

מבוא לחוגים ומודולים

עוזי וישנה

16 במרץ 2017

מבוא לחוגים ומודולים

מהדורה 1.342

הקדמה. תורת החוגים עשירה בשיטות ורעיונות, וחובקת דוגמאות מכל תחומי המתמטיקה. קורס ראשון בתחום מוגבל, מטבע הדברים, למושגים הפשוטים יותר. אחרי פרק מבוא כללי, המציג חוגים, אידאלים והומומורפיזמים, הפרק השני נותן הצצה לתורת המבנה ועוסק בכמה מחלקות חשובות של חוגים, ובטכניקה היסודית של מיקום ביחס לאידיאל ראשוני. הפרק השלישי מוקדש לתחומי שלמות, שהם החוגים החשובים ביותר מנקודת המבט של תורת המספרים והגאומטריה האלגברית. הפרק הרביעי מוקדש לפולינום מעל תחומי שלמות, ובמיוחד מעל שדות. הפרק החמישי הוא מבוא לתורת המודולים, שהם המרחבים שעליהם פועלים החוגים השונים.

חוברת זו ערוכה ומסודרת לפי תוכנית הלימודים בקורס 'אלגברה מופשטת 2' לתלמידי מתמטיקה, 88-212, באוניברסיטת בר-אילן. הקורס (בהיקף של ארבע שעות הרצאה ושעתיים תרגיל, לאורך סמסטר אחד) הוא קורס שני באלגברה מודרנית (אחרי קורס סמסטריאלי בחבורות), והוא מכסה את היסודות של תורת החוגים, ואת תורת המודולים מעל תחומים ראשיים, עם היישומים של תורה זו לאלגברה לינארית. לצד החוברת הזו, ניתן להעזר גם בחוברת תרגילים השייכת לאותו קורס.

החומר מחולק לסעיפים ותת-סעיפים, המסודרים כך שמושגים חיוניים יופיעו מוקדם ככל האפשר, תוך שילוב של כמה דוגמאות נחוצות. בכל נושא מובאות ההגדרות והתוצאות העיקריות, כשהן פרושות לתרגילים קצרים ונוחים לעיכול. כל טענות העזר והשיטות הסטנדרטיות נוסחו כתרגילים. המהדורה הארוכה, המונחת לפניכם, כוללת הדרכה מפורטת ולפעמים פתרון מלא לתרגילים רבים, בעיקר אלו שיש להם אופי תאורטי יותר. סדר התרגילים בתוך כל סעיף נבחר בזהירות, כשכל תרגיל מופיע מיד כאשר הונחה התשתית לרעיונות הדרושים כדי לפתור אותו (אך בכפוף לאילוץ המקובל, והמתסכל במידת מה, הקובע שסדר המשפטים בעמוד מוכרח להיות קווי). תרגילים השייכים לאותה מדרגה לוגית מופיעים בסדר יורד של מידת הכלליות והעניין.

החידוש, במידה שיש כאן כזה, הוא בהצמדת דרגת קושי לכל תרגיל: תרגילים קלים, מדרגה (*), דורשים בדרך-כלל שליטה בהגדרות ותו לא; את רובם של אלה אפשר - ורצוי - לפתור בעל-פה, תוך ציון ההגדרה או העובדה הרלוונטית. תרגילים טכניים מורכבים, לא רגילים או סתם קשים סומנו ב- (***) . שאר התרגילים קיבלו את הציון (**). סימנים נוספים, כמו ב- (**) או ב- (**), מציינים שהתרגיל עשוי להיות קשה או קל יותר מכפי שנראה במבט ראשון. במספר מקומות הרחבנו מעבר לרמה הנדרשת בקורס.

כל התרגילים מנוסחים בלשון זכר, ועם הלומדות הסליחה. אודה לכל מי שיביא לתשומת ליבי שגיאות מתמטיות, השמטות, כפילויות או שגיאות כתיב, כדי שאוכל לתקן במהדורה הבאה.

עוזי וישנה, 9.2015

תוכן עניינים

9	1 חוגים ואידיאלים
9	1.1 מושגי יסוד
9	1.1.1 אברים של חוגים
10	אבר האפס
10	קומוטטיביות
10	אברי יחידה
11	אברים הפיכים
12	חוגים עם חילוק
13	מחלקי אפס ואברים רגולריים
14	תחומים ותחומי שלמות
15	אברים נילפוטנטיים
15	המאפיין
15	1.1.2 תת-חוגים
16	תת-חוגים בלי יחידה
16	המרכז והמרכז
17	יוצרים של תת-חוג
17	1.1.3 חוגים לא אסוציאטיביים
18	חוגים אלטרנטיביים
18	חוגי לי
19	חוגי ז'ורדן
19	חוגים לא אסוציאטיביים עם חילוק
21	איזוטופיות
21	1.2 אידיאלים וחוגי מנה
22	1.2.1 אידיאלים חד-צדדיים ודו-צדדיים
22	איחוד וחיתוך
23	קבוצת יוצרים
23	אידיאלים אמיתיים
24	1.2.2 סכום ומכפלה של אידיאלים
24	סכומים סופיים וכלליים
25	מכפלה
26	סריג האידיאלים
27	מאפסים
28	1.2.3 חוגי מנה
29	1.2.4 הומומורפיזמים
29	הומומורפיזמים של חוגים בלי יחידה

30	הגרעין והתמונה	
31	חוגים איזומורפיים	
31	משפטי האיזומורפיזם	1.2.5
32	תת-החוג היסודי	
32	הומומורפיזם ויוצרים	
33	החוג החופשי	
34	דוגמאות ובניה של חוגים	1.3
34	בניות קלאסיות	1.3.1
34	חוג השלמים	
34	מטריצות	
36	חוג האנדומורפיזמים	
37	פולינומים	
38	מכפלה ישרה של חוגים	
39	סכום ישר של חוגים	
39	אלגברות	1.3.2
40	אלגברות חבורה	
40	אלגברת הקוטרניונים	
41	חוגים סדורים	
41	איחוד על שרשראות	
41	גבול ישר	
42	גבול הפוך	
45	אידיאלים ראשוניים ומקסימליים	2
45	אידיאלים מקסימליים	2.1
45	קיומם של אידיאלים מקסימליים	2.1.1
47	אידיאלים מינימליים	
47	אידיאלים מקסימליים של חוגי פונקציות	
47	חוגים פשוטים	2.1.2
48	הקשר לאידיאלים מקסימליים	
48	חוגים פשוטים קומוטטיביים	
48	בניה של חוגים פשוטים	
49	חוגים n -פשוטים	
49	פירוק למכפלה ישרה	2.2
49	אידיאלים קו-מקסימליים	2.2.1
50	משפט השאריות הסיני	2.2.2
51	משפט השאריות הסיני מעל השלמים	
52	אידמפוטנטים	2.2.3
53	אידמפוטנטים מרכזיים בתורת המבנה	
53	פירוק פירס	
54	חוגים בוליאניים	
55	אידיאלים אידמפוטנטיים	
55	חוגים מקומיים	2.3
57	שדה המספרים הממשיים	
62	מסננים וחוגים בוליאניים	
62	אידיאלים ראשוניים	2.4

62	חוגים ראשוניים	2.4.1
64	אידיאלים ראשוניים	2.4.2
66	רדיקלים	2.4.3
66	מיקום ושדה השברים	2.5
66	מיקום מרכזי	2.5.1
67	הכללה למקרה הלא רגולרי	
68	האוניברסליות של המיקום	
68	האידיאלים של $S^{-1}R$	
70	חוג השברים הטוטאלי	
70	מיקום באידיאל ראשוני	2.5.2
72	שדה השברים	2.5.3
73	3 תחומי שלמות	
73	חוגי שלמים ריבועיים	3.1
74	האינוולוציה, העקבה והנורמה	
75	חוגים בעלי נורמה	3.1.1
75	אברים ראשוניים ואי-פריקים	3.2
75	יחס החילוק	3.2.1
76	תאור לפי אידיאלים	
76	אברים הפיכים	3.2.2
76	אברים הפיכים של $\mathcal{O}_D$	
77	אברים אי-פריקים	3.2.3
79	אברים ראשוניים	3.2.4
79	פירוק לגורמים	3.3
79	חוגים אטומיים	3.3.1
81	חוגים נתריים	3.3.2
83	תחומי פריקות יחידה	3.3.3
84	תחומים ראשיים	3.3.4
86	מחלק משותף מקסימלי	
87	תחומי gcd	
88	תחומי בזו	
90	כפולה משותפת מינימלית	
93	חוגים אוקלידיים	3.3.5
94	אוקלידיות של חוגים סמוכים	
94	אוקלידיות של חוגי שלמים	
95	הראשוניים של $\mathbb{Z}[\sqrt{-1}]$	
96	שימושים נוספים בתורת המספרים	
97	תנאי הכרחי לאוקלידיות	
97	קוואזי-אוקלידיות	
98	הערכות ותחומי הערכה	3.4
98	הערכות ותחומי הערכה	3.4.1
98	חבורות סדורות	
99	הערכה של שדה	
100	תחומי הערכה	
101	הערכות מדרגה 1	

102	הערכות בדידות מדרגה 1	
103	טורי לורן ודוגמאות נוספות	3.4.2
103	טורי לורן	
105	שדה Puiseux	
105	טורי לורן בשני משתנים	
107	טורי חזקות דועכים מעל שדה הערכה	
108	טורי חזקות ארוכים	

4 פולינומים ושדות

109	מבוא לתורת השדות	4.1
109	ממד של אלגברות	4.1.1
110	הפולינום המינימלי	4.1.2
110	שורשים ושדה מפצל	4.1.3
111	סיפוח שורשים	
111	פירוק של פולינומים	4.2
112	שורשים רציונליים	4.2.1
112	קריטריון אייזנשטיין	4.2.2
113	הלמה של גאוס	4.2.3
113	תכולה של פולינום	
114	הלמה של גאוס	
115	פירוק פולינומים מעל תחום פריקות יחידה	

5 מודולים

117	מבוא	5.1
117	הגדרה ודוגמאות	5.1.1
119	מושגי יסוד	5.1.2
119	תת־מודולים	
119	מודול מנה	
119	סכום של תת־מודולים	
120	מכפלה ישרה וסכום ישר	
120	הומומורפיזמים	
121	אלגברה לינארית של מודולים	5.1.3
121	מודולים חופשיים	
122	אינווריאנטיות הדרגה	
123	מודולים ציקליים	
124	פיתול	5.1.4
125	מודול נאמן	
125	מודולים מעל תחום ראשי	5.2
126	מודולים נוצרים סופית	5.2.1
127	מטריצת היחסים	
127	מטריצות מעל תחום ראשי	5.2.2
128	הצורה האלכסונית הקנונית	
129	יחידות הצורה האלכסונית	
130	מטריצות יחסים דומות	
131	פירוק למרכיבים ציקליים	5.2.3

132	תת־מודול הפיתול כמחובר ישר	
133	מיון החבורות האבליות הנוצרות סופית	
133	צורות קנוניות של מטריצות מעל שדה	5.2.4
134	מרחב וקטורי כמודול לפי מטריצה	
135	מחלקות צמידות	
136	הצורה הרציונלית	
136	המטריצה המלווה של פולינום	
137	צורת ז'ורדן	

פרק 1

חוגים ואידיאלים

הפרק הראשון עוסק במושגי היסוד של תורת החוגים: המבנים האלגבריים **חוג בלי יחידה וחוג**; האברים המיוחדים בחוג בלי יחידה; תת-חוגים, אידיאלים חד-צדדיים ודו-צדדיים; הומומורפיזמים וחוגי מנה; ומציג גם רשימה ארוכה של דוגמאות ודרכים לבנות חוגים חדשים מחוגים קיימים.

1.1 מושגי יסוד

בסעיף זה נגדיר חוגים, שהם האובייקטים המרכזיים של הקורס; נציג כמה תכונות פשוטות של אברים בחוג; וניתן שמות הולמים לחוגים שאבריהם מפגינים התנהגות מעניינת.

הגדרה 1.1.1 מערכת מתמטית $\langle R; 0; +, \cdot \rangle$ (שבה הפעולות $+$, $\cdot$ נקראת 'חיבור' ו'כפל' בהתאמה) נקראת **חוג בלי יחידה אם** $\langle R; 0; + \rangle$ חבורה אבלית, ופעולת הכפל היא אסוציאטיבית ודיסטריבוטיבית (מימין ומשמאל) ביחס לחיבור.

הגדרה 1.1.2 אם R **חוג בלי יחידה, החבורה** $\langle R; 0; + \rangle$ **נקראת החבורה החיבורית של** R .

להלן כמה דוגמאות מוכרות: חוג המספרים השלמים; כל שדה, כמו הרציונליים $\mathbb{Q}$ או הממשיים $\mathbb{R}$; והחוג של מטריצות מעל שדה, כמו $M_n(\mathbb{Q})$.

1.1.1 אברים של חוגים

במבוא לתורת החוגים מגדירים חבורה למחצה כמערכת מתמטית שיש לה פעולה אסוציאטיבית. בחבורה למחצה יכולים להיות אברי יחידה מימין ומשמאל, ואבר יחידה (דו-צדדי). חבורה למחצה שיש בה אבר יחידה נקראת **מונויד**. במונויד, אבר יכול להיות הפיך מימין ומשמאל, או הפיך (משני הצדדים). מונויד שבו כל האברים הפיכים נקרא **חבורה**. גם בתורת החוגים, הצעד הראשון הוא לזהות כמה אברים מיוחדים, כדי שנוכל להגדיר מהו חוג ("חוג בלי יחידה" שיש לו יחידה).

משם נתקדם ללמוד אברים יותר מעניינים, שלחלקם יש מקבילה בתורת המונוידים. מן התכונות האלה מתקבלות כמה משפחות מעניינות של חוגים; הדוגמא הידועה ביותר היא שדה, שאינו אלא חוג קומוטטיבי שבו כל האברים הפיכים.

אבר האפס

תרגיל 1.1.3 (*) האבר 0 בחוג מקיים $0 \cdot x = x \cdot 0 = 0$ לכל $x \in R$; ותכונה זו מאפיינת אותו (כלומר, אם $z \cdot x = z$ לכל x , אז $z = 0$). לכן הוא נקרא **אבר האפס**, בהא הידיעה: יש רק אחד כזה. הדרגה: $0 + 0 = 0$.

קומוטטיביות

הגדרה 1.1.4 אברים a, b בחוג הם **מתחלפים** אם $ab = ba$. אם כל האברים בחוג מתחלפים זה עם זה, הוא נקרא חוג קומוטטיבי.

אברי יחידה

הגדרה 1.1.5 יהי R חוג בלי יחידה. אבר $e \in R$ הוא **יחידה מימין** אם $xe = x$ לכל $x \in R$, ו**יחידה משמאל** אם $ex = x$ לכל $x \in R$. אם e יחידה גם מימין וגם משמאל, הוא נקרא **אבר יחידה**.

המינוח 'חוג בלי יחידה' אינו בא לייחס למערכת המתמטית הזו תכונה שלילית כלשהי, אלא רק לומר שאבר היחידה נעדר מן ההגדרה. מיד נראה שלחוג בלי יחידה יכול שיהיה אבר יחידה, ובמקרה כזה נקרא לו **חוג**.

דוגמא 1.1.6 חוג השלמים $\mathbb{Z}$ הוא 'חוג בלי יחידה', שיש בו אבר יחידה: המספר 1. לעומת זאת, $2\mathbb{Z}$ הוא חוג בלי יחידה, שאין בו אבר כזה.

תרגיל 1.1.7 (*) אם יש בחוג יחידה מימין e ויחידה משמאל e' אז יש בחוג אבר יחידה. הדרגה: $e = e'e = e'$.

תרגיל 1.1.8 (*) היחידה יחידה (אם היא קיימת). כלומר, בחוג לא יכולים להיות שני אברי יחידה. הדרגה: קל וחומר מתרגיל 1.1.7.



אבר היחידה מוגדר לפי האינטרקציה שלו עם אברים אחרים; אבל יש לו גם תכונה פנימית: $1^2 = 1$. כל יחידה מימין או משמאל מקיימת את השוויון הזה. בעקבות זאת, כל אבר $e \in R$ המקיים $e^2 = e$ נקרא **אידמפוטנט**. הדיאגרמה משמאל מציגה היררכיה גסה של טיפוסים חוגים. לפי תרגיל 1.1.7, אם יש בחוג אבר יחידה, אז אין בו יחידות נספות. לעומת זאת, יכולים להיות בחוג אידמפוטנטים רבים; נעסוק באברים כאלה בתת-סעיף 2.2.3.

הגדרה 1.1.9 חוג-בלי-יחידה שיש לו אבר יחידה נקרא **חוג (ולפעמים, לשם הדגשה, חוג עם יחידה)**.

כאשר יש אבר יחידה, הוא יחיד (תרגיל 1.1.8), ולכן נסמן את אבר היחידה בסימון השמור 1. כשיש סכנה לבלבול, מסמנים את היחידה של R בסימון 1_R . אפשר לפתח חלקים נכבדים מן התאוריה בקורס הזה עבור חוגים בלי יחידה; אלא שלרוב הדוגמאות החשובות יש יחידה, ולכן נתרכז בחוגים כאלה. ראו גם תרגילים 1.1.37, 1.2.23-1.2.24, המדגימים שתכונות מסויימות מסוגלות לייצר אבר יחידה; ותרגיל 1.2.78 (עמ' 30), המלמד שכל חוג בלי יחידה אפשר להרחיב לכדי חוג עם יחידה.

תרגיל 1.1.10 ()** אם $1_R = 0_R$ (ובאופן כללי יותר, אם אבר האפס הוא אבר יחידה ימני או שמאלי) אז $R = \{0\}$; זהו **חוג האפס**. כלומר, בכל חוג שאינו אפס, אברי האפס והיחידה שונים.

חוג בלי יחידה A_0 הוא **טריוויאלי** אם $A_0^2 = 0$, כלומר לכל $x, y \in A_0$ מתקיים $xy = 0$. בחוג כזה מוגדרת למעשה רק החבורה החיבורית, ומאידך על כל חבורה אבלית אפשר להגדיר מבנה של חוג טריוויאלי. לכן מקומם של חוגים טריוויאליים אינו בקורס על תורת החוגים, אלא בקורס בתורת החבורות האבליות.

תרגיל 1.1.11 (*) חוג עם יחידה אינו טריוויאלי, אלא אם הוא חוג האפס.

דוגמא 1.1.12 דוגמאות לחוגים קומוטטיביים: $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}/n\mathbb{Z}$ (השאריות מודולו n , עם החיבור והכפל מודולו n). דוגמאות לחוגים לא קומוטטיביים: $M_n(\mathbb{R}), M_n(\mathbb{Q})$.

אברים הפיכים

האמור בסעיף זה מתייחס למונויד הכפלי $\langle R, \cdot, 1 \rangle$, בלי קשר לפעולת החיבור, והוא תקף בכל מונויד.

הגדרה 1.1.13 יהי R חוג. אבר $x \in R$ הוא **הפיך מימין אם קיים אבר** $y \in R$ כך ש- $xy = 1$ (במקרה כזה y נקרא 'הפכי מימין של x '), ו**הפיך משמאל אם קיים** z כך ש- $zx = 1$ (z הוא 'הפכי משמאל של x '). האבר x הוא **הפיך אם קיים** y כך ש- $xy = yx = 1$.

אם אבר הפיך, אז הוא בוודאי הפיך מימין ומשמאל. בחוג קומוטטיבי כל המושגים האלה מתלכדים, אבל באופן כללי האפשרויות פתוחות: אבר יכול להיות לא הפיך מימין וגם לא הפיך משמאל; הוא יכול להיות הפיך מימין אבל לא משמאל, או להיפך; ויכולים להיות לו הפכיים ימניים רבים או הפכיים שמאליים רבים. בתרגיל 1.3.28 (עמ' 37) ניתן דוגמא לאבר הפיך משמאל אבל לא מימין (ולחיפך). עם זאת:

תרגיל 1.1.14 (*) אם x הפיך מימין ומשמאל אז הוא הפיך, ויש לו הפכי יחיד. הערה. הטענה אינה טריוויאלית משום שההנחה היא שקיימים y, z כך ש- $yx = xz = 1$, אבל א-פריורי איננו יודעים ש- $y = z$.

לכן, אם x הפיך, אפשר לסמן את ההפכי שלו בסימון x^{-1} .

תרגיל 1.1.15 (*) אם x הפיך אז גם x^{-1} הפיך ו- $(x^{-1})^{-1} = x$.

תרגיל 1.1.16 (*) אם x, y הפיכים, אז גם xy הפיך.

תרגיל 1.1.17 ()** בחוג קומוטטיבי, אם xy הפיך אז גם x, y הפיכים. הערה. טענה זו נכונה לפעמים גם בחוגים לא קומוטטיביים (למשל בחוגי מטריצות מעל שדה), אבל לא באופן כללי: ראו תרגיל 1.3.28 (עמ' 37).

הגדרה 1.1.18 מסמנים ב- $R^\times$ את אוסף האברים ההפיכים של R ; זוהי חבורת ההפיכים של R .

תרגיל 1.1.19 ()** לכל חוג R , $R^\times$ היא אכן חבורה.

חוגים עם חילוק

הגדרה 1.1.20 חוג A שבו פעולות הכפל מימין ומשמאל $\ell_a : x \mapsto ax$ ו $r_a : x \mapsto xa$ הפיכות (כפונקציות $A \rightarrow A$) לכל $a \neq 0$, נקרא חוג עם חילוק.

תרגיל 1.1.21 $(**+)$ התכונות הבאות שקולות עבור חוג A :

1. ℓ_a הוא חד-חד-ערכי לכל $a \neq 0$.

2. r_a הוא חד-חד-ערכי לכל $a \neq 0$.

3. A הוא תחום (היינו אין בו מחלקי אפס).

תרגיל 1.1.22 $(**+)$ התכונות הבאות שקולות עבור חוג A (עם יחידה):

1. ℓ_a הוא על לכל $a \neq 0$.

2. ℓ_a הפיך לכל $a \neq 0$.

3. כל אבר שונה מאפס של A הוא הפיך מימין.

4. כל אבר שונה מאפס של A הוא הפיך.

5. A הוא חוג עם חילוק.

הדרכה. $(1) \Leftrightarrow (2)$: ברור. $(1) \Leftrightarrow (3)$: יהי $a \neq 0$, אז לפי ההנחה יש a' כך ש- $aa' = \ell_a(a') = 1$. $(3) \Leftrightarrow (4)$: יהי $a \neq 0$, אז לפי ההנחה יש $a' \neq 0$ כך ש- $aa' = 1$ ויש a'' כך ש- $a'a'' = a$ כעת $a'' = aa'a'' = a$ ולכן $a' = a^{-1}$. $(4) \Leftrightarrow (5)$: לכל $a \neq 0$, $\ell_{a^{-1}}\ell_a = \ell_a\ell_{a^{-1}} = 1$ ו- $r_{a^{-1}}r_a = r_ar_{a^{-1}} = 1$. ברור. $(2) \Leftrightarrow (5)$: ברור.

תרגיל 1.1.23 $(***-)$ התכונות הבאות שקולות עבור חוג בלי יחידה $A_0 \neq 0$:

1. ℓ_a הוא על לכל $a \neq 0$.

2. ℓ_a הפיך לכל $a \neq 0$.

3. A_0 הוא חוג עם יחידה, עם חילוק.

הדרכה. $(1) \Leftrightarrow (3)$: ברור. $(2) \Leftrightarrow (1)$: לפי ההנחה $aR = \ell_a(R) = R$ לכל $a \neq 0$. נניח ש- $a, b \neq 0$, אז $abR = aR = R$ ולכן $ab \neq 0$. הוכחנו ש- R תחום, וזה מספיק לפי תרגיל 1.1.21. $(3) \Leftrightarrow (2)$: מכיון שכל אופרטור הכפל משמאל חד-חד-ערכיים, A_0 הוא תחום. לפי ההנחה $aA_0 = \ell_a(A_0) = aA_0$. מכאן לפי תרגיל 1.2.24, שיש ב- A_0 אבר יחידה. כעת אפשר ליישם את הגרירה $(2) \Leftrightarrow (5)$ בתרגיל 1.1.22.

תרגיל 1.1.24 $(*)$ A הוא חוג עם חילוק אם ורק אם יש ב- A פתרון יחיד x לכל משוואה $ax = b$ או $xa = b$ שבה $a \neq 0$.

תרגיל 1.1.25 $(**)$ הוכח, בחוג עם חילוק R , את זהות Hua: לכל $x, y \in R$, אם $x \neq 0, y \neq 0$ ו- y^{-1} אז מתקיים

$$(x^{-1} + (y^{-1} - x)^{-1})^{-1} = x - xyx.$$

תרגיל 1.1.26 (*)** אם לכל $a \neq 0$ קיים $x \in R$ כך ש- $ax = 1$, אז R הוא חוג עם חילוק.

(ראה גם תרגיל 2.1.33, עמ' 49.)

הגדרה 1.1.27 שדה הוא חוג קומוטטיבי עם חילוק.

אנו מכירים שדות רבים: $\mathbb{C}, \mathbb{R}, \mathbb{Q}$ או $\mathbb{Z}_p$ כאשר p ראשוני (באלה נטפל בזהירות בהמשך). לעומת זאת, בניה של חוג עם חילוק שאינו שדה היתה אתגר לא פשוט, ורק ב-1843 מצא ויליאם רואן המילטון את הדוגמא הראשונה (ראו תת-סעיף 1.3.2). גם את הדוגמא הזו נציג בהמשך.

חוגים עם חילוק דומים לשדות, בכך שאפשר לפתח מעליהם אלגברה לינארית: אפשר להגדיר מעליהם מרחבים וקטוריים, למרחב וקטורי מעל חוג עם חילוק יש בסיס, יש ממד מוגדר היטב, אפשר לייצג העתקות לינאריות כמטריצות, אפשר לדרג מטריצות בפעולות אלמנטריות, וכו'.

חסרון בולט לתאוריה הזו הוא בכך שאין דטרמיננטה. מעל שדה, הדטרמיננטה היא פונקציה כפלית $\det: GL_n(F) \rightarrow F^\times$. תכונה זו אינה ניתנת להכללה: מעל חוג עם חילוק הדטרמיננטה המוגדרת לפי סכום מתחלף של המכפלות על אלכסונים מוכללים אינה כפלית. עם זאת יש הומומורפיזם חלש יותר, $GL_n(R) \rightarrow R^\times / R'$, הנקרא **דטרמיננטת דודונה** (Dieudonné).

מחלקי אפס ואברים רגולריים

הגדרה 1.1.28 אם $z, z' \neq 0$ מקיימים $zz' = 0$, אז z נקרא **מחלק אפס שמאלי**, ו- z' **מחלק אפס ימני**. אבר שונה מאפס שאינו מחלק אפס שמאלי הוא **רגולרי משמאל**, ואבר שאינו מחלק אפס ימני הוא **רגולרי מימין**. אבר שהוא רגולרי גם מימין וגם משמאל נקרא **רגולרי**.

תרגיל 1.1.29 (*) אם z רגולרי משמאל אז הוא ניתן לצמצום משמאל: $zx = x'z$ נובע $x = x'$.

תרגיל 1.1.30 ()** נניח ש- z הוא מחלק אפס שמאלי. אז לכל $x \in R$, $xz = 0$ מחלק אפס שמאלי אלא אם $xz = 0$.

תרגיל 1.1.31 ()** קבוצת האברים הרגולריים של R סגורה לכפל.

תרגיל 1.1.32 (*)** יהיו R חוג ו- $a \in R$. נסמן ב- ℓ_a את פעולת הכפל משמאל $x \mapsto ax$ וב- r_a את פעולת הכפל מימין $x \mapsto xa$.

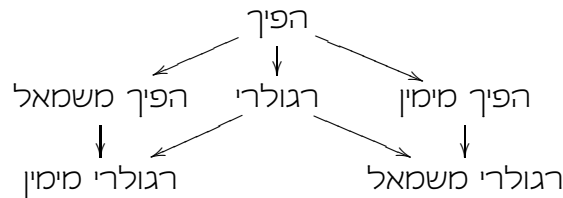
1. ℓ_a חד-חד-ערכי אם ורק אם a רגולרי משמאל.

2. ℓ_a על אם ורק אם a הפיך מימין. הדרכה: לחוג יש אבר יחידה.

3. אם ℓ_a על אז r_a חד-חד-ערכי.

4. אם a רגולרי משמאל והפיך מימין, אז הוא הפיך. הדרכה: $a(a'a - 1) = 0$.

5. מארבעת התנאים " ℓ_a " חד-חד-ערכי, " ℓ_a " על, " r_a " חד-חד-ערכי, " r_a " על אפשר לכאורה להרכיב 2^4 הנחות על a . הראה שהן מצטמצמות למעשה ל-6 האפשרויות הבאות (נוסף על קבוצת ההנחות הריקה):



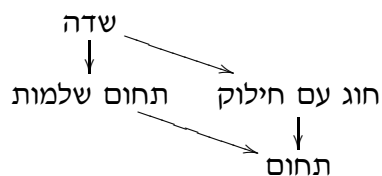
מכיוון שמחלקי אפס מרחיקים את החוג מלהיות שדה, שהוא החוג ה'מוצלח' ביותר, חשוב לנו להכיר חוגים שבהם יש הרבה אברים רגולריים.

תרגיל 1.1.33 (*+) אם כל האברים של R רגולריים משמאל, אז כולם רגולריים גם מימין.

תחומים ותחומי שלמות

הגדרה 1.1.34 חוג שאין בו מחלקי אפס נקרא **תחום**. חוג קומוטטיבי בלי מחלקי אפס נקרא **תחום שלמות**.

טענה 1.1.35 בתחום מתקיימות תכונות הצמצום מימין (כלומר, מ- $xy = x'y$ עם $y \neq 0$ נובע $x = x'$); ותכונות הצמצום משמאל.



תרגיל 1.1.36 (*) חוג עם חילוק הוא תחום.

בפי שהסברנו בסעיף הראשון, אנו עוסקים לאורך כל הקורס בחוגים עם יחידה. בכמה מקרים אפשר לקבל את היחידה בחינם, בלי שנצטרך להניח את קיומה מראש.

תרגיל 1.1.37 (*) אידימפוטנט בתחום בלי יחידה הוא אבר (ה)יחידה. הדרכה. הגדרנו תחום בהגדרה 1.1.34. גם ללא אבר יחידה, $e(a - ea) = ea - e^2a = 0$ גורר $ea = a$ לכל a , וכך גם מימין. **הערה.** בתחום עם יחידה אין אידימפוטנטים לא טריוויאליים בגלל $e(1 - e) = 0$.

תרגיל 1.1.38 (*) בתחום, כל אבר הפיך משמאל הוא הפיך. הדרכה. אם $xy = 1$ אז $(yx)^2 = yxyx = yx$ ולכן $yx = 1$.

תרגיל 1.1.39 ()** כל תחום סופי הוא חוג עם חילוק. הדרכה. כל מונויד סופי עם צמצום הוא חבורה.

תרגיל 1.1.40 ()** נתבונן בחוג $R = \left\{ \begin{pmatrix} 0 & a & b & c \\ 0 & 0 & 0 & -b \\ 0 & 0 & 0 & a \\ 0 & 0 & 0 & 0 \end{pmatrix} : a, b, c \in \mathbb{Z} \right\}$ הראה

שכל אבריו נילפוטנטיים מסדר 2 (כלומר מקיימים $x^2 = 0$), אבל הוא אינו קומוטטיבי.

אברים נילפוטנטיים

הגדרה 1.1.41 אבר $a \in R$ הוא **נילפוטנטי** אם קיים $n \geq 1$ כך ש- $a^n = 0$.

תרגיל 1.1.42 (*) כל אבר נילפוטנטי (שונה מאפס) הוא מחלק אפס.

תרגיל 1.1.43 ()** בחוג קומוטטיבי, אם a נילפוטנטי אז לכל x גם ax נילפוטנטי. תן דוגמא נגדית לטענה זו בחוג שאינו קומוטטיבי.

תרגיל 1.1.44 ()** בחוג קומוטטיבי, סכום של אברים נילפוטנטיים הוא נילפוטנטי.

תרגיל 1.1.45 ()** אם $a \in R$ נילפוטנטי אז $1 - a$ הפיך.

המאפיין

הגדרה 1.1.46 יהי R חוג. המספר $n > 0$ הקטן ביותר כך ש- $\underbrace{1 + \dots + 1}_n = 0$, אם קיים כזה, נקרא **המאפיין של R** . אם לא קיים n כזה, אומרים שהמאפיין הוא אפס.

דוגמא 1.1.47 המאפיין של $\mathbb{Z}/n\mathbb{Z}$ הוא n , והמאפיין של $\mathbb{Z}$ הוא 0.

תרגיל 1.1.48 (*) אם n הוא המאפיין של R , אז $\underbrace{x + \dots + x}_n = 0$ לכל $x \in R$.

תרגיל 1.1.49 ()** המאפיין של תחום הוא אפס או מספר ראשוני.

1.1.2 תת-חוגים

הגדרה 1.1.50 יהי R חוג. תתקבוצה של R נקראת **תת-חוג** אם S סגורה לחיבור, חיסור וכפל, וכוללת את אבר היחידה של R .

תרגיל 1.1.51 ()** אם $S \subseteq R$ תת-חוג, אז S הוא חוג בזכות עצמו, עם הפעולות המצומצמות מ- R .

תרגיל 1.1.52 (*) תת-חוג של חוג קומוטטיבי הוא חוג קומוטטיבי.

תרגיל 1.1.53 ()** תת-חוג של תחום הוא תחום. תת-חוג של תחום שלמות הוא תחום שלמות.

תרגיל 1.1.54 ()** תן דוגמא לתת-חוג של שדה שאינו שדה.

הסיבה לתופעה האחרונה היא הרגישות של תכונת ההפיכות לחוג: בהחלט יתכן ש- $a \in S \subseteq R$ יהיה הפיך ב- R אבל לא ב- S (משום ש- $a^{-1} \in R$ אבל $a^{-1} \notin S$). **שימו לב.** לסימון a^{-1} יש משמעות רק כאשר ברור מההקשר על איזה חוג R מדובר, שבו a הפיך; באופן כללי, איננו יכולים לבטא את הטענה a' אינו הפיך ב- S' בסימון $a'^{-1} \notin S'$!

תרגיל 1.1.55 (*)** תהי Λ משפחה של תת-חוגים של חוג R . הראה שגם החיתוך $\bigcap_{S \in \Lambda} S$ הוא תת-חוג (השווה לתרגיל 1.1.59).

תת-חוגים בלי יחידה

הגדרה 1.1.56 יהי R חוג בלי יחידה. תת-קבוצה $S \subseteq R$ הסגורה לפעולות החיבור, החיסור והכפל נקראת **תת-חוג בלי יחידה של R** .

דוגמא 1.1.57 חוג (עם יחידה) S עשוי להיות תת-חוג בלי יחידה של חוג (עם יחידה) אחר R , בלי להכיל את אבר היחידה שלו: $\begin{pmatrix} * & 0 \\ 0 & 0 \end{pmatrix} \subseteq \begin{pmatrix} * & * \\ 0 & * \end{pmatrix}$. במקרה כזה S אינו תת-חוג של R , משום שאין להם אותו אבר יחידה.

תרגיל 1.1.58 ()** לגבי כל אחד מן הבאים בדוק שהוא חוג בלי יחידה; בדוק האם יש לו אבר יחידה; לגבי כל הכלה (לרבות אלו שאינן מפורשות) קבע האם מדובר בתת-חוג:

$$\begin{pmatrix} * & 0 \\ 0 & 0 \end{pmatrix} \subseteq \begin{pmatrix} * & * \\ 0 & 0 \end{pmatrix} \subseteq \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \subseteq \begin{pmatrix} * & * \\ * & * \end{pmatrix}.$$

כרגיל, אין מניעה לכך ש- R או S יהיו חוגים (עם יחידה).

תרגיל 1.1.59 (*)** תהי Λ משפחה של תת-חוגים בלי יחידה של חוג בלי יחידה R . הראה שגם החיתוך $\bigcap_{S \in \Lambda} S$ הוא תת-חוג בלי יחידה.

המרכז והמרקז

הגדרה 1.1.60 יהי R חוג. **המרכז של R** הוא $Z(R) = \{z \in R : \forall x \in R : zx = xz\}$.

תרגיל 1.1.61 ()** הראה שהמרכז של חוג הוא תת-חוג שלו.

תרגיל 1.1.62 ()** הוכח שהמרכז של חוג R הוא תת-חוג מלא, כלומר, שאם $\alpha \in Z(R)$ הוא הפיך ב- R , אז הוא הפיך כבר ב- $Z(R)$. הדרכה: לכל $x \in R$, $\alpha^{-1} \in Z(R)$ ומכאן $\alpha^{-1}x - x\alpha^{-1} = \alpha^{-1}(x\alpha - \alpha x)\alpha^{-1} = 0$.

בדומה לזה אפשר להגדיר את המרקז:

הגדרה 1.1.63 תהי $A \subseteq R$ תת-קבוצה של חוג. **המרקז של A** הוא

$$C_R(A) = \{x \in R : \forall a \in A : ax = xa\}.$$

תרגיל 1.1.64 ()** הראה שהמרכז של כל תת-קבוצה הוא תת-חוג.

תרגיל 1.1.65 ()** 1. הראה שאם $A \subseteq A'$ אז $C_R(A') \subseteq C_R(A)$.

2. הראה שלכל קבוצה A , $A \subseteq C_R(C_R(A))$.

3. הסק ש- $C_R(C_R(C_R(A))) = C_R(A)$.

יוצרים של תת-חוג

יש שתי דרכים יעילות לתאר תת-חוג: דרך אחת היא על-ידי משוואות המגדירות את אבריו (למשל, תת-החוג של המטריצות המשולשיות עליונות, בתוך חוג המטריצות, מוגדר על-ידי האילוצים $a_{ij} = 0$ לכל $i > j$). דרך שניה, כמו בחבורות, היא על-ידי קבוצת יוצרים. יהיו $R_0 \subseteq R$ חוג ותת-חוג, ותהי X קבוצה שאבריה מתחלפים עם אברי R_0 .

הגדרה 1.1.66 תת-החוג הנוצר (מעל R_0) **על-ידי** X הוא חיתוך כל תת-החוגים $S \subseteq R$ המכילים את R_0 ואת X . מסמנים תת-חוג זה בסימון $R_0[X]$. אם $R_0[X] = R$, אומרים ש- R נוצר על-ידי X .

אם הקבוצה $X = \{a_1, \dots, a_k\}$ סופית, מסמנים $R_0[X] = R_0[a_1, \dots, a_k]$ במקרה זה אומרים ש- R נוצר סופית מעל R_0 .

תרגיל 1.1.67 (*) תת-החוג הנוצר על-ידי X הוא תת-החוג הקטן ביותר (ביחס להכלה) בין כל תת-החוגים המכילים את R_0 ואת X .

תרגיל 1.1.68 ()** נניח ש- R חוג קומוטטיבי (די בכך ש- $a \in Z(R)$). אז

$$R_0[a] = \{\alpha_0 + \dots + \alpha_n a^n : \alpha_0, \dots, \alpha_n \in R_0\}.$$

תרגיל 1.1.69 (*)** מצא קבוצת יוצרים של $\mathbb{Q}$ מעל $\mathbb{Z}$. הראה שאין קבוצת יוצרים סופית כזו. מצא קבוצת יוצרים מינימלית (כלומר, כזו שאין לה תת-קבוצה אמיתית היוצרת בעצמה).

1.1.3 חוגים לא אסוציאטיביים

החוגים שהגדרנו בסעיף הראשון, ושלמד בכל שאר הקורס, מקיימים את כוונה האסוציאטיביות של הכפל. אם מוותרים על האסוציאטיביות של הכפל התאוריה נעשית כללית מדי, ובדרך כלל אינה מעניינת. עם זאת החלפת האסוציאטיביות בהנחות אחרות מולידה כמה מערכות חשובות.

חוג לא אסוציאטיבי הוא מבנה אלגברי עם שתי פעולות, חיבור וכפל, המקיים את האקסיומות המגדירות חוג למעט אולי האסוציאטיביות של הכפל, וקיומו של אבר היחידה. למערכות כאלה יש חשיבות רבה בתחומים שונים של המתמטיקה. אי-אסוציאטיביות משמיטה מן התאוריה עובדות שאנו לוקחים כמובנות מאליהן: Ra אינו בהכרח אידיאל שמאלי, אבר הפיך מימין ומשמאל אינו בהכרח הפיך, סכום של אידיאלים נילפוטנטים אינו בהכרח נילפוטנטי, ועוד. החוגים שלנו ישארו אסוציאטיביים בכל הסעיפים האחרים של החוברת.

כדי להבדיל את פעולת הכפל בחוג לא אסוציאטיבי מן הכפל האסוציאטיבי, משתמשים לפעמים בסמונים אחרים, כגון $[a, b]$, $a \bullet b$, וכדומה.

הגדרה 1.1.70 בחוג לא אסוציאטיבי R , מגדירים $(a, b, c) = (ab)c - a(bc)$; **ביטוי זה הוא האסוציאטור של** a, b, c .

תרגיל 1.1.71 (*) חוג R הוא אסוציאטיבי אם הוא מקיים את הזהות $(a, b, c) = 0$.

הגדרה 1.1.72 המך כזו של חוג לא אסוציאטיבי A הוא אוסף האברים a המקיימים $(a, A, A) = (A, a, A) = (A, A, a) = [a, A] = 0$. (זהו תת-חוג של A).

חוגים אלטרנטיביים

הגדרה 1.1.73 חוג נקרא **אלטרנטיבי** אם הוא מקיים את הזהויות $(a, a, b) = (a, b, b) = 0$ (אפשר להכליל ולהגדיר חוג אלטרנטיבי שמאלי או ימני).

תרגיל 1.1.74 (*) כל חוג אסוציאטיבי הוא אלטרנטיבי.

תרגיל 1.1.75 (*) בחוג אלטרנטיבי, $(x_{\sigma 1}, x_{\sigma 2}, x_{\sigma 3}) = \text{sgn}(\sigma)(x_1, x_2, x_3)$ (מכאן שמן של האלגברות האלה).

חוג המטריצות מעל חוג לא אסוציאטיבי מוגדר באותה דרך שבה מגדירים מטריצות מעל חוג אסוציאטיבי (הגדרה 1.3.4).

תרגיל 1.1.76 ()** אם חוג המטריצות $M_2(A)$ הוא אלטרנטיבי משמאל, אז A מוכרח להיות חוג אסוציאטיבי.

תרגיל 1.1.77 (*)** (משפט ארטין) בחוג אלטרנטיבי, כל תת-חוג הנוצר על-ידי שני אברים הוא אסוציאטיבי.

חוגי לי

הגדרה 1.1.78 חוג לא אסוציאטיבי, שפעולת הכפל שלו $[a, b] \mapsto (a, b)$ מקיימת $[a, b] = -[b, a]$ ואת זהות יעקובי $0 = [[a, b], c] + [[b, c], a] + [[c, a], b]$, נקרא **חוג לי**.

תרגיל 1.1.79 ()** יהי R חוג אסוציאטיבי. החוג R^- מוגדר כקבוצה R עם אותה פעולת חיבור, ופעולת הכפל $[a, b] = ab - ba$. הראה ש- R^- הוא חוג לי (לפי משפט פואנקרה-בירקהוף-וויט, כל חוג לי שהוא מרחב וקטורי מעל שדה, מוכל בחוג מהצורה R^-).

תרגיל 1.1.80 ()** מצא זהות מהצורה $[[[a, b], [c, d]], e] + [[e, [a, b]], c] + [[e, [c, d]], a] = 0$ המתקיימת בכל חוג לי.

תרגיל 1.1.81 ()** בדוק את הזהות

$$[[[x_1, x_2], x_3], x_4] + [[[x_4, x_3], x_2], x_1] + [[[x_3, x_4], x_1], x_2] + [[[x_2, x_1], x_4], x_3] = 0.$$

תרגיל 1.1.82 ()** בדוק את הזהות

$$\sum_{i=0}^4 \sigma^i([[[[x_5, x_4], x_3], x_2] - [[[x_5, x_2], x_4], x_3] - [[[x_5, x_3], x_2], x_4], x_1]) = 0$$

כאשר σ פועל על המשתנים $x_1, \dots, x_5$ באופן ציקלי, $x_i \mapsto x_{i+1}$.

תרגיל 1.1.83 (*)** (Magnus, Karrass and Solitar, "Combinatorial Group Theory"; ex. 5.6.10) תהי X_1 קבוצה סדורה. הקבוצה X_2 מוגדרת כקבוצת הזוגות $[y, x]$ $(y, x \in X_1)$ עם יחס הסדר $[y, x] > [y', x']$ אם ורק אם $x > x'$ או $x = x'$ ו- $y > y'$. הסדר מורחב ל- $X_1 \cup X_2$ לפי הקביעה שכל אבר ב- X_2 גדול מכל אבר ב- X_1 . יהי $n \geq 3$. אברי הקבוצה X_n הם האברים מהצורה $[[u, v], w]$ כאשר $u \in X_i$, $v \in X_j$, $w \in X_k$, $i + j + k = n$, ו- $[u, v] > w \geq v$. הסדר על X_n מוגדר כמקודם $([u, v] > [u', v'])$ אם $v > v'$ או $v = v'$ ו- $u > u'$; ומומשך לכל $X_1 \cup \dots \cup X_n$ על-ידי הקביעה שכל אבר ב- X_n גדול מכל אבר בקבוצות הקודמות. הוכח שהסדר על $\bigcup X_n$ הוא לינארי.

(הקבוצה $\bigcup X_n$ היא בסיס ל"אלגברת לי החופשית הנוצרת על-ידי X_1 ", שלא נגדיר כאן. לפי נוסחת ויט, $|\bigcup X_n| = \frac{1}{n} \sum_{d|n} \mu(n/d) |X_1|^d$.)

חוגי ז'ורדן

הגדרה 1.1.84 חוג לא אסוציאטיבי שבו 2 הפיך, שפעולת הכפל שלו $a \bullet b \mapsto (a, b)$ מקיימת $a \bullet b = b \bullet a$ ואת זהות ז'ורדן $(a \bullet b) \bullet (a \bullet a) = a \bullet (b \bullet (a \bullet a))$, נקרא חוג ז'ורדן.

תרגיל 1.1.85 ()** יהי R חוג אסוציאטיבי שבו 2 הפיך. החוג R^+ מוגדר כקבוצה R עם אותה פעולת חיבור, ופעולת הכפל $a \bullet b = ab + ba$. הראה ש- R^+ הוא חוג ז'ורדן.

תרגיל 1.1.86 (*)** לכל חוג אלטרנטיבי R , R^+ הוא חוג ז'ורדן.

חוגים לא אסוציאטיביים עם חילוק

חוג לא אסוציאטיבי A (לאו דווקא עם יחידה) נקרא חוג עם חילוק אם הפעולות $\ell_a : x \mapsto ax$ ו- $r_a : x \mapsto xa$ הפיכות (כאופרטורים לינאריים $A \rightarrow A$) לכל $a \neq 0$.

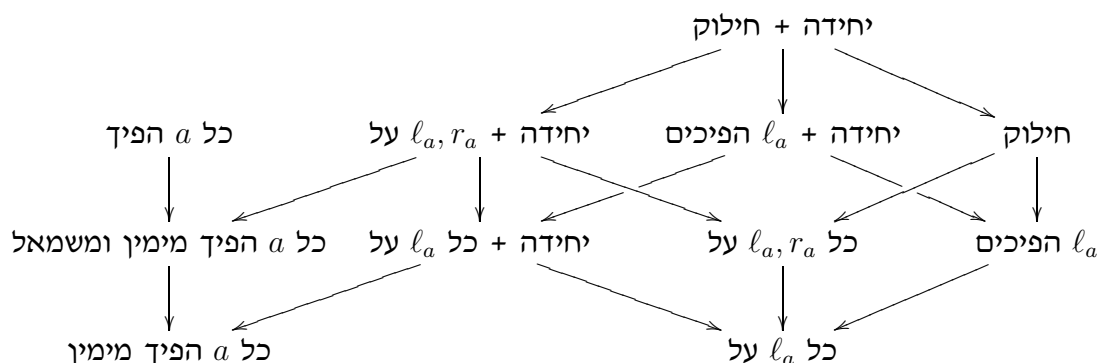
תרגיל 1.1.87 (*) יהי A חוג לא אסוציאטיבי. התכונות הבאות שקולות:

1. כל ℓ_a חד-חד-ערכי,

2. כל r_a חד-חד-ערכי,

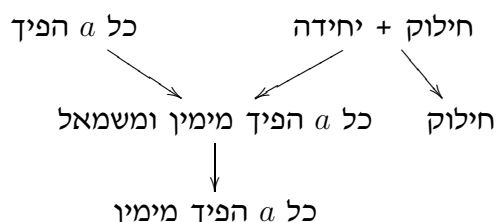
3. A הוא תחום (כלומר אין בו מחלקי אפס).

הדיאגרמה הבאה מציגה תכונות אפשריות של חוג לא אסוציאטיבי (כשנאמר "כל a " הכוונה לכל $a \neq 0$), עם הקשרים הלוגיים ביניהן. כל ההגדרות מתלכדות במקרה האסוציאטיבי אל ההגדרה של חוג עם חילוק (זה מוכח בתרגילים 1.1.22 ו-1.1.23). כמו במקרה האסוציאטיבי, אבר a הוא הפיך אם יש b כך ש- $ab = ba = 1$.



תרגיל 1.1.88 (**)** הוסף חצים נכונים לדיאגרמה, אם יש כאלו, ותן דוגמאות נגדיות המראות שאין גרירות אחרות.

תרגיל 1.1.89 ()** תהי D אלגברת חילוק מממד אינסופי מעל השדה F . נבחר העתקה לינארית חד-חד-ערכית $f: D \rightarrow D$ שאינה על. נגדיר $a * b = f(a)b$. אז $(D, *)$ אופרטורי הכפל משמאל הפיכים; אבל אופרטורי הכפל מימין אינם כאלה, ולכן $(D, *)$ אינה אלגברת חילוק (אפשר לבחור בנוסף $f(1) = 1$ כדי לשמור על אבר היחידה).



תרגיל 1.1.90 (*)** הראה שעבור אלגברות מממד סופי, אם כל ℓ_a על, אז A אלגברת חילוק. הסק שהדיאגרמה הקודמת מתכווצת לזו הנתונה לצד התרגיל הזה.

מדרגה. תרגיל 1.1.21.

תרגיל 1.1.91 (**)** האם בחוג עם חילוק (עם יחידה) כל אבר הוא הפיך? מה אם נוסיף את ההנחה שהממד מעל המרכז סופי?

תרגיל 1.1.92 ()** בחוג לא אסוציאטיבי עם חילוק: אם u יחידה משמאל, אין אידמפוטנט מלבד u .

תרגיל 1.1.93 (*)** תן דוגמאות לאלגברות לא אסוציאטיביות עם חילוק מממד 2, עם התכונות הבאות:

1. יש יחידה משמאל, אבל אין יחידה. הדרכה: $A = Fu + Fy$ כאשר $yu = \theta y, uy = y, u^2 = u$

2. יש אידמפוטנט יחיד, אבל אין יחידה מימין או משמאל. הדרגה: $B = Fe + Fy$ כאשר $y^2 = \theta e, ey = ye = \theta y, e^2 = e, \theta \notin F^2$

3. יש שני אידמפוטנטים בלתי תלויים. הדרכה. $C = Fe + Fe'$ כאשר $e'^2 = e'$, $e^2 = e$.
 $\theta \notin F^2$ כאשר $e'e = e + e'$, $ee' = (1 - \theta)e - \theta e'$.

4. אין אידמפוטנטים. הדרכה. $D = Fx + Fy$ כאשר $x^2 = -\theta x$, $xy = x + 2\theta y$, $yx = -2x + y$.
 $y^2 = -\theta x$ כאשר $\theta \notin F^2$ ו- $(\theta + 3)^2 - 8 \notin F^2$.

תרגיל 1.1.94 (*)** [דוגמא: ממד סופי, כל האברים הפיכים, לא אלגברת חילוק].
 יהי F שדה. על המרחב הוקטורי $A = F + Fx + Fy$ נגדיר כפל לפי $xy = 1$,
 $x^2 = y^2 = 0$, $yx = -1$. הראה שכל אבר של A הפיך מימין ומשמאל, אבל A
 אינה אלגברת חילוק. אם $\text{char} F = 2$, הראה שכל אברי A הפיכים, ו- A אינה
 אלגברת חילוק.

איזוטופיות

יהי A מרחב וקטורי מעל שדה F . שתי פעולות בילינאריות $m, m': A \times A \rightarrow A$ הן
איזוטופיות אם יש העתקות לינאריות הפיכות $f, g, h: A \rightarrow A$ כך ש- $h(m'(x, y)) =$
 $m(f(x), g(y))$ (זוהי בעצם "החלפת בסיס" משולשת, בשתי הכניסות והיציאה של
 פעולת הכפל).

תרגיל 1.1.95 (*) יחס האיזוטופיות הוא יחס שקילות על אוסף פעולות הכפל
 האפשריות על A .

תרגיל 1.1.96 (*) איזוטופיה שבה $f = g = h$ אינה אלא איזומורפיזם.

איזוטופיה כללית אינה שומרת על אסוציאטיביות, ולכן הערך שלה בתורת החוגים
 האסוציאטיבית מוגבל ביותר. עם זאת עבור אלגברות לא אסוציאטיביות יש לה תפקיד
 מעניין: היא יכולה לייצר אברי יחידה.

תרגיל 1.1.97 (-)** תהי $(A, \cdot)$ אלגברה לא אסוציאטיבית עם אבר u כך ש-
 $\ell_u: x \mapsto ux$ הפיך. הראה שהפעולה $\#$ המוגדרת לפי $u(x \# y) = xy$ מגדירה
 אלגברה איזוטופית, שבה u יחידה משמאל. הדרכה. $u \# y = \ell_u^{-1}(uy) = \ell_u^{-1}\ell_u(y) = y$.

תרגיל 1.1.98 ()** ("הטריק של קפלנסקי") האלגברה A איזוטופית לאלגברה
 עם יחידה אם ורק אם יש בה אברים u, v כך ש- ℓ_u, r_v הפיכים. אכן, אם $u, v \in A$
 ו- ℓ_u, r_v הפיכים, אז uv הוא אבר יחידה עבור הפעולה $x * y = r_v^{-1}(x)\ell_u^{-1}(y)$.
 הדרכה. באלגברה עם יחידה אפשר לבחור $u = v = 1$, והאיזוטופיה שומרת על הפיכות של אופרטורי הכפל.
 בכיוון ההפוך, אם A נתונה אז $y = \ell_u\ell_u^{-1}(y) = u\ell_u^{-1}(y) = \ell_u\ell_u^{-1}(y) = y$ נתונה שני
 $x * (uv) = (uv) * y = r_v^{-1}(uv)\ell_u^{-1}(y) = u\ell_u^{-1}(y) = \ell_u\ell_u^{-1}(y) = y$ ומצד שני
 $r_v^{-1}(x)\ell_u^{-1}(uv) = r_v^{-1}(x)v = r_v r_v^{-1}(x) = x$.

1.2 אידיאלים וחוגי מנה

בסעיף זה נציג את האובייקטים המשחקים תפקיד מרכזי במבנה הפנימי של חוג:
 אידיאלים חד-צדדיים ודו-צדדיים, הומומורפיזמים וחוגי מנה.

1.2.1 אידיאלים חד-צדדיים ודו-צדדיים

כדי להבין חוגים טוב יותר, עלינו ללמוד תת-קבוצות שהמבנה שלהן קשור לזה של החוג כולו. כל הקבוצות שנלמד הן תת-חבורות של החבורה החיבורית.

הגדרה 1.2.1 יהי R חוג. תת-חבורה חיבורית $L \subseteq R$ נקראת **אידיאל שמאלי** אם לכל $a \in L$ ו- $x \in R$ מתקיים $xa \in L$; במקרה זה מסמנים $L \leq_\ell R$. בדומה לזה L **אידיאל ימני** אם $ax \in L$ לכל $a \in L$ ו- $x \in R$; מסמנים $L \leq_r R$. אם I אידיאל שמאלי וימני, הוא נקרא **אידיאל דו-צדדי** (או **סתם אידיאל**), ואז מסמנים $I \triangleleft R$.

תרגיל 1.2.2 (*) הקבוצה $\{0\}$ היא אידיאל של R ; זהו האידיאל הטריוויאלי.

תרגיל 1.2.3 (*) החוג כולו הוא אידיאל, הנקרא **אידיאל לא אמיתי**; ראו תת-הסעיף "אידיאלים אמיתיים" בהמשך. לפעמים המונח אידיאל מתייחס לאידיאל אמיתי דווקא (כלומר, כל אידיאל המוכל ממש בחוג).

האידיאלים הדו-צדדיים אנלוגיים לתת-החבורות הנורמליות של חבורה. בחוג קומוטטיבי המושגים אידיאל ימני, שמאלי או דו-צדדי מתלכדים.

תרגיל 1.2.4 ()** לכל $a \in R$, הקבוצה $Ra = \{xa : x \in R\}$ היא אידיאל שמאלי של R .

תרגיל 1.2.5 ()** אם $L \leq R$ אידיאל שמאלי, אז לכל $a \in R$, גם La אידיאל שמאלי.

תרגיל 1.2.6 (*)** אידיאל הוא תת-קבוצה של R הסגורה לחיבור ולחיסור, וסופגת כפל. הראה שההנחה על סגירות לחיסור אינה נחוצה. האם תכונה זו נכונה גם כאשר R חוג בלי יחידה?

תרגיל 1.2.7 (*) נניח ש- $I \triangleleft R$ אידיאל, ו- $S \subseteq R$ תת-חוג המכיל את I . אז $I \triangleleft S$.

תרגיל 1.2.8 ()** נניח ש- $I \triangleleft R$ אידיאל, ו- $S \subseteq R$ תת-חוג. אז $I \cap S$ אידיאל של S .

הגדרה 1.2.9 אידיאל שמאלי מהצורה Ra נקרא **אידיאל (שמאלי) ראשי**.

איחוד וחיתוך

תרגיל 1.2.10 ()** תהי Λ משפחה של אידיאלים שמאליים (ימניים, דו-צדדיים) של חוג R . הוכח שהחיתוך $\bigcap_{L \in \Lambda} L$ הוא אידיאל שמאלי (ימני, דו-צדדי). הערה: השווה לתרגיל 1.1.59.

תרגיל 1.2.11 (*) בפרט, אם $L_1, L_2 \leq_\ell R$ אז $L_1 \cap L_2 \leq_\ell R$, וכך לכל חיתוך סופי.

תרגיל 1.2.12 (*)** נתבונן בחוג המטריצות $M_2(\mathbb{Q})$. אז $\left\{ \begin{pmatrix} * & 0 \\ * & 0 \end{pmatrix} \right\}$ הוא אידיאל שמאלי, ו- $\left\{ \begin{pmatrix} * & * \\ 0 & 0 \end{pmatrix} \right\}$ אידיאל ימני. החיתוך שלהם אינו אידיאל.

תרגיל 1.2.13 ()** יהי $I \triangleleft R$ אידיאל בחוג. הראה ש- $M_2(R)$ $\triangleleft \begin{pmatrix} R & R \\ I & R \end{pmatrix}$.

תרגיל 1.2.14 ()** יהיו $I, I' \triangleleft R$ אידיאלים. הראה ש- $I \cup I'$ אידיאל אם ורק אם $I' \subseteq I$ או $I \subseteq I'$.

תרגיל 1.2.15 ()** הוכח שהאיחוד $\bigcup_{\lambda} I_{\lambda}$ של שרשרת אידיאלים בחוג R (לאו דווקא בת מניה) הוא אידיאל. (השווה לתרגיל 1.3.71, עמ' 41).
בפרט, אם $I_1 \subseteq I_2 \subseteq \dots$ אידיאלים, אז האיחוד $\bigcup I_n$ הוא אידיאל.

קבוצת יוצרים

את האידיאל הקטן ביותר המכיל קבוצה $X \subseteq R$ מסמנים בסימון $\langle X \rangle$ (השווה להגדרה 1.1.66). אידיאל זה הוא החיתוך של כל האידיאלים המכילים את X .

תרגיל 1.2.16 (*)** יהי $a \in R$. הראה ש- $\langle a \rangle = \{\sum_{i=1}^n x_i a x'_i : x_i, x'_i \in R\}$ כאשר הסכומים כולם סופיים אבל n אינו מוגבל.

אידיאל שיש לו קבוצת יוצרים סופית הוא אידיאל נוצר סופית.

אידיאלים אמיתיים

הגדרה 1.2.17 אידיאל (שמאלי, ימני או דו-צדדי) של R נקרא **אמיתי** אם הוא מוכל ממש ב- R .

תרגיל 1.2.18 ()** אידיאל שמאלי אמיתי אינו מכיל אף אבר הפיך משמאל.

תרגיל 1.2.19 ()** אידיאל (חד- או דו-צדדי) I הוא אמיתי אם ורק אם $1 \notin I$.

תרגיל 1.2.20 ()** Ra הוא אידיאל שמאלי אמיתי אם ורק אם a אינו הפיך משמאל.

תרגיל 1.2.21 ()** נניח ש- R קומוטטיבי, ויהי $a \in R$. אז $Ra = \langle a \rangle$ הוא אידיאל אמיתי אם ורק אם a לא הפיך.

תרגיל 1.2.22 ()** בהמשך לתרגיל 1.2.15, הראה שאם כל האידיאלים I_{λ} אמיתיים (ובחוג יש אבר יחידה), אז גם $\bigcup I_{\lambda}$ אמיתי. הדרכה: תרגיל 1.2.19.

תרגיל 1.2.23 (*)** יהי A_0 חוג בלי יחידה. אם יש a כך ש- $A_0 a = a A_0 = A_0$, אז A_0 חוג עם יחידה.

הדרכה: לפי ההנחה יש $e \in A_0$ כך ש- $ae = a$. יהי $c \in A_0$. לפי ההנחה קיים x כך ש- $xa = c$; אבל אז $ce = xae = xa = c$, והראינו ש- e יחידה מימין. באותו אופן יש e' כך ש- $e'a = a$, ומכיוון שאפשר לכתוב כל c בצורה $c = ay$, $c' = ay = c'e' = e'c = e'a = a$. לפי תרגיל 1.1.7, $e' = e$ הוא אבר היחידה של A_0 .

תרגיל 1.2.24 (*)** יהי A_0 תחום בלי יחידה. אם יש $a \in A_0$ כך ש- $aA_0 = A_0$, אז A_0 תחום עם יחידה.

הדרכה: לפי ההנחה יש $e \in A_0$ כך ש- $ae = a$. אבל אז $ae^2 = ae$, ולכן $0 = (e^2 - e)a$. מכיוון ש- A_0 תחום, $e^2 = e$. לפי תרגיל 1.1.37 (עמ' 14), אידמפוטנט בתחום הוא אבר יחידה.

תרגיל 1.2.25 ()** התכונות הבאות שקולות עבור חוג בלי יחידה לא טריוויאלי:

1. ℓ_a הוא על לכל $a \neq 0$.

2. אין בחוג אידיאלים ימניים אמיתיים.

3. אין בחוג אידיאלים שמאליים אמיתיים.

4. זהו חוג עם חילוק, עם יחידה.

הדרכה. נסמן את החוג ב- A_0 . (1) $\Leftrightarrow$ (2): נניח ש- $A_0 \leq_r C$, $0 \neq a \in C$ אז $A = aA_0 \subseteq C$ ולכן $C = A_0$. (1) $\Leftrightarrow$ (2): נסמן $I = \{x \in A_0 : xA_0 = 0\}$ אז $I \leq_r A_0$, ולפי ההנחה יש שתי אפשרויות: אם $I = A_0$ אז $I A_0 = 0$ בסתירה להנחה ש- A_0 אינו טריוויאלי. מכיוון שאין בחוג אידיאלים ימניים לא טריוויאליים, בהכרח $I = 0$. לכן, לכל $a \neq 0$, $aA_0 \neq 0$, אבל זהו אידיאל ימני, ומכאן ש- $A_0 = aA_0 = \text{Im}(\ell_a)$. (1) $\Leftrightarrow$ (4): תרגיל 1.1.23 (עמ' 12). (3) $\Leftrightarrow$ (4): תנאי (4) סימטרי להחלפת ימין-שמאל, ולכן הגרירה נובעת מ-(2) $\Leftrightarrow$ (4) שכבר הוכחנו.

1.2.2 סכום ומכפלה של אידיאלים

סכומים סופיים וכלליים

יהי R חוג. הסכום של תת-קבוצות $A, B \subseteq R$ הוא

$$A + B = \{a + b : a \in A, b \in B\};$$

בדומה לזה מגדירים

$$-A = \{-a : a \in A\},$$

$$A - B = A + (-B)$$

תרגיל 1.2.26 (*) $A \subseteq R$ הוא תת-חבורה חיבורית אם ורק אם $A + A = -A = A$

תרגיל 1.2.27 (**) יהיו $L_1, L_2 \subseteq R$ אידיאלים שמאליים (ימניים, דו-צדדיים). אז $L_1 + L_2$ הוא אידיאל שמאלי (ימני, דו-צדדי).

תרגיל 1.2.28 (**) חיבור קבוצות בחוג הוא אסוציאטיבי וקומוטטיבי: $(A + B) + C = A + (B + C)$ ו- $A + B = B + A$

הגדרה 1.2.29 תהי Λ משפחה של אידיאלים שמאליים של R . אז הסכום $\sum_{L \in \Lambda} L$ מוגדר כאוסף הסכומים הסופיים $x_1 + \dots + x_n$ עבור $x_i \in L_i \in \Lambda$.

באלגברה כל הסכומים סופיים. כדי שנוכל לחבר אינסוף קבוצות, יש להניח שכמעט כולן כוללות את אפס כאבר.

תרגיל 1.2.30 (**) הסכום של משפחת אידיאלים הוא איחוד כל הסכומים הסופיים.

תרגיל 1.2.31 (**) אם כל $L \in \Lambda$ הוא אידיאל שמאלי (ימני, דו-צדדי), אז גם $\sum_{L \in \Lambda} L$ הוא אידיאל שמאלי (ימני, דו-צדדי).

דוגמא 1.2.32 סכום של תת-חוגים אינו בהכרח תת-חוג. למשל, סכום של תת-החוגים $S_1 = \begin{pmatrix} * & * & 0 \\ * & * & 0 \\ 0 & 0 & * \end{pmatrix}$ ו- $S_2 = \begin{pmatrix} * & 0 & 0 \\ 0 & * & * \\ 0 & * & * \end{pmatrix}$ של $M_3(\mathbb{Q})$ הוא $\begin{pmatrix} * & * & 0 \\ * & * & * \\ 0 & * & * \end{pmatrix}$, שאינו סגור לכפל.

מכפלה

בתורת החבורות המכפלה של שתי תת־קבוצות שווה לקבוצת המכפלות. בתורת החוגים ההגדרה אחרת: המכפלה שווה לאוסף הסכומים הסופיים של מכפלות, משום שרק כך אפשר להבטיח שהמכפלה סגורה לחיבור.

הגדרה 1.2.33 המכפלה של קבוצות $A, B \subseteq R$ מוגדרת כאוסף של סכומים סופיים,

$$A \cdot B = \{a_1 b_1 + \cdots + a_n b_n : a_i \in A, b_i \in B\}.$$

תרגיל 1.2.34 (*)** תן דוגמא לאידיאלים $I, J \triangleleft R$ בחוג (קומוטטיבי) R , כך שאוסף המכפלות $\{xy : x \in I, y \in J\}$ אינו סגור לחיבור.

תרגיל 1.2.35 ()** כפל קבוצות בחוג הוא פעולה אסוציאטיבית: לכל $A, B, C \subseteq R$ מתקיים $(AB)C = A(BC)$. הכפל גם דיסטריבוטיבי ביחס לחיבור: $(A+B)C = AC + BC$ ו- $A(B+C) = AB + AC$.

תרגיל 1.2.36 ()** תת־חבורה חיבורית $L \subseteq R$ היא:

1. תת־חוג אם ורק אם $LL \subseteq L$;
2. אידיאל שמאלי אם ורק אם $RL \subseteq L$;
3. אידיאל ימני אם ורק אם $LR \subseteq L$;
4. אידיאל אם ורק אם $RL + LR \subseteq L$.

תרגיל 1.2.37 ()** יהיו $a, b \in R$ אברים בחוג קומוטטיבי R . אז $Ra \cdot Rb = Rab$ במובן זה כפל של אידיאלים ראשיים מכליל את הכפל של אברים בחוג.

תרגיל 1.2.38 (+)** אם $IJ = K$ אידיאלים של חוג קומוטטיבי ו- I, K ראשיים, אז גם J ראשי.

תרגיל 1.2.39 ()** אם $L \leq_\ell R$ אז $LB \leq_\ell R$ לכל $B \neq \emptyset$.

המכפלה מאפשרת ליצור מאידיאל שמאלי ואידיאל ימני אידיאל דו־צדדי:

תרגיל 1.2.40 ()** הראה שאם $L \leq_\ell R$ אידיאל שמאלי ו- $T \leq_r R$ אידיאל ימני, אז $LT \triangleleft R$.

ובפרט:

תרגיל 1.2.41 ()** הראה שהמכפלה IJ של שני אידיאלים $I, J \triangleleft R$ היא אידיאל של R .

תרגיל 1.2.42 ()** לכל שני אידיאלים $I, J \triangleleft R$, $IJ \subseteq I \cap J$.

תרגיל 1.2.43 ()** אם R חוג קומוטטיבי ו- S_1, S_2 תת-חוגים, אז $S_1 S_2$ הוא תת-חוג.

תרגיל 1.2.44 (*)** תן דוגמא לחוג (לא קומוטטיבי) R עם שני תת-חוגים S_1, S_2 כך שהמכפלה $S_1 S_2$ אינה תת-חוג. **הצעה.** קח $S_1 = F + yR$ ו- $S_2 = F + Rx$ כאשר F שדה ו- $R = F\langle x, y \rangle$ היא האלגברה החופשית מעליו (הגדרה 1.2.106). נסה למצוא דוגמא שבה $R = M_n(F)$.

תרגיל 1.2.45 ()** יהי R חוג עם מרכז $Z = Z(R)$, ויהי $S \subseteq R$ תת-חוג. הראה ש- ZS הוא תת-חוג של R . (עובדה זו מוליכה להגדרה 2.4.6)

תרגיל 1.2.46 ()** יהי $L \leq_\ell R$ אידיאל שמאלי; אז לכל קבוצה A, LA הוא אידיאל שמאלי. בפרט, כל קבוצה מהצורה Lx היא אידיאל שמאלי.

טענה 1.2.47 יהי I אידיאל של R . אם A הוא תת-חוג, אידיאל שמאלי או אידיאל, אז $A + I$ הוא תת-חוג, אידיאל שמאלי או אידיאל, בהתאמה.

בפרט:

תרגיל 1.2.48 (*)** יהיו $I \triangleleft R$ ו- $S \subseteq R$ אידיאל ותת-חוג. אז $I + S$ הוא תת-חוג של R .

סריג האידיאלים

הגדרה 1.2.49 קבוצה $\mathcal{F}$ עם יחס סדר חלקי נקראת **סריג** אם לכל שני אברים $x, y \in \mathcal{F}$ יש מינימום לקבוצת האברים הגדולים מ- x, y , ומקסימום לקבוצת האברים הגדולים מ- x, y .

יהי $\mathcal{F}$ סריג. את האבר המינימלי הגדול מ- x, y מסמנים $x \vee y$, ואת המקסימלי בקבוצת האברים הקטנים מהם מסמנים $x \wedge y$.

תרגיל 1.2.50 ()** הפעולות הבינאריות $\vee, \wedge$ מקיימות את התכונות הבאות:

$$1. \text{קומוטטיביות: } x \wedge y = y \wedge x, x \vee y = y \vee x.$$

$$2. \text{אסוציאטיביות: } (x \wedge y) \wedge z = x \wedge (y \wedge z), (x \vee y) \vee z = x \vee (y \vee z).$$

$$3. \text{ספיגה: } x \vee (x \wedge y) = x, x \wedge (x \vee y) = x.$$

$$4. \text{אידמפוטנטיות: } x \wedge x = x, x \vee x = x.$$

תרגיל 1.2.51 (-)** תכונת האידמפוטנטיות נובעת מתכונת הספיגה. הדרכה: חשב את $x \vee (x \wedge (x \vee x))$.

תרגיל 1.2.52 (*)** תהי $\mathcal{F}$ קבוצה המצוידת בפעולות בינאריות המקיימות את האקסיומות שבתרגיל 1.2.50, אז $x \leq y$ אם ורק אם $x \wedge y = x$ (אם ורק אם $x \vee y = y$) מגדיר יחס סדר חלש על $\mathcal{F}$, ועבורו $x \vee y$ הוא האבר המינימלי בין כל האברים הגדולים מ- x, y , ו- $x \wedge y$ האבר המקסימלי בין הקטנים מ- x, y .

תרגיל 1.2.53 ()** אוסף תת-הקבוצות של קבוצה X , המסודר לפי הכלה, הוא סריג.

אוסף האידיאלים של חוג סדור ביחס להכלה.

משפט 1.2.54 אוסף האידיאלים של חוג, עם יחס ההכלה, הוא סריג, שבו $I \vee J = I + J$ ו- $I \wedge J = I \cap J$.

הוכחה. האידיאל הקטן ביותר המכיל את I, J הוא $I + J$, והאידיאל הגדול ביותר המוכל בשניהם הוא $I \cap J$. $\square$

מאפסים

הגדרה 1.2.55 אם $B \subseteq R$ תת-קבוצה כלשהי, המאפס השמאלי של B הוא $\text{ann}_l(B) = \{x \in R : xB = 0\}$. המאפס הימני הוא $\text{ann}_r(B) = \{x \in R : Bx = 0\}$. אם R קומוטטיבי שני המושגים מתלכדים כמובן, ואפשר לכתוב $\text{ann}(B)$.

(נחזור לנושא זה בהגדרה 5.1.60).

תרגיל 1.2.56 ()** לכל תת-קבוצה B , המאפס השמאלי $\text{ann}_l(B)$ הוא אידיאל שמאלי של R ; המאפס הימני $\text{ann}_r(B)$ הוא אידיאל ימני.

תרגיל 1.2.57 ()** כל מאפס שמאלי שווה למאפס השמאלי של אידיאל ימני כלשהו.

תרגיל 1.2.58 ()** מאפס שמאלי של אידיאל שמאלי הוא אידיאל דו-צדדי: אם $I \leq_l R$ אידיאל שמאלי, אז $\text{ann}_l(I) \triangleleft R$.

תרגיל 1.2.59 (*)** 1. הראה שאם $I \subseteq J$ אז $\text{ann}_l(J) \subseteq \text{ann}_l(I)$.

2. הראה ש- $I \subseteq \text{ann}_r(\text{ann}_l(I))$.

3. הראה שלכל קבוצה $B \subseteq R$, $\text{ann}_l(\text{ann}_r(\text{ann}_l(B))) = \text{ann}_l(B)$.

תרגיל 1.2.60 ()** $\text{ann}_l(I + J) = \text{ann}_l(I) \cap \text{ann}_l(J)$.

תרגיל 1.2.61 (*)** יהי R חוג קומוטטיבי. לכל שני אידיאלים $I, A \triangleleft R$, נסמן

$$(A : I) = \{x \in R : Ix \subseteq A\}.$$

יהיו $I, J, A, B, C \triangleleft R$.

1. $(A : I)$ הוא אידיאל. זהו האידיאל הגדול ביותר המקיים $(A : I)I \subseteq A$.
בפרט $A \subseteq (A : I)$.

2. $(0 : I) = \text{ann}_r(I)$.

3. מונוטוניות: אם $I \subseteq J$ אז $(A : J) \subseteq (A : I)$ ו- $(I : A) \subseteq (J : A)$.

4. הפעולות $m_I(A) = IA$ ו- $d_I(A) = (A : I)$ מקיימות $m_I d_I m_I = m_I$ ו- $d_I m_I d_I = d_I$.

$$5. (B : C)(A : B) \subseteq (A : C).$$

$$6. A(B : I) \subseteq (AB : I).$$

$$7. ((A : B) : C) = (A : BC).$$

$$8. I \subseteq (A : (A : I)).$$

$$9. (A : I) \subseteq (AB : IB).$$

$$10. (A : I + J) = (A : I) \cap (A : J).$$

תרגיל 1.2.62 ()** יהי $L \leq_\ell R$ אידיאל שמאלי.

הראה שהמאדל $L^* = \{x \in R : Lx \subseteq L\}$ הוא תת-החוג הגדול ביותר של R שבו L הוא אידיאל דו-צדדי.

תרגיל 1.2.63 ()** לכל אידיאל שמאלי $L \leq_\ell R$ ואבר $b \in R$, נסמן $Lb^{-1} = \{x : xb \in L\}$ (איננו מגדירים כאן את b^{-1}).

1. הראה ש- Lb^{-1} ו- Lb הם אידיאלים שמאליים.

2. נניח ש- $Lb \subseteq L$ (כלומר $b \in L^*$, ראה תרגיל 1.2.62). אז $Lb^{-1}b = L \cap Rb$ ו- $Lbb^{-1} = L + 0b^{-1}$.

$$Lbb^{-1}b = Lb \subseteq Lb^{-1}b \subseteq L \subseteq Lbb^{-1} \subseteq Lb^{-1} = Lb^{-1}bb^{-1},$$

ואלו כל האידיאלים שאפשר לקבל מ- L על-ידי הפעלת האופרטורים $L \mapsto Lb$ ו- $L \mapsto Lb^{-1}$ לסירוגין.

1.2.3 חוגי מנה

יהי R חוג. לכל תת-חבורה I של החבורה החיבורית, חבורת המנה R/I הכוללת את כל הקוסטים $a + I = \{a + x : x \in I\}$ היא אכן חבורה. השאלה היא מתי פעולת הכפל של נציגים מוגדרת היטב, ומתי אוסף הקוסטים הוא חוג.

תרגיל 1.2.64 ()** פעולת הכפל $(a + I)(b + I) = ab + I$ מוגדרת היטב (כלומר, בלתי תלויה בנציגים), אם ורק אם $I \triangleleft R$.

תרגיל 1.2.65 ()** נניח ש- $I \triangleleft R$. אז R/I עם הפעולות לפי נציגים הוא חוג, שבו אבר היחידה הוא $1 + I$.

1.2.4 הומומורפיזמים

הומומורפיזם הוא פונקציה בין מבנים, השומרת על הפעולות (ועל היחסים והקבועים, כשיש כאלה).

הגדרה 1.2.66 יהיו R, S חוגים. הומומורפיזם של חוגים הוא פונקציה $\varphi: R \rightarrow S$ השומרת על החיבור והכפל, כלומר, מקיימת $\varphi(x+y) = \varphi(x) + \varphi(y)$ ו- $\varphi(xy) = \varphi(x)\varphi(y)$, ומקיימת בנוסף את התנאי $\varphi(1_R) = 1_S$. (ראו הכללה בהגדרה 1.2.69).

יש סוגי הומומורפיזם שקיבלו שמות מיוחדים:

הגדרה 1.2.67 הומומורפיזם $R \rightarrow S$ נקרא אפימורפיזם או הטלה אם הוא על; מונומורפיזם או שיכון אם הוא חד-חד-ערכי; איזומורפיזם אם הוא חד-חד-ערכי ועל.

הגדרה 1.2.68 הומומורפיזם מחוג לעצמו, $R \rightarrow R$, נקרא אנדומורפיזם; ואם הוא חד-חד-ערכי ועל, אוטומורפיזם.

כל המונחים האלה מקובלים גם בתורת החבורות.

הומומורפיזמים של חוגים בלי יחידה

הגדרה 1.2.69 יהיו R, S חוגים בלי יחידה. פונקציה $\varphi: R \rightarrow S$ המקיימת $\varphi(x+y) = \varphi(x) + \varphi(y)$ ו- $\varphi(xy) = \varphi(x)\varphi(y)$ נקראת הומומורפיזם של חוגים בלי יחידה.

כלומר, הומומורפיזם של חוגים בלי יחידה אינו נדרש לקיים את התנאי $\varphi(1_R) = 1_S$.
אכן, אם R או S הם חוגים בלי יחידה, אין מנוס מלדבר על הומומורפיזמים כאלה.

תרגיל 1.2.70 ()** יהיו R, S חוגים. הפונקציה $R \rightarrow S$ המוגדרת לפי $\varphi(x) = 0$ לכל $x \in R$ היא הומומורפיזם של חוגים בלי יחידה, אבל אינה הומומורפיזם.

לפעמים הומומורפיזם של חוגים בלי יחידה מוכרח בכל זאת להיות הומומורפיזם של חוגים:

תרגיל 1.2.71 ()** אם R חוג (עם יחידה) ו- $\varphi: R \rightarrow S$ אפימורפיזם של חוגים בלי יחידה, אז S חוג עם יחידה ו- φ הוא אפימורפיזם של חוגים.

תרגיל 1.2.72 (-)** אם R חוג עם יחידה ו- $\varphi: R \rightarrow S$ הומומורפיזם, $\varphi \neq 0$, ובנוסף S תחום (הגדרה 1.1.34), אז S חוג עם יחידה ו- $\varphi(1_R) = 1_S$. (הדרכה. הראה ש- $\varphi(1_R)^2 x = \varphi(1_R)x$ לכל $x \in S$).

תרגיל 1.2.73 ()** מצא את כל ההומומורפיזמים של חוגים בלי יחידה $\mathbb{Z} \rightarrow \mathbb{Z}$, ואת כל אלה מביניהם שהם הומומורפיזמים של חוגים.

הגרעין והתמונה

לכל הומומורפיזם מתלווים שני מבנים מוכרים:

הגדרה 1.2.74 יהי $\varphi: R \rightarrow S$ הומומורפיזם של חוגים (עם יחידה או בלעדיה). התמונה של φ היא $\text{Im}(\varphi) = \{\varphi(x) : x \in R\}$. הגרעין של φ הוא $\text{Ker}(\varphi) = \{x \in R : \varphi(x) = 0\}$.

תרגיל 1.2.75 ()** התמונה של הומומורפיזם $R \rightarrow S$ היא תת-חוג של S , והגרעין הוא אידיאל של R .

לכן כל הומומורפיזם הוא על התמונה של עצמו. לכל מונומורפיזם $\varphi: R \rightarrow S$, $\text{Im}(\varphi)$ היא איזומורפיזם בין R לבין התמונה $\text{Im}(\varphi)$, שהיא תת-חוג של S . לכן אפשר לראות ב- R תת-חוג של S , וזו הסיבה לכך שמונומורפיזם נקרא גם **שיכון**. לפעמים מסמנים שיכון $R \rightarrow S$ בסימן $R \hookrightarrow S$.

תרגיל 1.2.76 (-)** $\varphi: R \rightarrow S$ הוא חד-חד-ערכי אם ורק אם $\text{Ker}(\varphi) = 0$.

לפי תרגיל 1.2.75 כל גרעין הוא אידיאל; גם ההיפך נכון - כל אידיאל הוא גרעין של הומומורפיזם:

תרגיל 1.2.77 (+)** יהי $I \triangleleft R$ אידיאל. הראה שהפונקציה $\theta: R \rightarrow R/I$ המוגדרת לפי $\theta(a) = a + I$ היא אפימורפיזם. אפימורפיזם זה נקרא **ההטלה הקנונית** ביחס ל- I .

תרגיל 1.2.78 ()** יהי R חוג-בלי-יחידה. הגדר $R^1 = \mathbb{Z} \times R$ עם החיבור לפי רכיבים והכפל $(n, x)(m, y) = (nm, ny + mx + xy)$. הוכח ש- $\hat{R}$ חוג עם יחידה, וש- $(0, x) \mapsto x$ הוא שיכון של חוגים בלי יחידה $R \rightarrow R^1$. כלומר, כל חוג בלי יחידה אפשר לשכן בחוג עם יחידה.

תרגיל 1.2.79 (-)** בהמשך לתרגיל 1.2.78, תאר את האידיאלים של $\hat{R}$.

כהכללה של תרגיל 1.2.75, מתקיימת התכונה הבאה:

תרגיל 1.2.80 ()** יהי $\varphi: R \rightarrow S$ הומומורפיזם. לכל $I \triangleleft S$, המקור $\varphi^{-1}(I)$ הוא אידיאל של R .

תרגיל 1.2.81 ()** אם $\varphi: R \rightarrow S$ על, אז לכל אידיאל $I \triangleleft R$ גם $\varphi(I) \triangleleft S$.

ובכל זאת, באופן כללי תמונת אידיאל אינה בהכרח אידיאל:

תרגיל 1.2.82 (-)** תן דוגמא לכך שהתמונה של אידיאל אינה בהכרח אידיאל.

חוגים איזומורפיים

כמו בתורת החבורות (ובכל מבנה מתמטי אחר), איזומורפיזם הוא פונקציה חד-חד-ערכית ועל בין מבנים, השומרת על הפעולות (ועל היחסים והקבועים, כשיש כאלה).

הגדרה 1.2.83 יהיו R, R' חוגים. **איזומורפיזם של חוגים** הוא פונקציה חד-חד-ערכית ועל $\varphi: R \rightarrow R'$ השומרת על החיבור והכפל, כלומר, מקיימת $\varphi(x+y) = \varphi(x) + \varphi(y)$ ו- $\varphi(xy) = \varphi(x)\varphi(y)$, ומקיימת בנוסף את התנאי $\varphi(1_R) = 1_{R'}$.

(ראו הגדרה 1.2.66)

תרגיל 1.2.84 ()** יהי $\varphi: R \rightarrow R'$ איזומורפיזם של חוגים. הראה שהפונקציה ההפוכה $\varphi^{-1}: R' \rightarrow R$ גם היא איזומורפיזם.

חוגים שיש ביניהם איזומורפיזם הם **חוגים איזומורפיים**. האיזומורפיזם מאפשר לתרגם כל טענה אלמנטרית מחוג אחד לרעהו, ולכן כשהחוגים איזומורפיים חושבים עליהם כאילו הם למעשה אותו חוג. בבעיות תאורטיות מעוניינים במיון של חוגים **עד כדי איזומורפיזם**, ולא מעבר לכך, משום שלכל חוג אפשר להצמיד באופן מלאכותי מחלקה שלמה של חוגים איזומורפיים: $R \cong R \times \{\omega\}$ לכל אבר ω של הקבוצה האוניברסלית. כדי להראות שחוגים אינם איזומורפיים די להצביע על תכונה שבה הם שונים: חוג קומוטטיבי אינו יכול להיות איזומורפי לחוג לא קומוטטיבי, וכן הלאה. ההוכחה שחוגים מסויימים הם כן איזומורפיים עשויה לדרוש הכרה טובה של שני החוגים, וטכניקות מגוונות.

1.2.5 משפטי האיזומורפיזם

משפטי האיזומורפיזם של חוגים דומים לאלו של חבורות.

משפט 1.2.85 (משפט האיזומורפיזם הראשון) לכל הומומורפיזם של חוגים $\phi: R \rightarrow S$, חוג המנה $R/\text{Ker}(\phi)$ איזומורפי ל- $\text{Im}(\phi)$.

תרגיל 1.2.86 ()** יהי $I \triangleleft R$ אידיאל. הראה ש- $M_n(I)$ אידיאל של $M_n(R)$, וש- $M_n(R)/M_n(I) \cong M_n(R/I)$.

תרגיל 1.2.87 ()** הראה ש- $\mathbb{Z}_n \cong \mathbb{Z}/n\mathbb{Z}$.

תרגיל 1.2.88 (*)** נסמן $i = \sqrt{-1}$. הוכח: $\mathbb{Z}[i]/\langle 2+i \rangle \cong \mathbb{Z}[i]/\langle 2-i \rangle \cong \mathbb{Z}/5\mathbb{Z}$.

משפט 1.2.89 (משפט האיזומורפיזם השני) אם $I \triangleleft R$ אידיאל ו- $S \subseteq R$ תת-חוג, אז: $S+I$ תת-חוג של R (זהו תרגיל 1.2.48), I אידיאל שלו (תרגיל 1.2.7), $S \cap I$ אידיאל של S (תרגיל 1.2.8), ומתקיים

$$S/S \cap I \cong (S+I)/I.$$

תרגיל 1.2.90 ()** יהיו $\varphi: R \rightarrow S$ הומומורפיזם ו- $I \triangleleft S$. לפי תרגיל 1.2.80, $I' = \varphi^{-1}(I) \triangleleft R$. הראה ש- $R/I' \cong (\text{Im}(\varphi) + I)/I \subseteq S/I$.

תרגיל 1.2.91 ()** יהיו $\varphi: R \hookrightarrow R'$ שיכון ו- $I' \triangleleft R'$. אם $I = I' \cap R$ אז יש שיכון $R/I \hookrightarrow R'/I'$.

משפט 1.2.92 (משפט האיזומורפיזם השלישי) אם $I \subseteq J$ אידיאלים של R , אז J/I אידיאל של R/I , ו- $(R/I)/(J/I) \cong R/J$.

טענה 1.2.93 כל הומומורפיזם הוא הרכבה של שיכון, איזומורפיזם, והטלה.

הוכחה. יהי $\varphi: R \rightarrow S$ הומומורפיזם. נסמן $K = \text{Ker}(\varphi)$, ואז $R \rightarrow R/K$ הטלה ו- $R/K \cong \text{Im}(\varphi) \hookrightarrow S$ שיכון, וההרכבה $R \rightarrow R/K \cong \text{Im}(\varphi) \hookrightarrow S$ שווה ל- φ . $\square$

תרגיל 1.2.94 ()** יהיו R חוג ו- $I \triangleleft R$ אידיאל שלו. אז לכל אידיאל $A \triangleleft R$, $I \subseteq A/I \triangleleft R/I$; ולהיפך, כל אידיאל $\alpha \triangleleft R/I$ הוא מהצורה $\alpha = A/I$ עבור $A \triangleleft R$. מתאים $(A = \bigcup_{x \in \alpha} x)$.

תרגיל 1.2.94 מאפשר לסכם את משפטי האיזומורפיזם במשפט מרכזי על אידיאלים:

משפט 1.2.95 (משפט ההתאמה) יהי I אידיאל של חוג R . ההתאמה $A \mapsto A/I$ היא איזומורפיזם של סריגים מאוסף R שמכילים את I , אל אוסף האידיאלים של R/I . ההתאמה שומרת הכלה, חיבור, כפל וחיתוך, ומנות.

תת-החוג היסודי

תרגיל 1.2.96 ()** לכל חוג R קיים הומומורפיזם יחיד $\mathbb{Z} \rightarrow R$.

התמונה של $\mathbb{Z}$ ב- R היא תת-חוג, הנקרא **תת-החוג היסודי** של R . (תת-החוג היסודי נקרא בדרך כלל "תת-החוג הראשוני", אלא שהקשר בינו לבין חוג ראשוני שיוגדר בהמשך רופף למדי, והעדפנו לשנות את הטרמינולוגיה המקובלת.)

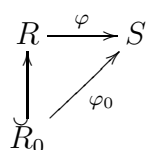
תרגיל 1.2.97 ()** לפי משפט 1.3.2 לגרעין של $\mathbb{Z} \rightarrow R$ יש הצורה $n\mathbb{Z}$, לאיזשהו n טבעי. הראה ש- n הוא המאפיין של R .

תרגיל 1.2.98 ()** יהי R חוג שהמאפיין שלו n . הראה ש- $\mathbb{Z}_n$ (איזומורפי ל) תת-חוג של R . תת-חוג זה נקרא **תת-החוג היסודי** של R .

אם R נוצר סופית מעל תת-החוג היסודי שלו (הגדרה 1.1.66), אומרים שהוא **נוצר סופית**.

הומומורפיזם ויוצרים

תרגיל 1.2.99 (*) יהיו R, S חוגים, $R_0 \subseteq R$ תת-חוג, ו- $\varphi: R \rightarrow S$ הומומורפיזם. הצמצום $\varphi_0: R_0 \rightarrow S$ של φ מ- R_0 ל- R , המוגדר לפי $\varphi_0(c) = \varphi(c)$ (לכל $c \in R_0$), הוא הומומורפיזם.



הגדרה 1.2.100 יהיו $R_0 \subseteq R$ חוגים, ויהיו $\varphi: R \rightarrow S$ ו- $\varphi_0: R_0 \rightarrow S$ הומומורפיזמים. אומרים ש- φ **מרחיב את** φ_0 אם φ_0 הוא הצמצום של φ אל R_0 .

תרגיל 1.2.101 (+)** יהי R_0 תת-חוג של R . נניח ש- $R = R_0[X]$ כאשר $X \subset R$. הראה שאם לשני הומומורפיזמים $R \rightarrow S$ אותו צמצום ל- R_0 והם מסכימים על אברי X , אז הם שווים.

תרגיל 1.2.102 ()** יהי $\varphi: R \rightarrow S$ הומומורפיזם, ויהי $R[x]$ חוג הפולינומים במשתנה אחד מעל R . הראה שלכל אבר a במרכז $C_S(\text{Im}(\varphi))$ קיים הומומורפיזם יחיד $\bar{\varphi}: R[x] \rightarrow S$ המרחיב את φ ומקיים $\bar{\varphi}(x) = a$. כאשר φ שיכון, זהו "הומומורפיזם ההצבה" $x \mapsto a$.

תרגיל 1.2.103 ()** אם R נוצר על-ידי אבר אחד מעל תת-חוג מרכזי R_0 , אז R הוא חוג מנה של חוג הפולינומים $R_0[x]$.

תרגיל 1.2.104 ()** כל חוג קומוטטיבי נוצר סופית מעל R_0 הוא מנה של חוג פולינומים $R_0[\lambda_1, \dots, \lambda_n]$.

תרגיל 1.2.105 (*)** (בהמשך לתרגיל 1.2.102) תן דוגמא לחוג R עם תת-חוג R_0 ואבר $t \in R$ כך ש- $R = R_0[t]$ (כלומר, R נוצר מעל R_0 על-ידי t ; הוא אינו בהכרח חוג פולינומים), עם חוג S והומומורפיזם $\varphi: R \rightarrow S$, עם אבר $a \in S$, כך שלא קיים הומומורפיזם המרחיב את φ ומעביר את t ל- a .

החוג החופשי

בסעיף זה נספק הכללה לתרגיל 1.2.103. תהי X קבוצה של סמלים. **המונויד החופשי** מעל X הוא האוסף F_X של מילים $x_1 \cdots x_n$, $x_1, \dots, x_n \in X$, עם פעולת ההדבקה. המלה הריקה היא האבר הנייטרלי של המונויד.

הגדרה 1.2.106 יהי R_0 חוג. **החוג החופשי הנוצר על-ידי X מעל R_0** הוא אוסף כל הביטויים הפורמליים $\sum \alpha_i w_i$ כאשר $\alpha_i \in R_0$ ו- $w_i \in F_X$, עם פעולות החיבור והכפל הטבעיות; כמו בחוג הפולינומים, הסקלרים מ- R_0 מתחלפים עם כל אבר של X . את החוג החופשי מסמנים ב- $R_0\langle X \rangle$.

דוגמא 1.2.107 אם $X = \{x\}$ קבוצה בת אבר אחד, $R_0\langle X \rangle$ אינו אלא חוג הפולינומים $R_0[x]$.

אם $X = \{x, y\}$ אז $R_0\langle X \rangle$ כולל ביטויים כמו $x - yxx + 3xy$. שלא כמו בחוג הפולינומים בשני משתנים, בחוג הזה $xy \neq yx$.

תרגיל 1.2.108 (-)** יהי $\varphi: R_0 \rightarrow S$ הומומורפיזם, ויהי $R\langle X \rangle$ החוג החופשי הנוצר על-ידי הקבוצה X מעל R_0 . הראה שלכל פונקציה $f: X \rightarrow C_S(\text{Im}(\varphi))$ קיים הומומורפיזם יחיד $\bar{\varphi}: R\langle X \rangle \rightarrow S$ כך ש- $\bar{\varphi}(c) = \varphi(c)$ לכל $c \in R$ ו- $\bar{\varphi}(x) = f(x)$ לכל $x \in X$.

תרגיל 1.2.109 (-)** כל חוג S הנוצר סופית מעל R_0 הוא מנה של חוג חופשי $R_0\langle x_1, \dots, x_n \rangle$ ל- n כלשהו. **הערה.** אם $\varphi: R_0\langle x_1, \dots, x_n \rangle \rightarrow S$, כל קבוצת יוצרים של $\text{Ker}(\varphi)$ (כאידיאל) נקראת קבוצת **יחסים** עבור S .

1.3 דוגמאות ובניה של חוגים

יש מעט מאוד מקרים שבהם בונים חוג מההתחלה, כלומר על-ידי הגדרת פעולות חיבור וכפל על קבוצה ובדיקת כל האקסיומות. בדרך כלל הבניה מתחילה בחוג אחר, מוכר יותר, ומתקדת משם. שתי בניות מסוג זה כבר פגשנו: המעבר מחוג לתת-חוג, והמעבר לחוג מנה. בסעיף זה נכיר כמה מהבניות נוספות.

1.3.1 בניות קלאסיות

חוג השלמים

הדוגמא המכוננת לחוג היא חוג השלמים, $\mathbb{Z}$. אפשר לבנות אותו מתוך מערכת פאנו (של המספרים הטבעיים) בעזרת הגדרת פעולות של חיבור וכפל על מחלקות שקילות של זוגות סדורים. חוג השלמים הוא החוג היחיד ממאפיין אפס שאין לו תת-חוגים (עם יחידה).

טענה 1.3.1 לכל $a \in \mathbb{Z}$ ו- $b > 0$ יש $q, r \in \mathbb{Z}$ כך ש- $a = qr + b$ ו- $0 \leq r < b$.

הוכחה. בנפרד עבור המקרים $a > 0$ ו- $a < 0$, באינדוקציה על $|a|$. $\square$

משפט 1.3.2 כל אידיאל של $\mathbb{Z}$ הוא ראשי.

הוכחה. יהי $I \triangleleft \mathbb{Z}$, $0 \neq I$ אידיאל שונה מאפס. יהי $a \in I$ אבר חיובי מינימלי. ברור ש- $\langle a \rangle \subseteq I$. יהי $x \in I$, אז אפשר לכתוב $x = qa + r$ כאשר $0 \leq r < a$, אבל אז $r = x - qa \in I$ ומכיון ש- $r < a$ ו- a מינימלי, לא יתכן ש- $0 < r$. לכן $r = 0$ ומכאן ש- $x = qa \in \langle a \rangle$. $\square$

תרגיל 1.3.3 ()** חוגי המנה של $\mathbb{Z}$ הם החוגים $\mathbb{Z}/n\mathbb{Z}$ שבהם הפעולות הן חיבור וכפל מודולריים.

מטריצות

הקורא שלמד אלגברה לינארית כבר מכיר את חוגי המטריצות $M_n(F)$, כאשר F שדה. המבנה העיקרי של חוגי מטריצות, עם זאת, אינו תלוי בסוג הסקלרים שמעליהם עובדים. יהי R חוג. התוצאות העיקריות בסעיף זה הן משפט 1.3.10 על המרכז של חוג מטריצות, ומשפט 1.3.12 על האידיאלים של חוג מטריצות.

הגדרה 1.3.4 לכל $1 \leq n$, חוג המטריצות $M_n(R)$ הוא אוסף המטריצות מסדר $n \times n$ מעל R , עם פעולת החיבור לפי רכיבים ופעולת הכפל $(AB)_{ij} = \sum_k A_{ik} B_{kj}$.

תרגיל 1.3.5 (+)** $M_n(R)$ הוא אכן חוג, ואבר היחידה שלו הוא מטריצת היחידה (בדוק את כל האקסיומות!).

המטריצות e_{ij} , שכל רכיביהן 0 פרט לרכיב ה- (i, j) השווה ל-1, נקראות **יחידות מטריצות**.

תרגיל 1.3.6 (*) $1_n = \sum e_{ii}$ הוא אבר היחידה של $M_n(R)$.

תרגיל 1.3.7 ()** יחידות המטריצות מקיימות: $e_{ij}e_{kl} = \delta_{jk}e_{il}$, כאשר $\delta_{\alpha\beta}$ היא הדלתא של קרונקר (השווה ל-1 אם $\alpha = \beta$ ול-0 אחרת).

תרגיל 1.3.8 ()** כל אבר של $M_n(R)$ אפשר להציג באופן יחיד כסכום $\sum_{i,j} a_{ij}e_{ij}$ עבור $a_{ij} \in R$. יתרה מזו, $a_{ij}1_n = \sum_k e_{ki}ae_{jk}$.

תרגיל 1.3.9 (+)** אם $n \geq 2$ אז $M_n(R)$ אינו תחום וגם אינו קומוטטיבי.

משפט 1.3.10 המך K של $M_n(R)$ כולל בדיוק את המטריצות הסקלריות שבאלכסון רכיב $z \in Z(R)$. הדרכה. מטריצה המתחלפת עם כל $e_{\alpha\beta}$, $\alpha \neq \beta$, היא סקלרית.

תרגיל 1.3.11 ()** הראה שהאוסף הכולל את המטריצות המשולשות עליונות מסדר n , $B_n(F) = \{A \in M_n(F) : \forall (i < j) a_{ij} = 0\}$, הוא תת-חוג של $M_n(F)$.

משפט 1.3.12 יהי R חוג. לכל $A_0 \triangleleft R$, $M_n(A_0) = A_0 M_n(R)$, הוא אידיאל של $M_n(R)$, וכל אידיאל של $M_n(R)$ הוא מהצורה הזו.

הוכחה. נסמן ב- 1_n את מטריצת היחידה מסדר n . יהי $A \triangleleft M_n(R)$. אז $A \cap R1_n \triangleleft R1_n$. לפי תרגיל 1.2.8 (עמ' 22), ולכן אפשר לכתוב עבור אידיאל $A_0 \triangleleft R$. $A_0 \triangleleft R$ מחד, לכל $a_{ij} \in A_0$ מתקיים $\sum a_{ij}e_{ij} = \sum (a_{ij}1_n)e_{ij} \in A \cap R1_n$ ולכן $M_n(A_0) \subseteq A$. יהי $a \in A$, אז לכל i, j , $\sum_k e_{ki}ae_{jk} \in A \cap R1_n$, ולכן $a = \sum_{i,j} a_{ij}e_{ij}$. $A_0 M_n(R) \subseteq A$. יהי $a \in A$, אז לכל i, j , $\sum_k e_{ki}ae_{jk} \in A \cap R1_n$, ולכן $a = \sum_{i,j} a_{ij}e_{ij}$. $A_0 M_n(R) \subseteq A$. $\square$

איך מזהים חוג מטריצות, באופן כללי? יהי T חוג. אברים $\epsilon_{ij} \in T$ ($i, j = 1, \dots, n$) נקראים מערכת של יחידות מטריצות אם

$$\begin{aligned}\epsilon_{ij}\epsilon_{kl} &= \delta_{jk}\epsilon_{il}; \\ \epsilon_{11} + \dots + \epsilon_{nn} &= 1\end{aligned}$$

(בפרט, $\epsilon_{11}, \dots, \epsilon_{nn}$ הם אידמפוטנטים אורתוגונליים). יחידות המטריצות הסטנדרטיות בחוג $T = M_n(R)$ הן אכן מערכת כזו, ושם אפשר לכתוב $T = \sum Re_{ij} = \sum e_{ij}R$.

טענה 1.3.13 חוג שיש בו מערכת של יחידות מטריצות הוא חוג מטריצות (פעל תת-חוג). ביתר פירוט, יהי T חוג שיש בו מערכת של יחידות מטריצות, $\{\epsilon_{ij}\}_{i,j=1,\dots,n}$. אז $T \cong M_n(R)$ ו- $R = \epsilon_{11}T\epsilon_{11}$ הוא תת-חוג.

הוכחה. R סגור לכפל משום ש- $\epsilon_{11}T\epsilon_{11} \subseteq \epsilon_{11}T\epsilon_{11}$. נסמן ב- e_{ij} את יחידות המטריצות הסטנדרטיות של $M_n(R)$, $M_n(R) = \sum Re_{ij} = \sum e_{ij}R$ ונגדיר העתקה $\psi: T \rightarrow M_n(R)$ לפי $\psi: t \mapsto \sum_{i,j} (\epsilon_{1i}t\epsilon_{j1})e_{ij}$ זו פונקציה כפלית כי

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

כעת, לכל קבוצת אברים $t_{ij} \in T$,

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

וזוהו האבר הכללי של $M_n(R)$. לכן הפונקציה על. לבסוף, אם $\psi(t) = 0$ אז $\epsilon_{i1} t \epsilon_{1j} = 0$ לכל i, j , ואז גם $\sum_{ij} \epsilon_{i1} (\epsilon_{1i} t \epsilon_{j1}) \epsilon_{1j} = 0$ ולכן $t = (\sum_i \epsilon_{ii}) t (\sum_j \epsilon_{jj}) = \sum_{ij} \epsilon_{i1} (\epsilon_{1i} t \epsilon_{j1}) \epsilon_{1j} = 0$. $\square$

תרגיל 1.3.14 (*)** מצא הנחות מינימליות על האסוציאטורים (הגדרה 1.1.70) המאפשרות להוכיח את טענה 1.3.13 גם כאשר החוג T אינו אסוציאטיבי.

מסקנה 1.3.15 מנה של חוג מטריצות הוא חוג מטריצות.

מסקנה 1.3.16 אם $M_n(R)$ הוא תת-חוג (עם יחידה) של T , אז T בעצמו חוג מטריצות.

מטריצה משולשית היא **יוניפוטנטית** אם האלכסון שלה הוא מטריצת היחידה.

תרגיל 1.3.17 (+)** יהי R חוג עם חילוק. הראה שכל מטריצה הפיכה $A \in M_n(R)$ אפשר לפרק, באופן יחיד, כמכפלה $U_1 D L_1$, כאשר U_1 ו- L_1 מטריצות משולשיות יוניפוטנטיות, עליונה ותחתונה בהתאמה, ו- D אלכסונית. הדרכה. חשב את המקרה $n = 2$ והמשך באינדוקציה.

הסק שכל מטריצה הפיכה אפשר לפרק באופן יחיד למכפלה $U_1 L$ כאשר U_1 משולשית עליונה יוניפוטנטית, ו- L משולשית תחתונה.

תרגיל 1.3.18 (*)** נניח ש- R קומוטטיבי. הגדר את הדטרמיננטה $\det : M_n(R) \rightarrow R$, והוכח שהיא כפלית. הדרכה. הכפילות נובעת מאותו חישוב כמו מעל שדה. ראה גם תרגיל 2.5.50 (עמ' 72).

תרגיל 1.3.19 (*)** כאשר R קומוטטיבי, מטריצה $A \in M_n(R)$ הפיכה אם ורק אם $\det(A)$ הפיכה ב- R . הדרכה. לחלק השני הפעל את נוסחאות קרמר: $A \cdot \text{adj}(A) = |A| \cdot I$.

תרגיל 1.3.20 ()** יהי R חוג קומוטטיבי, ויהי $A \in M_n(R)$ מטריצה ו- $v \in R^n$ וקטור. אם $Av = 0$ אז $\det(A)v = 0$. הדרכה. $\det(A)v = \text{adj}(A)Av = 0$.

תרגיל 1.3.21 ()** אם R אינו קומוטטיבי אז אין פונקציה כפלית $\det : M_2(R) \rightarrow R$ המקיימת $\det\left(\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}\right) = ab$. הדרכה. התבונן במטריצות $\begin{pmatrix} 1 & 0 \\ 0 & a \end{pmatrix}, \begin{pmatrix} b & 0 \\ 0 & 1 \end{pmatrix}$.

חוג האנדומורפיזמים

את חוג המטריצות (לעת עתה, מעל שדה, אבל בחלק האחרון נכליל עובדה זו לכל חוג) אפשר לזהות עם העתקות ליניאריות של מרחב וקטורי. בדומה לזה, אפשר לבנות חוג מכל חבורה אבלית.

דוגמא 1.3.22 תהי A חבורה אבלית. אז $\text{End}(A)$, עם פעולת החיבור $(f+g)(x) = f(x) + g(x)$ והרכבת פונקציות הפוכה ככל $f \cdot g = g \circ f$, הוא חוג, הנקרא **חוג האנדומורפיזמים של A** .

(את הסיבה להיפוך הסדר בכפל לא נסביר כאן.)

תרגיל 1.3.23 ()** $\text{End}(\mathbb{Z}_n) \cong \mathbb{Z}_n$

תרגיל 1.3.24 ()** $\text{End}(\mathbb{Z}_n \times \mathbb{Z}_n) \cong M_2(\mathbb{Z}_n)$

תרגיל 1.3.25 ()** חבורת האברים $\text{End}(G)^\times$ היא $\text{Aut}(G)$.

תרגיל 1.3.26 ()** יהי V מרחב וקטורי מעל שדה F . נסמן ב- $\text{End}_F(V)$ את אוסף ההעתקות הליניאריות $V \rightarrow V$. הראו ש- $\text{End}_F(V)$ הוא תת-חוג של $\text{End}(V)$ שהוגדר בדוגמא 1.3.22.

תרגיל 1.3.27 (*)** יהי V מרחב וקטורי בעל בסיס E בן n אברים. נגדיר העתקה $\text{End}(V) \rightarrow M_n(F)$ לפי $T \mapsto [T]_E$, כאשר $[T]_E$ היא המטריצה המייצגת של T לפי E . הראה שזהו איזומורפיזם.

תרגיל 1.3.28 (*)** יהי $V = F^\mathbb{N}$ מרחב הסדרות האינסופיות מעל השדה F . נסמן $S(v_0, v_1, \dots) = (v_1, \dots)$, $T(v_0, v_1, \dots) = (0, v_1, v_2, \dots)$. הראה שבחוג $\text{End}_F(V)$, $ST = 1$, אבל S אינו הפיך משמאל ו- T אינו הפיך מימין.

תרגיל 1.3.29 (*)** תאר את החוג $\text{End}(\mathbb{Z}_2 \times \mathbb{Z}_4)$.

תרגיל 1.3.30 (*)** 1. יהי $I \triangleleft R$ אידיאל בחוג. הראה ש- $S = \begin{pmatrix} R/I & R/I \\ I & R \end{pmatrix}$ הוא חוג (עם פעולות הכפל הטבעיות; שים לב שזה אינו חוג מטריצות במובן הרגיל של המלה, הגדרה 1.3.4).

2. הראה ש- $S^{-1} \triangleleft \begin{pmatrix} 0 & R/I \\ I & I \end{pmatrix}$, וחשב את חוג המנה.

3. עבור $R = \mathbb{Z}/p^2\mathbb{Z}$ ו- $I = pR$, הראה ש- $S \cong \text{End}(\mathbb{Z}/p \times \mathbb{Z}/p^2)$. [George Bergmann הוכיח (ב-1974) ש- S אינו ניתן לשיכון באף חוג מטריצות מעל חוג קומוטטיבי].

פולינומים

יהי R חוג.

הגדרה 1.3.31 חוג הפולינומים (במשתנה λ) מעל R הוא האוסף $R[\lambda]$ של ביטויים פורמליים $\sum_{i=0}^n a_i \lambda^i + \sum_{i=0}^m a'_i \lambda^i = \sum_{i=0}^{n+m} a_i \lambda^i$ עם $a_i \in R$ ו- $n \geq 0$ כלשהו, עם פעולות החיבור והכפל $\sum_{i=0}^n (a_i + a'_i) \lambda^i$ ו- $\sum_{i=0}^{n+m} a_i a'_j \lambda^{i+j}$.

אם כך, כל אבר של $R[\lambda]$ אפשר להציג כסכום סופי $\sum_i a_i \lambda^i$. ביטויים כאלה נקראים פולינומים.

תרגיל 1.3.32 (*)** $R[\lambda]$ הוא אכן חוג, ו- R הוא תת-חוג שלו (כשחושבים על אבר $a_0 \in R$ כעל פולינום ממעלה 0, ראו להלן). בפרט, אבר האפס ואבר היחידה של R הם אברי האפס והיחידה של $R[\lambda]$.

תרגיל 1.3.33 (*) אם R קומוטטיבי אז גם $R[\lambda]$ קומוטטיבי.

תרגיל 1.3.34 ()** $R[\lambda]$ הוא החוג הנוצר מעל R על-ידי λ (ראה הגדרה 1.1.66).

על החוג $R[\lambda]$ מוגדרת הפונקציה $\deg : R[\lambda] \rightarrow \mathbb{N} \cup \{-\infty\}$ לפי $\deg(\sum_i a_i \lambda^i) = \max\{i : a_i \neq 0\}$. הדרגה של אבר האפס, אם כן, היא $-\infty$, משום שקבוצת המקדמים השונים מאפס ריקה.

תרגיל 1.3.35 ()** פונקציית המעלה מקיימת

$$\deg(f + g) \leq \max\{\deg(f), \deg(g)\}$$

–

$$\deg(fg) \leq \deg(f) + \deg(g).$$

טענה 1.3.36 אם R תחום, אז לכל $f, g \in R[\lambda]$ מתקיים $\deg(fg) = \deg(f) + \deg(g)$.

מסקנה 1.3.37 אם R תחום, אז גם $R[\lambda]$ הוא תחום.

תרגיל 1.3.38 (+)** נניח ש- R הוא תחום. הראה ש- $R^\times = R[\lambda]^\times$: האברים ההפיכים של $R[\lambda]$ הם האברים ההפיכים של R .

תרגיל 1.3.39 (*)** תאר את האברים ההפיכים של $\mathbb{Z}_4[\lambda]$.

אפשר לחזור על בניית חוג הפולינומים, וכך לקבל חוגים כמו $\mathbb{Q}[x, y] = (\mathbb{Q}[x])[y]$ או $\mathbb{Z}[x_1, \dots, x_n]$.

תרגיל 1.3.40 ()** החוגים $\mathbb{Q}[x][y]$ ו- $\mathbb{Q}[y][x]$ איזומורפיים. הערה. בדרך כלל אומרים שחוגים אלה שווים, בלי לדקדק בקטנות.

מכפלה ישרה של חוגים

הגדרה 1.3.41 תהי $\{R_i : i \in \Lambda\}$ משפחה של חוגים. המכפלה הישרה $\prod R_i$ היא, לפי ההגדרה, המכפלה הקרטזית של החוגים, עם פעולות החיבור והכפל לפי רכיבים. כלומר, אברי $\prod R_i$ הם הפונקציות $f : \Lambda \rightarrow \bigcup R_\lambda$ כך ש- $f(\lambda) \in R_\lambda$ לכל $\lambda \in \Lambda$.

תרגיל 1.3.42 (*) הראה ש- $\prod R_i$ הוא חוג (עם אבר היחידה $1 = (1_{R_i})$).

תרגיל 1.3.43 ()** חבורת ההפיכים של המכפלה הישרה היא $(\prod R_\lambda)^\times = \prod R_\lambda^\times$.

להלן כמה תרגילים על הומומורפיזמים אל מכפלה ישרה.

תרגיל 1.3.44 ()** הראה שלכל $i_0 \in \Lambda$, אוסף הוקטורים $\{(r_i) : r_{i_0} = 0\}$ הוא אידיאל של $\prod R_i$, והחיתוך של כל האידיאלים האלה (לכל $i_0 \in \Lambda$) הוא אפס.

תרגיל 1.3.45 ()** אם לכל $i \in \Lambda$ נתון חוג S_i והומומורפיזם $\varphi_i : R \rightarrow S_i$, אז הפונקציה $R \rightarrow \prod S_i$ המוגדרת לפי $x \mapsto (\varphi_i(x))$ היא הומומורפיזם, שהגרעין שלו $\bigcap \text{Ker}(\varphi_i)$. בפרט, אם $\bigcap \text{Ker}(\varphi_i) = 0$ אז R משוכן במכפלה $\prod S_i$.

תרגיל 1.3.46 ()** גרסה סופית של תרגיל 1.3.45: אם נתונים הומומורפיזמים $\varphi_1 : R \rightarrow S_1$ ו- $\varphi_2 : R \rightarrow S_2$, אז $x \mapsto (\varphi_1(x), \varphi_2(x))$ הוא הומומורפיזם $R \rightarrow S_1 \times S_2$ שהגרעין שלו $\text{Ker}(\varphi_1) \cap \text{Ker}(\varphi_2)$.

סכום ישר של חוגים

הגדרה 1.3.47 תהי $\{R_i : i \in \Lambda\}$ משפחה של חוגים. הסכום הישר $\oplus R_i$ הוא, לפי ההגדרה, תת-חוג של $\prod R_i$ הכולל את הפונקציות f שהן כמעט תמיד אפס.

תרגיל 1.3.48 $(**)$ הראה ש- $\oplus R_i$ הוא חוג בלי יחידה (!).

תרגיל 1.3.49 $(*)$ אם Λ סופית אז $\oplus R_\lambda = \prod R_\lambda$.

תרגיל 1.3.50 $(*)$ $\oplus R_i$ הוא תת-חוג (בלי יחידה) של $\prod R_i$.

1.3.2 אלגברות

הגדרה 1.3.51 חוג A המכיל במרכזו שלו שדה F , נקרא **אלגברה מעל אותו שדה**.

תרגיל 1.3.52 $(**)$ יהי A מרחב וקטורי מעל שדה F . כדי להגדיר על A מבנה של אלגברה, יש להגדיר פעולת כפל אסוציאטיבית, הממשיכה את פעולת הכפל של F .

נציג דרך כללית להפוך מרחב וקטורי לחוג. יהי A מרחב וקטורי מעל שדה F , עם בסיס $a_1, \dots, a_n$. נניח שבחרנו **קבועי מבנה** $\gamma_{ij,k} \in F$, באופן כזה שלכל i, j, k, r מתקיים

$$\sum_t \gamma_{ij,t} \gamma_{tk,r} = \sum_t \gamma_{it,r} \gamma_{jk,t}.$$

(זוהי מערכת של n^4 משוואות ריבועיות ב- n^3 נעלמים.)

תרגיל 1.3.53 $(***)$ הוכח שבמקרה זה, פעולת הכפל המוגדרת לפי $a_i a_j = \sum_t \gamma_{ij,t} a_t$ ומומשכת ל- A באמצעות הדיסטריוטיביות היא אסוציאטיבית; הפעולה הופכת את A לחוג בלי יחידה. **הערה.** כל שאר התכונות, למעט אסוציאטיביות, הן אוטומטיות.

תרגיל 1.3.54 $(**)$ אם, בנוסף לזה, $\gamma_{1j,t} = \gamma_{j1,t} = \delta_{jt}$, אז a_1 הוא אבר יחידה של A , וכך A נעשה חוג עם יחידה.

בניה זו היא כללית ביותר, אבל מערכת המשוואות המסובכת הופכת אותה לבלתי מעשית: גם כשמתארים אלגברה באמצעות קבועי המבנה, קשה לחשוף מהם את התכונות שלה (למשל, איך תנסח בשפה של קבועי המבנה את התכונה " A היא תחום"? " A היא שדה"?). משום כך מכירה תורת החוגים בניות קונקרטיות רבות ושונות, העוקפות את הצורך להתמודד עם קבועי המבנה.

תרגיל 1.3.55 $(**)$ מצא את קבועי המבנה המגדירים את $M_n(F)$ כאלגברה מעל F , לפי אברי הבסיס e_{ij} .

אלגברות חבורה

תרגיל 1.3.56 ()** יהיו F שדה ו- G חבורה. הראה שהמרחב הוקטורי $F[G] = \text{span}_F G$ עם פעולת הכפל המורחבת מן החבורה לפי דיסטריבוטיביות, היא חוג. (אלגברה זו נקראת **אלגברת החבורה** של G).

תרגיל 1.3.57 (+)** נניח ש- G חבורה סופית. הראה שהמרכז של $F[G]$ נפרש על-ידי האברים $\hat{C} = \sum_{g \in C} g$ כאשר $C \subseteq G$ הן מחלקות הצמידות של החבורה.

אלגברת הקוטרניונים

בסעיף זה נבנה את אלגברת הקוטרניונים, שהיא הדוגמא הראשונה שהתגלתה לחוג עם חילוק שאינו שדה.

פעולת **הצמוד המרוכב** $\mathbb{C} \rightarrow \mathbb{C}$ מוגדרת לפי $\overline{a + bi} = a - bi$.

תרגיל 1.3.58 ()** הראה שפעולת הצמוד המרוכב $\mathbb{C} \rightarrow \mathbb{C}$ מקיימת את החוקים $\overline{\overline{x}} = x$, $\overline{xy} = \overline{y} \overline{x}$, $\overline{x + y} = \overline{x} + \overline{y}$ (פונקציה כזו נקראת **אינוולוציה**).

תרגיל 1.3.59 ()** הראה שהפונקציה $M_2(\mathbb{C}) \rightarrow M_2(\mathbb{C})$ המוגדרת לפי $(a_{ij}) \mapsto (\overline{a_{ji}})$ היא אינוולוציה. נסמן את התמונה של a תחת פונקציה זו ב- $\bar{a}$.

$$\mathbb{H} = \left\{ \begin{pmatrix} x & y \\ -\bar{y} & \bar{x} \end{pmatrix} : x, y \in \mathbb{C} \right\} \subseteq M_2(\mathbb{C})$$

תרגיל 1.3.60 (+)** בדוק ש- $\dim_{\mathbb{R}} \mathbb{H} = 4$.

תרגיל 1.3.61 ()** הראה ש- $\mathbb{H}$ תת-חוג של $M_2(\mathbb{C})$.

תרגיל 1.3.62 ()** הראה שלכל $u \in M_2(\mathbb{C})$, $u^2 - \text{tr}(u)u + \det(u) = 0$, כאשר $\text{tr} : M_2(\mathbb{C}) \rightarrow \mathbb{C}$ ו- $\det : M_2(\mathbb{C}) \rightarrow \mathbb{C}$ הן העקבה והדטרמיננטה הרגילות.

תרגיל 1.3.63 ()** (בהמשך לתרגיל 1.3.59) לכל $z \in \mathbb{H}$ בנוסף, $z\bar{z} = \bar{z}z = \det(z)$ ו- $z + \bar{z} = \text{tr}(z)$.

טענה 1.3.64 $\mathbb{H}$ הוא חוג עם חילוק.

הוכחה. הדטרמיננטה של $z = \begin{pmatrix} x & y \\ -\bar{y} & \bar{x} \end{pmatrix} \in \mathbb{H}$ היא $|x|^2 + |y|^2 > 0$, ולכן z הפיך ב- $M_2(\mathbb{C})$. מכאן ש- $z^{-1} = \det(z)^{-1}(\text{tr}(z) - z) \in \mathbb{H}$. $\square$

תרגיל 1.3.65 ()** כתוב $j = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ ו- $\hat{i} = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$. הראה ש- $\hat{i}^2 = j^2 = -1$ ו- $j\hat{i} = -\hat{i}j$. הראה ש- $\mathbb{H} = \text{span}_{\mathbb{R}} \{1, \hat{i}, j, \hat{i}j\}$.

המשיך הסעיף מכליל את הבניה הקודמת, מעל שדה כללי.

תרגיל 1.3.66 ()** יהיו F שדה ו- $a, b \in F$. נסמן

$$i_1 = \begin{pmatrix} 0 & a & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -a \\ 0 & 0 & -1 & 0 \end{pmatrix}, \quad j_1 = \begin{pmatrix} 0 & 0 & b & 0 \\ 0 & 0 & 0 & b \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix} \in M_4(F).$$

הראה ש- $i_1^2 = a$, $j_1^2 = b$ ו- $j_1 i_1 = -i_1 j_1$. חשב את הדטרמיננטה של $\alpha + \beta i_1 + \gamma j_1 + \delta i_1 j_1$ ותן תנאי פשוט המבטיח ש- $F[i_1, j_1]$ הוא חוג עם חילוק.

חוגים סדורים

חוג סדור הוא חוג המצויד ביחס סדר ליניארי חזק $>$, כך ש- $x > y$ אם ורק אם $x - y > 0$, וכך שהסכום והמכפלה של אברים חיוביים היא אבר חיובי. חוג סדור שהוא שדה נקרא **שדה סדור**.

תרגיל 1.3.67 (*) המאפיין של חוג סדור הוא אפס.

תרגיל 1.3.68 (*) כל סכום של ריבועים הוא חיובי.

תרגיל 1.3.69 ()** תהי $P \subseteq R$ קבוצה סגורה לכפל וחיבור בחוג, ונסמן $-P = \{-x : x \in P\}$. אם $P \cup \{0\} \cup -P = R$ ו- $P \cap -P = \emptyset$ אז $x > y$ אם $x - y \in P$. הופך את R לחוג סדור. ולהיפך: אם R חוג סדור, אז $P = \{x \in R : x > 0\}$ מקיימת התכונות המוזכרות לעיל.

איחוד על שרשראות

הגדרה 1.3.70 משפחה של קבוצות נקראת **שרשרת אם מבין כל שתיים מהן, אחת מוכלת בשניה**.

תרגיל 1.3.71 ()** תהי $\Lambda = \{R_\lambda\}$ שרשרת של חוגים, כלומר, לכל λ, λ' , אחד מבין R_λ ו- $R_{\lambda'}$ הוא תת-חוג (עם יחידה) בשני. הראה שהאיחוד $\bigcup R_\lambda$ הוא חוג.

תרגיל 1.3.72 (-)** אם מחלישים את הטענה בתרגיל 1.3.71 כך שההכלה היא של תת-חוגים בלי יחידה, האיחוד הוא חוג בלי יחידה.

תרגיל 1.3.73 ()** הראה שאם כל החוגים בשרשרת שבתרגיל 1.3.71 הם תחומים, חוגים עם חילוק או שדות, אז האיחוד הוא תחום, חוג עם חילוק או שדה, בהתאמה.

תרגיל 1.3.74 ()** יהי F שדה. לכל n אפשר לראות את $M_n(F)$ כתת-חוג בלי יחידה של $M_{n+1}(F)$. תאר את האברים והפעולות ב"חוג המטריצות הסופיות" $\bigcup_{n=1}^{\infty} M_n(F)$. (הסבר מדוע אי אפשר להגדיר פעולת כפל בין מטריצות אינסופיות.)

גבול ישר

האיחוד בתרגיל 1.3.74 דרש בחירה קונקרטית של עותק של $M_n(F)$ ב- $M_{n+1}(F)$; לכאורה, התוצאה תלויה בעותק שנבחר, והתמונה הכללית נראית די מסובכת. מושג הגבול הישר של חוגים מאפשר לטפל באיחוד של שרשראות בצורה כללית יותר.

הגדרה 1.3.75 תהי סדרה $R_0 \rightarrow R_1 \rightarrow R_2 \rightarrow \dots$ של חוגים עם הומומורפיזמים $\varphi_i : R_i \rightarrow R_{i+1}$ ($i = 0, \dots$). לכל $i < j$ מגדירים $\varphi_{ij} : R_i \rightarrow R_j$ לפי $\varphi_{ij} = \varphi_{j-1} \circ \dots \circ \varphi_i$. לכן $\varphi_{jk} \circ \varphi_{ij} = \varphi_{ik}$ לכל $i < j < k$. על $\bigcup R_n$ מגדירים יחס שקילות הקובע ש- $x_i \in R_i$ ו- $x_j \in R_j$ שקולים אם יש $k > i, j$ כך ש- $\varphi_{ik}(x_i) = \varphi_{jk}(x_j)$ (כלומר, x_j "מסכימים לבסוף"). **הגבול הישר של המערכת R_i מוגדר כחוג של מחלקות השקילות $\sim$ על $\bigcup R_i$, עם הפעולות הטבעיות.**

(זהו מקרה פרטי של הגדרה כללית יותר, שבה מוחלפת סדרת החוגים ב"מערכת מכוונת").

תרגיל 1.3.76 (*) אם כל ההומומורפיזמים $R_i \rightarrow R_{i+1}$ הם הכלולות, הגבול הישר אינו אלא איחוד השרשרת.

תרגיל 1.3.77 (*) הגדר במדויק את פעולות החיבור והכפל בגבול ישר של חוגים. הראה שמתקבל חוג. מיהם אברי האפס והיחידה?

תרגיל 1.3.78 (*)** יהי F שדה. נסמן $R_n = F[x]$ לכל $n \geq 0$. נגדיר שיכונים $R_n \rightarrow R_{n+1}$ לפי $x \mapsto x^{n+1}$. הראה שאפשר לזהות את הגבול הישר של המערכת הזו עם החוג שאבריו הם סכומים סופיים של מונומים מהצורה αx^r עבור $\alpha \in F$, $0 < r \in \mathbb{Q}$.

הוכח ש- $\lim_{\rightarrow} R_n$ אינו איזומורפי לחוג פולינומים בכל מספר של משתנים. (חוג זה מופיע בתרגילים 2.3.7, 3.3.12).

תרגיל 1.3.79 (*)** כל חוג הוא גבול ישר של חוגים נוצרים סופית.

גבול הפוך

הגדרה 1.3.80 תהי $R_0 \leftarrow R_1 \leftarrow R_2 \leftarrow \dots$ סדרה של חוגים עם הומומורפיזמים $\varphi_i : R_{i+1} \rightarrow R_i$ ($i \geq 0$). הגבול ההפוך של הסדרה (נקרא גם גבול פרוייקטיבי) הוא החוג

$$\lim_{\leftarrow} R_n = \left\{ (x_n) \in \prod R_n : \forall n, \varphi_n(x_{n+1}) = x_n \right\}.$$

(כמו במקרה של גבול ישר, זהו מקרה פרטי של הגדרה כללית יותר, שבה מוחלפת סדרת החוגים ב"מערכת מכוונת").

תרגיל 1.3.81 ()** על $\lim_{\leftarrow} R_n$ נגדיר את פעולות החיבור והכפל לפי רכיבים. הראה שהגבול ההפוך של סדרת החוגים הוא אכן חוג.

תרגיל 1.3.82 (*)** הראה שאם משמיטים מספר סופי של אברים מן הזנב, מתקבל חוג איזומורפי. הראה שאם n_k סדרת אינדקסים עולה, אז הגבול ההפוך של הסדרה המדוללת $\dots \leftarrow R_{n_2} \leftarrow R_{n_1}$, עם ההומומורפיזמים המתקבלים מהרכבה $R_{n_{i+1}} \rightarrow R_{n_i}$ לפי $\varphi_{n_i} \circ \dots \circ \varphi_{n_{i+1}-1}$, איזומורפי לגבול ההפוך של הסדרה המקורית.

תרגיל 1.3.83 (*)** הראה שאם כל ההומומורפיזמים φ_i הם על, אז ההטלה על הרכיב ה- m , $(\lim_{\leftarrow} R_n) \rightarrow R_m$, גם היא על.

תרגיל 1.3.84 (*)** הראה ש- $F[x]/\langle x \rangle^n \cong \lim_{\leftarrow} F[x]/\langle x \rangle^n$.

תרגיל 1.3.85 (*)** הראה ש- $F[[x]][[y]]/\langle x, y \rangle^n = \lim_{\leftarrow} F[x, y]/\langle x, y \rangle^n = F[[x]][[y]]$.

תרגיל 1.3.86 (*)** יהי $M \triangleleft R$ אידיאל. נתבונן בסדרה

$$R/M \leftarrow R/M^2 \leftarrow R/M^3 \leftarrow R/M^4 \leftarrow \dots,$$

עם ההטלות הטבעיות $\varphi_i : R/M^{i+2} \rightarrow R/M^{i+1}$ כך $\text{Ker}(\varphi_{i-1}) = M^i/M^{i+1}$. נניח שיש פונקציות אדיטיביות $\theta_i : R/M^{i+1} \rightarrow R/M^{i+2}$ כך ש- $\theta_i \circ \varphi_i = \text{Id}_{R/M^{i+1}}$.

נתבונן בסכום הפורמלי $\sum_{i=0}^{\infty} M^i/M^{i+1}$ עם החיבור לפי רכיבים, והכפל המוגדר על הרכיבים $M^i/M^{i+1} \times M^j/M^{j+1} \rightarrow M^{i+j}/M^{i+j+1}$ לפי המכפלה הטבעית $(a_i + M^{i+1})(b_j + M^{j+1}) = a_i b_j + M^{i+j+1}$. נניח בנוסף שההעתקות θ_i עקביות עם הפעולה הזו במובן הבא: לכל $x_n \in M^n/M^{n+1}$ ו- $y_m \in M^m/M^{m+1}$, ולכל $k \geq n+m$, מתקיים $\theta_{k-1} \cdots \theta_{n+m}(x_n y_m) = \theta_{k-1} \cdots \theta_n x_n \cdot \theta_{k-1} \cdots \theta_m y_m$. כאשר הכפל באגף ימין הוא הכפל ב- R/M^k .
הראה ש-

$$\lim_{\leftarrow} R/M^{i+1} \cong \sum_{i=0}^{\infty} M^i/M^{i+1}.$$

הדרכה. נגדיר העתקה $\Psi: \lim_{\leftarrow} R/M^{i+1} \rightarrow \sum_{i=0}^{\infty} M^i/M^{i+1}$ לפי $\Psi(a_0, a_1, a_2, \dots) = (x_0, x_1, x_2, \dots)$ כאשר $x_i = a_i - \theta_{i-1}a_{i-1}$ בדיוק בגלל שלפי ההנחה $\varphi_{i-1}(a_i - \theta_{i-1}a_{i-1}) = 0$. הפונקציה הפיכה, עם $a_i = x_i + \theta_{i-1}x_{i-1} + \theta_{i-1}\theta_{i-2}x_{i-2} + \dots + \theta_{i-1} \cdots \theta_0 x_0$. די להראות ש- Ψ^{-1} שומרת כפל על רכיבים, היינו $\Psi^{-1}(xy) = \Psi^{-1}(x)\Psi^{-1}(y)$ כאשר $x = (0, \dots, x_n, 0, \dots)$ ו- $y = (0, \dots, y_m, 0, \dots)$. כדי להשוות את שני האגפים די להשוות רכיב רחוק מספיק. הרכיב ה- $k \geq n+m$ ב- $\Psi^{-1}(xy)$ הוא $\theta_{k-1} \cdots \theta_{n+m}(x_n y_m)$ וב- $\Psi^{-1}(x)\Psi^{-1}(y)$ הוא $\theta_{k-1} \cdots \theta_n x_n \cdot \theta_{k-1} \cdots \theta_m y_m$, והם שווים לפי ההנחה.

פרק 2

אידיאלים ראשוניים ומקסימליים

בין החוגים הקומוטטיביים, הדוגמאות החשובות ביותר לחוגים הן שדות ותחומי שלמות; חוגים אלו קשורים לאידיאלים מקסימליים וראשוניים, באופן שנסביר בהמשך. בפרק הזה נעסוק באידיאלים מקסימליים וראשוניים גם במקרה הכללי יותר, של חוגים לא קומוטטיביים.

2.1 אידיאלים מקסימליים

כשלומדים את המבנה של סריג האידיאלים בולטת לעין העובדה שתמיד יש בסריג הזה אבר מינימלי (אידיאל האפס) ואבר מקסימלי (החוג עצמו). אפשר לקבל אפיון טוב יותר של חוגים אם מתרכזים דווקא באידיאלים אמיתיים, כלומר, מוציאים את החוג עצמו מן החשבון.

הגדרה 2.1.1 אידיאל אמיתי $M \triangleleft R$ הוא מקסימלי אם הוא מקסימלי בין האידיאלים האמיתיים, כלומר, אין אידיאל אמיתי $M' \supset M$.

תרגיל 2.1.2 ()** בחוג קומוטטיבי R , $M \triangleleft R$ מקסימלי אם ורק אם לכל $x \notin M$ יש $y \in R$ כך ש- $xy \in M$ ו- $1 - xy \in M$.

2.1.1 קיומם של אידיאלים מקסימליים

הלמה של צורן היא כלי עבודה שימושי, המאפשר להוכיח שקיים בקבוצה סדורה אבר מקסימלי, גם כאשר אין שום דרך להצביע על אבר מקסימלי באופן מפורש. עבורנו, התפקיד העיקרי של הלמה הוא להראות שבכל חוג יש אידיאלים מקסימליים.

משפט 2.1.3 (הלמה של צורן) תהי $(\Lambda, \leq)$ קבוצה סדורה לא ריקה. אם לכל שרשרת לא ריקה Λ^- יש חסם מלעיל, אז יש ב- Λ אבר מקסימלי.

תזכורת. שרשרת היא קבוצת אברים סדורה לינארית (כלומר, מבין כל שני אברים, יש אחד הגדול מן השני). חסם מלעיל של שרשרת הוא אבר x הגדול מכל האברים בשרשרת. **הערה.** לא מספיק להניח שקיים חסם עליון לשרשראות בנות מניה: הסודר $\aleph_1$ מקיים הנחה זו אבל אין לו אבר מקסימלי.

מסקנה 2.1.4 תהי $\mathcal{F}$ משפחה של תת-קבוצות של קבוצה Ω . אם לכל שרשרת של אברים ב- $\mathcal{F}$ גם $\bigcup A_\lambda \in \mathcal{F}$, אז יש ב- $\mathcal{F}$ אבר מקסימלי.

משפט 2.1.5 כל אידיאל I בחוג עם יחידה R מוכל באידיאל מקסימלי.

הוכחה. משפחת האידיאלים האמיתיים המכילה את I מקיימת את התנאי של מסקנה 2.1.4 לפי תרגיל 1.2.22 (עמ' 23). $\square$

מסקנה 2.1.6 לכל חוג (עם יחידה!) יש אידיאל מקסימלי.

מעניין שטענה זו אינה נכונה בחוגים ללא יחידה (היכן השתמשנו באבר היחידה בהוכחה?)

תרגיל 2.1.7 (***) (דוגמא לחוג בלי יחידה שאין לו אידיאל מקסימלי) את החוג של טורי לורן פגשנו בהגדרה 3.4.51. נתבונן בחוגים $S_n = F[[x]]$, עם השיכונים $S_n \rightarrow S_{n+1}$ לפי $x \mapsto x^{n+1}$. נסמן $S = \lim_{\rightarrow} S_n$ (השווה לתרגיל 1.3.78, עמ' 42).

1. הסבר מדוע $\sum_{n=0}^{\infty} x^{1/n!} \notin S$, למרות שכל המונחים של הסכום הזה נמצאים ב- S .

2. הראה שהפונקציה ν מתרגיל 3.4.55 ממשיכה לפונקציה $\nu: S \rightarrow \mathbb{Q}$ המקיימת את התכונות המוזכרות שם.

3. לכל $\beta > 0$ ממשי, $I_\beta = \{f \in S: \nu(f) > \beta\}$ ו- $I'_\beta = \{f \in S: \nu(f) \geq \beta\}$ הם אידיאלים של S (הם שווים אלא אם β רציונלי).

4. יהי $I \triangleleft S$. אז $I = \bigcup_{n=1}^{\infty} (I \cap S_n)$, ולכל n יש $0 \leq \alpha_n \in \frac{1}{n!}\mathbb{Z}$ יחיד כך ש- $I \cap S_n = \{f \in S_n: \nu(f) \geq \alpha_n\}$ (תרגיל 3.4.59, עמ' 104). הראה שהסדרה $\{\alpha_n\}$ יורדת.

5. ניקח $\alpha = \lim \alpha_n$. הראה ש- $I = I_\alpha$ או $I = I'_\alpha$.

6. אוסף האידיאלים של S מהווה שרשרת (מעוצמה א).

7. $S_0 = \{f \in S: \nu(f) > 0\}$ הוא האידיאל המקסימלי היחיד של S .

8. לחוג-בלי-יחידה S_0 אין אידיאל אמיתי מקסימלי.

חוג ללא אידיאל מקסימלי

תרגיל 2.1.8 (**) אוסף האברים ההפיכים בחוג קומוטטיבי הוא המשלים של איחוד האידיאלים המקסימליים.

תרגיל 2.1.9 (**) אידיאל שהוא מקסימלי בין האידיאלים הנוצרים סופית, הוא מקסימלי.

תרגיל 2.1.10 (***) תן דוגמא להומומורפיזם $\phi: R \rightarrow S$ עם אידיאל מקסימלי $M \triangleleft S$ כך ש- $\phi^{-1}(M) \triangleleft R$ אינו מקסימלי.

תרגיל 2.1.11 (***) יהי $\phi: R \rightarrow S$ אפימורפיזם של חוגים. הראה שאם $M \triangleleft R$ מקסימלי, אז $\phi(M) \subseteq S$ (שהוא אידיאל לפי תרגיל 1.2.81, עמ' 30) שווה ל- S או מקסימלי.

תרגיל 2.1.12 (**) יהיו $\varphi: R \hookrightarrow R'$ שיכון (של חוגים עם יחידה), M אידיאל מקסימלי של R , ו- M' אידיאל מקסימלי של R' המכיל את תמונת M . אז יש שיכון $R/M \hookrightarrow R'/M'$ (השווה לתרגיל 1.2.91, עמ' 32).

אידיאלים מינימליים

נאמר שאידיאל שונה מאפס הוא **אידיאל מינימלי** אם הוא אינו מכיל אף אידיאל שונה מאפס אחר.

תרגיל 2.1.13 (*) כל אידיאל מינימלי בחוג קומוטטיבי הוא ראשי.

תרגיל 2.1.14 (*)** בתחום שלמות אין אידיאלים מינימליים.

תרגיל 2.1.15 (*)** תן דוגמא לחוג שבו כל אידיאל אמייתי שונה מאפס הוא מינימלי.

אידיאלים מקסימליים של חוגי פונקציות

יהי K מרחב טופולוגי קומפקטי (אפשר להניח ש- $K = [a, b]$ הוא קטע סגור על הישר הממשי). נסמן ב- $C(K)$ את אוסף הפונקציה הרציפות $K \rightarrow \mathbb{C}$, עם פעולות החיבור והכפל הנקודתיות, כלומר $(f+g)(x) = f(x) + g(x)$ ו- $(fg)(x) = f(x)g(x)$.

תרגיל 2.1.16 ()** הראה ש- $C(K)$ הוא חוג.

תרגיל 2.1.17 ()** לכל נקודה $z \in K$, $M_z = \{f : f(z) = 0\}$, שהוא הגרעין של ההומומורפיזם $C(K) \rightarrow \mathbb{C}$ המוגדר לפי $f \mapsto f(z)$, הוא אידיאל מקסימלי.

תרגיל 2.1.18 (*)** כל אידיאל מקסימלי של $C(K)$ הוא מהצורה M_z . פתרון. יהי M אידיאל שאינו מוכל באף M_z . אז לכל $z \in K$ יש $f_z \in M$ כך ש- $f_z(z) \neq 0$; לפי הרציפות יש קבוצה פתוחה V_z שבה f אינו מתאפס. ברור ש- $\{V_z\}$ כיסוי של K , ולפי הקומפקטיות יש לו תת-כיסוי סופי $V_{z_1}, \dots, V_{z_n}$. אבל אז $g = \sum f_{z_i} \overline{f_{z_i}} \in M$ חיובית ממש בכל K , ולכן g הפיכה; מכאן ש- $M = C(K)$.

הבחנה זו היא הצעד הראשון בכיוון הקומפקטיפיקציה של Stone-Čech, שאינה מענייננו בקורס זה.

ראוי להזכיר גם את **משפט גלפנד-קולמוגורוב** (Gillman-Jerison, Rings of continuous functions, משפט 7.3): אם K קומפקטי והאוסדורף, אז $C(K)$ (עד כדי איזומורפיזם) קובע את K (עד כדי הומומורפיזם).

2.1.2 חוגים פשוטים

מה קורה כשמחלקים חוג באידיאל מקסימלי? מסתבר שהחוג המתקבל הוא **חוג פשוט**. במונח 'חוג פשוט' יש משהו אירוני, משום שאלו בדרך כלל החוגים הקשים ביותר לטיפול: הרי אין להם אידיאלים וחוגי מנה.

הגדרה 2.1.19 **חוג פשוט** הוא חוג שאין לו אידיאלים אמיתיים לא טריוויאליים.

במלים אחרות:

תרגיל 2.1.20 (*) חוג הוא פשוט אם ורק אם 0 אידיאל מקסימלי שלו.

תרגיל 2.1.21 ()** אם A פשוט, אז כל הומומורפיזם של חוגים $A \rightarrow B$ הוא שיכון.

הקשר לאידיאלים מקסימליים

משפט 2.1.22 יהי R חוג. אידיאל $M \triangleleft R$ הוא מקסימלי אם ורק אם חוג המנה R/M הוא פשוט.

הוכחה. זהו מקרה פרטי של משפט ההתאמה 1.2.95. $\square$

מסקנה 2.1.23 לכל חוג (עם יחידה) יש חוגי מנה פשוטים (לפי משפט 2.1.22 ומסקנה 2.1.6).

חוגים פשוטים קומוטטיביים

משפט 2.1.24 חוג קומוטטיבי הוא פשוט אם ורק אם הוא שדה.

הוכחה. חוג קומוטטיבי הוא שדה אם ורק אם כל אבריו הפיכים; הטענה נובעת מתרגיל 1.2.21 (עמ' 23). $\square$

מסקנה 2.1.25 יהי R חוג קומוטטיבי. אידיאל $M \triangleleft R$ הוא מקסימלי אם ורק אם R/M שדה. הערה. אפשר להוכיח זאת גם ישירות מתרגיל 2.1.2 (עמ' 45).

יותר מזה: כל חוג פשוט, לאו דווקא קומוטטיבי, הוא למעשה אלגברה, משום שהמרכז שלו הוא שדה:

משפט 2.1.26 המרכז של חוג פשוט הוא שדה.

הוכחה. יהי $Z = Z(R)$ המרכז של החוג הפשוט R . יהי $\alpha \in Z$, $\alpha \neq 0$, אז $R\alpha$ הוא אידיאל שונה מאפס של R , ולכן $1 \in R\alpha$, ומכאן α הפיך ב- R . לפי תרגיל 1.1.62 (עמ' 16) נובע מכאן ש- α הפיך ב- $Z(R)$. $\square$

חוג-בלי-יחידה R הוא פשוט אם אין לו אידיאלים לא טריוויאליים, ובנוסף $R^2 \neq 0$.

תרגיל 2.1.27 (+)** כל חוג-בלי-יחידה קומוטטיבי פשוט הוא שדה. הדרכה. יש הומומורפיזם $R \rightarrow \text{End}(R)$ לפי $\ell_a: a \mapsto$ הסק שלכל $a \neq 0$ מתקיים $aR = R$. אבל $\{x: ax = 0\} \triangleleft R$, ולכן מ- $ab = 0$ אפשר להסיק $a = 0$ או $b = 0$. בחר $a \neq 0$. אז יש $e \in R$ כך ש- $ae = a$. הוכח ש- e אבר יחידה של החוג. מכאן ש- R חוג סע יחידה, ועל עליו משפט 2.1.24.

בניה של חוגים פשוטים

תרגיל 2.1.28 ()** לחוג עם חילוק אין אידיאלים שמאליים אמיתיים לא טריוויאליים. בפרט, כל חוג עם חילוק הוא פשוט. הדרכה. תרגיל 1.2.19 (עמ' 23).

תרגיל 2.1.29 ()** אם A חוג פשוט אז גם $M_n(A)$ פשוט. הדרכה. משפט 1.3.12.

בפרט, כל חוג מטריצות מעל חוג עם חילוק הוא פשוט. לפי **משפט ודרברן** (שלא נוכיח כאן), כל חוג פשוט מממד סופי מעל המרכז שלו הוא מהצורה הזו.

תרגיל 2.1.30 ()** בהמשך לתרגיל 1.3.73 (עמ' 41), הראה שאיחוד על-פני שרשרת של חוגים פשוטים היא חוג פשוט.

חוגים n -פשוטים

תרגיל 2.1.31 ()** חוג R הוא פשוט אם ורק אם לכל $a \in R$, $a \neq 0$ קיימים $x_1, \dots, x_k, y_1, \dots, y_k \in R$ כך ש- $x_1ay_1 + \dots + x_kay_k = 1$.

הגדרה 2.1.32 אם לכל $a \in R$, $a \neq 0$ קיימים $x_1, \dots, x_n, y_1, \dots, y_n \in R$ כך ש- $\sum x_iay_i = 1$, כאשר n קבוע, אז R הוא חוג n -פשוט.

התנאי נעשה חלש יותר ככל ש- n גדול יותר; כל חוג n -פשוט הוא פשוט, אבל חוג פשוט אינו חייב להיות n -פשוט לאף n .

חוג חילוק



1-פשוט



2-פשוט



תרגיל 2.1.33 (*) חוג הוא 1-פשוט אם לכל $a \neq 0$ יש x, y כך ש- $xay = 1$. הראה שכל חוג עם חילוק הוא 1-פשוט. (מאידך יש חוגים 1-פשוטים שאינם חוגים עם חילוק, [Cohn, 2005]; השווה לתרגיל 1.1.26 (עמ' 13)).

תרגיל 2.1.34 ()** תחום 1-פשוט הוא חוג עם חילוק. הדרכה. אם $ax = 1$ אז $ay = 1$ הפך משמאל ולכן הפך לפי תרגיל 1.1.38 (עמ' 14); לכן a הפך.

2.2 פירוק למכפלה ישרה

לעתים קרובות, חוגי המנה של חוג R הם קלים יותר לטיפול. מאידך ההטלה אל חוג המנה אינה משכנת את R , והפתרון הוא לנסות לשכן את R במכפלה של כמה מנות. הרעיון הכללי פשוט למדי:

תרגיל 2.2.1 (*)** תהי $\mathcal{F}$ משפחה של אידיאלים של חוג R . הראה שהגרעין של הפונקציה $R \rightarrow \prod_{I \in \mathcal{F}} R/I$ המוגדרת לפי $x \mapsto (x + I)_{I \in \mathcal{F}}$ הוא החיתוך $\bigcap_{I \in \mathcal{F}} I$. בפרט אם $\bigcap I = 0$ אז R משוכן במכפלה $\prod R/I$. הדרכה. זהו מקרה פרטי של תרגיל 1.3.45 (עמ' 38).

מפאת חשיבותה של התוצאה, ננסח גם כאן גרסה סופית:

תרגיל 2.2.2 (*)** אם $I_1, \dots, I_n$ אידיאלים של חוג R ו- $I_1 \cap \dots \cap I_n = 0$ אז $R \hookrightarrow R/I_1 \times \dots \times R/I_n$ הוא שיכון $x \mapsto (x + I_1, \dots, x + I_n)$.

השאלה היא, כמובן, מתי ההעתקה $R \rightarrow \prod R/I_i$ היא איזומורפיזם; כשזה קורה, קיבלנו פירוק של R למכפלה ישרה של חוגי מנה.

2.2.1 אידיאלים קו-מקסימליים

הגדרה 2.2.3 אידיאלים (אמיתיים) $I, J \triangleleft R$ הם קו-מקסימליים אם $I + J = R$.

לדוגמא:

תרגיל 2.2.4 (*) אידיאל הוא מקסימלי אם ורק אם הוא קו-מקסימלי ביחס לכל אידיאל שאינו מוכל בו.

תרגיל 2.2.5 (*) כל שני אידיאלים מקסימליים (שונים) הם קו-מקסימליים.

תרגיל 2.2.6 (*) קו-מקסימליות 'עולה כלפי מעלה', כלומר, אם I, J קו-מקסימליים ו- $I' \subseteq I, J' \subseteq J$, אז בוודאי I', J' קו-מקסימליים.

תרגיל 2.2.7 ()** אם $II' = 0$ אז כל אידיאל מקסימלי מכיל את I או את I' .
הדרכה: אחרת $M + I = M + I' = R$ ולכן $M + II' = M$ ו- $R = (M + I)(M + I') \subseteq M + II' = M$.

תרגיל 2.2.8 ()** אם R קומוטטיבי ו- $ab = 0$ אז כל אידיאל מקסימלי מכיל לפחות אחד מבין a, b . הדרכה: תרגיל 2.2.7.

תרגיל 2.2.9 (-*)** 1. נניח ש- $I_1, \dots, I_n$ כולם קו-מקסימליים ביחס ל- J . הוכח שגם $I_1 \cdots I_n$ קו-מקסימלי ביחס ל- J . הדרכה: לכל i כתוב $a_i + b_i = 1$ עם $a_i \in I_i$ ו- $b_i \in J$; חשבו על $1 = (a_1 + b_1) \cdots (a_n + b_n)$.

2. אם I, J קו-מקסימליים אז לכל n גם I^n, J קו-מקסימליים.

3. אם I, J קו-מקסימליים אז לכל n, m גם I^n, J^m קו-מקסימליים.

תרגיל 2.2.10 ()** אם I, J קו-מקסימליים אז $I \cap J = IJ + JI$. הדרכה: כתוב $1 = a + b$ עבור $a \in I$ ו- $b \in J$; אז לכל $x \in I \cap J$ מתקיים $x = ax + bx \in JI + IJ$.

תרגיל 2.2.11 (*)** נניח ש- $I_1, \dots, I_n$ קו-מקסימליים בזוגות. אז

$$I_1 \cap \cdots \cap I_n = \sum_{\sigma \in S_n} I_{\sigma(1)} \cdots I_{\sigma(n)}.$$

הדרכה: אינדוקציה על n , בעזרת תרגיל 2.2.9(1) ו- $I_{\sigma(1)} \cdots I_{\sigma(n-1)} \cap I_n = \sum_{\sigma \in S_{n-1}} I_{\sigma(1)} \cdots I_{\sigma(n-1)} I_n$ קו-מקסימליים.

תרגיל 2.2.12 (**)** נניח ש- $I_1, \dots, I_n$ קו-מקסימליים בזוגות. מצא את המספר הקטן ביותר t שעבורו יש תמורות $\sigma_1, \dots, \sigma_t \in S_n$, כך שמובטח השוויון $I_1 \cap \cdots \cap I_n = \sum_{j=1}^t I_{\sigma_j(1)} \cdots I_{\sigma_j(n)}$.

תרגיל 2.2.13 ()** אם R חוג קומוטטיבי ו- $I_1, \dots, I_n$ קו-מקסימליים בזוגות, אז $I_1 \cap \cdots \cap I_n = I_1 \cdots I_n$.

תרגיל 2.2.14 ()** יהי $S \subseteq R$ תת-חוג. יהי $L \leq_\ell R$ כך ש- $L \subseteq S$. אם $B \leq_\ell R$ קו-מקסימלי ל- L ב- R , אז $B \cap S$ קו-מקסימלי ל- L ב- S .

2.2.2 משפט השאריות הסיני

משפט 2.2.15 (משפט השאריות הסיני) יהיו $I_1, \dots, I_m \triangleleft R$ אידיאלים קו-מקסימליים בזוגות. אז ההעתקה של תרגיל 2.2.2 היא איזומורפיזם

$$R/(I_1 \cap \cdots \cap I_m) \cong R/I_1 \times \cdots \times R/I_m.$$

תרגיל 2.2.16 ()** הוכח את משפט השאריות הסיני. הדרכה: מספיק להוכיח, לכל i , שקיים $x \in R$ כך שלכל j מתקיים $x \equiv \delta_{ij} \pmod{I_j}$. לכל $i \neq j$ כתוב $1 = t_j + s_j$ עבור $t_j \in I_i$ ו- $s_j \in I_j$, וקח $x = s_1 \cdots s_{i-1} s_{i+1} \cdots s_m$.

ובגרסה מעט שונה:

תרגיל 2.2.17 ()** יהיו אידיאלים קו-מקסימליים של חוג R . אז לכל $x_1, \dots, x_n \in R$ יש למערכת המשוואות

$$x \equiv x_i \pmod{I_i}$$

פתרון ב- R (שהוא יחיד עד כדי הוספת אבר מ- $I_1 \cap \dots \cap I_n$).

תרגיל 2.2.18 ()** אם לחוג R יש k אידיאלים מקסימליים שהחיתוך שלהם הוא אפס, אז R איזומורפי למכפלה של k חוגים.

תרגיל 2.2.19 (*)** יהיו $A, B, C \triangleleft R$ אידיאלים. הוכח שהתכונות הבאות שקולות:

$$1. \left\{ \begin{array}{l} t \equiv x \equiv y \pmod{C} \\ t \equiv z \equiv x \pmod{B} \\ t \equiv y \equiv z \pmod{A} \end{array} \right\} \text{ אז יש } t \in R \text{ כך ש-} \left\{ \begin{array}{l} x \equiv y \pmod{C} \\ z \equiv x \pmod{B} \\ y \equiv z \pmod{A} \end{array} \right\} \text{ אם}$$

$$2. B \cap (A + C) \subseteq C + (A \cap B)$$

$$3. B \cap (A + C) = (B \cap A) + (B \cap C) \text{ ("דיסטריבוטיות").}$$

הדרכה: עבור (1) $\iff$ (2) עבור $z = 0$. עבור (2) $\iff$ (1) התונבן ב- $C + A$; $x - z = (x - y) + (y - z) \in C + A$; לפי ההנחה יש $c' \in C$ ו- $d \in A \cap B$ כך ש- $x - z = c' + d$; $x - z = c' + d$ $\iff$ (2) $X \subseteq Y$ אם ורק אם $X = X \cap Y$. (לאפיון תכונה (3), ראה הערה 5.2.58. לשלשת אידיאלים שאינם מקימים את התנאי, ראה תרגיל 2.5.43)

משפט השאריות הסיני מעל השלמים

הגדרה 2.2.20 יהי R חוג קומוטטיבי. נאמר ש- $a, b \in R$ קו-מקסימליים אם Ra ו- Rb קו-מקסימליים (את המושגים 'זרים' ו'זרים במובן החלישי' נגדיר בהמשך: הגדרות 3.3.70, 3.3.116). במלים אחרות קיימים $\alpha, \beta \in R$ כך ש- $\alpha a + \beta b = 1$.

תרגיל 2.2.21 ()** יהי R חוג קומוטטיבי עם $a_1, \dots, a_n \in R$ זרים בזוגות, במובן החזק. אז $R/Ra_1 \cdots a_n \cong R/Ra_1 \times \cdots \times R/Ra_n$. הדרכה: תרגיל 2.2.13.

תרגיל 2.2.22 ()** יהיו $n_1, \dots, n_t \in \mathbb{Z}$ מספרים זרים בזוגות. אז

$$\mathbb{Z}_{n_1 \cdots n_t} \cong \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_t}$$

(זהו איזומורפיזם של חוגים, המכליל את האיזומורפיזם שאולי ראיתם בתורת החבורות).

ובגרסה נוספת:

תרגיל 2.2.23 ()** יהיו $n_1, \dots, n_t \in \mathbb{Z}$ מספרים זרים בזוגות. לכל $a_1, \dots, a_t \in \mathbb{Z}$ קיים x יחיד מודולו $n_1 \cdots n_t$ כך ש- $x \equiv a_i \pmod{n_i}$ לכל i .

תרגיל 2.2.24 (*)** הראה שאם n, m זרים אז חבורות אוילר מקיימות $U_{nm} \cong U_n \times U_m$. הדרכה. תרגיל 2.2.22 ותרגיל 1.3.43.

תרגיל 2.2.25 ()** פונקציית אוילר מוגדרת לפי $|\{1 \leq a \leq n : a \text{ זר ל-} n\}|$. הסק מתרגיל 2.2.24 את הנוסחה $\phi(p_1^{n_1} \cdots p_t^{n_t}) = (p_1 - 1)p_1^{n_1-1} \cdots (p_t - 1)p_t^{n_t-1}$.

תרגיל 2.2.26 ()** הראה שתנאי הדיסטריבוטיביות מתרגיל 2.2.19 מתקיים עבור כל שלושה אידיאלים של $\mathbb{Z}$.

2.2.3 אידמפוטנטים

משפט השאריות הסיני מפרק חוגים כמכפלה ישרה של חוגים. מתברר שפירוק לסכום ישר קשור לסוג מיוחד של אברים בחוגים: $e = (1, 0) \in R_1 \times R_2$ מקיים את השוויון $e^2 = e$. בעקבות זאת, נגדיר (כפי שכבר רמזנו בתרגיל 1.1.37, עמ' 14):

הגדרה 2.2.27 אבר $e \in R$ נקרא **אידמפוטנט** אם $e^2 = e$.

למשל, אבר האפס ואבר היחידה הם אידמפוטנטים. אלו הם **האידמפוטנטים הטריוויאליים**.

תרגיל 2.2.28 (*) אם e אידמפוטנט, אז גם $1 - e$ אידמפוטנט.

הגדרה 2.2.29 אידמפוטנטים e_1, e_2 הם **אורתוגונליים** אם $e_1 e_2 = e_2 e_1 = 0$.

תרגיל 2.2.30 (*) לכל אידמפוטנט e , האידמפוטנטים $e, 1 - e$ אורתוגונליים.

תרגיל 2.2.31 ()** יהיו e_1, e_2 אידמפוטנטים אורתוגונליים. אז גם סכומם $e_1 + e_2$ הוא אידמפוטנט.

תרגיל 2.2.32 ()** מגדירים יחס סדר (**הסדר של Rees**) על אוסף האידמפוטנטים בחוג: $e \leq f$ אם $ef = fe = e$.

1. הראה שזהו אכן יחס סדר.

2. אם $e \leq f$ אז $Re \subseteq Rf$. אם f מרכזי, גם ההיפך נכון.

3. נאמר שאידמפוטנט e הוא **מחובר** של אידמפוטנט f , אם $f - e$ אידמפוטנט אורתוגונליים. הראה ש- $e \leq f$ אם ורק אם e מחובר של f .

תרגיל 2.2.33 ()** אם e_1, e_2 מתחלפים, אז $e_1 \circ e_2 = e_1 + e_2 - e_1 e_2$ הוא אידמפוטנט, ומתקיים $e_1 \circ e_2 \leq e_1, e_2 \leq e_1 \circ e_2$.

תרגיל 2.2.34 (*) הראה שבקבוצה שכל אבריה מתחלפים, הפעולה $x \circ y = x + y - xy$ היא אסוציאטיבית.

תרגיל 2.2.35 (*)** אם $e_1, \dots, e_n$ אידמפוטנטים מתחלפים, אז $e_1 \circ \dots \circ e_n$ יוצר את האידאל $\langle e_1, \dots, e_n \rangle$. (בהזמנות זו חשב את $e_1 \circ \dots \circ e_n$ כפולינום ב- $e_1, \dots, e_n$, והיזכר בעקרון ההכלה וההפרדה.)

תרגיל 2.2.36 (+)** אם e, e' אידמפוטנטים וגם ee' אידמפוטנט, אז $ee'e, e'ee', e'ee'e$ אידמפוטנטים. יש שמונה אברים (לכל היותר) במוניד e, e' יוצרים, וכולם, פרט אולי ל- e' , הם אידמפוטנטים.

תרגיל 2.2.37 (+)** יהיו e, e' אידמפוטנטים (לאו דווקא מתחלפים). הראה ש- $ee'e + e' - ee'e$ אידמפוטנט אם ורק אם $ee', e'e$ אידמפוטנטים.

תרגיל 2.2.38 ()** אם $e \in R$ אידמפוטנט ו- $I \triangleleft R$, אז גם התמונה $e + I \in R/I$ היא אידמפוטנט. באופן כללי יותר, המעבר לחוג מנה שומר על אידמפוטנטים, על האורתוגונליות ועל יחס הסדר (אלא שאידמפוטנט לא טריוויאלי עשוי להפוך לטריוויאלי בחוג המנה).

אידמפוטנטים מרכזיים בתורת המבנה

הדוגמא הכללית ביותר לאידמפוטנט מרכזי היא אבר יחידה של מחובר ישר של R :

תרגיל 2.2.39 ()** אפשר לפרק את R לסכום ישר $R = R_1 \oplus R_2$, אם ורק אם יש ב- R אידמפוטנט מרכזי. הדרכה. אם $R = R_1 \oplus R_2$, אז $(1, 0)$ הוא אידמפוטנט מרכזי. בכיוון ההפוך, אם e אידמפוטנט מרכזי, אז Re הוא תת-חוג-בלי-יחידה של R , ו- $R \cong Re \oplus R(1 - e)$.

אידמפוטנט שלא ניתן לפרק לסכום של אידמפוטנטים אורתוגונליים נקרא **אידמפוטנט פרימיטיבי** (במלים אחרות, הוא אידמפוטנט מינימלי בין השונים מאפס).

תרגיל 2.2.40 ()** חוג נקרא **אי-פריד** אם אי אפשר לפרק אותו לסכום ישר $R = R_1 \oplus R_2$ (כאשר $R_1, R_2 \neq 0$). הראה ש- R אי-פריד אם ורק אם אין לו אידמפוטנטים מרכזיים. הדרכה. זהו תרגיל 2.2.39.

תרגיל 2.2.41 (+)** (הכללה של תרגיל 2.2.39) הראה שאפשר לפרק את R לסכום ישר $R = R_1 \oplus \dots \oplus R_n$ אם ורק אם יש בו אידמפוטנטים מרכזיים אורתוגונליים $e_1, \dots, e_n$ שסכומם 1. הראה שאפשר לפרק את R לסכום ישר של n תת-חוגים אי-פרידים, אם ורק אם יש בו מערכת של n אידמפוטנטים מרכזיים אורתוגונליים ופרימיטיביים שסכומם 1.

תרגיל 2.2.42 (*)** נתבונן במרחב הוקטורי $V = \text{span}\{e_0, \dots, e_{2^n-1}\}$ מעל שדה F , עם פעולת הכפל $e_i e_j = e_{i \oplus j}$. הראה ש- V איזומורפי, כאלגברה, לסכום הישר $F \oplus \dots \oplus F$.

פירוק פירס

בתת-הסעיף הקודם ראינו שלאידמפוטנטים מרכזיים יש כח לפרק את החוג לסכום ישר. נראה מה אפשר לעשות באידמפוטנטים שאינם מרכזיים.

תרגיל 2.2.43 (+)** נניח ש- $e_1, \dots, e_n \in R$ הם אידמפוטנטים שסכומם 1. נסמן $R_{ij} = e_i R e_j$.

הראה ש- R_{ij} הן חבורות אבליות, ש- $R = \bigoplus R_{ij}$ (סכום ישר של תת-חבורות אבליות), ש- $R_{ij} R_{kl} = 0$ אם $j \neq k$, וש- $R_{ij} R_{jk} \subseteq R_{ik}$. הסק ש- R_{ii} הם תת-חוגים, כאשר e_{ii} הוא אבר היחיד של R_{ii} .

פירוק זה, דמוי הפירוק של מטריצות, נקרא **פירוק פירס** של R .

תרגיל 2.2.44 ()** יהי $R = \bigoplus R_{ij}$ פירוק פירס ביחס לאידמפוטנטים $e_1, \dots, e_n \in R$. אידיאל של R הוא **הומוגני** ביחס לפירוק אם הוא נוצר על-ידי אברים הומוגניים (שהם, לפי ההגדרה, אברים השייכים לאחד המרכיבים (R_{ij})). הראה שכל אידיאל דו-צדדי $I \triangleleft R$ הוא הומוגני. הדרכה: $I = \bigoplus I_{ij}$ כאשר $I_{ij} = e_i I e_j = I \cap A_{ij}$. הראה שכל אידיאל R/I מנה יש פירוק פירס ביחס לאותם אידמפוטנטים (אלא שחלק מהמרכיבים עשויים להתאפס).

תרגיל 2.2.45 (+)** נניח $R = M_n(S)$ הוא חוג מטריצות. הראה שפירוק פירס של R ביחס לאידמפוטנטים $e_{11}, \dots, e_{nn}$ הוא $R = \bigoplus S e_{ij}$.

חוגים בוליאניים

הגדרה 2.2.46 **חוג בוליאני** הוא חוג שכל אבריו אידמפוטנטים.

תרגיל 2.2.47 ()** הראה שבחוג בוליאני $x + x = 0$ לכל x . הראה שכל חוג בוליאני הוא קומוטטיבי.

תרגיל 2.2.48 ()** החוג הבוליאני היחיד שהוא שדה הוא $\mathbb{F}_2 = \{0, 1\}$.

תרגיל 2.2.49 (+)** תהי Ω קבוצה כלשהי. נגדיר על קבוצת החזקה $P(\Omega)$ את הפעולות $a \cdot b = a \cap b$ ו- $a \Delta b = a \cup b$. הראה שמתקבל חוג בוליאני. חוג כזה נקרא **אלגברה הקבוצות** של Ω .

על חוג בוליאני מוגדר יחס הסדר מתרגיל 2.2.32, אם $y \leq x$ אם $xy = y$.

תרגיל 2.2.50 ()** האידיאל הראשי הנוצר על-ידי x הוא $Rx = \{y : y \leq x\}$. הדרכה: אם $y = ax$ ו- $xy = ax^2 = ax = y$ ואם $y \leq x$ ו- $y = yx \in Rx$.

תרגיל 2.2.51 ()** בחוג בוליאני, כל אידיאל נוצר סופית הוא ראשי. הדרכה: תרגיל 2.2.35.

אומרים ש- $x \in R$ הוא **אטום** אם $Rx = \{0, x\}$. כל שני אטומים אורתוגונליים זה לזה.

תרגיל 2.2.52 ()** x הוא אטום ורק אם הוא מינימלי בקבוצת האברים השונים מאפס, אם ורק אם האידיאל Rx מינימלי בקבוצת האידיאלים השונים מאפס.

תרגיל 2.2.53 (+)** יהי R חוג בוליאני. נסמן ב- T את קבוצת האטומים של R . נגדיר $\psi: R \rightarrow P(T)$ לפי $\psi(a) = \{x \in T : x \leq a\}$. הראה ש- ψ הומומורפיזם של חוגים. הדרכה: לכל אבר x , $xa = xb = x$ אם ורק אם $x \leq a$ ו- $x \leq b$; ואם x אטום, $x(a+b) = x$ ו- $x(a+b) = x$ אם ורק אם $xb = x$ ו- $xa = 0$ או $xb = 0$ ו- $xa = x$. הראה שאם R סופי, ψ הוא איזומורפיזם. הדרכה: כשהחוג סופי, בכל אידיאל יש אטומים; ו- $\psi(\sum x_i) = \{x_1, \dots, x_n\}$.

כלומר, כל חוג בוליאני סופי הוא אלגברת הקבוצות של קבוצה מתאימה. במקרה האינסופי ψ שהגדרנו אינה בהכרח שיכון (אולי אין מספיק אטומים מתחת לכל a).

תרגיל 2.2.54 (*)** תן דוגמא לחוג בוליאני בלי אטומים.

עם זאת, לפי משפט ההצגה של Stone, כל חוג בוליאני מוכל באלגברת קבוצות:

תרגיל 2.2.55 (*)** כל חוג בוליאני מוכל באלגברה של קבוצות. הדרכה. יהי R חוג בוליאני. נסמן ב- Ω את קבוצת האידיאלים המקסימליים של R . נגדיר $\varphi: R \rightarrow P(\Omega)$ לפי $\varphi(a) = \{M \in \Omega: a \notin M\}$. הראה שזהו הומומורפיזם של חוגים. הראה שלכל $a \in R$ $0 \neq a$ יש אידיאל מקסימלי M כך ש- $a \in M$ ו- $1 - a \notin M$ (תרגיל 2.2.8, עמ' 50). הסק ש- φ שיקוף.

תרגיל 2.2.56 (-)** תחום שלמות בוליאני הוא שדה מסדר 2.

תרגיל 2.2.57 (-)** חוג מנה של חוג בוליאני הוא בוליאני.

אידיאלים אידמפוטנטיים

יהי R חוג. אידיאל $J \triangleleft R$ הוא **אידיאל אידמפוטנטי** אם $J^2 = J$.

תרגיל 2.2.58 (*)** כל אידיאל אידמפוטנטי נוצר סופית בחוג קומוטטיבי הוא מהצורה $J = Re$ כאשר e אידמפוטנט. הדרכה. כתוב $J = \sum Ra_i$. לפי ההנחה יש מקדמים $b_{ij} \in J$ כך ש- $a_i = \sum_j b_{ij} a_j$; כלומר $A = (b_{ij}) \in M_n(J)$ מקיימת $Av = v$ כאשר $v = (a_1, \dots, a_n)^t$. נסמן $\epsilon = 1 - \det(1 - A)$. מכיון ש- $(1 - A)v = 0$, מתרגיל 1.3.20 מקבלים $(1 - \epsilon)v = 0$ ולכן $(1 - \epsilon)J = 0$. מאידך $A \equiv 0 \pmod{J}$, ולכן $\det(1 - A) \equiv 1 \pmod{J}$ ו- $\epsilon \in J$. הראינו ש- $(1 - \epsilon)J = 0$ ולכן $\epsilon \in (1 - \epsilon)J$ ואידמפוטנט; אבל $\epsilon R \subseteq J = \epsilon J \subseteq \epsilon R$.

תרגיל 2.2.59 (*)** מצא אידיאל אידמפוטנטי בתחום שלמות, שאינו נוצר סופית. הדרכה. בנה תחום ובו סדרת אידיאלים ראשיים $J_0, J_1, \dots$ כך ש- $J_n^2 = J_{n-1}$, והתבונן ב- $J = \sum J_n$.

2.3 חוגים מקומיים

הגדרה 2.3.1 חוג קומוטטיבי שיש לו אידיאל מקסימלי יחיד נקרא **חוג מקומי**.

תרגיל 2.3.2 ()** יהי M האידיאל המקסימלי של חוג מקומי (קומוטטיבי) R . אז $R^\times = R - M$, כלומר x הפיך אם ורק אם $x \notin M$ (ראה תרגיל 2.1.8, עמ' 46).

תרגיל 2.3.3 (+)** אם $M \triangleleft R$ אידיאל מקסימלי שכל אבריו נילפוטנטיים, אז M הוא האידיאל המקסימלי היחיד של R . הדרכה. תרגיל 1.1.45 (עמ' 15). הערה. אידיאל שכל אברו נילפוטנטיים נקרא אידיאל נילי.

טענה 2.3.4 התכונות הבאות של חוג קומוטטיבי שקולות זו לזו:

1. החוג מקומי;
2. מכל שני אברים שסכומם 1, לפחות אחד מוכרח להיות הפיך;
3. אוסף האברים הלא-הפיכים סגור לחיבור.

הוכחה. $1 \Leftarrow 2$: יהי R חוג מקומי, מקומי ו- $x + y = 1$; אם x, y לא הפיכים אז Rx, Ry אידיאלים אמיתיים ולכן מוכלים באידיאל המקסימלי היחיד M , אבל אז $1 = x + y \in M$, סתירה. $2 \Leftarrow 3$: אם x, y לא הפיכים ו- $x + y = u$ הפיך, אז $u^{-1}x + u^{-1}y = 1$ כאשר $u^{-1}x$ ו- $u^{-1}y$ לא הפיכים. $3 \Leftarrow 1$: יהיו M, M' אידיאלים מקסימליים שונים, אז $1 \in R = M + M'$ בסתירה להנחה שאוסף הלא-הפיכים סגור לחיבור. $\square$

תרגיל 2.3.5 (*)** לכל $M \triangleleft R$ מקסימלי ולכל $n > 1$, R/M^n מקומי. בפרט, לכל n , החוג $\mathbb{Q}[\epsilon]/\langle \epsilon^n \rangle$ הוא מקומי. (הכללה של דוגמא זו מופיעה בתרגיל 4.1.5 (עמ' 109).)

תרגיל 2.3.6 (*)** יהי F שדה. הראה שחוג טורי החזקות הפורמליים $F[[x]]$ הוא חוג מקומי, שהאידיאל המקסימלי היחיד שלו הוא $\langle x \rangle$. הדרכה. משפט 3.4.58.

תרגיל 2.3.7 ()** החוג $R = \bigcup F[x^{1/n!}]$ מתרגיל 1.3.78 אינו מקומי; השווה לחוג $S = \bigcup F[[x^{1/n!}]]$ מתרגיל 2.1.7 (עמ' 46) שהוא כן מקומי.

נתבונן באוסף כל הסכומים מהצורה $\sum_{i=0}^{\infty} a_i p^i$ כאשר $a_i \in \mathbb{Z}$. לכל n , השארית של הסכום מודולו p^n מוגדרת היטב. נאמר ששני סכומים הם שווים אם השאריות שלהם מודולו p^n שוות, לכל n . את אוסף הסכומים המוגדרים באופן זה מסמנים ב- $\mathbb{Z}_p$.

תרגיל 2.3.8 ()** הראה שכל אבר של $\mathbb{Z}_p$ אפשר להציג באופן יחיד בצורה $\sum_{i=0}^{\infty} a_i p^i$ עם $a_i \in \{0, \dots, p-1\}$.

תרגיל 2.3.9 (*)** הראה ש- $\mathbb{Z}_p$, עם פעולות החיבור והכפל המוגדרות בדומה לאלו של $\mathbb{Z}[[x]]$, הוא חוג קומוטטיבי (שים לב להבדל בהגדרת השוויון בין החוגים: ב- $\mathbb{Z}[[x]]$ אם שני אברים שווים, כל המקדמים שלהם שווים; ראה תרגיל 2.3.14).

תרגיל 2.3.10 (*)** הראה ש- $\mathbb{Z}_p$ הוא הגבול ההפוך של סדרת החוגים $\mathbb{Z}/p\mathbb{Z} \leftarrow \mathbb{Z}/p^2\mathbb{Z} \leftarrow \mathbb{Z}/p^3\mathbb{Z} \leftarrow \dots$ (ראה הגדרה 1.3.80).

תרגיל 2.3.11 (*)** הראה שכל אבר ב- $\mathbb{Z}_p$ אפשר להציג באופן יחיד כסכום $\sum_{i=0}^{\infty} a_i p^i$ עם מקדמים $a_i \in \{0, \dots, p-1\}$.

תרגיל 2.3.12 ()** הראה שההעתקה $\mathbb{Z} \rightarrow \mathbb{Z}_p$ המוגדרת על-ידי פיתוח לפי בסיס p , היא שיכון. הדרכה. שים לב ש- $1 + \sum_{i=0}^{\infty} (p-1)p^i = 0$. הראה שבתמונה $\mathbb{Z}_p$, כל מספר שלם זר ל- p הוא הפיך.

תרגיל 2.3.13 ()** הוכח ש- $\mathbb{Z}_p$ הוא חוג מקומי, שהאידיאל המקסימלי היחיד שלו נוצר על-ידי p . כל אידיאל של $\mathbb{Z}_p$ הוא מהצורה $p^n \mathbb{Z}_p$ לאיזשהו n (השווה לתרגיל 3.4.59, עמ' 104).

תרגיל 2.3.14 (*)** הראה ש- $\mathbb{Z}_p$ $\cong \mathbb{Z}[[x]]/\langle x-p \rangle$.

תרגיל 2.3.15 (*)** הראה בעזרת תרגיל 2.3.10 ש- $\mathbb{Z}_2 \times \mathbb{Z}_3 \cong \lim_{\leftarrow} (\mathbb{Z}/12^n \mathbb{Z})$.

שדה המספרים הממשיים

תרגיל 2.3.16 ()** לכל שדה סדור F יש שיכון יחיד $\mathbb{Q} \hookrightarrow F$.

תרגיל 2.3.17 ()** התכונות הבאות של שדה סדור F הן שקולות:

1. לכל $a > 0$ יש $n \in \mathbb{N}$ כך ש- $\frac{1}{n} < a$;
2. לכל a יש $n \in \mathbb{N}$ כך ש- $a < n$;
3. לכל $a, b > 0$ יש $n \in \mathbb{N}$ כך ש- $a < nb$.

שדה בעל תכונות אלה נקרא **ארכימדי**.

תרגיל 2.3.18 (*) תת-שדה של שדה ארכימדי הוא ארכימדי.

תרגיל 2.3.19 ()** יהיו $F \subseteq K$ שדות סדורים. אבר של K הוא **אינסופי** (ביחס ל- F) אם הוא גדול מכל אבר של F , ו**אינפיניטיסימלי** (ביחס ל- F) אם הוא קטן בערכו המוחלט מכל אבר חיובי של F . $a \in K$ אינסופי אם ורק אם a^{-1} אינפיניטיסימלי. אם אין אברים כאלה, ההרחבה **חסומה**. ההרחבה חסומה של הרציונליים אינה אלא שדה ארכימדי.

נניח ש- F תת-שדה של K . הראה שהאוסף R של אברים סופיים של K הוא חוג מקומי, ושאוסף האינפיניטיסימלים $\mathcal{E}$ הוא האידיאל המקסימלי של R . הראה שיש שיכון $F \hookrightarrow R/\mathcal{E}$, וזו ההרחבה חסומה.

סדרת אברים $x_1, x_2, \dots$ בשדה סדור **מתכנסת ל- x** אם לכל $0 < \epsilon$ (בשדה!) יש N כך שאם $n > N$ אז $|x_n - x| < \epsilon$. הסדרה **מתכנסת** אם יש x שהיא מתכנסת אליו. הסדרה נקראת **סדרת קושי** אם לכל $0 < \epsilon$ יש N כך שאם $n, n' > N$ אז $|x_n - x_{n'}| < \epsilon$. אם השדה ארכימדי, אפשר להניח בכל המקרים ש- $\epsilon = \frac{1}{m}$ כאשר m מספר טבעי. שדה סדור הוא **שלם במובן של סדרות** אם כל סדרת קושי מתכנסת.

תרגיל 2.3.20 (+)** יהיו $R \subseteq \mathbb{Q}^{\mathbb{N}}$ האוסף של סדרות קושי מעל $\mathbb{Q}$, $M \subseteq R$ האוסף של סדרות המתכנסות לאפס, ו- $J \subseteq M$ האוסף של סדרות המתאפסות לבסוף. הוכח ש- R הוא חוג, ו- $J, M \triangleleft R$.

טענה 2.3.21 החוג R/J (פתרגיל 2.3.20) הוא מקומי, ו- M/J הוא האידיאל המקסימלי היחיד שלו.

הוכחה. לפי תרגיל 2.1.2 (עמ' 45) די להראות שכל אבר של R/J שאינו ב- M/J הוא הפיך. אם $(x_n) + J \in R/J$ ו- $(x_n) \notin M$ אז אפשר להחליף את (x_n) בנציג ללא אפסים. סדרת קושי שאינה מתכנסת לאפס חסומה הרחק מאפס, ולכן $(x_n^{-1}) \in R$. $\square$

הגדרה 2.3.22 שדה השאריות $\mathbb{R} = R/M \cong (R/J)/(M/J)$ נקרא **שדה המספרים הממשיים**.

תרגיל 2.3.23 (-)** (המשך לטענה 2.3.21) נסמן ב- R^+ את קבוצת הסדרות בחוג R שכמעט כל אבריהן חיוביים.

1. יהי $x \in R-M$; אז $x \in R^+$ או $-x \in R^+$, אבל לא שניהם. הדרכה. תחילה הוכח שאם בסדרת קושי יש אינסוף אברים חיוביים ואינסוף אברים שליליים, אז היא מתכנסת לאפס.

2. אם $x \in R-M$ הוא אבר של R^+ אז $x + M \subseteq R^+$.

3. היחס " $x > y$ " אם $x \neq y$ ו- $x - y \in R^+$ מוגדר היטב על R/M .

טענה 2.3.24 $\mathbb{R}$ הוא שדה סדור לגבי יחס הסדר המוגדר בתרגיל 2.3.23.

תרגיל 2.3.25 (***) (בהמשך לתרגיל 2.3.20)

1. ההעתקה $a \mapsto (a, a, \dots)$ השולחת כל מספר לסדרה הקבועה המתאימה, מהווה שיכון $\mathbb{Q} \hookrightarrow R$.

2. $\mathbb{Q} + M$ הוא תת-החוג של R שאבריו הם הסדרות המתכנסות.

3. הראה שהשיכון האלכסוני $\mathbb{Q} \hookrightarrow R$ ממשיך לשיכון

$$\mathbb{Q} = \mathbb{Q}/(\mathbb{Q} \cap M) \cong (\mathbb{Q} + M)/M \hookrightarrow R/M = \mathbb{R}.$$

תרגיל 2.3.26 (***) $\mathbb{R}$ ארכימד.

משפט 2.3.27 $\mathbb{R}$ שדה סדור שלם במובן של סדרות.

תרגיל 2.3.28 (*)** הוכח את משפט 2.3.27 (משפט זה נשאר נכון כאשר מחליפים בבניה את $\mathbb{Q}$ בכל שדה סדור $(F, +, \cdot)$). **פתרון.** תהי $\alpha^1, \alpha^2, \dots \in R/M$ סדרת קושי. בחר נציגים $\alpha^m = (x_n^m) + M$, כאשר לכל m $(x_1^m, x_2^m, \dots)$ היא סדרת קושי. לכל m קיים N_m כך ש- $|x_n^m - x_{n'}^m| < \frac{1}{m}$ לכל $n, n' \geq N_m$; נבחר $y_m = x_{N_m}^m$ ונסמן $\beta = (y_1, y_2, \dots)$.

1. $\beta \in R$. הוכחה: נקבע m . לפי ההנחה קיים N_0 כך שלכל $m', m'' \geq N_0$, $|\alpha^{m'} - \alpha^{m''}| < \frac{1}{m}$. לפי הגדרת יחס הסדר ב- R פירושו של דבר הוא שלכל m', m'' קיים $N_{m', m''} \geq N_m, N_{m'}, N_{m''}$ כך ש- $|x_n^{m'} - x_n^{m''}| < \frac{1}{m}$ עבור $n \geq N_{m', m''}$. בפרט $|x_{N_{m'}}^{m'} - x_{N_{m''}}^{m''}| = |y_{m'} - y_{m''}|$ קטן או שווה לסכום $|x_{N_{m'}}^{m'} - x_{N_{m', m''}}^{m'}| + |x_{N_{m', m''}}^{m'} - x_{N_{m', m''}}^{m''}| + |x_{N_{m', m''}}^{m''} - x_{N_{m''}}^{m''}| \leq \frac{3}{m}$.

2. β מוגדר היטב ב- R/M . הוכחה: הסדרה (y_m) אמנם תלויה בנציגים, אבל לכל m , אם $\alpha^m = (x_n^m) + M$ ו- N_m' מוגדר לפי (x_n^m) בדומה להגדרת N_m לפי (x_n^m) , אז קיים $N_0 > N_m, N_m'$ כך ש- $|x_n^m - x_n^{m'}| < \frac{1}{m}$ לכל $n \geq N_0$, ואז $|y_m - y_{m'}| \leq \frac{3}{m}$. לכן $(y_m) - (y_{m'}) \in M$.

3. $\alpha^1, \alpha^2, \dots \rightarrow \beta$. הוכחה: יהי $m \in \mathbb{N}$. מכיוון ש- $(\alpha^1, \alpha^2, \dots)$ היא סדרת קושי, קיים $N > m$ כך ש- $|\alpha^n - \alpha^{n'}| < \frac{1}{m}$ לכל $n, n' \geq N$. יהי $n \geq N$. נוכיח ש- $|\alpha^n - \beta| < \frac{3}{m}$. לשם כך די להוכיח ש- $|x_k^n - \beta_k| < \frac{3}{m}$ לכל $k \geq \max\{N, N_n\}$. מכיוון ש- $\beta_k = x_{N_k}^k$, קיים N_{nk} כך שלכל $n, k \geq N_{nk}$, $|x_k^n - x_{N_k}^k| < \frac{1}{m}$. כעת נבחר $N' = \max\{N_{nk}, N_n, N_k\}$, ואז $|x_k^n - x_{N_k}^k| \leq |x_k^n - x_{N'}^n| + |x_{N'}^n - x_{N'}^k| + |x_{N'}^k - x_{N_k}^k| < \frac{1}{n} + \frac{1}{m} + \frac{1}{k} < \frac{3}{m}$.

קבוצה A בשדה סדור היא **חסומה מלעיל** אם קיים t כך ש- $a < t$ לכל $a \in A$.
אבר t הוא **חסם עליון** של A אם t חסם מלעיל שלה, ואף $s < t$ אינו חסם מלעיל.
כשהוא קיים, חסם עליון הוא יחיד. שדה סדור הוא **שלם במובן של חסמים** אם לכל קבוצה חסומה מלעיל יש חסם עליון.

משפט 2.3.29 שדה סדור הוא שלם במובן של חסמים אם ורק אם הוא גם ארכימדי וגם שלם במובן של סדרות.

תרגיל 2.3.30 (-)** הוכח את המשפט. פתרון. נניח ש- F שלם במובן של חסמים. נניח שסדרת המספרים הטבעיים חסומה מלעיל, אז יש לה חסם עליון t ; גם $t - 1$ הוא חסם מלעיל של הקבוצה, וזו סתירה להנחה ש- t חסם עליון. מכאן שהשדה ארכימדי.
נניח ש- $\{x_n\}$ סדרת קושי; לכל i נסמן ב- t_i את החסם התחתון של הקבוצה $\{x_i, x_{i+1}, \dots\}$ (לכל קבוצה חסומה מלעיל יש חסם תחתון). נסמן ב- t את החסם העליון של הקבוצה $\{t_1, t_2, \dots\}$. לכל n קיים i כך ש- $t - 1/n < t_i \leq t$, וקיים m_n כך ש- $t_i \leq x_{m_n} < t_i + 1/n$. לכן $t - 1/n < x_{m_n} < t + 1/n$, ותת-הסדרה x_{m_n} מתכנסת ל- t . לכן גם הסדרה x_n מתכנסת לאותו גבול.

נעת נניח ש- F שדה סדור ארכימדי, ושהוא שלם במובן של סדרות. תהי A קבוצה חסומה מלעיל. בגלל הארכימדיות, לכל n , קיים חסם מלעיל t_n של הקבוצה כך ש- $t_n - 1/n$ אינו חסם מלעיל. הסדרה המתקבלת היא סדרת קושי, שגבולה הוא חסם עליון של A .

מסקנה 2.3.31 $\mathbb{R}$ שלם במובן של חסמים.

משפט 2.3.32 שדה ארכימדי המכיל שדה שלם, שווה לו.

תרגיל 2.3.33 ()** הוכח את המשפט: אם $F \subseteq K$ שדות ארכימדיים ו- F שלם, $F = K \cap F$. פתרון. יהי $x \in K$. לפי הארכימדיות של K קיים $n \in \mathbb{N}$ כך ש- $x < n$, ולכן n חסם מלעיל של הקבוצה $A = \{a \in F : a < x\}$. מכיוון ש- F שלם, יש לקבוצה זו חסם עליון $t \in F$. אם $x > t$ אז קיים n טבעי כך ש- $t + \frac{1}{n} < x$ ואז $t + \frac{1}{n} \in A$, בסתירה להגדרת t . אם $x < t$ אז קיים n טבעי כך ש- $t - \frac{1}{n} < x$, אולם $t - \frac{1}{n} \in A$, שוב סתירה להגדרת t . לכן $x = t \in F$.

תרגיל 2.3.34 (*)** יהי F שדה סדור ארכימדי. אפשר לחזור על הבניה של $\mathbb{R} = \mathbb{R}_Q$ ו- $M = M_Q, R = R_Q$ שבתרגיל 2.3.20 וטענה 2.3.21 עם F במקום $\mathbb{Q}$, ולבנות את השדה $\mathbb{R}_F = R_F/M_F$. הראה שבכל המקרים מתקבל אותו שדה. פתרון. $\mathbb{R}_F$ הוא ארכימדי שלם לפי ההוכחה של טענה זו בתרגיל 2.3.28 עבור $\mathbb{R}_Q$. השיכון $Q \hookrightarrow F$ מגדיר שיכון $R_Q \hookrightarrow R_F$ שעבורו $M_Q = M_F \cap R_Q$, ולכן (תרגיל 2.1.12) מגדיר שיכון $\mathbb{R}_Q \hookrightarrow \mathbb{R}_F$. לפי משפט 2.3.32, $\mathbb{R}_F = \mathbb{R}_Q = \mathbb{R}$.

משפט 2.3.35 כל שדה ארכימדי מוכל ב- $\mathbb{R}$.

תרגיל 2.3.36 ()** הוכח את המשפט. פתרון. בדומה לשיכון $Q \hookrightarrow \mathbb{R}_Q$ של תרגיל 2.3.25 יש שיכון $F \hookrightarrow \mathbb{R}_F$, ולפי תרגיל 2.3.34, $\mathbb{R}_F = \mathbb{R}_Q = \mathbb{R}$.

מסקנה 2.3.37 יש שדה ארכימדי שלם אחד ויחיד.

הוכחה. יהי F ארכימדי ושלם. לפי משפט 2.3.35, $F \subseteq \mathbb{R}$, ולפי משפט 2.3.34 יש שוויון. $\square$

לסיכום, השדה $\mathbb{R}$ של הגדרה 2.3.25 הוא השדה הסדור הארכימדי השלם היחיד.

תרגיל 2.3.38 (-)** (בהמשך לתרגיל 2.3.20)

1. נסמן ב- I_n את אוסף הסדרות ב- R המתאפסות בקואורדינטה ה- n . הוכח ש- $R/I_n \cong \mathbb{Q}$, ולכן I_n הם אידיאלים מקסימליים של R (מכאן ש- R אינו מקומי).

2. נסמן $J_n = I_{n+1} \cap I_{n+2} \cap \dots$. הראה שלכל n , $R/J_n \cong R$.

3. הראה ש- $J = \bigcup_{n \geq 1} J_n$.

4. כל ה- I_n קו-מקסימליים ביחס ל- J .

תרגיל 2.3.39 (*)** הראה שבתרגיל 2.3.20, $M^2 = M$.

תרגיל 2.3.40 ()** נסמן ב- $S \subseteq R$ את אוסף הסדרות המתכנסות לאבר של $\mathbb{Q}$. הראה ש- S/J חוג מקומי שהאידיאל המקסימלי שלו הוא M/J , ושההטלה $S \rightarrow S/M = \mathbb{Q}$ היא אופרטור הגבול (ראה תרגיל 2.3.25).

תרגיל 2.3.41 (*)** נסמן ב- B את אוסף הסדרות החסומות מעל $\mathbb{Q}$. הראה ש- $J \subset M \subset S \subset R \subset B \subset \mathbb{Q}^{\mathbb{N}}$ (על-פי ההגדרות בתרגילים 2.3.20, 2.3.40), ו- J אידיאל של $\mathbb{Q}^{\mathbb{N}}$ ו- M אידיאל של B .

התרגילים האחרונים בסעיף זה יכולים לשמש מבוא לאנליזה לא סטנדרטית. **מסנן** (על $\mathbb{N}$) הוא אוסף לא ריק $\mathcal{F} \subseteq \mathcal{P}(\mathbb{N})$ של תת-קבוצות, הסגור לחיתוך סופי ולהגדלה, ושאינו כולל את הקבוצה הריקה.

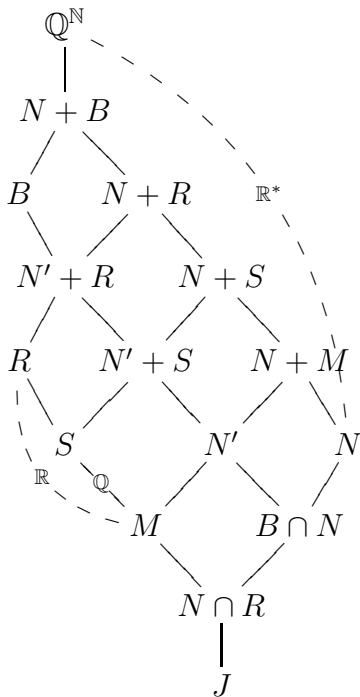
תרגיל 2.3.42 (*) אם T קבוצה לא ריקה, הראה שאוסף כל הקבוצות $\mathcal{F}_T = \{A : T \subseteq A\}$ הוא מסנן. מסנן כזה נקרא **מסנן עיקרי**. מסנן הוא עיקרי אם ורק אם חיתוך כל הקבוצות בו אינו ריק.

תרגיל 2.3.43 (*) הראה שאוסף הקבוצות שהמשלים שלהן סופי הוא מסנן. זהו **המסנן הקו-סופי**.

מסנן $\mathcal{F}$ הוא **על-מסנן** אם לכל קבוצה $A \subseteq \mathbb{N}$, הוא מכיל את A או את A^c .

תרגיל 2.3.44 (*)** הוכח שקיים על-מסנן לא עיקרי. **הדרכה**: העזר בלמה של צורן כדי לבנות על-מסנן המכיל את המסנן הקו-סופי.

תרגיל 2.3.45 ()** בעל-מסנן לא עיקרי, כל קבוצה היא אינסופית.



תרגיל 2.3.46 (*)** יהי $\mathcal{F}$ על-מסנן לא עיקרי. עבור $A \in \mathcal{F}$ ו- $(x_n) \in \mathbb{Q}^{\mathbb{N}}$, נסמן ב- x_A את הסדרה

$$(x_A)_n = \begin{cases} x_n & n \in A \\ 0 & n \notin A \end{cases}$$

$\mathbb{Q}^{\mathbb{N}}$ נסמן $x_n \stackrel{\mathcal{F}}{=} y_n$ אם קיים $A \in \mathcal{F}$ כך ש- $x_A = y_A$ (כלומר $\{n: x_n = y_n\} \in \mathcal{F}$). נסמן $x_n \xrightarrow{\mathcal{F}} 0$ אם קיים $A \in \mathcal{F}$ כך ש- $(x_A)_n \rightarrow 0$.

1. הראה ש- $N = \{(x_n) \in \mathbb{Q}^{\mathbb{N}}: x_n \stackrel{\mathcal{F}}{=} 0\}$ הוא אידיאל מקסימלי של $\mathbb{Q}^{\mathbb{N}}$; שדה המנה $\mathbb{Q}^{\mathbb{N}}/N$, שאפשר לסדר, הוא מודל לא סטנדרטי של הממשיים. הראה גם ש- $J \subseteq N \cap R \subseteq M$.

הדרכה. לכל $A \in \mathcal{F}$ ולכל סדרה, $x - x_A \in N$.

2. הראה ש- $N'' = \{(x_n) \in \mathbb{Q}^{\mathbb{N}}: x_n \xrightarrow{\mathcal{F}} 0\} = M + N$.

3. הראה ש- $N' = \{(x_n) \in B: x_n \xrightarrow{\mathcal{F}} 0\}$ ובפרט $N' \triangleleft B$. הוכח ש- $N' \cap B = M + N \cap B$ (לפי ההגדרה בתרגיל 2.4.24, עמ' 65).

4. מצא שיכון $\mathbb{R} = R/M \hookrightarrow B/N'$, והראה ש- B/N' איזומורפי לחוג מנה של תת-החוג $(B+N)/N$ של $\mathbb{Q}^{\mathbb{N}}/N$.

מסמנים $B \subseteq^* A$ אם $|A - B| < \infty$ (זה יחס טרנזיטיבי). על-מסנן נקרא **נקודת- P** אם כל שרשרת יורדת בו, לגבי היחס $\subseteq^*$, היא חסומה מלמעלה.

תרגיל 2.3.47 (*)** בהמשך לתרגיל 2.3.46. הראה שאם $\mathcal{F}$ הוא נקודת- P , אז $B = R + N'$. הדרכה. תהי $(x_n) \in B$ סדרה חסומה, הנמצאת בקטע Δ_0 . נסמן $U_0 = \mathbb{N} \in \mathcal{F}$. נחלק את הקטע Δ_0 לשני חלקים שווים אורך, $\Delta_0 = \Delta_1 \cup \Delta'_1$. נסמן $U_1 = \{n \in U_0: x_n \in \Delta_1\}$ ו- $U'_1 = U_0 - U_1$. על-ידי החלפת החצאים זה בזה אם יש צורך, נוכל להניח ש- $U_1 \in \mathcal{F}$. באופן כזה נגדיר סדרה יורדת של קבוצות $U_n \in \mathcal{F}$. לפי ההנחה על המסנן, יש $V \in \mathcal{F}$ כך ש- $V \subseteq^* U_n$ לכל n . הסדרה x_V היא סדרת קושי, משום שלכל n , כל אבריה פרט למספר סופי שייכים ל- Δ_n ; לכן $x = x_V + (x - x_V) \in R + N \cap B = R + N'$.

תרגילים נוספים אודות מסננים:

תרגיל 2.3.48 ()** על-מסנן אינו עיקרי אם ורק אם הוא מכיל את המסנן הקו-סופי. הדרכה. על-מסנן שאינו מכיל את המסנן הקו-סופי, כולל קבוצה סופית.

תרגיל 2.3.49 ()** מסנן הוא על-מסנן אם ורק אם הוא מסנן מקסימלי.

תרגיל 2.3.50 ()** אם $\mathcal{F}$ על-מסנן עיקרי ו- $A \cup B \in \mathcal{F}$, אז $A \in \mathcal{F}$ או $B \in \mathcal{F}$.

תרגיל 2.3.51 ()** בכל על-מסנן לא עיקרי יש סדרה יורדת, לגבי יחס ההכללה, שהחיתוך שלה ריק (ולכן לא ניתן להכליל את ההגדרה של נקודת- P ולדרוש שיהיה במסנן חסם תחתון ביחס להכללה).

תרגיל 2.3.52 (*) היחס $=^*$, המוגדר כך ש- $A =^* B$ אם ורק אם $A \subseteq^* B \subseteq^* A$, הוא יחס שקילות. כל מחלקת שקילות היא בת-מניה.

תרגיל 2.3.53 ()** יהי $\mathcal{F}$ מסנן עיקרי לא ראשי. אם $A \in \mathcal{F}$ ו- $B =^* A$ אז $B \in \mathcal{F}$.

תרגיל 2.3.54 (*)** תהי S קבוצת אינדקסים, ונניח שלכל $s \in S$, $\mathcal{F}_s$ הוא מסנן. יהי $\mathcal{G}$ מסנן על S . אז $\int_{\mathcal{G}} \mathcal{F} = \bigcup_{G \in \mathcal{G}} \bigcap_{s \in G} \mathcal{F}_s$ הוא מסנן. אם $\mathcal{G}$ עיקרי עם חיתוך $\int_{\mathcal{G}} \mathcal{F} = \mathcal{F}_x$ אז $\{x\}$.

מסננים וחוגים בוליאניים

תהי X קבוצה. אם $\mathcal{F} \subseteq P(X)$, נסמן ב- $\bar{\mathcal{F}} = \{A^c : A \in \mathcal{F}\}$ את קבוצת המשלימים.

תרגיל 2.3.55 ()** הקבוצה $\mathcal{F}$ היא מסנן על X , אם ורק אם $\bar{\mathcal{F}}$ היא אידיאל אמיתי של החוג $P(X)$ מתרגיל 2.2.49 (עמ' 54). הדרכה. העזר בזכות $A \Delta (A - B) = A \cup B$: קבוצה $I \subseteq P(X)$ היא אידיאל אם ורק אם I סגורה כלפי מטה וביחס לפעולת ההפרש הסימטרי; אם ורק אם היא סגורה כלפי מטה ולא־חוד.

תרגיל 2.3.56 ()** $\mathcal{F}$ הוא על-מסנן על X , אם ורק אם $\bar{\mathcal{F}}$ אידיאל ראשוני. הדרכה. $\mathcal{F}$ על-מסנן אם ורק אם $\mathcal{F} \cup B^c \subseteq \mathcal{F}$ מבע $A^c \in \mathcal{F}$ או $B^c \in \mathcal{F}$; אם ורק אם $\bar{\mathcal{F}}$ מבע $A \cap B \in \bar{\mathcal{F}}$ או $B \in \bar{\mathcal{F}}$.

2.4 אידיאלים ראשוניים

2.4.1 חוגים ראשוניים

הגדרה 2.4.1 חוג R הוא ראשוני אם לכל שני אידיאלים A, B , אם $AB = 0$ אז בהכרח $A = 0$ או $B = 0$.

הגדרה שקולה: החוג ראשוני אם מ- $A, B \neq 0$ נובע $AB \neq 0$.

תרגיל 2.4.2 ()** כל חוג פשוט הוא ראשוני. הדרכה. אין לו אידיאלים $\neq 0$.

תרגיל 2.4.3 ()** חוג R הוא ראשוני אם ורק אם לכל $a, b \neq 0$ קיים $x \neq 0$ כך ש- $axb \neq 0$ (ובמילים אחרות, אם $aRb = 0$ גורר $a = 0$ או $b = 0$).

תרגיל 2.4.4 ()** כל תחום הוא חוג ראשוני. הדרכה. אם $A, B \neq 0$ יש $a \in A$ ו- $0 \neq b \in B$ ו- $ab \in AB \neq 0$.

תרגיל 2.4.5 ()** בחוג ראשוני R , כל אידיאל שמאלי נחתך עם כל אידיאל ימני. הדרכה. יהיו $R \leq_\ell L$ ו- $R \leq_r A$ אידיאלים שונים מאפס, אז $RA, LR \subseteq R$ ולכן $RALR \neq 0$; מכאן ש- $L \subseteq A$ ו- $0 \neq AL \subseteq A \cap L$ (השווה לתרגיל 1.2.42, עמ' 25).

הגדרה 2.4.6 יהי R חוג עם מרכז $Z = Z(R)$, ויהי $S \subseteq R$ תת-חוג. בתרגיל 1.2.45 (עמ' 26) ראינו ש- ZS הוא תת-חוג של R . אם $R = ZS$, אומרים ש- R הוא הרחבה מרכזית של S .

תרגיל 2.4.7 (*) יהי $S \subseteq R$ תת-חוג. אז R היא הרחבה מרכזית של S אם ורק אם קיימת קבוצה $Z_0 \subseteq Z(R)$ כך ש- $R = S[Z_0]$.

משפט 2.4.8 אם לחוג S יש הרחבה מרכזית שהיא חוג פשוט, אז S ראשוני.

הוכחה. תהי $R = ZS$ ההרחבה המרכזית של S , כאשר $Z = Z(S)$. לכל אידיאל $A \triangleleft S$, $ZA \triangleleft R$ מכיוון ש- $Z(SA) = Z(S)A = Z(ZS)A = Z(S)(ZA) = Z(S)(ZA)R = R(ZA)R$. יהיו $0 \neq A, B \triangleleft S$; מכיוון ש- R פשוט, $ZA = ZB = R$, ולכן $ZAB = ZAZB = R^2 = R$, ולכן $AB \neq 0$. $R \neq 0$. $\square$

תרגיל 2.4.9 (*)** הוכח ש- $M_n(\mathbb{Z})$ הוא חוג ראשוני שאינו פשוט (אם $n > 1$) אינו תחום.

תרגיל 2.4.10 ()** תהי R הרחבה מרכזית של S . אם $P \triangleleft R$ ראשוני, אז גם $P \cap S \triangleleft S$ ראשוני. הדרכה. יהיו $a, b \in S$ כך ש- $aSb \subseteq P \cap S$. אז $aSb \subseteq (P \cap S)Z \subseteq (P \cap S)R = P \cap R = P$. ולכן $a \in P$ או $b \in P$.

טענה 2.4.11 בין החוגים הקומוטטיביים, החוגים הראשוניים הם בדיוק תחומי השלמות.

הוכחה. יהי R חוג קומוטטיבי ראשוני. אם $ab = 0$ אז $(Ra)(Rb) = 0$ ולכן $Ra = 0$ או $Rb = 0$. הכיוון ההפוך הוא תרגיל 2.4.4. $\square$

תרגיל 2.4.12 (*)** המרכז של חוג ראשוני הוא תחום שלמות.

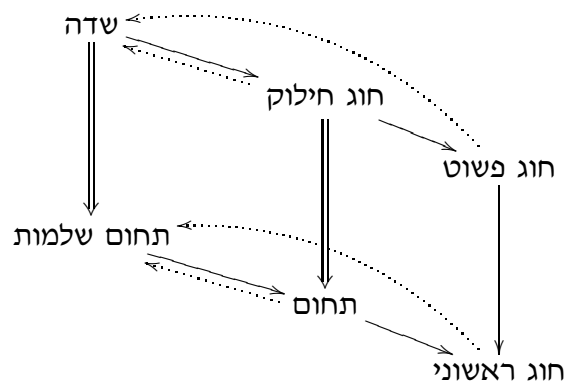
תרגיל 2.4.13 (*)** הראה ש- $M_2(F) \not\subseteq \left\{ \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \right\}$, כאשר F שדה, הוא תת-חוג של חוג פשוט שאינו ראשוני.

תרגיל 2.4.14 (*)** הראה שאיחוד על-פני שרשרת של חוגים ראשוניים הוא חוג ראשוני. הערה. השווה לתרגיל 2.1.30 (עמ' 48).

באור 2.1 מופיעות כל משפחות החוגים שפגשנו עד כה. $\alpha \longrightarrow \beta$ פירושו שכל α הוא β . $\alpha \implies \beta$ פירושו שכל תת-חוג של חוג מטיפוס α (ובפרט החוג עצמו) הוא β . בסימון $\alpha \dashrightarrow \beta$ מתלכדות, במקרה, שתי משמעויות: המרכז של α הוא β , וכל חוג קומוטטיבי מטיפוס α הוא β .

תרגיל 2.4.15 ()** חוג בלי יחידה הוא ראשוני אם הוא מקיים את הגדרה 2.4.1. הראה שכל אידיאל של חוג ראשוני הוא ראשוני (כחוג בלי יחידה).

תרגיל 2.4.16 ()** בהמשך לתרגיל 2.4.15, נתבונן בחוג בלי יחידה $R = \mathbb{Z}\epsilon$, שהכפל מוגדר בו לפי החוק $\epsilon^2 = \epsilon$. הראה ש- R ראשוני אבל R^1 (שהוגדר בתרגיל 1.2.78, עמ' 30) אינו ראשוני.



איור 2.1: טיפוסים חוגים שפגשנו עד כה (משמעותם של החצים מוסברת בטקסט)

2.4.2 אידיאלים ראשוניים

הגדרה 2.4.17 אידיאל $P \triangleleft R$ הוא ראשוני אם לכל שני אידיאלים $A, B \triangleleft R$, אם $AB \subseteq P$ אז $A \subseteq P$ או $B \subseteq P$.

מכיוון שזהו מושג מרכזי, כדאי להכיר כמה הגדרות שקולות שלו:

תרגיל 2.4.18 ()** התכונות הבאות שקולות עבור אידיאל $P \triangleleft R$:

1. P ראשוני.

2. לכל שני אידיאלים $A \not\subseteq P$ ו- $B \not\subseteq P$, מתקיים $AB \not\subseteq P$.

3. אם $AB \subseteq P$ אז $A \subseteq P$ או $B \subseteq P$.

4. אם $A \not\subseteq P$ ו- $AB \subseteq P$ אז $B \subseteq P$.

5. אם $B \not\subseteq P$ ו- $AB \subseteq P$ אז $A \subseteq P$.

תרגיל 2.4.19 (+)** $P \triangleleft R$ ראשוני אם ורק אם לכל שני אידיאלים $P \subset A$ ו- $P \subset B$ מתקיים $AB \not\subseteq P$. ('כי' מסמן הכלה ממש.) **הדגמה.** P ראשוני אם $AB \not\subseteq P$ לכל שני אידיאלים שאינם מוכלים ב- P , וזה בוודאי גורר את התכונה הזו עבור אידיאלים המכילים ממש את P . מצד שני, נניח ש- $AB \not\subseteq P$ לכל A, B המכילים ממש את P , ויהיו A, B אידיאלים שאינם מוכלים ב- P . אז $A + P, B + P$ מכילים ממש את P , ולכן $(A + P)(B + P) = AB + AP + PB + P^2 \subseteq AB + P$. אבל $AB \not\subseteq P$, ולכן $AB + P \not\subseteq P$. גם AB אינו מוכל ב- P .

תרגיל 2.4.20 ()** אידיאל $P \triangleleft R$ הוא ראשוני אם ורק אם חוג המנה R/P ראשוני.

בפרט,

תרגיל 2.4.21 (*) אידיאל האפס ראשוני בחוג R אם ורק אם R עצמו ראשוני.

תרגיל 2.4.22 ()** כל אידיאל מקסימלי הוא ראשוני.

תרגיל 2.4.23 (*)** בחוג כלשהו: $P \triangleleft R$ ראשוני אם ורק אם לכל $a, b \in R$, אם $aRb \subseteq P$ אז $a \in P$ או $b \in P$.

תרגיל 2.4.24 (*)** בחוג קומוטטיבי, $P \triangleleft R$ ראשוני אם ורק אם לכל $a, b \in R$, אם $ab \in P$ אז $a \in P$ או $b \in P$.

תרגיל 2.4.25 (*)** יהי R חוג קומוטטיבי. האיחוד על-פני שרשרת של אידיאלים ראשוניים ב- R הוא אידיאל ראשוני.

תרגיל 2.4.26 (*)** תהי $R_1 \subseteq R_2 \subseteq \dots$ שרשרת של חוגים קומוטטיביים. נניח $P_i \triangleleft R_i$ אידיאלים ראשוניים כך ש- $P_1 \subseteq P_2 \subseteq \dots$. הראה ש- $\bigcup P_i \triangleleft \bigcup R_i$ ראשוני. הערה. זוהי הכללה של תרגיל 2.4.25.

תרגיל 2.4.27 ()** תהי $R_1 \subseteq R_2 \subseteq \dots$ שרשרת של חוגים. נניח ש- $P_i \triangleleft R_i$ אידיאלים ראשוניים, כך ש- $R_i \cap P_i = Q$ עבור $P_i = Q$. הראה ש- $Q \triangleleft \bigcup R_i$ ראשוני.

תרגיל 2.4.28 (**)** תן דוגמא נגדית לתרגיל 2.4.25 במקרה הלא קומוטטיבי. הדרכה. [דוגמא של ברגמן, אצל [1968, Passmann]: R הוא האלגברה החופשית $\langle F(a, x) : a \in P_n \rangle$ הם ראשוניים כי אם u, v מונומים כך ש- $uv \in P_n$ לכל m אז יש תת-מלה $ax^i a$ ב- u או ב- v ; אבל $uP_n = vP_n$ ראשוני כי $a^2 \in RaRaR$ ו- $a \notin RaRaR$.

תרגיל 2.4.29 (*)** הראה שהחיתוך על-פני שרשרת של אידיאלים ראשוניים הוא ראשוני. הדרכה. תהי $\{P_\alpha\}$ שרשרת כזו. נניח ש- $AB \subseteq \bigcap P_\alpha$. אז לכל α , $A \subseteq P_\alpha$ או $B \subseteq P_\alpha$. נניח ש- $A \not\subseteq P_{\alpha'}$ ו- $B \not\subseteq P_{\alpha''}$; אז $A \not\subseteq P_{\alpha'}$ ו- $B \not\subseteq P_{\alpha''}$, סתירה לכך ש- $AB \subseteq \bigcap P_\alpha$.

תרגיל 2.4.30 ()** בכל חוג R , אם $P \triangleleft R$ ראשוני ו- $ab \in P$ כאשר $a \in Z(R)$, אז $a \in P$ או $b \in P$.

תרגיל 2.4.31 (*)** יהי $\phi: R \rightarrow S$ אפימורפיזם של חוגים. הראה שאם $P \triangleleft S$ ראשוני, אז גם $\phi^{-1}(P) \triangleleft R$ (שהוא אידיאל לפי תרגיל 1.2.80, עמ' 30) הוא ראשוני.

תרגיל 2.4.32 (*)** תן דוגמא המראה שתמונת אידיאל ראשוני תחת אפימורפיזם אינה בהכרח אידיאל ראשוני.

תרגיל 2.4.33 ()** תן דוגמא לחוג R שאינו ראשוני, עם אידיאל $P \triangleleft R$ שהוא ראשוני גם כאידיאל וגם כחוג (בלי יחידה). הדרכה. $\mathbb{Z} \times \mathbb{Z}$.

תרגיל 2.4.34 ()** בתרגיל 1.2.61 (עמ' 27) הגדרנו את האידיאלים $(I : J)$. הראה שאם P ראשוני בחוג קומוטטיבי R , אז לכל אידיאל I , $(P : I) \in \{P, R\}$.

2.4.3 רדיקלים

תרגיל 2.4.35 (*) נניח ש- C חוג קומוטטיבי. הראה שהאוסף $\text{Nil}(C)$ של אברים נילפוטנטים ב- C הוא אידיאל. (נקרא הרדיקל הנילי של C).

תרגיל 2.4.36 (*) יהי R חוג כלשהו. אבר $x \in R$ נקרא קוואזי-הפיך אם $1 - x$ הפיך. אידיאל שמאלי $I \triangleleft C$ נקרא קוואזי הפיך אם כל אבר שלו הוא קוואזי-הפיך. הראה שהסכום של אידיאלים שמאליים קוואזי-הפיכים הוא קוואזי הפיך. הדרגה ראשית הוכח את הטענה לסכום של שני אידיאלים: אם $x \in I$ ו- $x' \in I'$ אז $(1 - (x + x'))^{-1} = (1 - (1 - x)^{-1}x')^{-1}(1 - x)^{-1}$.

הגדרה 2.4.37 רדיקל ג'ייקובסון $\text{Jac}(R)$ של R הוא הסכום כל האידיאלים השמאליים הקוואזי-הפיכים של R .

תרגיל 2.4.38 (*)** הראה ש- $\text{Jac}(R)$ הוא אידיאל דו-צדדי.

תרגיל 2.4.39 ()** $\text{Jac}(R)$ הוא האידיאל השמאלי הקוואזי-הפיך הגדול ביותר של R (כלומר, הוא קוואזי-הפיך ומכיל כל אידיאל שמאלי קוואזי-הפיך אחר); וגם האידיאל הימני הקוואזי-הפיך הגדול ביותר של R .

תרגיל 2.4.40 (*) כאשר R קומוטטיבי, $\text{Nil}(R) \subseteq \text{Jac}(R)$.

2.5 מיקום ושדה השברים

2.5.1 מיקום מרכזי

אבר שונה מאפס בחוג R נקרא רגולרי אם הוא אינו מחלק אפס לא מימין ולא משמאל.

תרגיל 2.5.1 ()** יהיו $R \subseteq Q$ חוגים. כל אבר של R שהוא הפיך ב- Q , הוא רגולרי ב- R .

תהי S תת-קבוצה של חוג R . מטרתנו בסעיף זה לבנות חוג המכיל את R , שבו כל אברי S הפיכים. לשם כך נניח כמה הנחות על S :

1. S מוכלת במרכז של R .

2. כל אברי S רגולריים.

3. S סגורה לכפל.

4. $1 \in S$.

תרגיל 2.5.2 (*) אם הקבוצה S מקיימת את ההנחות 1,2,3, אז $S \cup \{1\}$ מקיימת את 1,2,4,3.

תנאי 4, אס-כך, אינו מעכב את הבניה. המטרה היא, כאמור, לבנות חוג המכיל את R שבו אברי S הפיכים, ותנאי 2 הכרחי לזה לפי תרגיל 2.5.1. קיימות בניות כלליות יותר של "חוגי שברים", שבהן מסתפקים בקיום הומומורפיזם טבעי מ- R אל החוג החדש, ואז ניתן להחליף את תנאים 1,2 בתנאים חלשים יותר.

נגדיר על $S \times R$ יחס שקילות: $(s, r) \equiv (s', r')$ אם $s'r = sr'$.

תרגיל 2.5.3 ()** הראה שזהו אכן יחס שקילות. היכן השתמשנו בהנחה ש- S מרכזית? ובכך שב- S אין מחלקי אפס?

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

תרגיל 2.5.4 ()** הראה שהפעולות מוגדרות היטב. הדרכה. העזר בכך ש- $\frac{r}{s} = \frac{r'}{s'}$ אם ורק אם $sr' = s'r$.

תרגיל 2.5.5 (*)** הראה ש- $S^{-1}R$, עם הפעולות שהוגדרו לעיל, הוא חוג, שאבר היחידה שלו $\frac{1}{1}$.

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

תרגיל 2.5.6 ()** הראה ש- ι הוא שיכון.

מכיוון שכך, אפשר לזהות את R עם העותק האיזומורפי $\iota R = \{\frac{r}{1} : r \in R\}$ שהוא תת-חוג של $S^{-1}R$.

תרגיל 2.5.7 ()** הראה שאברי $\iota S = \{\frac{s}{1} : s \in S\}$ הפיכים ב- $S^{-1}R$. לכן אפשר לכתוב $S^{-1} = \{\frac{1}{s} : s \in S\}$.

תרגיל 2.5.8 ()** תהי $A \subseteq S^{-1}R$ תת-קבוצה הסגורה לחיבור ולכפל באברים של ιS . הראה שהמכפלה של תת-קבוצות ב- $S^{-1}R$, המוגדרת לפי הגדרה 1.2.33, היא קבוצת המכפלות $\{ \frac{1}{s} \cdot a : s \in S, a \in A \}$.

תרגיל 2.5.9 ()** הראה ש- $\iota: R \rightarrow S^{-1}R$ היא על, אם ורק אם כל אברי S הפיכים כבר ב- R .

הכללה למקרה הלא רגולרי

נניח ש- S היא תת-קבוצה מרכזית וסגורה לכפל של חוג R , הכוללת את אבר היחידה. איננו מניחים שאברי S רגולריים.

תרגיל 2.5.10 ()** הראה שאם היחס שהוגדר בתת-הסעיף הקודם הוא יחס שקילות, אז אברי S רגולריים. הדרכה. בדוק את התנאים $(1, 0) \equiv (s, 0) \equiv (1, r)$.

כמקודם, נגדיר על $S \times R$ יחס שקילות: $(s, r) \sim (s', r')$ אם קיים $\bar{s} \in S$ כך ש- $\bar{s}s'r = \bar{s}sr'$.

תרגיל 2.5.11 ()** הראה שזהו אכן יחס שקילות.

תרגיל 2.5.12 ()** הראה שאם כל אברי S רגולריים, אז היחס שהוגדר כאן מתלכד עם היחס שהוגדר לפני תרגיל 2.3.12 (עמ' 56).

כבמקרה הרגולרי, נסמן את מחלקת השקילות של (s, r) בסימון $\frac{r}{s}$, ונסמן $S^{-1}R = \{\frac{r}{s} : s \in S, r \in R\}$, עם אותן הגדרות לחיבור והכפל.

תרגיל 2.5.13 ()** הראה שהפעולות מוגדרות היטב. הערה. בדיקה זו מסובכת יותר, כמובן, מזו של תרגיל 2.5.4.

תרגיל 2.5.14 (*)** עם הפעולות שהוגדרו לעיל הוא חוג. הדרגה. בדוק שהוכחת תרגיל 2.5.5 תקפה גם במקרה הלא רגולרי, ללא כל שינוי.

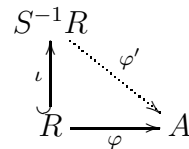
גם במקרה הזה אפשר להגדיר העתקה $\iota: R \rightarrow S^{-1}R$ לפי $r \mapsto \frac{r}{1}$, וכאן מתגלה ההבדל המהותי:

תרגיל 2.5.15 ()** הראה ש- $\text{Ker}(\iota) = \{r \in R: (\exists s \in S) sr = 0\}$, והסק ש- ι שיכון אם ורק אם כל אברי S רגולריים.

האוניברסליות של המיקום

נאמר שהומומורפיזם $R \rightarrow R'$ הוא "הופך S " אם התמונה של כל אבר של S הפיכה ב- R' .

משפט 2.5.16 יהי $\varphi: R \rightarrow A$ הומומורפיזם הופך S . אז קיים הומומורפיזם יחיד $\varphi': S^{-1}R \rightarrow A$ כך ש- $\varphi = \varphi' \circ \iota$.



תרגיל 2.5.17 (*)** יהי $\varphi: R \rightarrow A$ שיכון הופך S . אז ההומומורפיזם $\varphi': S^{-1}R \rightarrow A$ של משפט 2.5.16 הוא שיכון.

כלומר, כל חוג המכיל את ιR שבו אברי ιS הפיכים, מכיל גם את $S^{-1}R$. לכן $S^{-1}R$ הוא החוג הקטן ביותר המכיל את ιR שבתוכו אברי ιS הפיכים.

תרגיל 2.5.18 ()** אם $S_1 \subseteq S_2$ שני מונוידים בתחום השלמות R , מצא שיכון $S_1^{-1}R \hookrightarrow S_2^{-1}R$.

האידיאלים של $S^{-1}R$

השאלה הטבעית כעת היא מה קורה לאידיאלים של R כשעוברים להרחבה $S^{-1}R$. נחזור להניח שכל אברי S רגולריים.

אם $A \triangleleft R$, נסמן $S^{-1}A = \{\frac{a}{s}: a \in A, s \in S\}$. לפי תרגיל 2.5.8, זוהי המכפלה $S^{-1} \cdot A$ בתוך החוג $S^{-1}R$.

תרגיל 2.5.19 ()** הסבר כיצד יתכן ש- $\frac{x}{1} \in S^{-1}A$ גם אם $x \notin A$.

תרגיל 2.5.20 (*)** 1. לכל $A \triangleleft R$, $S^{-1}A$ הוא אידיאל של $S^{-1}R$;

2. לכל $T \triangleleft S^{-1}R$, $T = S^{-1}(T \cap R)$.

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

הדרכה. הבדיקה ש- $S^{-1}A$ הוא אידיאל מיידי. יהי $T \triangleleft S^{-1}R$ אז $A = T \cap R$ הוא אידיאל של R לפי תרגיל 1.2.8 (עמ' 22), ומכיוון ש- $A \subseteq T$, מתקיים $S^{-1}A \subseteq S^{-1}T = T$. מאידך, לכל $\frac{a}{s} \in T$, $\frac{a}{s} \in S^{-1}A$ ולכן $\frac{a}{1} = \frac{s}{1} \cdot \frac{a}{s} \in ST = T$, מכאן ש- $\frac{a}{1} \in A$ ולכן $T \subseteq S^{-1}A$. אם כן, $T = S^{-1}(T \cap R)$ הוא מהצורה המבוקשת.

תרגיל זה מראה שההעתקות

$$\{S^{-1}R \text{ של אידיאלים של } R\} \xrightleftharpoons[\Psi: T \mapsto T \cap R]{S^{-1}A \mapsto A: \Phi} \{R \text{ של אידיאלים של } R\}$$

מוגדרות היטב, וגם שההרכבה $\Phi \circ \Psi: T \mapsto S^{-1}(T \cap R)$ היא הזהות. מכאן ש- Ψ חד-חד-ערכית, ו- 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 2.5.21 (*)** 1. יהי $A \triangleleft R$. אז $S^{-1}A$ אידיאל אמיתי אם ורק אם $S \cap A = \emptyset$.

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

כלומר, ההעתקות שהוגדרו קודם לכן פועלות גם על הקבוצות המצומצמות

$$\{S^{-1}R \text{ של אידיאלים אמיתיים של } R\} \xrightleftharpoons[\Psi: T \mapsto T \cap R]{S^{-1}A \mapsto A: \Phi} \{R \text{ הזרים ל-} S\}$$

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

תרגיל 2.5.22 ()** 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 2.5.23 (*)** יהי $P \triangleleft R$ ראשוני זר ל- S , אז $S^{-1}P \cap R = P$.

הדרכה. ההכלה $P \subseteq S^{-1}P \cap R$ טריוויאלית. נניח ש- $\frac{a}{s} \in S^{-1}P \cap R$ כאשר $a \in P$ ו- $s \notin P$. מכיוון ש- $s \notin P$, $(RsR)(RxR) = RsxR = RaR \subseteq P$, ולכן $s \notin P$ ולכן $s \notin P$ ולפי הראשונות נובע מכך ש- $\frac{a}{1} \in P$. מכאן ש- $\frac{a}{s} \in P$.

תרגיל 2.5.24 (*)** אם $P \triangleleft R$ ראשוני זר ל- S , אז $S^{-1}P$ ראשוני. הדרכה. נניח ש- $T_1 T_2 \subseteq S^{-1}P$ עבור $T_1, T_2 \triangleleft R$. נכתוב $T_i = S^{-1}A_i$ עבור $A_i \triangleleft R$, ואז

$$A_1 A_2 \subseteq (S^{-1}A_1 \cdot S^{-1}A_2) \cap R = T_1 T_2 \cap R \subseteq S^{-1}P \cap R = P$$

לפי תרגיל 2.5.23. מכיוון ש- P ראשוני, יש i שעבורו $A_i \subseteq P$, ואז $T_i = S^{-1}A_i \subseteq S^{-1}P$.

תרגיל 2.5.25 (*)** אם $T \triangleleft S^{-1}R$ ראשוני, אז $T \cap R$ אידיאל ראשוני של R .

הדרכה. נניח ש- $A_1 A_2 \subseteq T \cap R$ עבור $A_1, A_2 \triangleleft R$. אז $S^{-1}(A_1 A_2) \subseteq S^{-1}(T \cap R) \subseteq T$ ולכן $S^{-1}A_1 \cdot S^{-1}A_2 \subseteq T$. מכיוון ש- T ראשוני נובע מכך ש- $S^{-1}A_i \subseteq T$ ל- i מתאים. לכן $A_i \subseteq S^{-1}A_i \cap R \subseteq T \cap R$.

משני התרגילים האחרונים נובע שההתאמות

$$\{S^{-1}R \text{ אידיאלים ראשוניים של } S^{-1}R\} \xleftrightarrow[\Psi: T \mapsto T \cap R]{S^{-1}A \mapsto A: \Phi} \left\{ \begin{array}{l} R \text{ אידיאלים ראשוניים של } R \\ \text{הזרים ל-} S \end{array} \right\}$$

מוגדרות היטב, ולפי תרגילים 2.5.20 ו-2.5.23, הן הפוכות זו לזו. אם כך, הוכחנו:

משפט 2.5.26 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 $S^{-1}P \mapsto P \cap R, S^{-1}P \mapsto T$.

תרגיל 2.5.27 (+)** כל אידיאל $I \triangleleft R$ זר ל- S מוכל באידיאל ראשוני זר ל- S . הדרכה. לפי ההנחה $S^{-1}I \triangleleft S^{-1}R$ הוא אידיאל אמיתי, ולכן הוא מוכל באידיאל מקסימלי $M \triangleleft S^{-1}R$, שהוא בהכרח מהצורה $M = S^{-1}P$ עבור $P \triangleleft R$ ראשוני. לכן $I \subseteq S^{-1}P \cap R = P$ ו- $I \subseteq S^{-1}I \subseteq S^{-1}P$.

תרגיל 2.5.28 (+)** יהי $A \triangleleft R$ אידיאל זר ל- S . הראה ש- $r + A \mapsto \frac{r}{1} + S^{-1}A$ הוא הומומורפיזם מוגדר היטב $R/A \rightarrow S^{-1}R/S^{-1}A$, שהגרעין שלו הוא $(S^{-1}A \cap R)/A$. לכן הוא מתפצל להטלה ושיכון

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

לעומת זאת:

תרגיל 2.5.29 (+)** יהי $P \triangleleft R$ אידיאל ראשוני שהוא זר ל- S . הראה שקיים שיכון $R/P \hookrightarrow S^{-1}R/S^{-1}P$. הדרכה. תרגילים 2.5.28 ו-2.5.23.

תרגיל 2.5.30 ()** תן דוגמא לאידיאל $A \triangleleft R$ שאינו ראשוני, כך ש- $S^{-1}A$ ראשוני. הדרכה. תרגיל 2.5.22.

חוג השברים הטוטאלי

את הבניה של חוג השברים אפשר להכליל לכל חוג קומוטטיבי:

תרגיל 2.5.31 ()** יהי R חוג קומוטטיבי. הראה שהאוסף $D(R)$ של אברים רגולריים הוא סגור לכפל (תרגיל 1.1.31, עמ' 13). הראה שבחוג $D(R)^{-1}R$, הנקרא חוג השברים הטוטאלי של R , כל האברים הרגולריים הפיכים.

תרגיל 2.5.32 ()** חשב את חוג השברים הטוטאלי של $\mathbb{Z} \times \mathbb{Z}$.

2.5.2 מיקום באידיאל ראשוני

תרגיל 2.5.33 ()** יהי P אידיאל של תחום שלמות R . הראה שהמשלים $S = R - P$ כולל אברים רגולריים בלבד, ושהוא סגור לכפל אם ורק אם P ראשוני.

אם $P \triangleleft R$ אידיאל ראשוני של תחום שלמות R , אפשר לפי התרגיל להפעיל את הבניה של סעיף 2.5.1 ולקבל חוג $\{\frac{x}{b} : x \in R, b \notin P\}$, שבו כל אבר מחוץ ל- P הוא הפיך. את החוג הזה מסמנים ב- R_P , והוא נקרא **המיקום** של R ב- P . לכל אידיאל $A \triangleleft R$ מסמנים $A_P = (R - P)^{-1}A$. לפי תרגיל 2.5.21, $A_P \triangleleft R_P$ הוא אידיאל אמיתי אם $A \subseteq P$; אחרת, $A_P = R_P$.

תרגיל 2.5.34 (-)** יש התאמה חד-חד-ערכית ועל בין אידיאלים ראשוניים של R המוכללים ב- P , לבין אידיאלים ראשוניים של R_P . הדרכה. זהו משפט 2.5.26 עבור $S = R - P$.

תרגיל 2.5.35 ()** יהי P אידיאל ראשוני של חוג קומוטטיבי R . אז R_P מקומי, והאידיאל המקסימלי שלו הוא $P_P = (R - P)^{-1}P$. הדרכה. תרגיל 2.5.34.

התרגיל האחרון מראה מה הרווחנו ממיקום באידיאל ראשוני P : התוצאה היא חוג מקומי, שבו 'נעלמו' כל האידיאלים שאינם מוכללים ב- P . מיקום כזה מאפשר ללמוד את P ללא הפרעות חיצוניות.

תרגיל 2.5.36 ()** תאר את המיקום $\mathbb{Z}_{(7)}$. מצא אבר $t \in \mathbb{Q}$ כך ש- $\mathbb{Z}_{(7)}[t] = \mathbb{Q}$.

תרגיל 2.5.37 (+)** הראה שיש שיכון מהמיקום $\mathbb{Z}_p \hookrightarrow \mathbb{Z}_{(p)}$. הדרכה. תרגיל 2.3.12 (עמ' 56).

תרגיל 2.5.38 ()** אם R תחום שלמות אז לכל אידיאל ראשוני $P \triangleleft R$ יש שיכון $R_P \hookrightarrow q(R)$. הדרכה. תרגיל 2.5.18.

משפט 2.5.39 יהי R תחום שלמות ויהי $A \triangleleft R$ אידיאל. אז

$$A = \bigcap_{P \triangleleft R} A_P$$

כאשר החיתוך הוא בתוך שדה השברים $F = q(R)$, על-פני כל האידיאלים המקסימליים של R (בין אם הם מכילים את A ובין אם לאו).

הוכחה. ההכלה $A \subseteq A_P$ ברורה. בכיוון ההפוך, יהי $b^{-1}a \in F$ אבר השייך לכל המיקומים A_P ; כלומר, $a \in bA_P$ לכל אידיאל מקסימלי $P \triangleleft R$. עלינו להראות ש- $b^{-1}a \in A$, ואז $a \in Ab$.

יהי $J = \{x \in R : xa \in Ab\} = R \cap a^{-1}bA$; ברור שזהו אידיאל של R . אם $J \triangleleft R$ אידיאל אמיתי אז הוא מוכל באידיאל מקסימלי M , ואז $b^{-1}a \in M$. ואז $b^{-1}a \in A_M$. מסיקים ש- $b^{-1}a = b_1^{-1}a_1$ עבור $a_1 \in A$ ו- $b_1 \notin M$. אבל אז $b_1a = a_1b \in Ab$, כך ש- $b_1 \in J \subseteq M$. בסתירה לבחירת b_1 . מכאן ש- $1 \in J$ ולכן $a \in Ab$. $\square$

תרגיל 2.5.40 ()** כל תחום שלמות הוא חיתוך של חוגים מקומיים (עם אותו שדה שברים).

משפט 2.5.39 חושף תוצאה חשובה ביותר:

תרגיל 2.5.41 ()** יהיו $A, B \triangleleft R$ אידיאלים בתחום שלמות. אם $A_P = B_P$ לכל $P \triangleleft R$ מקסימלי, אז $A = B$.

תרגיל 2.5.42 (*)** התבונן בחוג $R = \mathbb{Z}[\sqrt{-3}]$ עם האידיאל המקסימלי $M = \langle 2, 1 + \sqrt{-3} \rangle$.

1. הראה שהמיקום R_M איזומורפי ל- $\mathbb{Z}_{(2)}[\pi \mid \pi^2 = 2\pi - 4]$. הדרכה. קח $\pi = 1 + \sqrt{-3}$.

2. הראה שכל אידיאל של R_M מכיל חזקה של $\langle 2 \rangle$. הדרכה. עבור $a + b\pi$, $a, b \in \mathbb{Z}_{(2)}$. אם ורק אם a איזוגי. לכן כל אידיאל מכיל אבר מהצורה $2a + b\pi$. הראה שהאידיאל מכיל את $4(a^2 + ab + b^2)$. השקול עד כדי הפכים לחזקה של 2.

3. הראה שהאידיאלים היחידים של R_M המכילים את $\langle 4 \rangle$ הם M , $A = \langle 4, \pi \rangle$, $B = \langle 4, \pi - 2 \rangle$ ו- $C = \langle 2 \rangle$.

4. הראה שהאידיאלים היחידים של R_M הם מהצורה $2^i M$, $2^i A$, $2^i B$, $2^i \langle 2 \rangle$.
 הדרכה. יהי $I \triangleleft R_M$ אידיאל שאינו מכיל את $\langle 2 \rangle$. מכיון ש- $I \subseteq M$, כל אבר של I הוא מהצורה $2a + \pi b$ $(a, b \in \mathbb{Z}_{(2)})$, אבל מכיון ש- $I \not\subseteq \langle 2 \rangle$ יש בו אבר $2a + \pi b$ עם $b \notin \langle 2 \rangle$. עם כך b הפך ולכן יש $c \in \mathbb{Z}_{(2)}$ כך ש- $\pi \equiv 2c \pmod{I}$. אבל אז $4(c^2 - c + 1) \equiv 0 = \pi^2 - 2\pi + 4 \in I$, כלומר $4 \in I$. לפי הסעיף הקודם $I = M, A, B, C$. סיים באינדוקציה.

תרגיל 2.5.43 ()** אשר שהאידיאלים A, B, C של תרגיל 2.5.42 אינם מקיימים את תנאי הדיסטריבוטיביות של תרגיל 2.2.19. (עמ' 51).

2.5.3 שדה השברים

כבסעיף הקודם, נניח ש- R תחום שלמות. אידיאל האפס הוא אידיאל ראשוני, ואכן $S = R - \{0\}$ מקיים את כל הדרישות של תת-סעיף 2.5.1.

תרגיל 2.5.44 ()** אם $S = R - \{0\}$ אז $S^{-1}R$ שדה; שדה זה נקרא **שדה השברים של R** , ומסמנים אותו ב- $q(R)$.

משפט 2.5.45 כל תחום שלמות משוכן בשדה.

לאור תרגיל 1.1.54 (עמ' 15), תחומי שלמות הם בדיוק תת-החוגים של שדות. (ההכללה המתבקשת למקרה הלא קומוטטיבי אינה נכונה: לא כל תחום ניתן לשיכון בחוג עם חילוק, אלא שדוגמאות כאלה חורגות מהיקפו של הקורס שלנו.)

תרגיל 2.5.46 (*) הראה ש- $\mathbb{Q}$ הוא שדה השברים של $\mathbb{Z}$.

תרגיל 2.5.47 (+)** יהי F שדה. נסמן ב- $F(x)$ את החוג של כל המנות $\frac{f}{g}$ כאשר $f, g \in F[x]$ ו- $g \neq 0$. הראה שזהו שדה השברים של חוג הפולינומים $F[x]$.

תרגיל 2.5.48 (+)** תאר את שדה השברים של חוג הפולינומים $\mathbb{Z}[z_1, \dots, z_n]$.

תרגיל 2.5.49 (+)** יהי F שדה. הראה ששדה השברים של $F[[x]]$ הוא $F((x))$.

תרגיל 2.5.50 (*)** פתור את תרגיל 1.3.18 (עמ' 36) (לכל חוג קומוטטיבי R , הדטרמיננטה $\det: M_n(R) \rightarrow R$ היא כפלית), מבלי לחזור על הוכחת הטענה מעל שדות. הדרכה. נשתמש בבניה של **מטריצות גנריות**: נתבונן בחוג $S = \mathbb{Z}[x_{ij}, y_{ij}]$ עם $2n^2$ יוצרים. לפי וריאציה על תרגיל 1.2.104 (עמ' 33), לכל $A, B \in M_n(R)$ יש הומומורפיזם $\varphi: S \rightarrow R$, המשרה הומומורפיזם $\bar{\varphi}: M_n(S) \rightarrow M_n(R)$ שעבורו $A \mapsto B$ ו- $(x_{ij}) \mapsto (y_{ij})$. מכיון ש- S מוכל בשדה השברים שלו $\mathbb{Q}(x_{ij}, y_{ij})$ ולפי הכפלויות של הדטרמיננטה מעל שדות, מתקיים $\det(A) \det(B) = \det((x_{ij})(y_{ij})) = \det((x_{ij})) \det((y_{ij})) \mapsto \det(A) \det(B)$ ויהי $c = \det((x_{ij})(y_{ij})) \mapsto AB$ משום שכל מטריצות הוא פונקציה פולינומאלית, ולכן $\det(A) \det(B) = \varphi(c) = \det(AB)$.

תרגיל 2.5.51 (+)** יהי F שדה. נניח ש- $A_0, A_1, \dots \subseteq F$ הן תת-חבורות אבליות. הראה ש- $\sum A_n x^n$ הוא תת-חוג של $F[x]$ אם ורק אם $A_n A_m \subseteq A_{n+m}$ לכל n, m . בפרט, $A_0 \subseteq F$ הוא תת-חוג (אולי בלי יחידה).

פרק 3

תחומי שלמות

בתרגיל 1.1.54 (עמ' 15) ומשפט 2.5.45 ראינו שתחומי שלמות הם תת-החוגים של שדות. בפרק זה נלמד מחלקות שונות של תחומי שלמות, במטרה להכליל שתי דוגמאות חשובות: המספרים השלמים וחוגים של פולינומים.

3.1 חוגי שלמים ריבועיים

בסעיף זה נציץ לתורת המספרים האלגברית על-ידי הצגת משפחה של חוגים הקרובים במובן מסויים לחוג השלמים $\mathbb{Z}$. חוגים אלה ישמשו אותנו לבחון את המושגים הכלליים שאנו לומדים בשאר הפרק.

הרחבה ריבועית של $\mathbb{Q}$ היא שדה המכיל את $\mathbb{Q}$, שהממד שלו כמרחב וקטורי מעל $\mathbb{Q}$ הוא 2.

תרגיל 3.1.1 ()** כל הרחבה ריבועית של $\mathbb{Q}$ היא מהצורה $\mathbb{Q}[\sqrt{D}] \subseteq \mathbb{C}$, כאשר $D \in \mathbb{Z}$ הוא שלם ללא גורמים ריבועיים.

תרגיל 3.1.2 (-*)** מצא הצגה $\mathbb{Q}[\sqrt{D}] \hookrightarrow M_2(\mathbb{Q})$.

אנו מגדירים, לכל $D \in \mathbb{Z}$ שאין לו גורמים ריבועיים, $\mathcal{O}_D = \mathbb{Z}[\frac{1+\sqrt{D}}{2}]$ אם $D \equiv 1 \pmod{4}$ ו- $\mathcal{O}_D = \mathbb{Z}[\sqrt{D}]$ אחרת. שימו לב שתמיד $\mathbb{Z}[\sqrt{D}] \subseteq \mathcal{O}_D$. באופן כללי יותר, נגדיר את $\mathcal{O}_D$ על-ידי סילוק הגורמים הריבועיים: אם $D = n^2 D_0$ כאשר D_0 ללא גורמים ריבועיים, נגדיר $\mathcal{O}_D = \mathcal{O}_{D_0}$. החוגים $\mathcal{O}_D$ הם חוגי השלמים הריבועיים.

תרגיל 3.1.3 (*) לכל $D \equiv 1 \pmod{4}$, $\frac{1+\sqrt{D}}{2} \in \mathcal{O}_D$. הדרכה: אם D חופשי מגורמים ריבועיים אין מה להוכיח, ואם $D = a^2 D_0$ אז $\mathcal{O}_D = \mathcal{O}_{D_0}$ ואם $\frac{1+\sqrt{D_0}}{2} \in \mathcal{O}_{D_0}$ משום ש- a אי-זוגי.

תרגיל 3.1.4 (*) עבור D החופשי מגורמים ריבועיים,

$$\mathcal{O}_D = \begin{cases} \mathbb{Z} + \mathbb{Z}\frac{1+\sqrt{D}}{2} = \{a + b\sqrt{D} : 2a, 2b, a-b \in \mathbb{Z}\} & D \equiv 1 \pmod{4} \\ \mathbb{Z} + \mathbb{Z}\sqrt{D} = \{a + b\sqrt{D} : a, b \in \mathbb{Z}\} & D \not\equiv 1 \pmod{4} \end{cases}.$$

תרגיל 3.1.5 ()** לכל D , $\mathbb{Z}[\sqrt{D}] \cong \mathbb{Z}[\lambda]/\langle \lambda^2 - D \rangle$, אם $D \equiv 1 \pmod{4}$, אז $\mathcal{O}_D \cong \mathbb{Z}[\lambda]/\langle \lambda^2 - \lambda - \frac{D-1}{4} \rangle$.

תרגיל 3.1.6 ()** חוג השברים של $\mathcal{O}_D$ הוא $\mathbb{Q}[\sqrt{D}]$.

טענה 3.1.7 אם $\mathbb{Z} + \mathbb{Z}\alpha$ הוא תת-חוג של $\mathbb{C}$, אז $\alpha \in \mathcal{O}_D$ עבור $D \in \mathbb{Z}$ כלשהו.

הוכחה. נניח ש- $\alpha^2 = n\alpha + m$ עבור $n, m \in \mathbb{Z}$, אז $\alpha = \frac{n \pm \sqrt{n^2 + 4m}}{2}$. נסמן $D = n^2 + 4m$. אם n זוגי אז $\alpha \in \mathbb{Z}[\sqrt{D}]$, ואחרת $\alpha \in \mathbb{Z}[\frac{1+\sqrt{D}}{2}]$.
 $\alpha = \frac{n-1}{2} + \frac{1+\sqrt{D}}{2} \in \mathbb{Z}[\frac{1+\sqrt{D}}{2}]$, $D \equiv 1 \pmod{4}$.
 $\square$

האינוולוציה, העקבה והנורמה

תרגיל 3.1.8 ()** הפונקציה $\mathbb{Q}[\sqrt{D}] \rightarrow \mathbb{Q}[\sqrt{D}]$ המוגדרת לפי $x + y\sqrt{D} \mapsto x - y\sqrt{D}$ היא אינוולוציה. (ראה תרגיל 3.58, עמ' 40.)

תרגיל 3.1.9 ()** הפונקציה $T: \mathbb{Q}[\sqrt{D}] \rightarrow \mathbb{Q}$ המוגדרת לפי $T(z) = z + \bar{z}$ היא אדיטיבית. פונקציה זו היא העקבה.

תרגיל 3.1.10 ()** הפונקציה $N: \mathbb{Q}[\sqrt{D}] \rightarrow \mathbb{Q}$ המוגדרת לפי $N(z) = z\bar{z}$ היא כפלית. פונקציה זו היא הנורמה.

קל לחשב שלכל $a, b \in \mathbb{Q}$, $T(a + b\sqrt{D}) = 2a$ ו- $N(a + b\sqrt{D}) = a^2 - Db^2$.

תרגיל 3.1.11 ()** לכל $x \in \mathbb{Q}[\sqrt{D}]$ מתקיים $x^2 - T(x)x + N(x) = 0$.

תרגיל 3.1.12 ()** אם $R \subseteq \mathbb{Q}[\sqrt{D}]$ תת-חוג כך ש- $N(x) \in \mathbb{Z}$ לכל $x \in R$, אז גם $T(x) \in \mathbb{Z}$ לכל $x \in R$. הדרכה. $T(x) = N(x+1) - N(x) - 1$.

תרגיל 3.1.13 ()** נניח ש- $x \in \mathbb{Q}[\sqrt{D}]$ מקיים $N(x), T(x) \in \mathbb{Z}$. אז $x \in \mathbb{Z}[\frac{1+\sqrt{D}}{2}]$.

תרגיל 3.1.14 ()** הנורמה תמיד מקבלת ערכים שלמים על $\mathbb{Z}[\sqrt{D}]$. הנורמה שלמה על $\mathbb{Z}[\frac{1+\sqrt{D}}{2}]$ אם ורק אם $D \equiv 1 \pmod{4}$.

תרגיל 3.1.15 (*) $N(n + m\frac{1+\sqrt{D}}{2}) = n^2 + nm + \frac{1-D}{4}m^2$.

תרגיל 3.1.16 (*)** יהי R תחום שלמות. הראה שהפונקציה $N_0: R \rightarrow \mathbb{N} \cup \{\infty\}$ המוגדרת לפי $N_0(a) = |R/Ra|$ היא כפלית. הדרכה. $|R/Rab| = |R/Ra| \cdot |Ra/Rab|$. לפי משפט האיזומורפיזם השלישי. מצא התאמה חד-חד-ערכית ועל $R/Rb \rightarrow Ra/Rab$; ראה גם תרגיל 5.1.38 (עמ' 121).

תרגיל 3.1.17 ()** כל אידיאל שונה מאפס של $\mathcal{O}_D$ נחתך עם $\mathbb{Z}$ באופן לא טריוויאלי. הסק: כל חוג מנה של $\mathcal{O}_D$ הוא סופי. לכן הנורמה המוגדרת על $\mathcal{O}_D$ בתרגיל 3.1.16 מקבלת ערכים טבעיים בלבד.

תרגיל 3.1.18 (*)** הראה שלכל $x \in \mathbb{Z}[\sqrt{D}]$, $N(x) = |\mathbb{Z}[\sqrt{D}]/\langle x \rangle|$, כלומר, הנורמה של תרגיל 3.1.16 מתלכדת עם הנורמה הריבועית הרגילה. הדרכה. כתוב $x = a + b\sqrt{D}$. העזר בתרגיל 3.1.16 כדי לעבור למקרה שבו a, b זרים, והראה שבמקרה זה $\mathbb{Z}[\sqrt{D}]/\langle x \rangle \cong \mathbb{Z}/N(x)\mathbb{Z}$. בעזרת תרגיל 3.1.5.

תרגיל 3.1.19 (*)** הוכח שלכל $x \in \mathcal{O}_D$, $|\mathcal{O}_D/\langle x \rangle| = N(x)$, כאשר N היא הנורמה המוגדרת בתרגיל 3.1.10. הדרכה. המקרה $D \not\equiv 1 \pmod{4}$ מכוסה על-ידי תרגיל 3.1.18. פתור את המקרה השני באותו אופן, שוב בעזרת תרגיל 3.1.5. הערה. שים לב שאם $\mathbb{Z}[\sqrt{D}] \neq \mathcal{O}_D$, הסימון $\langle x \rangle$ מתייחס לקבוצות שונות בשני המקרים.

3.1.1 חוגים בעלי נורמה

הגדרה 3.1.20 תחום שלמות R הוא בעל נורמה אם יש $N: R \rightarrow \mathbb{Z}$ כפליית, כך שמי- $1 \pm N(u) =$ נובע ש- u הפיך.

תרגיל 3.1.21 ()** תחום שלמות בעל מנות סופיות הוא בעל נורמה.

תרגיל 3.1.22 ()** החוגים מהצורה $\mathbb{Z}[\sqrt{D}]$ ו- $\mathcal{O}_D$ הם בעלי מנות סופיות, ולכן בעלי נורמה.

3.2 אברים ראשוניים ואי-פריקים

הגישה היסודית לתחומי שלמות, והמוקדמת ביותר מבחינה הסטורית, היא דרך האברים שלהם. בחוג המספרים השלמים אפשר לפרק כל מספר לגורמיו הראשוניים באופן יחיד - זהו המשפט היסודי של האריתמטיקה. הרעיון הוא, אם כך, לבחון עד כמה דומים תחומי שלמות כלליים לחוג המספרים השלמים. מתברר שכבר בהגדרה של מספר ראשוני מסתתר סיבוך מסויים: שתי הגדרות מתקבלות על הדעת, והן אינן שקולות זו לזו.

3.2.1 יחס החילוק

יהי R תחום שלמות. אומרים שאבר a מחלק אבר b אם קיים x כך ש- $b = ax$. במקרה כזה מסמנים $a | b$.

תרגיל 3.2.1 ()** יחס החילוק הוא רפלקסיבי וטרנזיטיבי.

תרגיל 3.2.2 (*) לכל אבר $a \in R$ מתקיים $a | 0$.

תרגיל 3.2.3 (*) $u \in R$ הפיך אם ורק אם $u | 1$.

בדרך כלל יחס החילוק אינו אנטי-סימטרי, ולכן הוא אינו יחס סדר.

הגדרה 3.2.4 נאמר ש- $a, b \in R$ הם חברים אם $a | b$ ו- $b | a$. לחילופין, קיים $u \in R^\times$ כך ש- $b = ua$. במקרה כזה נסמן $a \sim b$.

נאמר ש- $a | b$ הוא מחלק אמיתי אם a מחלק את b אבל אינו חבר שלו.

תרגיל 3.2.5 (*) כתוב את מחלקות החברות ב- $\mathbb{Z}$.

תרגיל 3.2.6 ()** נניח ש- $a \sim a_1$ ו- $b \sim b_1$. הראה ש- $a | b$ אם ורק אם $a_1 | b_1$.

כלומר, יחס החילוק מוגדר היטב על מחלקות חברות.

תרגיל 3.2.7 ()** יחס החילוק הוא יחס סדר חלש על מחלקות החברות.

ביחס הזה, האבר הקטן ביותר הוא מחלקת האברים ההפיכים, והגדול ביותר הוא המחלקה של 0, הכוללת את 0 לבדו. מכיוון שאנו עוסקים בתחומי שלמות, אפשר לשכן את החוג בשדה השברים שלו, ולנסח את יחס החילוק באופן הבא: נניח $a, b \in R$. אז a מחלק את b אם ורק אם $a^{-1}b \in R$.

תרגיל 3.2.8 (-)** תן דוגמא לתת-חוג $R_0 \subseteq R$ עם אברים $a, b \in R_0$ כך ש- a מחלק את b ב- R אבל לא ב- R_0 .

כלומר, למרות שהסימון אינו מציג זאת במפורש, יחס החילוק תלוי בחוג. מצד שני:

תרגיל 3.2.9 (+)** נניח ש- $R = R_0 \cap q(R_0)$. אם $a, b \in R_0 \subseteq R$ ו- a מחלק את b ב- R , אז a מחלק את b ב- R_0 .

תאור לפי אידיאלים

את כל התכונות שהוצגו לעיל אפשר לתאר גם בשפת האידיאלים.

תרגיל 3.2.10 ()** $a \mid b$ אם ורק אם $Rb \subseteq Ra$.

תרגיל 3.2.11 ()** a מחלק אמיתי של b אם ורק אם $Rb \subset Ra$.

תרגיל 3.2.12 ()** $a \sim b$ אם ורק אם $Rb = Ra$.

תרגיל 3.2.13 ()** u הפיך אם ורק אם $Ru = R$.

3.2.2 אברים הפיכים

האברים ההפיכים הם האברים ה'טריוויאליים' של תחום השלמות, ודווקא משום כך חשוב להכיר אותם כדי להבין את החוג.

תרגיל 3.2.14 (*) האברים ההפיכים ב- $\mathbb{Z}$ הם ± 1 .

תרגיל 3.2.15 ()** האברים ההפיכים בחוג פולינומים $R[x]$ מעל תחום שלמות R הם הסקלרים ההפיכים של R . בפרט, האברים ההפיכים בחוג פולינומים $F[x]$ מעל שדה F הם האברים השונים מאפס ב- F .

אברים הפיכים של $\mathcal{O}_D$

תרגיל 3.2.16 (*) אם $a \mid b$ ב- $\mathcal{O}_D$, אז $N(a) \mid N(b)$. בפרט, אם u הפיך אז $N(u) = \pm 1$.

תרגיל 3.2.17 ()** יהי $D < 0$ שלם ללא גורמים ריבועיים. אז חבורת ההפיכים של $\mathcal{O}_D$ היא $\{\pm 1, \pm\sqrt{-1}\}$ עבור $D = -1$, $\{\pm 1, \frac{\pm 1 \pm \sqrt{-3}}{2}\}$ עבור $D = -3$, ו- $\{\pm 1\}$ בכל מקרה אחר. הדרכה. ראה תרגיל 3.2.16.

תרגיל 3.2.18 (*)** יהי $D > 0$. אם $x \in \mathbb{Q}[\sqrt{D}]$, נכתוב $x = x' + x''\sqrt{D}$ עבור $x' \in \mathbb{Q}$, $x'' \in \mathbb{Q}$. הראה ש- $x \in \mathbb{Z}[\sqrt{D}]$ הפיך אם ורק אם (x', x'') הוא פתרון למשוואת פל $x'^2 - Dx''^2 = \pm 1$.

תרגיל 3.2.19 (*)** נניח ש- $p > 2$ ראשוני. למשוואה $x^2 \equiv -1 \pmod{p}$ יש פתרון אם ורק אם $p \equiv 1 \pmod{4}$.

תרגיל 3.2.20 (*)** נניח ש- $D > 0$ וחופשי מריבועים. בתרגיל זה נוכיח ש- $\mathbb{Z}[\sqrt{D}]^\times \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}$, בהנחה שקיימים אברים הפיכים לא טריוויאליים (עובדה שאותה אפשר להוכיח, למשל, באמצעות פיתוח השורש $\sqrt{D}$ לשבר משולב). לכל $x, y \in \mathbb{Z}[\sqrt{D}]$, נאמר ש- $y > x$ אם $y' > x'$ וגם $y'' > x''$ (יחס סדר זה אינו הופך את $\mathbb{Z}[\sqrt{D}]$ לחוג סדור, משום שהוא אינו ליניארי). באותו אופן נאמר ש- x חיובי אם $x', x'' > 0$.

1. לכל אבר הפיך x , גם $x, \bar{x}, -x, -\bar{x}$ הפיכים (וכלם שונים זה מזה, אלא אם $x = \pm 1$).

2. נניח ש- $x \neq \pm 1$. אחד מבין $x, -x, \bar{x}, -\bar{x}$ הוא חיובי.

3. יהיו $x \neq y$ שני אברים הפיכים חיוביים. אז $x < y$ או $y < x$. הדרכה. נניח ש- $y' \geq x'$; הראה שאם $y'' < x''$ אז $D = 2$ ו- $y = 1$.

4. נניח ש- $0 < x < y$ הפיכים. הראה ש- $yx^{-1} > 0$. הדרכה. כתוב $yx^{-1} = Dy''^2 + N(y)$. הראה ש- $x'^2 = Dx''^2 + N(x)$ ושים לב ש- $x^{-1} = N(x)\bar{x}$.

5. יהי x_0 האבר ההפיך החיובי המינימלי. הראה שכל אבר הפיך חיובי הוא חזקה טבעית של x_0 .

6. הראה שכל אבר הפיך הוא מהצורה $\pm x_0^n$ עבור $n \in \mathbb{Z}$ (בין אם $N(x) = 1$ ובין אם $N(x) = -1$).

תרגיל 3.2.21 (*)** יהי $D > 0$ וחופשי מריבועים. הוכח ש- $\mathcal{O}_D^\times \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}$. הדרכה. אם $D \not\equiv 1 \pmod{4}$, זהו תרגיל 3.2.20. הוכח את המקרה הנותר באופן דומה, תוך התייחסות למשוואה $a^2 - Db^2 = \pm 4$.

תרגיל 3.2.22 (*)** הראה שחבורת ההפיכים של $\mathcal{O}_5 = \mathbb{Z}[\frac{1+\sqrt{5}}{2}]$ נוצרת על-ידי 1 ו- $\frac{1+\sqrt{5}}{2}$; ושחבורת ההפיכים של $\mathbb{Z}[\sqrt{5}]$ נוצרת על-ידי 1 ו- $2 + \sqrt{5}$. $(\frac{1+\sqrt{5}}{2})^3 = 2 + \sqrt{5}$.

3.2.3 אברים אי-פריקים

כל אבר בתחום שלמות אפשר לפרק באופן טריוויאלי, בצורה $a = au \cdot u^{-1}$ כאשר u הפיך; פירוק כזה, שבו אחד הגורמים הפיך, נקרא **פירוק טריוויאלי**.

הגדרה 3.2.23 יהי R תחום שלמות. נאמר שאבר $a \in R$ (שונה מאפס, שאינו הפיך) הוא **אי-פריק** אם מתקיימות התכונות השקולות הבאות:

1. אין ל- a פירוק לא טריוויאלי.

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

3. אם $a = xy$ אז x הפיך או y הפיך.

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

5. אם $x \mid a$ אז $x \sim a$ או $x \sim x$ הפיך.

תרגיל 3.2.24 ()** הראה שההגדרות לאי-פריקות אכן שקולות.

תרגיל 3.2.25 ()** אבר $a \in R$ הוא אי-פריק אם ורק אם האידיאל Ra מקסימלי בין כל האידיאלים הראשיים (האמיתיים) של R .

תרגיל 3.2.26 ()** מצא דוגמאות לתחומי שלמות $R_0 \subseteq R$ ו- $p \in R_0$ כך ש-

1. p אי-פריק ב- R_0 אבל פריק ב- R ;

2. p אי-פריק ב- R אבל פריק ב- R_0 .

תרגיל 3.2.27 ()** יהי $D \in \mathbb{Z}$ שלם. יהיו $x, y \in \mathcal{O}_D$.

1. אם $x \mid y$ אז $N(x) \mid N(y)$.

2. x הפיך אם ורק אם $N(x) = \pm 1$.

3. אם $N(x)$ אי-פריק ב- $\mathbb{Z}$, אז x אי-פריק ב- $\mathcal{O}_D$.

תרגיל 3.2.28 ()** 1. האבר $2 \in \mathbb{Z}[\sqrt{-6}]$ אי-פריק, אבל הנורמה שלו פריקה.

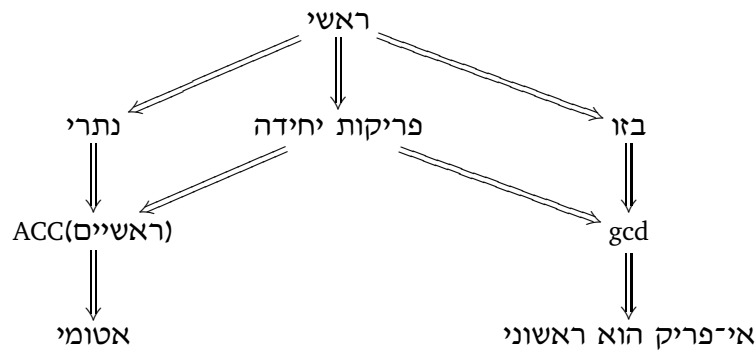
2. בחוג $\mathbb{Z}[\sqrt{6}]$ האבר 2 פריק.

תרגיל 3.2.29 ()** אם $p \in \mathbb{Z}$ ראשוני ואין אברים מנורמה $\pm p$ ב- $\mathbb{Z}[\sqrt{D}]$ או ב- $\mathcal{O}_D$, אז p אי-פריק שם.

תרגיל 3.2.30 ()** נניח ש- $D < 0$. אין ב- $\mathcal{O}_D$ אברים עם נורמה 2 או 3, אלא אם $D = -1, -2, -3, -7, -11$.

תרגיל 3.2.31 ()** אם $D \equiv 5 \pmod{8}$, אין ב- $\mathcal{O}_D$ אברים עם נורמה ± 2 . הדרכה: התבונן בנוסחה שבתרגיל 3.1.15 (עמ' 74) מודולו 4.

תרגיל 3.2.32 ()** אם $D \equiv 1 \pmod{4}$, אין ב- $\mathbb{Z}[\sqrt{D}]$ אברים עם נורמה ± 2 . מאידך, מצא אבר מנורמה 2 ב- $\mathcal{O}_{17}$.



איור 3.1: טיפוסים של תחומי שלמות (להוכחת הגרירות, ראה תרגילים 3.3.22, 3.3.51, 3.3.80, 3.3.18, 3.3.86, 3.3.75, 3.3.40)

3.2.4 אברים ראשוניים

בעוד שאבר אי-פריק נמדד לפי תכונותיו העצמיות, ראשוניות, שמיד נראה שהיא תכונה חזקה יותר, נוגעת לאינטרקציה של האבר עם אברים אחרים.

3.2.33 הגדרה אבר $p \in R$ הוא ראשוני אם $p \mid ab$ נובע ש- $p \mid a$ או $p \mid b$.

3.2.34 תרגיל ()** כל אבר ראשוני הוא אי-פריק.

3.2.35 תרגיל ()** האבר p הוא ראשוני אם ורק אם R_p אידיאל ראשוני.

3.2.36 תרגיל ()** 1. המספר 2 לעולם אינו ראשוני ב- $\mathbb{Z}[\sqrt{D}]$.

הדרכה. הראה ש- $\mathbb{Z}[\sqrt{D}]/\langle 2 \rangle \cong \mathbb{F}_2[\epsilon \mid \epsilon^2 = 0]$.

2. הוא ראשוני ב- $\mathcal{O}_D$ אם ורק אם $D \equiv 5 \pmod{8}$.

3.2.37 תרגיל (*)** $\mathbb{Q}[x, y, z]/\langle z^2 - xy \rangle$ הוא תחום שלמות, שבו x אי-פריק ואינו ראשוני. (השווה לתרגיל 3.3.33, עמ' 83).

3.3 פירוק לגורמים

בסעיף זה נעסוק בכמה סוגים חשובים של תחומי שלמות, שרובם מוגדרים על-פי סוג הפירוק לגורמים שיש לאברים שלהם. המצב הטוב ביותר מבחינה זו הוא כאשר כל אבר אפשר לפרק לגורמים באופן יחיד. כדי לנתח את התכונה הזו, נציג שתי משפחות של חוגים שהגדרתן נוגעת בקיום הפירוק, ואז נלמד תנאים המבטיחים שהפירוק יהיה יחיד. כמה ממשפחות החוגים שנפגוש מופיעות בדיאגרמה 3.1.

3.3.1 חוגים אטומיים

3.3.1 הגדרה תחום שלמות שבו לכל אבר שונה מאפס יש פירוק לגורמים אי-פריקים נקרא אטומי.

לצורך הגדרה זו ודומותיה אנחנו מסכימים שמכפלה ריקה היא מחלקת החברות של אבר היחידה, כלומר של האברים ההפיכים. הפירוק לגורמים אי-פריקים אינו בהכרח יחיד. לעומת זאת, פירוק לגורמים ראשוניים - אם קיים כזה - הוא יחיד (תרגיל 3.3.35).

תרגיל 3.3.2 ()** הראה ש- $\mathbb{Z}$ אטומי.

תרגיל 3.3.3 (*)** כל החוגים מהצורה $\mathcal{O}_D$ (של סעיף 3.1) הם אטומיים.

תרגיל 3.3.4 (-)** כל שדה הוא אטומי, באופן ריק.

תרגיל 3.3.5 (*)** החוגים $\mathbb{Q}[x, y]$ ו- $\mathbb{Z}[x]$ הם אטומיים.

תרגיל 3.3.6 ()** הראה שבפירוקים $-6 = \sqrt{-6} \cdot \sqrt{-6} = -2 \cdot 3$ בחוג $\mathbb{Z}[\sqrt{-6}]$, כל הגורמים אי-פריקים, אינם חברים זה לזה, ואינם ראשוניים.

דוגמא 3.3.7 בחוג $\mathbb{Z}[\sqrt{-7}]$, $(1 - \sqrt{-7})(1 + \sqrt{-7}) = 2 \cdot 2$, שני פירוקים שונים לגורמים איפריקים, שבאחד מהם שני גורמים ובשני שלושה. (חוג שבו מספר הגורמים האי-פריקים של a קבוע, גם אם אין בהכרח פריקות יחידה, נקרא Half Factorial Domain).

תרגיל 3.3.8 (*)** יהי $A = A(\mathbb{C})$ חוג הפונקציות האנליטיות ב- $\mathbb{C}$. הראה ש- $f \in A$ הוא הפיך אם ורק אם $f(z) \neq 0$ לכל $z \in \mathbb{C}$. הראה שכל אבר אי-פריק חסר ל- $\alpha - z$ עבור $\alpha \in \mathbb{C}$ כלשהו. הוכח שכל אבר אי-פריק של A הוא ראשוני. הראה ש- A אינו אטומי. *הדרכה:* לטענה האחרונה, הראה שכל מכפלה של אי-פריקים דומה לפולינום.

תרגיל 3.3.9 (*)** יהי $A(\mathbb{C})$ החוג מתרגיל 3.3.8. הראה שהאידיאל $\langle z \rangle \triangleleft A(\mathbb{C})$ הוא מקסימלי, ותאר את האברים בחוג המקומי $A(\mathbb{C})_{\langle z \rangle}$, כתת-חוג של שדה הפונקציות המרומורפיות. הראה שחוג זה הוא אטומי.

תרגיל 3.3.10 ()** תן דוגמא לחוג אטומי עם תת-חוג שאינו אטומי.

תרגיל 3.3.11 (*)** נתבונן בחוג $R' = F[x, y, yx^{-1}, yx^{-2}, \dots] \subseteq F(x)[y]$. הראה ש- R' אינו אטומי.

דוגמא נוספת לחוג שאינו אטומי:

תרגיל 3.3.12 (*)** יהי R החוג מתרגיל 1.3.78 (עמ' 42). הגדר "מעלה עליונה" ו"מעלה תחתונה" $\deg, \overline{\deg}: R \rightarrow \mathbb{Q}$, באופן המתבקש. הראה שפונקציית הרוחב $\nu(f) = \overline{\deg}(f) - \deg(f)$ היא אדיטיבית: $\nu(fg) = \nu(f) + \nu(g)$. הוכח: כל מחלק של מונום הוא מונום. אף מונום אינו אי-פריק. הסק שהחוג אינו אטומי.

חוג אטומי שחוג הפולינומים מעליו אינו אטומי:

תרגיל 3.3.13 (***) התבונן בחוג

$$R = k[t, \lambda, \lambda', \mu, \mu'] [t^{-n} \lambda \lambda', t^{-n} \mu \mu']_{n=1,2,\dots}.$$

הראה ש- R אטומי, ושהפולינום $\lambda \lambda' x + \mu \mu' \in R[x]$ אינו מכפלה של גורמים אי-פריקים, כך ש- $R[x]$ אינו אטומי.

(ראה גם מאמרו של משה רויטמן, Polynomial extensions of atomic domains, J. Pure and Applied Algebra 87(2), 187–199, (1993), שבו הוא נותן דוגמא לתחום שלמות אטומי R (עם תכונות נוספות) כך ש- $R[x]$ אינו אטומי.)

תרגיל 3.3.14 (**) חוג הפולינומים בכל קבוצה של משתנים מעל $\mathbb{Z}$ הוא אטומי.

תרגיל 3.3.15 (**) אטומיות אינה עוברת לתחומי מנה. הדרכה. כל תחום שלמות הוא מנה של חוג מהצורה $\mathbb{Z}[\{t_\alpha\}]$, ואלו אטומיים לפי תרגיל 3.3.14.

3.3.2 חוגים נתריים

הצעד הבא שלנו הוא למצוא תנאי שיבטיח שחוג הוא אטומי. נתחיל בהגדרה כללית שאותה נחקור בהמשך הסעיף.

הגדרה 3.3.16 נאמר שחוג מקיים את תנאי השרשרת העולה אם כל שרשרת עולה של אידיאלים שמאליים $L_1 \subseteq L_2 \subseteq \dots$ נעשית קבועה. כלומר, לא קיימות בו שרשראות אינסופיות עולות ממש $L_1 \subset L_2 \subset \dots$.

חוג המקיים את תנאי השרשרת העולה נקרא חוג נתרי, על-שם אמי נתר, תלמידתו של דויד הילברט.

באופן דומה אפשר להגדיר את תנאי השרשרת העולה על כל קבוצה סדורה. אומרים שחוג (קומוטטיבי) מקיים את תנאי השרשרת העולה על אידיאלים ראשיים אם כל שרשרת עולה של אידיאלים ראשיים מוכרחה להסתיים. נזכיר ש- $a \mid b$ הוא מחלק אמיתי אם a, b אינם חברים.

טענה 3.3.17 תנאי השרשרת העולה על אידיאלים ראשיים שקול לטענה שאין שרשרת של מחלקים אמיתיים $a_1 \mid a_2 \mid \dots \mid a_n \mid \dots$.

משפט 3.3.18 תחום המקיים את תנאי השרשרת העולה על אידיאלים ראשיים הוא אטומי.

הוכחה. נניח ש- $a_0 \neq 0$ הוא אבר שאינו מכפלה של גורמים אי-פריקים. נגדיר באינדוקציה סדרת מחלקים אמיתיים $a_0 \mid a_1 \mid \dots \mid a_n \mid \dots$: לפי הנחת האינדוקציה a_n אינו מכפלה של גורמים אי-פריקים, ולכן יש לו מחלק לא טריוויאלי $a_{n+1} \mid a_n$ שגם הוא אינו מכפלה של גורמים אי-פריקים. כעת $Ra_0 \subset Ra_1 \subset \dots$ סדרה עולה של אידיאלים ראשיים. $\square$

ההיפך אינו נכון:

תרגיל 3.3.19 (*)** Atomic rings without ACC on principal ideals, J. Algebra **74**, 223-231, ב-1982) נותן אברהם זקס דוגמה לחוג אטומי שאינו מקיים את תנאי השרשרת העולה על אידיאלים ראשיים. יהי F שדה; נסמן $A = F[x, y, z^*]$, כאשר $x = \{x_0, x_1, \dots\}$, $y = \{y_0, y_1, \dots\}$, ו- z^* מסמן את הקבוצה $\{z^{2^{-n}}\}$. תהי $S \subseteq F[z^*]$ קבוצת הפולינומים שאינם מתאפסים ב-0. הראה ש- $S^{-1}A$ הוא חוג אטומי שאינו מקיים את תנאי השרשרת העולה על אידיאלים ראשיים. (זקס משאיר את השאלה האם A עצמו אטומי - פתוחה). הדוגמה הראשונה לתחום שלמות אטומי שאינו מקיים את תנאי השרשרת על אידיאלים ראשיים ניתנה על-ידי Anne Grams, 1974.

תרגיל 3.3.20 ()** כל חוג בעל נורמה (הגדרה 3.1.20) הוא אטומי.

תרגיל 3.3.21 ()** אם R אטומי אז גם $R[t]$ אטומי.

נעבור לדון בתחומים נתריים. ראשית, תחום נתרי מקיים את תנאי השרשרת העולה, ולכן הוא אטומי:

תרגיל 3.3.22 (*) תחום שלמות נתרי מקיים את תנאי השרשרת העולה על אידיאלים ראשיים.

נאמר שחוג מקיים את **עקרון המקסימום**, אם בכל מחלקה של אידיאלים של החוג יש אידיאל מקסימלי (באותה מחלקה!). מתברר שעקרון חשוב זה שקול לנתריות:

תרגיל 3.3.23 ()** חוג מקיים את תנאי השרשרת העולה אם ורק אם הוא מקיים את עקרון המקסימום.

בזכות עקרון המקסימום, מחלקת החוגים הנתריים היא אולי המחלקה החשובה ביותר בתורת החוגים. התרגיל הבא נותן למחלקה זו משנה חשיבות:

תרגיל 3.3.24 (*)** כל חוג מנה של חוג נתרי הוא נתרי.

נציג כמה דוגמאות קלות:

תרגיל 3.3.25 (*) כל חוג סופי הוא נתרי.

תרגיל 3.3.26 (*)** חוג השלמים $\mathbb{Z}$ הוא נתרי, כלומר, אין בו שרשראות עולות של אידיאלים. מאידך, יש בו שרשראות יורדות.

מתברר שנתריות קשורה לקיומן של קבוצות יוצרים סופיות.

תרגיל 3.3.27 (*)** חוג הוא נתרי אם ורק אם כל אידיאל שמאלי שלו נוצר סופית (כאידיאל). הדרכה. תהי $I_1 \subseteq I_2 \subseteq \dots$ שרשרת; קח $J = \cup I_i$, אז לפי ההנחה $J = Rb_1 + \dots + Rb_t$ לאיזהו אברים $b_1, \dots, b_t$. לכן קיים n כך שכל $b_i \in I_n$, ומכאן $I_n = I_{n+1} = I_{n+2} = \dots$.

תרגיל 3.3.28 (*)** חוג הפולינומים $\mathbb{Q}[x_1, x_2, \dots]$ מקיים את תנאי השרשרת העולה על אידיאלים ראשיים (לפי מעלה כוללת), אבל אינו נתרי.

תרגיל 3.3.29 (*)** תת-החוג $R = \mathbb{Q}[xy, xy^2, xy^3, \dots]$ של $\mathbb{Q}[x, y]$ אינו נוצר סופית. החוג R גם אינו נתרי.

משפט 3.3.30 (משפט הבסיס של הילברט) אם R חוג נתרי אז גם חוג הפולינומים $R[x]$ הוא נתרי.

הוכחה. נניח ש- $R[x]$ אינו נתרי. אז יש לו אידיאל שמאלי $I \leq_\ell R[x]$ שאינו נוצר סופית. נבחר $f_0 = 0$, ולכל $j > 0$ יהי $f_j \in I$ פולינום ממעלה n_j שהיא מינימלית כך ש- $f_j \notin \sum_{i < j} R[x]f_i$. יהי a_j המקדם העליון של f_j . אם $a_j \in \sum_{i < j} Ra_i$ אז אפשר לכתוב $a_j = \sum_{i < j} r_i a_i$ 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 , ועם אותן תכונות, בסתירה. לכן $\sum Ra_i$ אינו נוצר סופית, וגם R אינו נתרי. $\square$

שילוב של תרגילים 3.3.26, 1.2.104 ו-3.3.24 עם המשפט, מראה שכל חוג קומוטטיבי נוצר סופית הוא נתרי.

3.3.3 תחומי פריקות יחידה

הגדרה 3.3.31 תחום שלמות נקרא **תחום פריקות יחידה** אם כל אבר שלו מתפרק כמכפלה של גורמים אי-פריקים באופן יחיד, עד כדי סדר וחברות.

(יש הקוראים לתחום פריקות יחידה "תחום גאוס").

אלו הם, אם כן, החוגים שבהם מתקיימת גרסה של המשפט היסודי של האריתמטיקה. בשנת 1847 הציע Gabriel Lamé הוכחה למשפט האחרון של פרמה, על העדר פתרונות שלמים למשוואה $x^p + y^p = z^p$, שהיה מבוסס על הפירוק לגורמים $z^p = \prod (x + \rho_p^i y)$ בחוג $\mathbb{Z}[\rho_p]$. ג'וזף ליוביל הבחין בשגיאה: הפתרון של Lamé מניח שהפירוק לגורמים בחוג $\mathbb{Z}[\rho_p]$ הוא יחיד, וזה לא תמיד כך. הבחנה זו הביאה את ארנסט קומר לחקור את תכונת הפריקות היחידה (ולהוכיח את משפט פרמה עבור ראשוניים רגולריים). החסרון בהגדרה הוא שהיא אינה מסבירה "מדוע" הפירוק הוא יחיד, ולשם כך נצטרך למצוא תכונות אחרות, חזקות יותר, המבטיחות פירוק יחיד לגורמים. הקשר לחוגים אטומיים הוא ברור:

תרגיל 3.3.32 (*) כל תחום פריקות יחידה הוא אטומי.

תרגיל 3.3.33 (*)** החוג $\mathbb{Q}[x^2, xy, y^2] \subseteq \mathbb{Q}[x, y]$ הוא אטומי, אבל אינו תחום פריקות יחידה: x^2, xy, y^2 כולם אי-פריקים בו ואינם חברים, אבל $x^2 \cdot y^2 = (xy)^2$.

טענה 3.3.34 בתחום פריקות יחידה, כל אבר אי-פריק הוא ראשוני.

תרגיל 3.3.35 (*)** נניח שלאבר a בתחום שלמות יש פירוק לגורמים ראשוניים. אז זהו הפירוק היחיד שלו לגורמים אי-פריקים.

משפט 3.3.36 התכונות הבאות של תחום שלמות R הן שקולות:

1. R הוא תחום פריקות יחידה.

2. R הוא תחום אטומי שבו כל אי-פריק הוא ראשוני.

3. כל אבר (שונה מאפס) של R הוא מכפלה של ראשוניים.

הוכחה. תחום פריקות יחידה הוא אטומי (תרגיל 3.3.32) וכל אבר אי-פריק בו הוא ראשוני (טענה 3.3.34). מצד שני, כשכל אי-פריק הוא ראשוני, הפירוק לגורמים יחיד לפי תרגיל 3.3.35. $\square$

הערה 3.3.37 לפי ההגדרה, תחום פריקות יחידה הוא תחום אטומי שבו כל שני פירוקים לגורמים אי-פריקים הם באותו אורך ובעלי גורמים חברים עד כדי סדר. ב-2011 הראו *W. W. Smith* ו-*J. Coykendall*, *J. Algebra* 332(1), 62–70, (2011), שכדי שתחום אטומי יהיה בעל פריקות יחידה די להניח שהגורמים חברים עד כדי סדר בפירוקים מאותו אורך.

תרגיל 3.3.38 (*)** אם כל אבר שונה מאפס בתחום שלמות R הוא מכפלה של אי-פריקים שכולם, למעט אחד לכל היותר, הם ראשוניים, אז R הוא תחום פריקות יחידה.

תרגיל 3.3.39 ()** בכל תחום שלמות, כל מחלק של מכפלת ראשוניים $p_1 \cdots p_n$ דומה למכפלה $p_{i_1} \cdots p_{i_t}$ לאיזשהם $1 \leq i_1 < \cdots < i_t \leq n$.

תרגיל 3.3.40 (*)** כל תחום פריקות יחידה מקיים את תנאי השרשרת העולה על אידיאלים ראשיים. הדרכה. תרגיל 3.3.39.

משפט 3.3.41 (משפט קפלנסקי) תחום שלמות הוא תחום פריקות יחידה אם ורק אם כל אידיאל ראשוני שונה מאפס מכיל אבר ראשוני.

הוכחה. יהי R תחום פריקות יחידה, ויהי $P \triangleleft R$ אידיאל ראשוני עם $a \in P, a \neq 0$. נפרק $a = p_1 \cdots p_n$ לגורמים ראשוניים. מכיוון ש- $p_1 \cdots p_n \in P$, אחד הגורמים שייך ל- P . בכיוון ההפוך, נניח ש- R תחום שלמות שבו כל אידיאל ראשוני שונה מאפס מכיל אבר ראשוני. נתבונן במוניד S הנוצר על-ידי כל האברים ההפיכים וכל האברים הראשוניים של R . ניקח אידיאל מקסימלי $S^{-1}P \triangleleft S^{-1}R$, אז $P \cap S = \emptyset$, וכדי שלא לסתור את ההנחה בהכרח $P = 0$. מכאן ש- $S^{-1}R$ שדה, כלומר כל אבר שונה מאפס של R שייך ל- S . $\square$

תרגיל 3.3.42 (*)** תחום שלמות הוא אטומי אם ורק אם כל אידיאל ראשוני שונה מאפס מכיל אבר אי-פריק. הדרכה. יהי R תחום אטומי, ויהי $P \triangleleft R$ אידיאל ראשוני עם $a \in P, a \neq 0$. נפרק $a = \pi_1 \cdots \pi_n$ לגורמים אי-פריקים. מכיוון ש- $\pi_1 \cdots \pi_n \in P$, אחד הגורמים שייך ל- P .

בכיוון ההפוך, נניח ש- R תחום שלמות שבו כל אידיאל ראשוני שונה מאפס מכיל אבר אי-פריק. נתבונן במוניד S הנוצר על-ידי כל האברים ההפיכים וכל האברים האי-פריקים של R . ניקח אידיאל מקסימלי $S^{-1}P \triangleleft S^{-1}R$, אז $P \cap S = \emptyset$, וכדי שלא לסתור את ההנחה בהכרח $P = 0$. מכאן ש- $S^{-1}R$ שדה, כלומר כל אבר שונה מאפס של R שייך ל- S .

תרגיל 3.3.43 ()** נתבונן בחוגים $R = F[x, y] \subset R' = F[x, y, yx^{-1}] \subseteq F(x, y)$. הראה ש- R' אינו מהצורה $S^{-1}R$ לאף מוניד $S \subseteq R$. בפרט, לא כל הרחבה של תחום פריקות יחידה מתקבלת על-ידי מיקום.

3.3.4 תחומים ראשיים

הגדרה 3.3.44 תחום ראשי הוא תחום שלמות שבו כל אידיאל נוצר על-ידי אבר אחד.

זהו מקרה קיצוני של תכונת הנתריות (תרגיל 3.3.27), ולכן

תרגיל 3.3.45 (*) כל תחום ראשי הוא נתר.

טענה 3.3.46 בתחום ראשי, אם a אי-פריק אז Ra אידיאל מקסימלי.

הוכחה. לפי תרגיל 3.2.25, Ra מקסימלי בין האידיאלים הראשיים של R , אבל מכיוון שכל האידיאלים ראשיים, פירושו של דבר הוא ש- Ra מקסימלי. $\square$

תרגיל 3.3.47 ()** נניח ש- R תחום ראשי. הראה שאם p אי-פריק ואינו מחלק את a אז Ra, Rp קו-מקסימליים.

כעת מאפשר משפט השאריות הסיני (2.2.15) לחשב את חוגי המנה של כל תחום ראשי:

תרגיל 3.3.48 ()** כל מנה (לא טריוויאלית) של תחום ראשי היא סכום סופי של חוגים מקומיים. ביתר פירוט, יהי R תחום ראשי. נניח ש- $a = p_1^{e_1} \cdots p_t^{e_t}$ הפירוק של $a \in R$ לגורמים אי-פריקים. אז $R/\langle a \rangle = R/\langle p_1^{e_1} \rangle \oplus \cdots \oplus R/\langle p_t^{e_t} \rangle$. בנוסף לזה, כל גורם $R/\langle p^e \rangle$ הוא חוג מקומי, והוא שדה אם ורק אם $e = 1$.

תרגיל 3.3.49 ()** בתחום ראשי, כל אבר אי-פריק הוא ראשוני. הדרכה: תרגילים 3.3.47 ו-2.2.9; לחילופין, טענה 3.3.46.

תרגיל 3.3.50 ()** בתחום ראשי, כל אידיאל ראשוני שונה מאפס הוא מקסימלי. הדרכה: אם $Rb \subseteq Rp$ אידיאלים ראשוניים אז $b \mid a$ ו- $a \sim b$ כי a ראשוני.

תרגיל 3.3.51 ()** כל תחום ראשי הוא תחום פריקות יחידה. הדרכה: משפט 3.3.36 ו-תרגיל 3.3.49.

משפט 3.3.52 (המשפט היסודי של האריתמטיקה) $\mathbb{Z}$ הוא תחום פריקות יחידה.

הוכחה. תרגיל 3.3.51 ומשפט 1.3.2. $\square$

תרגיל 3.3.53 (*)** $\mathbb{Z}[x]$ תחום פריקות יחידה נתר, אבל אינו ראשי.

תרגיל 3.3.54 ()** בחוג $R = \mathbb{Q}[x, y]$, x ראשוני אבל $\langle x \rangle$ אינו מקסימלי.

תרגיל 3.3.55 (*)** יהי R תחום ראשי עם שדה שברים F . עבור חוג ביניים $R \subseteq R' \subseteq F$, נסמן $S = \{a \in R : a^{-1} \in R'\}$. הראה ש- $R' = S^{-1}R$.

תרגיל 3.3.56 (*)** ראשיות 'עולה למעלה', כלומר, אם R תחום ראשי ו- $R \subseteq R'$ אז גם R' ראשי.

תרגיל 3.3.57 (*)** תחום שלמות הוא ראשי אם ורק אם הוא תחום פריקות יחידה, וכל אידיאל ראשוני שונה מאפס הוא מקסימלי. הדרכה: תחום ראשי הוא תחום פריקות יחידה לפי תרגיל 3.3.51, וכל אידיאל ראשוני שונה מאפס הוא מקסימלי לפי תרגיל 3.3.50. לכיוון ההפוך העזר בעובדה (שלא הוכחנו) שתחום שלמות שבו כל אידיאל ראשוני הוא ראשי, הוא תחום ראשי בעצמו.

מחלק משותף מקסימלי

אחת התכונות העיקריות של תחום ראשי היא שלכל שני אברים בו יש מחלק משותף מקסימלי, שהוא אף צירוף שלם של האברים. תכונה זו מזמינה הכללה של תחומים ראשיים, הנקראת תחומי בזו, שתטופל בסעיף הבא. בסעיף זה נדון במשפחה עוד יותר רחבה של חוגים, שבה דורשים שהמחלק המשותף המקסימלי יהיה מוגדר, ותו לא.

הגדרה 3.3.58 יהי R תחום שלמות. אבר d הוא מחלק משותף של $a, b \in R$ אם $d \mid a, b$. אבר d הוא מחלק משותף מקסימלי (ממ"מ) של $a, b \in R$, אם הוא מחלק משותף, וכל מחלק משותף מחלק אותו. אם קיים מחלק משותף מקסימלי, מסמנים אותו ב- (a, b) .

תרגיל 3.3.59 ()** אם a, b יש ממ"מ d , אז d' הוא ממ"מ אם ורק אם $d \sim d'$. במילים אחרות, הממ"מ הוא מחלקת חבורות. הדרכה: אם d, d' מחלקים משותפים מקסימליים, אז $d' \mid d$ ו- $d \mid d'$.

כמובן, לא לכל שני אברים בתחום שלמות יש ממ"מ.

תרגיל 3.3.60 ()** d הוא מחלק משותף מקסימלי של a, b אם ורק אם Rd הוא מינימום בין האידיאלים הראשיים המכילים את $Ra + Rb$.

תרגיל 3.3.61 ()** הוכח שהתכונות הבאות שקולות עבור $a, b \in R$:

1. d הוא ממ"מ של a, b .

2. $x \mid a, b$ אם ורק אם $x \mid d$.

3. Rd מינימלי בין האידיאלים הראשיים המכילים את $Ra + Rb$.

תרגיל 3.3.62 ()** אם $a \sim a'$ ו- $b \sim b'$ אז $(a, b) \sim (a', b')$.

תרגיל 3.3.63 (*)** יהי R תחום שלמות עם שדה השברים F . נסמן

$$\bar{I} = \{x \in F : \exists y \in R \implies xy \in I\}.$$

הראה שזהו אידיאל של R המכיל את I . (השווה להגדרת $(R:(R:I))$ בתרגיל 1.2.61).

תרגיל 3.3.64 (*)** הראה של- $a, b \in R$ יש ממ"מ אם ורק אם $\overline{Ra + Rb}$ ראשי.

תרגיל 3.3.65 (*)** בחוג $R = \mathbb{Q}[abc, bcd, bd, cd, ab, ac] \subseteq \mathbb{Q}[a, b, c, d]$, אין ל- ab^2cd, abc^2d מחלק משותף מקסימלי.

תרגיל 3.3.66 ()** אם $d = (a, b)$ קיים, אז $(a/d, b/d) = 1$. הדרכה: אם $x \mid a/d, b/d$ אז $xd \mid a, b$ ולכן $xd \mid d$ ו- $x \sim 1$.

תרגיל 3.3.67 ()** אם (b, c) ו- (ab, ac) קיימים, אז $(ab, ac) = a(b, c)$. הדרכה: נסמן $d = (b, c)$. מכיון ש- $d \mid b, c$ ברור ש- $ad \mid ab, ac$ ולכן $ad \mid (ab, ac)$. נכתוב $(ab, ac) = ax \mid ab, ac$ ולכן $ax \mid b, c$ ו- $x \mid d$. מכאן ש- $(ab, ac) = ax \mid ad$.

תרגיל 3.3.68 ()** אם (b, c) קיים אז לכל ראשוני p , גם (pb, pc) קיים. הדרכה. ברור $p \mid pb, pc \mid pc$. נניח $p \mid pb, pc \mid pc$ ו- $p \nmid x$. אם $p \mid x$ אז אפשר לפרק $x = px'$ ואז $x' \mid b, c$ ולכן $x' \mid (b, c)$ ו- $x = px' \mid p(b, c)$. אם $p \nmid x$, נכתוב $xb' = pc'$ ו- $x' = pb'$ או $x' = pc'$ ו- $x \mid b, c$ ומכאן $p \mid b', c'$ ו- $x \mid (b, c)$.

עם זאת, מכך ש- (b, c) קיים לא נובע ש- (ab, ac) קיים:

תרגיל 3.3.69 (*)** נתבונן בחוג $R = \mathbb{Z}[2\sqrt{-2}] = \mathbb{Z}[\theta : \theta^2 = -8]$. נראה שיש שני אי-פריקים a, b כך של- $4a, 4b$ אין מחלק משותף מקסימלי.

1. האברים האי-פריקים היחידים שהנורמה שלהם מחלקת את 144 הם (עד כדי סימן) $2, 3, \theta, 1 \pm \theta, 2 \pm \theta, 4 \pm \theta$.

2. $2 \cdot 2 \cdot 3 = (2 + \theta)(2 - \theta)$ ו- $2 \cdot 2 \cdot (1 - \theta) = -(2 + \theta)^2$ הם הפירוקים היחידים לגורמים אי-פריקים (עד כדי חברות) של האברים $12, 4(1 - \theta)$.

3. המחלקים המשותפים היחידים של $12, 4(1 - \theta)$ הם $1, 2, 4, 2 + \theta$.

4. ל- $12, 4(1 - \theta)$ אין מחלק משותף מקסימלי.

5. $(6, 2(1 - \theta)) = 2$.

הגדרה 3.3.70 אברים $a, b \in R$ הם זרים במובן החלש אם אין להם אף מחלק משותף שאינו הפיך.

תרגיל 3.3.71 (*) $a, b \in R$ זרים במובן החלש אם ורק אם 1 הוא מחלק משותף מקסימלי שלהם (כלומר $(a, b) = 1$).

תרגיל 3.3.72 (*) אם אברים $a, b \in R$ הם קו-מקסימליים (הגדרה 2.2.20) אז הם זרים במובן החלש.

תחומי gcd

את (מחלקת החברות של) המחלק המשותף המקסימלי של a, b , אם הוא קיים, מסמנים כאמור ב- (a, b) . בתחומי פריקות יחידה (וגם בתחומי בזו שנלמד בהמשך) לכל שני אברים יש מחלק משותף מקסימלי, ולכן נלמד כאן את התכונה הזו כשהיא עומדת בזכות עצמה.

הגדרה 3.3.73 תחום שלמות שבו לכל שני אברים יש מחלק משותף מקסימלי נקרא תחום gcd.

למה 3.3.74 בתחום פריקות יחידה, לכל a, b קיימים ראשוניים $p_1, \dots, p_n$ שאינם חברים, ומספרים חיוניים $\alpha_1, \dots, \alpha_n, \beta_1, \dots, \beta_n \geq 0$, והפיכים u, v , כך ש- $a = up_1^{\alpha_1} \dots p_n^{\alpha_n}$ ו- $b = vp_1^{\beta_1} \dots p_n^{\beta_n}$.

הוכחה. ראשית פרק את a ואת b לגורמים, ואז החלף כל גורם של b החבר לגורם של a , בגורם של a . $\square$

תרגיל 3.3.75 ()** כל תחום פריקות יחידה הוא תחום gcd. הדרכה. בעקבות למה 3.3.74, $\min\{\alpha_1, \beta_1\} \dots \min\{\alpha_n, \beta_n\}$ הוא מחלק משותף מקסימלי.

תרגיל 3.3.76 (*) בחוג gcd מתקיים $(a, (b, c)) \sim ((a, b), c)$.

תרגיל 3.3.77 (-*)** בחוג $\gcd$, אם $(a, b) \sim (a, c) \sim 1$ ו- $(a, bc) \sim 1$ אז $(a, b) \sim (a, c)$. הדרכה: לפי תרגילים 3.3.76 ו-3.3.67, $(a, bc) = ((a, ac), bc) = (a, (ac, bc)) \sim (a, (a, b)c) = (a, c) \sim 1$.

תרגיל 3.3.78 (-*)** בתחום $\gcd$, אם $(a, b) \sim 1$ אז גם $(a^2, b^2) \sim 1$. הדרכה: $(a, b^2) \sim 1$ לפי תרגיל 3.3.77.

תרגיל 3.3.79 (*) נניח ש- R תחום $\gcd$. הראה שאם p אי-פריק ואינו מחלק את a אז $(a, p) \sim 1$; זוהי הכללה של תרגיל (3.3.47).

תרגיל 3.3.80 ()** בתחום $\gcd$, כל אבר אי-פריק הוא ראשוני. הדרכה: תרגילים 3.3.79 ו-3.3.77. (זוהי גרסה חזקה של תרגיל (3.3.49)).

משפט 3.3.81 תחום שלמות הוא תחום פריקות יחידה אם ורק אם הוא תחום $\gcd$ אטומי.

הוכחה. לפי משפט 3.3.36 ותרגילים 3.3.35 ו-3.3.75. $\square$

תרגיל 3.3.82 (-*)** הראה שבחוג $R = \mathbb{Q}[x^2, y^2, z^2, xy, xz, yz]$ אין ל- x^2yz^2 ול- xyz^2 ממ"מ, ולכן תחום זה אינו $\gcd$.

תחומי בזו

הגדרה 3.3.83 יהי R תחום שלמות. אם $Ra + Rb = Rd$, נאמר ש- d הוא מחלק משותף מקסימלי חזק של a, b .

תרגיל 3.3.84 (*) כל ממ"מ חזק הוא בפרט ממ"מ: אם $Ra + Rb$ אידיאל ראשי, אז היוצר שלו הוא ממ"מ.

לפי תרגיל 3.3.84, ממ"מ הוא ממ"מ חזק אם ורק אם הוא מהווה צירוף שלם של האברים. מחלקים מושתפים מקסימליים כאלה קיימים אם ורק אם כל אידיאל הנוצר על-ידי שני אברים הוא ראשי; קל לראות שההגדרה שקולה לתכונה הבאה:

הגדרה 3.3.85 חוג שבו כל אידיאל נוצר סופית הוא ראשי נקרא חוג בזו.

החוגים נקראים כך על-שם המתמטיקאי הצרפתי Étienne Bézout, 1730-1783. אם כן, חוגי בזו הם החוגים שבהם לכל שני אברים יש מחלק משותף מקסימלי חזק.

תרגיל 3.3.86 ()** כל תחום בזו הוא תחום $\gcd$. הדרכה: ממ"מ חזק הוא ממ"מ.

תרגיל 3.3.87 (+*) תחום שלמות הוא ראשי אם ורק אם הוא נתר ו-גם בזו.

תרגיל 3.3.88 (-*)** כל תחום פריקות יחידה שהוא בזו הוא ראשי.

תרגיל 3.3.89 ()** 1. החוג $R = \bigcup F[x^{1/n!}]$ מתרגיל 1.3.78 (עמ' 42) הוא תחום בזו אבל אינו אטומי (ולכן אינו ראשי).

2. החוג $\mathbb{Z} + x\mathbb{Q}[x]$ הוא תחום בזו אבל אינו ראשי. הדרכה: x אינו אטומי.

תרגיל 3.3.90 (-*)** לכל R שהוא חוג- $\gcd$ ואינו אטומי, $R[t]$ הוא חוג- $\gcd$ שאינו בזו ואינו אטומי (ממילא אינו תחום פריקות יחידה).

תרגיל 3.3.91 (*)** 1. חוג השווה לאיחוד של תת-חוגים ראשיים הוא חוג בזו:

$$\text{ראשי} \iff \text{איחוד תת-חוגים ראשיים} \iff \text{בזו}$$

2. החוג $R = \mathbb{Z} + x\mathbb{Q}[x]$ הוא תחום בזו, אבל אינו איחוד של תת-חוגים ראשיים.

הדרכה. אם $R_0 \subseteq R$ תת-חוג ראשי ו- $x \in R_0$ אז לכל ראשוני $p \in \mathbb{Z}$, $R_0 p + R_0 x$ ראשי ב- R_0 ולכן נוצר על-ידי p ולכן $\frac{x}{p} \in R_0$; לכן $\mathbb{Q}x \subseteq R_0$; אבל $R = R_0$ אינו ראשי כי האידיאל $x\mathbb{Q}[x]$ אינו נוצר סופית.

תרגיל 3.3.92 ()** הוכח, ללא שימוש בתחומי gcd, שבתחום בזו כל אבר אי-פריק הוא ראשוני. הדרכה. לאור תרגיל 2.1.9 (עמ' 46), המסקנה של טענה 3.3.46 נכונה בכל תחום בזו.

תרגיל 3.3.93 ()** החוג $\mathbb{Q}[x, y]$ הוא תחום gcd נתרי שאינו בזו (ולכן אינו ראשי).

תרגיל 3.3.94 (*)** נניח ש- $D \equiv 1 \pmod{4}$. הוכח ש-2 אי-פריק ב- $\mathbb{Z}[\sqrt{D}]$ אבל אינו ראשוני. הדרכה. 2 אי-פריק כי אין אברים מנורמה ± 2 (תרגיל 3.2.32, עמ' 78), אבל 2 אינו ראשוני כי $2 \mid (1 + \sqrt{D})^2$ ו- $2 \nmid (1 + \sqrt{D})$. הערה. נימוק זה אינו פועל על $\mathcal{O}_D$, כי שם $2 \mid (1 + \sqrt{D})$.

תרגיל 3.3.95 (*)** נניח ש- $D \leq -3$. הוכח ש-2 אי-פריק ב- $\mathbb{Z}[\sqrt{-D}]$ אבל אינו ראשוני. הדרכה. 2 אי-פריק כי אין אברים מנורמה ± 2 . בחר x עם אותה זוגיות כמו D , אז $2 \mid x^2 + D$ אבל $(x + \sqrt{D})(x - \sqrt{D}) \notin \mathbb{Z}[\sqrt{D}]$.

תרגיל 3.3.96 (*)** נניח ש- $D \equiv 1 \pmod{8}$.

1. הראה שהאידיאל $I = \left\langle 2, \frac{1+\sqrt{D}}{2} \right\rangle$ של $\mathcal{O}_D$ הוא אידיאל אמיתי.

2. אם, בנוסף, $D \leq -15$, אז I אינו אידיאל ראשי, ולכן $\mathcal{O}_D$ לא ראשי.

3. כאשר $D = 17$, $I = \left\langle 2, \frac{1+\sqrt{D}}{2} \right\rangle$ הוא האידיאל הראשי הנוצר על-ידי $\frac{5+\sqrt{D}}{2}$.

הדרכה. מצא אפימורפיזם $\mathcal{O}_D \rightarrow \mathbb{Z}/2\mathbb{Z}$; לחלק השני העזר בתרגיל 3.2.30. הערה. כאשר $D \equiv 5 \pmod{8}$, $\frac{5-D}{8} \cdot 2 + \frac{-1+\sqrt{D}}{2} \cdot \frac{1+\sqrt{D}}{2} = 1$ ולכן I אינו אמיתי.

הערה 3.3.97 ידוע ש- $\mathcal{O}_D$ הוא תחום ראשי עבור $D < 0$ בדיוק בתשעה המקרים $D = -1, -2, -3, -7, -11, -19, -43, -67, -163$. ראה משפט 3.3.142 לחמשת המקרים הראשונים, ותרגיל 3.3.169 לששי. (גאוס הוא הראשון ששער שיש מספר סופי של $D < 0$ שעבורם $\mathcal{O}_D$ ראשי. ב-1934 הראו Heilbronn ו-Linfoot שיש לכל היותר ערך אחד נוסף של D מלבד התשעה המובאים לעיל, ושאל קיים ערך כזה, אז השערת רימן המוכללת אינה נכונה. Heegner הוכיח שהערך העשירי אינו קיים ב-1952, אלא שההוכחה לא היתה שלמה; הבעיה נפתרה בסופו של דבר על-ידי Baker, Stark ו-1966, 1967).

הערה 3.3.98 לא ידוע האם בין החוגים $\mathcal{O}_D$ עם $0 < D$ יש אינסוף חוגים ראשיים.

היזכר בהגדרה 2.2.20:

הגדרה 3.3.99 אברים $a, b \in R$ הם קו-מקסימליים אם $Ra + Rb = R$. במלים אחרות, 1 הוא מחלק משותף מקסימלי חזק של a, b ; כלומר, Ra, Rb קו-מקסימליים.

תרגיל 3.3.100 ()** d הוא מחלק משותף מקסימלי חזק של a, b אם ורק אם אפשר לכתוב $a = da'$ ו- $b = db'$ עבור a', b' קו-מקסימליים.

כפולה משותפת מינימלית

את הכפולה המשותפת המינימלית מגדירים באופן אנלוגי למחלק המשותף המקסימלי.

הגדרה 3.3.101 יהי R תחום שלמות. אבר m הוא **כפולה משותפת מינימלית** (כמ"מ) של $a, b \in R$ אם $a, b \mid m$, ולכל $y \mid m$ מתקיים $a, b \mid y$.

תרגיל 3.3.102 ()** הוכח שהתכונות הבאות שקולות עבור $a, b \in R$:

1. m הוא כפולה משותפת מינימלית של a, b .

2. $a, b \mid y$ אם ורק אם $m \mid y$.

3. Rm מקסימלי יחיד בין האידיאלים הראשיים המוכללים ב- $Ra \cap Rb$.

תרגיל 3.3.103 ()** כפולה משותפת מינימלית של זוג אברים, אם היא קיימת, היא יחידה עד-כדי חברות.

את הכפולה המשותפת המינימלית של a, b , אם היא קיימת, מסמנים ב- $[a, b]$. בין מחלק משותף וכפולה משותפת יש חוסר סימטריה מסויים, הנעוץ בעובדה הבאה (שאין לה נוסח מקביל לממ"מ), ובזכותה אין צורך בהגדרה של "כפולה משותפת מינימלית חזקה".

תרגיל 3.3.104 ()** בכל תחום שלמות, m הוא כפולה משותפת מינימלית של a, b אם ורק אם $Ra \cap Rb = Rm$.

תרגיל 3.3.105 ()** אם m הוא כמ"מ של a, b אז $m \mid ab$.

טענה 3.3.106 אם $[a, b]$ קיים, אז $(a, b) = \frac{ab}{m}$ קיים ו- $\frac{ab}{m}$.

הוכחה. ברור ש- $\frac{ab}{m}$ מחלק את a, b . אם $x \mid a, b$ אז $x \mid \frac{ab}{x}$ ולכן $\frac{ab}{x} \in Ra \cap Rb = Rm$.
 $\square$ $x \mid \frac{ab}{m}$

תרגיל 3.3.107 ()** אם לשני אברים $a, b \in R$ יש כמ"מ (a, b) וכפולה משותפת מינימלית $[a, b]$, אז $(a, b)[a, b] \sim ab$.

טענה 3.3.108 אם $Ra + Rb = Rd$ אז $\frac{ab}{d}$ הוא כפולה משותפת מינימלית.

הוכחה. ראשית, $\frac{ab}{d} \in R$ משום ש- $d \mid ab$. כתוב $d = \alpha a + \beta b$. ברור ש- $\frac{ab}{d}$ מתחלק ב- a, b . אם $a, b \mid x$ אז $ab \mid dx = \alpha ax + \beta bx$.
 $\square$

מסקנה 3.3.109 לכל a, b בתחום שלמות:

1. אם יש כמ"מ חזק, אז יש כמ"מ;

2. אם יש כמ"מ, אז יש כמ"מ.

טענה 3.3.110 (Jacobson, Section IV.3) יהי R חוג gcd. אז $\frac{ab}{(a,b)}$ הוא כפולה משותפת מינימלית של a, b .

הוכחה. נניח $x \mid a, b$. צריך להוכיח שגם $x \mid \frac{ab}{(a,b)}$. כתוב $x = ay$, אז $b \mid ay$, ולכן, לפי תרגילים 3.3.76 ו-3.3.67, $(b, y(a, b)) = (b, (ya, yb)) = ((b, yb), ya) = (b, ya) = b$, ומכאן ש- $x(a, b) = ay(a, b) = ab \mid x$ ו- $\frac{ab}{(a,b)} \mid x$. הכיוון ההפוך טריוויאלי. $\square$

בפרט, בחוג gcd (שבו מניחים, א־פריורי, את קיומו של ממ"מ לכל שני אברים) יש כמ"מ לכל שני אברים. טענה 3.3.110 חזקה מטענה 3.3.108 כשמתבוננים בכל החוג, אבל חלשה ממנה עבור אברים נתונים. ביתר פירוט, טענה 3.3.110 מראה שבחוג gcd יש כמ"מ לכל שני אברים, בעוד שטענה 3.3.108 מראה זאת רק לתחומי בזו. מאידך, טענה 3.3.108 מספקת כמ"מ ל- a, b אם יש להם ממ"מ חזק, בעוד שאם מניחים רק שיש להם ממ"מ, בהחלט יתכן שאין להם כפולה משותפת מינימלית (ראה תרגיל 3.3.113).

תרגיל 3.3.111 ()** אם $[b, c]$ קיים אז לכל $a \neq 0$, $[ab, ac]$ קיים ושווה ל- $a[b, c]$. הדרכה. ברור ש- $a[b, c] \mid ab, ac$. נניח ש- $ab, ac \mid x$; נכתוב $x = abb' = acc'$ וכן $b, c \mid (x/a)$ ולכן $[b, c] \mid x/a$ ו- $a[b, c] \mid x$.

תרגיל 3.3.112 (*)** $[b, c]$ קיים אם ורק אם (ab, ac) קיים לכל $a \neq 0$. הדרכה. אם $[b, c]$ קיים אז $[ab, ac] = a[b, c]$ לפי תרגיל 3.3.111 ו- $(ab, ac) = abc/[b, c] = a(b, c)$ לפי טענה 3.3.106. בכיוון ההפוך, נניח שכל (ab, ac) קיים, ונראה ש- $[a, b]$ קיים ושווה ל- $ab/(a, b)$. אכן, ברור ש- $ab/(a, b) \mid ab, a$, ואם $a, b \mid x$ אז $ab \mid xa, xb$ ולכן $ab/(a, b) \mid (xa, xb) = x(a, b)$ ולכן $ab/(a, b) \mid x$. (D. Khurana, "On GCD and LCM in domains: a conjecture of Gauss", Resonance 8, 2003.)

תרגיל 3.3.113 (*)** בחוג $R = \mathbb{Z}[\delta]$, $\delta = \sqrt{-7}$, האברים $1 + \delta, 2$ זרים במובן החלש (כלומר, 1 הוא ממ"מ שלהם), אבל אין להם כמ"מ. הדרכה. המספרים מנומרה המחלקת את 16 הם $1 \pm \delta, 2 \pm \delta, 3 \pm \delta, 4$. הכמ"מ, אם קימת, צריכה לחלק את 8 וגם את $2(1 + \delta)$, שאין להם מחלקים משותפים פרט ל- $2, 1 + \delta$, שאינם מחלקים זה את זה.

תרגיל 3.3.114 (*)** בהמשך לתרגיל 3.3.113, לאברים $1 + \delta, 2$ יש כמ"מ, 1, אבל לכפולות שלהם $(1 + \delta) \cdot 2, 4 \cdot 2$ אין כמ"מ. הדרכה. נניח ש- $d = (8, 4(1 + \delta))$ אז $d \mid 4, 4(1 + \delta)$ כלומר $d = 4$, והרי $1 + \delta$ לא מחלק את 4.

תרגיל 3.3.115 (*)** בכל תחום שלמות: ל- a, b יש כמ"מ אם ורק אם ל- ta, tb יש כמ"מ.

הגדרה 3.3.116 אברים $a, b \in R$ הם זרים אם ab הוא כפולה משותפת מינימלית שלהם, כלומר $Ra \cap Rb = Rab$.

תרגיל 3.3.117 (+)** אם a, b קו־מקסימליים אז הם זרים. אם a, b זרים אז הם זרים במובן החלש (ראה הגדרה 3.3.70).

תרגיל 3.3.118 (+)** בתחום R המקיים את תנאי השרשרת העולה על אידיאלים ראשיים (ובפרט, בכל תחום נתרי), אפשר להציג כל אבר $\alpha \in F = q(R)$ כשבר $\alpha = \frac{a}{b}$ כאשר a, b זרים במובן החלש. הדרכה. קח $Ra \subseteq R \cap R\alpha$ מקסימלי. אפשר לכתוב $\alpha = \frac{a}{b}$ אם $d \mid a, b$ אבל $\frac{a}{d}, \frac{b}{d} \in R \cap R\alpha$ ומהמקסימליות נובע $d \sim 1$.

תרגיל 3.3.119 ()** בתחום בזו, שני אברים הם זרים במובן החלש אם ורק אם הם קו־מקסימליים.

תרגיל 3.3.120 ()** התנאים הבאים שקולים:

	ext	$S^{-1}R$	R_P	מנה	$R[x]$	$R[[x]]$
ראשי	כן	כן	כן	כן	לא ²	לא ²
נתרי	לא ¹	כן	כן	כן	כן	כן
בזו	כן	כן	כן	כן	לא ²	לא ²
תפ"י	לא ¹	כן	כן	לא ³	כן	
שרשרת	לא			לא ³	כן	כן
אטומי	לא			לא ³	לא ⁴	כן
gcd				לא ³	כן ⁵	
נורמלי		כן ⁵	כן ⁵			

איור 3.2: טבלת סיכום (לא שלמה)

1. a, b זרים.

2. $a \mid b$ נובע $a \mid cb$.

דוגמא 3.3.121 בחוג $R = \mathbb{Z}[x, y]$, האזורים x, y זרים (xy הוא כמ"ע), ולכן גם זרים במובן החלש ($(x, y) = 1$), למרות שאין להם מ"ע במובן החזק (ובפרט אינם קו-מקסימליים): האידיאל $Rx + Ry$ אינו ראשי.

תרגיל 3.3.122 ()** אם $[a, b]$ קיים, אז אפשר לכתוב $a = da'$ ו- $b = db'$, כאשר $d = (a, b)$ ו- a', b' זרים. הדרכה: נכתוב $Ra \cap Rb = Rm$; אז $a, b \mid m$ ולכן אפשר לכתוב $m = aa' = bb'$. כעת $Ra' \cap Rb' = Ra'b' = Rm$, ומכיוון ש- a', b' זרים, $a' \mid m$ ולכן יש d כך ש- $d = a'b'$, ומהצבה מתקבל $a = db'$ ו- $b = da'$. לבסוף $d = \frac{ab}{m} = (a', b')$ לפי טענה 3.3.106.

תרגיל 3.3.123 (*+)** השלם ונמק את טבלה 3.2. לכל אחת ממחלקות החוגים הבאות - תחומים ראשיים, תחומים נתריים, תחומי בזו, תחומי פריקות יחידה, תחומים המקיימים את תנאי השרשרת העולה על מחלקים, תחומים אטומיים, תחומי gcd - קבע האם, בהנחה ש- R שייך למחלקה גם R' שייך למחלקה, כאשר:

$$1. R \subseteq R' \subseteq F = q(R).$$

$$2. R' = S^{-1}R \text{ עבור תת-מונויד } S \text{ של } R.$$

$$3. R' = R_P \text{ עבור אידיאל ראשוני } P \triangleleft R.$$

$$4. R' = R/P \text{ הוא מנה של } R \text{ ביחס לאידיאל ראשוני.}$$

$$5. R' = R[x].$$

$$6. R' = R[[x]].$$

הדרכה חלקית. העזר בדוגמאות $[R_3 = F[\lambda_1, \lambda_2, \dots], R_2 = \mathbb{Z}, R_1 = \mathbb{Q}[x, y, \frac{x}{y}, \frac{x}{y^2}, \dots]]$; 4-ראה תרגיל 3.3.13 (עמ' 81); 5 הוא תרגיל 9 בעמ' 42 בספר של קפלנסקי.

3.3.5 חוגים אוקלידיים

נותרה לנו משימה חשובה: למצוא דרך טכנית להוכיח שחוג מסויים הוא ראשי.

הגדרה 3.3.124 יהי R תחום שלמות. פונקציה $d: R \rightarrow \mathbb{N} \cup \{-\infty\}$ המקיימת $d(0) < d(x)$ לכל $x \neq 0$ נקראת פונקציה אוקלידית אם

$$(E1) \quad d(a) \leq d(b) \text{ לכל } a \mid b, \text{ וכן}$$

$$(E2) \quad \text{לכל } b \neq 0 \text{ ולכל } a \text{ קיימים } q, r \text{ כך ש-} a = qb + r \text{ ו-} d(r) < d(b).$$

תחום שלמות שמוגדרת עליו פונקציית אוקלידית נקרא תחום אוקלידי.

אקסיומה $(E2)$, שהיא ליבת ההגדרה, מאפשרת הוכחות באינדוקציה.

תרגיל 3.3.125 (*) $d: R \rightarrow \mathbb{N} \cup \{-\infty\}$ המקיימת $d(0) < d(x)$ לכל $x \neq 0$ ואת התנאי $(E1)$ היא אוקלידית, אם ורק אם לכל $b \neq 0$ ולכל a קיים q כך ש-
 $d(a - qb) < d(b)$

תרגיל 3.3.126 (*) בחוג אוקלידי, $d(1) \leq d(x)$ לכל $x \neq 0$.

תרגיל 3.3.127 (-)** בחוג אוקלידי, a הפיך אם ורק אם $d(a) = d(1)$.

תרגיל 3.3.128 ()** $\mathbb{Z}$ חוג אוקלידי ביחס לפונקציה $d(n) = |n|$.

תרגיל 3.3.129 ()** יהי R חוג כלשהו. אם $f, g \in R[x]$ פולינומים כך שהמקדם העליון של g הפיך משמאל, אז קיימים $q, r \in R[x]$ כך ש- $f = qg + r$ ו- $\deg(r) < \deg(g)$.

תרגיל 3.3.130 ()** יהי F שדה. הראה שחוג הפולינומים $F[x]$ הוא אוקלידי ביחס לפונקציית המעלה.

תרגיל 3.3.131 ()** יהי F שדה. הראה שהחוג $F[[x]]$ של טורי טיילור הוא אוקלידי ביחס לפונקציית ν שהוגדרה בתת-סעיף 3.4.2.

תרגיל 3.3.132 (-)** כל חוג אוקלידי הוא ראשי. הדרכה: העזר בהוכחה של משפט 1.3.2: אם $0 \neq a \in I$ אידיאל, אז $0 \neq a \in I$ עם $d(a)$ מינימלי הוא יוצר של I .

אקסיומה $(E1)$ אמנם אינה נובעת מאקסיומה $(E2)$, אבל די בתנאי השני כדי להבטיח אוקלידיות:

תרגיל 3.3.133 (*)** נניח שפונקציה $d: R \rightarrow \mathbb{N} \cup \{-\infty\}$ המקיימת $d(0) < d(x)$ לכל $x \neq 0$ מקיימת את תנאי $(E2)$. הוכח שהפונקציה δ המוגדרת לפי $\delta(x) = \min_{x' \in \langle x \rangle} d(x')$ מקיימת את $(E1)$ ו- $(E2)$, ולכן R אוקלידי.

תרגיל 3.3.134 (*)** נגדיר על $\mathbb{Z}$ את הפונקציה $d(n) = \begin{cases} |n| & n \neq t \\ |T| & n = t \end{cases}$ כאשר $t, T \in \mathbb{Z}$ הם קבועים. הראה שתנאי $(E2)$ מתקיים, והסק ש- $(E1)$ אינו נובע ממנו.

אוקלידיות של חוגים סמוכים

תרגיל 3.3.135 (*)** יהי R תחום אוקלידי עם שדה שברים F , ותהי $S \subseteq R$ תת-קבוצה סגורה לכפל. הראה שהפונקציה $\bar{d}(x) = \min \{d(t) : t \in Sx \cap R\}$ על $S^{-1}R$ מקיימת את אקסיומה (E2), ולכן (לפי תרגיל 3.3.133) $S^{-1}R$ אוקלידי. הדרכה. כל $x \in S^{-1}R$ אפשר לכתוב בצורה $x = s^{-1}a$ עם $a \in R$ ולכל $s \in S$ מתקיים $\bar{d}(s^{-1}a) \leq d(a)$; אם $a = qb + r$ אז $s^{-1}a = (s^{-1}s')a + s^{-1}r$ ומקיים $\bar{d}(s^{-1}r) < \bar{d}(s'^{-1}b)$.

תרגיל 3.3.136 (**)** יהי R תחום אוקלידי עם שדה שברים F , ויהי $R \subseteq R' \subseteq F$ חוג ביניים. האם R' אוקלידי ביחס לפונקציה $\bar{d}(x) = \min \{d(t) : t \in Rx \cap R\}$?

אוקלידיות של חוגי שלמים

נניח ש- $R = \mathcal{O}_D$ (למשל, עבור שלם D); היזכר גם בתרגיל 3.1.6, עמ' 74). נסמן ב- $|N|$ את הפונקציה $x \mapsto |N(x)|$.

תרגיל 3.3.137 ()** אפשר להרחיב את N לפונקציה כפלית $N : F = \mathbb{Q}(R) \rightarrow \mathbb{Q}$ לפי $N\left(\frac{x}{y}\right) = \frac{N(x)}{N(y)}$. הדרכה. הראה שהפונקציה מוגדרת היטב.

תרגיל 3.3.138 (*) הפונקציה $|N|$ מקיימת תמיד את התנאי (E1).

נסמן $B(a) = \{x \in F : |N(x - a)| < 1\}$, "כדור היחידה" סביב a .

למה 3.3.139 חוג אוקלידי ביחס לפונקציה $|N|$ אם ורק אם כדורי היחידה סביב אברי R מכסים את F , כלומר לכל $x \in F$ קיים $a \in R$ כך ש- $|N(x - a)| < 1$.

תרגיל 3.3.140 (*)** אם $R \subseteq R'$ חוגים עם אותו שדה שברים, כך שקיימת פונקציה כפלית $N : R' \rightarrow \mathbb{Z}$ ו- R אוקלידי ביחס לנוסחה המצומצמת אליו, אז גם R' אוקלידי.

תרגיל 3.3.141 ()** יהי D שלם כלשהו. נסמן עבור $a, b \in \mathbb{Q}$ את ה"אריחים"

$$S_{a+b\sqrt{D}} = \left\{ a' + b'\sqrt{D} \in \mathbb{Q}[\sqrt{D}] : |a' - a| \leq \frac{1}{2}, |b' - b| \leq \frac{1}{2} \right\}$$

ו-

$$S'_{a+b\sqrt{D}} = \left\{ a' + b'\sqrt{D} \in \mathbb{Q}[\sqrt{D}] : |a' - a| \leq \frac{1}{2}, |b' - b| \leq \frac{1}{4} \right\}.$$

1. $\mathbb{Q}[\sqrt{D}]$ מכוסה באריחים S_x שמרכזיהם $x \in \mathbb{Z}[\sqrt{D}]$.

2. כאשר $D \equiv 1 \pmod{4}$, $\mathbb{Q}[\sqrt{D}]$ מכוסה באריחים S'_x שמרכזיהם $x \in \mathcal{O}_D$.

משפט 3.3.142 החוגים $\mathcal{O}_D$ אוקלידיים עבור $D = -1, \pm 2, \pm 3, 5, -7, -11, 13$.

הוכחה. התנאי לכל שהאריח S_x יהיה מוכל בכדור היחידה B_x הוא ש- $D < 0$ ו- $\frac{1+|D|}{4} < 1$ או $D > 0$ ו- $\frac{D}{4} < 1$. לפי למה 3.3.139 ותרגיל 3.3.141.1, החוגים $\mathbb{Z}[\sqrt{D}]$ אוקלידיים עבור $D = -1, -2, -3, 2, 3$, ומקל וחומר (תרגיל 3.3.140) גם $\mathcal{O}_{-3}$ אוקלידי (בשאר המקרים $\mathcal{O}_D = \mathbb{Z}[\sqrt{D}]$).

בדומה לזה, אם $\frac{1}{4} + \frac{|D|}{16} < 1$ ו- $D < 0$, או $0 < \frac{D}{16} < 1$, אז S'_x מוכל בכדור היחידה B_x , וכך מכסה תרגיל 3.3.141.2 את המקרים הנוותרים. (הוכחה זו נכשלת עבור $D = -15$, משום שהאליפסות $|N| < 1$ סביב $0, 1, \frac{1+\sqrt{D}}{2}$ אינן מכסות את הפינה $(\frac{1}{2} + \frac{\sqrt{D}}{4})$. $\square$

כאשר $D < 0$, $\mathcal{O}_D$ אוקלידי בדיוק עבור $D = -1, -2, -3, -7, -11$, ובכל המקרים האלה הנורמה היא פונקציה אוקלידית (ראה המשפט לעיל ותרגיל 3.3.160). המקרה $D > 0$ מסובך יותר. ידוע שהחוגים $\mathcal{O}_D$ אוקלידיים ביחס לנורמה, כאשר $D > 0$, אם ורק אם $D = 2, 3, 5, 6, 7, 11, 13, 17, 19, 21, 29, 33, 37, 41, 57, 73$. עבור $D > 0$ יש חוגים שהם אוקלידיים אבל לא ביחס לנורמה (לדוגמא $\mathbb{Z}[\sqrt{14}]$, והמינון השלם אינו ידוע).

תרגיל 3.3.143 (*)** מצא מנה ושארית בחלוקה של $a = \frac{-153+103\sqrt{-11}}{2}$ ב- b . הדרכה. בשדה השברים $\mathbb{Q}[\sqrt{-11}]$ אפשר לחשב ש- $\mathcal{O}_{-11} = \mathbb{Z}[\frac{1+\sqrt{-11}}{2}]$ בחוג $13 + 5\sqrt{-11}$. $x = \frac{a}{b} = \frac{ab}{bb} = \frac{919}{222} + \frac{263}{111}\sqrt{-11} \approx 4.14 + 2.37\sqrt{-11}$. מבין הנקודות של $\mathbb{Z}[\sqrt{-11}]$, הנקודה הזו קרובה ביותר ל- $4 + 2\sqrt{-11}$, אלא ש- $N(x - (4 + 2\sqrt{-11})) = \frac{225}{148} > 1$, ולכן x אינו נמצא בכדור יחידה סביב נקודה של החוג הזה (זו הוכחה ש- $\mathbb{Z}[\sqrt{-11}]$ אינו אוקלידי). אפשר להתקרב בציר ה- y במחיר התרחקות בציר ה- x , אל הנקודה $\frac{9+5\sqrt{-11}}{2} \in \mathcal{O}_{-11}$, ואכן $N(x - \frac{9+5\sqrt{-11}}{2}) = \frac{47}{148} < 1$. אם כך, מנת החילוק היא $q = \frac{9+5\sqrt{-11}}{2}$ והשארית $r = a - qb = \frac{5-7\sqrt{-11}}{2}$. $N(r) = 141 < 444 = N(b)$ כאשר $a = qb + r$; $r = a - qb = \frac{5-7\sqrt{-11}}{2}$.

תרגיל 3.3.144 (*)** מצא, בחוג $\mathbb{Z}[\sqrt{-1}]$, מספרים a, b כך שאפשר לחלק את a ב- b ולקבל שארית עם $N(r) < N(b)$ בארבע דרכים שונות. הראה שזהו המספר המקסימלי. הראה שבחוג $\mathbb{Z}[\sqrt{-3}]$ אפשר לחלק עם שארית בשתי דרכים שונות לכל היותר. מצא מה המספר המקסימלי של חלוקות עם שארית ב- $\mathcal{O}_{-3}$ (ארבע), ב- $\mathcal{O}_{-7}$ (שלוש) וב- $\mathcal{O}_{-11}$ (שלוש).

הראשוניים של $\mathbb{Z}[\sqrt{-1}]$

החוג $\mathbb{Z}[\sqrt{-1}]$ נקרא **חוג השלמים של גאוס**. בתת-סעיף זה ננצל כמה עובדות ידועות היטב מתורת המספרים כדי למיין את הראשוניים של $\mathbb{Z}[\sqrt{-1}]$.

תרגיל 3.3.145 (*) $\mathbb{Z}[\sqrt{-1}]$ הוא תחום פריקות יחידה.

טענה 3.3.146 (משפט וילסון) לכל ראשוני טבעי p , $(p-1)! \equiv -1 \pmod{p}$.

הוכחה. בחבורת אוילר U_p , אם $a^2 \equiv 1$ אז $(a-1)(a+1) \equiv 0 \pmod{p}$ ולכן $a \equiv \pm 1$. לכן אפשר לפרק את החבורה, למעט האברים 1 ו- -1 , לזוגות שונים a, a^{-1} , ומכאן שמכפלת כל האברים $(p-1)!$ שווה למכפלת הזוגות, שהיא 1 , כפול -1 . $\square$

תרגיל 3.3.147 ()** אם $p \equiv 1 \pmod{4}$ ראשוני, אז קיים $x \in \mathbb{Z}$ כך ש- $x^2 \equiv -1 \pmod{p}$. הדרכה. קח $x = (\frac{p-1}{2})!$ אז $x^2(-1)^{\frac{p-1}{2}} = x^2$ ו- $-1 \equiv (p-1)! = 1 \cdot 2 \cdots \frac{p-1}{2} \cdot \frac{p+1}{2} \cdots (p-1) = x^2(-1)^{\frac{p-1}{2}}$. פתרון נוסף. החבורה U_p ציקלית וסדרה מתחלק ב- 4 , לכן יש בה אבר מסדר 4 , וריבועו הוא האבר היחיד מסדר 2 .

תרגיל 3.3.148 ()** לכל ראשוני $\pi \in \mathbb{Z}[\sqrt{-1}]$, $N(\pi)$ הוא או ראשוני טבעי, או ריבוע של ראשוני כזו. **הדרכה.** אם $n = p_1 \cdots p_t$ אז $\pi \bar{\pi} = n$ מכפלה של ראשוניים, אז יש ראשוני p כך ש- $p | \pi$, וז $p^2 | N(\pi)$ (יתכן שתצטרך להיזכר בתרגיל 3.2.9, עמ' 76).

תרגיל 3.3.149 (*)** ראשוני טבעי p הוא ראשוני ב- $\mathbb{Z}[\sqrt{-1}]$ אם ורק אם $p \equiv -1 \pmod{4}$. **הדרכה.** מצד אחד, אם $p \not\equiv -1 \pmod{4}$ אז קיים x כך ש- $x^2 \equiv -1 \pmod{p}$, ואז $p | (x + \sqrt{-1})(x - \sqrt{-1})$ ואינו מחלק אף אחד מהגורמים, ולכן p אינו יכול להיות ראשוני. מצד שני, אם p אינו ראשוני אז $p = \pi \bar{\pi} = a^2 + b^2$ עבור $a, b \in \mathbb{Z}$ מתאימים, ואז בהכרח $p \not\equiv -1 \pmod{4}$.

תרגיל 3.3.150 ()** לכל ראשוני טבעי $p \equiv 1 \pmod{4}$ יש פתרון יחיד למשוואה $a^2 + b^2 = p$, $a, b \in \mathbb{N}$.

תרגיל 3.3.151 (*)** (הקריטריון של אוילר) מספר טבעי n הוא סכום של שני ריבועים אם ורק אם בפירוק שלו לגורמים ראשוניים, כל גורם השקול ל-3 מודולו 4 מופיע מספר זוגי של פעמים.

תרגיל 3.3.152 ()** התכונות הבאות שקולות עבור ראשוני $p > 2$: p הוא סכום של שני ריבועים; $p \equiv 1 \pmod{4}$; p אינו ראשוני ב- $\mathbb{Z}[\sqrt{-1}]$; יש אבר $x \in \mathbb{Z}[\sqrt{-1}]$ עם $N(x) = p$.

תרגיל 3.3.153 (*)** הוכח שהראשוניים של $\mathbb{Z}[\sqrt{-1}]$ הם, עד כדי חברות:

- $1 + \sqrt{-1}$
- ראשוניים $p \equiv -1 \pmod{4}$ ב- $\mathbb{Z}$
- לכל $p \equiv 1 \pmod{4}$, זוג המספרים $a \pm b\sqrt{-1}$ כאשר $a^2 + b^2 = p$.

תרגיל 3.3.154 ()** נסמן ב- $r_2(x)$ את מספר הדרכים להביע את המספר הטבעי x כסכום של שני ריבועים $x = n^2 + m^2$, כאשר n, m שלמים. מצא את הערך הממוצע של r_2 , כלומר את $\frac{1}{N} \sum_{x=0}^N r_2(x)$ כפונקציה מקורבת של N . ("בעיית המעגל של גאוס" מבקשת קירוב טוב מזה שמצאת).

שימושים נוספים בתורת המספרים

ממשפט 3.3.142 נובע שהחוגים $\mathcal{O}_D$, עבור $D = -1, \pm 2, \pm 3, 5, -7, -11, 13$, הם תחומי פריקות יחידה. לפריקות יחידה יש משמעות רבה בפתרון משוואות דיופנטיות הקשורות לתבנית הנורמה, כפי שנדגים כאן על קצה המזלג.

תרגיל 3.3.155 (*)** הראה שהפתרונות היחידים למשוואה $a^2 + 2b^2 = c^3$ עבור $a, b, c \in \mathbb{Z}$, כאשר a, b זרים, הם מהצורה $a = x^3 - 6xy^2$, $b = 3x^2y - 2y^3$, $c = x^2 + 2y^2$.

הדרכה. נקודת המוצא היא העובדה ש- $R = \mathbb{Z}[\sqrt{-2}]$ תחום פריקות יחידה. נפרק לגורמים ראשוניים ב- R : $c = \prod q_i$, $a + b\sqrt{-2} = \prod p_i$. נראה ש- $a + b\sqrt{-2}$ ו- $a - b\sqrt{-2}$ זרים. אכן, נניח שגורם ראשוני π מחלק את $a + b\sqrt{-2}$ ואת $a - b\sqrt{-2}$, אז הוא מחלק את הסכום וההפרש $2a, 2b\sqrt{-2}$; בעזרת צירוף מתאים $\alpha a + \beta b = 1$, נובע ש- $\pi | 2\sqrt{-2}$. לכן $\pi = \sqrt{-2}$, אבל אז יוצא ש- $\sqrt{-2} | a$ ולכן a זוגי. נכתוב $a = 2a_1$, אז $a^2 + 2b^2 = 2(b^2 + 2a_1^2)$ ולכן גם $c = 2c_1$; אבל אז $8 | 2(b^2 + 2a_1^2)$ ו-8 זוגי, בסתירה להנחה. כעת, אם q_i מחלק אחד מהגורמים $a \pm b\sqrt{-2}$ הוא אינו מחלק את השני, ולכן q_i^3 מחלק את אותו גורם. מכאן שעד כדי סימן $(x + y\sqrt{-2})^3 = (x + b\sqrt{-2})$ עבור x, y שלמים, כפי שהיה להוכיח.

תנאי הכרחי לאוקלידיות

נניח ש- R תחום שלמות. נגדיר $R_0^* = \{0\}$, ולכל $n \geq 0$ נגדיר באינדוקציה

$$R_{n+1}^* = \{a \in R : R = Ra + R_n^*\} \cup R_n^*.$$

אם R תחום אוקלידי עם פונקציה אוקלידית d המקבלת את הערכים $d_0 < d_1 < \dots$, נגדיר $R_n(d) = \{a \in R : d(a) \leq d_n\}$. לפי ההנחה $R_0(d) = R_0^*$, ולפי תרגיל 3.3.127, $R_1(d) = R_1^* = R^\times$.

תרגיל 3.3.156 ()** תהי d פונקציה אוקלידית על תחום שלמות R . הראה ש- $R_n(d) \subseteq R_n^*$ לכל n .

תרגיל 3.3.157 (*)** נגדיר $d^*(a) = \min_n \{d(a) : a \in R_n^*\}$. בדוק ש- $R_n(d^*) = R_n^*$. הראה שאם $\bigcup_n R_n^* = R$, אז d^* פונקציה אוקלידית על R .

תרגיל 3.3.158 (*)** תחום שלמות R הוא אוקלידי אם ורק אם $\bigcup_n R_n^* = R$.

תרגיל 3.3.159 (*)** אם $a \in R_2^*$ אז $|R/Ra| \leq |R^\times|$. הסק: אם לכל $a \in R$ שאינו הפיך מתקיים $|R/Ra| > |R^\times|$, אז $R_2^* = R_1^*$, ולכן R אינו אוקלידי.

תרגיל 3.3.160 (*)** יהי $D < 0$. הראה שלכל $-1, -2, -3, -7, -11$, $\mathcal{O}_D$ אינו אוקלידי. הדרכה: הפעל את תרגיל 3.3.159 על תרגילים 3.2.30 ו-3.1.19.

תרגיל 3.3.161 (*)** הראה שלכל פונקציה אוקלידית על R , $d(a) \geq d^*(a)$. כלומר, d^* היא הפונקציה האוקלידית האיטית ביותר על R . הדרכה: תרגיל 3.3.156.

תרגיל 3.3.162 ()** חשב את הקבוצות R_n^* עבור החוג $R = \mathbb{Z}$. הראה שלכל n , $d^*(n) = \lceil \log_2(|n| + 1) \rceil$ (שהוא מספר הספרות הבינאריות הנחוצות להצגת $|n|$). בדוק ישירות ש- d^* היא פונקציה אוקלידית על $\mathbb{Z}$.

תרגיל 3.3.163 ()** בהמשך לתרגיל 3.3.130 (עמ' 93), הראה שעבור חוג הפולינומים $d^* = \deg, R = F[x]$.

קוואזי-אוקלידיות

הגדרה 3.3.164 יהי R תחום שלמות. פונקציה $d: R \rightarrow \mathbb{N} \cup \{-\infty\}$ המקיימת $d(0) < d(x)$ לכל $x \neq 0$ נקראת פונקציה קוואזי-אוקלידית אם לכל $y \neq 0$ ולכל $x \notin Ry$, קיים $z \in Rx + Ry$ כך ש- $d(z) < d(y)$.

תרגיל 3.3.165 ()** כל פונקציה אוקלידית היא בפרט קוואזי-אוקלידית.

תרגיל 3.3.166 ()** לתחום שלמות יש פונקציה קוואזי-אוקלידית אם ורק אם הוא תחום ראשי.

הדרכה: אם R תחום ראשי, אז הפונקציה ℓ המחזירה לכל אבר את מספר הגורמים הראשוניים בפירוק שלו, היא פונקציה קוואזי-אוקלידית. בכיוון ההפוך, אם יש לתחום שלמות פונקציה קוואזי-אוקלידית, אז הוא ראשי, בדומה לתרגיל 3.3.132 (עמ' 93).

תהי $N: R \rightarrow \mathbb{Z}$ פונקציה כפלית. בתרגיל 3.3.137 (עמ' 94) ראינו שאפשר להרחיב אותה לפונקציה $N: F \rightarrow \mathbb{Q}^\times$, כאשר $F = \mathbb{Q}(R)$.

תרגיל 3.3.167 ()** הפונקציה $|N|: R \rightarrow \mathbb{Z}$ היא קוואזי-אוקלידית אם ורק אם לכל $\alpha \in F$ שאינו ב- R , איחוד הכדורים המנוקבים $\bigcup_{c \in R} \{\beta \in F: 0 < |N(c - \beta)| < 1\}$ חותך את $R\alpha$ בנקודה כלשהי פרט ל-0. כלומר: אם ורק אם לכל $\alpha \in F$ כך ש- $\alpha \notin R$ יש $\beta \in R + R\alpha$ כך ש- $|N(\beta)| < 1$.

תרגיל 3.3.168 (*)** יהי $R = \mathcal{O}_D$ כאשר $D \equiv 1 \pmod{4}$. כדי להראות ש- $|N|: \mathcal{O}_D \rightarrow \mathbb{N}$ היא פונקציה קוואזי-אוקלידית, די להניח בתרגיל 3.3.167 ש- $-\frac{1}{2} < a \leq \frac{1}{2}, 0 < b \leq \frac{1}{4}$ כאשר $a + b\sqrt{D}$.

תרגיל 3.3.169 (*)** הראה ש- $|N|$ היא פונקציה קוואזי-אוקלידית על $\mathcal{O}_{-19}$. לכן $\mathcal{O}_{-19}$ ראשי אבל אינו אוקלידי (תרגיל 3.3.160). הדרכה: נניח ש- $D < 0, D \equiv 1 \pmod{4}$. איחוד כדורי היחידה סביב הנקודות $c \in \mathbb{Z}$ מכסה את הרצועה B_0 של הנקודות $x = a + b\sqrt{D} \in \mathbb{Q}[\sqrt{D}]$ עם $|b| < \sqrt{\frac{3}{4|D|}}$. ואיחוד הכדורים שמרכזם ב- $c + \frac{1+\sqrt{D}}{2}, c \in \mathbb{Z}$, מכסה את הרצועה $B_{1/2}$ המוגדרת לפי $|b - \frac{1}{2}| < \sqrt{\frac{3}{4|D|}}$. (רצועות אלה מכסות את המלבן היסודי אם $|D| < 12$; בכך הוכחנו ש- $\mathcal{O}_{-3}, \mathcal{O}_{-7}, \mathcal{O}_{-11}$ קוואזי-אוקלידיים, כפי שכבר נובע ממשפט 3.3.142). נניח ש- $|D| \leq 27$ (המקרים המעניינים הם $D = -15, -19, -23$). אם $x = a + b\sqrt{D}$ שייך לרצועה שלא כוסתה $\sqrt{\frac{3}{4|D|}} \leq b \leq \frac{1}{2} - \sqrt{\frac{3}{4|D|}}$, אז $2x$ שייך לרצועה $B_{1/2}$; לכן, לכל x כזה, $2x$ שייך לכדור יחידה מנוקב, למעט נקודה בודדת, $x_0 = \frac{1+\sqrt{D}}{4}$. עבור $D = -15, -23$, $x_0 \in \mathcal{O}_D$ חותך באופן טריוויאלי את איחוד הכדורים המנוקבים; לכן $|N|$ אינה קוואזי-אוקלידית, ובאמת $\mathcal{O}_D$ אינו ראשי (תרגיל 3.3.96, עמ' 89). עבור $D = -19$ אפשר להציל את הנקודה הבעייתית: $x_0 = \frac{\sqrt{D}-1}{2} \cdot \frac{D-1}{8}$. שייך לכדור המנוקב סביב $\frac{D+3}{8}$.

הגדרה 3.3.170 יהי R תחום שלמות. פונקציה כפלית $d: R \rightarrow \mathbb{N}$ נקראת נורמת קוין אם לכל $x, y \in R$ שאינם מחלקים זה את זה, יש $z \in Rx + Ry$ כך ש- $d(z) < d(x), d(y)$.

תרגיל 3.3.171 (**)** הוכח ש- R תחום פריקות יחידה אם ורק אם יש לו נורמת קוין. |הדרכה: C.S. Queen, "Factorial domains", Proc Amer Math Soc 124(1), 1996, 11–16.

3.4 הערכות ותחומי הערכה

3.4.1 הערכות ותחומי הערכה

חבורות סדורות

הגדרה 3.4.1 חבורה אבלית עם יחס סדר לינארי, כך שאם $\alpha < \beta$ אז $\alpha + \gamma < \beta + \gamma$, נקראת חבורה סדורה (ליתר דיוק, "חבורה אבלית סדורה לינארית", משום שאפשר לסדר גם חבורות לא אבליות, ואפשר לדון גם בחבורות שהסדר עליהן אינו לינארי).

תרגיל 3.4.2 (*) אם $\alpha > \beta$ אם ורק אם $\alpha - \beta > 0$.

תרגיל 3.4.3 (*) הסכום של אברים חיוביים הוא חיובי.

תרגיל 3.4.4 (*) אם $\alpha \leq \alpha'$ ו- $\beta \leq \beta'$ אז $\alpha + \beta \leq \alpha' + \beta'$.

תרגיל 3.4.5 (*) חבורה סדורה היא חסרת פיתול.

תרגיל 3.4.6 (*) תת-חבורה של חבורה סדורה היא סדורה.

תרגיל 3.4.7 ()** תהייה $\Gamma_1 \times \Gamma_2$ חבורות סדורות. אז $\Gamma_1 \times \Gamma_2$ עם הסדר הלכסיקוגרפי היא חבורה סדורה.

תרגיל 3.4.8 (*)** מצא את כל הדרכים לסדר לינארית את $\mathbb{Z}^2$.

על חבורה סדורה מוגדרת **טופולוגיית הסדר**, שאוסף הקטעים הפתוחים $(\alpha, \beta) = \{\gamma \in \Gamma : \alpha < \gamma < \beta\}$ מהווה בסיס שלה. כלומר, קבוצה $U \subseteq \Gamma$ היא פתוחה אם ורק אם לכל $c \in U$ יש $\alpha, \beta \in \Gamma$ כך ש- $\alpha < c < \beta$ ו- $(\alpha, \beta) \subset U$.

תרגיל 3.4.9 ()** פעולת החיבור והנגדי בחבורה הן רציפות ביחס לטופולוגיית הסדר.

תרגיל 3.4.10 (*)** תן דוגמא לחבורה סדורה שטופולוגיית הסדר שלה דיסקרטית, מלבד $\Gamma = \mathbb{Z}$.

הערכה של שדה

הערכה היא פונקציה משדה לחבורה סדורה. הערכות הן כלי מרכזי בשימושים של תורת החוגים, ובפרט בגאומטריה אלגברית. הערכה משרה על השדה טופולוגיה, ומכניסה לדיון מושגים טופולוגיים מרכזיים כמו קומפקטיות ושלמות.

הגדרה 3.4.11 יהי F שדה, ותהי Γ חבורה אבלית סדורה כלשהי. הומומורפיזם $\nu : F \setminus \{0\} \rightarrow \Gamma$ המקיים את התנאי

$$\nu(x + y) \geq \min\{\nu(x), \nu(y)\}$$

נקראת **הערכה של F** . משלימים את ההגדרה ב- $\nu(0) = \infty$, כך שמתקבלת פונקציה $\nu : F \rightarrow \Gamma \cup \{\infty\}$.

תרגיל 3.4.12 (*) בהגדרה לעיל אפשר להחליף את F בחוג כלשהו; הראה שחוג שיש לו הערכה מוכרח להיות תחום.

תרגיל 3.4.13 (*) יהי F שדה עם הערכה ν . הוכח שלכל $x, y \in F$, אם $\nu(x) \neq \nu(y)$ אז $\nu(x + y) = \min\{\nu(x), \nu(y)\}$.

תרגיל 3.4.14 (*) אם $x + y + z = 0$, אז שניים מבין $\nu(x), \nu(y), \nu(z)$ שווים.

תרגיל 3.4.15 ()** יהי F שדה עם הערכה ν . הראה ש-

$$\mathcal{O}_\nu = \{x \in F : \nu(x) \geq 0\}$$

הוא תת-חוג של F (הנקרא **חוג ההערכה**), וש-

$$I_\nu = \{x \in F : \nu(x) > 0\}$$

הוא אידיאל שלו (הנקרא **אידיאל ההערכה**).

תרגיל 3.4.16 ()** הוכח ש- $\mathcal{O}_\nu$ הפיך אם ורק אם $\nu(u) = 0$. הסק ש- I_ν אידיאל מקסימלי של $\mathcal{O}_\nu$. חוג המנה $\bar{F} = \mathcal{O}_\nu / I_\nu$ נקרא **שדה השאריות** של F .

קבוצה מהצורה $B_\gamma(a) = \{x \in F : \nu(x - a) > \gamma\}$ נקראת **כדור פתוח** ב- F . ככל שהערך γ גדול יותר, הכדור קטן יותר. במילים אחרות, הנקודות a, b "קרובות" יותר ככל שהערך $\nu(a - b)$ גדול יותר.

תרגיל 3.4.17 ()** 1. אם שני כדורים פתוחים נחתכים, אז אחד מהם מוכל בשני.

2. לכל $\gamma \in \Gamma$, הכדורים $B_\gamma(a)$ זרים זה לזה.

תרגיל 3.4.18 ()** אוסף הכדורים הפתוחים $B_\gamma(a)$ מהווה בסיס לטופולוגיה על F , הנקראת **טופולוגיית ההערכה** של F .

תרגיל 3.4.19 ()** טופולוגיית ההערכה היא האוסדורף. הדרכה. לכל $a \neq b$, $B_{\nu(a-b)}(a)$ ולכן $\{a\}$ סגורה.

תרגיל 3.4.20 ()** כל כדור $B_\gamma(a)$ הוא קבוצה פתוחה וסגורה. הדרכה. תרגיל 3.4.17: הכדור $B_\gamma(a)$ שווה למשלים של איחוד הכדורים הזרים לו באותו רדיוס.

תרגיל 3.4.21 ()** הטופולוגיה הנוצרת על-ידי הכדורים הפתוחים $B_\gamma(a)$ שווה לטופולוגיה הנוצרת על-ידי הכדורים הסגורים $\bar{B}_\gamma(a) = \{x \in F : \nu(x - a) \geq \gamma\}$. הדרכה. מספיק להוכיח שהכדורים הפתוחים הם קבוצות פתוחות בטופולוגיה הנוצרת על-ידי הכדורים הסגורים, והכדורים הסגורים הם קבוצות פתוחות בטופולוגיה הנוצרת על-ידי הכדורים הפתוחים. ואכן, $\bar{B}_\gamma(a) = B_\gamma(a) \cup \bigcup_{x: \nu(x-a)=\gamma} B_\gamma(x)$, ומאידך $B_\gamma(a) = \bigcup_{\delta < \gamma} \bar{B}_\delta(a)$.

תרגיל 3.4.22 ()** טופולוגיית ההערכה היא הגדולה ביותר שעבורה פונקציית ההערכה $\nu: F \rightarrow \Gamma$ רציפה, כאשר Γ מצויד בטופולוגיית הסדר.

תחומי הערכה

יהי R תחום שלמות; את שדה השברים שלו נסמן ב- F .

הגדרה 3.4.23 **תחום שלמות** R נקרא **תחום הערכה** אם לכל $x \in F^\times$ מתקיים $x \in R$ או $x^{-1} \in R$.

תרגיל 3.4.24 ()** כל תחום הערכה הוא מקומי.

תרגיל 3.4.25 ()** כל תחום הערכה מקיים את תכונת בזו.

תרגיל 3.4.26 ()** יהי R תחום הערכה. נגדיר על החבורה $F^\times / R^\times$ יחס סדר לפי $\alpha R^\times \leq \beta R^\times$ כאשר $\alpha R \subseteq \beta R$. אז $F^\times / R^\times$ היא חבורה סדורה.

משפט 3.4.27 **התנאים הבאים שקולים עבור תחום שלמות R :**

1. R הוא תחום הערכה.

2. יש שדה עם הערכה לחבורה סדורה כלשהי, ש- R הוא חוג ההערכה שלו.

3. אוסף האידיאלים של R מהווה שרשרת.

4. אוסף האידיאלים הראשיים של R מהווה שרשרת.

הוכחה. (1) $\Leftarrow$ (2): לפי תרגיל 3.4.26 $\Gamma = F^\times/R^\times$ היא חבורה סדורה; $\alpha \mapsto \alpha R^\times$ היא הערכה שחוג ההערכה שלה הוא R . (2) $\Leftarrow$ (3): יהיו $I, I' \triangleleft R$ שאינם מוכלים זה בזה. ניקח $x \in I$ ו- $x' \in I'$ כך ש- $x \notin I'$ ו- $x' \notin I$. אפשר להניח ש- $x^{-1}x' \in R$ ואז $x' \in Rx \subseteq I$ ובסתירה להנחה. (3) $\Leftarrow$ (4): ברור. (4) $\Leftarrow$ (1): יהי $x \in F$; כתוב $x = a/b$ כאשר $a, b \in R$ או ש- $Ra \subseteq Rb$ ואז $a/b \in R$ או ש- $Rb \subseteq Ra$ ואז $b/a \in R$. $\square$

מהם האידיאלים של חוג הערכה? יהי R חוג ההערכה של $\nu: F \rightarrow \Gamma$. אז לכל $0 < \gamma \in \Gamma$, $\{x \in F: \nu(x) > \gamma\}$ הוא אידיאל של R . אלו אידיאלים מיוחדים, המתאימים לאברים של Γ .

כדי לתאר את המצב הכללי, נאמר שקבוצה $A \subseteq \Gamma$ היא **חתך** אם היא אינה ריקה, אינה כל Γ , וסגורה כלפי מעלה. (זוהי הגדרה כללית יותר מן ההגדרה של חתכי דדקינד). נסמן את קבוצת החתכים ב- $\tilde{\Gamma}$. יש שיכון שומר סדר $\Gamma \hookrightarrow \tilde{\Gamma}$ לפי $\gamma \mapsto [\gamma, \infty) = \{x: x \geq \gamma\}$.

תרגיל 3.4.28 (*) חשב את $\mathbb{Z}^2$ כאשר החבורה סדורה בסדר הלקסיקוגרפי.

תרגיל 3.4.29 (**)** תאר את החבורות Γ שעבורן $\tilde{\Gamma} = \Gamma$.

תרגיל 3.4.30 ()** לכל אידיאל $I \triangleleft \Gamma$, $\nu(I) = \{\nu(x): 0 \neq x \in I\}$ הוא חתך.

תרגיל 3.4.31 (*)** ההתאמה $I \mapsto \nu(I)$ בין אידיאלים של R לבין חתכים של $\nu(R) \subseteq \Gamma$ שומרת הכלה, והיא חד-חד-ערכית ועל.

הערכות מדרגה 1

תרגיל 3.4.32 (*)** לחבורה סדורה יש שיכון ל- $\mathbb{R}$ אם ורק אם היא אינה מכילה עותק של $\mathbb{Z}^2$ עם הסדר הלקסיקוגרפי. הדרגה. ארכימדיות. (עם זאת, לכל קבוצה סדורה $\Gamma \hookrightarrow \mathbb{R}$ עם תמונה בדידה, יש שיכון $\mathbb{Z} \times \Gamma \hookrightarrow \mathbb{R}$ כקבוצה סדורה עם תמונה בדידה; ובפרט לכל n יש שיכון של קבוצות סדורות $\mathbb{Z}^n \hookrightarrow \mathbb{R}$. הדרגה. כל קטע פתוח הומיאומורפי ל- $\mathbb{R}$ באופן שומר סדר.)

הערכה מדרגה 1 היא הערכה $\nu: F \rightarrow \mathbb{R}$ (כמובן שתמונת ההערכה עשויה להיות תת-חבורה סדורה כלשהי של $\mathbb{R}$). היתרון של הערכות אלה הוא שבניגוד לסתם הערכה, המשרה על החוג טופולוגיית האוסדורף, הערכה מדרגה 1 מגדירה טופולוגיה מטריית, ומאפשרת להגדיר שדות שלמים, שבהם סדרות קושי מתכנסות.

תרגיל 3.4.33 ()** תהי $\nu: F \rightarrow \mathbb{R}$ הערכה מדרגה 1. הראה שהפונקציה $d(x, y) = e^{-\nu(x-y)}$ (כאשר $e > 1$ קבוע כלשהו) היא מטריקה על F , המשרה את טופולוגיית ההערכה מתרגיל 3.4.18.

הגדרה 3.4.34 השדה F הוא **שלם ביחס להערכה** ν אם כל סדרת קושי (ביחס למטריקה של תרגיל 3.4.33) מתכנסת.

תרגיל 3.4.35 (*)** יהי F שדה עם הערכה מדרגה 1. הראה שהשדה שלם אם ורק אם לכל סדרה $a_n \in F$ עם $\nu(a_n) \rightarrow \infty$, הטור $\sum a_n$ מתכנס.

תרגיל 3.4.36 (*)** הגדר **השלמה** של שדה עם הערכה, והראה שהיא תמיד קיימת, ומהווה שדה שלם ביחס לטופולוגיה המטרית.

תרגיל 3.4.37 ()** כאשר $\Gamma \subseteq \mathbb{R}$ כחבורה סדורה: אם Γ דיסקרטית (בטופולוגיה הרגילה של הממשיים) אז $\tilde{\Gamma} = \Gamma \cong \mathbb{Z}$, ואחרת $\tilde{\Gamma} = \mathbb{R} \cup \Gamma$ (לכל נקודה ב- Γ יש עותק "ממשי" ועותק רפאים).

הערכות בדידות מדרגה 1

הגדרה 3.4.38 הערכה $\nu: F \rightarrow \mathbb{Z}$ נקראת **הערכה בדידה** (מדרגה 1). חוג ההערכה $\mathcal{O}_\nu$ נקרא במקרה זה **תחום הערכה בדידה**.

הערכות בדידות קל יחסית לתאר, והן מהוות כלי חשוב ומועיל בתורת המספרים האלגברית.

הערה 3.4.39 המונח "הערכה בדידה" הוא מטעה במקצת, משום שהוא אינו מתאר את חבורת ההערכה Γ : חבורה סדורה היא בדידה ביחס לטופולוגיית הסדר אם ורק אם היא איזומורפית ל- $\mathbb{Z}^n$ עם הסדר הלכסיקוגרפי.

התכונה היסודית של הערכה בדידה היא שקיים אבר $\pi \in F$, שנקרא **מאחד** (uniformizer), שעבורו $\nu(\pi) = 1$.

תרגיל 3.4.40 (*) כל אבר של F הוא מהצורה $\pi^n u$ עבור $n \in \mathbb{Z}$, $u \in \mathcal{O}_\nu^\times$. כל אבר בחוג ההערכה $\mathcal{O}_\nu$ הוא מהצורה $\pi^n u$ עבור $n \geq 0$, $u \in \mathcal{O}_\nu^\times$.

ראינו במשפט 3.4.27 שכל תחום הערכה הוא מהצורה $\mathcal{O}_\nu$ כאשר $\nu: F \rightarrow \Gamma$ היא הערכה של שדה. כעת נאפיין מתי $\Gamma \cong \mathbb{Z}$.

תרגיל 3.4.41 (*)** תחום הערכה הוא תחום הערכה בדידה, אם ורק אם הוא ראשי. הדרכה. אם $\nu: F \rightarrow \mathbb{Z}$ הערכה בדידה, אז כל אידיאל של $\mathcal{O}_\nu$ נוצר על-ידי חזקה של π .

בכיוון ההפוך, תהי $\nu: F \rightarrow \Gamma$ הערכה כלשהי, ויהי $R = \mathcal{O}_\nu$. נניח ש- R ראשי. נסמן ב- π יוצר של אידיאל ההערכה I_ν . נראה ש- $\Gamma = \mathbb{Z}\nu(\pi)$. יהי $x \in F^\times$. אפשר להניח ש- $\nu(x) > 0$. תחילה נניח ש- $\nu(\pi^n) > \nu(x)$ לכל n . נתבונן באידיאל $J = \langle x, \pi^{-1}x, \pi^{-2}x, \dots \rangle$. לפי ההנחה זהו אידיאל ראשי, כלומר יש $a \in R$ כך ש- $J = Ra$. אפשר להציג $a = \sum r_i \pi^{-i} x$, כאשר $r_i \in R$ והסכום כמובן סופי. מכיוון ש- ν הערכה, $\nu(a) \geq \min \{ \nu(r_i \pi^{-i} x) \} \geq \nu(x)$. אבל אז לא יתכן ש- $\pi^{-(n+1)}x \in Ra$ מכאן שקיים n כך ש- $\nu(\pi^{-n}x) = \min \{ \nu(\pi^{-i}x) \}$ עבור n כלשהו. ונקבל $\nu(x) = \nu(\pi^n)$ ונקבל $\nu(x) \leq \nu(\pi^n)$ ניקח n מינימלי כזה, ונראה כי $\pi^n x^{-1} \in I_\nu$ גורר $\nu(\pi^n x^{-1}) \leq \nu(\pi)$ בסתירה למינמליות.

תרגיל 3.4.42 (+)** תחום הערכה הוא ראשי אם ורק אם הוא נתר. הדרכה. תחום הערכה מקיים את תכונת בזו.

הדרך הקלה לבנות הערכה בדידה היא כך:

הנה שתי דוגמאות סטנדרטיות:

103

הגדרה 3.4.51 החוג $R((x))$ של טורי לורך מעל R כולל את הסכומים האינסופיים הפורמליים $\sum_{i=-n}^{\infty} a_i x^i$ (עבור n כלשהו ו- $a_i \in R$), עם החיבור הטבעי והכפל המכליל את זה של פולינומים. האוסף $R[[x]] \subseteq R((x))$ של טורי חזקות פורמליים, כולל את הסכומים $\sum_{i=0}^{\infty} a_i x^i$.

הביטויים הנראים כסכומים אינסופיים בהגדרת $R((x))$ הם ביטויים פורמליים, ולא סכומים.)

תרגיל 3.4.52 (***) $R[[x]] \subseteq R((x))$ הם אכן חוגים.

תרגיל 3.4.53 (*) חוג הפולינומים $R[x]$ הוא תת-חוג של $R[[x]]$.

תרגיל 3.4.54 (***) $R[[x]][x^{-1}] = R((x))$

לאברים של $R((x))$ אין מעלה מוגדרת, משום שהסכום יכול להמשיך לאינסוף. מאידך הסכומים תמיד מתחילים בנקודה סופית, ולכן אפשר להגדיר פונקציה

$$\nu: R((x)) \rightarrow \mathbb{Z} \cup \{\infty\}$$

לפי $\nu(\sum_{i=-n}^{\infty} a_i x^i) = \min_i \{a_i \neq 0\}$. האבר היחיד עם $\nu(f) = \infty$ הוא $f = 0$. את המקדם הנמוך ביותר ב- f מסמנים ב- $\bar{f}$: $f = \bar{f}x^{\nu(f)} + \dots$.

תרגיל 3.4.55 (*) הפונקציה $\nu: R((x)) \rightarrow \mathbb{Z} \cup \{\infty\}$ היא הערכה, וחוג ההערכה הוא $R[[x]]$.

תרגיל 3.4.56 (***) תהי $g_0, g_1, \dots$ סדרה של אברים בחוג $R[[x]]$. אז הסכום $\sum_{n=0}^{\infty} g_n x^n$ מוגדר היטב כאבר של $R[[x]]$.

תרגיל 3.4.57 (***) כל אבר מהצורה $1 + xf$, עבור $f \in R[[x]]$, הוא הפיך ב- $R[[x]]$. הדרכה. נוסחת הסכום של טור הנדסי: $\frac{1}{1-q} = \sum q^i$; ותרגיל 3.4.56.

משפט 3.4.58 האברים ההפיכים ב- $R[[x]]$ הם אלו שהמקדם החופשי שלהם הפיך.

תרגיל 3.4.59 (***) יהי F שדה. הוכח שכל אידיאל של $F[[x]]$ הוא מהצורה $\langle x^t \rangle$ לאיזשהו $t \geq 0$. הדרכה. משפט 3.4.58.

משפט 3.4.60 חבורת ההפיכים של $R((x))$ היא $R^\times \langle x \rangle (1 + xR[[x]])$. כאשר $\langle x \rangle = \{x^i : i \in \mathbb{Z}\}$ היא החבורה הכפלית הנוצרת על-ידי x .

מסקנה 3.4.61 נייח ש- F שדה, אז גם $F((x))$ שדה.

תרגיל 3.4.62 (***) הממד של $F[[x]]$ מעל F הוא $2^{\aleph_0 + |F|}$.

אפשר להגדיר את החוגים $R((x)) \subseteq R[[x]]$ לכל חוג R .

תרגיל 3.4.63 (***) הפונקציה $\nu: R((x)) \rightarrow \mathbb{Z} \cup \{\infty\}$ מקיימת תמיד את אי-השוויון $\nu(fg) \geq \nu(f) + \nu(g)$. היא מהווה הערכה אם ורק אם R תחום.

תרגיל 3.4.64 (***) יהי R תחום. הראה ש- $\nu: R((x)) \rightarrow \mathbb{Z}$ שהוגדרה מיד לפני תרגיל 3.4.55 (עמ' 104) היא הערכה, המתלכדת עם $\deg$ על תת-חוג $R[x]$. הראה ש- $R((x))$ שלם; זוהי ההשלמה של $R[x]$ ביחס להערכה $-\deg$.

טענה 3.4.65 אם R תחום, אז גם $R((x))$ תחום.

הוכחה. אם $f, g \in R((x))$ אז $\nu(fg) = \nu(f) + \nu(g) < \infty$.

מסקנה 3.4.66 נייח ש- D חוג עם חילוק, אז גם $D((x))$ חוג עם חילוק.

שדה Puiseux

תרגיל 3.4.67 (*)** הגדר את האיחוד $\bigcup F((x^{1/n!}))$ בדומה להגדרת הגבול הישר בתרגיל 1.3.78. (זהו שדה לפי תרגיל 1.3.73, והוא נקרא **שדה Puiseux**). הראה שאם F סגור אלגברית אז גם $\bigcup F((x^{1/n!}))$ סגור אלגברית.

תרגיל 3.4.68 ()** הגדר הערכה $\nu: \bigcup F((x^{1/n!})) \rightarrow \mathbb{Q}$. הראה שחוג ההערכה הוא $\bigcup F[[x^{1/n!}]]$.

טורי לורן בשני משתנים

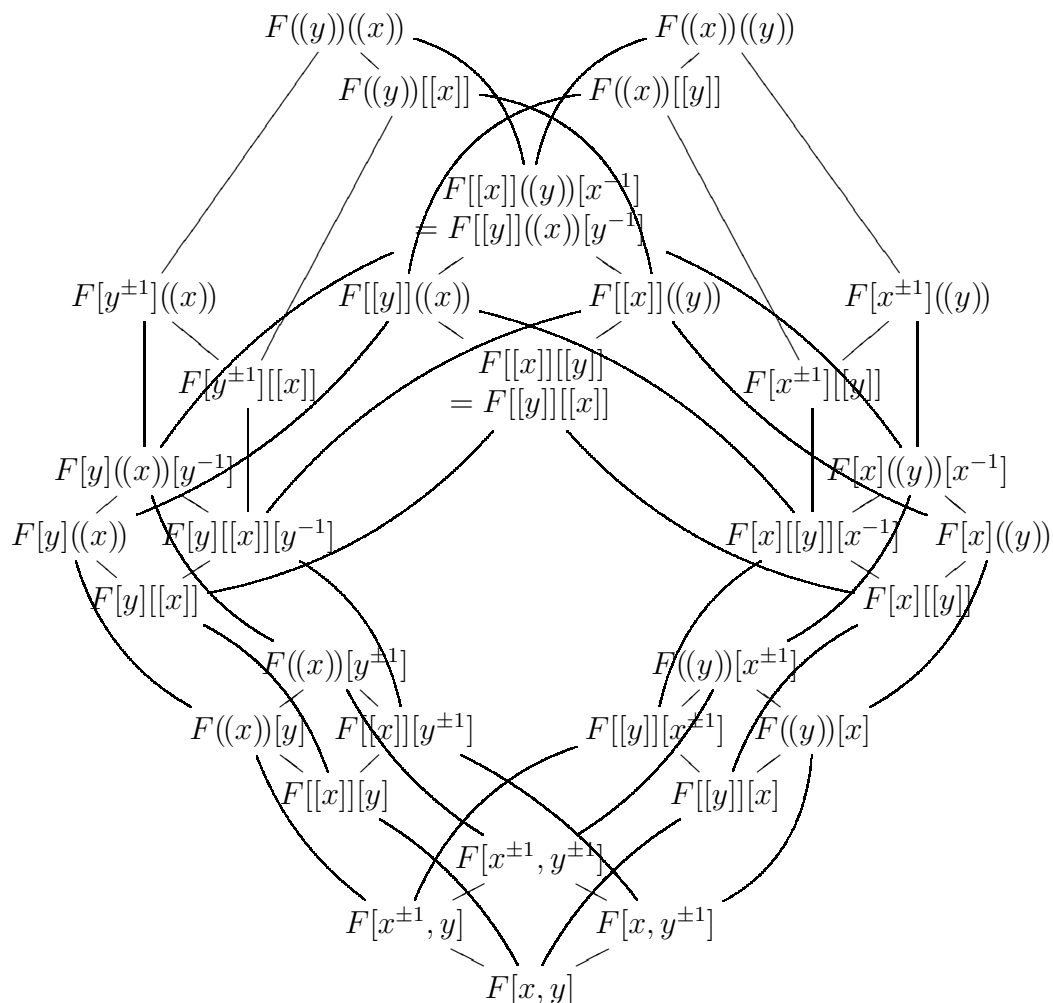
על הבניות של טורי לורן אפשר לחזור עם משתנים חדשים, כפי שהגדרנו את חוג הפולינומים $F[x, y] = F[x][y]$. בעוד שעבור פולינומים מתקיים $F[x][y] = F[y][x]$ (על-ידי זיהוי מתאים של פולינומים בשני החוגים), בניות בטורים פורמליים הן מסובכות יותר.

תרגיל 3.4.69 (*)** הוכח את ההכלות

$$F[[x]][y] \subset F[y][[x]] \subset F[[y]][[x]] \subset F[[y]]((x)) \subset F((x))[[y]] \subset F((x))((y)),$$

והראה שבכל מקרה ההכלה היא אמיתית.

תרגיל 3.4.70 (*)** הוכח שהתרשים הבא מתאר נאמנה את כל החוגים שאפשר לקבל מ- F על-ידי סיפוח המשתנים x, y בארבעה אופנים: סיפוח משתנה לחוג פולינומים, בניה של טורי חזקות פורמליים, וסיפוח ההפכי של משתנה לחוג שבו הוא קיים כאבר (הבניה של טורי לורן מתקבלת לפי תרגיל 3.4.54, עמ' 104). הוכח את כל יחסי ההכלה, ובדוק שאין הכללות נוספות. צבע את התרשים בצבעים עליזים. **הדרכה.** צייר, עבור כל חוג, את ה'חתימות' האפשריות $\{(i, j): a_{ij} \neq 0\} \subseteq \mathbb{Z}^2$ של אברים $f = \sum a_{ij} x^i y^j$ בחוג.



תרגיל 3.4.71 (*)** הראה ש-

$$F[[x]][[y]]^\times = F^\times (1 + xF[[x]])(1 + yF[[y]])(1 + xyF[[x]][[y]]),$$

וזו מכפלה ישירה של חבורות.

תרגיל 3.4.72 (*)** נסמן ב- $E = q(F[[x]][[y]])$ את שדה השברים (ראה תת-סעיף 2.5.3).

1. הראה ש- $F((x))((y)), F((y))((x))$ ו- $F[[x]][[y]][x^{-1}, y^{-1}] \subset E \subset F((x))((y)), F((y))((x))$ הדרכה. $x + y$ אינו הפיך ב- $F[[x]][[y]][x^{-1}, y^{-1}]$.

2. תאר את E .

תרגיל 3.4.73 (*)** הראה ששדה השברים $E = q(F[[x, y]])$ אינו שלם ביחס להערכה ν_y (היינו ההערכה מדרגה 1 של $(F[[x]][[y]])$). הדרכה. תהי $f: \mathbb{N} \rightarrow \mathbb{N}$ פונקציה מונוטונית עולה כך ש- $f(k+1) - f(k) \rightarrow \infty$. נראה ש- $\sum y^{f(n)} x^{-n} \in F[[x]][[y]]$ שכל מחובריו ב- E , אינו שייך ל- E .

נניח שכן. אז יש $a_{ij} \in F$, לא כולם אפס, כך ש- $F[[x]][[y]] \ni \sum_{i,j \geq 0} a_{ij} x^i y^j \sum y^{f(n)} x^{-n} \in F[[x]][[y]]$. נחשב את המכפלה:
 $\sum_{i,j \geq 0} a_{ij} x^i y^j \cdot \sum y^{f(n)} x^{-n} = \sum_{r=-\infty}^{\infty} \sum_{s=0}^{\infty} (\sum_{n: n \geq \max\{0, -r\}, f(n) \leq s} a_{r+n, s-f(n)}) x^r y^s$
אבר של $F[[x]][[y]]$ נדרש לכל $r < 0$ ו- $s \geq 0$, $\sum_{n: n \geq \max\{0, -r\}, f(n) \leq s} a_{r+n, s-f(n)} = 0$. יהי $u \geq 0$. אז יש k כך ש- $f(k+1) - f(k) > u$. נבחר $s = f(k) + u$ ו- $r = -k$. מתקבל $a_{0u} = 0$. אבל אז אפשר לחלק ב- x ולחזור על ההוכחה, עד שכל $a_{ij} = 0$.

טורי חזקות דועכים מעל שדה הערכה

תרגיל 3.4.74 (*)** יהי R חוג עם הערכה לא-ארכימדית ν . לכל מספר ממשי α , הראה ש-

$$A_\alpha = \left\{ \sum_{n=0}^{\infty} a_n x^n : \nu(a_n) \geq \alpha n \right\} \subseteq R[[x]]$$

הוא תת-חוג. הראה ש- A_α תת-חוג מלא של $R[[x]]$: כל אבר של A_α שהוא הפיך ב- $R[[x]]$ הפיך כבר ב- A_α .

הראה שאם $\alpha < \beta$, אז $A_\beta \subset A_\alpha$, כלומר הכלה אמיתית; הסק שבחוג $R[[x]]$ יש שרשרת של א תת-חוגים. הראה ש- $\bigcap_{\alpha} A_\alpha = R$, ו- $\bigcup_{\alpha} A_\alpha$ הוא תת-חוג אמיתי של $R[[x]]$.

השווה את החוגים האלה לחוגים A'_α שבו מחליפים את התנאי $\nu(a_n) \geq \alpha n$ ב-"קיים C כך ש- $\nu(a_n) > \alpha n + C$ ", ולחוגים A^*_α שבהם מחליפים את התנאי ב-" $\liminf \frac{\nu(a_n)}{n} \geq \alpha$ " או ב-" $\inf \frac{\nu(a_n)}{n} \geq \alpha$ ".

שאלות למחשבה נוספת: האם $\bigcap_{\alpha < t} A_\alpha = A_t$? האם $\bigcup_{\alpha > t} A_\alpha = A_t$? יהי $p \in R$ אבר בעל $\nu(p) = 1$. הגדר $A_\alpha(p)$ כהצבת px עבור x בכל אבר של A_α ; השווה את $A_\alpha(p)$ ל- $A_{\alpha+1}$.

הגדרה 3.4.75 יהי F שדה עם הערכה ν . נגדיר

$$F\{\{t\}\} = \left\{ \sum a_i t^i : \inf \nu(a_i) > -\infty, \lim_{j \rightarrow \infty} \nu(a_j) = \infty \right\}.$$

תרגיל 3.4.76 ()** הראה ש- $F\{\{t\}\}$ הוא חוג.

תרגיל 3.4.77 ()** $F\{\{t\}\}$ מכיל ממש את האיחוד $\bigcup_{\alpha > 0} A_\alpha[t^{-1}]$ (כאשר A_α הם החוגים מתרגיל 3.4.74).

תרגיל 3.4.78 ()** הראה ש- $F\{\{t\}\}$ הוא שדה, ושהחבורה הכפלית שלו היא

$$F\{\{t\}\}^\times = F^\times \langle t \rangle (1 + tF[[t]])(1 + I_F[[t^{-1}]])$$

כאשר $I_F = \{a \in F : \nu(a) > 0\}$ הוא אידיאל ההערכה של F (זו מכפלה ישרה).

תרגיל 3.4.79 ()** הראה ש- $\nu(\sum a_i t^i) = \inf \nu(a_i)$ מגדיר הערכה של $F\{\{t\}\}$.

תרגיל 3.4.80 (*)** הראה ששדה השברים של $F\{\{t\}\}$ הוא $\overline{F}((t))$.

תרגיל 3.4.81 (*)** הראה ש- $F((y))((x)) = F((x))\{\{y\}\}$.

טורי חזקות ארוכים

תהי Γ חבורה סדורה היטב, ויהי F שדה.

תרגיל 3.4.82 ()** הראה שאלגברת החבורה $F[\Gamma]$ (מתרגיל 1.3.56, עמ' 40) היא תחום שלמות.

תרגיל 3.4.83 ()** הראה ש- $F[\Gamma] \rightarrow F$ הנוגדרת לפי

$$\nu(\sum \alpha_g g) = \min \{g : \alpha_g \neq 0\}$$

היא הערכה.

תרגיל 3.4.84 ()** נסמן ב- $F^{(\Gamma)}$ את החוג שאבריו הם כל הסכומים הפורמליים $\sum \alpha_g g$ (אולי אינסופיים), עם התכונה שלכל $\gamma \in \Gamma$, הקבוצה $\{g : g < \gamma, \alpha_g \neq 0\}$ סופית, עם פעולת הכפל המושרית מ- $F[\Gamma]$ (מדוע הפעולה מוגדרת?). הראה ש- $F^{(\Gamma)}$ הוא השלמה של $F[\Gamma]$ ביחס ל- ν . הראה ש- $F^{(\Gamma)}$ הוא שדה. הראה שאם Γ חבורה חליקה, אז $F^{(\Gamma)}$ סגור אלגברית.

תרגיל 3.4.85 (*) תאר את החוג $F^{(\Gamma)}$ של תרגיל 3.4.84 עבור $\Gamma = \mathbb{Z}$.

יהי F שדה, ותהי Γ חבורה לינארית (בכתיב כפלי). **טור חזקות ארוך** הוא סכום פורמלי $\sum_{\gamma \in \Gamma^+} a_\gamma \gamma$, שהתומך שלו $\{\gamma : a_\gamma \neq 0\}$ סדור היטב (כאשר $\Gamma^+ = \{\gamma \in \Gamma : \gamma \geq 0\}$). מסמנים ב- $F[[\Gamma]]$ את אוסף כל טורי החזקות הארוכים.

תרגיל 3.4.86 (*)** הוכח ש- $F[[\Gamma]]$ הוא חוג (יש להוכיח שהכפל מוגדר היטב).

תרגיל 3.4.87 (*)** נסמן ב- $F((\Gamma))$ את השדה של טורי לורן הארוכים, המוגדרים באותו אופן כמו טורי חזקות, פרט לכך שמסכמים על Γ במקום Γ^+ . הראה ש- $F((\Gamma))$ הוא שדה השברים של $F[[\Gamma]]$. הראה ש- $F^{(\Gamma)} \subseteq F((\Gamma))$.

תרגיל 3.4.88 ()** מצא הערכה $\nu : F((\Gamma)) \rightarrow \Gamma$.

פרק 4

פולינומים ושדות

4.1 מבוא לתורת השדות

בפרק הקודם הוכחנו שאם F הוא שדה, אז חוג הפולינומים $F[x]$ הוא אוקלידי. בפרט זהו חוג ראשי, ולכן יש בו פריקות יחידה; כל פולינום אי-פריק p הוא גם ראשוני, והאידיאל שיוצר אבר אי-פריק הוא מקסימלי. לכן חוג המנה $F[x]/\langle p \rangle$ הוא שדה.

4.1.1 ממד של אלגברות

נזכיר שאלגברה מעל שדה F היא חוג שהשדה משוכן במרכז שלו. (למעשה לפי תרגיל 2.1.21 (עמ' 47), כל הומומורפיזם של שדה לתוך חוג אחר הוא שיכון.) שדה K המכיל שדה F נקרא **שדה הרחבה** של F .

תרגיל 4.1.1 (*) תהי A אלגברה מעל שדה F . אז A הוא מרחב וקטורי מעל F (ולכן יש לו מימד מעל F , שאנו מסמנים $[A:F]$).

תרגיל 4.1.2 ()** הממד כפלי: אם $F \subseteq K$ ו- V מרחב וקטורי מעל K , אז $\dim_F V = [K:F] \dim_K V$.

תרגיל 4.1.3 (*) תהי A אלגברה מעל F . לכל אידיאל $I \triangleleft A$, אפשר לשכן $F = A/I$ ולכן גם $F/(F \cap I) \cong (F + I)/I \subseteq A/I$.

תרגיל 4.1.4 ()** יהי $f \in F[x]$, ממעלה $n = \deg(f)$. אז הקוסטים של $1, \dots, x^{n-1}$ הם בסיס של חוג המנה $F[x]/\langle f \rangle$. בפרט, הממד של $F[x]/\langle f \rangle$ הוא n .

תרגיל 4.1.5 ()** אם $p(x)$ פולינום אי-פריק מעל F , אז לכל $e \geq 1$, החוג $F[x]/\langle p^e \rangle$ הוא מקומי. זהו שדה אם ורק אם $e = 1$. הדרכה. תרגיל 2.3.5 (עמ' 56).

תרגיל 4.1.6 ()** לכל $f \in F[x]$, $0 \neq f$, הוא סכום ישר של אלגברות מקומיות מממד סופי. הדרכה. נניח ש- $f(x) = p_1(x)^{e_1} \cdots p_t(x)^{e_t}$, כאשר p_i פולינומים אי-פריקים. אז $F[x]/\langle f \rangle \cong F[x]/\langle p_1^{e_1} \rangle \oplus \cdots \oplus F[x]/\langle p_t^{e_t} \rangle$. (עמ' 85).

4.1.2 הפולינום המינימלי

פולינום שהמקדם המוביל שלו הוא 1 נקרא **פולינום מתוקן**. לפי תרגיל 1.3.38 (עמ' 38) כל פולינום הוא, באופן יחיד, מכפלה של סקלר שונה מאפס בפולינום מתוקן. תהי A אלגברה מעל שדה F , עם אבר $a \in A$.

תרגיל 4.1.7 (*) יש הומומורפיזם יחיד $\Phi_a: F[x] \rightarrow A$ שהוא הזהות על אברי F ומעביר $x \mapsto a$. זהו הומומורפיזם ההצבה. (זהו מקרה פרטי של תרגיל 1.2.102, עמ' 33.)

את תמונת הפולינום $f(x) = \sum \alpha_i x^i$ אפשר לסמן $f(a) = \sum \alpha_i a^i$. הומומורפיזם ההצבה הוא חד-חד-ערכי אם לכל $f \neq 0$ גם $f(a) \neq 0$. במקרה זה $F[x] \cong F[a] \subseteq A$, ונקרא a **אבר טרנסצנדנטי**. אחרת a הוא **אבר אלגברי**; הגרעין הוא אידיאל ראשי, והיוצר (שאפשר להניח שהוא מתוקן) נקרא **הפולינום המינימלי של a** .

תרגיל 4.1.8 ()** הפולינום המינימלי של a הוא הפולינום בעל המעלה הקטנה ביותר המאפס את a .

תרגיל 4.1.9 ()** אם $[A:F] < \infty$ אז כל אבר של A הוא אלגברי.

לפי משפט האיזומורפיזם הראשון, $F[x]/\text{Ker}(\Phi_a) \cong \text{Im}(\Phi_a) = F[a] \subseteq A$.

תרגיל 4.1.10 ()** אם A תחום ו- $a \in A$ אז Φ_a ראשוני, ולכן (מדוע?) שדה $F[a]$.

פולינומים אי-פריקים יתפסו בפרק זה מקום מרכזי. לפעמים, הכלי החזק ביותר להוכחת הטענה שפולינום f הוא אי-פריק הוא ההבחנה הבאה:

תרגיל 4.1.11 (*)** יהי $K \supseteq F$ שדה הרחבה של F . נניח ש- $K = F[a]$, וש- $f(a) = 0$, כאשר $\deg(f) = [K:F]$. אז אי-פריק.

4.1.3 שורשים ושדה מפצל

פולינום $f \in F[x]$ נקרא גם **פולינום מעל F** . אם $F \subseteq K$ ו- f פוליןום מעל F , אז K הוא **שדה מפצל** מעל F .

יהי $f \in F[x]$. יהי $c \in F$. לפי האוקלידיות של חוג הפולינומים, אפשר לפרק עם שארית $f(x) = q(x)(x - c) + r(x)$, כאשר $\deg(r) < \deg(x - c) = 1$, כלומר, $\deg(r) \leq 0$, ולכן $r(x) = r \in F$. כעת נציג $c \mapsto x$ ונקבל $f(c) = r$. הוכחנו, אם-כך, ש- $(x - c) \mid f(x) - f(c)$.

תרגיל 4.1.12 (*) $f(c) = 0$ אם ורק אם $(x - c) \mid f(x)$. במקרה כזה c נקרא **שורש של f** . (תרגיל זה נקרא גם "המשפט הקטן של בזו".)

תרגיל 4.1.13 ()** לפולינום ממעלה n מעל שדה יש לכל היותר n שורשים בשדה.

תרגיל 4.1.14 (*)** תת-חבורה סופית של החבורה הכפלית של שדה היא תמיד ציקלית. הדרכה. אם החבורה, מסדר n , אינה ציקלית, אז יש לה אקספוננט $e < n$, וכל אבריה הם שורשים של הפולינום $x^e - 1$.

תרגיל 4.1.15 ()** לכל מספר ראשוני p , חבורת אוילר $U_p = \mathbb{Z}/\mathbb{Z}p^\times$ היא ציקלית. הדרכה. לפי תרגיל 4.1.14 עבור השדה $\mathbb{Z}/\mathbb{Z}p$.

תרגיל 4.1.16 ()** אם f פולינום ממעלה $\deg(f) \leq 3$ ואין לו שורשים, אז הוא אי-פריק ב- $F[x]$.

תרגיל 4.1.17 ()** תן דוגמא לפולינום ממעלה 4 מעל שדה, שהוא פריק שם למרות שאין לו שורשים בשדה.

תרגיל 4.1.18 (*) הראה שהמשפט הקטן של בזו (תרגיל 4.1.12) תקף לפולינומים מעל כל חוג קומוטטיבי. מאידך תן דוגמא לחוג (לא קומוטטיבי) שמעליו יש לפולינום $f(x) = x^2$ אינסוף שורשים.

סיפוח שורשים

מה עושים אם לפולינום אין שורשים בשדה?

משפט 4.1.19 יהי $p \in F[x]$ פולינום אי-פריק. אז קיים שדה הרחבה $K \supseteq F$ שבו יש ל- p שורש.

הוכחה. נבחר $K = F[x]/\langle p \rangle$, שהוא שדה כי p אי-פריק. נסמן $\bar{x} = x + \langle p \rangle$, אז $\square$
 $p(\bar{x}) = \Phi_{\bar{x}}(p) = p(x) + \langle p \rangle = \langle p \rangle = 0_K$

תרגיל 4.1.20 ()** הראה כיצד שדה המספרים המרוכבים $\mathbb{C}$ מתקבל כהרחבה של $\mathbb{R}$ ביחס לפולינום $x^2 + 1$.

השדה F מפצל את $f(x) \in F[x]$ אם אפשר לפרק $f(x) = (x - \alpha_1) \cdots (x - \alpha_n)$ עבור $\alpha_1, \dots, \alpha_n \in F$. כמובן, יתכן ששדה לא יפצל את f , ושדה הרחבה שלו יפצל את הפולינום.

משפט 4.1.21 לכל פולינום $f \in F[x]$ יש שדה מפצל, שממדו מעל F לכל היותר $(\deg f)!$.

הוכחה. באינדוקציה על מעלת הפולינום. אם $\deg f = 1$ אין מה להוכיח. נניח שהטענה נכונה לפולינומים ממעלה $n > 1$ ויהי f פולינום ממעלה n . יהי p גורם אי-פריק של f . לפי משפט 4.1.19 יש הרחבה $K \supseteq F$ ממימד $\deg p$ שבה יש ל- p שורש; לפי תרגיל 4.1.12, מעל K , f מתפרק למכפלה של גורם ליניארי וגורם f_1 ממעלה $n-1$. השדה E המפצל את f_1 מעל K מפצל גם את f , וממדו $[E:F] = [E:K][K:F] \leq (n-1)!(\deg p) \leq n!$. $\square$

4.2 פירוק של פולינומים

מכיוון שפולינומים אי-פריקים הם המפתח לתורת השדות, עלינו לפתח שיטות לזיהוי פולינומים כאלה. אם הפולינום מוגדר מעל שדה, עומדים לרשותנו תרגילים 4.1.16 ו-4.1.11. בסעיף זה נניח שהפולינום מוגדר מעל תחום שלמות, ונפתח שיטות התלויות במבנה של חוג המקדמים.

פירוק לגורמים תלוי, כמו תמיד, בחוג המקדמים, ובהחלט יתכן שפולינום יהיה פריק במקום שבו הוא מוגדר, ואי-פריק מעל שדה השברים: למשל $2(x^2 + 1)$ פריק ב- $\mathbb{Z}[x]$, אבל אי-פריק ב- $\mathbb{Q}[x]$ (משום שהגורם 2 הפיך ב- $\mathbb{Q}$). כדי לבדוד את הבעיה הזו, נקרא לפירוק $f = gh$ **פירוק אמיתי** רק אם $\deg(g), \deg(h) \geq 1$ (למרות שפירוק "לא אמיתי" הוא פירוק לכל דבר ועניין בחוג הפולינומים $(R[\lambda])$).

4.2.1 שורשים רציונליים

תרגיל 4.2.1 ()** יהיו R תחום פריקות יחידה, ו- F שדה השברים שלו. אז כל $\alpha \in F$ אפשר להציג, באופן יחיד, בצורה $\alpha = \frac{a}{b}$ כך שאין ל- a, b גורמים ראשוניים משותפים. צורה זו נקראת **הצורה המצומצמת** של α .

משפט 4.2.2 יהיו R תחום פריקות יחידה. נניח ש- $f(\lambda) = a_n \lambda^n + \dots + a_0 \in R[\lambda]$. אם $\frac{a}{b} \in F = q(R)$ הוא שורש של f (הנתון בצורה מצומצמת), אז $a \mid a_0$ ו- $b \mid a_n$.

תרגיל 4.2.3 (*)** יהי p ראשוני. יהי $f \in \mathbb{Z}[x]$ פולינום שהמקדם המוביל שלו זר ל- p , וכך ש- $f(0), f(1), \dots, f(p-1)$ אינם מתחלקים ב- p . הראה של- f אין שורשים רציונליים.

הגדרה 4.2.4 תחום שלמות הוא נורמלי אם כל שורש של פולינום מתוקן מעל R הנמצא בשדה השברים של R , נמצא ב- R עצמו.

תרגיל 4.2.5 ()** הראה שכל תחום פריקות יחידה הוא נורמלי.

תרגיל 4.2.6 (*)** תחום gcd הוא נורמלי. הדרכה. זוהי גרסה חזקה של תרגיל 4.2.5. נניח ש- $\alpha = \frac{r}{s} \in F = q(R)$ מקיים $\alpha^n + a_{n-1}\alpha^{n-1} + \dots + a_0 = 0$, כאשר $a_0, \dots, a_{n-1} \in R$. מכיון ש- R תחום gcd, אפשר להניח ש- $\gcd(r, s) = 1$. מכיון ש- $r^n = -s(a_{n-1}r^{n-1} + \dots + s^{n-1}a_0)$, מקבלים $s \mid r^n$, אבל מכיון ש- $\gcd(r, s) = 1$ נובע גם $\gcd(r^n, s) = 1$, ולכן $s \sim 1$ ו- $\alpha \sim r \in R$.

תרגיל 4.2.7 (*)** תן דוגמא לתחום שלמות שאינו נורמלי.

4.2.2 קריטריון אייזנשטיין

יהיו R תחום שלמות, ו- $F = q(R)$ שדה השברים שלו.

תרגיל 4.2.8 ()** $f \in R[\lambda]$ אי-פריק מעל F אם ורק אם אין לו פירוק אמיתי מעל R (כפי שהגדרנו לעיל, פירוק אמיתי הוא פירוק שבו שני הגורמים אינם סקלרים).

משפט 4.2.9 (קריטריון אייזנשטיין) נניח ש- $P \triangleleft R$ אידיאל ראשוני. אם כל המקדמים של $f(x) = a_0 + a_1x + \dots + a_nx^n$ פרט למקדם העליון נמצאים ב- P , ובנוסף $a_n \notin P$ ו- $a_0 \notin P^2$, אז אין ל- f פירוק אמיתי מעל R .

הוכחה. נניח ש- $f = gh$ פירוק אמיתי מעל R . נכתוב $g = b_kx^k + \dots + b_0$ ו- $h = c_{n-k}x^{n-k} + \dots + c_0$, כאשר $0 < k < n$. נתבונן בפולינומים אלה מעל תחום השלמות R/P . נניח ש- $b_i, c_j \notin P$ עבור $0 \leq i \leq k, 0 \leq j \leq n-k$. מינימליים. הכפלת הפולינומים מעל R/P מראה ש- $a_{i+j} \equiv b_ic_j \pmod{P}$ (כאשר $a_{i+j} \equiv 0 \pmod{P}$ אם $i+j > n$). אם $i+j = n$, ובמקרה זה $i = k$ ו- $j = n-k$, ובפרט $b_0, c_0 \in P$ ו- $a_0 = b_0c_0 \in P^2$. □

גרסה מעל $\mathbb{Z}$:

תרגיל 4.2.10 ()** יהי p מספר ראשוני. יהי $f(x) = a_0 + a_1x + \dots + a_nx^n \in \mathbb{Z}[x]$ פולינום, כך ש- $a_0, \dots, a_{n-1} \in p\mathbb{Z}$, $a_n \notin p\mathbb{Z}$ ו- $a_0 \notin p^2\mathbb{Z}$. אז אין ל- f פירוק אמיתי מעל $\mathbb{Q}$. בפרט, f אי-פריק מעל $\mathbb{Q}$.

תרגיל 4.2.11 (*)** מצא דוגמא נגדית לקריטריון אייזנשטיין כאשר P הוא האידיאל הנוצר על-ידי אבר אי-פריק של R (שאינו ראשוני).

תרגיל 4.2.12 ()** אם $f \in F[x]$ פריק, אז לכל $a, b \in F, a \neq 0$, גם $f(ax + b)$ פריק.

תרגיל 4.2.13 ()** הראה שהפולינום $\frac{x^p-1}{x-1}$, כאשר p מספר ראשוני, הוא אי-פריק מעל $\mathbb{Q}$.

תרגיל 4.2.14 (*)** הראה ש- $x^6 - x^3 + 1$ אי-פריק מעל $\mathbb{Q}$.

4.2.3 הלמה של גאוס

הקשר בין פריקות של פולינום מעל תחום שלמות R ופריקות מעל שדה השברים שלו הוא חמקמק למדי. פולינום מעל R יכול להיות אי-פריק מעל $F = q(R)$, ופריק מעל R (פירוק שאינו אמיתי, ראה תרגיל 4.2.8). גרוע מזה, פולינום יכול להיות אי-פריק מעל תחום שלמות R , ופריק מעל שדה השברים שלו, משום שבכל פירוק מופיעים מקדמים שאינם ב- R (ראו דוגמא בתרגיל 4.2.37, עמ' 116). הלמה של גאוס מראה שאם R הוא תחום ראשי, אז כל פולינום אי-פריק מעל R הוא גם אי-פריק מעל שדה השברים. בסעיף זה, אם לא יצוין אחרת, נניח ש- R תחום gcd (ההוכחות לפעמים קלות יותר אם מחזקים את ההנחה לכך ש- R תחום פריקות יחידה). בתחומי gcd מוגדרת מכפלה משותפת מקסימלית, ואברים הם זרים אם הם המחלק המשותף המקסימלי שלהם הוא 1. כל תחום פריקות יחידה הוא תחום gcd משום שמכפלת הגורמים המשותפים של a, b , עד כדי חברות, עם חזרות, היא שמכפלה המשותפת המינימלית שלהם.

הערה 4.2.15 כל $\alpha \in F^\times$ אפשר לכתוב בצורה $\alpha = \frac{a}{b}$ עם $a, b \in R$ זרים. אם R תחום פריקות יחידה, הצגה זו היא יחידה עד כדי חברות.

תכולה של פולינום

הגדרה 4.2.16 התכולה של פולינום $f(\lambda) = a_n \lambda^n + \dots + a_1 \lambda + a_0 \in R[\lambda]$ היא המחלק המשותף המקסימלי של המקדמים $a_0, \dots, a_n$. את התכולה נסמן ב- $c(f)$.

כתמיד, התכולה מוגדרת עד-כדי חברות.

הערה 4.2.17 לכל $f \in R[\lambda]$ ו- $a \in R$, $c(af) = a \cdot c(f)$ (לפי תרגיל 3.3.67).

הגדרה 4.2.18 $f \in R[\lambda]$ הוא פרימיטיבי אם מקדמיו זרים, כלומר $c(f) = 1$.

תרגיל 4.2.19 (*) לכל פולינום $f \in R[\lambda]$, $c(f) | f$, בפרט, כל פולינום אי-פריק מעל R הוא פרימיטיבי.

לפי תרגיל 4.2.19 אפשר להגדיר לכל פולינום f , $\hat{f} = \frac{1}{c(f)} f \in R[\lambda]$.

תרגיל 4.2.20 ()** פולינום מהצורה $\hat{f}$ הוא פרימיטיבי.

תרגיל 4.2.21 ()** ההצגה של פולינום $f \in R[\lambda]$ כמכפלה $f = c(f)\hat{f}$ של סקלר ופולינום פרימיטיבי היא יחידה עד כדי כפל באבר הפיך: אם $f = af_1$ כאשר f_1 פרימיטיבי אז $a \sim c(f)$ ו- $\hat{f} \sim \hat{f}_1$.

הפירוק של תרגיל 4.2.21 חל גם מעל F :

תרגיל 4.2.22 ()** לכל $f \in F[\lambda]$, קיימים $c(f) \in F^\times$ ו- $\hat{f} \in R[\lambda]$ פרימיטיבי, יחידים עד כדי כפל באבר הפיך של R , כך ש- $f = c(f)\hat{f}$. הדרכה: לצורך הקיום כתוב $f = \frac{1}{b}f_0$ עם $f_0 \in R[\lambda]$ ואז $f = \frac{c(f_0)}{b}\hat{f}_0$. היחידות נובעת מכך שאם $\frac{c}{b}f_1 = \frac{c}{d}g_1$, כאשר f_1, g_1 פרימיטיביים, אז $\frac{a}{b} \sim \frac{c}{d}$ כך ש- $ad \sim c(adf_1) = c(bcg_1) \sim bc^{-1}adf_1 = bcg_1$.

תרגיל 4.2.23 (*) אם $f \in R[\lambda]$ פרימיטיבי אז כל פירוק שלו הוא אמיתי. בפרט אם f פרימיטיבי ואי-פריק מעל F אז הוא אי-פריק מעל R .

הלמה של גאוס

משפט 4.2.24 (הלמה של גאוס - פרימיטיביות) $c(fg) = c(f)c(g)$. בפרט, המכפלה של פולינומים פרימיטיביים היא פרימיטיבית.

הוכחה. לפי הערה 4.2.17 מספיק להוכיח את הטענה על פרימיטיביות.

1. אם R תחום פריקות יחידה: נניח ש- $c(fg)$ אינו הפיך, אז יש לו גורם ראשוני p , ואז $fg \equiv 0 \pmod{pR[\lambda]}$. אבל $R/\langle p \rangle$ הוא תחום, ולכן אחד הגורמים f או g מוכרח להיות אפס שם, ואז התכולה שלו מתחלקת ב- p .

2. במקרה הכללי (היינו כאשר R תחום-gcd): באינדוקציה על מספר המונומים השונים מאפס ב- f, g . נניח בשלילה ש- $c(fg) \neq 1$. נסמן ב- $a\lambda^n, b\lambda^m$ את המקדמים המובילים של f, g , בהתאמה. לפי ההגדרה, $c(fg) \mid ab$, ולפי תרגיל 3.3.77 (עמ' 88) נובע מכך ש- $(c(fg), a) \neq 1$ או $(c(fg), b) \neq 1$; אפשר להניח ש- $d = (c(fg), a) \neq 1$. מכיוון ש- $c(a\lambda^n g), d \mid c(fg)$, קיבלנו שגם $d \mid c((f - a\lambda^n)g) = c(f - a\lambda^n)c(g)$, ולכן $d \mid c(f)$ בסתירה להנחה.

□

תרגיל 4.2.25 (*)** נניח ש- $f, g \in R[\lambda]$ ו- f פרימיטיבי. אם $f \mid g$ מעל F , אז $f \mid g$ מעל R .

מתרגיל 4.2.21 מתקבלת ההכללה הבאה של משפט 4.2.24:

מסקנה 4.2.26 $\widehat{fg} = \widehat{f}\widehat{g}$ לכל $f, g \in R[\lambda]$.

תרגיל 4.2.27 (*)** בתחום שלמות כללי התכולה (כמחלק משותף מקסימלי של המקדמים) אינה מוגדרת, אבל תמיד אפשר להתבונן באידיאל $C(f)$ הנוצר על-ידי המקדמים. הראה שגם טענה 4.2.17 וגם משפט 4.2.24 אינם נכונים עבור $C(f)$. הדרכה: קח $R = F[x, y]$, עם הפולינומים $f = x\lambda + y$ ו- $g = x\lambda - y$. $C(fg) = \langle x^2, y^2 \rangle \subset \langle x, y \rangle^2 = \mathcal{A}$. $g = x\lambda - y$ ו- $f = x\lambda + y$ אינם נכונים עבור $C(f)C(g)$.

תרגיל 4.2.28 (+)** בהמשך לתרגיל 4.2.27, הוכח את הגרסה הבאה של משפט 4.2.24, הנכונה מעל כל חוג קומוטטיבי R : נאמר ש- $f \in R[\lambda]$ הוא **פולינום קו-מקסימלי** אם $C(f) = R$. אז המכפלה של פולינומים קו-מקסימליים היא קו-מקסימלית. הדרכה. אחרת קח אידיאל מקסימלי המכיל את כל המקדמים של f, g , ועבור לחוג המנה.

למה 4.2.29 יהי $f \in R[\lambda]$. לכל פירוק $f = g_1 \cdots g_n$ עם $g_1, \dots, g_n \in F[\lambda]$, מתקיים $f = c(f)\hat{g}_1 \cdots \hat{g}_n$.

הוכחה. על-ידי כפל במכנה משותף והוצאת התכולה של כל פולינום מחוץ לסוגריים מתקבל $af = b\hat{g}_1 \cdots \hat{g}_n$ עבור $a, b \in R$. לפי הערה 4.2.17, $ac(f) = c(af) = c(b\hat{g}_1 \cdots \hat{g}_n) = b$ ולכן אפשר לצמצם ולקבל $f = c(f)\hat{g}_1 \cdots \hat{g}_n$. $\square$

משפט 4.2.30 (הלמה של גאוס - אי-פריקות) אם פולינום $f \in R[\lambda]$ אי-פריק מעל R , אז הוא אי-פריק גם מעל F .

הוכחה. לפי תרגיל 4.2.19, f פרימיטיבי. אם f היה פריק מעל F , למה 4.2.29 היתה מנפקת פירוק אמיתי מעל R , בסתירה להנחה. $\square$

לסיכום (תרגיל 4.2.23 ומשפט 4.2.30), כאשר R תחום פריקות יחידה,

$$\text{אי-פריק מעל } R = \text{אי-פריק מעל } F + \text{פרימיטיבי.}$$

טענה 4.2.31 יהיו $f, g \in R[\lambda]$. אז $g \mid f$ ב- $R[\lambda]$ אם ורק אם $c(f) \mid c(g)$ ו- $\hat{g} \mid \hat{f}$.

הוכחה. כיוון אחד ברור. בכיוון ההפוך, נניח $f = gh$. אז $\hat{f} = c(f)\hat{g}\hat{h} = c(g)c(h)\hat{g}\hat{h}$, ולפי היחידות בטענה 4.2.22, $c(f) \sim c(g)c(h)$ ו- $\hat{f} \sim \hat{g}\hat{h}$. $\square$

מסקנה 4.2.32 יהיו $f, g \in R[\lambda]$. אם $g \mid f$ מעל F , אז $\hat{g} \mid \hat{f}$ מעל R .

הוכחה. לאחר כפל בסקלר $b \in R$ מתאים, $b \mid gf$ מעל R , ואז $\hat{g} \mid \hat{bf} = \hat{f}$. $\square$

פירוק פולינומים מעל תחום פריקות יחידה

טענה 4.2.33 יהי R תחום פריקות יחידה. אם $f, g \in R[\lambda]$, פרימיטיבי ו- $g \mid f$ מעל F , אז $f = g$ מעל R .

הוכחה. נתונים $f, g \in R[\lambda]$ ו- $h \in F[\lambda]$ כך ש- $g = fh$. כתוב $h = c(h)\hat{h}$, כאשר $c(h) \in F$. אז $g = c(h)f\hat{h}$ מעל R , ולכן $c(h)c(f)c(\hat{h}) = c(g) = 1$, ומכאן $c(h) = 1$, $h = \hat{h} \in R[\lambda]$. $\square$

משפט 4.2.34 אם R הוא תחום פריקות יחידה, אז כך גם $R[\lambda]$.

הוכחה. יהי $f \in R[\lambda] \subseteq F[\lambda]$. יש פירוק $f = g_1 \cdots g_n$ לגורמים אי-פריקים מעל F . לפי למה 4.2.29, $f = c(f)\hat{g}_1 \cdots \hat{g}_n$. כל $\hat{g}_i$ הוא חבר של g_i מעל F ולכן אי-פריק שם, ולפי תרגיל 4.2.23, $\hat{g}_i$ אי-פריק מעל R . קיבלנו אם כך פירוק של f לגורמים אי-פריקים ב- $R[\lambda]$.

נשאר להראות שכל אי-פריק הוא ראשוני. נניח ש- f אי-פריק ב- $R[\lambda]$; אז בוודאי $c(f) = 1$. נניח ש- $gh \mid f$ מעל R ; על-ידי הוצאת מכנה משותף אפשר להניח ש- $c(gh) = 1$. אבל מכיוון ש- f ראשוני ב- $F[\lambda]$, הוא מחלק אחד מבין g או h מעל F , ולפי טענה 4.2.33 הוא מחלק את אותו פולינום מעל R . $\square$

(אף משפט זה נקרא לפעמים 'הלמה של גאוס').

תרגיל 4.2.35 (*)** אם R תחום gcd, אז כך גם $R[\lambda]$.

תרגיל 4.2.36 ()** $\mathbb{Z}[\frac{1+\sqrt{-5}}{2}]$ ו- $\mathbb{Z}[\sqrt{-6}]$ אינם תחומי פריקות יחידה.

תרגיל 4.2.37 (*)** נסמן $\epsilon = \frac{1+\sqrt{-5}}{2}$. הראה שהפולינום

$$3x^2 + 4x + 3 = (3x + (1 + 2\epsilon))(x + \frac{3 - 2\epsilon}{3})$$

פריק מעל השדה $\mathbb{Q}[\epsilon]$, אבל הוא פרימיטיבי ואי-פריק מעל $\mathbb{Z}[\epsilon]$, בסתירה-לכאורה למשפט 4.2.30 (מדוע אין זו סתירה?).

תרגיל 4.2.38 (*)** נסמן $\delta = \sqrt{-6}$. אז $(\frac{\delta}{3}\lambda - 1) = -2\lambda^2 - 3$ כך ש- $2\lambda^2 + 3 \mid \delta\lambda + 3$ מעל $F = \mathbb{Q}[\delta]$ אבל לא מעל $R = \mathbb{Z}[\delta]$, בסתירה-לכאורה לטענה 4.2.33.

תרגיל 4.2.39 ()** אם $\alpha, \beta, \alpha', \beta' \in R$ אברים המקיימים $\alpha\beta' = \alpha'\beta$, אז בחוג $R[x]$ מתקיים $(\alpha x + \beta)(\alpha' x - \beta') = (\alpha x - \beta)(\alpha' x + \beta')$. אם $\alpha, \beta, \alpha', \beta'$ אי-פריקים, זו דוגמא לשני פירוקים אמיתיים של $\alpha\alpha'x^2 - \beta\beta'$, שהגורמים בהם אינם חברים זה לזה. (זה בלתי אפשרי כמובן אם R תחום פריקות יחידה.)

פרק 5

מודולים

נושאו של פרק זה הוא המודול, שהוא מבנה שחוג פועל עליו באמצעות כפל בסקלר. זוהי הכללה של מרחבים וקטוריים, שאינם אלא מודולים מעל שדה. תורת המודולים צועדת יד-ביד עם תורת המבנה של החוגים הכלליים, משום שהדרך הטובה ביותר ללמוד חוג היא דרך הפעולות שלו על מודולים. בפרק זה נסתפק בפיתוח התורה של מודולים מעל תחומי פריקות יחידה, המכלילה שתי תוצאות מרכזיות באלגברה ליניארית ובתורת החבורות: מיון החבורות האבליות הנוצרות סופית, ומיון מטריצות לפי צורת ז'ורדן.

5.1 מבוא

5.1.1 הגדרה ודוגמאות

הגדרה 5.1.1 יהי R חוג כלשהו. מודול מעל R הוא חבורה אבלית עם כפל בסקלר $R \times M \rightarrow M$, המקיים את האקסיומות $(\alpha\beta)x = \alpha(\beta x)$, $\alpha(x+y) = \alpha x + \alpha y$, $(\alpha+\beta)x = \alpha x + \beta x$, $1x = x$.

תרגיל 5.1.2 ()** בכל אחד מן המקרים הבאים הראה שמתקבל מודול מעל החוג המתאים.

1. מרחב וקטורי V מעל שדה F (עם פעולת הכפל בסקלר הנתונה);
2. אוסף הוקטורים R^n מעל R , עם הפעולה $r(r_1, \dots, r_n) = (rr_1, \dots, rr_n)$;
3. חבורה אבלית A מעל החוג $\mathbb{Z}$, עם הפעולה $n \cdot a = a + \dots + a$;
4. אידיאל שמאלי $L \leq_\ell R$ מעל R , עם הכפל המושרה מהחוג;
5. חוג מנה R/I מעל R , עם הכפל המושרה מהחוג;
6. F^n מעל חוג המטריצות $M_n(F)$, עם פעולת המטריצות על וקטורים.

תרגיל 5.1.3 (*)** הזכר בדוגמא 1.3.22, שבה הגדרנו את $\text{End}(M)$ עם פעולת ההרכבה ההפוכה $f \cdot g = g \circ f$. יש התאמה בין האפשרויות לראות את החבורה האבלית M כמודול מעל החוג R , לבין הומומורפיזמים (של חוגים עם יחידה) $R \rightarrow \text{End}(M)$.

תרגיל 5.1.4 (+)** יהי R חוג, ותהי M חבורה חיבורית. נניח שנתונה פעולה בינארית $\psi: R \times M \rightarrow M$, שנסמן $(a, x) \mapsto ax$. נגדיר על החבורה האבלית $R \oplus M$ פעולת כפל לפי $(a + x)(a' + x') = aa' + ax'$. הראה שפעולה זו הופכת את $R \oplus M$ לחוג אם ורק אם ψ הופכת את M למודול מעל R .

לדוגמא הבאה חשיבות מכרעת בחקירת מטריצות (כפי שנראה בסעיף 5.2.4):

תרגיל 5.1.5 ()** התאמה בין מודולים מעל $F[x]$ לבין העתקות לינאריות: הראה שכל מודול מעל חוג הפולינומים $F[x]$ הוא למעשה מרחב וקטורי V מעל F עם העתקה לינארית $V \rightarrow V$ המוגדרת לפי $x \mapsto v \cdot x$. גם להיפך, לכל מרחב וקטורי V ולכל העתקה לינארית $V \rightarrow V$ אפשר להפוך את V למודול מעל $F[x]$ על-ידי הפעולה $f(x) \cdot v = f(T)v$.
בפרט, לכל מטריצה $A \in M_n(F)$, אפשר להפוך את המרחב הוקטורי F^n למודול מעל $F[x]$, אם נגדיר $f(x) \cdot v = f(A)v$.

תרגיל 5.1.6 (-)** בדומה לתרגיל 5.1.5, כל מודול מעל $F[[x]]$ הוא מרחב וקטורי מעל F עם העתקה לינארית $T: V \rightarrow V$ שהיא נילית (T נילית אם לכל v יש n כך ש- $T^n(v) = 0$).
הראה שכל העתקה נילית של מרחב וקטורי מממד סופי היא נילפוטנטית (הגדרה 1.1.41), ותן דוגמא להעתקה נילית של מרחב הסדרות המתאפסות לבסוף, $F^{<\omega}$, שאינה נילפוטנטית.

תרגיל 5.1.7 (-)** חבורה אבלית A היא בעלת פיתול- p אם לכל $a \in A$ יש n כך ש- $p^n a = 0$. הראה שכל חבורה אבלית עם פיתול- p היא מודול מעל $\mathbb{Z}_p$.

תרגיל 5.1.8 ()** 1. יהיו $I \subseteq I', J \subseteq J'$ אידיאלים של חוג R . פעולת הכפל $I'/I \times J'/J \rightarrow I'J'/(IJ' + I'J)$ מוגדרת היטב.

2. לכל $I, J, K \triangleleft R$ פעולת הכפל $I/IK \times J/KJ \rightarrow IJ/IKJ$ מוגדרת היטב.

3. פעולת הכפל $K^a/K^{a+1} \times K^c/K^{c+1} \rightarrow K^{a+c}/K^{a+c+1}$ מוגדרת היטב לכל $K \triangleleft R$ ולכל $a, b, c \geq 1$.

4. לכל $J/KJ, J, K \triangleleft R$ הוא מודול מעל R/K .

תרגיל 5.1.9 (*)** יהי R חוג קומוטטיבי.

1. נניח ש- A, A', I, X, I', X' אידיאלים של R כך ש- $X \subseteq I$ ו- $X' \subseteq I'$. פעולת הכפל הטבעית ב- $S = \begin{pmatrix} R/A & I/X \\ I'/X' & R/A' \end{pmatrix}$ מוגדרת היטב אם ורק אם $IA, IA' \subseteq X$ ו- $I'A, I'A' \subseteq X'$, $IX', XI' \subseteq A, A'$ (עמ' 1.3.30, ראה תרגיל 1.3.30).

2. תנאים אלו מתקיימים אם ורק אם $(X : I), (X' : I') \subseteq A, A'$ (ראה תרגיל 1.2.61, עמ' 27).

3. נניח ש- I, X, I', X' אידיאלים כך ש- $X \subseteq I$ ו- $X' \subseteq I'$. אז קיימים A, A' המקיימים את התנאים אם ורק אם $I^2 X \subseteq X'$ ו- $I^2 X' \subseteq X$.

4. המתכון הכללי לבניית חוג מטריצות מוגדר היטב מהצורה S לעיל: בחר $X \subseteq I$ כלשהם. בחר I' כלשהו. בחר X' כך ש- $I' \cap (X : I^2) = \emptyset$.
בחר A, A' כך ש- $(X' : I') \subseteq (X : I)$, $I'X' \subseteq A, A' \subseteq (X : I)$.

5. פעולת הכפל ב- $\begin{pmatrix} R/A & I \\ I' & R/A' \end{pmatrix}$ מוגדרת היטב אם ורק אם $IA = I'A = 0$.

תרגיל 5.1.10 ()** אם R חוג ו- M מודול מעל R/I , אז M מודול מעל R לפי הפעולה $r \cdot m = (r + I) \cdot m$ (ראה תרגיל 5.1.89 (עמ' 125) לכיוון ההפוך).

תרגיל 5.1.11 ()** יהיו V, W מרחבים וקטוריים מעל שדה F . הראה ש- $\text{Hom}(V, W)$ הוא מודול מעל החוג $\text{End}(V) = \text{Hom}(V, V)$ (לפי הפעולה $(\varphi \cdot T) = T \circ \varphi$).

תרגיל 5.1.12 ()** יהי $\pi : W \rightarrow W'$ איזומורפיזם של מרחבים וקטוריים, ויהי V מרחב וקטורי כלשהו. אז $\bar{\pi} : \text{End}(V, W) \rightarrow \text{End}(V, W')$ המוגדר לפי $\bar{\pi}(T) = \pi \circ T$ הוא איזומורפיזם של מודולים מעל $\text{End}(V)$ (ראה תרגיל 5.1.11).

5.1.2 מושגי יסוד

תת-מודולים

הגדרה 5.1.13 אם M מודול מעל R , אז תת-חבורה חיבורית $N \leq M$ היא תת-מודול אם N סגור לכפל בסקלר; כך N הוא מודול מעל R בזכות עצמו.

תרגיל 5.1.14 (*) לכל מודול M , מודול האפס $\{0\}$ והמודול עצמו הם תת-מודולים של M .

תרגיל 5.1.15 ()** נתבונן ב- R כמודול מעל עצמו. הראה שתת-מודולים הם בדיוק האידיאלים השמאליים של R .

תרגיל 5.1.16 ()** החיתוך של משפחה כלשהי של תת-מודולים (של מודול נתון) הוא תת-מודול.

תרגיל 5.1.17 ()** הגדר, בדומה לנעשה בתת-סעיף 1.1.2, את תת-המודול הנוצר על-ידי קבוצת אברים $T \subseteq M$.

מודול מנה

הגדרה 5.1.18 יהיו $N \leq M$ מודול ותת-מודול. מודול המנה M/N הוא חבורת המנה $M/N = \{x + N : x \in M\}$, עם הכפל בסקלר $r(x + N) = rx + N$.

סכום של תת-מודולים

הגדרה 5.1.19 יהיו M מודול ו- $\{N_\lambda : \lambda \in \Lambda\}$ משפחה של תת-מודולים. הסכום $\sum_{\lambda \in \Lambda} N_\lambda$ הוא הסכום כחבורה (כלומר, אוסף הוקטורים מהצורה $x_1 + \dots + x_n$ עבור $x_i \in N_{\lambda_i}$, כאשר $\lambda_1, \dots, \lambda_n \in \Lambda$ כלשהם), עם הכפל בסקלר של M .

תרגיל 5.1.20 (*) הוכח: סכום של תת-מודולים הוא תת-מודול.

מכפלה ישרה וסכום ישר

הגדרה 5.1.21 הסכום $\sum N_\lambda$ מהגדרה 5.1.19 הוא סכום ישר אם ההצגה של כל אבר כסכום של אברים מן המרכיבים N_λ היא יחידה.

בדוק שההגדרות להלן מכלילות את המושגים המוכרים: תת-מרחב וקטורי, סכום של תת-מרחבים, סכום ישר, תת-חבורה (אבלית), חבורת מנה. כמו בחבורות ובמרחבים וקטוריים, אפשר לבנות ממודולים נתונים מודול חדש. נציג שתי בניות חשובות (השווה להגדרה 1.3.41). תהי M_λ משפחה של מודולים מעל R .

הגדרה 5.1.22 המכפלה הישרה החיצונית היא המכפלה הקרטזית $\prod M_\lambda$, עם פעולות החבור והכפל בסקלר לפי רכיבים.

הגדרה 5.1.23 הסכום הישר החיצוני הוא תת-מודול $\oplus M_\lambda$ של $\prod M_\lambda$ הכולל וקטורים שהם אפס כמעט בכל מקום (היינו בכל הרכיבים פרט למספר סופי).

תרגיל 5.1.24 ()** בדוק שהסכום הישר $\oplus M_\lambda$ הוא אכן תת-מודול של $\prod M_\lambda$.

תרגיל 5.1.25 ()** אם Λ סופית אז $\oplus M_\lambda = \prod M_\lambda$.

תרגיל 5.1.26 ()** נניח ש- $M = A \oplus B$ ו- $N = A \oplus (N \cap B)$ אז $N = A \oplus (N \cap B)$.

תרגיל 5.1.27 ()** בהמשך לתרגיל 5.1.12, הראה שלכל שלושה מרחבים וקטוריים V, W, W' , $\text{Hom}(V, W \oplus W') \cong \text{Hom}(V, W) \oplus \text{Hom}(V, W')$. בתור מודולים מעל $\text{End}(V)$. הדרכה. קבע את ההטלות $\pi: W \oplus W' \rightarrow W'$ ו- $\pi': W \oplus W' \rightarrow W$ והגדר $T \mapsto (\pi \circ T, \pi' \circ T)$.

תרגיל 5.1.28 ()** עקרונית, מודול מעל $R_1 \times R_2$ אינו אלא זוג סדור של מודולים, אחד מעל R_1 ואחד מעל R_2 . להלן פרטי הטענה. יהי R חוג עם אידמפוטנט מרכזי e (לפי תרגיל 2.2.39 (עמ' 53), פירושו של דבר ש- R מתפרק לסכום ישר, $R \cong Re + Re'$ כאשר $e' = 1 - e$). יהי M מודול מעל R . הראה ש- eM תת-מודול של M , שהוא גם מודול מעל Re . הסבר כיצד משרה M זוג סדור של מודולים, אחד מעל Re ואחד מעל Re' . הראה שכל זוג סדור כזה משרה מודול מעל R , ושההתאמות הופכות זו את זו.

הומומורפיזמים

הגדרה 5.1.29 יהיו M, N שני מודולים מעל חוג R . הומומורפיזם של מודולים הוא הומומורפיזם $\varphi: M \rightarrow N$ של חבורות אבליות, המקיים בנוסף $\varphi(rx) = r\varphi(x)$.

כרגיל, הומומורפיזם חד-חד-ערכי ועל הוא איזומורפיזם.

תרגיל 5.1.30 (*) אם $\phi: M \rightarrow N$ הומומורפיזם, אז התמונה $\text{Im}(\phi)$ היא תת-מודול של N , והגרעין $\text{Ker}(\phi)$ הוא תת-מודול של M .

תרגיל 5.1.31 ()** משפט האיזומורפיזם הראשון: אם $\phi: M \rightarrow N$ הומומורפיזם של מודולים, אז $M/\text{Ker}(\phi) \cong \text{Im}(\phi)$.

תרגיל 5.1.32 ()** משפט האיזומורפיזם השני: $(N + K)/K \cong N/(K \cap N)$ לכל $N, K \leq M$.

תרגיל 5.1.33 ()** משפט האיזומורפיזם השלישי: $(M/K)/(N/K) \cong M/N$ לכל $K \leq N \leq M$.

תרגיל 5.1.34 (-)** סריג תת-מודולים הוא **סריג מודולרי**: אם $A \subseteq C$, אז $(A + B) \cap C = A + (B \cap C)$.

תרגיל 5.1.35 (-)** יהיו $A, B \leq M$ תת-מודולים, $\varphi: M \rightarrow N$ הומומורפיזם, $K = \text{Ker}(\varphi)$. הוכח $\varphi(A \cap B) = \varphi(A) \cap \varphi(B)$ אם ורק אם $A \cap (B + K) \subseteq (A \cap B) + K$.

תרגיל 5.1.36 ()** אם $\phi: M \rightarrow N$ הומומורפיזם חד-חד-ערכי ו- $K \leq M$, אז $M/K \cong \phi(M)/\phi(K)$.

תרגיל 5.1.37 (+)** אם M מודול מעל חוג R ו- $I \triangleleft R$ אידיאל, אז M/IM מודול מעל R/I , לפי הפעולה $(r + I) \cdot (x + IM) = rx + IM$.

תרגיל 5.1.38 ()** יהי R תחום, ויהיו $a, b \in R$. ההתאמה $R/Rb \rightarrow Ra/Rab$ לפי $x + Rb \mapsto xa + Rab$ היא איזומורפיזם של מודולים מעל R/Rb (ראה תרגיל 3.1.16, עמ' 74).

5.1.3 אלגברה לינארית של מודולים

יהי M מודול מעל חוג R .

הגדרה 5.1.39 תתיקבוצה $T \subseteq M$ היא **פורשת** אם כל אבר $x \in M$ אפשר להציג כסכום $r_1x_1 + \dots + r_nx_n$ עבור $r_1, \dots, r_n \in R$ ו- $x_1, \dots, x_n \in T$.

המודול נוצר סופית אם יש לו קבוצה פורשת סופית.

תרגיל 5.1.40 ()** יהי R תחום שלמות ויהי $b \in R$ אבר לא הפיך. הראה ש- $R[\frac{1}{b}]$ אינו נוצר סופית כמודול מעל R .

הגדרה 5.1.41 קבוצה $T \subseteq M$ היא **בלתי תלויה** אם מהשוויון $r_1x_1 + \dots + r_nx_n = 0$ עבור $x_1, \dots, x_n \in T$ ו- $r_1, \dots, r_n \in R$ נובע $r_1 = \dots = r_n = 0$.

מודולים חופשיים

קבוצה פורשת ובלתי תלויה נקראת **בסיס**. בניגוד למצב במרחבים וקטוריים, לא לכל מודול יש בסיס:

תרגיל 5.1.42 ()** לחבורה $\mathbb{Z}_n$, כמודול מעל $\mathbb{Z}$, אין בסיס.

תרגיל 5.1.43 (+)** יהי M מודול כלשהו, ויהי F מודול בעל בסיס B . הראה שלכל פונקציה $f: B \rightarrow M$ יש הרחבה יחידה להומומורפיזם $\hat{f}: F \rightarrow M$ (השווה לתרגיל 1.2.108, עמ' 33).

מודול שיש לו בסיס נקרא **מודול חופשי**. מספר האברים בבסיס נקרא **דרגה** של המודול (יתכן שלאותו מודול תהיה יותר מדרגה אחת, אבל ראו להלן).

טענה 5.1.44 כל מודול בעל בסיס בגודל n מעל R איזומורפי ל- R^n .

תרגיל 5.1.45 (*)** למודול חופשי הנוצר סופית, יש בסיס סופי. הדרכה: אִפְרִיז, יתכן שהמודול נוצר סופית, אבל שכל בסיס שלו הוא אינסופי. כתוב את האברים של קבוצה פורשת כצירופים ליניאריים של אברי בסיס כלשהו.

תרגיל 5.1.46 ()** כל מודול נוצר סופית הוא מנה של R^n לאיזשהו n .

תרגיל 5.1.47 ()** $\text{End}(R^n) \cong M_n(R)$

תרגיל 5.1.48 (*)** יהי R תחום שלמות שבו יש אברים לא הפיכים a, b שהם קו־מקסימליים (כלומר $Ra + Rb = R$). אז המודול $M = R^\infty$ של סדרות אינסופיות, אינו חופשי. הדרכה: נתבונן בתת-המודול $M_0 = \sum Re_i$ של סדרות המתאפסות לבסוף, ובמנה $N = M/M_0$. לכל i , $Ra^i + Rb^i = R$ ולכן $\{a^i e_i, b^i e_i\}$ פורשים את M_0 . נוכיח ש- $\text{Hom}(N, R) = 0$. יהי $\psi: N \rightarrow R$ הומומורפיזם. יהי $x = (\alpha_i a^i) \in M$ אבר כלשהו; לכל n , שקול מודולו M_0 ל- $(0, \dots, 0, \alpha_n, \alpha_{n+1}a, \dots)$ ולכן $\psi(x) \in a^n R$; מכאן ש- $\psi(x) \in \bigcap_{n \geq 1} a^n R = 0$. מאותה סיבה גם $\psi(y) = 0$ לכל $y = (\beta_i b^i)$, ולכן $\psi = 0$. אבל אם M היה חופשי, אפשר היה לקבל הומומורפיזם לא טריוויאלי מהטלה על אבר בסיס מחוץ ל- M_0 .

אינווריאנטיות הדרגה

הגדרה 5.1.49 חוג R הוא **סופי חלש** (weakly finite) אם כל קבוצת יוצרים בת n אברים של R^n היא בלתי תלויה. החוג הוא בעל מספר בסיס אינווריאנטי (invariant basis number) אם הדרגה של מודול חופשי נוצר סופית מעליו, מוגדרת היטב.

תרגיל 5.1.50 (+)** R סופי חלש אם לכל $A, B \in M_n(R)$, אם $AB = I$ אז $BA = I$. הערה: חוג סופי במובן ה-חלש אם התכונה הזו מתקיימת עבור n מסויים. חוגים סופיים 1-חלש נקראים כך בשל הפירוש בשפת הפונקציות, הקובע ש(עבור פונקציות המוגדרות על-ידי כפל משמאל בקבוע), פונקציה חד-חד-ערכית מהחוג אל עצמו היא על. זוהי ההגדרה של דדקינד לקבוצות סופיות.

תרגיל 5.1.51 (+)** R הוא בעל מספר בסיס אינווריאנטי אם מקיומן של מטריצות $A \in M_{n \times m}(R)$ ו- $B \in M_{m \times n}(R)$ כך ש- $AB = I_n$ ו- $BA = I_m$ נובע $n = m$.

תרגיל 5.1.52 ()** כל חוג סופי חלש הוא בעל מספר בסיס אינווריאנטי.

תרגיל 5.1.53 ()** אם $M \cong R^n$, אז $M/IM \cong (R/I)^n$ כמודול מעל R/I . הדרכה: תרגיל 5.1.37 ומשפט האיזומורפיזם הראשון.

משפט 5.1.54 כל חוג קומוטטיבי הוא בעל מספר בסיס אינווריאנטי.

הוכחה: קח $P \triangleleft R$ מקסימלי, אז M/PM הוא מרחב וקטורי מעל השדה R/P , ואם $M \cong R^n$ אז $M/PM \cong R^n/PR^n = (R/P)^n$ בעל מימד מוגדר היטב. $\square$

תרגיל 5.1.55 ()** השתמש בקריטריון של תרגיל 5.1.51 והמעבר לחוג מנה כדי להראות שכל חוג קומוטטיבי הוא סופי חלש.

לכן הדרגה של מודול חופשי מעל חוג קומוטטיבי מוגדרת היטב, כמו המימד של מרחבים וקטוריים. יש משפחות נוספות של חוגים שמעליהם הדרגה מוגדרת היטב (למשל, חוגים עם חילוק), ועם זאת, זו אינה תכונה אוניברסלית:

תרגיל 5.1.56 (*)** יהי F שדה, ו- $V = F^{\mathbb{N}_0}$ מרחב הסדרות האינסופיות. הראה ש- $V \cong V \oplus V$. נסמן $R = \text{End}(V)$. הסק מתרגיל 5.1.27 ש- $R \cong R \oplus R$ (כמודולים מעל R). הסק ש- R הוא מודול חופשי מכל דרגה סופית מעל עצמו.

תרגיל 5.1.57 (*)** (גישה מפורשת לתרגיל 5.1.56)

1. יהי V מרחב וקטורי. הגדר העתקות $\pi_i: V \oplus V \rightarrow V$ לפי $\pi_i(x_1, x_2) = x_i$, ו- $\mu_i: V \rightarrow V \oplus V$ לפי $\mu_1(x) = (x, 0)$, $\mu_2(x) = (0, x)$. הראה ש- $\pi_i \mu_j = \delta_{ij}$.
 $\mu_1 \pi_1 + \mu_2 \pi_2 = 1$

2. נניח שהומומורפיזמים $\phi_i, \psi_i: V \rightarrow V$ מקיימים $\phi_i \psi_j = \delta_{ij}$, $\psi_1 \phi_1 + \psi_2 \phi_2 = 1$. אז $\mu_1 \phi_1 + \mu_2 \phi_2: V \rightarrow V \oplus V$ ו- $\psi_1 \pi_1 + \psi_2 \pi_2: V \oplus V \rightarrow V$ הם איזומורפיזמים הפוכים זה לזה. מצא ϕ_i, ψ_i כנ"ל עבור המרחב V של תרגיל 5.1.56. (לחילופין, נניח ש- $\alpha: V \rightarrow V \oplus V$ הוא איזומורפיזם; הראה ש- $\psi_j = \alpha^{-1} \mu_j$ ו- $\phi_i = \pi_i \alpha$.)

3. נסמן $R = \text{End}_F(V)$. כתוב איזומורפיזם מפורש $R \rightarrow R \oplus R$ בתור מודולים מעל R . הדרכה. העזר בתרגילים 5.1.12 ו-5.1.27 כדי לקבל את האיזומורפיזם $T \mapsto (\phi_1 \circ T, \phi_2 \circ T)$.

4. כתוב איזומורפיזם מפורש של חוגים $R \cong M_2(R)$.

מודולים ציקליים

יהי M מודול מעל חוג R .

תרגיל 5.1.58 (*) הראה שלכל $x \in M$, $Rx = \{rx: r \in R\}$ הוא תת-מודול של M .

אם יש ב- M אבר x כך ש- $M = Rx$, אז M נקרא **מודול ציקלי**.

תרגיל 5.1.59 ()** הראה ש- R^n הוא מודול ציקלי מעל $M_n(R)$. מצא אידיאל שמאלי של $M_n(R)$ כך ש- $R^n \cong M_n(R)/L$.

הגדרה 5.1.60 יהי $x \in M$ אבר כמודול. **המאפס של x הוא קבוצת האברים** $\text{ann}_R(x) = \{r \in R: rx = 0\}$.

תרגיל 5.1.61 (*) הסבר את הקשר בין המאפס הזה לבין זה המופיע בהגדרה 1.2.55. (עמ' 27).

תרגיל 5.1.62 ()** $\text{ann}_R(x) \leq_\ell R$ (ובאופן כללי $\text{ann}_R(x)$ אינו אידיאל של R).

תרגיל 5.1.63 ()** יש איזומורפיזם של מודולים $R/\text{ann}_R(x) \cong Rx$.

תרגיל 5.1.64 ()** כל מודול ציקלי איזומורפי למנה R/L עבור אידיאל שמאלי L .

תרגיל 5.1.65 (*)** נניח ש- R חוג קומוטטיבי, ו- $L, L' \leq R$ אידיאלים (שמאליים). אם $R/L \cong R/L'$ כמודולים, אז $L' = L$. הדרכה. ראה הגדרה 5.1.79 ותרגילים 5.1.82 ו-5.1.81; $L' = \text{Ann}(R/L') = \text{Ann}(R/L) = L$.

תרגיל 5.1.66 (*)** הראה שתרגיל 5.1.65 אינו נכון לחוגים לא קומוטטיביים. הדרכה. תרגיל 5.1.68; או בחר $R = M_2(\mathbb{Q})$, $L = Re_{11}$, $L' = Re_{22}$.

תרגיל 5.1.67 (*)** הראה ש- $R/L \cong R/L'$ אם ורק אם יש $u, w \in R$ כך ש- $uw \in 1 + L$, $wu \in 1 + L'$, $L'u \subseteq L$, $Lu \subseteq L'$.

תרגיל 5.1.68 ()** לכל אידיאל שמאלי $L \leq R$ ואבר הפיך $u \in R$, $R/L \cong R/Lu$.

תרגיל 5.1.69 (*)** נניח ש- $R/L \cong R/L'$ כאשר L, L' מקסימליים. האם קיים $u \in R$ הפיך כך ש- $L' = Lu$?

מודול שאין לו תת-מודולים לא טריוויאליים נקרא **מודול פשוט**.

תרגיל 5.1.70 ()** כל מודול פשוט הוא ציקלי. (השווה לתרגיל 2.1.13, עמ' 47).

תרגיל 5.1.71 (*)** מודול R/L הוא פשוט אם ורק אם L אידיאל שמאלי מקסימלי.

5.1.4 פיתול

יהי M מודול מעל תחום שלמות R . אבר $x \in M$, $x \neq 0$ הוא **מפותל** אם קיים $r \in R$, $r \neq 0$ כך ש- $rx = 0$. המודול עצמו הוא **מודול מפותל** אם כל האברים בו מפותלים, ו**חסר פיתול** אם אין בו אברים מפותלים. (אם R אינו תחום שלמות, אבר x נקרא מפותל רק אם קיים r שאינו מחלק אפס כך ש- $rx = 0$).

תרגיל 5.1.72 (*) תן דוגמא למודול שאינו מפותל ואינו חסר פיתול.

תרגיל 5.1.73 (*) האברים של קבוצה בלתי תלויה הם חסרי פיתול.

תרגיל 5.1.74 (*) כל מודול חופשי (מעל תחום שלמות) הוא חסר פיתול.

תרגיל 5.1.75 ()** הראה שאם R תחום שלמות, אוסף האברים המפותלים ב- M הוא תת-מודול; זהו **תת-מודול הפיתול** של M , שנסמן ב- $t(M)$.

תרגיל 5.1.76 (*)** הראה ש- $M/t(M)$ חסר פיתול.

תרגיל 5.1.77 (*)** מעל תחום שלמות R , כל מודול חסר פיתול ונוצר סופית איזומורפי לתת-מודול של מודול חופשי נוצר סופית. הדרכה. תהי S קבוצת יוצרים סופית של R . תהי $S_0 \subseteq S$ תת-קבוצה מקסימלית היוצרת תת-מודול חופשי, שאותו נסמן ב- F . לכל $x \in S - S_0$, $F + Rx$ אינו חופשי ולכן יש $r_x \in R$ כך ש- $r_x x \in F$. נסמן ב- r את מכפלת הסקלרים r_x . נתבונן בהומומורפיזם $M \rightarrow M$ המוגדר לפי כפל ב- r . הוא חד-חד-ערכי כי M חסר פיתול, ולכן M איזומורפי לתמונה שהיא תת-מודול של F , שהוא מודול חופשי ונוצר סופית.

תרגיל 5.1.78 (*)** לכל מודול נוצר סופית יש תת-מודול חופשי F כך ש- M/F מפותל. הדרכה. קח קבוצת יוצרים מקסימלית של תת-מודול חופשי, כבתרגיל 5.1.77.

מודול נאמן

הגדרה 5.1.79 המאפס של מודול M מעל חוג R הוא $\text{Ann}(M) = \{r \in R : rM = 0\}$.

תרגיל 5.1.80 (*) הראה ש- $\text{Ann}(M) \triangleleft R$ (השווה לתרגיל 5.1.62).

תרגיל 5.1.81 (**) אם $M \cong M'$ אז $\text{Ann}(M) = \text{Ann}(M')$. יהי $\varphi: M \rightarrow M'$ איזומורפיזם. אם $rM = 0$ אז $r\varphi(M) = \varphi(rM) = \varphi(0) = 0$ וגם בכיוון ההפוך.

תרגיל 5.1.82 (**) $\text{Ann}(R/L)$ הוא האידיאל הדו-צדדי הגדול ביותר המוכל ב- L .

תרגיל 5.1.83 (**) $\text{Ann}(R/L)$ נאמן אם ורק אם L אינו מכיל אידיאל דו-צדדי שונה מאפס.

מודול נאמן הוא מודול שהמאפס שלו הוא אפס.

תרגיל 5.1.84 (**) כל מודול חסר פיתול הוא נאמן.

תרגיל 5.1.85 (*) המודול M נאמן אם ורק אם לא קיים $r \in R$ כך ש- $rM = 0$.

תרגיל 5.1.86 (***) המודול M נאמן אם ורק אם ההומומורפיזם $R \rightarrow \text{End}(M)$ שבתרגיל 5.1.3 (עמ' 117) הוא חד-חד-ערכי.

תרגיל 5.1.87 (**) מודול מפותל ונוצר סופית מעל תחום שלמות אינו יכול להיות נאמן.

תרגיל 5.1.88 (***) תן דוגמא למודול נאמן ומפותל מעל $\mathbb{Z}$ (השווה לתרגיל 5.1.87).

תרגיל 5.1.89 (**) הראה שכל מודול M מעל R הוא גם מודול מעל $R/\text{Ann}_R(M)$ (זהו הכיוון ההפוך לתרגיל 5.1.10, עמ' 119).

תרגיל 5.1.90 (**) הראה שאם V הוא מודול מעל $F[[x]]$ ו- $\dim_F(V)$ סופי, אז V למעשה מודול מעל $F[x]/\langle x \rangle^n \cong F[x]/\langle x \rangle^n$ עבור n מתאים.

הגדרה 5.1.91 יהי $c \in R$ סקלר השייך למרכז של החוג. המאפס של c הוא תת-מודול $\text{Ann}_M(c) = \{x \in M : cx = 0\}$.

תרגיל 5.1.92 (***) (הלמה של פטינג, גרסה מוחלשת) יהי M מודול מעל חוג C , עם $z \in Z(C)$, ויהי $k \geq 0$. אם $\text{Ann}_M(z^{k+1}) \subseteq \text{Ann}_M(z^k)$, אז $z^k M \cap \text{Ann}_M(z) = 0$.

5.2 מודולים מעל תחום ראשי

בפרק זה נתאר את המבנה של מודולים נוצרים סופית מעל תחום ראשי.

5.2.1 מודולים נוצרים סופית

לאור תרגיל 5.1.46 (עמ' 122), כדי לתאר מודולים נוצרים סופית עלינו להכיר את תת-המודולים של R^n . לכל מודול M , נסמן ב- $\text{rank}(M)$ את המספר הקטן ביותר של אברים בקבוצה הפורשת את M .

משפט 5.2.1 יהי R חוג ראשי. אם $N \leq M$ אז $\text{rank} N \leq \text{rank} M$.

הוכחה. תהי $\{x_1, \dots, x_n\}$ קבוצת יוצרים של M . עלינו להוכיח שגם את N אפשר לפרוש על-ידי n אברים לכל היותר. לכל $1 \leq k \leq n$ קח $M_k = Rx_1 + \dots + Rx_k$ ו- $N_k = N \cap M_k$. נסמן גם $M_0 = N_0 = 0$. לכל $k = 1, \dots, n$, התבונן ב-

$$I_k = \langle c \in R : cx_k \in N + M_{k-1} \rangle.$$

קח יוצר $c_k \in I_k$, ואבר $v_k \in (c_k x_k + M_{k-1}) \cap N \subseteq N_k$ (אם $I_k = 0$ אז $c_k = 0$ ונבחר $v_k = 0$). נראה ש- $N_k \subseteq Rv_k + M_{k-1}$. אכן, כל וקטור ב- N_k שייך לאיזשהו קוסט $rx_k + M_{k-1} \subseteq Rc_k x_k + M_{k-1} = Rv_k + M_{k-1}$ אבל אז $r \in I_k$ וממילא $rx_k + M_{k-1} \subseteq N_k$. מכאן ש- $N_k = Rv_k + M_{k-1}$. וכך הוכחנו ש- $N_k = Rv_1 + \dots + Rv_k$. בסופו של דבר, עבור $k = n$, $v_1, \dots, v_n$ פורשת את N . $\square$

(הטענה נכונה גם לדרגות אינסופיות, אבל לא נוכיח זאת כאן.)

תרגיל 5.2.2 (*)** יהי R תחום ראשי. הראה שתת-מודול של מודול חופשי הוא חופשי. הדרכה. התאם את ההוכחה של משפט 5.2.1: הקבוצה $v_1, \dots, v_n$, לאחר השמטת האפסים, היא בסיס.

תרגיל 5.2.3 ()** משפט 5.2.1 מאפיין תחומים ראשיים: אם R קומוטטיבי וכל תת-מודול של מודול חופשי מדרגה n הוא חופשי מדרגה n , אז R ראשי. הדרכה. תרגיל 5.1.15 (עמ' 119); למעשה די להניח את התכונה הזו ל- $n = 1$.

תרגיל 5.2.4 (*)** אם R חוג נתרן, אז כל תת-מודול של R^n נוצר סופית.

תרגיל 5.2.5 ()** הראה שהדרגה של אידיאלים של $\mathbb{Z}[x]$ (סופית אבל) אינה חסומה. הדרכה. התבונן ב- $I = \langle 2^n, 2^{n-1}x, \dots, 2x^{n-1}, x^n \rangle$.

תרגיל 5.2.6 (*)** יהי R תחום ראשי. כל מודול נוצר סופית חסר פיתול מעל R הוא חופשי. הדרכה. תרגיל 5.1.77 (עמ' 124) ומשפט 5.2.2.

תרגיל 5.2.7 ()** יהי M מודול מעל חוג R . נסמן ב- $M[x]$ את האוסף של פולינומים ב- x שמקדמיהם מ- M ; זהו מודול מעל $R[x]$ עם הפעולה הטבעית. הוכח שאם כל תת-מודול של M נוצר סופית, אז גם כל תת-מודול של $M[x]$ נוצר סופית (מעל $R[x]$). הדרכה. זהו משפט הבסיס של הילברט, 3.3.30 (עמ' 83).

מטריצת היחסים

לכל מטריצה $A \in M_n(R)$, $A \cdot R^n = \{Ax : x \in R^n\}$ הוא תת-מודול של R^n , ונסמן $M_A = R^n / A \cdot R^n$. המטריצה A נקראת **מטריצת יחסים** של $M_A = R^n / A \cdot R^n$.

תרגיל 5.2.8 ()** תת-המודול $A \cdot R^n$ של R^n נפרש על-ידי העמודות של A .

(תת-מודול של R^n אפשר להציג בצורה $A \cdot R^n$ גם כאשר A אינה בהכרח ריבועית, בהתאם למספר היוצרים הנתון. משפט 5.2.1 מבטיח שאפשר להציג את אותו מודול גם בעזרת מטריצה ריבועית, אבל לצורך הניתוח המופיע בהמשך, החלפה זו אינה הכרחית.)

תרגיל 5.2.9 (*)** אם R ראשי, אז כל תת-מודול של R^n הוא מהצורה $A \cdot R^n$ עבור $A \in M_n(R)$ כלשהי. הדרגה. משפט 5.2.1.

מסקנה 5.2.10 כל מודול נוצר סופית מעל תחום ראשי הוא מהצורה M_A .

תרגיל 5.2.11 ()** יהי M מודול נוצר סופית מעל תחום שלמות R ; אז יש הטלה $\varphi: R^n \rightarrow M$ עם גרעין $K = \text{Ker}(\varphi)$, כך ש- $M \cong R^n / K$. נניח ש- $e_1, \dots, e_n$ בסיס ל- R^n . אם $\{\sum_i a_{ij} e_i\}_j$ קבוצה הפורשת את K (אין צורך שזה יהיה בסיס), אז $A = (a_{ij})$ היא מטריצת יחסים של M . הדרגה. לכל j , $\sum_i a_{ij} e_i$ הוא וקטור עמודה, השווה לעמודה ה- j במטריצה (a_{ij}) .

תרגיל 5.2.11 מספק אלגוריתם לחישוב מטריצת יחסים של מודול נוצר סופית M מעל תחום שלמות R .

1. נבחר קבוצה פורשת $x_1, \dots, x_n$ של M .

2. נגדיר אפימורפיזם של מודולים $\varphi: R^n \rightarrow M$ לפי $e_i \mapsto x_i$, כלומר $\sum r_i x_i \mapsto \sum r_i e_i$.

3. נמצא קבוצת וקטורים $\sum a_{ij} e_i$ הפורשת את הגרעין $\text{Ker}(\varphi)$.

4. אז $A = (a_{ij})$ היא מטריצת יחסים של M ; כלומר $M \cong M_A$.

5.2.2 מטריצות מעל תחום ראשי

הגדרה 5.2.12 יהי R תחום שלמות כלשהו. נגדיר על $M_n(R)$ יחס שקילות: המטריצות A, B דומות ($A \sim B$) אם ורק אם קיימות $P, Q \in GL_n(R)$ כך ש- $B = PAQ$.

תרגיל 5.2.13 (*) הוכח שדמיון מטריצות הוא אכן יחס שקילות.

תרגיל 5.2.14 (-)** אם $A \sim B$ אז $\det(A) \sim \det(B)$.

תרגיל 5.2.15 (*) עבור $n = 1$ המטריצות $(a), (b)$ דומות אם ורק אם a, b חברים.

תרגיל 5.2.16 ()** הראה שאם R הוא שדה אז יש בדיוק $n + 1$ מחלקות דמיון ב- $M_n(R)$, המאופיינות על-ידי דרגת המטריצה.

הצורה האלכסונית הקנונית

פעולות שורה ועמודה אלמנטריות מעבירות מטריצה נתונה למטריצה דומה לה. כמו מעל שדה, יש שלושה סוגי **פעולות אלמנטריות**: כפל שורה בקבוע הפיך; הוספת כפולה של שורה לשורה אחרת; והחלפת שורות. פעולות אלה מתקבלות על-ידי כפל משמאל במטריצה אלמנטרית מתאימה. כפל באותן מטריצות, מימין, שקול לביצוע פעולות אלמנטריות על העמודות. לפני שנמשיך, כדאי להבין באיזו מידה פעולות כאלה מתארות היטב את יחס השקילות שהגדרנו.

הערה 5.2.17 כל פעולה אלמנטרית על שורות או עמודות אפשר לתרגם לכפל במטריצה הפיכה, אבל, שלא כמו מעל שדה, ההיפך אינו נכון: יש מטריצות הפיכות שאינן מכפלת מטריצות אלמנטריות מאותו סדר.

יהי R חוג קומוטטיבי. אפשר להגדיר את חבורת המטריצות ההפיכות $GL(R)$ $\cup GL_n(R)$ (כאשר $GL_n(R)$ מזהה עם הבולקים בפינה השמאלית-עליונה של $GL_{n+1}(R)$, עם אבר היחידה בפינה הימנית-תחתונה), ולהשוות אותה לתת-החבורה שלה $E(R) = \cup E_n(R)$, הנוצרת על-ידי מטריצות אלמנטריות. מתברר ש- $E(R) \triangleleft GL(R)$, ושחבורת המנה $K_1(R) = GL(R)/E(R)$ היא אבליה. אם מצטמצמים למטריצות מדרג n מקבלים חבורת מנה $SK_1(R)$. ידוע למשל ש- $SK_1(R) = 1$ אם R מקומי (אפילו לא קומוטטיבי). בחוג אוקלידי כל $GL_n(R)$ נוצרת על-ידי המטריצות האלמנטריות מסדר n (זה חזק יותר מן הטענה $K_1(R) = 1$; מדוע?).

בסתם תחום שלמות המטריצות האלמנטריות אינן יוצרות את המטריצות ההפיכות. אם התחום ראשי (או באופן כללי יותר "תחום דזקינד", שלא נגדיר כאן), הכשלון הזה מוסבר כולו על-ידי מטריצות 2×2 . במילים אחרות, $E_n(R)$ ו- $GL_2(R)$ יוצרות יחד את $GL_n(R)$.

תרגיל 5.2.18 ()** מעל כל תחום שלמות, אם $Ra + Rb = Rd$ אז יש $P \in GL_2(R)$ כך ש- $(a, b)P = (d, 0)$. הדרכה. נציג $d = \alpha a + \beta b$ ו- $\begin{pmatrix} \alpha & -b/d \\ \beta & a/d \end{pmatrix}$ הפיכה, ו- $(a, b) \begin{pmatrix} \alpha & -b/d \\ \beta & a/d \end{pmatrix} = (d, 0)$.

משפט 5.2.19 יהי R תחום ראשי. כל מטריצה $A \in M_n(R)$ דומה למטריצה אלכסונית עם $d_1 \mid d_2 \mid \dots \mid d_n$.

הוכחה. נגדיר את ה'אורך' של אבר שונה מאפס להיות הדרגה שלו (אם R אוקלידי) או מספר הגורמים הראשוניים שלו (במקרה הכללי).

ההוכחה היא באינדוקציה על מימד המטריצה, ועבור מטריצות בגודל קבוע, באינדוקציה על האורך המינימלי של רכיב במטריצה. על-ידי מעבר למטריצה דומה, אפשר להניח ש- A מוצגת בצורה שבה אורך הרכיב הקצר ביותר הוא המינימלי האפשרי. על-ידי החלפת שורות ועמודות אפשר להניח שרכיב זה, a , נמצא במקום ה- $(1, 1)$.

טענה: לכל רכיב b בשורה הראשונה מתקיים $a \mid b$. אם R אוקלידי אפשר לראות זאת על-ידי חילוק עם שארית. אחרת, אפשר להניח ש- b במקום ה- $(1, 2)$. נכתוב $Ra + Rb = Rd$ כאשר d קצר מ- a (תרגיל 3.3.39, עמ' 84). לפי תרגיל 5.2.18, יש $P \in GL_2(R)$ הפיכה כך ש- $\begin{pmatrix} a & b \\ * & * \end{pmatrix} P = \begin{pmatrix} d & 0 \\ * & * \end{pmatrix}$, בסתירה למינימליות האורך של a .

באותו אופן a מחלק גם את רכיבי העמודה הראשונה, ועל-ידי פעולה אלמנטרית מתאימה אפשר להניח שהשורה והעמודה הראשונות הן אפס למעט הרכיב שבפינה. כעת $A = (a) \oplus A'$ עם A' ממימד $n - 1$, ובאינדוקציה A' דומה למטריצה אלכסונית

$\text{diag}(d_2, \dots, d_n)$ עם $d_2 \mid \dots \mid d_n$. נחבר את השורה השניה לראשונה, וקיבלנו מטריצה שקולה שבה d_2 מופיע ברכיב ה- $(1, 2)$; לפי הטענה $d_1 \mid d_2$, כדרוש. $\square$

תרגיל 5.2.20 (-)** נסח את הוכחת המשפט כאלגוריתם המחזיר את הצורה האלכסונית הדומה למטריצה נתונה.

תרגיל 5.2.21 (-)** מעל כל תחום שלמות R , יש מטריצה הפיכה $\begin{pmatrix} a & b \\ * & * \end{pmatrix} \in \text{GL}_2(R)$ אם ורק אם $Ra + Rb = R$.

תרגיל 5.2.22 (+)** נניח ש- $a_1, \dots, a_n \in R$, כאשר R חוג ראשי. הוכח שקיימת P הפיכה כך ש- $(a_1, \dots, a_n)P = (d, 0, \dots, 0)$ כאשר d המחלק המשותף המקסימלי.

תרגיל 5.2.23 (+)** אם $Ra_1 + \dots + Ra_n = R$ אז יש Q הפיכה שהשורה הראשונה שלה היא $(a_1, \dots, a_n)$.

תרגיל 5.2.24 (-)** אם $A \in M_n(R)$ דומה למטריצה אלכסונית אז $A \sim A^t$. הדרכה. $A \sim D = D^t \sim A^t$.

תרגיל 5.2.25 (*)** יהי R תחום שלמות. לכל $a, b \in R$, $\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} \sim \begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix}$ אם ורק אם $Ra + Rb$ ראשי. הדרכה. אם $Ra + Rb = Rd$ הפעל את תרגיל 5.2.18. נניח שהמטריצות דומות. כתוב $\begin{pmatrix} x & y \\ z & u \end{pmatrix} \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix} \begin{pmatrix} x' & y' \\ z' & u' \end{pmatrix}$; החישוב מראה ש- $x' = x$, $y' = z$, $z' = xa = zb$, $u' = m$. נסמן $m = xa = zb$. אז $Rab = (Ra + Rb)m$, ולפי תרגיל 1.2.38 (עמ' 25) יוצא ש- $Ra + Rb$ ראשי.

יחידות הצורה האלכסונית

נראה כיצד הכללה של תרגיל 5.2.14 מאפשרת להוכיח שהצורה האלכסונית היא יחידה.

הגדרה 5.2.26 יהי R חוג קומוטטיבי, ותהי $A \in M_n(R)$. נסמן ב- $\Delta_k(A)$ את האידיאל הנוצר על-ידי כל המינורים בגודל $k \times k$ במטריצה A .

תרגיל 5.2.27 (*) $\Delta_n(A) = R \cdot \det(A)$

תרגיל 5.2.28 ()** לכל $B \in M_k(R)$, $\Delta_k(B) \subseteq \Delta_{k-1}(B)$, הדרכה. פיתוח דטרמיננטה לפי שורה או עמודה.

תרגיל 5.2.29 (-)** לכל $A \in M_n(R)$, $\Delta_n(A) \subseteq \Delta_{n-1}(A) \subseteq \dots \subseteq \Delta_1(A)$, הדרכה. העזר בתרגיל 5.2.28.

תרגיל 5.2.30 (*)** אם $B = PA$ עבור מטריצה P כלשהי, אז לכל k , $\Delta_k(B) \subseteq \Delta_k(A)$. הדרכה. אפשר להניח ש- $P \in M_{k \times n}$, $A \in M_{n \times k}$, ואז

$$\begin{aligned} \det(PA) &= \sum_{\sigma \in S_k} \text{sgn}(\sigma) \prod_i (PA)_{i, \sigma(i)} \\ &= \sum_{\sigma} \text{sgn}(\sigma) \prod_i \sum_j P_{ij} A_{j, \sigma(i)} \\ &= \sum_{j_1, \dots, j_k} P_{1, j_1} \dots P_{k, j_k} \left(\sum_{\sigma} \text{sgn}(\sigma) \cdot A_{j_1, \sigma(1)} \dots A_{j_k, \sigma(k)} \right); \end{aligned}$$

הסכום בסוגריים הוא מינור אם $j_1, \dots, j_k$ שונים זה מזה, ושווה לאפס אחרת.

תרגיל 5.2.31 ()** אם $B \sim A$ אז $\Delta_k(B) = \Delta_k(A)$. הדרכה. תרגיל 5.2.30.

תרגיל 5.2.32 (-*)** יהי R תחום שלמות. אם $\text{diag}(d_1, \dots, d_n) \sim \text{diag}(d'_1, \dots, d'_n)$ כאשר $d_1 \mid \dots \mid d_n$ ו- $d'_1 \mid \dots \mid d'_n$, אז $d'_i \sim d_i$ לכל i . הדרכה. $\Delta_k(\text{diag}(d_1, \dots, d_n)) = d_1 \cdots d_k R$ ולכן $d_1 \cdots d_k = d'_1 \cdots d'_k$ לכל k .

משפט 5.2.33 כל מטריצה מעל תחום ראשי דומה למטריצה יחידה מהצורה $\text{diag}(d_1, \dots, d_n)$ עם $d_1 \mid \dots \mid d_n$, עד כדי חבורות של הקבועים.

הוכחה. לפי משפט 5.2.19 $A \sim \text{diag}(d_1, \dots, d_n)$ כאשר $d_1 \mid \dots \mid d_n$. היחידות נובעת מתרגיל 5.2.32. $\square$

למטריצה האלכסונית היחידה מהצורה $\text{diag}(d_1, \dots, d_n)$ עם $d_1 \mid \dots \mid d_n$ הדומה ל- A , קוראים הצורה האלכסונית הקנונית של A . האברים $d_1, \dots, d_n$ עצמם נקראים הגורמים האיננווריאנטיים של A .

תרגיל 5.2.34 ()** יהי R תחום שלמות. אם כל מטריצה ב- $M_2(R)$ דומה למטריצה אלכסונית, אז R מקיים את תכונת בזו. הדרכה. אם $\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} \sim \begin{pmatrix} d & 0 \\ 0 & d' \end{pmatrix}$ אז לפי תרגיל 5.2.31 אפשר להניח ש- $d' = 0$ ו- $Rd = Ra + Rb$.

תרגיל 5.2.35 (**)** האם משפט 5.2.19 תקף מעל כל תחום בזו?

מטריצות יחסים דומות

תרגיל 5.2.36 ()** 1. אם $B = AQ$, Q הפיכה, אז $A \cdot R^n = B \cdot R^n$.

2. אם $B = PA$, P הפיכה, אז $M_A \cong M_B$.

מסקנה 5.2.37 אם $A, B \in M_n(R)$ דומות אז $M_A \cong M_B$ (כמודולים מעל R).

תרגיל 5.2.38 (-*)** R חוג קומוטטיבי. הראה שאם המודולים R/Ra ו- R/Rb איזומורפיים, אז $a \sim b$. הדרכה. ראה תרגיל 5.1.65, עמ' 124.

תרגיל 5.2.39 (++) האברים $2 + \sqrt{-1}$ ו- $2 - \sqrt{-1}$ של $\mathbb{Z}[\sqrt{-1}]$ אינם חברים. האם יש סתירה בין תרגילים 1.2.88 (עמ' 31) ו-5.2.38?

תרגיל 5.2.40 (**)** מצא הוכחה ישירה לטענה ההפוכה למסקנה 5.2.37: אם $M_A \cong M_B$ אז A, B דומות (ראה מסקנה 5.2.47).

לפי מסקנה 5.2.10 כל מודול נוצר סופית מעל תחום ראשי הוא מהצורה M_A עבור מטריצה מתאימה A . לאחר שהשלמנו את מיון המטריצות במשפט 5.2.33, לא נותר אלא לתרגם מיון זה לשפת המודולים. כידוע, הסכום הישר של מטריצות הוא מטריצת בלוקים, שהמטריצות הנתונות מסודרות בה לאורך האלכסון הראשי.

תרגיל 5.2.41 ()** תהינה A, B מטריצות בלוקים מסדר n, m , בהתאמה. אז $M_{A \oplus B} \cong M_A \oplus M_B$.

תרגיל 5.2.42 ()** נניח ש- $A = \text{diag}(d_1, \dots, d_n)$ אלכסונית. אז $M_A = \bigoplus R/d_i R$ סכום של מודולים ציקליים.

5.2.3 פירוק למרכיבים ציקליים

ממשפט 5.2.33 אפשר להסיק ישירות את התוצאה המרכזית בתורת המבנה של מודולים מעל חוג ראשי.

טענה 5.2.43 יהיו הגורמים האינזיריאנטיים של מטריצה $A \in M_n(R)$. אז

$$M_A \cong R/d_1R \oplus \cdots \oplus R/d_nR.$$

הוכחה. לפי ההגדרה $A \sim \text{diag}(d_1, \dots, d_n)$, ואז $M_A \cong M_{(d_1) \oplus \cdots \oplus (d_n)}$ לפי מסקנה 5.2.37; מודול זה מתפרק לסכום ישר $M_{(d_1)} \oplus \cdots \oplus M_{(d_n)} = R/d_1R \oplus \cdots \oplus R/d_nR$ לפי תרגיל 5.2.42. $\square$

כלומר:

משפט 5.2.44 מעל תחום ראשי, כל מודול נוצר סופית הוא סכום ישר של מודולים ציקליים.

האברים $d_i \in R$ נקראים **המחלקים** של M . אם d_i הפיך, הוא תורם את הגורם $R/d_iR = 0$ ואפשר להשמיט אותו. מאידך אם $d_{k+1} = 0$, אז המרכיב $R/d_{k+1}R \oplus \cdots \oplus R/d_nR \cong R^{n-k}$ הוא תת-מודול חופשי של M .

תרגיל 5.2.45 (*)** הראה שהמודול $\mathbb{Z}[x]/\langle 4, 2x \rangle$ אינו ניתן להצגה כסכום ישר של מודולים ציקליים מעל $\mathbb{Z}[x]$.

משפט 5.2.46 ההצגה של מודול נוצר סופית M מעל תחום ראשי R בצורה $M \cong R/d_1R \oplus \cdots \oplus R/d_nR$ כאשר $d_1 \mid \cdots \mid d_n$ אינו הפיך, היא יחידה עד כדי החלפת d_i בחברים.

הוכחה. נניח ש- m מקסימלי כך ש- $d_m \neq 0$, וכך $t(M) = R/d_1R \oplus \cdots \oplus R/d_mR$ והמנה $M/t(M) \cong R^{n-m}$. לפי משפט 5.1.54, $n - m$ מוגדר היטב. נתבונן מעתה ב- $M' = t(M)$. לכל ראשוני $p \in R$, $pM' = t(M)/pM'$ הוא מרחב וקטורי מעל השדה R/pR , שממדו שווה למספר גורמי ההרכב המתחלקים ב- p . הממד הזה מקבל את הערך המקסימלי האפשרי, m , כאשר $p \mid d_1$. יהי $p \mid d_1$. האורך וגורמי ההרכב של $pM' = \bigoplus R/\frac{d_i}{p}R$ מוגדרים היטב, ומהם אפשר לשחזר את האורך וגורמי ההרכב של M' . $\square$

מסקנה 5.2.47 כל מודול נוצר סופית מעל תחום ראשי R אפשר להציג בצורה M_A , כאשר A יחידה עד כדי החלפת A ב- $I_k \oplus A$ ודמיון.

הוכחה. לפי מסקנה 5.2.10 יש למודול הצגה בצורה M_A , ולפי משפט 5.2.19 אפשר להניח ש- $A = \text{diag}(d_1, \dots, d_n)$ כאשר $d_1 \mid \cdots \mid d_n$. לאחר ניכוי הגורמים ההפיכים, הנותרים יחידים עד-כדי חברות לפי משפט 5.2.46. $\square$

תרגיל 5.2.48 ()** אם $A, B \in M_n(R)$ כאשר R ראשי, אז $M_A \cong M_B$ נובע ש- $A \sim B$.

תרגיל 5.2.49 (*)** מעל תחום ראשי, כל מודול חסר פיתול הוא חופשי.

הערה 5.2.50 חוג קומוטטיבי נקרא חוג FGC אם כל מודול נוצר סופית מעל R הוא סכום ישר של מודולים ציקליים. תחום שלמות R הוא FGC אם ורק אם R הוא תחום בזו כמעט מקסימלי (R כמעט מקסימלי אם כל חוג מנה אמיתי שלו הוא מקסימלי; חוג הוא מקסימלי אם קיום פתרון לכל תת-מערכת סופית של מערכת משוואות $x \equiv a_\lambda \pmod{L_\lambda}$, כאשר $L_\lambda \triangleleft R$, מבטיח פתרון למערכת כולה).

יתרה מזו, מעל תחום שלמות FGC , ההצגה של מודול נוצר סופית כסכום $R/I_1 \oplus \dots \oplus R/I_n$, כאשר $I_1 \subseteq \dots \subseteq I_n \subset R$, היא יחידה. [Lecture Notes in Mathematics 723, Willy Brandal, 1979, משפטים 5.2, 9.4, 9.5]

בין תחומי בזו הכמעט מקסימליים אפשר למנות כל תחום הערכה מקסימלי, ואלו אינם בהכרח תחומים ראשיים. למשל, כל חוג של טורי חזקות ארוכים (תת-סעיף 3.4.2) הוא תחום הערכה מקסימלי.

תרגיל 5.2.51 (-*)** מודולים מעל החוג $R = \mathbb{Z}[\sigma \mid \sigma^2 = 1]$ הם חבורות אבליות עם אנדומורפיזם מסדר 2. הראה שהחבורה האבלית $A = \langle \beta, \gamma \mid 4\beta = 2\gamma = 0 \rangle$, שהיא מודול מעל R לפי הפעולה $\sigma\beta = -\beta$ ו- $\sigma\gamma = \gamma + 2\beta$, אינה סכום ישר של תת-מודולים ציקליים. הדרכה. כל תת-מודול מכיל את $\langle 2\beta \rangle$; למעשה, יש סדרה מדויקת קצרה יחידה $0 \rightarrow \mathbb{Z}/2\mathbb{Z} \rightarrow A \rightarrow (\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}) \rightarrow 0$.

תת-מודול הפיתול כמחובר ישר

נאמר שלמודול M יש פיתול מתפרק אם יש פירוק לסכום ישר $M = t(M) \oplus M'$.

תרגיל 5.2.52 (+*) אם קיים פירוק $M = t(M) \oplus M'$, אז M' יחיד עד כדי איזומורפיזם. הדרכה. $M' \cong M/t(M)$.

תרגיל 5.2.53 ()** למודול יש פיתול מתפרק אם ורק אם אפשר לכתוב אותו כסכום ישר של מודול מפותל ומודול חסר-פיתול. הדרכה. אם הפיתול מתפרק אז $M = t(M) \oplus M'$ כאשר $M' \cong M/t(M)$ חסר פיתול. מאידך אם $M = T \oplus M'$ כאשר T מפותל ו- M' חסר פיתול, אז $t(M) = t(T) \oplus t(M') = T \oplus 0$.

תרגיל 5.2.54 (*)** מעל תחום ראשי, לכל מודול נוצר סופית יש פיתול מתפרק.

תרגיל 5.2.55 (*)** יהי R תחום שלמות, ויהיו $a, b, c \in R$. נסמן

$$M'^c = M'_{a,b}^c = (Rx + Ry)/Rc(ax - by).$$

1. הראה ש- $t(M') \cong (Ra \cap Rb)/Rabc$ ו- $M'/t(M') \cong (Ra + Rb)$. הדרכה. נסמן $T = \{\lambda x - \lambda'y : b\lambda = a\lambda'\} \cong (Ra \cap Rb)/Rabc$ ואז $T = t(M')$.

2. נסמן גם $M = M_{a,b}^c = (Ra \cap Rb)/Rabc \oplus (Ra + Rb)$. הראה שאם M' בעל פיתול מתפרק, אז $M' \cong M$. ראה תרגיל 5.2.56 להמשך.

תרגיל 5.2.56 (*)** אם R תחום gcd שבו כל מודול נוצר סופית הוא בעל פיתול מתפרק, אז R תחום בזו. הדרכה. בהמשך לתרגיל 5.2.55, נניח ש- a, b זרים (במובן ש- $Ra \cap Rb = Rab$). הראה ש- $A = \begin{pmatrix} 1 & 0 & 0 \\ 0 & ca & -cb \\ 0 & 0 & 0 \end{pmatrix}$ היא מטריצת יחסים של $M'_{a,b}$, וש- $A = \begin{pmatrix} c & 0 & 0 \\ 0 & a & -b \\ 0 & 0 & 0 \end{pmatrix}$ היא מטריצת יחסים של $M_{a,b}^c$. בחר $c = ab$. הראה שאם המטריצות דומות אז $Ra + Rb = R$. לשם כך, פתור את המשוואה $PA = A'P'$ עבור הפיכות P, P' .

הערה 5.2.57 לפי תרגיל 5.2.56 תחום gcd שמעליו כל מודול נוצר סופית הוא בעל פיתול מתפרק, הוא תחום בזו. מכאן נובע שכל תחום פרופר (ראה להלן) בעל gcd הוא תחום בזו.

הערה 5.2.58 התכונה מתרגיל 5.2.54 נכונה בכל תחום פרופר (תחום פרופר הוא תחום שלמות שבו לכל אידיאל I יש אידיאל I' כך ש- $II' = I$ ראשי; תכונה זו שקולה לכך שכל שלושה אידיאלים מקיימים את התנאי (3) של תרגיל 2.2.19. **תחום דדקינד** הוא תחום פרופר נטרי). (הוכחה, המשתמשת בכמה מונחים שלא הגדרנו: $M/t(M)$ חסר פיתול. מעל תחום פרופר נובע מכך שהוא שטוח. מכיוון ש- $M/t(M)$ שטוח ונוצר סופית, הוא פרויקטיבי. לכן הוא מחובר ישר ב- M).
(למעשה, (כפי שהראה לי Francois Couchot):

• תחום שלמות הוא פרופר אם ורק אם לכל מודול נוצר סופית יש פיתול מתפרק, ו- R_M קוהרנטי (= כל מודול נוצר סופית הוא מוצג סופית) לכל $M \triangleleft R$ מקסימלי. ולכן:

• תחום שלמות נטרי הוא דדקינד אם ורק אם לכל מודול נוצר סופית יש פיתול מתפרק.

תרגיל 5.2.59 (*)** אם R תחום שלמות ולכל מודול M יש פיתול מתפרק, אז R שדה. [הדרכה. תרגיל I.8.7 ב-L. Fuchs and L. Salce, "Modules over Non-Noetherian Domains"] נניח $R = R[\frac{1}{b}]$. ניקח $Q = R[\frac{1}{b}]$. נתבונן במודול $M = \sum_{i \geq 0} Rx_i$ המוגדר על-ידי היחסים $b^i x_i = x_0$. יש הטלה טבעית $\varphi: M \rightarrow Q$ לפי $x_i \mapsto b^{-i}$. הראה ש- $t(M) = \text{Ker}(\varphi)$. לכל i נבחר קבוצה $R_i \subseteq R$ כך שלכל אבר של $R/b^i R$ יש נציג יחיד ב- R_i . הראה שאפשר להציג כל אבר של M באופן יחיד בצורה $a_0 x_0 + \sum_{i=1}^n a_i x_i$ כאשר $a_0 \in R$ ו- $a_i \in R_i$. הראה ש- $Rx_0 = \bigcap b^i M$. הסק ש- $Q = t(M) \oplus M$, ולכן $t(M)$ אינו מחובר ישר ב- M . [כתרגיל נוסף, הראה ש- $t(M) \cong \bigoplus R/b^i R$]

מיון החבורות האבליות הנוצרות סופית

את המיון של חבורות אבליות נוצרות סופית מקבלים ממשפט 5.2.46 כמסקנה מיידיית:

משפט 5.2.60 כל חבורה אבליית נוצרת סופית אפשר להציג באופן יחיד כסכום של חבורות ציקליות, $A = \bigoplus \mathbb{Z}/d_i \mathbb{Z}$, עם $d_1 | \dots | d_n$, כאשר $d_1 \neq 1$.

תרגיל 5.2.61 ()** אם $A = \bigoplus \mathbb{Z}/d_i \mathbb{Z}$ ההצגה הקנונית של חבורה אבליית A , אז $\exp(A) = d_n$.

תרגיל 5.2.62 ()** החבורה A לעיל סופית אם ורק אם $d_n \neq 0$.

5.2.4 צורות קנוניות של מטריצות מעל שדה

בסעיף זה נלמד את הצורות השונות שבהן אפשר להפוך את המרחב הוקטורי F^n למודול מעל חוג הפולינומים $R = F[x]$, ונקבל הצגות שונות של מטריצות ריבועיות. נסכם את התוצאות העיקריות שקיבלנו בסעיף הקודם, עבור מודולים נוצרים סופית מעל תחום ראשי R :

1. כל מטריצה $A \in M_n(R)$ דומה לצורה אלכסונית יחידה $\text{diag}(d_1, \dots, d_n)$ עם $d_1 | \dots | d_n$ (משפט 5.2.33).

2. כל מודול נוצר סופית איזומורפי לסכום ישר של מודולים ציקליים $R/d_1R \oplus \dots \oplus R/d_nR$, עם $d_1 \mid \dots \mid d_n$ יחידים עד כדי חבורות (משפט 5.2.46).

3. כל מודול נוצר סופית איזומורפי ל- $R^n/A \cdot R^n$ עבור $A \in M_n(R)$ יחידה עד כדי דמיון (מסקנה 5.2.47).

מרחב וקטורי כמודול לפי מטריצה

יהי V מרחב וקטורי n -ממדי מעל שדה F , ותהי $T: V \rightarrow V$ העתקה ליניארית. בסעיף זה נלמד את V כמודול מעל $F[x]$ לפי T , כלומר $x \cdot v = T(v)$, כפי שתואר בתרגיל 5.1.5 (עמ' 118). את המודול המתקבל נסמן ב- V_T .

תרגיל 5.2.63 ()** תת-המודולים של V כמודול מעל $F[x]$ ביחס ל- T הם בדיוק תת-המרחבים ה- T -אינווריאנטיים של V , כלומר תת-מרחבים $U \leq V$ כך ש- $T(U) \subseteq U$.

תרגיל 5.2.64 ()** נניח ש- V, V' הם מרחבים וקטוריים מעל F . תהייה $T: V \rightarrow V$ ו- $T': V' \rightarrow V'$ העתקות ליניאריות. הראה ש- $V \oplus V'$ כמודול מעל $F[x]$ לפי $T \oplus T'$ איזומורפי - כמודול - לסכום הישר של V (כמודול לפי T) ו- V' (כמודול לפי T').

(תוצאות אלה קושרת תת-מודולים של V עם הצגת A בצורת בלוקים משולשת, ופירוק של V לסכום ישר של תת-מודולים עם ההצגה של A כמטריצת בלוקים.)

כרגיל, אפשר לבחור בסיס $v_1, \dots, v_n$ הקובע איזומורפיזם $V \cong F^n$ לפי $v \mapsto [v]$, ומטריצה מייצגת $A = [T]$, כך ש- $[Tv] = A[v]$. כלומר, $T(v_j) = \sum_i A_{ij}v_i$. יהי $e_1, \dots, e_n$ הבסיס הסטנדרטי של F^n מעל F , כך ש- $Ae_j = \sum_i A_{ij}e_i$.

תרגיל 5.2.65 ()** כמודול, $V = \sum Fv_i = \sum F[x]v_i$, ולכן V_T הוא מודול מנה של המודול החופשי $F[x]^n$.

כדי להבין את V כמודול מעל $F[x]$, נמצא לו מטריצת יחסים. נסמן ב- I_n את מטריצת היחידה מסדר n .

משפט 5.2.66 המטריצה $xI_n - [T]$ היא מטריצת יחסים של V_T .

הוכחה. נסמן $A = [T]$. נסמן ב- $\bar{e}_i$ את וקטורי הבסיס הסטנדרטי של $F[x]^n$. ההתאמה $\bar{e}_i \mapsto v_i$ מגדירה אפימורפיזם $F[x]^n \rightarrow V$ באופן הבא: $\sum f_i(x)\bar{e}_i \mapsto \sum f_i(T)v_i$. בפרט, לכל j , $x\bar{e}_j \mapsto T(v_j) = \sum_i A_{ij}v_i$, ומכאן ש-

$$w_j = \sum_i (\delta_{ij}x - A_{ij})\bar{e}_i = x\bar{e}_j - \sum_i A_{ij}\bar{e}_i \mapsto 0.$$

נראה ש- $K = \sum_j F[x]w_j$, המוכל ב- $\text{Ker}(\varphi)$ לפי החישוב, שווה לגרעין כולו. מכאן יצא שהוקטורים w_j ($j = 1, \dots, n$) פורשים את הגרעין, ולפי תרגיל 5.2.11 (עמ' 127) נקבל ש- $xI_n - A$ היא מטריצת יחסים של המודול, משום שהעמודה ה- j שלה היא הוקטור $(\delta_{ij}x - A_{ij})_i$.

נותר, אם כך, להראות ש- $K = \text{Ker}(\varphi)$. נסמן $\bar{V} = \sum F\bar{e}_i$ תת-מרחב של $F[x]^n$ שאינו תת-מודול מעל $F[x]$. הצמצום של φ אל $\bar{V}$ הוא איזומורפיזם $\bar{V} \rightarrow V$. מכיוון

ש- $x\bar{V} \subseteq K + \bar{V}$ ברור ש- $x\bar{e}_j = w_j + \sum_i A_{ij}\bar{e}_i \in K + \bar{V}$ מכאן נובע באינדוקציה ש- $x^\ell \bar{V} \subseteq K + \bar{V}$ לכל ℓ , ולכן $F[x]^n = \sum_\ell x^\ell \bar{V} = K + \bar{V}$. נבחין ש- $\text{Ker}(\varphi) \cap \bar{V} = 0$, שהרי $\varphi(\sum \alpha_i \bar{e}_i) = \sum \alpha_i v_i$, כך שלמעשה $F[x]^n = K \oplus \bar{V}$.

□ כעת אפשר להפעיל את φ על וקטור כללי, ולהסיק ש- $\text{Ker}(\varphi) = K$.
מסקנה 5.2.67 לכל מטריצה $A \in M_n(F)$, יש איזומורפיזם של מודולים מעל $F[x]$,
 $(F^n)_A \cong F[x]^n / (xI_n - A)F[x]^n$.

מחלקות צמידות

תרגיל 5.2.68 (+)** אם $xI_n - A$ ו- $xI_n - B$ דומות, אז ל- A, B יש אותו פולינום אופייני. הדרכה. קח את הדטרמיננטה של $xI_n - A = P(x)(xI_n - B)Q(x)$.

נאמר שמטריצות $A, B \in M_n(F)$ הן **צמודות** אם יש $P \in \text{GL}_n(F)$ כך ש-
 $B = PAP^{-1}$.

תרגיל 5.2.69 (*) הצמידות היא יחס שקילות על חוג המטריצות $M_n(R)$.

טענה 5.2.70 $(F^n)_A \cong (F^n)_B$ אם ורק אם המטריצות $A, B \in M_n(F)$ צמודות.

הוכחה. כל איזומורפיזם $(F^n)_A \rightarrow (F^n)_B$ הוא בפרט איזומורפיזם של מרחבים וקטוריים, כלומר העתקה מהצורה $\varphi: v \mapsto Pv$ כאשר $P \in \text{GL}_n(F)$. נבדוק מתי העתקה כזו היא איזומורפיזם של מודולים: $PAv = \varphi(Av) = \varphi(xv) = x\varphi(v) = B\varphi(v) = BPv$ לכל $v \in F^n$, כלומר $PA = BP$.

□

משפט 5.2.71 המטריצות A, B צמודות אם ורק אם $xI_n - A$ ו- $xI_n - B$ דומות.

הוכחה. אם $B = PAP^{-1}$ עבור $P \in \text{GL}_n(F)$ אז P הפיכה גם מעל $F[x]$ ו-
 $xI_n - A = P(xI_n - B)P^{-1}$. נניח ש- $xI_n - A$ ו- $xI_n - B$ דומות. לפי מסקנה 5.2.37, המודולים $F[x]^n / (xI_n - A)F[x]^n$ ו- $F[x]^n / (xI_n - B)F[x]^n$ איזומורפיים, ולפי מסקנה 5.2.67 פירושו של דבר הוא שיש איזומורפיזם מ- F^n כמודול מעל $F[x]$ לפי A , אל אותו מרחב כמודול לפי B . בפרט, זהו איזומורפיזם של מרחבים וקטוריים מעל F , שאפשר להציג על-ידי מטריצה הפיכה. אבל אז $P(Av) = P(xv) = xP(v) = BP(v)$ ולכן $[P]A = B[P]$. □

תרגיל 5.2.72 (**)** מצא הוכחה למשפט שאינה משתמשת במסקנה 5.2.67: הראה שאם קיימות $P(x), Q(x) \in \text{GL}_n(F[x])$ כך ש- $xI_n - A = P(x)(xI_n - B)Q(x)$ אז A, B צמודות.

אם כך, יש התאמה בין:

• הדרכים לראות את F^n כמודול מעל $F[x]$, עד כדי איזומורפיזם;

• מחלקות הצמידות ב- $M_n(F)$;

• המטריצות מהצורה $xI_n - A$ עד כדי דמיון;

• וסדרות הגורמים האינוריאנטים $d_1(x) | \dots | d_t(x)$ עם $\sum \deg d_i(x) = n$, עד כדי חברות.

הצורה הרציונלית

יהיו $d_1(x) | \cdots | d_n(x)$ הגורמים האינוריאנטים של $xI_n - A$ (מעל $F[x]$).

תרגיל 5.2.73 ()** הוכח שהפולינום המינימלי של A הוא $d_n(x)$.

תרגיל 5.2.74 ()** הוכח שהפולינום האופייני של A הוא $d_1(x) \cdots d_n(x)$. הדרכה.

תרגיל 5.2.14, עמ' 127.

תרגיל 5.2.75 (-)** הוכח ש- $\sum \deg(d_i(x)) = n$.

המטריצה המלווה של פולינום

הגדרה 5.2.76 יהי $f = \lambda^m - \sum_{i=0}^{m-1} a_i \lambda^i \in F[\lambda]$ פולינום מתוקן ממעלה m . **המטריצה המלווה של f היא $C_f \in M_m(F)$ המוגדרת לפי**
 $C_f = \sum_{i=1}^{m-1} e_{i+1,i} + \sum_{i=0}^{m-1} \alpha_i e_{i+1,m}$

(פורמלית, אם הפולינום f הוא סקלר, מגדירים C_f להיות המטריצה הריקה, בגודל 0×0 , שהיא אבר נייטרלי ביחס לסכום ישר של מטריצות.)

תרגיל 5.2.77 ()** הוכח ש- $\det(xI_m - C_f) = f(x)$, ובפרט $f(C_f) = 0$.

תרגיל 5.2.78 ()** $(F^m)_{C_f} \cong F[x]/\langle f \rangle$ לכל פולינום מתוקן f ממעלה m . הדרכה.
 בחר בסיס $v_0, \dots, v_{m-1}$ של $V = F^m$. לפי ההגדרה, $C_f^i v_0 = v_i$ לכל $i < m$, $v_0 = f(C)v_0 = 0$.
 לכן $V = F[x]v_0$ הוא מודול ציקלי, והמאפס שלו הוא $\langle f \rangle$ (סיים בעזרת תרגיל 5.1.63, עמ' 123).

כלומר, אם C היא מטריצה מלווה לפולינום, אז $(F^m)_C$ הוא מודול ציקלי.

מסקנה 5.2.79 תהי $\hat{C} = C_{f_1} \oplus \cdots \oplus C_{f_k}$ סכום ישר של בלוקים שכל אחד מהם מטריצה מלווה, אז

$$F[x]^n / (xI_n - \hat{C})F[x]^n \cong F[x]/\langle f_1 \rangle \oplus \cdots \oplus F[x]/\langle f_k \rangle,$$

כאשר $n = \sum \deg f_i$.

הוכחה. לפי תרגיל 5.2.78, $F[x]/\langle d_i \rangle \cong (F^m)_{C_{d_i}}$ לכל i , והסכום הישר איזומורפי לפי תרגיל 5.2.64 ל- $(F^n)_{\hat{C}}$, האיזומורפי בתורו ל- $F[x]^n / (xI_n - \hat{C})F[x]^n$ לפי מסקנה 5.2.67. $\square$

תרגיל 5.2.80 ()** תהי $C = C_f$ המטריצה המלווה של פולינום מתוקן f . אז הגורמים האינוריאנטים של $xI_m - C$ הם $1 | \cdots | 1$.

הדרכה. לפי מסקנה 5.2.67, $(F^m)_C \cong F[x]^m / (xI_m - C)F[x]^m$; מאידך, לפי תרגיל 5.2.78, $(F^m)_C \cong F[x]/\langle f \rangle$.
 הוא מודול ציקלי. התוצאה נובעת, אם כך, מיחידות הפירוק של $F[x]^m / (xI_m - C)F[x]^m$ למרכיבים ציקליים.

הגדרה 5.2.81 תהי $A \in M_n(F)$ מטריצה. **הצורה הרציונלית של A היא מטריצת הבלוקים**
 $C_{d_1} \oplus \cdots \oplus C_{d_n}$, כאשר $d_1 | \cdots | d_n$ הם הגורמים האינוריאנטים של $xI_n - A$ (מעל $F[x]$).

משפט 5.2.82 כל מטריצה צמודה לצורה הרציונלית שלה.

הוכחה. יהיו $d_1, \dots, d_n$ הגורמים האינוריאנטיים של $xI_n - A$, ונסמן $m_i = \deg(d_i(x))$. נתבונן במודול $F[x]^n / (xI_n - A)F[x]^n$. לפי טענה 5.2.43 הוא מתפרק לסכום ישר $\oplus F[x] / \langle d_i \rangle$, האיזומורפי ל- $F[x]^n / (xI_n - \hat{C})F[x]^n$ לפי מסקנה 5.2.79. אבל אז $xI_n - A$ ו- $xI_n - \hat{C}$ דומות (תרגיל 5.2.48, עמ' 131), ולפי משפט 5.2.71, A צמודה ל- $\hat{C}$. $\square$

משפט 5.2.83 תהי $\hat{C} = C_{d_1} \oplus \dots \oplus C_{d_n}$ כאשר $d_1(x) \mid \dots \mid d_n(x)$ הם פולינומים, כך ש- $\sum \deg(d_i) = n$. אז אלו הם הגורמים האינוריאנטיים של $xI_n - \hat{C}$.

הוכחה. נסמן ב- $d'_1(x) \mid \dots \mid d'_n(x)$ את הגורמים האינוריאנטיים של $xI_n - \hat{C}$. מצד אחד $F[x]^n / (xI_n - \hat{C})F[x]^n$ איזומורפי לסכום הישר של $F[x] / d'_i(x)F[x]$, ומצד שני הוא איזומורפי לסכום הישר של $F[x] / d_i(x)F[x]$ לפי מסקנה 5.2.79. השוויון נובע ממשפט 5.2.46. $\square$

תרגיל 5.2.84 (***) הראה שאם f, g פולינומים זרים אז $C_f \oplus C_g$ צמוד ל- C_{fg} .

להלן שתי מסקנות הנובעות מן התאוריה שפיתחנו.

תרגיל 5.2.85 (***) תהי $A \in M_n(F)$. הוכח ש- A צמודה ל- A^t . הדרכה. הפעל את תרגיל 5.2.24 (עמ' 129) ומשפט 5.2.71. (אינני מכיר הוכחה ישירה לטענה זו.)

תרגיל 5.2.86 (***) יהיו $F \subseteq K$ שדות. הוכח שאם $A, B \in M_n(F)$ והמטריצות צמודות מעל K , אז הן צמודות כבר מעל F . הדרכה. הראה שאחרי הרחבת הסקלרים, $F[x]/fK[x]$ הופך להיות $K[x]/fK[x]$. מכאן של- $xI - A$ אותם גורמים אינוריאנטיים מעל F ומעל K .

צורת ז'ורדן

דרך הצורה הרציונלית, תרגיל 5.2.84 מאפשר להציג כל מטריצה כסכום ישר של מטריצות מלוות של פולינומים, שכל אחד מהם הוא חזקת ראשוני. אם השדה סגור אלגברית, כל פולינום כזה הוא מהצורה $(x - \lambda)^k$, ומכאן אנו מגיעים לצורה קנונית חדשה.

בלוק ז'ורדן מסדר k של λ הוא המטריצה $J_k(\lambda) = \lambda I_k + \sum e_{i,i+1}$.

תרגיל 5.2.87 (***) הראה שהפולינום המינימלי של $J_k(\lambda)$ הוא $(x - \lambda)^k$.

תרגיל 5.2.88 (***) הוכח ש- $C_{(x-\lambda)^k}$ צמודה ל- $J_k(\lambda)$.

משפט 5.2.89 אם הפולינום האופייני של $A \in M_n(F)$ מתפצל ב- F , אז A צמודה לסכום ישר של בלוקי ז'ורדן.

תרגיל 5.2.90 (***) הוכח שהפירוק לסכום של בלוקי ז'ורדן הוא יחיד עד כדי סדר.