא 9.5.32 $G = S_4$. לחבורה הזו יש חמש מחלקות צמידות, וחבורת הקומוטטורים שווה ל־A_4, כך שיש לה שתי הצגות לינאריות. למעשה, מכיוון ש־$S_4/K_4 \cong S_3$ (כאשר $K_4 = \langle (12)(34), (13)(24) \rangle$, לפי הפעולה על חלוקות של $\{1,2,3,4\}$ לזוגות), אפשר להרים את ההצגות של S_3, וזה משאיר עוד שתי הצגות. אם נסמן את הממדים ב־n_4, n_5, נקבל $1^2+1^2+2^2+n_4^2+n_5^2 = 24$, ולכן $n_4 = n_5 = 3$. כך מגיעים לטבלה הבאה:

	1	6	8	6	3
	1	$(\cdot\cdot)$	$(\cdot\cdot\cdot)$	$(\cdot\cdot\cdot\cdot)$	$(\cdot\cdot)(\cdot\cdot)$
χ_1	1	1	1	1	1
sgn	1	-1	1	-1	1
χ	2	0	-1	0	-1
χ_3	3	a	b	c	d
$\chi_{3'}$	3	a'	b'	c'	d'

מחישוב המכפלות הפנימיות מקבלים $3+6a+8b+6c+3d = \langle \chi_1, \chi_3 \rangle = 0$ ו־$0 = \langle \mathrm{sgn}, \chi_3 \rangle = 3-6a+8b-6c+3d$, כך ש־$a+c=0$ ו־$3+8b+3d=0$. לזה אפשר להוסיף את העובדה שכל אחד מן הערכים a,b,c,d הוא סכום של שלושה שורשי יחידה מהסדר המתאים למחלקה (2, 3, 4, ו־2 בהתאמה). לכן $d, c = -a \in \{\pm 1, \pm 3\}$, ולפי המשוואות גם $b = -\frac{3}{8}(1+d) \in \mathbb{Q}$, וכסכום של שורשי יחידה מסדר שלוש נובע ש־$b \in \{3, 0\}$. אבל $b=3$ בלתי אפשרי, ולכן $b=0$ ו־$d=-1$. הנימוקים האלו חלים על השורה $\chi_{3'}$. יחס שור השני על המחלקות $1, (\cdot\cdot)$ נותן את המשוואה $3a+3a'+0+1-1 = 0$, כך ש־$a' = -a$. אותו יחס על המחלקה $(\cdot\cdot)$ מול עצמה נותן $\frac{24}{6} = 1+1+a^2+a^2$, כך ש־$a^2 = 1$. לכן הטבלה היא

	1	6	8	6	3
	1	$(\cdot\cdot)$	$(\cdot\cdot\cdot)$	$(\cdot\cdot\cdot\cdot)$	$(\cdot\cdot)(\cdot\cdot)$
χ_1	1	1	1	1	1
sgn	1	-1	1	-1	1
χ	2	0	-1	0	-1
χ_3	3	1	0	-1	-1
$\chi_{3'}$	3	-1	0	1	-1

9.5.12 אלגברת מחלקות הצמידות

לכל מחלקת צמידות $C \subseteq G$ סימנו $\hat{C} = \sum_{g \in C} g$, וראינו שאברים אלו מהווים בסיס למרכז של אלגברת החבורה. מכיוון ש־$\hat{C}_i$ במרכז של אלגברת החבורה, הפעלת ההצגה ה־u נותנת מטריצה סקלרית, שהעקבה שלה $\chi_u(\hat{C}_i) = h_i \chi_u(g_i)$. לכן $\rho^{(u)}(\hat{C}_i) = \frac{h_i}{n_u}\chi_u(g_i)$.

לכל שלוש מחלקות C_i, C_j, C_k, ולכל $x_k \in C_k$, נסמן ב־$m_{ij}^k \in \mathbb{Z}$ את מספר הפתרונות למשוואה $x_i x_j = x_k$, עם $x_i \in C_i$, $x_j \in C_j$. על־ידי הצמדה רואים שהמספר אינו תלוי בבחירת $x_k \in C_k$. השוואת מקדמים מראה ש־

$$\hat{C}_i \hat{C}_j = \sum_k m_{ij}^k \hat{C}_k.$$

נפעיל את ההצגה ה־u, ונקבל

$$\frac{h_i}{n_u}\chi_u(g_i)\frac{h_j}{n_u}\chi_u(g_j) = \sum_k m_{ij}^k \frac{h_k}{n_u}\chi_u(g_k),$$

כלומר, המודול $\mathbb{Z}\frac{h_1}{n_u}\chi_u(g_1)+\cdots+\mathbb{Z}\frac{h_t}{n_u}\chi_u(g_t)$, שהוא נוצר סופית, סגור לכפל. לכן כל איבר שלו הוא שלם אלגברי:

טענה 9.5.33 לכל u,i, $\frac{h_i}{n_u}\chi_u(g_i)$ הוא שלם אלגברי.

משפט 9.5.34 *הממד של הצגה אי־פריקה מחלק את סדר החבורה.*

הוכחה. לפי (9.4),

$$\frac{|G|}{n_u}=\sum_i \frac{h_i\chi_u(g_i)}{n_u}\overline{\chi_u(g_i)},$$

וזהו סכום של מכפלות של שלמים אלגבריים. לכן המספר הרציונלי $\frac{|G|}{n_u}$ הוא שלם אלגברי, ולכן שלם. □

9.5.13 משפט ברנסייד

תרגיל 9.5.35 תהי $A\in \mathrm{M}_n(F)$ מטריצה המקיימת $A^d=1$ כאשר d זר ל־$\mathrm{char}F$. הראה שאם הפולינום האופייני של A מתפצל ב־F וכל הערכים העצמיים של A שווים, אז A סקלרית.

למה 9.5.36 אם $(n_u,h_i)=1$ אז או ש־$\chi_u(g_i)=0$ או ש־$\rho_u(g_i)$ סקלרית.

הוכחה. נכתוב $sn_u+s'h_i=1$ עבור $s,s'\in\mathbb{Z}$. נתבונן בערך $\alpha=\frac{\chi_u(g_i)}{n_u}$, אז $\alpha=s\chi_u(g_i)+s'\frac{h_i}{n_u}\chi_u(g_i)$ הוא צירוף שלם של שלמים אלגבריים, ולכן שלם אלגברי בעצמו. לכן גם כל $\sigma(\alpha)$ הוא שלם אלגברי, וגם $\mathrm{N}(\alpha)=\mathrm{N}_{\mathbb{Q}[\omega_N]/\mathbb{Q}}(\alpha)=\prod_\sigma\sigma(\alpha)$ שלם אלגברי.

נסמן ב־N את הסדר של g_i, וב־ω_N שורש יחידה פרימיטיבי מסדר N, כך ש־$\alpha\in\mathbb{Q}[\omega_N]$. לפי הערה 9.5.10, $|\alpha|\leq 1$, ואותו נימוק חל על $\sigma(\alpha)$ לכל $\sigma\in\mathrm{Gal}(\mathbb{Q}[\omega_N]/\mathbb{Q})$. לכן גם $\mathrm{N}(\alpha)\in\mathbb{Q}$ הוא בעל ערך מוחלט קטן או שווה ל־1, ומכאן ש־$\mathrm{N}(\alpha)=0,\pm1$. לכן גם $\alpha=0$ או $|\alpha|=1$; $\chi_u(g_i)=0$ במקרה הראשון, ו־$\rho_u(g_i)$ סקלרית בשני לפי תרגיל 9.5.35. □

מסקנה 9.5.37 נניח ש־G פשוטה לא אבלית. אם ρ הצגה אי־פריקה לא־טריוויאלית ו־$(\dim(\rho),h_i)=1$ אז $\chi_\rho(g_i)=0$.

הוכחה. מכיוון ש־G פשוטה וההצגה לא טריויאלית, $K=\mathrm{Ker}(\rho^{(u)})=1$. נתבונן בתמונה ההפוכה של המטריצות הסקלריות, $N=(\rho^{(u)})^{-1}(\mathrm{Z}(\mathrm{GL}_{n_u}(F)))$; גם זו תת־חבורה נורמלית של G, ולכן $N=1$ או $N=G$. במקרה השני ρ משכן את G בתוך חבורת המטריצות הסקלריות, בסתירה להנחה ש־G לא אבלית. לכן $N=1$, כלומר $\rho(g)$ אינה סקלרית, ולכן $\chi_u(g_i)=0$ לפי למה 9.5.36. □

למה 9.5.38 תהי G חבורה פשוטה. אז אין ב־G מחלקת צמידות מסדר חזקה של ראשוני.

הוכחה. אפשר להניח ש־G לא אבלית. נניח שהגודל h_i של מחלקת הצמידות C_i הוא חזקה של הראשוני p, ונקבע $g_i\in C_i$. לפי יחס שור השני, $0=\sum_u\chi_u(g_i)\overline{\chi_u(1)}=\sum_u n_u\chi_u(g_i)$. בסכום משמאל משתתפים שלושה מרכיבים: $\chi_1(g_i)=1$ עבור ההצגה הטריוויאלית, הסכום עבור ההצגות ממימד זר ל־p שהוא אפס לפי מסקנה 9.5.37, והסכום עבור הצגות שממימדן מתחלק ב־p. מכיוון שהסכום הוא אפס יוצא ש־$\frac{1}{p}$ שלם אלגברי, בסתירה. □

משפט 9.5.39 (משפט ברנסייד) *חבורה מסדר p^iq^j אינה פשוטה.*

הוכחה. **תהי P תת־חבורת p־סילו של G. נתבונן במרְכָּז $Z = \mathrm{Z}(P)$, שאינו טריוויאלי כי P חבורת־p. נבחר $1 \neq z \in Z$, ונתבונן במרכֵּז $H = \mathrm{C}_G(z)$, המכיל את P. לכן $[G\colon H]$ הוא חזקה של q; אבל זהו מספר האברים במחלקת הצמידות של z, שאינו יכול להיות חזקת ראשוני לפי למה 9.5.38, ולכן הוא שווה ל־1. כלומר, $z \in \mathrm{Z}(G)$, בסתירה להנחה ש־G פשוטה.** $\square$

מסקנה 9.5.40 כל חבורה G מסדר $p^i q^j$ היא פתירה.

הוכחה. **לפי המשפט יש לחבורה כזו תת־חבורה נורמלית N, ולפי הנחת האינדוקציה $N, G/N$ פתירות.**$\square$

פרק 10

המכפלה הטנזורית

10.1 מכפלה טנזורית של מטריצות

כאשר מבצעים חישובים במטריצות בלוקים, נוח להגדיר את הסכום הישר $A \oplus B$ כמטריצה שממדיה הם סכום הממדים של A ו־B, עם שני הבלוקים A, B באלכסון.

תהיינה $A \in \mathrm{M}_n(F)$ ו־$B \in \mathrm{M}_m(F)$. מגדירים $A \otimes B \in \mathrm{M}_{nm}(F)$ כמטריצה של $n \times n$ בלוקים, שרכיביה הם $a_{ij}B$. מכפלה זו (שאפשר להגדיר בדיוק באותו אופן גם למטריצות לא ריבועיות) מקיימת את התכונות:

$$A \otimes (B \oplus B') = A \otimes B \oplus A \otimes B';$$

$$A \otimes (B + B') = A \otimes B + A \otimes B';$$

$$(A \otimes B)(A' \otimes B') = AA' \otimes BB'.$$

תרגיל 10.1.1 $\mathrm{tr}(A \otimes B) = \mathrm{tr}(A)\mathrm{tr}(B)$.

תרגיל 10.1.2 חשב את הדטרמיננטה $\det(A \otimes B)$ כפונקציה של $\det(A)$, $\det(B)$ וממדי המטריצות.

10.2 מכפלה טנזורית של מרחבים וקטוריים

סכום ישר של מרחבים וקטוריים מוגדר לפי $F^n \oplus F^m = F^{n+m}$. את המכפלה נגדיר באותו אופן, $F^n \otimes F^m = F^{nm}$. נניח ש־$A \in \mathrm{M}_n(F)$ ו־$A' \in \mathrm{M}_{n'}(F)$. הסכום הישר $A \oplus A'$ מגדיר העתקה לינארית על הסכום הישר של המרחבים, לפי $(A \oplus A')(v \oplus v') = Av \oplus A'v'$.

בדומה לזה, נרצה שהמכפלה הטנזורית $A \otimes A'$ תהיה העתקה $F^n \otimes F^m \to F^n \otimes F^m$. במקום להגביל את התאור לבסיסים הסטנדרטיים, נתבונן במקרה הכללי. נבחר בסיסים $B = \{b_i\}$ ו־$B' = \{b'_j\}$ של מרחבים וקטוריים V, V', בהתאמה, ונגדיר את $V \otimes V'$ כמרחב הוקטורי שנפרש, פורמלית, על־ידי קבוצת הסמלים $B \otimes B' = \{b_i \otimes b'_j\}$. ברור ש־$\dim(V \otimes V') = \dim(V)\dim(V')$. לכל $v = \sum \alpha_i b_i \in V$ ו־$v' = \sum \alpha'_{i'} b'_{i'} \in V'$ נסמן $v \otimes v' = \sum_{i,i'} \alpha_i \alpha'_{i'} b_i \otimes b'_{i'}$.

תרגיל 10.2.1 הוכח את התכונות $(u+v)\otimes w = u\otimes w+v\otimes w$, $u\otimes(v+w) = u\otimes v+u\otimes w$, $(\alpha u)\otimes w = u\otimes(\alpha w) = \alpha(u\otimes w)$.

תרגיל 10.2.2 תהיינה $T: V\to V$ ו־$T': V'\to V'$ העתקות לינאריות. נגדיר את המכפלה $T\otimes T': V\otimes V'\to V\otimes V'$ לפי $(T\otimes T')(b_i\otimes b'_{i'}) = T(b_i)\otimes T'(b'_{i'})$. הראה ש־$[T\otimes T']_{B\otimes B'} = [T]_B\otimes[T']_{B'}$.

10.3 מכפלה טנזורית של אלגברות

בהמשך לסעיף הקודם, נניח ש־A, A' אלגברות מעל שדה F. על המכפלה הטנזורית $A\otimes A'$ אפשר להגדיר כפל לפי $(a\otimes a')(b\otimes b') = ab\otimes a'b'$.

תרגיל 10.3.1 בהנחה ש־A, A' אלגברות אסוציאטיביות, גם $A\otimes A'$ אסוציאטיבית. (זו תכונה קלה, אבל לא טריוויאלית: מכפלה טנזורית של אלגברות לי, למשל, אינה אלגברת לי. אבל אם C אלגברה קומוטטיבית אסוציאטיבית ו־L אלגברת לי, אז $C\otimes L$ היא אלגברת לי.)

תת־האלגברות $A\otimes F$ ו־$F\otimes A'$ של $A\otimes A'$ איזומורפיות ל־A ול־A' בהתאמה, ומתחלפות איבר איבר. (המכפלה הטנזורית היא האלגברה הקטנה ביותר המכילה עותקים מתחלפים של שתי האלגברות.)

תרגיל 10.3.2 $A \cong F\otimes A$.

תרגיל 10.3.3 $A\otimes B \cong B\otimes A$; $A\otimes(B\otimes C) \cong (A\otimes B)\otimes C$.

תרגיל 10.3.4 הראה ש־$\mathrm{Z}(A\otimes A') = \mathrm{Z}(A)\otimes\mathrm{Z}(A')$.

דוגמא 10.3.5 **נניח ש־A אלגברה מעל שדה F, ו־$K \supseteq F$ הרחבה. אז $K\otimes_F A$ היא אלגברה מעל $K = K\otimes_F F$, עם $\dim_K(K\otimes_F A) = \dim_F(A)$.**

תרגיל 10.3.6 $\mathrm{M}_n(F)\otimes\mathrm{M}_m(F) \cong \mathrm{M}_{nm}(F)$.

תרגיל 10.3.7 תהי A אלגברה מעל F, אז $A[\lambda] \cong A\otimes F[\lambda]$.

תרגיל 10.3.8 $\mathbb{Q}[\sqrt{2}]\otimes_{\mathbb{Q}}\mathbb{Q}[\sqrt{7}] \cong \mathbb{Q}[\sqrt{2}, \sqrt{7}]$.

תרגיל 10.3.9 לכל הרחבה ריבועית (במאפיין שונה מ־2), $K\otimes_F K \cong K \times K$. למשל, $\mathbb{C}\otimes_{\mathbb{R}}\mathbb{C} \cong \mathbb{C} \times \mathbb{C}$.

10.4 מכפלה טנזורית של הצגות

סכום ישר של המטריצות מוביל להגדרת סכום ישר של הצגות: $(\psi \oplus \psi')(g) = \psi(g) \oplus \psi'(g)$. באותו אופן, מכפלה טנזורית של מטריצות מאפשרת להגדיר מכפלה טנזורית של הצגות, שהיא הצגה של המכפלה הקרטזית של שתי חבורות: בהנתן $\psi : F[G] \rightarrow \mathrm{M}_n(F)$ ו־$\psi' : F[G'] \rightarrow \mathrm{M}_{n'}(F)$, מגדירים

$$\psi \otimes \psi' : G \times G' \rightarrow \mathrm{M}_{nn'}(F)$$

לפי $(\psi \otimes \psi')(g, g') = \psi(g) \otimes \psi'(g')$.

תרגיל 10.4.1 הראה ש־$\psi \otimes \psi'$ היא אכן הצגה של $G \times G'$.

תרגיל 10.4.2 הקרקטר של הצגה כזו הוא מכפלת הקרקטרים: $\chi_{\psi \otimes \psi'} = \chi_\psi \chi_{\psi'}$.

טענה 10.4.3 לכל שתי חבורות G, H, $F[G \times H] \cong F[G] \otimes_F F[H]$.

מסקנה 10.4.4 נסמן ב־X_G את טבלת הקרקטרים של החבורה G. אז בסידור מתאים של מחלקות הצמידות וההצגות, $X_{G \times H} = X_G \otimes X_H$.

10.5 מכפלה טנזורית של מודולים

עד כאן יכולנו להעזר בבסיס מעל שדה. מאד לא נוח לעבוד עם הגדרה כזו, משום שבכל צעד צריך להוכיח שהתוצאה אינה תלויה בבסיס. יתרה מזו, אנו רוצים הגדרה שתפעל גם כאשר אין בסיס כלל.

הגדרה 10.5.1 *יהי R חוג, ויהיו M_R מודול ימני ו־${}_RN$ מודול שמאלי. אז המכפלה הטנזורית $M \otimes_R N$ היא החבורה האבלית הנוצרת על־ידי הסמלים $m \otimes n$ ($m \in M, n \in N$), בכפוף ליחסים הבאים:*

$$(m + m') \otimes n = m \otimes n + m' \otimes n, \qquad (m, m' \in M, n \in N)$$

$$m \otimes (n + n') = m \otimes n + m \otimes n', \qquad (m \in M, n, n' \in N)$$

$$m\alpha \otimes n = m \otimes \alpha n \qquad (m \in M, n \in N, \alpha \in R).$$

בניגוד למכפלה טנזורית של אלגברות, המכילה עותק של שני הגורמים, מכפלה טנזורית מעל חוג כללי אינה "שטוחה", ומידע עלול ללכת לאיבוד.

תרגיל 10.5.2 $(\mathbb{Z}/4\mathbb{Z}) \otimes (\mathbb{Z}/3\mathbb{Z}) = 0$.

כדי להוכיח תכונות של המכפלה הטנזורית, בהעדר שדה בסיס שמעליו אפשר להפעיל אלגברה לינארית, נגדיר את המושג הטכני הבא:

הגדרה 10.5.3 *יהיו M, N מודולים כבהגדרה הקודמת, ותהי C חבורה אבלית.* ***העתקה מאוזנת*** *היא פונקציה $f: M \times N \to C$ המקיימת את שלוש התכונות $f(m+m', n) = f(m,n) + f(m',n)$, $f(m, n+n') = f(m,n) + f(m,n')$, ו־$f(m\alpha, n) = f(m, \alpha n)$ (זהו* ***אינו*** *הומומורפיזם של חבורות; המבנה של $M \times N$ כחבורה חיבורית, שבה $(m,n) + (m',n') = (m+m', n+n')$,* ***אינו*** *בא כאן לידי ביטוי כלל).*

הגדרה 10.5.4 *נאמר שחבורה T עם פונקציה $\theta: M \times N \to T$ היא* ***אוניברסלית*** *ביחס למכפלות מאוזנות מ־$M \times N$* *אם לכל העתקה מאוזנת $f: M \times N \to C$ קיים הומומורפיזם יחיד של חבורות $\bar{f}: T \to C$, כך ש־$\bar{f} \circ \theta = f$.*

טענה 10.5.5 לכל M, N, מודול ימני ומודול שמאלי מעל R, המכפלה הטנזורית $M \otimes_R N$ היא אוניברסלית ביחס למכפלות מאוזנות (כלומר לכל $f: M \times N \to C$ מאוזנת קיים הומומורפיזם יחיד $\bar{f}: M \otimes_R N \to C$ כך ש־$\bar{f}(a \otimes b) = f(a,b)$.)

הוכחה. לפי משפט האיזומורפיזם הראשון. $\square$

תרגיל 10.5.6 גישה קטגורית להגדרה: נתונים מודולים M, N. נניח שקיימת חבורה אבלית T עם פונקציה $\theta: M \times N \to T$, שהיא אוניברסלית ביחס להעתקות מאוזנות. אז T יחידה עד־כדי איזומורפיזם.

על־פי ההגדרה הזו, המכפלה הטנזורית היא חבורה אבלית, בלי הגדרה טבעית של כפל בסקלרים מ־R. הפקדנו שני מודולים, וקיבלנו רק חבורה חיבורית. כדי להתגבר על החסרון הזה נטפל בבי־מודולים, ונזכיר שאם R חוג קומוטטיבי אז כל מודול הוא אוטומטית בימודול מעל R, R; כמו כן, כל מודול שמאלי הוא בימודול מעל $R, \mathbb{Z}$, וכל מודול ימני הוא בימודול מעל $\mathbb{Z}, R$.

הגדרה 10.5.7 *יהיו R, S, T חוגים, ויהיו ${}_RM_S$ ו־${}_SM_T$ בימודולים. אז $N \otimes_S M$, שהוגדר לעיל, הוא R, T־בימודול לפי פעולות הכפל בסקלר*

$$r(x \otimes y) = (rx) \otimes y,$$

$$(x \otimes y)t = x \otimes (yt).$$

תרגיל 10.5.8 כל חוג R אפשר לראות כמודול מעל $R^e = R \otimes_C R^{\mathrm{op}}$, לפי הפעולה $(a \otimes b)(x) = axb$. הראה ש־R מודול פשוט מעל R^e אם ורק אם R חוג פשוט.

תרגיל 10.5.9 יהיו $C \subseteq R$ חוגים, כאשר C קומוטטיבי. הראה שההעתקה $R \otimes_C R^{\mathrm{op}} \to \mathrm{End}_C(R)$ על־ידי $(a \otimes b^{\mathrm{op}})x = axb$ היא הומומורפיזם.

10.6 ההצגה המושרית

תהיינה $H \leq G$ חבורה ותת־חבורה. כל הצגה $\rho : H \to \mathrm{End}(V)$ של H משרה הצגה של G. נציג כאן שלוש דרכים להגדיר את ההצגה המושרית, מן המופשטת למוחשית ביותר.

ראשית, דרך המכפלה הטנזורית.

הגדרה 10.6.1 תהי G חבורה עם תת־חבורה H, ותהי V הצגה של H, כלומר מודול מעל $F[H]$. אז $\tilde{V} = F[G] \otimes_{F[H]} V$ נקראת **ההצגה המושרית** מ־H ל־G. אם $\rho : F[H] \to \mathrm{End}(V)$ היא ההצגה המקורית, מסמנים את ההצגה המושרית ב־ρ^G.

תרגיל 10.6.2 תהיינה $K < H < G$ חבורות, ותהי ρ הצגה של K. הראה ש־$\rho^G = (\rho^H)^G$.

הגדרה שניה, כמרחב וקטורי:

הגדרה 10.6.3 תהי G חבורה עם תת־חבורה H, ותהי $\rho : H \to \mathrm{End}(V)$ הצגה של H. ההצגה המושרית היא המודול $\mathrm{Ind}_H^G(\rho) = \{f : G \to V :\ \forall g \in G, h \in H : f(gh) = \rho(h)f(g)\}$ עם הפעולה $(\mathrm{Ind}(g) \cdot f)(x) = f(g^{-1}x)$.

תרגיל 10.6.4 הוכח ש־$\mathrm{Ind}_H^G(\rho) \cong F[G] \otimes_{F[H]} V$ כמודולים מעל $F[G]$, כאשר V הוא המודול המושרה על־ידי ρ.

תרגיל 10.6.5 הראה, על־פי ההגדרה השניה, שההצגה המושרית מן המודול הטריוויאלי $V = F$ היא המודול של מרחב המנה $F[G/H]$.

כדי לחשב את ההצגה המושרית $F[G] \otimes_{F[H]} V$ באופן מפורש, נפעל באופן הבא. נכתוב $G = \cup a_i H$, אז לכל $g \in G$ ולכל i יש j יחיד כך ש־$g a_i \in a_j H$ (הפונקציה $g : i \mapsto j$ היא הפעולה מוכרת מהעידון של משפט קיילי). כעת אם H פועלת על מודול V (כאשר ההצגה היא $\rho : F[H] \to \mathrm{End}(V)$), נכתוב את V^n כסכום פורמלי $\oplus x_i V$, ונגדיר $g x_i v = x_j (x_j^{-1} g x_i) v$. זוהי **ההצגה המושרית**, ρ^G.

תרגיל 10.6.6 חשב את ρ^G במקרה המיוחד $H \triangleleft G$.

טענה 10.6.7 תהיינה $H < G$ חבורות, ρ, ρ' הצגות של H. אז $(\rho \oplus \rho')^G = \rho^G \oplus \rho'^G$.

טענה 10.6.8 תהיינה $H < G$ חבורות, ρ הצגה של H, σ הצגה של G. אז $\sigma^G \otimes \rho = (\sigma \otimes \rho|_H)^G$. בפרט, $(\rho|_H)^G = 1^G \otimes \rho$.

את הקרקטר המושרה, כלומר הקרקטר של ההצגה המושרית, אפשר לחשב בעזרת הנוסחה הבאה:

טענה 10.6.9 $\chi^G(g) = \sum_{a_i^{-1} g a_i \in H} \chi(a_i^{-1} g a_i)$.

טענה 10.6.10 יהיו χ קרקטר של G ו־ψ קרקטר של תת־חבורה H. אז $(\psi, \chi_H)_H = (\psi^G, \chi)_G$.

הוכחה. נפרק לקוסטים $G = \bigcup_{i=1}^{m} x_i H$, ונחשב:

$$\begin{aligned}
(\psi^G, \chi)_G &= \frac{1}{|G|}\sum_g \psi^G(g)\overline{\chi(g)} \\
&= \frac{1}{|G|}\sum_g \sum_{a_i^{-1}ga_i\in H} \psi(a_i^{-1}ga_i)\overline{\chi(g)} \\
&= \frac{1}{|G|}\sum_i \sum_{g\in a_iHa_i^{-1}} \psi(a_i^{-1}ga_i)\overline{\chi(a_i^{-1}ga_i)} \\
&= \frac{1}{|G|}\sum_i \sum_{h\in H} \psi(h)\overline{\chi(h)} \\
&= \frac{m|H|}{|G|}(\psi, \chi_H)_H = (\psi, \chi_H)_H.
\end{aligned}$$

□

כדי לחשב את פעולות הצמצום וההשראה, די להכיר אותן עבור קרקטרים אי־פריקים. לפי נוסחת הדואליות, ידיעת הפירוק של ההצגות המושרות מן ההצגות האי־פריקות של H, שקולה לידיעת הפירוק של ההצגות המצומצמות מן ההצגות האי־פריקות של G.

תרגיל 10.6.11 נקבע $G = S_4$ ו־$H = D_4$ עם השיכון הטבעי $H \hookrightarrow G$. חשב את פעולות הצמצום וההשראה בין ההצגות האי־פריקות של שתי החבורות.

10.6.1 משפט האינדוקציה

נאמר שתת־חבורה היא p־אלמנטרית אם היא מכפלה של חבורת־p בחבורה ציקלית מסדר זר ל־p. אחת התוצאות היסודיות בתורת ההצגות היא **משפט האינדוקציה של בראוור**, שלפיו חוג הקרקטרים של חבורה סופית G נוצר, כחוג מעל השלמים, על־ידי הקרקטרים המושרים מתת־חבורות אלמנטריות (היינו p־אלמנטריות לאיזשהו p). נובע מכך למשל ש־$\mathbb{Q}[\rho_e]$ הוא שדה פיצול של החבורה כאשר $e = \exp(G)$.

פרק 11

שאלות חזרה

1. רשום את הקרקטרים של חבורה מסדר 5.
2. הוכח שכל חוג ארטיני שמאלי הוא נתרי שמאלי.
3. תן דוגמא לחוג פרימיטיבי שאין לו אידיאל שמאלי מינימלי $\neq 0$.
4. תן דוגמא לחוג פרימיטיבי שאינו פשוט.
5. הוכח: אם R ראשוני ארטיני אז הוא מטריצות מעל חוג עם חילוק (העזר רק במשפט הצפיפות ובלמה של שור).
6. הוכח ש־$\mathbb{C}[G]$ אינו יכול להיות חוג ראשוני עבור חבורה סופית $G \neq 1$ (זה לא נכון עבור חבורה מסדר אינסופי).
7. הוכח שמספר הקרקטרים האי־פריקים של G שווה למספר מחלקות הצמידות של G.
8. מצאו את כל ההצגות האי־פריקות של $\mathbb{Z}_2 \times \mathbb{Z}_2$.
9. תנו דוגמא לחוג פרימיטיבי שאינו פשוט ארטיני, אבל עם $\operatorname{soc}(R) = 0$.
10. הגדר את הרדיקל של ג'ייקובסון. מהו הרדיקל של $\mathbb{Z}_n$, כאשר $n \in \mathbb{N}$?
11. הוכח את משפט הצפיפות.
12. הוכח: כל חוג פרימיטיבי הוא ראשוני; אם R חוג ראשוני עם אידיאל שמאלי מינימלי L, אז כל מודול נאמן מעל R איזומורפי ל־L.
13. הגדר חוג ראשוני למחצה. הגדר אינוולוציה. הוכח שאם R חוג ארטיני עם אינוולוציה אנאיזוטרופית (כלומר $aa^* \neq 0$ לכל $a \neq 0$), אז R ראשוני למחצה.
14. תהיינה G, H חבורות סופיות. הוכח ש־$F[G \times H] \cong F[G] \otimes F[H]$.
15. תן דוגמא לאלגברות פשוטות A, B מעל שדה F, כך ש־$A \otimes_F B$ אינו פשוטה.
16. הוכח: אם M מודול בעל משלימים, אז הוא פשוט למחצה.
17. הוכח: חוג פרימיטיבי קומוטטיבי הוא שדה.

18. בנה את טבלת הקרקטרים של S_4.

19. יהי $R = \mathrm{M}_2(\mathbb{Z}_4) \oplus \mathrm{M}_2(\mathbb{Z}_6)$. חשב את $J(R)$.

20. יהי R חוג. הוכח ש־$J(J(R)) = J(R)$ וש־$J(R/J(R)) = 0$.

21. יהי R חוג קומוטטיבי ארטיני בלי אברים נילפוטנטיים. הוכח ש־R הוא סכום ישר של שדות.

22. הראה שאלגברת החבורה $\mathbb{R}[\mathbb{Z}]$ אינה ארטינית.

23. תאר את האידיאלים הראשוניים־למחצה של $\mathbb{Z}$.

24. הגדר חוג ראשוני; חוג פרימיטיבי. הוכח שכל חוג פרימיטיבי הוא ראשוני. תן דוגמא לחוג ראשוני שאינו פרימיטיבי.

25. הגדר $\mathrm{soc}(M)$, והוכח ש־$\mathrm{soc}(M)$ שווה לחיתוך כל תת־המודולים הגדולים של M.

26. הוכח שחבורת התמורות הזוגיות A_4 בעל 4 מחלקות צמידות. בנה את לוח הקרקטרים של A_4.

27. הוכח: אם G חבורה סופית, אז יש ל־$\mathbb{C}[G]$ מספר סופי של מודולים פשוטים, עד כדי איזומורפיזם.

28. הוכח: אם R פשוט למחצה ארטיני, אז $\mathrm{M}_2(R)$ פשוט למחצה ארטיני.