מבנים אלגבריים

עוזי וישנה

מבנים אלגבריים

מהדורה 2.58 למתרגל

הקדמה. חוברת זו ערוכה ומסודרת לפי תוכנית הלימודים בקורס 'מבנים אלגבריים' למדעי המחשב, 89-214, באוניברסיטת בר־אילן. הקורס (בהיקף של שעתיים הרצאה ושעה תרגיל, לאורך סמסטר אחד) מכסה שלושה נושאים: חבורות (עד המיון של חבורות אבליות סופיות, אך ללא משפטי סילו או סדרות הרכב), חוגים (בעיקר קומוטטיביים, ומאלה החומר הנחוץ לפירוק פולינומים ובניה של שדות) ושדות (סופיים). מצאתי לנכון להקדים מבוא לתורת המספרים, שבמהלכו פוגשים בדרך רמז גם את עקרונות היסוד של תחומי השלמות. החוברת מבוססת על חוברות תרגילים שכתבתי לקורסים בתורת החבורות (88-211) ובתורת החוגים (88-212).

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 למספר רב של תרגילים נוחים 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 (**־), מציינים שהתרגיל עשוי להיות קשה או קל יותר מכפי שנראה במבט ראשון. מספר התרגילים מספיק כדי לפתור חלק מן התרגילים בכיתה, חלק כתרגילי בית, ואת השאר לקראת המבחן, אבל בדרך כלל נמנעתי מלתת וריאציות קלות על תרגילים קיימים. במספר מקומות הרחבתי מעבר לרמה הנדרשת בקורס.

כל התרגילים מנוסחים בלשון זכר, ועם הלומדות הסליחה.

אודה לכל מי שיביא לתשומת ליבי שגיאות, השמטות, כפילויות או שגיאות כתיב, כדי שאוכל לתקנם במהדורה הבאה.

עוזי וישנה, 9.2010

תוכן עניינים

1 מבוא לתורת המספרים 5

1.0 המספרים השלמים . . . 5
1.1 יחס החלוקה . . . 6
1.2 אוקלידיות . . . 6
1.3 המחלק המשותף המקסימלי . . . 7
1.4 ראשוניים ופירוק לגורמים . . . 9
1.5 שקילות מודולו n . . . 10

2 חבורות למחצה ומונוידים 13

2.1 חבורות למחצה . . . 13
2.2 מונוידים . . . 14

3 חבורות ותת־חבורות 17

3.1 חבורות . . . 17
3.2 סדר של חבורה . . . 19
3.3 דוגמאות לחבורות . . . 19
3.4 אבליות . . . 23
3.5 מכפלה ישרה חיצונית . . . 24
3.6 תת־חבורות . . . 25

4 משפט לגרנז' 27

4.1 יוצרים של חבורה ותת־החבורה הנוצרת . . . 27
4.2 קוסטים ומשפט לגרנז' . . . 29
4.3 סדר של איבר . . . 30
4.4 יישומים בתורת המספרים . . . 31
4.5 שימושים להצפנה . . . 34
4.6 חבורות ציקליות . . . 35
4.7 כפל תת־חבורות . . . 37

5 הומומורפיזמים ותת־חבורות נורמליות 39

5.1 הומומורפיזמים . . . 39
5.2 גרעין ותמונה . . . 39
5.3 תת־חבורה נורמלית . . . 41
5.4 חבורת מנה . . . 42

5.5 משפט האיזומורפיזם הראשון 44

6 סריג תת־החבורות 45

6.1 חיתוך ומכפלה של תת־חבורות 45

6.2 מכפלה ישרה פנימית 45

6.3 משפטי האיזומורפיזם 47

6.4 סריג תת־החבורות 48

6.5 אינדקס של תת־חבורות 49

6.6 משפט ההתאמה 50

7 הצמדה ומחלקות הצמידות 51

7.1 המרְכָּז 51

7.2 מרכְּזים 53

7.3 מחלקות צמידות 54

7.4 שוויון המחלקות 58

8 אוטומורפיזמים 61

8.1 חבורת האוטומורפיזמים 61

8.2 המנרמל 64

9 חבורות של תמורות 67

9.1 משפט קיילי 67

9.2 הסימן של תמורה 68

9.3 תמורות מקריות 72

10 חבורות אבליות 75

10.1 תת־חבורת הקומוטטורים 75

10.2 משפט קושי 77

10.3 האקספוננט 78

10.4 הפירוק הפרימרי 79

10.5 חבורות־p אבליות 80

10.6 משפט המיון לחבורות אבליות סופיות 81

10.7 חבורות אבליות אינסופיות 84

11 מבוא לחוגים 87

11.1 חוגים, תת־חוגים ואידיאלים 87

11.2 הומומורפיזמים וחוגי מנה 89

11.3 אידיאלים בחוג קומוטטיבי 90

11.4 תחומי שלמות 92

12 מבוא לשדות סופיים 97

12.1 שורשים של פולינומים 97

12.2 שדות 98

12.3 שדות סופיים 99

פרק 1

מבוא לתורת המספרים

לפרק הראשון מטרה משולשת: נפגוש את הדוגמא הראשונה למערכת אקסיומות פשוטה (התכונות הבסיסיות של פעולות החשבון ויחס בין המספרים הטבעיים) שאפשר להוציא ממנה מסקנות מרחיקות לכת (הפירוק היחיד לגורמים); נתאמן בשיטות האלמנטריות של תורת החוגים, שעוד נכליל בהמשך; וחשוב מכל, נקבל כמה תוצאות חיוניות לבניית הדוגמאות שנראה בהמשך הקורס.

מושגים: יחס החלוקה, מחלק משותף מקסימלי; חילוק עם שארית ואלגוריתם אוקלידס; איברים זרים; מספרי אי־פריק ומספר ראשוני. פירוק יחיד לגורמים. שקילות מודולו n. משפט השאריות הסיני.

1.0 המספרים השלמים

בפרק זה, **מערכת המספרים השלמים** היא המערכת הכוללת מלבד הקבוצה $\mathbb{Z}$ של המספרים השלמים, גם את פעולות החיבור $(+)$ והכפל $(\cdot)$ ואת יחס הסדר ($<$ ו־$\leq$), עם התכונות המוכרות מבית הספר היסודי: $a+(b+c)=(a+b)+c$, אם $a<b$ ו־$0<c$ אז $ac<bc$, וכדומה (בקורס הזה נדלג על הפיתוח המסודר של השלמים מתוך **מערכת פאנו** של המספרים הטבעיים, ובמקום זה נניח את תוצאת הפיתוח כאקסיומות).

את הערך המוחלט מגדירים לפי יחס הסדר: $|a|=a$ אם $a\geq 0$, ו־$|a|=-a$ אם $a<0$.

קבוצת המספרים הטבעיים $\mathbb{N}=\{a\in\mathbb{Z}\colon\ a\geq 0\}$ מקיימת את **תכונת הסדר הטוב**, שלפיה לכל קבוצה לא ריקה יש איבר מינימלי.

תרגיל 1.0.1 (**) הסק מתכונת הסדר הטוב את אקסיומת האינדוקציה: אם $A\subseteq\mathbb{N}$ היא קבוצה המקיימת את שתי ההנחות

- $0\in A$,
- לכל $n\in\mathbb{N}$, אם $n\in A$ אז $n+1\in A$,

אז $A=\mathbb{N}$.

1.1 יחס החלוקה

מגדירים יחס בינארי על המספרים השלמים:

הגדרה 1.1.1 $a|b$ ("a *מחלק את* b") *אם קיים* $c \in \mathbb{Z}$ *כך ש־* $b = ac$.

תרגיל 1.1.2 (*) הוכח שהיחס טרנזיטיבי ורפלקסיבי. יחס כזה נקרא **קדם־סדר**.

תרגיל 1.1.3 (*) יחס החלוקה אינו אנטי־סימטרי (ולכן הוא איננו יחס סדר חלקי חלש).

תרגיל 1.1.4 (*) אם $a \mid b$ ו־$b \neq 0$ אז $|a| \leq |b|$.

תרגיל 1.1.5 (**) מצא את האיברים המינימליים והמקסימליים ביחס לקדם־סדר שהגדרנו.

הגדרה 1.1.6 *האיברים* $a, b \in \mathbb{Z}$ *הם* ***חברים*** *אם* $a \mid b$ *ו־*$b \mid a$*. במקרה כזה מסמנים* $a \sim b$.

תרגיל 1.1.7 (+*) הראה ש־a, b חברים אם ורק אם $b = \pm a$.

תרגיל 1.1.8 (+*) הוכח שיחס החברות הוא יחס שקילות.

תרגיל 1.1.9 (*) כתוב במפורש את מחלקת החברות של המספר a. האם לכל המחלקות אותו גודל?

יחס החברות מאפשר לעדן ולשפר את יחס החלוקה.

הגדרה 1.1.10 *מחלקת החברות* $[a]$ *מְחלקת את* $[b]$ *אם* $a \mid b$.

תרגיל 1.1.11 (**) הוכח שיחס החלוקה בין מחלקות מוגדר היטב. כלומר, אם $a \sim a'$ ו־$b \sim b'$, אז $a \mid b$ אם ורק אם $a' \mid b'$.

משפט 1.1.12 *היחס 'מחלק' הוא יחס סדר חלש (כלומר, אנטיסימטרי, רפלקסיבי וטרנזיטיבי) על אוסף מחלקות החברות ב־*$\mathbb{Z}$.

העובדה שיחס החלוקה אינו יחס סדר על $\mathbb{Z}$ 'מאכזבת' ומפריעה. הפתרון הטבעי הוא לצמצם את ההסתכלות אל קבוצת המספרים הטבעיים, $\mathbb{N}$, שהיא תת־קבוצה מיוחדת של המספרים השלמים, הסגורה לחיבור וכפל, ומכילה נציג אחד מכל מחלקת חברות. בניגוד לפתרון הזה, שאינו זמין בחוגים אחרים, המעבר למחלקות חברות אפשרי תמיד.

1.2 אוקלידיות

משפט 1.2.1 ('האוקלידיות של $\mathbb{Z}$') *לכל* $n \in \mathbb{Z}$ *ו־*$d \neq 0$ *קיימים* q, r *כך ש־* $n = qd + r$ *ו־*$0 \leq r < |d|$.

אוקלידיות היא שם אחר לעובדה שאפשר לחלק עם שארית. לו היינו מאמצים כאן את ההגדרה הכללית לאוקלידיות של תחום שלמות, היינו מחליפים את התנאי $0 \leq r$ ב־ $|r| < |d|$; ראו הגדרה 11.4.38.

תרגיל 1.2.2 (**) נניח שהטענה של משפט 1.2.1 מתקיימת כאשר $n, d > 0$. הסק ממקרה זה את המשפט השלם.

1.3 המחלק המשותף המקסימלי

1.3.1 הגדרת המחלק המשותף המקסימלי

הגדרה 1.3.1 *יהיו $n,m\in\mathbb{Z}$. מספר d נקרא* ***מחלק משותף מקסימלי*** *של n,m* ***אם הוא מקסימלי*** *לגבי יחס החלוקה בין כל המחלקים המשותפים. כלומר, d* ***מחלק את*** *n* ***ואת*** *m, ומתחלק בכל מחלק משותף אחר.*

שימו לב שא-פריורי, לא ברור שתמיד קיים מספר כזה. גם אם d הוא הגדול ביותר בין המחלקים המשותפים לגבי יחס הסדר הרגיל, מדוע בעצם הוא מוכרח להתחלק בכל מחלק משותף אחר? (התשובה לכך מופיעה בהמשך הסעיף, ונסמכת על משפט 1.3.7, שאינו טריוויאלי כלל ועיקר.)

תרגיל 1.3.2 (**) אם d הוא מחלק משותף מקסימלי של a,b, ו־$a'\sim a$, $b'\sim b$, $d'\sim d$, אז d' הוא מחלק משותף מקסימלי של a',b' (במלים אחרות, אפשר לומר שמחלקת החברות $[d]$ היא מחלק משותף מקסימלי של מחלקות החברויות $[a],[b]$).

תרגיל 1.3.3 (**) הוכח ש**אם** קיים מחלק משותף מקסימלי של n ו־m, אז הוא יחיד עד כדי חברות.

תרגיל 1.3.4 (*) לכל a, a הוא מחלק משותף מקסימלי של $a,0$.

1.3.2 $\mathbb{Z}$ כחוג ראשי

הגדרה 1.3.5 ***לכל a,b שלא שניהם אפס, נסמן ב־(a,b) את המספר הגדול ביותר בקבוצת המחלקים המשותפים של a ו־b (גדול ביותר לגבי יחס הסדר הרגיל).***

תרגיל 1.3.6 (*+) (a,b) קיים לכל a,b שאינם שניהם אפס.

משפט 1.3.7 ***לכל $n,m\in Z$, קיימים $\alpha,\beta\in Z$ כך ש־ $\alpha n+\beta m=(n,m)$.***

תרגיל 1.3.8 (***) הוכח את המשפט. **הדרכה.** נסמן ב־e את המינימום של הקבוצה $I_0=\min\{x>0|\exists\alpha,\beta:x=\alpha n+\beta m\}$ ו־$d=(a,b)$. $d\,|\,e$ כי e צירוף ליניארי של a,b. כתוב $a=qe+r$, והראה $r=0$, ולכן $e\,|\,a$; בדומה $e\,|\,b$; לכן $e\leq d$. מכאן $d=e\in I_0$.

תרגיל 1.3.9 (+)** נניח ש־ a,b אינם שניהם אפס. הוכח ש־$d=(a,b)$ הוא מחלק משותף מקסימלי של a,b. **הדרכה.** ברור שכל מחלק של d מחלק את a ואת b. נניח ש־x מחלק את a ואת b, אז הוא מחלק את d לפי מפשט 1.3.7.

תרגיל 1.3.10 (+)** נניח שלמספרים $n_1,\dots,n_t$ אין מחלק משותף גדול מ־1. הראה שקיימים $\alpha_1,\dots,\alpha_t$ כך ש־ $\alpha_1n_1+\cdots+\alpha_tn_t=1$. **הדרכה.** אינדוקציה על t בעזרת משפט 1.3.7.

1.3.3 אלגוריתם אוקלידס

האוקלידיות של חוג השלמים מאפשרת לחשב את המחלק המשותף המקסימלי. התרגיל הבא הוא נקודת המפתח לאלגוריתם:

תרגיל 1.3.11 (**) אם $a = qb + r$ אז $(a,b) = (b,r)$.

דוגמא: $(1146,486) = (486,174) = (174,138) = (138,36) = (36,30) = (30,6) = (6,0) = 6$.

תרגיל 1.3.12 (***) תאר אלגוריתם הנעזר בחילוק עם שארית כדי לחשב את המחלק המשותף המסימלי של שני מספרים נתונים.

תרגיל 1.3.13 (***) הוכח שהסיבוכיות של האלגוריתם שתארת היא לוגריתמית בגדול מבין שני מספרי הקלט. הראה שמספר פעולות החילוק הוא לוגריתם לפי הבסיס $\phi = \frac{1+\sqrt{5}}{2}$. הסבר במה מספרי פיבונאצ'י, המוגדרים לפי $F_n = F_{n-1} + F_{n-2}$, קשורים לכאן.

תרגיל 1.3.14 (*) מצא את $(5614, 1260)$ ואת $(7821, 6429)$.

תרגיל 1.3.15 (+)** הראה שלכל n, $(4n+3, 7n+5) = 1$.

תרגיל 1.3.16 (**) מצא את כל המספרים השלמים n כך ש־ $(n+1) \,|\, (n^2+9)$.

האפשרות להציג את המחלק המשותף המקסימלי כצירוף שלם היא כל־כך שימושית, עד שכדאי להכיר אלגוריתם לחישוב מהיר של המקדמים הללו. האלגוריתם 'רוכב', למעשה, על האלגוריתם לחישוב המחלק המשותף המקסימלי עצמו, והוא נקרא אלגוריתם אוקלידס המוכלל.

תרגיל 1.3.17 (**) נסמן $d = (n,m)$. אם $n = qm + r$ ו־$d = \alpha m + \beta r$ אז $\beta n + (\alpha - \beta q)m = d$.

דוגמא. $(234,61) = (61,51) = (51,10) = (10,1) = (1,0) = 1$. **כעת:** $(1)1 + (0)0 = 1$; **לכן** $(0)10 + (1)1 = 1$; **לכן** $(1)51 - (5)\cdot 10 = 1$; **לכן** $(-5)\cdot 61 + (6)51 = 1$, **ובסופו של דבר** $(6)234 + (-23)\cdot 61 = 1$.

תרגיל 1.3.18 (***) תאר אלגוריתם לחישוב המחלק המשותף המקסימלי של זוג מספרים, והצגה שלו כצירוף שלם שלהם.

תרגיל 1.3.19 (**) מצא $\alpha, \beta \in \mathbb{Z}$ כך ש־ $1525\alpha + 927\beta = 1$.

תרגיל 1.3.20 (+)** בהמשך לתרגיל 1.3.15, מצא $\alpha, \beta \in \mathbb{Z}$ (התלויים ב־n) כך ש־ $(4n+3)\alpha + (7n+5)\beta = 1$.

1.3.4 מספרים זרים

הגדרה 1.3.21 *המספרים* n, m ***הם זרים אם*** $(n,m) = 1$.

טענה 1.3.22 אם a, b זרים ו־$a \,|\, bc$, אז $a \,|\, c$.

תרגיל 1.3.23 (**) הוכח את הטענה. ***הדרכה.*** כתוב $\alpha a + \beta b = 1$.

תרגיל 1.3.24 (*) הראה שהמסקנה של טענה 1.3.22 אינה נכונה אם מוותרים על הדרישה ש־ a, b יהיו זרים.

1.3.5 תרגילים נוספים

תרגיל 1.3.25 (**) הראה שלכל שני מספרים n,m אפשר לכתוב $n=dn'$ ו־$m=dm'$ כאשר $d=(n,m)$ ו־n',m' זרים.

תרגיל 1.3.26 (**) $(kn,km)=k(n,m)$.

תרגיל 1.3.27 (**) אם $(m,k)=1$, אז $(n,mk)=(n,m)\cdot(n,k)$.

תרגיל 1.3.28 (**) הוכח: $(n,mk)|(n,m)\cdot(n,k)$. **הדרכה**. כתוב $an+bm=(n,m), cn+dk=(n,k)$

תרגיל 1.3.29 (**) אם $(n,m)=1$, אז $(n,mk)=(n,k)$.

תרגיל 1.3.30 (**) אם $d\,|\,d'$ אז לכל m, $\frac{d}{(d,m)}\mid\frac{d'}{(d',m)}$.

תרגיל 1.3.31 (**) הוכח ש־k זר ל־nm אם ורק אם k זר ל־n ול־m.

***הגדרה 1.3.32** הכפולה המשותפת המינימלית של n ו־m, המסומנת ב־$[n,m]$, היא המספר הקטן החיובי ביותר המתחלק בשניהם.*

תרגיל 1.3.33 (***) הוכח: $(n,m)[n,m]=nm$. **הדרכה**. העזר בתרגיל 1.3.25.

תרגיל 1.3.34 (**) $\mathbb{N}$ עם יחס החלוקה הוא סריג, שבו $n\vee m=[n,m]$, $n\wedge m=(n,m)$ (ראה תת־סעיף 6.4).

תרגיל 1.3.35 (+***) לכל n,m,k מתקיים $[n,(m,k)]=([n,m],[n,k])$ במונחי התרגיל הקודם, $n\vee(m\wedge k)=(n\vee m)\wedge(n\vee k)$, ולכן הסריג $(\mathbb{N},|)$ "דיסטריבוטיבי".

תרגיל 1.3.36 (־***) יהיו n,m מספרים שלמים.
א. הוכח שקיימים $a|A$ ו־$b|B$ כך ש־ $n=aB$, $m=Ab$ ו־$(A,B)=1$.
ב. הראה שאם $n\neq m$ אז a,b,A,B כנ"ל הם יחידים. **הדרכה**. חשב את $(\frac{n}{(n,m)}^k,m)$, כאשר k גדול מספיק.

1.4 ראשוניים ופירוק לגורמים

***הגדרה 1.4.1** מספר $p\in\mathbb{Z}$ הוא ראשוני אם הוא אינו יכול לחלק מכפלה בלי לחלק את אחד הגורמים שלה.*

הגדרה זו, שבחרנו מסיבות שתתבררנה כשנטפל בתחומי שלמות כלליים, אינה ההגדרה המקובלת למספר ראשוני; צמד התרגילים 1.4.4 ו־1.4.6 מראה שההגדרה המקובלת שקולה לזו שנתנו כאן.

***הגדרה 1.4.2** מספר $p\in\mathbb{Z}$ הוא אי־פריק, אם בכל פירוק $p=ab$, בהכרח $a\sim 1$ או $b\sim 1$.*

כל מספר מתחלק בהפיכים ובחברים שלו, ולכן אלו נקראים 'מחלקים טריוויאליים'.

תרגיל 1.4.3 (*) התכונות הבאות שקולות:

1. p אי־פריק.
2. אם $p=ab$ אז $p\sim a$ או $p\sim b$.
3. אם $p\,|\,a$ אז $a\sim 1$ או $a\sim p$.

תרגיל 1.4.4 **(־**)** כל ראשוני הוא אי־פריק.

תרגיל 1.4.5 **(*)** אם p אי־פריק, אז לכל n, $p\,|\,n$ או $(p,n)=1$.

תרגיל 1.4.6 **(+**)** כל אי־פריק הוא ראשוני. **הדרכה.** יהי p אי־פריק, ונניח $p\,|\,ab$. אם $p\nmid a$ אז $(p,a)=1$ לפי תרגיל 1.4.5, ולפי 1.3.22, $p\,|\,b$.

תרגיל 1.4.7 **(+*)** הראה ש־ $p\in\mathbb{Z}$ ראשוני אם ורק אם אין לו אף מחלק לא טריוויאלי.

תרגיל 1.4.8 **(**)** כל מספר טבעי אפשר להציג כמכפלה של גורמים ראשוניים. **הדרכה.** אינדוקציה שלמה.

משפט 1.4.9 ***הפירוק של מספר טבעי לגורמים ראשוניים הוא יחיד עד־כדי סדר.***

תרגיל 1.4.10 **(־***)** הוכח את המשפט.

תרגיל 1.4.11 **(+**)** תן קריטריון לכך ש־$n=p_1^{a_1}\cdots p_t^{a_t}$ יחלק את $n'=p_1^{a_1'}\cdots p_t^{a_t'}$ (כאשר $a_i,a_i'\geq 0$), ונוסחה למחלק המשותף המקסימלי.

תרגיל 1.4.12 **(*)** מצא את הפירוק לראשוניים של המספרים 5720, 12960, 8888 ו־ 4096.

משפט 1.4.13 **(אוקלידס)** ***יש אינסוף מספרים ראשוניים.***

תרגיל 1.4.14 **(+**)** הוכח את המשפט. **הדרכה.** נניח שהראשוניים היחידים הם $p_1,\dots,p_n$. התבונן ב־ $N=p_1\cdots p_n+1$.

תרגיל 1.4.15 **(**)** הוכח שיש אינסוף ראשוניים מהצורה $4n+1$.

תרגיל 1.4.16 **(***)** הוכח שיש אינסוף ראשוניים מהצורה $4n-1$.

תרגיל 1.4.17 **(**)** הוכח שיש אינסוף ראשוניים מהצורה $6n-1$.

תרגיל 1.4.18 **(***)** מצאו את כל הזוגות של ראשוניים p,q כך ש־ $2+p+q\,|\,6pq$.

1.5 שקילות מודולו n

יהי $0\neq n\in\mathbb{Z}$ קבוע. נגדיר יחס על המספרים השלמים:

הגדרה 1.5.1 ***a שקול ל־ b מודולו n*** (***כותבים:*** $a\equiv b \pmod n$) ***אם*** $n|(a-b)$.

תרגיל 1.5.2 **(*)** הוכח ששקילות מודולו n היא יחס שקילות (כלומר, טרנזיטיבית, סימטרית ורפלקסיבית).

*שקילות מודולו n היא יחס. בשפות מחשב שונות מגדירים **פעולה** של חילוק עם שארית שאותה מסמנים ב־mod, כפי שנראה, הטיפול במחלקות שקילות גמיש ונוח יותר מאשר בשאריות*

טענה 1.5.3 אם $a \equiv a' \pmod{n}$ ו־$b \equiv b' \pmod{n}$, אז $a+b \equiv a'+b' \pmod{n}$ ו־$ab \equiv a'b' \pmod{n}$.

תרגיל 1.5.4 (+**) הוכח את הטענה.

פירושו של דבר הוא שפעולות החיבור והכפל של מחלקות שקילות מודולו n, המבוצעות על נציגים, מוגדרות היטב. עובדה זו תהיה לנו לעזר רב בהמשך.

תרגיל 1.5.5 (-***) הוכח שלכל $a > 1$ ולכל n, m, $(a^n-1, \frac{a^{nm}-1}{a^n-1})$ מחלק את m. הסק ש־ $a^n-1, \frac{a^{n \cdot a}-1}{a^n-1}$ זרים. **הדרכה.** $a^n \equiv 1 \pmod{a^n-1}$.

1.5.1 משפט השאריות הסיני

משפט 1.5.6 (משפט השאריות הסיני) *יהיו n, m זרים. לכל a, b, קיים x יחיד מודולו nm כך ש־ $x \equiv a \pmod{n}$ ו־$x \equiv b \pmod{m}$.*

תרגיל 1.5.7 (+**) הוכח את המשפט. **הדרכה.** נניח ש־ $\alpha n + \beta m = 1$. הראה ש־ $x = \alpha nb + \beta ma$ פתרון. את היחידות הוכח לפי ספירה.

תרגיל 1.5.8 (+**) הוכח את הגרסה הבאה של המשפט: אם $n_1, \dots, n_t$ זרים בזוגות, אז לכל $a_1, \dots, a_t$ קיים x יחיד מודולו $n = n_1 \cdots n_t$ המקיים $x \equiv a_i \pmod{n_i}$.

תרגיל 1.5.9 (**) פתור את מערכות המשוואות $\left\{\begin{array}{c} x \equiv 4 \pmod{8} \\ x \equiv 5 \pmod{15} \end{array}\right\}$.

תרגיל 1.5.10 (**) פתור את מערכות המשוואות $\left\{\begin{array}{c} x \equiv 1 \pmod{5} \\ x \equiv -1 \pmod{6} \\ x \equiv 2 \pmod{7} \end{array}\right\}$.

תרגיל 1.5.11 (**) הראה שלמערכת $\left\{\begin{array}{c} x \equiv 5 \pmod{12} \\ x \equiv 6 \pmod{8} \end{array}\right\}$ אין פתרונות. הראה שלמערכת $\left\{\begin{array}{c} x \equiv 4 \pmod{12} \\ x \equiv 6 \pmod{8} \end{array}\right\}$ יש יותר מאחד (מודולו $8 \cdot 12$). מדוע אין זו סתירה למשפט?

תרגיל 1.5.12 (-***) n, m שלמים. מצא תנאי הכרחי ומספיק על a, b לכך שלמערכת $\left\{\begin{array}{c} x \equiv a \pmod{n} \\ x \equiv b \pmod{m} \end{array}\right\}$ יהיה פתרון יחיד מודולו $[n, m]$.

פרק 2

חבורות למחצה ומונוידים

בפרק הקצר הזה נכיר את המערכות האלגבריות הפרימיטיביות ביותר - אלו שיש להן רק פעולה אחת עם מספר אקסיומות מינימלי. המטרה העיקרית היא להתרגל לרעיון של פעולה אבסטרקטית, שרק בגללו יש צורך לפתח מבנים אלגבריים כלליים.

מושגים: פעולה אסוציאטיבית, חבורה למחצה, איבר יחידה, איבר אפס; מונויד, איבר הפיך.

2.1 חבורות למחצה

פעולה בינרית על קבוצה A היא פונקציה $*: A \times A \to A$. *שימו לב שלפי ההגדרה, הפעולה "מוגדרת היטב", כלומר, לכל שני איברים $x, y \in A$ יש ערך יחיד $x * y$, ו"סגורה" - הערך הזה שייך ל־A.*

פעולה $*$ היא אסוציאטיבית אם $a * (b * c) = (a * b) * c$.

הגדרה 2.1.1 *חבורה למחצה היא מערכת מתמטית הכוללת קבוצה עם פעולה אסוציאטיבית עליה.*

תרגיל 2.1.2 (־*)** הראה שאם הפעולה אסוציאטיבית, אז החזקה מוגדרת היטב (כלומר, כל הדרכים להכפיל איבר x בעצמו n פעמים מביאות לאותה תוצאה).

תרגיל 2.1.3 (*) קבוצת המספרים הזוגיים עם פעולת הכפל, היא חבורה למחצה.

תרגיל 2.1.4 (*) תהי S קבוצה. נגדיר $a * b = b$. הוכח ש־ $(S, *)$ חבורה למחצה.

הסיבה לכך שאסוציאטיביות היא תכונה חשובה ונפוצה כל־כך, היא שהרכבת פונקציות היא אסוציאטיבית.

תרגיל 2.1.5 (*) תהי X קבוצה. האוסף X^X של פונקציות $X \to X$, עם פעולת ההרכבה של פונקציות, הוא חבורה למחצה.

תרגיל 2.1.6 (**) קבע האם קבוצת המספרים הממשיים $\mathbb{R}$, עם הפעולה $a * b = \frac{1}{2}(a^2 + b^2)$, היא חבורה למחצה.

תרגיל 2.1.7 **(**)** נניח שבחבורה למחצה A אפשר לקרוא את הגורמים מתוך המכפלה, כלומר, אם $ab = cd$ אז $a = c$ ו־$b = d$. הוכח ש־ $|A| = 1$.

הגדרה 2.1.8 ***איזומורפיזם של חבורות למחצה $(X,*), (Y,\star)$ הוא פונקציה חד־חד־ערכית ועל $f : X \to Y$, כך ש־ $f(x*x') = f(x)\star f(x')$. אם קיים איזומורפיזם בין החבורות למחצה, אומרים שהן איזומורפיות, ומסמנים $X \cong Y$.***

תרגיל 2.1.9 **(**)** איזומורפיות היא תכונה טרנזיטיבית, סימטרית ורפלקסיבית. *מנקודת המבט של תורת הקבוצות האקסיומטית יש כאן אי־דיוק מסויים, אבל אפשר לומר שאיזומורפיות היא יחס שקילות.*

תרגיל 2.1.10 **(**)** יש בדיוק חמש חבורות למחצה בנות 2 אברים עד־כדי איזומורפיזם. כלומר, יש חמש חבורות למחצה בנות 2 אברים, שאינן איזומורפיות זו לזו, וכל חבורה למחצה בת שני אברים איזומורפית לאחת מהן.

הגדרה 2.1.11 ***איבר e בחבורה למחצה S הוא* איבר יחידה *אם לכל $x \in S$, $xe = xe = x$.***

תרגיל 2.1.12 **(*)** אם יש בחבורה למחצה איבר יחידה, אז הוא יחיד.

תרגיל 2.1.13 **(**)** הראה ש־ $M = \left\{ \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} : a, b \in \mathbb{R} \right\}$ היא חבורה למחצה. האם יש לה איבר יחידה?

הגדרה 2.1.14 ***אם איבר z בחבורה למחצה מקיים $za = az = z$ לכל a, הוא נקרא* איבר אפס.**

תרגיל 2.1.15 **(*)** הראה שאם קיים בחבורה למחצה איבר אפס, אז הוא יחיד.

תרגיל 2.1.16 **(**)** תן דוגמא לחבורה למחצה עם איבר אפס, ולחבורה למחצה ללא איבר אפס.

2.2 מונוידים

הגדרה 2.2.1 ***חבורה למחצה עם איבר יחידה נקראת* מונויד.**

תרגיל 2.2.2 **(**)** תהי A קבוצה. הוכח ש־ $M = A^A = \{f : A \to A\}$ עם פעולת ההרכבה הוא מונויד.

תרגיל 2.2.3 **(*)** מצא אלו מן המערכות הבאות הן מונוידים:
$\mathbb{Z}$ עם פעולת החיסור.
$\mathbb{R}^+ = \{x : x > 0\}$ עם פעולת הכפל.
$\mathrm{M}_2(\mathbb{R})$ עם פעולת הכפל של מטריצות.

תרגיל 2.2.4 **(*)** קבע לגבי כל אחת מהמערכות הבאות האם היא חבורה למחצה והאם היא מונויד.
אוסף המטריצות $\mathrm{M}_n(F)$ עם פעולת הכפל.
אוסף הפונקציות הרציפות $[0,1] \to \mathbb{R}$, עם כפל $(f * g)(t) = f(t) \cdot g(t)$.
אוסף המספרים הרציונליים עם הכפל הרגיל.

תרגיל 2.2.5 (**) אם אחת מבין שתי חבורות למחצה איזומורפיות היא מונויד, אז גם השניה כך.

תרגיל 2.2.6 (**) כתוב את לוחות הכפל של כל המונוידים בעלי 2 אברים.

תרגיל 2.2.7 (***) כתוב את לוחות הכפל של שבעה המונוידים בעלי 3 אברים.

תרגיל 2.2.8 (**) השלם את לוח הכפל של מונויד $M = \{e, a, b, c\}$ שבו e איבר יחידה, $ab = c$, $bc = a$ ו־$ca = b$.

תרגיל 2.2.9 (**) הראה שכל חבורה למחצה S אפשר להרחיב למונויד $S' = S \cup \{e\}$, אם נגדיר את e להיות איבר היחידה במבנה החדש.

תרגיל 2.2.10 (**) תאר את המונויד המתקבל לאחר חזרה n פעמים על הבניה של תרגיל 2.2.9, כשמתחילים ממונויד האפס $M = \{0\}$.

תרגיל 2.2.11 (**) א. M מונויד. נקבע $z \in M$, ונרחיב את הפעולה לפי $zm = mz = z$. הוכח ש־ $M \cup \{z\}$ מונויד, שבו z הוא איבר האפס.
ב. נניח ש־ $M = \{0\}$. תאר את המונויד המתקבל אחרי n הפעולות של התהליך הזה.

הגדרה 2.2.12 *יהי M מונויד עם איבר היחידה 1. איבר $a \in M$ הוא **הפיך** אם קיים $b \in M$ כך ש־ $ab = ba = 1$.*

תרגיל 2.2.13 (**) אם a הפיך, אז האיבר b שמספקת ההגדרה הוא יחיד.

לכן, אם a הפיך, מוצדק לקרוא לאיבר b המקיים $ab = ba = 1$ **ההפכי** של a, בהא הידיעה, ולסמן אותו בסימון a^{-1}.

תרגיל 2.2.14 (*) אם a הפיך, אז גם a^{-1} הפיך, ו־$(a^{-1})^{-1} = a$.

תרגיל 2.2.15 (**) אם a, b הפיכים, אז גם ab הפיך, ו־$(ab)^{-1} = b^{-1}a^{-1}$.

הגדרה 2.2.16 *את אוסף האיברים ההפיכים במונויד M מסמנים ב־$U(M)$.*

טענה 2.2.17 לכל מונויד M, $U(M)$ הוא חבורה.

תרגיל 2.2.18 (**) הוכח את הטענה. כתוב בזהירות מה בדיוק צריך להוכיח; למשל, מדוע פעולת הכפל ב־$U(M)$ מוגדרת היטב?

תרגיל 2.2.19 (***) תן דוגמא למונויד עם איברים a, b כך ש־ $ab = 1$ אבל a ו־b אינם הפיכים. **הדרכה**. חשוב על $X = \mathbb{N}^{\mathbb{N}}$.

תרגיל 2.2.20 (**) אם במונויד מתקיים $aba = a$ ו־$ab^2a = 1$, אז $a = b^{-1}$.

תרגיל 2.2.21 (**) יהי $(M, \bullet)$ מונויד, ויהי $a \in M$. נגדיר $x * y = x \bullet a \bullet y$. הוכח ש־ $(M, *)$ חבורה למחצה. מצא תנאי הכרחי ומספיק לכך ש־ $(M, *)$ מונויד.

תרגיל 2.2.22 (***) יהי $\lambda < -1/4$ מספר ממשי. נגדיר $x \circ y = \frac{xy+\lambda}{x+y-1}$.

1. הוכח שהקטע $I = (-\frac{1}{2}, \infty)$ הוא חבורה למחצה ביחס לפעולה $\circ$.
2. נניח ש־ $\lambda = e^2 + e$ עבור $e \in I$ (בדוק ש־ e יחיד). הוכח ש־ e איבר אפס של הפעולה.
3. נרחיב את הפעולה $\circ$ לקטע $[-\frac{1}{2}, \infty]$ על־ידי מעבר לגבול: $(-\frac{1}{2}) \circ a = \lim_{x\to(-\frac{1}{2})^+} x \circ a$ וכן $\infty \circ a = \lim_{x\to\infty} x \circ a$. בדוק ש־ $(-\frac{1}{2}) \circ (-\frac{1}{2}) = \infty$, וש־ ∞ הוא איבר יחידה בקטע החדש.
4. נסמן $a^* = (-\frac{1}{2}) \circ a$. בדוק ש־ $a^{**} = a$ וש־ $a^* \circ b^* = a \circ b$.
5. הראה ש־ e תמיד בין a ל־ a^*.
6. הוכח שלמשוואה $a \circ x = b$ קיים פתרון אם ורק אם b בין a ל־ a^*.
7. מצא את כל תת־הקבוצות הקשירות של $[-\frac{1}{2}, \infty]$, הסגורות ביחס לפעולה.
8. הוכח שלכל $a \in I$, $\lim_{n\to\infty} a^n = e$. [רמז. פרק לגורמים את $a \circ b - e$.]

תרגיל 2.2.23 (־*)** 1. פעולת האקספוננט $x \mapsto e^x$ היא איזומורפיזם של המונויד $(\mathbb{R}, +, 0)$ אל המונויד $(\mathbb{R}^+, \cdot, 1)$.

2. נגדיר פעולות $\oplus_n$ (עבור $n \in \mathbb{Z}$) הקשורות ביניהן באמצעות היחס $e^{a \oplus_n b} = e^a \oplus_{n+1} e^b$. נניח שהפעולה הראשונה בסדרה, $\oplus_1$, היא פעולת החיבור. הראה שהפעולה השנייה היא הכפל $x \oplus_2 y = xy$.
3. הראה ש־$x \oplus_3 y = x^{\log(y)} = y^{\log(x)}$, ו־$x \oplus_4 y = e^{e^{\log\log(x)\log\log(y)}}$.
4. הראה ש־$a \oplus_0 b = \log(e^a + e^b)$ ו־$a \oplus_{-1} b = \log(\log(e^{e^a} + e^{e^b}))$.
5. מהי הקרן הגדולה ביותר $[c, \infty)$ שבה מוגדרת הפעולה $\oplus_n$?
6. חשב את הגבול $\lim_{n\to-\infty}(a \oplus_n b)$.
7. מצא מה צריך להיות הערך של e (עד כאן הנחנו רק ש־$e > 1$), כך ש־$2 \oplus_2 2 = 4$. חשב עבור בחירה זו את $2 \oplus_n 2$ לכל n.

פרק 3

חבורות ותת־חבורות

כאן נפגוש את גיבורת החלק הראשון של הקורס, החבורה, ונכיר כמה דוגמאות חשובות.

מושגים: מונויד עם צמצום, חבורה. איזומורפיזם. סדר של חבורה. $\mathbb{Z}_n$. חבורות אוילר. החבורות הסימטריות. החבורות הדיהדרליות. החבורה הליניארית הכללית. חבורה אבלית. מכפלה ישרה חיצונית. תת־חבורה.

3.1 חבורות

הגדרה 3.1.1 ***חבורה*** *היא מונויד שבו כל האיברים הפיכים. במלים אחרות, חבורה היא מערכת מתמטית הכוללת קבוצה G, פעולה אסוציאטיבית $*: G\times G \to G$ ואיבר יחידה $1 \in G$, כך שכל האיברים של G הפיכים.*

הסימן 1 עשוי להטעות, משום שבמקרים רבים אברי החבורה כלל אינם מספרים, או שדווקא המספר 0 הוא איבר היחידה (אכן, יש ספרים המעדיפים לסמן את איבר היחידה באות e). כדי למנוע בלבול, אם מעורבות בבעיה כמה חבורות, אנו עשויים לסמן את איבר היחידה של G בסימון 1_G.

כל קבוצה עם איבר אחד (ופעולת הכפל ההכרחית) היא חבורה. כל החבורות האלה איזומורפיות, ונקראות **החבורה הטריוויאלית**. לפעמים, במקום לסמן חבורה זו ב־$G = \{1\}$, נכתוב פשוט $G = 1$.

תרגיל 3.1.2 (*) אם G חבורה אז $U(G) = G$.

הגדרה 3.1.3 *למונויד יש תכונת הצמצום משמאל אם $ab = ac$ גורר $b = c$. באופן דומה מוגדר גם צמצום מימין.*

תרגיל 3.1.4 (*) בדוק שבמונויד יש צמצום מימין ומשמאל אם ורק אם לוח הכפל שלו הוא ריבוע לטיני.

משפט 3.1.5 *מונויד סופי עם צמצום משמאל הוא חבורה.*

תרגיל 3.1.6 **(***)** הוכח את המשפט.

תרגיל 3.1.7 **(-***)** תן דוגמא למונויד (אינסופי) עם צמצום משמאל שאינו חבורה.

תרגיל 3.1.8 **(**)** S חבורה למחצה סופית, ו־$Sa = aS = S$ לכל $a \in S$. הוכח ש־ S מונויד.

תרגיל 3.1.9 **(***)** אם בחבורה למחצה יש פתרון לכל משוואה מן הצורה $ax = b$ או $xa = b$, אז זו חבורה.

תרגיל 3.1.10 **(**)** תן דוגמא למונויד ציקלי סופי (כלומר, מונויד שיש לו איבר $a \in M$ כך ש־$M = \{a^n : n \in \mathbb{N}\}$), שאינו חבורה.

תרגיל 3.1.11 **(**)** אם X, Y חבורות ו־$f : X \to Y$ איזומורפיזם של חבורות למחצה, אז הוא מעביר את איבר היחידה של X לאיבר היחידה של Y, ואת ההפכי של איבר להפכי של התמונה שלו.

הגדרה 3.1.12 ***אם יש איזומורפיזם בין חבורות, אומרים שהן איזומורפיות*** (בדיוק כמו במקרה של חבורות למחצה או מונוידים).

תרגיל 3.1.13 **(+*)** הראה שבחבורה בת יותר מאיבר אחד, (יש איבר יחידה אבל) אין איבר אפס (ראה הגדרה 2.1.14).

תרגיל 3.1.14 **(**)** תהי G חבורה עם $a, b \in G$. הוכח: למשוואה $xax = b$ יש פתרון אם ורק אם ab הוא ריבוע (כלומר, מהצורה y^2) ב־ G.

תרגיל 3.1.15 **(-***)** תהי G חבורה עם $a \in G$. הוכח: למשוואה $x^2ax = a^{-1}$ יש פתרון אם ורק אם a הוא חזקה שלישית ב־ G.

תרגיל 3.1.16 **(+**)** אברים a, b בחבורה מקיימים $a^2 = 1, ab^2a^{-1} = b^3$. הוכח ש־ $b^5 = 1$.

תרגיל 3.1.17 **(**)** קבע האם הקבוצה $\{x \in \mathbb{R} :\ \tan(x) \in \mathbb{Q}\}$ היא חבורה ביחס לפעולת החיבור.

תרגיל 3.1.18 **(**)** הוכח שהמערכות הבאות הן חבורות:

א. $\left\{ \begin{pmatrix} x & y \\ -y & x \end{pmatrix} : x, y \in \mathbb{R}, x^2 + y^2 > 0 \right\}$, עם כפל המטריצות הרגיל.

ב. $\mathbb{R}^* = \mathbb{R} \cup \{\infty\}$ עם הפעולה $a * b = \frac{a+b}{1-ab}$ אם $a, b \neq \infty$ ו־$ab \neq 1$; $a * \frac{1}{a} = \infty$; $a * \infty = -\frac{1}{a}$; $\infty * \infty = 0$.

תרגיל 3.1.19 **(**)** נתבונן בפונקציות הממשיות $f_a : x \mapsto \frac{x}{\sqrt{1+ax^2}}$. הוכח ש־ $\{f_a : a \in \mathbb{R}\}$ היא חבורה ביחס להרכבת פונקציות.

תרגיל 3.1.20 **(-***)** תן דוגמא לקבוצה סופית עם פעולה בינארית לא אסוציאטיבית, עם איבר יחידה וצמצום מימין ומשמאל, שיש בה איברים לא הפיכים. **הצעה.** קח $M = \{1, \epsilon, a_0, a_1, a_2\}$ עם פעולת הכפל $\epsilon * a_i = a_{i+1}$, $a_i * \epsilon = a_{i-1}$, $a_i * a_i = \epsilon$, $a_i * a_{i+1} = 1$, $a_i * a_{i-1} = a_{i+1}$.

3.2 סדר של חבורה

הגדרה 3.2.1 ***הסדר*** *של חבורה הוא מספר האיברים בחבורה.*

פריט המידע החשוב ביותר על חבורה סופית הוא הסדר שלה. בהמשך נראה שאפשר ללמוד הרבה על חבורה מידיעת הסדר שלה לבדו, אם כי בדרך־כלל יש כמה חבורות לא איזומורפיות מאותו סדר.

תרגיל 3.2.2 (**) כתוב את לוחות הכפל של כל החבורות מסדר $2, 3, 4$.

תרגיל 3.2.3 (**) העזר בכלל הצמצום כדי להראות שיש חבורה אחת מסדר 5, עד כדי איזומורפיזם.

אומרים שאיברים $a, b \in G$ בחבורה הם **מתחלפים** אם $ab = ba$.

תרגיל 3.2.4 (**) כתוב את לוח הכפל של חבורה מסדר 6, עם איברים τ, σ שאינם מתחלפים, המקיימים $1 = \sigma^3 = \tau^2$. **הדרכה**. אברי החבורה הם $1, \sigma, \sigma^2, \tau, \sigma\tau, \sigma^2\tau$: הוכח שכל אלה שונים זה מזה, ומצא את $\tau\sigma$ בהנחה שהוא איבר באותה רשימה.

תרגיל 3.2.5 (*) לחבורות איזומורפיות יש אותו סדר (וראה תרגיל 3.3.18).

3.3 דוגמאות לחבורות

איך מתארים חבורה? בשלב זה, הדרך היחידה שאנו מכירים לתאר חבורה היא באמצעות לוח הכפל שלה. כמובן שזו דרך לא יעילה. כתחליף, נוכל להסתפק בתאור נוסחאתי (כלומר, נוסחת כפל במקום לוח כפל), אלא שלעתים מהצגה כזו קשה ללמוד באיזו חבורה מדובר. בסעיף הזה נכיר כמה דוגמאות, כדי שנוכל לקרוא לחבורות הנפוצות ביותר בשמן, ואחר־כך נלמד להרכיב חבורות חדשות מאלו שאנו מכירים.

3.3.1 החבורות הציקליות $\mathbb{Z}$ ו־$\mathbb{Z}_n$:

החבורה האינסופית הפשוטה ביותר היא $(\mathbb{Z}, +, 0)$. אם 'מקפלים' את החבורה הזו למחלקות שקילות, מקבלים חבורה אחת מכל סדר. נקבע $n \geq 1$.

תרגיל 3.3.1 (*) הראה שיש בדיוק n מחלקות שקילות מודולו n. **הדרכה**. הראה שכל מספר שקול לאחד מבין $0, 1, \dots, n-1$, ושאלה אינם שקולים זה לזה.

תרגיל 3.3.2 (**) הזכר בטענה 1.5.3, והראה שפעולת החיבור $[a] + [b] = [a + b]$ מוגדרת היטב.

כשמגדירים העתקה מקבוצה לקבוצה (ופעולה בינרית בכלל זה), עולה לפעמים צורך להוכיח שהפעולה מוגדרת היטב. ישנן שני מצבים שכיחים. בראשון, אם $f : A \to B$, מגדירים את $f(\alpha)$ באופן מסויים, וצריך לוודא

אכן $f(\alpha) \in B$. המקרה השני הוא כאשר A אוסף של מחלקות שקילות, ובהגדרת $f(\alpha)$ מבצעים בחירה (בדרך כלל של נציג מהמחלקה α). לדוגמא, בפעולת החיבור כתבנו "$[x] + [y] = [x + y]$", במקום "יהיו α, β מחלקות; נבחר נציגים x, y כך ש־ $\alpha = [x]$, $\beta = [y]$; נגדיר $\alpha + \beta = [x + y]$". צריך לוודא שבחירת נציגים x', y' עם אותן תכונות תביא לאותה תוצאה.

תרגיל 3.3.3 (**) הראה שאוסף המחלקות $[0], \ldots, [n-1]$ הוא חבורה ביחס לחיבור:

1. הראה שהפעולה אסוציאטיבית.
2. הראה שיש איבר יחידה (מהו?).
3. הראה שלכל איבר קיים הפכי. מהו איבר היחידה? מהו ההפכי של $[a]$?

הגדרה 3.3.4 ***החבורה של מחלקות השקילות מודולו n, ביחס לפעולת החיבור, נקראת $\mathbb{Z}_n$ (וגם $\mathbb{Z}/n\mathbb{Z}$, מסיבות שיובררו בסעיף 5.4).***

שני הסימונים, $\mathbb{Z}_n$ וגם $\mathbb{Z}/n\mathbb{Z}$, עשויים להתייחס לשלושה עצמים שונים: קבוצת מחלקות השקילות מודולו n, המערכת המתמטית הכוללת את הקבוצה הזו עם פעולת החיבור (זו חבורה); והמערכת המתמטית הכוללת את הקבוצה עם פעולות החיבור והכפל ("חוג").

תרגיל 3.3.5 (*) אם $n \neq m$ אז החבורות $\mathbb{Z}_n, \mathbb{Z}_m$ אינן איזומורפיות.

3.3.2 חבורות אוילר U_n:

כמקודם, נקבע $n \geq 1$.

תרגיל 3.3.6 (**) הזכר בטענה 1.5.3, והראה שפעולת הכפל $[a] \cdot [b] = [a \cdot b]$ מוגדרת היטב.

תרגיל 3.3.7 (**) הראה שאוסף מחלקות השקילות $\mathbb{Z}_n$, עם פעולת ה**כפל**, הוא מונויד, אבל אינו חבורה אלא במקרה הטריוויאלי $n = 1$.

תרגיל 3.3.8 (*) המחלק המשותף המקסימלי תלוי רק במחלקת השקילות מודולו n. במלים אחרות, אם $a \equiv a' \pmod{n}$ אז $(a, n) = (a', n)$.

תרגיל 3.3.9 (-*)** איבר $[a] \in \mathbb{Z}_n$ הוא הפיך ביחס לכפל אם ורק אם $(a, n) = 1$.

תרגיל 3.3.10 (***) אם $(a, n) = (b, n) = 1$, אז $(ab, n) = 1$.

הגדרה 3.3.11 **חבורת אוילר מסדר n**, ***U_n, היא אוסף מחלקות השקילות מודולו n, של מספרים הזרים ל־n, עם פעולת הכפל.***

החבורות נקראות על־שם לאונרד אוילר, 1707–1783.

תרגיל 3.3.12 (***) הראה שההפכי של $a \in U_n$ הוא מספר α המקיים $\alpha a + \beta n = 1$ לאיזשהו β.

תרגיל 3.3.13 (**) הראה ש־U_n היא חבורה:

1. הראה שהפעולה אסוציאטיבית.
2. הראה שיש איבר יחידה (מהו?).
3. הראה שלכל איבר קיים הפכי. מהו ההפכי של $[a]$? **הדרכה**. ראה תרגיל 3.3.12.

תרגיל 3.3.14 (**) הראה ש־ $U_n = U(\mathbb{Z}_n, \cdot)$ (ראה הגדרה 2.2.16).

למרות ש־U_n נקראת 'חבורת אוילר מסדר n', מספר האיברים בחבורה הזו אינו n אלא

$$\varphi(n) = |\{1 \leq a \leq n : (a,n) = 1\}|;$$

הפונקציה φ נקראת **פונקציית אוילר**.

תרגיל 3.3.15 (*) חשב את $\varphi(n)$ עבור $n = 1, 2, \ldots, 12$.

תרגיל 3.3.16 (*) כתוב את לוח הכפל של החבורות U_n, עבור $n = 2, 3, 4, 5, 6$, $7, 8, 9, 10, 12$.

תרגיל 3.3.17 (**) הוכח:

1. $U_6 \cong U_4 \cong U_3 \cong \mathbb{Z}_2$,
2. $U_{10} \cong U_5 \cong \mathbb{Z}_4$,
3. $U_9 \cong U_7 \cong \mathbb{Z}_6$.

תרגיל 3.3.18 (**) U_5 ו־U_8 מאותו סדר אבל אינן איזומורפיות.

3.3.3 החבורות הסימטריות S_n

הגדרה 3.3.19 *פונקציה חד־חד־ערכית ועל מקבוצה לעצמה, $\sigma : X \to X$, נקראת* ***תמורה***.

הגדרה 3.3.20 *את אוסף כל התמורות $\sigma : X \to X$ נסמן S_X. לשם הקיצור, עבור הקבוצה $X = \{1, \ldots, n\}$ מסמנים $S_X = S_n$. אנו מכפילים תמורות מימין לשמאל, כמו הרכבת פונקציות: $(\sigma\tau)(a) = \sigma(\tau(a))$.*

תמורה ב־S_n היא פונקציה מהקבוצה $\{1, \ldots, n\}$ אל עצמה. צורת רישום אפשרית אחת היא לתאר את σ במטריצה של שתי שורות, $\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix}$.

תרגיל 3.3.21 (*) חשב את המכפלות הבאות:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 4 & 5 & 2 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 2 & 5 & 3 & 1 \end{pmatrix},$$

$$\begin{pmatrix} 1 & 2 & \cdots & n-1 & n \\ 2 & 3 & \cdots & n & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & \cdots & m & m+1 & \cdots & n \\ 2 & 3 & \cdots & 1 & m+1 & \cdots & n \end{pmatrix} \begin{pmatrix} 1 & 2 & \cdots & n-1 & n \\ 2 & 3 & \cdots & n & 1 \end{pmatrix}.$$

תרגיל 3.3.22 (+**) הוכח שאם $|X| = |Y|$ אז $S_X \cong S_Y$.

תרגיל 3.3.23 (*) S_X, עם פעולת הרכבת הפונקציות, היא חבורה.

תרגיל 3.3.24 (*) הוכח ש־ $|S_n| = n!$.

תרגיל 3.3.25 (**) כתוב את לוח הכפל של S_1, S_2 ו־S_3 (השווה את לוח הכפל האחרון לזה של תרגיל 3.2.4). בדוק ש־$S_2 \cong \mathbb{Z}_2$.

הגדרה 3.3.26 *אם* $1 \leq r_1, \dots, r_t \leq n$ *שונים זה מזה, תמורה* σ *המעבירה* $r_1 \mapsto r_2 \mapsto \cdots \mapsto r_t \mapsto r_1$ *(וקובעת את שאר האברים) נקראת* ***מחזור****. ומסמנים* $\sigma = (r_1\, r_2\, \cdots\, r_t)$*.* ***הסדר*** *של המחזור הוא האורך שלו,* $o(\sigma) = t$*.*

הקבוצה $\{r_1, \dots, r_t\}$ נקראת **התומך** של המחזור; **מחזורים זרים** הם מחזורים שהתומכים שלהם זרים.

תרגיל 3.3.27 (**) מחזורים זרים - מתחלפים.

משפט 3.3.28 *כל תמורה ב־S_n אפשר לכתוב כמכפלה של מחזורים זרים.*

תרגיל 3.3.29 (*) הצג את כל האברים ב־ S_3 במכפלות של מחזורים.

תרגיל 3.3.30 (*) כתוב כמכפלת מחזורים את התמורות הבאות:
$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 4 & 7 & 1 & 3 & 2 & 5 & 6 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 5 & 3 & 9 & 10 & 1 & 6 & 8 & 7 & 2 & 4 \end{pmatrix}.$$

תרגיל 3.3.31 (*) חשב את המכפלות $(6\,1\,3\,4)(3\,2\,4)(1\,2\,4\,7)$, $(1\,2)(1\,3)\cdots(1\,n)$.

תרגיל 3.3.32 (*) כתוב בצורה המלאה וכמכפלה של מחזורים זרים, את התמורות הבאות: $\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 6 & 4 & 3 & 1 & 5 \end{pmatrix}$, $\beta = (143)(25)(6)$, $\gamma = (12)(14)(23)(42)(14)$, $\delta = \alpha\beta\gamma$.

תרגיל 3.3.33 (**) הראה שאם τ_1, τ_2 מחזורים זרים, $\alpha \neq \tau_1(\alpha)$ ו־$\beta \neq \tau_2(\beta)$, אז $(\alpha\beta) \cdot \tau_1 \cdot \tau_2$ מחזור באורך $o(\tau_1) + o(\tau_2)$.

3.3.4 החבורות הדיהדרליות D_n

יהי $n \geq 2$. החבורה הסימטרית S_n היא אוסף כל הדרכים לערבב את העצמים $1, \dots, n$. אם נטיל מגבלות על סוגי הערבוב המותרים, נקבל חבורות קטנות יותר. למשל, החבורה D_n מוגדרת כאוסף הדרכים לפעול על מצולע בן n צלעות, כך שיתפוס בסוף הפעולה את אותו המקום במרחב. יש שתי פעולות יסודיות: סיבוב ימינה ב־$\frac{1}{n}$ המעגל (שנסמן באות σ), ושיקוף בציר קבוע כלשהו העובר דרך מרכז המצולע ואחד הקודקודים (שנסמן באות τ).

תרגיל 3.3.34 (**) בדוק שהפעולות מקיימות את היחסים $\sigma^n = 1$, $\tau^2 = 1$, ו־$\tau\sigma\tau^{-1} = \sigma^{-1}$.

תרגיל 3.3.35 (**) הראה שיש בדיוק $2n$ דרכים למקם מצולע משוכלל בן n צלעות, כך שיתפוס מקום מוגדר מראש.

תרגיל 3.3.36 (**) הראה שהפעולות $\sigma^i\tau^j$, $i=0,\dots,n-1$, $j=0,1$, שונות זו מזו.

הגדרה 3.3.37 ***החבורה הדיהדרלית מסדר*** n, D_n, ***היא הקבוצה***

$$\{\sigma^i\tau^j : i=0,\dots,n-1, j=0,1\},$$

עם הפעולה $\sigma^i\tau^j \cdot \sigma^{i'}\tau^{j'} = \sigma^{i+(-1)^j i' (\bmod n)}\tau^{j+j' (\bmod 2)}$.

תרגיל 3.3.38 (**) בדוק שהפעולה אסוציאטיבית. הראה ש־ $\sigma^0\tau^0$ הוא איבר היחידה, וש־ $(\sigma^i\tau^j)^{-1} = \sigma^{-(-1)^j i}\tau^j$. הסק ש־ D_n היא חבורה מסדר $2n$.

תרגיל 3.3.39 (**) הוכח ש־ $D_3 \cong S_3$.

תרגיל 3.3.40 (**) הוכח: $\mathrm{Z}(D_n) = \langle \sigma^{n/2} \rangle$ אם n זוגי, ו־ $\mathrm{Z}(D_n)=1$ אחרת.

תרגיל 3.3.41 (***) כל תת־החבורות של החבורה הדיהדרלית D_n הן מן הטיפוסים הבאים: $\mathbb{Z}_2\times\mathbb{Z}_2$, ציקליות מסדר m או דיהדרליות מסדר m, כאשר $m|n$.

3.3.5 חבורות המטריצות הקלאסיות

יהי F שדה (למשל, $F=\mathbb{Q},\mathbb{R},\mathbb{C}$, אבל גם $\mathbb{Z}_p$ כאשר p ראשוני (ראה תרגיל 4.4.2)).

תרגיל 3.3.42 (+*) הראה שאוסף המטריצות $\mathrm{M}_n(F)$, ביחס לפעולת הכפל, הוא מונויד שיש לו איבר אפס.

הגדרה 3.3.43 $\mathrm{GL}_n(F) = \{A\in \mathrm{M}_n(F) : \det(A)\neq 0\}$.

תרגיל 3.3.44 (+*) $\mathrm{GL}_n(F) = U(\mathrm{M}_n(F))$.

תרגיל 3.3.45 (+**) רשום את אברי החבורה $\mathrm{GL}_2(\mathbb{Z}_2)$. הוכח ש־ $\mathrm{GL}_2(\mathbb{Z}_2)\cong S_3$.

3.4 אבליות

הגדרה 3.4.1 *אברים* x,y *בחבורה* ***מתחלפים*** ***אם*** $xy=yx$. ***אם כל שני אברים בחבורה מתחלפים, אומרים שהיא*** ***אבלית***.

בחבורה אבלית פעולת הכפל היא קומוטטיבית, ולפעמים קוראים לחבורה כזו גם 'חבורה קומוטטיבית'. קוראים להן חבורות אבליות על־שמו של נילס הנריק אבל, 1802–1829, ממייסדי תורת החבורות

פעולת החבורה נקראת בדרך כלל 'כפל', ומסומנת בהתאם. בחבורות אבליות לפעמים מעדיפים להשתמש בסימון חיבורי. אם מדובר בקבוצה של מספרים, למשל, (שמוגדרות עליה מראש פעולות חיבור וכפל), יתכן שיהיה עלינו להבהיר האם מדובר בחבורה ביחס לחיבור או לכפל.

תרגיל 3.4.2 (*) הראה שהחבורות $\mathbb{Z}_n$ כולן אבליות.

תרגיל 3.4.3 (*) הראה שהחבורות U_n כולן אבליות.

תרגיל 3.4.4 (**) הראה שהחבורה הסימטרית S_n אינה אבלית, אלא במקרים $n = 1, 2$.

תרגיל 3.4.5 (**) הראה שהחבורה הדיהדרלית D_n אינה אבלית, אלא במקרים $n = 1, 2$.

תרגיל 3.4.6 (**) בחבורה מתקיים $x^2 = 1$ לכל איבר. הוכח שהחבורה אבלית.

תרגיל 3.4.7 (*) הוכח: $(xy)^2 = x^2y^2$ לכל x, y אם ורק אם החבורה אבלית.

תרגיל 3.4.8 (***) נסמן ב־ Φ_n את התכונה "$\forall x \forall y : (xy)^n = x^n y^n$" (שיכולה להתקיים או לא להתקיים בחבורה נתונה). התכונה Φ_1 מתקיימת תמיד, והתכונה Φ_2 שקולה לאבליות לפי תרגיל 3.4.7. הוכח:

1. אם Φ_n אז לכל x, y מתקיים $x^n y^{n-1} = y^{n-1} x^n$.
2. אם Φ_n אז לכל x, $x^{n(n-1)}$ מתחלף עם כל אברי החבורה.
3. אם $\Phi_n \wedge \Phi_{n+1} \wedge \Phi_{n+2}$ אז החבורה אבלית.

3.5 מכפלה ישרה חיצונית

הגדרה. אם G_1, G_2 חבורות, מגדירים על הקבוצה $G_1 \times G_2$ של כל הזוגות הסדורים פעולה לפי רכיבים, $(g_1, g_2)(g_1', g_2') = (g_1 g_1', g_2 g_2')$. החבורה המתקבלת היא **המכפלה הישרה החיצונית** של G_1, G_2. בסעיף 6.2 נלמד גם מהי מכפלה ישרה פנימית (ונראה שלמעשה אין הבדל בין השתיים).

תרגיל 3.5.1 (*) $G_1 \times G_2$ היא חבורה. איבר היחידה הוא $(1_{G_1}, 1_{G_2})$, וההפכי של איבר נתון על־ידי $(g_1, g_2)^{-1} = (g_1^{-1}, g_2^{-1})$.

תרגיל 3.5.2 (*) ה"קומוטטיביות" וה"אסוציאטיביות" של מכפלה ישרה חיצונית:
א. $G \times H \cong H \times G$.
ב. $(G \times H) \times K \cong G \times (H \times K)$.

תרגיל 3.5.3 (**) מצא את כל לוחות הכפל האפשריים של חבורה מסדר 4. הראה שאלו בדיוק לוחות הכפל של $\mathbb{Z}_4$ ושל $\mathbb{Z}_2 \times \mathbb{Z}_2$.

תרגיל 3.5.4 (**) הראה ש־ $U_8 \cong \mathbb{Z}_2 \times \mathbb{Z}_2$.

תרגיל 3.5.5 (**) $D_2 \cong \mathbb{Z}_2 \times \mathbb{Z}_2$.

3.6 תת־חבורות

תהי G חבורה.

הגדרה 3.6.1 ***תת־קבוצה לא ריקה $H \subseteq G$ היא תת־חבורה של G אם היא סגורה לכפל ולהיפוך, כלומר, לכל $x, y \in H$ מתקיים $xy \in H$ ו־$x^{-1} \in H$. במקרה זה H עצמה היא חבורה (עם הכפל המצומצם מ־G, ואותו איבר יחידה), מסמנים $H \leq G$.***

תרגיל 3.6.2 (*) תהא $* \colon G \times G \to G$ פעולה בינארית על חבורה למחצה G; פורמלית, זוהי קבוצה של שלשות סדורות $(x, y, x*y) \in G \times G \times G$. הראה ש־ $* \cap (H \times H \times H)$ היא פעולה בינארית מוגדרת היטב על תת־הקבוצה $H \subseteq G$ אם ורק אם H סגורה לכפל.

תרגיל 3.6.3 (*) בכל חבורה G יש שתי תת־חבורות $G, 1$.

תרגיל 3.6.4 (*) אם $G \leq H, H \leq N$, אז $G \leq N$.

תרגיל 3.6.5 (**) אם $M \leq G$ סגור לכפל (אבל לא בהכרח ביחס לפעולת ההיפוך), אז M נקרא **תת־מונויד** של G. הוכח שכל תת־מונויד של חבורה הוא בעל תכונת הצמצום משמאל.

תרגיל 3.6.6 (**) אם G חבורה סופית ו־$H \subseteq G$ סגורה לכפל, אז H תת־חבורה.

תרגיל 3.6.7 (**)
1. אם N תת־חבורה של G, ו M תת־חבורה של H, אז $N \times M$ תת־חבורה של $G \times H$.
2. תן דוגמא לחבורה $G \times H$ עם תת־חבורה שאינה מתקבלת בצורה זו.

תרגיל 3.6.8 (**) תהיינה H, G_1, G_2 תת־חבורות של G. אם $H \subseteq G_1 \cup G_2$ אז $H \subseteq G_1$ או $H \subseteq G_2$.

תרגיל 3.6.9 (***) מצא דוגמא לתת־חבורות $H \subseteq G_1 \cup G_2 \cup G_3$ כך ש־ H אינה מוכלת בשום איחוד $G_i \cup G_j$. **הדרכה.** קח $G = \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$.

פרק 4

משפט לגרנז'

לאחר שהצגנו את מושגי היסוד בפרק הקודם, נוכיח את משפט לגרנז', שהוא התוצאה החשובה הראשונה בתורת החבורות, ונפגוש כמה שימושים שלו.

מושגים. יוצרים ותת־החבורה הנוצרת. קוסט. מחזור, חילוף. סדר של איבר. משפט פרמה, משפט אוילר, שאריות ריבועיות. חבורה ציקלית. כפל של תת־חבורות.

4.1 יוצרים של חבורה ותת־החבורה הנוצרת

תרגיל 4.1.1 (*) נניח ש־ $H_1, H_2 \leq G$ תת־חבורות. הוכח שהחיתוך $H_1 \cap H_2$ גם הוא תת־חבורה.

תרגיל 4.1.2 (*) נניח ש־ $H_1, \dots, H_n$ תת־חבורות של חבורה G. הוכח שהחיתוך $H_1 \cap \cdots \cap H_n$ גם הוא תת־חבורה.

טענה 4.1.3 החיתוך של משפחה כלשהי של תת־חבורות של G הוא תת־חבורה.

ב"משפחה כלשהי" הכוונה היא למשפחה שאינה דווקא סופית או בת־מניה. יתכן למשל שלכל מספר ממשי $\alpha \in \mathbb{R}$ מותאמת תת־חבורה $H_\alpha \leq G$, ואז הטענה היא ש־ $\bigcap_{\alpha \in \mathbb{R}} H_\alpha \leq G$.

תרגיל 4.1.4 (**) הוכח את הטענה.

תהי $X \subset G$ תת־קבוצה כלשהי של אברים בחבורה.

תרגיל 4.1.5 (**) הוכח שהחיתוך של כל תת־החבורות של G המכילות את X הוא תת־החבורה הקטנה ביותר המכילה את X (כלומר, זוהי תת־חבורה המכילה את X, ומוכלת בכל תת־חבורה אחרת המכילה את X).

תרגיל 4.1.6 (**) הוכח שהאוסף של כל המכפלות הסופיות ב־G של אברים מ־X או מ־$X^{-1} = \{x^{-1} : x \in X\}$, הוא תת־החבורה הקטנה ביותר המכילה את X.

הגדרה 4.1.7 *תת־החבורה שהוגדרה בכל אחד משני התרגילים הקודמים נקראת* ***תת־החבורה הנוצרת*** *על־ידי X, ומסמנים אותה ב־$\langle X \rangle$. אם $G = \langle X \rangle$, אומרים ש־X היא* ***קבוצת יוצרים*** *של G.*

לכתיב $\langle X\rangle$ יש משמעות רק כאשר X היא תת־קבוצה של חבורה ידועה G, המובנת מן ההקשר.

תרגיל 4.1.8 (***) הוכח שלחבורה U_{60} אין קבוצת יוצרים של שני אברים, ומצא קבוצת יוצרים עם שלושה אברים.

תרגיל 4.1.9 (*) תהי $H \leq G$ תת־חבורה, ותהי $X \subseteq G$ תת־קבוצה כלשהי. אז $X \subseteq H$ אם ורק אם $\langle X\rangle \subseteq H$.

תרגיל 4.1.10 (**) הוכח שתת־החבורה $V = \langle (12)(34),(13)(24)\rangle \leq S_4$ איזומורפית ל־ U_8.

תרגיל 4.1.11 (***) הוכח שתת־החבורה $\langle (1234),(13)\rangle$ של S_4 איזומורפית ל־ D_4.

תרגיל 4.1.12 (**) מצא את אברי תת־החבורה של S_6 הנוצרת על־ידי $(145)(263)$ ו־$(15)(36)$.

תרגיל 4.1.13 (**) מצא את אברי תת־החבורה $\langle (1324)(5768),(1526)(3847)\rangle \leq S_8$.

תרגיל 4.1.14 (**) זהה או תאר את החבורות הנוצרות על־ידי קבוצות המטריצות הבאות. בפרט, מה סדר החבורה בכל מקרה?

א. $D = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ ו־ $E = \begin{pmatrix} i & 0 \\ 0 & i \end{pmatrix}$. (כאן i הוא השורש הרביעי של 1); D, E^2.

ב. $F = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ ו־ $G = \begin{pmatrix} \omega & 0 \\ 0 & \omega^2 \end{pmatrix}$ ($\omega = \frac{-1+\sqrt{-3}}{2}$ הוא השורש השלישי של 1).

תרגיל 4.1.15 (***) זהה את החבורה הנוצרת על־ידי $A = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$ ו־ $B = \begin{pmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$; על־ידי A ו־ $C = \begin{pmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix}$.

4.1.1 יוצרים של S_n

הגדרה 4.1.16 *מחזור באורך 2 ב־S_n נקרא* **חילוף**. *כלומר, החילופים הם איברים מהצורה $(i\,j)$.*

איבר $x \neq 1$ בחבורה הוא (מסדר 2) אם $x^2 = 1$ (ראה סעיף 4.3).

תרגיל 4.1.17 (*) כל חילוף הוא איבר מסדר 2.

תרגיל 4.1.18 (*) הראה שלא כל איבר מסדר 2 ב־S_n ($n \geq 4$) הוא חילוף.

תרגיל 4.1.19 (**) S_n נוצרת על־ידי כל החילופים (ij). **הדרכה**. בדוק ש־ $(a_1 \dots a_t) = (a_1 a_t) \cdots (a_1 a_2)$.

תרגיל 4.1.20 (+***) S_n נוצרת על־ידי כל החילופים $(1j)$.

תרגיל 4.1.21 (-***) S_n נוצרת על־ידי האברים $\sigma_i = (i\,i+1)$, $i = 1, \ldots, n-1$. הראה ש־$\sigma_i^2 = 1$, $\sigma_i\sigma_j = \sigma_j\sigma_i$ אם $|i-j| > 1$, $\sigma_{i+1}\sigma_i\sigma_{i+1} = \sigma_i\sigma_{i+1}\sigma_i$ (*זוהי הצגת* Coxeter *של החבורה הסימטרית*).

תרגיל 4.1.22 (***) S_n נוצרת על־ידי החילוף $\tau = (12)$ והמחזור $\sigma = (1\,2\,3\,\cdots\,n)$.
הדרכה. חשב את $\sigma^k\tau\sigma^{-k}$ ואת $\sigma^j(\tau\sigma^{-1})^{j-i}\tau(\sigma\tau)^{i-j}\sigma^{-j}$.

תרגיל 4.1.23 (***) S_n נוצרת על־ידי המחזור $\sigma = (1\,2\,3\,\cdots\,n-1)$ והחילוף $\tau = (1\,n)$.

תרגיל 4.1.24 (-***) אם p ראשוני, S_p נוצרת על־ידי איבר כלשהו מסדר p וחילוף כלשהו.

תרגיל 4.1.25 (***) הפרך את הטענה הבאה: אם p ראשוני, S_p נוצרת על־ידי איבר כלשהו מסדר p ואיבר כלשהו מסדר 2.

תרגיל 4.1.26 (**) מצא את תת־החבורה של S_4 הנוצרת על־ידי כל המחזורים מהצורה (abc), a, b, c שונים.

תרגיל 4.1.27 (**) מצא את תת־החבורה של S_4 הנוצרת על־ידי כל התמורות מהצורה $(ab)(cd)$, a, b, c, d שונים.

תרגיל 4.1.28 (**) מצא את הגודל של חבורות התמורות הבאות:
א. $\langle(12), (23)(45)\rangle \subseteq S_5$.
ב. $\langle(12), (345)\rangle \subseteq S_5$
ג. $\langle(12), (123456)\rangle \subseteq S_6$.

תרגיל 4.1.29 (-***) יהי T עץ על הקודקודים $1, 2, \ldots, m$. לקשת המחברת את הקודקודים i, j מתאימים את החילוף (i, j). הוכח שמכפלת הקשתות על העץ, בכל סדר שיהיה, היא מחזור באורך m.

4.2 קוסטים ומשפט לגרנז'

תהיינה G חבורה ו־$H \leq G$ תת־חבורה. לכל $x \in G$, אנו מסמנים $Hx = \{hx \colon h \in H\}$ ו־$xH = \{xh \colon h \in H\}$.

הגדרה 4.2.1 *הקבוצות Hx נקראות קוסטים שמאליים של H, והקבוצות xH - קוסטים ימניים של H.*

נגדיר יחס שקילות על החבורה G: $x \equiv_H y$ אם $xy^{-1} \in H$.

תרגיל 4.2.2 (+*) הוכח שהיחס $\equiv_H$ הוא יחס שקילות.

תרגיל 4.2.3 (*) מחלקות השקילות של היחס $\equiv_H$ הן מהצורה Hx.
הסק: כמחלקות שקילות, שתי מחלקות Hx, Hy הן או שוות או נחתכות באופן ריק (קל להוכיח זאת כמובן גם באופן ישיר).

תרגיל 4.2.4 (+*) Hy היא קבוצת האיברים $x \in G$ שעבורם $y \in Hx$.

תרגיל 4.2.5 (**) לכל $x, y \in G$, $|Hx| = |Hy|$, ובפרט $|Hx| = |H|$.

תרגיל 4.2.6 (*) אם G אבלית, אז $Hg = gH$ לכל איבר $g \in G$ ותת־חבורה $H \leq G$.

הגדרה 4.2.7 האינדקס *(השמאלי) של H ב־G הוא מספר הקוסטים השמאליים של H בחבורה. את האינדקס מסמנים ב־ $[G\colon H]$.*

תרגיל 4.2.8 (+**) האינדקס הימני של H ב־G הוא מספר הקוסטים הימניים. הוכח שהאינדקס הימני תמיד שווה לשמאלי. **הדרכה.** חשוב על הפונקציה $Hx \mapsto x^{-1}H$ (מדוע לא $Hx \mapsto xH$?)

משפט 4.2.9 (משפט לגרנז') *אם $H \leq G$ חבורות סופיות, אז $|H|$ מחלק את $|G|$.*

תרגיל 4.2.10 (**) הראה ש־ $|G| = |H| \cdot [G\colon H]$, והסק את משפט לגרנז'.

תרגיל 4.2.11 (+**) נסמן ב־A_4 את תת־החבורה של S_4 הכוללת, מלבד הזהות, את התמורות שיש להן נקודות שבת אחת, ואת אלו המחליפות שני זוגות של ערכים. הוכח שזו אכן תת־חבורה. מה האינדקס שלה?

תרגיל 4.2.12 (**) נסמן ב־V את תת־החבורה של A_4 הכוללת, מלבד הזהות, את התמורות המחליפות שני זוגות של ערכים. הוכח שזו אכן תת־חבורה. כתוב את הקוסטים הימניים והשמאליים שלה ב־A_4.

תרגיל 4.2.13 (**) רשום את הקוסטים הימניים והשמאליים של תת־החבורות $H = \left\{I, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}\right\}$ ו־$\left\{I, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}\right\}$ $K =$ בחבורה S_3.

תרגיל 4.2.14 (**) מצא את הקוסטים של $\langle 41, 49, 31\rangle$ בחבורה U_{120}. (מה האינדקס שלה?)

4.3 סדר של איבר

הגדרה 4.3.1 *יהי $a \in G$. הסדר של האיבר a הוא $n > 0$ הקטן ביותר שעבורו $a^n = 1$, אם קיים כזה; אחרת אומרים שהסדר הוא אינסוף. אנו מסמנים את הסדר ב־$o(a)$.*

תרגיל 4.3.2 (*) אם $a \in H \leq G$ אז הסדר של a ב־H שווה לסדר ב־G.

תרגיל 4.3.3 (+*) הוכח שהסדר של a שווה לסדר של תת־החבורה הנוצרת, $\langle a\rangle$.

תרגיל 4.3.4 (-**) מצא את הסדר של כל אחד מהאיברים בחבורה D_4.

אחת ההבחנות השימושיות בתורת החבורות הסופיות:

תרגיל 4.3.5 (*) הסדר של איבר $a \in G$ מחלק את סדר החבורה.

תרגיל 4.3.6 (*) בחבורה סופית, יש N כך ש־$a^N = 1$ לכל a.

טענה 4.3.7 $x^n = 1$ אם ורק אם $o(x) \mid n$.

תרגיל 4.3.8 (**) אם $x,y \in G$ מתחלפים ו־$(o(x),o(y))=1$, אז $o(xy)=o(x)o(y)$.

תרגיל 4.3.9 (-***) הסדר של (x,y) בחבורה $G\times H$ הוא הכפולה המשותפת המינימלית $[o(x),o(y)]$. **הדרכה**. הראה ש־ $o(xy)|o(x)o(y)$, ומצא הצבה מתאימה כדי להוכיח $o(x)o(y) \mid o(xy)$.

תרגיל 4.3.10 (**) תהי $G=\{a_1,\dots,a_n\}$ חבורה אבלית. נסמן $b=a_1a_2\cdots a_n$.
א. הוכח: $b^2=1$.
ב. אם יש איבר יחיד מסדר 2, הוא שווה ל־b.
ד. בכל חבורה אבלית מסדר זוגי יש איבר מסדר 2.
ג. אם יש יותר מאיבר אחד מסדר 2, אז $b=1$. רמז. חשוב על $\{1,x,y,xy\}$.
ה. אם G מסדר אי־זוגי אז $b=1$.

תרגיל 4.3.11 (***) בחבורה מסדר זוגי יש איבר מסדר 2 (ראה משפט 10.2.1).

תרגיל 4.3.12 (***) הוכח: בחבורה מסדר $2p$ יש איבר מסדר p. **הדרכה**. אם קיים איבר מסדר p או $2p$ - סיימנו. לכן נניח שכל האברים מסדר $1,2$. אבל אז, קח $a\neq b$ מסדר 2, והעזר בתרגיל 3.4.6 כדי לקבל ש־$4\,|\,2p$.

תרגיל 4.3.13 (-***) יהי p מספר ראשוני. הראה שמספר האברים מסדר p בחבורה G מתחלק ב־$(p-1)$.

תרגיל 4.3.14 (**) נניח $n|m$, ויהיו $a\in U_{nm}$, ו־a^- הנציג של a ב־U_n. הוכח ש־ $\mathrm{ord}_{U_{nm}}(a)|m\cdot \mathrm{ord}_{U_n}(a)$.

תרגיל 4.3.15 (**) מצא את הסדר של המחזור $(r_1\cdots r_t)$, ואת הסדר של $\sigma=\tau_1\cdots\tau_u$, ו־$\tau_i$ הם מחזורים זרים מאורכים n_i.

תרגיל 4.3.16 (**) אין ב־S_4 איבר מסדר 6 (למרות ש־$6\,|\,24$).

תרגיל 4.3.17 (**) מצא ב־ S_7 איבר מסדר $5,6,7,10$. למה אין איבר מסדר 8?

4.4 יישומים בתורת המספרים

תרגיל 4.4.1 (*) אם p ראשוני אז $|U_p|=\varphi(p)=p-1$.

נזכיר **ששדה** הוא מבנה אלגברי F עם חיבור וכפל, שבו $(F,+,0)$ חבורה אבלית, $(F-\{0\},\cdot,1)$ חבורה אבלית, והכפל דיסטריבוטיבי ביחס לחיבור.

תרגיל 4.4.2 (-***) אם p ראשוני, אז $\mathbb{Z}_p$ (עם החיבור והכפל מודולו p) הוא שדה.

תרגיל 4.4.3 (+**) מצא את האברים מסדר 2 ב־U_p.

משפט 4.4.4 (משפט פרמה הקטן) *אם p ראשוני, אז לכל a זר ל־p,* $a^{p-1}\equiv 1 \pmod p$.

תרגיל 4.4.5 (**) הוכח את המשפט, על־ידי התבוננות בסדר של $[a]\in U_p$.

תרגיל 4.4.6 (*) חשב את $6^{48} \pmod{11}$.

תרגיל 4.4.7 (**) לכל n שלם, $n^5\equiv n \pmod{30}$.

תרגיל 4.4.8 (**) הראה שאם a זר ל־6, אז $a^2 \equiv 1 \pmod{24}$.

משפט 4.4.9 (משפט אוילר) *לכל n, אם a זר ל־n, $a^{\phi(n)} \equiv 1 \pmod{n}$.*

תרגיל 4.4.10 (*) הסבר כיצד משפט אוילר מכליל את משפט פרמה הקטן.

תרגיל 4.4.11 (**) לכל שני מספרים a, n, מתקיים $n|\phi(a^n-1)$.

תרגיל 4.4.12 (***־) לא קיים פתרון למשוואה $x^3 \equiv 2 \pmod{31}$.

4.4.1 פונקציית אוילר

תרגיל 4.4.13 (*+) אם p ראשוני, אז $\varphi(p^a) = p^{a-1}(p-1)$.

תרגיל 4.4.14 (***) אם n, m זרים אז $\varphi(nm) = \varphi(n)\varphi(m)$. **הדרכה**. משפט השאריות הסיני. המספרים הזרים ל־ nm הם אלו שזרים ל־ n ול־ m, תרגיל 1.3.31.

משני התרגילים האחרונים מתקבלת הנוסחה

$$\varphi(p_1^{\alpha_1}\cdots p_t^{\alpha_t}) = (p_1-1)p_1^{\alpha_1-1}\cdots(p_t-1)p_t^{\alpha_t-1}.$$

תרגיל 4.4.15 (*) חשב את $\varphi(540), \varphi(480), \varphi(1000)$.

תרגיל 4.4.16 (**) אם $n|m$ אז $\varphi(n)|\varphi(m)$.

תרגיל 4.4.17 (***) מצא את כל הערכים של n המקיימים $\varphi(n) \leq 6$ בשתי דרכים; לפי הנוסחה ל־ $\varphi(n)$, ובדרך הבאה: הראה שאם $p|n$ אז $p-1 \leq 6$. הסק ש־ $11, 13, 17, 19, 23, 29, 31 \in U_n$ ולכן $n \leq 20$. מצא את המועמדים שיש לבדוק.

תרגיל 4.4.18 (***+) הוכח ש־ $\liminf_{n\to\infty} \frac{\varphi(n)}{n} = 0$. **הדרכה**. נניח ש־ $\varphi(n) \leq m$, אז כל הגורמים הראשוניים של n קטנים מ־ $\cdots$. מכיוון שיש אינסוף ראשוניים, $\cdots$.

תרגיל 4.4.19 (***) בכל תת־חבורה לא טריוויאלית של U_{p^n} (p ראשוני), סכום האיברים מתחלק ב־ p^n.

4.4.2 שאריות ריבועיות

הגדרה 4.4.20 *יהי n מספר טבעי. מספר a (זר ל־n) נקרא שארית ריבועית מודולו n אם קיים $x \in U_n$ כך ש־ $x^2 \equiv a \pmod{n}$.*

תרגיל 4.4.21 (**) נניח ש־n, m מספרים זרים. הראה ש־a שארית ריבועית מודולו nm אם ורק אם הוא שארית ריבועית מודולו n וגם מודולו m. **הדרכה**. העזר במשפט השאריות הסיני, משפט 1.5.6.

הגדרה 4.4.22 *אם p ראשוני, **סימן לז'נדר** מוגדר כ־ $\left(\frac{a}{p}\right) = +1$ אם a הוא שארית ריבועית, ו־ $\left(\frac{a}{p}\right) = -1$ אחרת.*

תרגיל 4.4.23 (**) נניח ש־p ראשוני. הראה שאם $x^2 \equiv y^2 \pmod{p}$ אז $y \equiv \pm x \pmod{p}$.

תרגיל 4.4.24 (***) נניח ש־p ראשוני, אז $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right)$. **הדרכה**. העזר בתרגיל 4.4.23 כדי להראות שבדיוק מחצית מבין האברים ב־U_p הם שאריות ריבועיות.

תרגיל 4.4.25 (**) נניח ש־p ראשוני. $\left(\frac{a}{p}\right) = a^{\frac{p-1}{2}}$. **הדרכה**. תרגיל 10.6.27.

תרגיל 4.4.26 (**) הראה ש־-1 הוא שארית ריבועית מודולו הראשוני p אם ורק אם $p \equiv 1 \pmod{4}$ (או $p = 2$).

הגדרה 4.4.27 *עבור n איזוגי,* $n = p_1^{\alpha_1} \cdots p_t^{\alpha_t}$, *ו־*$a \in U_n$, ***סימן יעקובי*** *מוגדר כמכפלה* $\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right)^{\alpha_1} \cdots \left(\frac{a}{p_t}\right)^{\alpha_t}$.

תרגיל 4.4.28 (**+) אם $a \in U_n$ הוא שארית ריבועית מודולו n אז $\left(\frac{a}{n}\right) = +1$, אבל ההיפך אינו בהכרח נכון.

4.4.3 בדיקת ראשוניות

נתון מספר n. האם הוא ראשוני? בדיקת כל המחלקים הפוטנציאליים עד $\sqrt{n}$ (בפחות מזה אי אפשר להסתפק) היא תהליך מאד לא יעיל. יישום נכון של משפט לגרנז' לחבורת אוילר נותן מבחנים יעילים בהרבה.

לפי משפט פרמה, אם n ראשוני, אז לכל a זר ל־n מתקיים $a^{n-1} \equiv 1 \pmod{n}$. מכן נובע שאם $a^{n-1} \not\equiv 1 \pmod{n}$ עבור a כלשהו, אז n אינו ראשוני. הסיבוכיות של ביצוע המבחן הפשוט הזה עבור a אקראי היא רק $O(\log^3 n)$ (תרגיל 4.5.3), והוא לוכד את רוב המספרים שאינם ראשוניים. עם זאת, יש מספרים n שאינם ראשוניים ובכל זאת מקיימים $a^{n-1} \equiv 1 \pmod{n}$. מספר כזה נקרא **פסאודו ראשוני לפי פרמה** ביחס ל־a.

תרגיל 4.4.29 (**) הראה ש־$341 = 11 \cdot 31$ הוא פסאודו ראשוני לפי פרמה ביחס ל־2 (ואינו ראשוני).

תרגיל 4.4.30 (***־) הראה ש־561 פסאודו ראשוני לפי פרמה ביחס לכל $a \in U_{561}$. מספר כזה נקרא **מספר קרמייקל** (ראה תרגיל 10.6.44.)

מספר איזוגי n, שאינו ראשוני, נקרא **פסאודו־ראשוני לפי אוילר** ביחס ל־a אם $a^{\frac{n-1}{2}} \equiv \pm 1 \pmod{n}$.

תרגיל 4.4.31 (**+) כל פסאודו־ראשוני לפי אוילר הוא פסאודו־ראשוני לפי פרמה.

תרגיל 4.4.32 (***־) $1729 = 7 \cdot 13 \cdot 19$ הוא פסאודו־ראשוני לפי אוילר, ביחס לכל a.

יש אלגוריתם, מבוסס על 'משפט ההיפוך הריבועי של גאוס', המאפשר חישוב מהיר של סימן יעקובי (הגדרה 4.4.27). אלגוריתם זה הופך את ההגדרה הבאה לאפקטיבית: המספר n הוא **פסאודו־ראשוני לפי יעקובי** ביחס ל־a אם $a^{\frac{n-1}{2}} \equiv \left(\frac{a}{n}\right) \pmod{n}$.

תרגיל 4.4.33 (*+) כל פסאודו־ראשוני לפי יעקובי הוא פסאודו־ראשוני לפי אוילר.

למרות שיש מספרים שהם פסאודו־ראשוניים לפי יעקובי ביחס לערכים מסויימים של a, אין אף מספר שהוא פסאודו־ראשוני כזה ביחס לכל a (כלומר, אין אנלוג־יעקובי של מספרי קרמייקל). מכאן שאם מספר n מקיים $a^{\frac{n-1}{2}} \equiv \left(\frac{a}{n}\right) \pmod{n}$ למספיק ערכים של a, הוא מוכרח להיות ראשוני. עובדה זו היא הבסיס ל"מבחן סולובי־שטרסן" לבדיקת ראשוניות.

4.5 שימושים להצפנה

סעיף זה מניח היכרות ולו שטחית עם מושג הסיבוכיות

הצפנה, אחד הכלים החשובים ביותר בתקשורת המודרנית, היא הסתרה של מידע סודי, באופן שרק בעלי ה'מפתח' יכולים לקרוא את הסוד. יש תרחישים רבים ופרוטוקולים לאינספור, המסתמכים על הקושי האלגוריתמי לפתור בעיות מסויימות בתורת המספרים.

תרגיל 4.5.1 (**) הראה שהסיבוכיות של ביצוע פעולת חיבור היא ליניארית באורך הקלט, ושהסיבוכיות של פעולת הכפל היא (לכל היותר) ריבועית.

תרגיל 4.5.2 (**) הראה שהסיבוכיות של פעולת הרדוקציה של מספר מודולו n היא ליניארית באורך הקלט. הראה שהסיבוכיות של פעולות חיבור וכפל מודולריות אינה גדולה משל אותן פעולות כשלעצמן.

בפעולת העלאה בחזקה יש בעיה, משום שהתוצאה עלולה להיות ארוכה מאד ביחס לקלט. כאן באה לעזרתנו האריתמטיקה המודולרית.

תרגיל 4.5.3 (**) הראה שהסיבוכיות של פעולת ההעלאה בחזקה מודולו n היא (לכל היותר) ממעלה שלישית באורך הקלט.

תרגיל 4.5.4 (***) מהי הסיבוכיות של מציאת ההפכי בחבורת אוילר? (ראה תרגיל 3.3.12.)

4.5.1 RSA

הצפנה בשיטת RSA (על־שם הממציאים ריבסט, שמיר ואלדמן) נועדה לאפשר לכל אדם להצפין, אבל רק לבעל הסוד - לפענח. אם שני צדדים מבקשים לשוחח באופן סודי, על כל אחד מהם לממש את השיטה על המסרים המיועדים אליו.

הגדרה 4.5.5 ***בהצפנה בשיטת*** RSA***, בעל הסוד בוחר שני מספרים ראשוניים גדולים*** p,q***, ומפרסם את המכפלה*** $n=pq$ ***ומספר נוסף*** d ***(זר ל־***n***). כדי להצפין*** $x\in U_n$***, יש לחשב את*** $y=x^d$***. כדי לפענח, בעל הסוד מוצא (פעם אחת, באמצעות תרגיל 3.3.12) את ההפכי*** $e=d^{-1}\in U_n$***, ומחשב*** $x=y^e$.

תרגיל 4.5.6 (**) הוכח שפעולת הפענוח בשיטת RSA אכן מחזירה את הסוד x.

אחת הבעיות הקלאסיות הנחשבות לקשות היא **בעיית הפירוק**: למצוא את הפירוק של מספר נתון n לגורמיו הראשוניים. אלגוריתמים של בית־ספר מראים שהסיבוכיות אינה עולה על $O(\sqrt{n})$. את הסיבוכיות הטובה ביותר משיגות שיטות נפה מתוחכמות: $O(e^{c\log(n)^{1/3}\log\log(n)^{2/3}})$, עבור $c=4\cdot 3^{-2/3}$.

תרגיל 4.5.7 (+***) הראה שעבור מספרים מהצורה $n=pq$, כאשר p,q ראשוניים, בעיית הפירוק שקולה מבחינה אלגוריתמית לבעיה של חישוב פונקציית אוילר $\varphi(n)=(p-1)(q-1)$.

תרגיל 4.5.8 (+***) הסבר כיצד ידיעת e (בנוסף לידיעת d,n) בשיטת RSA מאפשרת למצוא את $\varphi(n)$.

אם כך, היכולת לפענח "לפי הספר" בשיטת RSA שקולה ליכולת לחשב את $\varphi(n)$, השקולה ליכולת לפרק את n. אם מאמינים שקשה לפרק את n, זוהי ראיה לבטיחות השיטה. עם זאת יש להעיר שאיש טרם הוכיח שהיכולת לפענח הצפנה זו שקולה ליכולת לפרק (משום שאולי אפשר למצוא את x מידיעת x^d בלי לדעת את e).

4.5.2 שיטת רבין

נציג כעת את שיטת ההצפנה שפיתח מיכאל רבין, והקרויה **שיטת רבין** על שמו. בהקשר זה, טוב לדעת שלכל שני ראשוניים שונים p,q, $U_{pq} \cong U_p \times U_q$ (תרגיל 10.6.18).

תרגיל 4.5.9 (**) יהי p ראשוני. הראה שלכל $z \in U_p$, $z^{\frac{p+1}{2}} = \left(\frac{z}{p}\right)z$.

תרגיל 4.5.10 (**) נניח ש־$p \equiv 3 \pmod 4$ ראשוני. הראה שלכל $x \in U_p$, בדיוק אחד מבין המספרים $\pm x$ הוא שארית ריבועית. ***הדרכה.*** תרגילים 4.4.26 ו־4.4.24.

תרגיל 4.5.11 (+**) יהי $p \equiv 3 \pmod 4$ ראשוני. נניח ש־$y = x^2 \in U_p$. הראה ש־$y^{\frac{p+1}{4}} = \pm x$. כלומר, העלאה בחזקת $\frac{p+1}{4}$ היא הפעולה של הוצאת שורש מן הערך $\pm x$ שיש לו שורש (בהמשך לתרגיל 4.5.10).

תרגיל 4.5.11 מראה שאם $p \equiv 3 \pmod 4$, אפשר, בקלות יחסית, לחשב שורשים ריבועיים מודולו p.

כמו שיטת RSA, שיטת רבין נועדה לאפשר לכל אדם להצפין, אבל רק לבעל הסוד - לפענח. נציג כאן גרסה מפושטת, שבה הפענוח אינו שלם.

הגדרה 4.5.12 ***בהצפנה בשיטת רבין, בעל הסוד בוחר שני מספרים ראשוניים גדולים p,q המקיימים $p,q \equiv 3 \pmod 4$, ומפרסם את המכפלה $n = pq$. כדי להצפין $x \in U_n$, יש לחשב את $y = x^2$. כדי לפענח, בעל הסוד מחשב את $a = y^{\frac{p+1}{4}} \pmod p$ ו־$b = y^{\frac{q+1}{4}} \pmod q$, ומרכיב בעזרת משפט השאריות הסיני את ארבעת המספרים מודולו $n = pq$ השקולים ל־$\pm a \pmod p$ ול־$\pm b \pmod q$.***

תרגיל 4.5.13 (**) הראה שאחד הערכים שקיבל המפענח בשיטת רבין שווה לערך המוצפן x.

תרגיל 4.5.14 (***) הראה שיריב המסוגל לחשב מתוך $x^2 \in U_n$ את ארבעת הערכים שמקבל בעל הסוד בשיטת רבין, כאשר $n = pq$, מסוגל לפרק בקלות את n לגורמיו הראשוניים.

התרגיל האחרון (בהתאמות הנדרשות לכך שלא תיארנו כאן את השיטה במלואה) מראה שהדרך היחידה לפענח, באופן שיטתי, סודות המוצפנים בשיטת רבין, היא לפרק את המספר $n = pq$ לגורמים.

4.6 חבורות ציקליות

הגדרה 4.6.1 ***חבורה הנוצרת על־ידי איבר יחיד נקראת חבורה ציקלית.***

במלים אחרות, חבורה G היא ציקלית אם יש איבר $x \in G$ כך שכל איבר בחבורה הוא חזקה של x.

כל חבורה מכילה תת־חבורות ציקליות - אלו הנוצרות על־ידי איברים בודדים בחבורה.

תרגיל 4.6.2 (**) כל חבורה מסדר ראשוני היא ציקלית.

תרגיל 4.6.3 (*) הוכח שחבורה ציקלית היא אבלית.

תרגיל 4.6.4 (+*) הוכח שחבורה מסדר n היא ציקלית אם ורק אם יש בה איבר מסדר n.

תרגיל 4.6.5 (**) הוכח ש־ U_9 ו־U_{11} ציקליות, וש־U_{12} ו־U_{16} אינן ציקליות.

4.6.1 יחידות

תרגיל 4.6.6 (*) הראה שכל החבורות $\mathbb{Z}_n$ ציקליות. הראה שהחבורה $\mathbb{Z}$ ציקלית.

משפט 4.6.7 *כל חבורה ציקלית מסדר n איזומורפית ל־$\mathbb{Z}_n$; כל חבורה ציקלית מסדר אינסופי איזומורפית ל־$\mathbb{Z}$.*

תרגיל 4.6.8 (**) תהי $G = \langle a \rangle$ חבורה ציקלית מסדר 10. מצא את האינדקסים ואת הקוסטים הימניים של $H_1 = \langle a^2 \rangle$ ושל $H_2 = \langle a^5 \rangle$.

4.6.2 תת־חבורות של חבורה ציקלית

תרגיל 4.6.9 (*) לכל $n \in \mathbb{Z}$, תת־החבורה הנוצרת על־ידי n כוללת את הקבוצה $n\mathbb{Z}$ של האברים המתחלקים ב־n.

תרגיל 4.6.10 (+**) כל תת־חבורה של $\mathbb{Z}$ היא מהצורה $n\mathbb{Z}$ עבור n מתאים. **הדרכה.** הזכר בהוכחה של משפט 1.3.7.

טענה 4.6.11 כל תת־חבורה של חבורה ציקלית היא ציקלית.

תרגיל 4.6.12 (**) הוכח את הטענה. **הדרכה.** אפשר להניח שהחבורה היא $\mathbb{Z}_n$; הראה שהאיבר עם הנציג החיובי הקטן ביותר יוצר את תת־החבורה.

תרגיל 4.6.13 (+**) הסדר של a, כאיבר בחבורה $\mathbb{Z}_n$, הוא $\frac{n}{(n,a)}$.

תרגיל 4.6.14 (**) לכל $d \,|\, n$, יש בדיוק $\varphi(d)$ אברים מסדר d ב־$\mathbb{Z}_n$. בפרט, יש בה $\varphi(n)$ יוצרים.

תרגיל 4.6.15 (-***) לכל n, $\sum_{d \,|\, n} \varphi(d) = n$. בדוק את הטענה עבור $n = 12, 20$.

תרגיל 4.6.16 (+**) בחבורה ציקלית מסדר המתחלק ב־d יש בדיוק d פתרונות למשוואה $x^d = 1$. **הדרכה.** שלב את תרגיל 4.6.14 וטענה 4.3.7 עם תרגיל 4.6.15 (קח d במקום n).

משפט 4.6.17 *בחבורה ציקלית מסדר n יש תת־חבורה יחידה מכל סדר $d \,|\, n$.*

תרגיל 4.6.18 (-***) הוכח את המשפט. **הדרכה.** תהי H תת־חבורה מסדר d. מכיוון שהיא ציקלית, יש בה $\varphi(d)$ אברים מסדר d, וזה מספרם בחבורה כולה.

תרגיל 4.6.19 (**) נניח שלחבורה G אין תת־חבורות פרט ל־ $G, 1$. הוכח ש־ G ציקלית מסדר ראשוני.

4.6.3 מכפלה של חבורות ציקליות

משפט 4.6.20 $\mathbb{Z}_n \times \mathbb{Z}_m \cong \mathbb{Z}_{nm}$ *אם ורק אם* $(n,m) = 1$.

תרגיל 4.6.21 (***) הוכח את המשפט. **הדרכה.** לכיוון "$\Leftarrow$" העזר בקיום איבר מסדר nm בחבורה $\mathbb{Z}_{nm}$. לכיוון "$\Rightarrow$" הפעל את משפט 1.3.7.

תרגיל 4.6.22 (***) לכל n, m, $\mathbb{Z}_n \oplus \mathbb{Z}_m \cong \mathbb{Z}_{\gcd(n,m)} \oplus \mathbb{Z}_{\mathrm{lcm}(n,m)}$.

תרגיל 4.6.23 (+**) כתוב איזומורפיזם מפורש $\mathbb{Z}_{12} \times \mathbb{Z}_{20} \cong \mathbb{Z}_4 \times \mathbb{Z}_{60}$. לאן עוברת תת־החבורה $\langle (6,0),(0,10) \rangle$? ולאן $\langle (1,0) \rangle$?

4.7 כפל תת־חבורות

בהמשך להגדרת הקוסטים, שבה הכפלנו איבר בקבוצה, אנו מגדירים עבור תת־קבוצות $A, B \subset G$:

$$AB = \{ab\colon\ a \in A, b \in B\},$$

$$A^{-1} = \{a^{-1}\colon\ a \in A\}.$$

תרגיל 4.7.1 (*) הוכח את התכונות

1. $A(BC) = (AB)C$,
2. $(AB)^{-1} = B^{-1}A^{-1}$,
3. $(A^{-1})^{-1} = A$.

תרגיל 4.7.2 (*+) אשר שתת־קבוצה $A \subseteq G$ היא תת־חבורה אם ורק אם $AA = A$ ו־$A^{-1} = A$.

תרגיל 4.7.3 (**) נניח ש־ $H \subseteq G$ תת־קבוצה, ונגדיר $\equiv_H$ כבסעיף 4.2. הוכח שאם $\equiv_H$ יחס שקילות, אז H תת־חבורה.

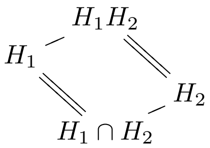
תת־החבורה הגדולה ביותר המוכלת בשתי תת־חבורות H_1, H_2 היא כמובן החיתוך $H_1 \cap H_2$. תת־החבורה הקטנה ביותר המכילה את שתיהם היא תת־החבורה הנוצרת על־ידי האיחוד, $\langle H_1 \cup H_2 \rangle = \langle H_1, H_2 \rangle$. אבל א־פריורי, האברים בתת־החבורה הנוצרת עשויים להיות מאוד מסובכים (למשל, $xyx'y'x''$ כאשר $x, x', x'' \in H_1$, $y, y' \in H_2$), והרי גם המכפלה H_1H_2, שהאברים שלה פשוטים ומובנים, מכילה כל אחת משתי תת־החבורות. האם היא חבורה בעצמה?

משפט 4.7.4 *המכפלה H_1H_2 של תת־החבורות H_2, H_1 היא תת־חבורה אם ורק אם $H_1H_2 = H_2H_1$.*

תרגיל 4.7.5 (**) הוכח את המשפט. **הדרכה**. תרגיל 4.7.2.

שימו לב שהתנאי $H_1H_2 = H_2H_1$ אינו אומר שכל איבר של H_1 מתחלף עם כל איבר של H_2, ואפילו לא שכל $x \in H_1$ מקיים $xH_2 = H_2x$. התנאי אומר רק שלכל $x_1 \in H_1$ ו־$x_2 \in H_2$ יש $x_2' \in H_2$ ו־$x_1' \in H_1$ כך ש־$x_2x_1 = x_1'x_2'$, ולהיפך.

תרגיל 4.7.6 (**) (*דוגמא נגדית ל"מכפלת תת־חבורות היא תמיד תת־חבורה"*): מצא תת־חבורות של S_3 שאינן מתחלפות.



טענה 4.7.7 אם $H_1, H_2 \leq G$ תת־חבורות מתחלפות, אז $[H_1H_2 : H_1] = [H_2 : H_1 \cap H_2]$.

במלים אחרות (כאשר H_1H_2 סופיות), $|H_1H_2| = \frac{|H_1|\cdot|H_2|}{|H_1 \cap H_2|}$.

תרגיל 4.7.8 (-***) הוכח את הטענה. **הדרכה.** הגדר פונקציה $f : H_1 \times H_2 \to H_1H_2$.

תרגיל 4.7.9 (+**) תהיינה $H_1, H_2 \leq G$ תת־חבורות. הראה שאם $H_1H_2 \subseteq H_2H_1$ אז $H_1H_2 = H_2H_1$. **הדרכה.** הפוך.

פרק 5

הומומורפיזמים ותת־חבורות נורמליות

בפרק זה נעשה את הצעדים הראשונים בתורת המבנה של החבורות. כשמתירים מעט את הרצועה בהגדרת האיזומורפיזם, נפתח בפנינו מגוון אפשרויות המביא באופן טבעי להגדרה של מושג חשוב ביותר: חבורת המנה.

מושגים: הומומורפיזם. גרעין ותמונה. תת־חבורה נורמלית. חבורת מנה. משפט האיזומורפיזם הראשון.

5.1 הומומורפיזמים

הגדרה 5.1.1 *תהיינה G ו־H חבורות. הומומורפיזם (של חבורות) $\phi\colon G{\to}H$ הוא פונקציה המקיימת את האקסיומות $\phi(xy) = \phi(x)\phi(y)$, $\phi(1_G) = \phi(1_H)$ ו־$\phi(x^{-1}) = \phi(x)^{-1}$ לכל $x, y \in G$.*

תרגיל 5.1.2 (**) כל פונקציה שומרת כפל $\phi\colon G \to H$ היא הומומורפיזם.

תרגיל 5.1.3 (**) מצא העתקה $\varphi : M \to N$ של מונוידים השומרת על הכפל אבל לא על היחידה. **הצעה.** קח $M = N = \mathbb{N}^2$ עם הכפל לפי רכיבים.

תרגיל 5.1.4 (*) הוכח שההעתקות הבאות הן הומומורפיזמים.
א. העתקת הדטרמיננטה $\det : \mathrm{GL}_n(F) \to (F, \cdot)$.
ב. $\nu : (\mathbb{C}^*, \cdot) \to (\mathbb{R}^*, \cdot)$ המוגדרת לפי $\nu(z) = z\bar{z}$.

תרגיל 5.1.5 (**) כמה הומומורפיזמים יש $\mathbb{Z}_{15}{\to}\mathbb{Z}_{12}$? $\mathbb{Z}_{20}{\to}S_3$? $D_4{\to}\mathbb{Z}_{16}$?

5.2 גרעין ותמונה

יהי $\phi : G \to H$ הומומורפיזם.

הגדרה 5.2.1 ***הגרעין** של ϕ הוא אוסף האיברים $\mathrm{Ker}(\phi) = \{g \in G\colon\ \phi(x) = 1\}$. **התמונה** של ϕ הוא אוסף האיברים $\mathrm{Im}(\phi) = \{\phi(x)\colon\ x \in G\}$.*

תרגיל 5.2.2 (**) לכל הומומורפיזם $\phi\colon G\to H$, $\mathrm{Ker}(\phi)$ היא תת־חבורה של G, ו־ $\mathrm{Im}(\phi)$ היא תת־חבורה של H.

תרגיל 5.2.3 (*) ϕ חד־חד־ערכית אם ורק אם $\mathrm{Ker}\,\phi = \{1\}$.

תרגיל 5.2.4 (**־) חשב את $\mathrm{Ker}\,\varphi$ עבור ההעתקות הבאות.

א. $\varphi : (\mathbb{Z}, +) \to (\mathbb{Z}, +)$ המוגדר לפי $\varphi(x) = 21x$.

ב. $\varphi : (\mathbb{R}, +) \to (\mathbb{R}^*, \cdot)$ המוגדר לפי $\varphi(x) = 2^x$.

ג. $\varphi : \mathbb{R}^* \to \mathbb{R}^*$ המוגדר לפי $\varphi(x) = x^4$.

ד. $\varphi : \mathbb{C}^* \to \mathbb{C}^*$ המוגדר לפי $\varphi(x) = x^4$.

תרגיל 5.2.5 (**) נניח ש־G נוצרת על־ידי קבוצת יוצרים X. אם שני הומומורפיזמים $\phi, \phi'\colon G\to H$ מסכימים על X, אז הם מתלכדים.

הגדרה 5.2.6 ***אם F שדה,*** $\mathrm{SL}_n(F) = \{A \in \mathrm{GL}_n(F) :\ \det(A) = 1\}$. ***זהו הגרעין של העתקת הדטרמיננטה*** $\mathrm{GL}_n(F)\to F^\times$.

תרגיל 5.2.7 (**) תהי G חבורה. אם A אבלית, אז אוסף ההומומורפיזמים $\mathrm{Hom}(G, A)$, עם חיבור לפי רכיבים ($(f + g)(a) = f(a) + g(a)$), הוא חבורה אבלית.

קבע מהו הסדר של $\mathrm{Hom}(S_3, \mathbb{Z}_4)$ ושל $\mathrm{Hom}(S_4, \mathbb{Z}_6)$.

הגדרה 5.2.8 *הומומורפיזם* $\phi\colon G\to H$ *נקרא* ***מונומורפיזם*** *(או:* ***שיכון****) אם הוא חד־חד־ערכי, ו****אפימורפיזם*** *אם הוא על.*

נזכיר שהומומורפיזם שהוא גם חד־חד־ערכי וגם על נקרא **איזומורפיזם**.

תרגיל 5.2.9 (***) אם $m|n$ אז יש מונומורפיזם יחיד $\varphi : \mathbb{Z}_m \to \mathbb{Z}_n$ ואפימורפיזם יחיד $\psi : \mathbb{Z}_n \to \mathbb{Z}_m$. מצא אותם. חשב את $\varphi \circ \psi$ ואת $\psi \circ \varphi$.

תרגיל 5.2.10 (*) יהי $\varphi : G_1 \to G_2$ איזומורפיזם. הוכח:

א. $o(\varphi(g)) = o(g)$.

ב. x, y מתחלפים אם ורק אם $\varphi(x), \varphi(y)$ מתחלפים.

ג. אם $H \le G_1$ אז $\varphi(H) \le G_2$.

תרגיל 5.2.11 (**) הוכח ש־ $\left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} : a, b \in \mathbb{R}, (a, b) \neq (0, 0) \right\}$, עם פעולת כפל המטריצות, איזומורפית ל־$\mathbb{C}^*$.

תרגיל 5.2.12 (**) מצא אפימורפיזם $\varphi : D_n \to \mathbb{Z}_2$.

תרגיל 5.2.13 (***) נניח ש־ $m|n$. הראה שקיימים אפימורפיזם $\alpha : D_n \to D_m$ ומונומורפיזם $\beta : D_m \to D_n$. חשב את $\alpha \circ \beta$ ואת $\beta \circ \alpha$.

5.3 תת־חבורה נורמלית

תרגיל 5.3.1 (*) אם H תת־חבורה של G, אז לכל $g \in G$ גם gHg^{-1} תת־חבורה.

משפט 5.3.2 *התכונות הבאות של תת־חבורה $H \leq G$ שקולות:*

1. *$H \subseteq gHg^{-1}$ לכל $g \in G$.*
2. *$H = gHg^{-1}$ לכל $g \in G$.*
3. *$Hg = gH$ לכל $g \in G$.*
4. *כל קוסט ימני הוא גם קוסט שמאלי.*
5. *כל קוסט שמאלי הוא גם קוסט ימני.*

הגדרה 5.3.3 *במקרה ש־$H \leq G$ מקיימת את התכונות שבמשפט, אומרים שהיא* ***תת־חבורה נורמלית,*** *ומסמנים $H \lhd G$.*

תרגיל 5.3.4 (*+)** אם כל קוסט ימני של H מוכל בקוסט שמאלי של H, אז $H \lhd G$.
פתרון. *יהי $g \in G$. לפי ההנחה יש g', g'' כך ש־ $gH \subseteq Hg'$ ו־ $g^{-1}H \subseteq Hg''$, ואז $H \subseteq gHg'' \subseteq Hg'g''$, לכן הקוסטים השמאליים $H, Hg'g''$ נחתכים ומוכרחים להיות שווים. מכאן ש־ $gHg'' = H$ ואז $gH = Hg''^{-1}$, ו־H מקיימת את תנאי 4 של משפט 5.3.2.*

תרגיל 5.3.5 (**) הגרעין של כל הומומורפיזם $G \to H$ הוא תת־חבורה נורמלית של G (ראה משפט 5.4.6).

תרגיל 5.3.6 (*) בחבורה אבלית, כל תת־חבורה היא נורמלית.

תרגיל 5.3.7 (**) אם $[G:H] = 2$ אז H נורמלית ב־ G.

תרגיל 5.3.8 (*) (נורמליות היא תורשתית). אם $N \leq K \leq G$ ו־N נורמלית ב־ G, אז N נורמלית ב־K.

תרגיל 5.3.9 (**) (נורמליות אינה טרנזיטיבית). מצא חבורות $N \lhd K \lhd G$, כך ש־ N אינה נורמלית ב־ G. **הצעה.** בחר $G = A_4$, $K = \langle (12)(34), (13)(24) \rangle$, ו־ $N = \langle (12)(34) \rangle$.

תרגיל 5.3.10 (**) תהי $A \subseteq G$ תת־קבוצה. נסמן $A^G = \left\{ gag^{-1} : g \in G, a \in A \right\}$. הוכח ש־ $\langle A^G \rangle$ היא תת־החבורה הנורמלית המינימלית של G המכילה את A.

תרגיל 5.3.11 (**) תת־החבורה הנוצרת על־ידי ריבועי אברים היא נורמלית.

תרגיל 5.3.12 (*-)** בחבורה לא־אבלית מסדר 8 יש תת־חבורה ציקלית נורמלית מסדר 4.

תרגיל 5.3.13 (**) לכל תת־חבורה $H \leq G$, החיתוך $\bigcap gHg^{-1}$ הוא תת־חבורה נורמלית של G [תת־חבורה זו נקראת **הליבה** של H, ומסמנים אותה ב־$\mathrm{Core}_G(H)$].
הראה שזוהי תת־החבורה הנורמלית הגדולה ביותר של G המוכלת ב־H (וראה תרגיל 6.5.2).

תרגיל 5.3.14 (+***) נניח שבחבורה מתקיים, עבור n קבוע, $(ab)^n = a^n b^n$ לכל a,b עבור n קבוע. נסמן $G^m = \{g^m : g \in G\}$.
א. הוכח כי G^n, G^{n-1} הן תת־חבורות נורמליות של G.
ב. כל אברי G^n מתחלפים עם כל אברי G^{n-1}.
ג. לכל a,b ב G, $(aba^{-1}b^{-1})^{n(n-1)} = 1$.

תרגיל 5.3.15 (-***) אם $A,B \leq G$ תת־חבורות אבליות של G, אז $A \cap B$ נורמלית ב־$\langle A, B\rangle$.

הגדרה 5.3.16 *חבורה G היא **פשוטה** אם אין לה תת־חבורות נורמליות.*

תרגיל 5.3.17 (**) נתון ש $\cdots \subseteq G_n \subseteq \cdots \subseteq G_2 \subseteq G_1$ חבורות פשוטות. הוכח שגם $G = \bigcup_n G_n$ פשוטה.

תרגיל 5.3.18 (**) הראה ש־ $\{\sigma \in S_5 : \ \sigma(2) = 2\}$ היא תת־חבורה. האם היא נורמלית?

5.4 חבורת מנה

כפל של קוסטים מוגדר כפי שמוגדר בסעיף 4.7 כפל של כל שתי תת־קבוצות.

משפט 5.4.1 *המכפלה של כל שני קוסטים שמאליים של H היא קוסט שמאלי, אם ורק אם H נורמלית.*

הוכחה. אם $H \lhd G$ אז $Hx \cdot Hy = H(xH)y = HHxy = Hxy$. בכיוון ההפוך נניח שלכל x,y יש z כך ש־$HxHy = Hz$; נבחר $y = 1$, אז לכל x יש z כך ש־$xH \subseteq HxH = Hz$, ו־H נורמלית לפי תרגיל 5.3.4.

□

תרגיל 5.4.2 (-***) תת־חבורה $H \leq G$ היא נורמלית אם ורק אם הפעולה $(Ha, Hb) \mapsto Hab$ על קבוצת הקוסטים השמאליים מוגדרת היטב.

תרגיל 5.4.3 (**) אם $N \lhd G$, הקבוצה G/N של הקוסטים של N ב־G, עם הפעולה $Na \cdot Nb = Nab$, היא חבורה, שאיבר היחידה שלה הוא N. האיבר ההפכי מחושב על־ידי $(Na)^{-1} = Na^{-1}$.

הגדרה 5.4.4 *אם $N \lhd G$, החבורה G/N נקראת **חבורת המנה**, או 'G מודולו N'.*

משפט 5.4.5 *תת־חבורה $H \leq G$ היא נורמלית אם ורק אם היא גרעין של הומומורפיזם מ־G לחבורה כלשהי.*

תרגיל 5.4.6 (**) הוכח את המשפט. **הדרכה.** N היא הגרעין של ההטלה $G \to G/N$ המוגדרת על־ידי $a \mapsto Na$.

תרגיל 5.4.7 (*) בכל חבורה G, תת־החבורות הטריוויאליות $1, G$ הן נורמליות.

תרגיל 5.4.8 (-**) תהיינה $H, K \leq G$ תת־חבורות. כל קוסט ימני של $H \cap K$ הוא חיתוך של קוסט ימני של H עם קוסט ימני של K.

תרגיל 5.4.9 (*) בדוק את הדוגמא הבאה: $G = \{1, 11, 29, 39\}$ היא תת־חבורה של U_{40}, ואברי חבורת המנה הם הקוסטים I, A, B, C כאשר $I = G$, $A = \{3, 7, 33, 37\}$, $B = \{9, 19, 21, 31\}$, $C = \{13, 17, 23, 27\}$. למעשה, $U_{40}/G \cong \mathbb{Z}_4$ עם יוצר A.

תרגיל 5.4.10 (**) תן דוגמא נגדית לטענה השגויה: 'אם $A, B \lhd G$ ו־$G/A \cong B$, אז $G/B \cong A$'. **הצעה**. קח $G = U_{15}$.

האם אפשר לחשב את החבורה G מתת־חבורה נורמלית שלה, N, ומחבורת המנה G/N? שתי הדוגמאות הבאות מראות שהתשובה שלילית.

תרגיל 5.4.11 (**) הראה שבכל אחת מהחבורות S_3, $\mathbb{Z}_6$ (שאינן איזומורפיות), קיימת תת־חבורה נורמלית איזומורפית ל־ $\mathbb{Z}_3$, כך שהמנה איזומורפית ל־ $\mathbb{Z}_2$.
האם קיימת בשתיהן תת־חבורה נורמלית איזומורפית ל־ $\mathbb{Z}_2$?

תרגיל 5.4.12 (**) תן דוגמא לחבורות אבליות $G_1 \not\cong G_2$ עם תת־חבורות נורמליות $N_i \lhd G_i$, כך ש־ $N_1 \cong N_2$ ו־$G_1/N_1 \cong G_2/N_2$. **הצעה**. קח $G_1 = \mathbb{Z}_{p^4}$, $N_1 = \langle p^2 \rangle \subseteq G_1$; $G_2 = \mathbb{Z}_{p^3} \times \mathbb{Z}_p$, $N_2 = \langle (p,1) \rangle \subseteq G_2$.

תרגיל 5.4.13 (**) האם יתכן ש־ N ו־G/N שתיהן אבליות אבל G איננה כזו?

תרגיל 5.4.14 (**) תהי H תת־חבורה מאינדקס 2 של חבורה G. הוכח כי $g^2 \in H$ לכל $g \in G$.

תרגיל 5.4.15 (**) תהי G חבורה, $H \lhd G$ מאינדקס n. הוכח כי $g^n \in H$ לכל $g \in G$.

תרגיל 5.4.16 (**) הוכח ש־ $S_4/V \cong S_3$.

תרגיל 5.4.17 (-***) הוכח ש־ $D_{2n}/\mathrm{Z}(D_{2n}) \cong D_n$.

תרגיל 5.4.18 (**) יהי F שדה. נסמן ב־ $B_n(F)$ את חבורת המטריצות המשולשיות־עליונות ההפיכות מעל F, ב־$U_n(F)$ את החבורה של מטריצות ב־$B_n(F)$ שרכיבי האלכסון שלהן כולם 1, וב־$T_n(F)$ את אוסף המטריצות הסקלריות ההפיכות. הוכח ש־$U_n(F) \lhd B_n(F)$, $B_n(F)/U_n(F) \cong T_n(F)$, $U_n(F)T_n(F) = B_n(F)$, ו־ $\mathrm{SL}_n(F) \cdot T_n(F) = \mathrm{GL}_n(F)$. (להרחבה ראה תרגיל 8.2.19).

תרגיל 5.4.19 (**) נסמן $B = \{A \in \mathrm{M}_2(\mathbb{R}) : \ \det(A) = \pm 1\}$. הוכח ש־$B \lhd \mathrm{GL}_n(\mathbb{R})$ ו־$\mathrm{GL}_n(\mathbb{R})/B \cong \mathbb{R}^\times/\langle -1 \rangle \cong (\mathbb{R}^+)^\times$.

תרגיל 5.4.20 (***) כל חבורה מסדר $2p$ איזומורפית ל־$\mathbb{Z}_{2p}$ או ל־D_p ($p > 2$ ראשוני).
הדרכה. לפי תרגיל 4.3.12 יש בחבורה איבר y מסדר p. נסמן $N = \langle y \rangle$, אז $N \lhd G$ לפי תרגיל 5.3.7. יהי $x \notin N$ - אז $x^2 \in N$. אם $x^2 \neq 1$ אז $o(x) = 2p$ ו־G ציקלית. לכן אפשר להניח $x^2 = 1$. לפי הנורמליות $xyx^{-1} = y^i$ לאיזשהו i, אבל $y = x^2yx^{-2} = y^{i^2}$, ולכן (תרגיל 4.4.3) $xyx^{-1} = y^{\pm 1}$. אם $xyx^{-1} = y$ אז $o(xy) = 2p$. אחרת, $G \cong D_p$.

5.5 משפט האיזומורפיזם הראשון

משפט 5.5.1 (משפט האיזומורפיזם הראשון) *יהי $\varphi : G \to H$ הומומורפיזם של חבורות. אז* $G/\operatorname{Ker}(\varphi) \cong \operatorname{Im}(\varphi)$.

משפט האיזומורפיזם הראשון שימושי כל־כך, עד שמעתה, אם נרצה להוכיח שחבורת מנה G/N איזומורפית לחבורה אחרת, כמעט לעולם לא נעשה זאת באופן ישיר; במקום זה, נבנה אפימורפיזם מ־G אל החבורה המבוקשת, ש־N היא הגרעין שלו.

תרגיל 5.5.2 (+)** הוכח את המשפט.

תרגיל 5.5.3 (*) אם $\varphi : G \to H$ על, אז $H \cong G/\operatorname{Ker}(\varphi)$, כלומר: H (איזומורפית ל־) חבורת מנה של G.

תרגיל 5.5.4 (*) $\mathbb{Z}_n \cong \mathbb{Z}/n\mathbb{Z}$.

תרגיל 5.5.5 (-)** $S^1 = \{z : |z| = 1\}$ היא תת־חבורה של $\mathbb{C}^*$, ו $\mathbb{C}^*/S^1 \cong \mathbb{R}^+$.

תרגיל 5.5.6 (**) על הקבוצה $G = \{(a,b) : a,b \in \mathbb{R}, a \neq 0\}$ מגדירים פעולה לפי $(a,b)(c,d) = (ac, ad+b)$. הוכח ש־ G חבורה. הראה ש־ $K = \{(1,b) : b \in \mathbb{R}\}$ נורמלית ב־ G, וש־ $G/K \cong \mathbb{R}^*$.
מצא תת־חבורה של $\mathrm{GL}_2(\mathbb{R})$ שהיא איזומורפית ל־G.

תרגיל 5.5.7 (**) $K \lhd G$, $G/K \cong \mathbb{Z}$. הוכח שלכל n קיימת ב־ G תת־חבורה מאינדקס n.

הגדרה 5.5.8 *יהי F שדה.* $\mathrm{O}_n(F)$ *היא* **חבורת המטריצות האורתוגונליות**, *כלומר* $\mathrm{O}_n(F) = \{A \in \mathrm{M}_n(F) : AA^{\mathrm{t}} = I\}$.

תרגיל 5.5.9 (**) הראה ש־ $\mathrm{O}_n(F) \leq \mathrm{GL}_n(F)$.

תרגיל 5.5.10 (*) הראה שאוסף המטריצות הסקלריות (מטריצות מהצורה aI) הוא תת־חבורה של המרכז של $\mathrm{GL}_n(F)$. (למעשה, זהו המרכז כולו.)

הגדרה 5.5.11 *יהי F שדה, ויהי $n \geq 1$. מגדירים* $\mathrm{SO}_n(F) = \mathrm{O}_n(F) \cap \mathrm{SL}_n(F)$, $\mathrm{PO}_n(F) = \mathrm{O}_n(F)/\{aI \in \mathrm{O}_n(F)\}$ *ו־* $\mathrm{SO}_n(F) = \mathrm{SO}_n(F)/\{aI \in \mathrm{SO}_n(F)\}$.

תרגיל 5.5.12 (*) מצא את המטריצות הסקלריות ב־$\mathrm{O}_n(\mathbb{R})$ וב־$\mathrm{SO}_n(\mathbb{R})$.

תרגיל 5.5.13 (+)** זהה במפורש את החבורות $\mathrm{O}_2(\mathbb{R})$, $\mathrm{PO}_2(\mathbb{R})$, $\mathrm{SO}_2(\mathbb{R})$, $\mathrm{SO}_2(\mathbb{R})$. הוכח ש־ $\mathrm{PO}_2(\mathbb{R}) \cong \mathrm{O}_2(\mathbb{R}) \cong S^1 \times \{\pm 1\}$, וש־$\mathrm{SO}_2(\mathbb{R}) = \mathrm{SO}_2(\mathbb{R}) \cong S^1$. בדוק שהאיזומורפיזם $\mathrm{SO}_2(\mathbb{R}) \to \mathrm{PO}_2(\mathbb{R})$ הוא $\pm a \mapsto a^2$.

תרגיל 5.5.14 (+)** אם n אי־זוגי, $\mathrm{PO}_n(\mathbb{R}) \cong \mathrm{SO}_n(\mathbb{R}) = \mathrm{SO}_n(\mathbb{R})$.

פרק 6

סריג תת־החבורות

פרק שישי,
שממנו ידע הקורא על נקלה את כל מה שמסופר בו
(ניקולאי וסיליביץ גוגול, "מעשה במריבה שרב איוואן איוונוביץ' עם איוואן ניקיפורוביץ'")

בפרק הזה נכיר עוד תכונות של אוסף תת־החבורות של חבורה, הקושרות תת־חבורות של חבורה לתת־החבורות של חבורת מנה שלה.

מושגים: חיתוך, מכפלה. תת־חבורות משלימות. קומוטטורים. מכפלה ישרה פנימית. משפט האיזומורפיזם השני. משפט האיזומורפיזם השלישי. סריג, מודולריות. משפט ההתאמה.

6.1 חיתוך ומכפלה של תת־חבורות

תרגיל 6.1.1 (**) *נורמליות מחלחלת:* אם $H \leq G$ ו־$N \lhd G$, אז $N \cap H \lhd H$. מצא דוגמא נגדית ל־ $N \cap H \lhd N$.

תרגיל 6.1.2 (**) אם $N_1, N_2 \lhd G$, אז גם $N_1 \cap N_2 \lhd G$.

תרגיל 6.1.3 (**) אם $A \lhd A_1, B \lhd B_1$ תת־חבורות של G, אז $A \cap B \lhd A_1 \cap B_1$.

תרגיל 6.1.4 (*) תהיינה $H_1, H_2 \leq G$.
א. אם H_1 או H_2 נורמלית, אז $H_1 H_2$ תת־חבורה של G.
ב. מצא דוגמא נגדית לטענה השגויה הבאה: 'אם אחת מהחבורות H_1, H_2 נורמלית, אז $H_1 H_2$ תת־חבורה נורמלית'.
ג. אם שתיהן נורמליות, אז $H_1 H_2 \lhd G$.

6.2 מכפלה ישרה פנימית

תת־חבורות $H, K \leq G$ הן **משלימות** אם $H \cap K = 1$ ו־$HK = G$.

תרגיל 6.2.1 (*) הראה שאם H, K משלימות אז $HK = KH$.

תרגיל 6.2.2 (*) נניח ש־H, K משלימות. אז לכל איבר $g \in G$ יש הצגה יחידה בצורה $g = hk$ עבור $h \in H$ ו־$k \in K$.

תרגיל 6.2.3 (‎-***) אם A,B תת־חבורות משלימות של G ו־$A \subseteq A_1 \leq G$, אז $[A_1 : A] = |A_1 \cap B|$.

תרגיל 6.2.4 (‎+***) תן דוגמא נגדית לטענה הבאה: אם אם A,B תת־חבורות משלימות של G ו־$A_0 \lhd A$, אז A_0B היא חבורה. **הצעה**. קח $G = A_4$, $A = V$.

איבר מהצורה $[x,y] = xyx^{-1}y^{-1}$ נקרא **קומוטטור** (משום שהוא מודד באיזו מידה x ו־y מתחלפים, או אינם מתחלפים, זה עם זה).

תרגיל 6.2.5 (*) $[x,y] = 1$ אם ורק אם $xy = yx$.

הגדרה 6.2.6 *תהיינה* $A,B \leq G$. $[A,B]$ *היא תת־החבורה של* G *הנוצרת על־ידי הקומוטטורים* $[a,b]$ *עבור* $a \in A, b \in B$.

תרגיל 6.2.7 (*) $[A,B] = 1$ אם ורק אם כל איבר $a \in A$ מתחלף עם כל איבר $b \in B$.

הגדרה 6.2.8 G *היא* **מכפלה ישרה פנימית** *של תת־חבורות* H,K *אם* H,K *משלימות, ו־*$[H,K] = 1$.

תרגיל 6.2.9 (*) אם G אבלית ו־H,K משלימות, אז G היא מכפלה ישרה שלהן.

תרגיל 6.2.10 (**) תהיינה H,K תת־חבורות משלימות. הוכח: $[H,K] = 1$ אם ורק אם $H,K \lhd G$.

תרגיל 6.2.11 (‎+***) תהי G מכפלה ישרה פנימית של H_1,H_2, ו־N תת־חבורה נורמלית המקיימת $N \cap H_1 = N \cap H_2 = 1$. הוכח ש־ $N \subseteq \mathrm{Z}(G)$.

תרגיל 6.2.12 (‎-**) המכפלה הישרה החיצונית $G = A \times B$ היא מכפלה ישרה פנימית של תת־החבורות $A \times \{1_B\}$ ו־$\{1_A\} \times B$.

מכפלה ישרה פנימית וחיצונית הן למעשה אותו הדבר:

משפט 6.2.13 *אם* G *מכפלה ישרה פנימית של* H,K*, אז* $G \cong H \times K$.

תרגיל 6.2.14 (**) הוכח את המשפט. **הדרכה**. הגדר $\varphi : H \times K \to G$ לפי $\varphi(h,k) = hk$.

תרגיל 6.2.15 (‎+***) $\mathbb{Z}_4$ אינה מכפלה פנימית ישרה של תת־חבורות.

תרגיל 6.2.16 (**) תהיינה $H_1,H_2,K \lhd G$. אם $G = H_1H_2K$ ומתקיים $H_1 \cap (H_2K) \subseteq K$, אז G/K מכפלה ישרה פנימית של H_2K/K ו־H_1K/K.

תרגיל 6.2.17 (***) נניח ש־ G מכפלה ישרה פנימית של $\langle \epsilon \rangle \cong \mathbb{Z}_2$ ו־G_0. הוכח שכל תת־חבורה של G שאינה מכילה את ϵ, איזומורפית לתת־חבורה של G_0. **הדרכה**. אם $H \not\subset G_0$, נפרק $H = H_0 \cup H_1$ כאשר $H_0 = H \cap G_0$ ו־$H_1 = H - H_0$. הראה ש־$H \cong H_0 \cup \epsilon H_1$.

6.2.1 מכפלה ישרה של כמה תת־חבורות

הגדרה 6.2.18 *החבורה G היא מכפלה ישרה פנימית של $H_1, \dots, H_t$ אם*
1. *לכל i*, $H_i \lhd G$.
2. *לכל i*, $H_i \cap (H_1 \cdots H_{i-1} H_{i+1} \cdots H_t) = 1$.
3. $G = H_1 \cdots H_t$.

תרגיל 6.2.19 (**) אשר שהגדרה 6.2.18, עבור $t = 2$, מסכימה עם הגדרה 6.2.8.

משפט 6.2.20 *אם G מכפלה ישרה פנימית של $H_1, \dots, H_t$, אז* $G \cong H_1 \times \cdots \times H_t$.

תרגיל 6.2.21 (-***) תן דוגמא לחבורה G אם תת־חבורות נורמליות $H_i \lhd G$, כך ש־ $G = H_1H_2H_3$ ו־ $H_i \cap H_j = 1$ לכל i, j, אבל G אינה בהכרח מכפלה ישרה פנימית של H_1, H_2, H_3.

תרגיל 6.2.22 (+**) נניח $H_i \lhd G$, $G = H_1H_2H_3$.
$1 = H_2 \cap H_3 = H_1 \cap H_2H_3$ אז G מכפלה ישרה פנימית של H_1, H_2, H_3.

6.3 משפטי האיזומורפיזם

בתרגילים לעיל הוכחנו שאם $H \leq G$ ו־$N \lhd G$, אז NH חבורה, $N \lhd NH$, ו־$N \cap H \lhd H$.

משפט 6.3.1 (משפט האיזומורפיזם השני) *תהי G חבורה עם תת־חבורה H ותת־חבורה נורמלית N. אז* $NH/N \cong H/N \cap H$.

תרגיל 6.3.2 (**) הוכח את המשפט. **הדרכה.** הגדר $\varphi : H \to NH/N$ לפי $\varphi(h) = hN$.

תרגיל 6.3.3 (**) נניח ש־ $N \lhd H_1$ הן תת־חבורות של G, ו־$H_2 \lhd G$ תת־חבורה נורמלית. הראה שההעתקה $H_1/N \to G/H_2$ המוגדרת לפי $h_1N \mapsto h_1H_2$, מוגדרת היטב אם ורק אם $N \subseteq H_2$. הראה שזהו איזומורפיזם אם ורק אם $N = H_1 \cap H_2$ ו־$G = H_1H_2$.

תרגיל 6.3.4 (**) תהי G חבורה עם תת־חבורה H ותת־חבורות נורמליות M, N. הוכח: אם $H \cap N = H \cap M$, אז $(HN)/N \cong (HM)/M$.

תרגיל 6.3.5 (**) תהי G חבורה עם תת־חבורה H ותת־חבורות נורמליות M, N. הוכח: אם $HN = KN$, אז $H/(H \cap N) \cong K/(K \cap N)$.

משפט 6.3.6 (משפט האיזומורפיזם השלישי) *תהיינה $K \leq N$ תת־חבורות נורמליות של חבורה G. אז* $(G/K)/(N/K) \cong G/N$.

תרגיל 6.3.7 (**) הוכח את המשפט. **הדרכה.** הגדר $\varphi : G/K \to G/N$ לפי $\varphi(gK) = gN$.

תרגיל 6.3.8 (**) תהיינה $A, B, C \lhd G$, כך ש־ $B \subseteq A$. הוכח ש־ AC/BC היא חבורת מנה של A/B.

תרגיל 6.3.9 (***) תהיינה H, B, C תת־חבורות של חבורה G, כך ש־ B, C נורמליות ו־$B \subseteq H$. מצא העתקות f חח"ע ו־g על, כך ש־ $\mathrm{Im}(f) = \mathrm{Ker}(g)$ בדיאגרמה:

$$0 \to \frac{H \cap C}{B \cap C} \xrightarrow{f} \frac{H}{B} \xrightarrow{g} \frac{HC}{BC} \to 0.$$

תרגיל 6.3.10 (***) H, K תת־חבורות נורמליות של G, עם מנות אבליות. הוכח ש־$G/H \cap K$ אבלית. **הדרכה.** בנה הומומורפיזם $G/H \cap K \to G/H \times G/K$.

תרגיל 6.3.11 (**) $N \lhd G$ ו־$N, G/N$ אבליות. H תת־חבורה של G. הוכח שקיימת $K \lhd H$, כך ש־ $K, H/K$ אבליות.

תרגיל 6.3.12 (***) יהי $\varphi : G_1 \to G_2$ הומומורפיזם. תהיינה $K_i \lhd H_i \leq G_i$ תת־חבורות. הוכח שאם $\varphi(H_1) \subseteq H_2$ ו־$\varphi(K_1) \subseteq K_2$, אז $\tilde{\varphi}(h_1K_1) = \varphi(h_1)K_2$ מגדיר הומומורפיזם $\tilde{\varphi} : H_1/K_1 \to H_2/K_2$. הראה שיתכן ש־ φ חד־חד־ערכית, אבל $\tilde{\varphi}$ אינה כזו.

תרגיל 6.3.13 (***) (הלמה של Zassenhaus)
תהיינה $A \lhd A^{\#}$, $B \lhd B^{\#}$, תת־חבורות של G.
א. $A^{\#} \cap B \lhd A^{\#} \cap B^{\#}$.
ב. $A(A^{\#} \cap B) \lhd A(A^{\#} \cap B^{\#})$.
ג. $\frac{A(A^{\#} \cap B^{\#})}{A(A^{\#} \cap B)} \cong \frac{B(A^{\#} \cap B^{\#})}{B(A \cap B^{\#})}$. **הדרכה.** התבונן ב־ $D = (A^{\#} \cap B)(A \cap B^{\#})$.

6.4 סריג תת־החבורות

6.4.1 סריגים

הגדרה 6.4.1 *קבוצה Λ עם יחס סדר חלש $\leq$ נקראת **סריג** אם לכל $a, b \in \Lambda$ יש חסם עליון וחסם תחתון לקבוצה $\{a, b\}$. במלים אחרות, מקסימום לקבוצה $\{x : x \leq a, x \leq b\}$, ומינימום לקבוצה $\{x : a \leq x, b \leq x\}$. את הראשון מסמנים $a \wedge b$ ואת השני $a \vee b$.*

תרגיל 6.4.2 (**) תהי X קבוצה. הראה שקבוצת החזקה $P(X)$, עם יחס ההכלה, היא סריג, שבו $A \vee B = A \cup B$ ו־$A \wedge B = A \cap B$.

תרגיל 6.4.3 (**) תן דוגמא לתת־קבוצה של $P(X)$ שאיננה סריג.

תרגיל 6.4.4 (**) הוכח את התכונות הבאות: $a \wedge b \leq a \leq a \vee b$; הפעולות $\wedge, \vee$ הן סימטריות ואסוציאטיביות; $x \leq a \wedge b$ אם ורק אם $x \leq a, b$; $a \vee b \leq x$ אם ורק אם $a, b \leq x$.

6.4.2 הסריג של תת־החבורות

טענה 6.4.5 אוסף תת־החבורות של חבורה, עם יחס ההכלה, הוא סריג.

תרגיל 6.4.6 (**) הוכח את הטענה: בדוק שלכל $H_1, H_2 \leq G$, $H_1 \cap H_2$ היא תת־החבורה הגדולה ביותר המוכלת ב־H_1, H_2 ו־$\langle H_1, H_2 \rangle$ היא תת־החבורה הקטנה ביותר המכילה את H_1, H_2.

תרגיל 6.4.7 (*) אם H_1H_2 תת־חבורה, אז $\langle H_1, H_2 \rangle = H_1H_2$ אבל אם לא, H_1H_2 אינה נמצאת בסריג תת־החבורות, ולכן אינה יכולה לשמש כחסם עליון.

6.4.3 מודולריות

תרגיל 6.4.8 (**-) הראה שבכל סריג, אם $A \leq C$ אז $(A \wedge B) \vee C \leq A \wedge (B \vee C)$.

הגדרה 6.4.9 *סריג הוא* **מודולרי** *אם לכל* $C \leq A$, $(A \wedge B) \vee C = A \wedge (B \vee C)$.

תרגיל 6.4.10 (**) הראה שסריג תת־הקבוצות $P(X)$ הוא מודולרי (כלומר, לכל שלוש קבוצות A, B, C, אם $C \subseteq A$ אז $(A \cap B) \cup C = A \cap (B \cup C)$).

תרגיל 6.4.11 (**) אם A, B, C תת־חבורות של G ו־$C \subseteq A$, אז $(A \cap B) \cdot C = A \cap (B \cdot C)$ (אלו אינן בהכרח תת־חבורות!).

תרגיל 6.4.12 (***) אוסף תת־החבורות הנורמליות של חבורה G הוא סריג מודולרי.

תרגיל 6.4.13 (***) הראה שהסריג של כל תת־החבורות אינו בהכרח מודולרי. **הצעה.** קח $G = S_4$, $A = \langle (12), (34) \rangle$, $C = \langle (12) \rangle$.

תרגיל 6.4.14 (**) תהיינה A, B, C תת־חבורות, כך ש־ $CA = CB$, $A \cap C = B \cap C$, ו־$A \subseteq B$. הוכח $A = B$.

תרגיל 6.4.15 (**) תהיינה $A, B, C \triangleleft G$, כך ש־ $A \subseteq B$. הוכח את האיזומורפיזם $BC/(A \cap BC) \cong C/A \cap C$.
קבל את משפט האיזומורפיזם השני כמקרה פרטי. **הדרכה.** קח $B = A$.

הגדרה 6.4.16 *סריג הוא* **דיסטריבוטיבי** *אם לכל* A, B, C *מתקיים השוויון*

$$A \vee (B \wedge C) = (A \vee B) \wedge (A \vee C).$$

תרגיל 6.4.17 (***-) הוכח: כל סריג דיסטריבוטיבי הוא מודולרי.

תרגיל 6.4.18 (**) סריג תת־החבורות הנורמליות אינו בהכרח דיסטריבוטיבי. **הדרכה.** יש להראות שלפעמים $(AB) \cap (AC) \supset A(B \cap C)$. בחר $G = \mathbb{Z}_2 \times \mathbb{Z}_2$.

6.5 אינדקס של תת־חבורות

תרגיל 6.5.1 (***+) תהיינה $A, B \leq G$ תת־חבורות.

1. $[A : A \cap B] \leq [G : B]$. **הדרכה.** הגדר $f : A \to \{aB : a \in A\}$ על.
2. $[A : A \cap B] = [G : B]$ אם ורק אם $G = AB$.
3. הסק ש־ $[G : A \cap B] \leq [G : A] \cdot [G : B]$.
4. אם $[G : A], [G : B]$ זרים, אז $[G : A \cap B] = [G : A] \cdot [G : B]$.
5. אם $AB \leq G$ (בפרט, אם $A \triangleleft G$ או $B \triangleleft G$), אז $[AB : A \cap B] = [AB : A] \cdot [AB : B]$.

תרגיל 6.5.2 (***+) תהי $H \leq G$ תת־חבורה מאינדקס $[G : H] = n$.
א. הוכח ש־ H מכילה תת־חבורה $N \triangleleft G$ מאינדקס $[G : N] \leq n^n$. **הדרכה.** הראה ש־ $[G : \bigcap gHg^{-1}] \leq [G : H]^{[G:H]}$.
ב. נניח ש־ $H \leq T \triangleleft G$ עם $[G : T] = m$. הראה שאפשר לשפר את החסם ל־ $[G : N] \leq m \cdot (n/m)^n$.

6.6 משפט ההתאמה

משפט 6.6.1 *יהי* $\varphi : G \to H$ *הומומורפיזם, עם גרעין* $K = \mathrm{Ker}(\varphi)$*. נסמן ב־* $\mathcal{L}_G$ *את אוסף תת־החבורות של* G *המכילות את* K*, וב־* $\mathcal{L}_H$ *את אוסף כל תת־החבורות של* $\mathrm{Im}\varphi$.

אז קיימת התאמה חד־חד־ערכית ועל $\alpha : \mathcal{L}_G \to \mathcal{L}_H$*, המקיימת:*

1. *(מונוטוניות) עבור* $G_1, G_2 \in \mathcal{L}_G$, $G_1 \le G_2$ ***אם ורק אם*** $\alpha(G_1) \le \alpha(G_2)$.
2. *(שמירה על חיתוך)* $\alpha(G_1 \cap G_2) = \alpha(G_1) \cap \alpha(G_2)$.
3. *(שמירה על מכפלה)* $\alpha(G_1 G_2) = \alpha(G_1)\alpha(G_2)$.
4. *(שמירה על אינדקס)* ***אם*** $G_1 \subseteq G_2$***, אז*** $[G_1 : G_2] = [\alpha(G_1) : \alpha(G_2)]$.
5. *(שמירה על נורמליות) לכל* $N, H \in \mathcal{L}_2$, $N \lhd H$ ***אם ורק אם*** $\alpha(N) \lhd \alpha(H)$.
6. *(שמירה על מנות)* ***אם*** $N, H \in \mathcal{L}_1$ *מקיימות* $N \lhd H$***, אז*** $H/N \cong \alpha(H)/\alpha(N)$.

המשפט נותן איזומורפיזם של סריגים.

תרגיל 6.6.2 (***) הוכח את המשפט. **הדרכה**. קח $\alpha(H) = \varphi(H) = \{\varphi(g) : g \in H\}$, ו־$\beta(M) = \varphi^{-1}(M) = \{g \in G : \varphi(g) \in M\}$. הראה שההעתקות מוגדרות היטב והופכות זו את זו, כלומר, $\alpha \circ \beta = id_{\mathcal{L}_H}$ וש־$\beta \circ \alpha = id_{\mathcal{L}_1}$.

פרק 7

הצמדה ומחלקות הצמידות

כפי שאפשר לנחש, וגם נראה במפורש בהמשך, קל יותר לפענח את המבנה של חבורה אבלית מאשר את המקרה הכללי. לכן טבעי שנחפש בכל חבורה תת־חבורות אבליות גדולות, ותת־חבורות המתנהגות כאילו הן אבליות ביחס לחבורה או לתת־חבורות שלה. זו תהיה גם הזדמנות להתאמן בשימוש נכון בכמתים.

מושגים: מרְכָּז. הקווטרניונים. מרכֵּז של איבר ושל תת־חבורה. מחלקת צמידות. שוויון המחלקות.

7.1 המרְכָּז

הגדרה 7.1.1 *תהי G חבורה.* ***המרְכָּז*** $\mathrm{Z}(G) = \{z \in G \colon \forall x \in G : zx = xz\}$ *הוא אוסף האיברים המתחלפים עם כל אברי G.*

תרגיל 7.1.2 (*) $\mathrm{Z}(G) \lhd G$.

תרגיל 7.1.3 (*) $\mathrm{Z}(G) = G$ אם ורק אם G אבלית.

תרגיל 7.1.4 (**) תהי G חבורה. אם $G/\mathrm{Z}(G)$ חבורה ציקלית, אז G אבלית.

תרגיל 7.1.5 (**) $N \lhd G$, $|N| = 2$. הוכח ש־ $N \subseteq \mathrm{Z}(G)$. תן דוגמא נגדית עבור $|N| = 3$.

תרגיל 7.1.6 (**) אם $N \lhd G$, אז גם $\mathrm{Z}(N) \lhd G$.

תרגיל 7.1.7 (+*) חשב את המרכז של S_3.

תרגיל 7.1.8 (+*) חשב את המרכז של D_4.

תרגיל 7.1.9 (**) $H \leq G$. הראה ש־ $H \cap \mathrm{Z}(G) \subseteq \mathrm{Z}(H)$, ותן דוגמא שבה מתקיים $H \cap \mathrm{Z}(G) \subset \mathrm{Z}(H)$.

תרגיל 7.1.10 (*) אם בחבורה יש איבר יחיד מסדר 2, אז הוא במרכז שלה. (האם יתכן שבחבורה יהיה איבר יחיד מסדר 3?)

תרגיל 7.1.11 (***) תן דוגמא לחבורה G עם שלוש תת־חבורות, H_1, H_2, H_3, כך ש־$\mathrm{Z}(H_1)$ מוכלת ממש ב־$\mathrm{Z}(G)$, $\mathrm{Z}(H_2)$ מכילה ממש את $\mathrm{Z}(G)$, ו־$\mathrm{Z}(H_3)$ אינה מוכלת ב־$\mathrm{Z}(G)$ ואינה מכילה אותה.

תרגיל 7.1.12 (**) לכל תת־חבורה נורמלית $N \lhd G$, $\mathrm{Z}(G)N/N \subseteq \mathrm{Z}(G/N)$. תן דוגמא לכך שההכלה עשויה להיות אמיתית.

תרגיל 7.1.13 (+)** אם $H \leq G$ ו־$N \lhd G$, אז $\mathrm{Z}(H)N/N \subseteq \mathrm{Z}(HN/N)$.

הגדרה 7.1.14 חבורת הקווטרניונים ***מסדר*** 8, Q***, היא החבורה שאבריה*** $\{\pm i^\alpha j^\beta\}$, $\alpha, \beta = 0, 1$, ***עם חוקי הכפל המוגדרים לפי*** $i^2 = j^2 = -1$, $ji = -ij$.

תרגיל 7.1.15 (*) הראה ש־ $\mathrm{Z}(Q) = \langle -1 \rangle$.

תרגיל 7.1.16 (**) הראה שיש ל־Q איבר יחיד מסדר 2, והסק ש־$Q \not\cong D_4$.

תרגיל 7.1.17 (**) חבורת המטריצות ב $\mathrm{GL}_2(\mathbb{C})$ הנוצרת על־ידי $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$, $\begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$ איזומורפית ל־Q.

תרגיל 7.1.18 (***) מצא את כל תת־החבורות של Q, והראה שכולן נורמליות וציקליות.

תרגיל 7.1.19 (***) הוכח שכל חבורה לא אבלית G מסדר 8 איזומורפית ל־D_4 או ל־Q. **הדרכה.** לפי תרגיל 3.4.6, יש בחבורה איבר x מסדר 4. תת־החבורה $\langle x \rangle$ נורמלית לפי תרגיל 5.3.7, אבל אינה מרכזית לפי תרגיל 7.1.4. לכן קיים y כך ש־ $yxy^{-1} \neq x$; מאידך זהו איבר מסדר 4 של $\langle x \rangle$. מכאן ש־$yxy^{-1} = x^{-1}$, ובפרט $y \notin \langle x \rangle$ ו־$G = \langle x, y \rangle$. לפי תרגיל 5.4.15 $y^2 \in \langle x \rangle$, ו־$y^2$ אינו יכול להיות מסדר 4 כי y אינו מסדר 8. לכן $y^2 \in \{1, x^2\}$. הראה שאם $y^2 = 1$ אז $G \cong D_4$, ואם $y^2 = x^2$ אז $G \cong Q$.

הגדרה 7.1.20 חבורת הקווטרניונים המוכללת Q_{2n} ***היא החבורה שאבריה הם*** $a^i b^j$ ***עבור*** $i = 0, \ldots, 2n-1$, $j = 0, 1$***, עם כללי הכפל*** $b^2 = a^n$, $b^4 = 1$, $bab^{-1} = a^{-1}$. ***זוהי חבורה מסדר*** $4n$.

תרגיל 7.1.21 (**) אשר ש־Q_{2n} חבורה. מה יש כאן להוכיח?

תרגיל 7.1.22 (*) $Q_4 = Q$.

תרגיל 7.1.23 (**) $\mathrm{Z}(Q_{2n}) = \langle a^n \rangle$, ו־$Q_{2n}/\mathrm{Z}(Q_{2n}) \cong D_n$.

7.1.1 המרכז של S_n

טענה 7.1.24 שני מחזורים $\sigma, \tau \in S_n$ מתחלפים אם ורק אם הם (כלומר - התומכים שלהם) זרים.

תרגיל 7.1.25 (-*)** הוכח את הטענה.

תרגיל 7.1.26 (-*)** מהי הצורה הכללית של תמורה המתחלפת עם $(1\,2\cdots r)$ ב־S_n?

תרגיל 7.1.27 (**) מה הצורה הכללית של תמורה המתחלפת עם (ij)?

תרגיל 7.1.28 (**) נניח $n \geq 3$. אז $\mathrm{Z}(S_n) = 1$.

תרגיל 7.1.29 (**) מה הצורה הכללית של תמורה המתחלפת עם (ijk)?

נסמן ב־A_n את תת־החבורה של S_n הנוצרת על־ידי המחזורים באורך 3 (ראו סעיף 9.2 להגדרה אחרת).

תרגיל 7.1.30 (**) נניח $n \geq 4$. אז $\mathrm{Z}(A_n) = 1$.

7.2 מרכְּזים

7.2.1 מרכֵּז של איבר

תהי G חבורה עם איבר $a \in G$.

הגדרה 7.2.1 ***המרכֵּז של a הוא אוסף האיברים*** $\mathrm{C}_G(a) = \{x \in G\colon\ xa = ax\}$.

תרגיל 7.2.2 (*) הראה ש־ $\mathrm{C}_G(a)$ היא תת־חבורה של G.

תרגיל 7.2.3 (*) $\mathrm{C}_G(a) = G$ אם ורק אם $a \in \mathrm{Z}(G)$.

תרגיל 7.2.4 (*) $\langle a \rangle \subseteq \mathrm{C}_G(a)$.

תרגיל 7.2.5 (*) $\bigcap_{a\in G} \mathrm{C}_G(a) = \mathrm{Z}(G)$.

תרגיל 7.2.6 (*) אם $\varphi : G \to H$ איזומורפיזם, אז $C_H(\varphi(x)) = \varphi(C_G(x))$.

תרגיל 7.2.7 (**) $\mathrm{C}_G(gxg^{-1}) = g \cdot \mathrm{C}_G(x) \cdot g^{-1}$.

תרגיל 7.2.8 (*) אם $H \leq G$ אז $\mathrm{C}_N(g) = N \cap \mathrm{C}_G(g)$.

תרגיל 7.2.9 (**) $g_1xg_1^{-1} = g_2xg_2^{-1}$ אם ורק אם $\mathrm{C}_G(x)g_1 = \mathrm{C}_G(x)g_2$.

תרגיל 7.2.10 (***) תהי G חבורה שבה $\mathrm{C}_G(x) = \langle x \rangle$ לכל $x \neq 1$. הוכח שלכל איבר ב־ G יש סדר ראשוני. תן דוגמא לחבורה כזו שאינה מסדר p^n.

תרגיל 7.2.11 (*) רשום את אברי המרכז של (123) ב־ S_3.

תרגיל 7.2.12 (**) רשום את אברי המרכז של (123) ב־ A_4.

תרגיל 7.2.13 (**) רשום את אברי המרכז של $(12)(34)$ ב־ S_4.

7.2.2 מרכֵּז של תת־חבורה

תהי $H \leq G$ תת־חבורה.

הגדרה 7.2.14 *המרכֵּז של H ב־G הוא* $\mathrm{C}_G(H) = \{g \in G : (\forall h \in H) gh = hg\}$.

תרגיל 7.2.15 (*) $\mathrm{C}_G(H)$ תת־חבורה של G.

תרגיל 7.2.16 (*) $\mathrm{Z}(H) = H \cap \mathrm{C}_G(H)$.

תרגיל 7.2.17 (*) $H \subseteq \mathrm{C}_G(H)$ אם ורק אם H אבלית.

תרגיל 7.2.18 (*) $\mathrm{Z}(G) = C_G(G)$.

תרגיל 7.2.19 (*) $\mathrm{C}_G(a) = \mathrm{C}_G(\langle a \rangle)$.

תרגיל 7.2.20 (*) $\mathrm{C}_G(H) = \bigcap_{a \in H} \mathrm{C}_G(a)$.

תרגיל 7.2.21 (**) $H\mathrm{C}_G(H)$ היא תמיד תת־חבורה של H.

תרגיל 7.2.22 (-)** אם $A \subseteq B$ אז $\mathrm{C}_G(B) \subseteq \mathrm{C}_G(A)$.

תרגיל 7.2.23 (**) $H \subseteq \mathrm{C}_G(\mathrm{C}_G(H))$.

תרגיל 7.2.24 (***) תהי $(\Gamma, \leq)$ קבוצה סדורה, עם פונקציה $\Psi : \Gamma \to \Gamma$ המקיימת את שתי האקסיומות הבאות:

1. אם $a \leq b$ אז $\Psi(a) \geq \Psi(b)$;
2. לכל $a \in \Gamma$, $a \leq \Psi^2(a)$,

אז $\Psi^3 = \Psi$.

תרגיל 7.2.25 (**) הסק מתרגילים 7.2.22, 7.2.23 ו־7.2.24 שלכל תת־חבורה $H \leq G$, $\mathrm{C}_G(\mathrm{C}_G(\mathrm{C}_G(H))) = \mathrm{C}_G(H)$.

תרגיל 7.2.26 (+*)** תהי $H \leq G$ תת־חבורה. הראה ש־

$$\mathrm{Z}(H) \cdot \mathrm{Z}(G) = H \cdot \mathrm{Z}(G) \cap \mathrm{C}_G(H).$$

7.3 מחלקות צמידות

הגדרה 7.3.1 *אברים* $x, y \in G$ *הם* **צמודים** *אם קיים* $g \in G$ *כך ש־* $y = gxg^{-1}$. *במקרה זה מסמנים* $x \sim y$.

תרגיל 7.3.2 (*) יחס הצמידות $\sim$ הוא יחס שקילות. (המחלקות נקראות מחלקות צמידות, ומסמנים אותן ב־$[x]$).

אין למחלקות הצמידות שום קשר ישיר עם הקוסטים שפגשנו בסעיף 4.2.

תרגיל 7.3.3 (*) $x \in \mathrm{Z}(G)$ אם ורק אם מחלקת הצמידות של x כוללת את x לבדו.

תרגיל 7.3.4 (*) בחבורה אבלית, יחס הצמידות טריוויאלי (כלומר, הוא יחס השוויון).

תרגיל 7.3.5 (+*) לכל $x,y \in G$, xy ו־yx צמודים.

תרגיל 7.3.6 (*) אם x,y צמודים, אז יש להם אותו סדר.

תרגיל 7.3.7 (+**) תן דוגמא לחבורה לא אבלית עם אברים מאותו סדר שאינם צמודים.

תרגיל 7.3.8 (*) תת־חבורה $H \leq G$ היא נורמלית אם ורק אם היא איחוד של מחלקות צמידות של G.

תרגיל 7.3.9 (**) מחלקות הצמידות ב־ A_4 (שהגדרנו בשאלה 4.2.11) הן בגדלים $1,3,4,4$. מצא כמה תת־חבורות נורמליות יש לה. מהו המרכז של איבר במחלקה מגודל 3?

לפי משפט לגרנז', הסדר של תת־חבורה מחלק תמיד את סדר החבורה. הכיוון ההפוך אינו נכון:

תרגיל 7.3.10 (**) ל־ A_4 אין תת־חבורה מסדר 6.

תרגיל 7.3.11 (**) לחבורה S_4 יש מחלקות צמידות בגדלים $1,3,6,6,8$. מהן תת־החבורות הנורמליות שלה ?

משפט 7.3.12 *לכל* $a \in G$, $|[a]|$ *שווה לאינדקס* $[G:\mathrm{C}_G(a)]$.

תרגיל 7.3.13 (-***) הוכח את המשפט. **הדרכה.** הגדר $f:G \to [a]$ לפי $f(x)=xax^{-1}$, וסיים בעזרת תרגיל 7.2.9.

תרגיל 7.3.14 (-**) מחלקת הצמידות של איבר a בחבורה היא בגודל 2. הוכח: יש לחבורה תת־חבורה נורמלית.

תרגיל 7.3.15 (***) החבורה $G=\mathrm{SL}_2(\mathbb{Z}_3)$ של מטריצות 2×2 מעל $\mathbb{Z}_3$ מדטרמיננטה 1, היא מסדר 24. א. מצא איבר $\neq 1$ במרכז של G.

ב. חשב את $\mathrm{C}_G(\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix})$, וזהה את החבורה עד כדי איזומורפיזם.

ג. קבע כמה מטריצות צמודות ל־$\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$. מה הפולינום המינימלי של כל אחת ואחת מהן?

תרגיל 7.3.16 (***) הוכח שבחבורה $\mathrm{GL}_2(\mathbb{Z})$, כל איבר מסדר 2 צמוד לאחת בדיוק מן המטריצות $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$, $\begin{pmatrix} 1 & 1 \\ 0 & -1 \end{pmatrix}$ ו־$\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$. הראה שמטריצות אלה אינן צמודות זו לזו. האם הטענה נכונה גם עבור $\mathrm{GL}_2(\mathbb{Q})$?

תרגיל 7.3.17 (**) אם $K \lhd A \lhd G$, אז A מכילה את כל הצמודים של K ב־ G.

תרגיל 7.3.18 (*) חשב את מחלקת הצמידות של $(g,h) \in G \times H$.

תרגיל 7.3.19 (***) א. חשב את תוחלת מספר הפתרונות למשוואה $xgx^{-1} = g'$ כאשר $g, g' \in G$ מקריות.
ב. חשב את תוחלת מספר הפתרונות למשוואה $xgx^{-1} = aga^{-1}$ כאשר $g, a \in G$ מקריות.

7.3.1 מחלקות צמידות ב־S_n

הגדרה 7.3.20 *תהי $\sigma \in S_n$ מכפלה של מחזורים זרים מאורכים $n_1, \dots, n_t$, כאשר $n_1 \leq \cdots \leq n_t$ ו־$n_1 + \cdots + n_t = n$.* ***מבנה המחזורים*** *של σ הוא הוקטור $[n_1, \dots, n_t]$. אם ערך מסויים חוזר על עצמו, נשתמש בסימון החזקה למען הקיצור.*

לדוגמא, מבנה המחזורים של הזהות הוא $[1, \dots, 1]$, או $[1^n]$. מבנה המחזורים של $(1234)(56)(78) \in S_9$ הוא $[4, 2^2, 1]$ (ולא $[4, 2^2]$ - המטרה היא שאפשר יהיה לקרוא את n מתוך מבנה המחזורים).

תרגיל 7.3.21 (+*) כתוב את כל מבני המחזורים האפשריים בחבורות S_3, S_4, ו־S_5.

תרגיל 7.3.22 (**) בתרגיל זה נמצא $\sigma \in S_8$ כך ש־ $\sigma(1234)(567) = (1246)(378)\sigma$.
א. נניח ש־ $\sigma(1) = 4$. חשב את $\sigma(2), \sigma(3), \sigma(4)$.
ב. נניח ש־ $\sigma(5) = 8$. חשב את $\sigma(5), \sigma(6)$.
ג. מצא את $\sigma(8)$.

תרגיל 7.3.23 (**) מצא $\sigma \in S_6$ כך ש־ $\sigma(12)(34) = (14)(35)\sigma$.

תרגיל 7.3.24 (**) כל התמורות הצמודות למחזור $(1 \cdots t)$ הם מחזורים מאורך t.

משפט 7.3.25 *תמורות הן צמודות ב־S_n אם ורק אם יש אותו מבנה מחזורים.*

תרגיל 7.3.26 (+**) הוכח את הכיוון הראשון של המשפט: תהי σ תמורה עם מבנה מחזורים $[n_1, \dots, n_t]$. הראה של־$\tau\sigma\tau^{-1}$ אותו מבנה מחזורים.

תרגיל 7.3.27 (***) הוכח את הכיוון השני: אם ל־σ ו־τ אותו מבנה מחזורים, אז הן צמודות. **הדרכה**. כתוב את התמורות זו מעל זו, בהתאמה למבנה המחזורים.

תרגיל 7.3.28 (*) מבני המחזורים ב־S_3 הם $[1^3]$, $[2,1]$, ו־$[3]$. מה הגודל של כל מחלקת צמידות ב־S_3 ?

תרגיל 7.3.29 (**) מצא את המחלקות ב־S_4 ואת הגודל של כל מחלקה.

תרגיל 7.3.30 (***) מצא את המחלקות ב־S_5 ואת הגודל של כל מחלקה.

תרגיל 7.3.31 (**) כמה דרכים יש להושיב שבעה אנשים סביב שולחנות עגולים שבאחד מהם שלושה מקומות ובשני ארבעה?

תרגיל 7.3.32 (**) כמה מחזורים מאורך r יש ב־ S_n?

תרגיל 7.3.33 (**) כמה צמודים יש ל־ $(123)(45)$ ב־ S_n?

תרגיל 7.3.34 (**) מצא את המרכז של $(12)(34)$ בחבורה S_5. הסק מהו $|[(12)(34)]|$.

תרגיל 7.3.35 (**) מצא את $C_{S_n}(\sigma)$ כאשר $\sigma = (1\,2\,3\,\cdots\,n)$. הדרכה. חשב את $|[\sigma]|$.

תרגיל 7.3.36 (***+) מצא שתי תת־חבורות H_1, H_2 אמיתיות של S_6, כך שכל איבר של S_6 צמוד לאיבר של אחת מהן. **הצעה.** קח $H_1 = S_5$ ו־$H_2 = \mathrm{Aut}(K_{3,3})$ (סעיף 8.1.3). (השווה לתרגיל 8.2.28).

7.3.2 מחלקות צמידות בתת־חבורה

יחס הצמידות תלוי בחבורה, ויתכן ש־$x, y \in H \leq G$ יהיו צמודים ב־G אבל לא ב־H.

תרגיל 7.3.37 (**) א. הראה ש־ $(1\,2\,3)$ ו־$(1\,3\,2)$ צמודים ב־ S_3 אבל אינם צמודים בתת־החבורה שהם יוצרים, $\langle(1\,2\,3)\rangle$.
ב. הראה ש־ $(1\,2\,3)$ ו־$(1\,2\,4)$ צמודים ב־ S_4 אבל לא בתת־החבורה A_4 (שהגדרנו בשאלה 4.2.11).

תרגיל 7.3.38 (**) אם $N \lhd G$ ו־Γ היא מחלקת צמידות של G החותכת באופן לא ריק את N, אז $\Gamma \subseteq N$.

תהי G חבורה עם תת־חבורה נורמלית N, ותהי Γ מחלקת צמידות של G, המוכלת ב־ N.

תרגיל 7.3.39 (*) Γ היא איחוד של מחלקות צמידות ב־ N.

תרגיל 7.3.40 (***+) אם $\Gamma = \Gamma_1 \cup \cdots \cup \Gamma_s$ כאשר Γ_i מחלקות של N, אז Γ_i שווי־גודל ו־$|\Gamma| = s \cdot |\Gamma_1|$.

כדי להבין כיצד מתפרקת Γ לאיחוד של מחלקות ב־N, נחשב גדלי מרכְּזים. נבחר $g \in \Gamma$. היזכר בתרגיל 7.2.8.

תרגיל 7.3.41 (***-) Γ מתפצלת ל־ $\frac{[G:N]}{[C_G(g):C_G(g)\cap N]}$ מחלקות צמידות של N. בפרט:
א. Γ מחלקת צמידות של N אם ורק אם $[G:N] = [\mathrm{C}_G(g):\mathrm{C}_G(g) \cap N]$.
ב. Γ מתפצל ל־ $[G:N]$ מחלקות לכל היותר.
ג. Γ מתפצל ל־ $[G:N]$ מחלקות אם ורק אם $\mathrm{C}_G(g) \subseteq N$.

תרגיל 7.3.42 (**) נסח את תרגיל 7.3.41 במקרה $[G:N] = 2$.

תרגיל 7.3.43 (**) הראה ש־$(123), (132)$ אינם צמודים ב־A_4. מצא את כל מחלקות הצמידות ב־ A_4.

7.4 שוויון המחלקות

שוויון המחלקות של חבורה G הוא השוויון

$$|G| = |\mathrm{Z}(G)| + \sum_{C \subseteq G, |C| \neq 1} |C|,$$

כאשר הסכום הוא על כל מחלקות הצמידות הלא־טריוויאליות של החבורה.

תרגיל 7.4.1 (**) הוכח את שוויון המחלקות. **הדרכה**. פרק את החבורה למחלקות צמידות, והעזר בתרגיל 7.3.3.

תרגיל 7.4.2 (*) אם G אבלית מסדר n, שוויון המחלקות שלה הוא $n = n$.

תרגיל 7.4.3 (**) כתוב את שוויון המחלקות של S_3 ושל S_4.

תרגיל 7.4.4 (**) כתוב את שוויון המחלקות של D_4 ושל חבורת הקווטרניונים Q.

תרגיל 7.4.5 (**) הראה ששוויון המחלקות של החבורה הדיהדרלית D_6 הוא $12 = 2+2+3+3+2$.

נזכיר שלפי משפט 7.3.12, הגודל של מחלקת צמידות מחלק את סדר החבורה, ולכן שוויון המחלקות הוא פירוק של $|G|$ לסכום של מחלקים של $|G|$.

תרגיל 7.4.6 (**) מצא את כל החבורות שיש להן בדיוק 2 מחלקות צמידות.

תרגיל 7.4.7 (***) א. הוכח שאם לחבורה יש בדיוק 3 מחלקות צמידות אז $G \cong \mathbb{Z}_3$ או $G \cong S_3$.
ב. אם לחבורה G יש בדיוק 4 מחלקות צמידות, אז $|G| \in 4, 8, 10, 12, 18, 20, 24, 42$.

תרגיל 7.4.8 (+***) תהי G חבורה לא אבלית מסדר pq, $p < q$.
א. $\mathrm{Z}(G) = 1$, ולכן שוויון המחלקות של G היא מהצורה $pq = 1 + \alpha p + \beta q$.
ב. במחלקות מגודל p יש אברים מסדר q, ולהיפך.
ג. (בכל חבורה) מספר האברים מסדר p מתחלק ב־ $(p-1)$.
ד. $\beta | (p-1)$(תרגיל 4.3.13), ולכן $\beta = p - 1$. מכאן ש־ $\alpha = (q-1)/p$. בפרט $q \equiv 1 \pmod{p}$.
ה. ל־G יש תת־חבורה יחידה מסדר q (ו־q תת־חבורות מסדר p).
(ראה תרגיל 10.2.7 להמשך תרגיל זה.)

7.4.1 חבורות־p

הגדרה 7.4.9 *יהי p ראשוני. **חבורת־p** (סופית) היא חבורה מסדר p^t ל־t כלשהו.*

התאוריה של חבורות p עשירה ומעניינת, ולא נוכל לגעת בה כאן אפילו על קצה המזלג. המשפט הבא הוא המשפט החשוב הראשון בנושא זה.

משפט 7.4.10 המרכז של חבורת־p אינו טריוויאלי.

תרגיל 7.4.11 (-***) הוכח את המשפט. **הדרכה**. שוויון המחלקות; הגודל של כל מחלקת צמידות הוא חזקה של p.

תרגיל 7.4.12 (**) כל חבורה מסדר p^2 היא אבלית. **הדרכה**. תרגיל 7.1.4.

תרגיל 7.4.13 (**) כל חבורה מסדר p^2 איזומורפית ל-$\mathbb{Z}_{p^2}$ או ל-$\mathbb{Z}_p \times \mathbb{Z}_p$. **הדרכה**. אם יש איבר מסדר p^2 סיימנו. אחרת קח שני איברים מסדר p, x, y, כך ש-$y \notin \langle x \rangle$, והראה ש-$G = \langle x, y \rangle \cong \mathbb{Z}_p \times \mathbb{Z}_p$.

פרק 8

אוטומורפיזמים

כדי לטפל בחבורה, אנחנו כותבים אותה באופן קונקרטי. באותה עת, חשוב להבין עד כמה אופן הכתיבה שבחרנו הוא מחוייב המציאות: באיזו מידה אפשר, כביכול, להחזיק את החבורה בזווית אחרת, בלי לשנות את התמונה. סימטריות כאלו נקראות אוטומורפיזמים.

מושגים: אוטומורפיזם, אוטומורפיזם פנימי. חבורת האוטומורפיזמים, חבורת האוטומורפיזמים הפנימיים, חבורת האוטומורפיזמים החיצוניים. גרף קיילי. המנרמל. משפט N/C. תת־חבורות צמודות. תת־חבורה קרקטריסטית. חבורה פשוטה.

8.1 חבורת האוטומורפיזמים

הגדרה 8.1.1 *איזומורפיזם מחבורה אל עצמה נקרא* ***אוטומורפיזם****.*

הגדרה 8.1.2 *אוסף האוטומורפיזמים של חבורה G נקרא '****חבורת האוטומורפיזם של G****', ומסמנים אותו בסימון $\mathrm{Aut}(G)$.*

תרגיל 8.1.3 (*) $\mathrm{Aut}(G)$ היא אכן חבורה.

גם חבורת האוטומורפיזמים של חבורה למחצה היא חבורה. למעשה אפשר להגדיר חבורת אוטומורפיזמים למבנים רבים אחרים; זהו מקור חשוב נוסף לדוגמאות של חבורות.

תרגיל 8.1.4 (*) נסח את תרגיל 5.2.5 עבור אוטומורפיזמים.

תרגיל 8.1.5 (**) נניח שחבורה G נוצרת על־ידי t יוצרים. הראה ש־ $|\mathrm{Aut}(G)| \leq |G|^t$.

תרגיל 8.1.6 (**) הוכח ש־ $\mathrm{Aut}(\mathbb{Z}_n) \cong U_n$. **הדרכה.** הגדר $\Phi\colon \mathrm{Aut}(\mathbb{Z}_n) \to U_n$ לפי $\Phi(\phi) = \phi(1)$.

תרגיל 8.1.7 (**) $\mathrm{Aut}(\mathbb{Z}_2 \times \mathbb{Z}_2) \cong S_3$.

תרגיל 8.1.8 (-**) $\mathrm{Aut}(\mathbb{Z}) \cong \mathbb{Z}_2$.

תרגיל 8.1.9 (+**) הוכח שחבורת האוטומורפיזמים של $\mathbb{Z}_p^n$ היא חבורת המטריצות $\mathrm{GL}_n(\mathbb{Z}_p)$ (ראה תת־סעיף 3.3.5). **הדרכה**. הומומורפיזם של החבורה $\mathbb{Z}_p^n$ אינו אלא העתקה ליניארית של $\mathbb{Z}_p^n$ לעצמו, כמרחב וקטורי מעל השדה $\mathbb{Z}_p$.

תרגיל 8.1.10 (***) תהי G חבורה סופית, ויהי $\varphi \in \mathrm{Aut}(G)$ אוטומורפיזם ללא נקודות שבת, כלומר, $\varphi(g) \neq g$ לכל $g \neq 1$.
א. הוכח. לכל g קיים x כך ש $g = x^{-1}\varphi(x)$.
ב. אם $\varphi \circ \varphi = I_G$, אז G אבלית.

תרגיל 8.1.11 (**) אם $(|G|, |H|) = 1$, אז $\mathrm{Aut}(G \times H) \cong \mathrm{Aut}(G) \times \mathrm{Aut}(H)$.

תרגיל 8.1.12 (**) הוכח ש־ $\mathrm{Aut}(S_3) \cong S_3$.

תרגיל 8.1.13 (***) הוכח ש־ $\mathrm{Aut}(S_4) \cong S_4$.

תרגיל 8.1.14 (***) הוכח ש־ $\mathrm{Aut}(A_4) \cong S_4$.

תרגיל 8.1.15 (+**) הראה ש־ $|\mathrm{Aut}(\mathbb{Z}_4 \times \mathbb{Z}_4)| = 96$. **הדרכה**. מצא התאמה (שאינה הומומורפיזם) $\mathrm{Aut}(\mathbb{Z}_4 \times \mathbb{Z}_4) \hookrightarrow \mathrm{M}_2(\mathbb{Z}_4)$.

תרגיל 8.1.16 (***) חשב את $\mathrm{Aut}(\mathbb{Z}_2 \times \mathbb{Z}_4)$.

תרגיל 8.1.17 (+**) הוכח ש־ $\mathrm{Aut}(\mathbb{Z}_2 \times \mathbb{Z}) \cong \mathbb{Z}_2 \times \mathbb{Z}_2$. **הדרכה**. מהם האיברים מסדר 2 של $\mathbb{Z}_2 \times \mathbb{Z}$?

תרגיל 8.1.18 (**) בחבורה G יש שני אברים a, b ואוטומורפיזם $\varphi : G \to G$ כך ש־ $\varphi(x) = x$ לכל $x \neq a, b$. מצא את G, φ ו־$\{a, b\}$.

תרגיל 8.1.19 (+**) יהי $\varphi : G \to G$ אוטומורפיזם לא טריוויאלי של חבורה סופית. הראה שלפחות מחצית מאברי החבורה מקיימים $\varphi(x) \neq x$.

8.1.1 אוטומורפיזמים פנימיים

לא תמיד קל לבנות ולגלות אוטומורפיזמים. עם זאת, יש אוטומורפיזמים שהחבורה תורמת במו ידיה, והם קושרים אל חבורת האוטומורפיזמים מושגים שפגשנו בפרקים הקודמים.

הגדרה 8.1.20 *לכל* $g \in G$*, נגדיר* $\gamma_g : G \to G$ *לפי* $\gamma_g(h) = ghg^{-1}$. γ_g *נקרא* **אוטומורפיזם פנימי**, *או* **אוטומורפיזם של הצמדה**.

תרגיל 8.1.21 (*) $\gamma_g \in \mathrm{Aut}(G)$.

תרגיל 8.1.22 (+*) $\gamma_g \circ \gamma_h = \gamma_{gh}$.

תרגיל 8.1.23 (+*) מצא תנאי הכרחי ומספיק לכך ש־ $\gamma_g = \gamma_h$.

תרגיל 8.1.24 (−***) נגדיר $\Gamma : G \to \mathrm{Aut}(G)$ לפי $\Gamma(g) = \gamma_g$.
א. הוכח ש־ Γ הומומורפיזם.
ב. הראה ש־ $\mathrm{Ker}\,\Gamma = \mathrm{Z}(G)$, והסק ש־ $\mathrm{Inn}(G) \cong G/\mathrm{Z}(G)$.

תרגיל 8.1.25 (*) לכל $\varphi \in \mathrm{Aut}(G)$ ו־$g \in G$, $\varphi \circ \gamma_g \circ \varphi^{-1} = \gamma_{\varphi(g)}$.
הסק ש־$\mathrm{Inn}(G) = \{\gamma_g : g \in G\}$ היא תת־חבורה נורמלית של $\mathrm{Aut}(G)$.

תרגיל 8.1.26 (-***) $\varphi \in \mathrm{C}_{\mathrm{Aut}(G)}(\mathrm{Inn}(G))$ אם ורק אם $\alpha(g) = \varphi(g)g^{-1}$ הוא הומומורפיזם $\alpha : G \to \mathrm{Z}(G)$.

תרגיל 8.1.27 (**) אם $\mathrm{Z}(G) = 1$ אז $\mathrm{Aut}(G) \leq \mathrm{Inn}(G) \cong G$. הוכח שבמקרה זה $\mathrm{C}_{\mathrm{Aut}(G)}(\mathrm{Inn}(G)) = 1$, ובפרט גם $\mathrm{Z}(\mathrm{Aut}(G)) = 1$. *כך אפשר, לכאורה, לבנות סדרה עולה של חבורות שהמרכז שלהן טריוויאלי. לפי משפט של* Wielandt, 1939*, המגדל הזה מסתיים אחרי מספר סופי של צעדים.*

הגדרה 8.1.28 $\mathrm{Out}(G) = \mathrm{Aut}(G)/\mathrm{Inn}(G)$ *נקראת* **חבורת האוטומורפיזמים החיצוניים** *של* G *למרות שאיבריה אינם אוטומורפיזמים.*

8.1.2 העלאה בחזקה

לחבורה יש 'יותר' אוטומורפיזמים של הצמדה ככל שהיא 'פחות' אבלית, וכאשר החבורה אבלית אין בכלל אוטומורפיזמים כאלה. מאידך, יש מקור אספקה אחר לאוטומורפיזמים של לחבורות אבליות, שחשיבותו תתברר כשנחקור את המבנה של החבורות האלה.

הגדרה 8.1.29 *לכל* $m \in \mathbb{Z}$*, נסמן* $\mu_m : G \to G$ *לפי* $\mu_m : g \mapsto g^m$.

ההנחה ש־μ_m היא הומומורפיזם היא תכונה φ_m מתרגיל 3.4.8; התכונה אינה מתקיימת בכל חבורה.

תרגיל 8.1.30 (*) אם G אבלית אז $\mu_m : G \to G$ היא הומומורפיזם.

תרגיל 8.1.31 (**) אם G אבלית ו־$(m, |G|) = 1$, אז $\mu_m \in \mathrm{Aut}(G)$ (השווה לתרגיל 9.1.9: μ_m חד־חד־ערכית גם אם אין מניחים אבליות).

בפרט כדאי לשים לב לאוטומורפיזם $\mu_{-1} : g \mapsto g^{-1}$. מתי הוא טריוויאלי?

תרגיל 8.1.32 (**) אם קיים g כך ש $\gamma_g(x) = x^{-1}$ לכל x, אז G אבלית.

תרגיל 8.1.33 (***) הראה שחבורת האוטומורפיזמים של חבורה סופית לעולם אינה טריוויאלית. **רמז.** חשוב על $\mathrm{Inn}(G)$, $x \mapsto x^{-1}$ ו־$\mathrm{GL}_n(\mathbb{Z}_2)$ מתרגיל 8.1.9.

תרגיל 8.1.34 (***) הראה שבלתי אפשרי כי $\mathrm{Aut}(G) \cong \mathbb{Z}_3$.

8.1.3 אוטומורפיזמים של גרפים

תלמידי 89-214 *מוזמנים לדלג על הסעיף.*

תהי V קבוצה. גרף על V הוא אוסף של זוגות סדורים על אברי V.
אוטומורפיזם של הגרף הוא תמורה $\sigma \in S_V$, המעבירה את קבוצת הזוגות לעצמה.
לדוגמא, חבורת האוטומורפיזמים של הגרף הריק על n נקודות היא S_n.

תרגיל 8.1.35 (**) חבורת האוטומורפיזמים של טבעת על n נקודות היא D_n.

תרגיל 8.1.36 (*) חבורת האוטומורפיזמים של גרף שווה לחבורת האוטומורפיזמים של הגרף המשלים.

תרגיל 8.1.37 (***) כתוב את כל הטריאנגולציות האפשריות של משושה משוכלל (יש 14 כאלה), וחבר בקשת כל זוג טריאנגולציות שניתן לעבור ביניהן על־ידי הזזת קו אחד. מצא את חבורת האוטומורפיזמים של הגרף המתקבל (הוכח ש־ S_3 היא חבורת מנה שלה).

אם מוגדרים כמה גרפים (נאמר, בצבעים שונים) על אותן נקודות, חבורת האוטומורפיזמים של המבנה היא החבורה של תמורות של הקודקודים, שהן אוטומורפיזמים של כל אחד ואחד מהגרפים.

תהי G חבורה עם יוצרים $g_1,\dots,g_t$. נבנה t גרפים על הקבוצה G: לכל i, הגרף T_i כולל את הזוגות (x,xg_i) לכל $x \in G$. מבנה זה נקרא **גרף קיילי** של G (ביחס ליוצרים $g_1,\dots,g_t$).

תרגיל 8.1.38 (**) צייר את גרף קיילי של S_3 ביחס ליוצרים $(12),(123)$ וביחס ליוצרים $(12),(23)$.

תרגיל 8.1.39 (***) צייר את גרף קיילי של החבורה הנוצרת על־ידי שני אברים x,y, המקיימים את היחסים $x^3=y^3=(xy)^2=1$.

תרגיל 8.1.40 (***) הוכח ש־G היא חבורת האוטומורפיזמים של גרף קיילי של G.

תרגיל 8.1.41 (***) צייר חלק מספיק גדול של גרף קיילי של החבורה $G=\langle x,y,z\rangle$ המוגדרת על־ידי היחסים $x^2=y^2=z^2=(xy)^3=(yz)^3=(zx)^3=1$, על־מנת להשתכנע שהחבורה אינסופית.

8.2 המנרמל

תהי H תת־חבורה של G.

תרגיל 8.2.1 (*) $H \lhd G$ אם ורק אם $\gamma_g(H)=H$ לכל $g \in G$.

הגדרה 8.2.2 ***המנרמל של H ב־G הוא*** $\mathrm{N}_G(H)=\{g\in G: gHg^{-1}=H\}$.

תרגיל 8.2.3 (*) $\mathrm{N}_G(H)$ היא תמיד תת־חבורה של G.

תרגיל 8.2.4 (*) $H \lhd \mathrm{N}_G(H)$.

תרגיל 8.2.5 (+*) $\mathrm{N}_G(H)$ היא תת־החבורה הגדולה ביותר של G שבה H נורמלית. יתרה מזו, אם $H \le H' \le G$, אז $H \lhd H'$ אם ורק אם $H' \subseteq \mathrm{N}_G(H)$.

תרגיל 8.2.6 (*) $H \lhd G$ אם ורק אם $\mathrm{N}_G(H)=G$.

תרגיל 8.2.7 (+*) $\mathrm{C}_G(H) \le \mathrm{N}_G(H)$.

תרגיל 8.2.8 (*) אם $H \subseteq K \subseteq G$, אז $\mathrm{N}_K(H)=\mathrm{N}_G(H)\cap K$.

תרגיל 8.2.9 (**) אם $K \subseteq H \le G$, $K \lhd G$, אז $\mathrm{N}_{G/K}(H/K)=\mathrm{N}_G(H)/K$.

נסמן $\mathrm{N}^0_G(H) = \{x \in G : xHx^{-1} \subseteq H\}$.

תרגיל 8.2.10 (*) תמיד $N^0_G(H) \subseteq \mathrm{N}_G(H)$. בנוסף לזה $\mathrm{N}^0_G(H)$ סגורה לכפל, ולכן היא תת־מונויד של $\mathrm{N}_G(H)$.

תרגיל 8.2.11 (**) הראה שאם H סופית, אז $\mathrm{N}^0_G(H) = \mathrm{N}_G(H)$.

תרגיל 8.2.12 (**) לכל תת־חבורה $A \leq G$, $A \subseteq \mathrm{N}_G(H)$ אם ורק אם $A \subseteq \mathrm{N}^0_G(H)$.

תרגיל 8.2.13 (***) תן דוגמא לחבורות אינסופיות $H \leq G$ כך ש־ $\mathrm{N}^0_G(H)$ אינה (סגורה להיפוך ולכן אינה) חבורה.

משפט 8.2.14 (משפט N/C) תהי $H \leq G$. קיים שיכון $N_G(H)/\mathrm{C}_G(H) \hookrightarrow \mathrm{Aut}(H)$.

תרגיל 8.2.15 (+)** הוכח את המשפט. **הדרכה**. הגדר $\varphi\colon N_G(H) \to \mathrm{Aut}(H)$ לפי $\varphi :$ $g \mapsto \gamma_g$. הוכח שהפונקציה הזו מוגדרת היטב (לשם כך הגדרנו את המנרמל!), וחשב את הגרעין שלה.

תרגיל 8.2.16 (+*) מה אומר משפט N/C במקרה $H = G$?

תרגיל 8.2.17 (**) תהי G חבורת־p עם תת־חבורה נורמלית H מסדר p. הוכח ש־ $H \subseteq \mathrm{Z}(G)$. **רמז**. משפט N/C.

תרגיל 8.2.18 (**) תהי G חבורה מסדר mp, כאשר $(p, m) = 1$ ו־$(p-1, m) = 1$. הוכח שאם $P \lhd G$ תת־חבורה נורמלית מסדר p, אז היא מרכזית. **הדרכה**. משפט N/C עם P.

תרגיל 8.2.19 (***) קח $G = \mathrm{GL}_n(F)$ כאשר F שדה. נסמן ב־B את חבורת המטריצות המשולשיות־עליונות.

1. הראה ש־$U = [B, B]$ היא חבורת המטריצות המשולשות עם אלכסון $1, \dots, 1$.
2. הראה ש־B/U איזומורפית לחבורת המטריצות הסקלריות T.
3. הראה ש־$B = UT$.
4. חשב את $\mathrm{N}_G(T)$.
5. הוכח ש־$W = \mathrm{N}_G(T)/T \cong S_n$.

תרגיל 8.2.19 הוא הצעד הראשון בתורת החבורות האלגבריות: G היא "חבורה אלגברית רדוקטיבית", B "תת־חבורת בורל" שלה (שהיא "תת־חבורה פתירה מקסימלית", ויחידה עד־כדי הצמדה), U היא "הרדיקל היוניפוטנטי", ו־W "חבורת וייל" של G.

8.2.1 תת־חבורות צמודות

הזכר בתרגיל 5.3.1, שלפיו כל תת־חבורה $H \leq G$ מוקפת ב'ענן' של תת־חבורות צמודות מהצורה gHg^{-1}. אלו תת־החבורות **הצמודות** ל־H.

תרגיל 8.2.20 (*) אם H_1, H_2 צמודות, אז הן איזומורפיות.

תרגיל 8.2.21 (+**) תן דוגמא לתת־חבורות איזומורפיות של חבורה G שאינן צמודות.

תרגיל 8.2.22 (*) $N_G(gHg^{-1}) = gN_G(H)g^{-1}$.

תרגיל 8.2.23 (*) $\mathrm{C}_G(gHg^{-1}) = g\mathrm{C}_G(H)g^{-1}$ (השווה לתרגיל **??**).

תרגיל 8.2.24 (**) $\mathrm{C}_G(H) \lhd N_G(H)$.

משפט 8.2.25 *מספר תת־החבורות של G הצמודות ל־H שווה ל־$[G\,:\,\mathrm{N}_G(H)]$.*

השווה למשפט 7.3.12.

תרגיל 8.2.26 (**) הראה ש־$g_1Hg_1^{-1} = g_2Hg_2^{-1}$ אם ורק אם $N_G(H)g_1 = N_G(H)g_2$. הוכח את המשפט **הדרכה**. הגדר פונקציה מ־G על אוסף החבורות הצמודות ל־H.

תרגיל 8.2.27 (**) $\left|\bigcup_{x\in G} xHx^{-1}\right| \leq |H| \cdot [G\,:\,\mathrm{N}_G(H)]$.

תרגיל 8.2.28 (***) תהי G חבורה סופית עם תת־חבורה אמיתית H. הוכח שלא יתכן כי $G = \bigcup gHg^{-1}$.

פרק 9

חבורות של תמורות

חבורות של תמורות הן אחת הדוגמאות החשובות ביותר, גם מבחינה תאורטית וגם בשימושים של תורת החבורות הסופיות. שאלות רבות בקומבינטוריקה ובאלגוריתמים הקשורים במבנים קומבינטוריים אפשר לתרגם לשפה של החבורות הסימטריות.

מושגים: משפט קיילי, העידון שלו. סימן של תמורה. חבורת התמורות הזוגיות. הלמה של Burnside.

9.1 משפט קיילי

בסעיף זה נראה שכל חבורה היא למעשה חבורה של תמורות.

תרגיל 9.1.1 (**) מצא הצגה של D_4 כחבורת תמורות (חשוב על פינות הריבוע).

משפט 9.1.2 (משפט קיילי) ***כל חבורה G איזומורפית לתת־חבורה של החבורה הסימטרית S_G.***

זכור (תרגיל 3.3.22) שאם G חבורה סופית, מסדר n, אז $S_G \cong S_n$. כלומר, המשפט נותן שיכון $G \hookrightarrow S_n$, כאשר $n = |G|$.

תרגיל 9.1.3 (**) הוכח את המשפט. **הדרכה**. הגדר $\Psi : G \to S_G$ לפי $\Psi(g) : x \mapsto gx$. הראה ש־$\Psi(gh) = \Psi(g)\Psi(h)$ והסק ש־Ψ מוגדרת היטב *כלומר, בהקשר הנוכחי, היא מחבירה תמורות ולא סתם פונקציות $G \to G$*.

תרגיל 9.1.4 (*) הצג את החבורות $\mathbb{Z}_4$ ו־U_8 כתת־חבורות של S_4.

תרגיל 9.1.5 (**) הצג את U_9 כתת־חבורה של S_6.

תרגיל 9.1.6 (**) הצג את S_3 כתת־חבורה של S_6, כך שלאף איבר מלבד הזהות אין נקודות שבת.

תרגיל 9.1.7 (***) הצג את חבורת הקווטרניונים Q כתת־חבורה של S_8, והראה שהיא אינה ניתנת לשיכון ב־S_7.

תרגיל 9.1.8 (+*) הראה ש־$\mathrm{Aut}(G) \leq S_G$.

תרגיל 9.1.9 (-*)** תהי G חבורה ו־m מספר זר ל־$|G|$. הוכח שההעתקה $g \mapsto g^m$ היא חד־חד־ערכית ועל. (זהו הומומורפיזם אם החבורה אבלית, אבל במקרה הכללי תרגיל 5.2.3 אינו חל.) **הדרכה**. העזר בשיכון של G לחבורת תמורות.

תרגיל 9.1.10 (***) מצא את כל החבורות G שעבורן התמונה של שיכון קיילי ב־S_G היא תת־חבורה נורמלית. **הדרכה**. התמונה נורמלית אם ורק אם $\forall a \forall \sigma \exists b : \sigma \ell_a = \ell_b \sigma$, כלומר $\forall a \forall \sigma \exists b \forall x : \sigma(ax) = b\sigma(x)$; הראה שמזה נובע $\forall a \forall \sigma \forall x : \sigma(ax) = \sigma(a)\sigma(1)^{-1}\sigma(x)$; בחר $\sigma = (1t)$ כדי להראות ש־$|G| \leq 4$; זה נובע כמובן גם ממשפט 9.2.36.

9.1.1 העידון של משפט קיילי

אם G חבורה גדולה, משפט קיילי המספק שיכון שלה ל־$S_{|G|}$ אינו נוח ואינו יעיל. **נניח שיש** ל־G תת־חבורה H, מאינדקס n.

תרגיל 9.1.11 (+*)** נסמן ב־ G/H את אוסף הקוסטים $\{xH\}$ (גם כאשר H אינה נורמלית). הראה שהפונקציה $\Psi : G \to S_{G/H}$ המוגדרת כך ש־ $\Psi(g)$ הוא הפונקציה $G/H \to G/H$ המוגדרת לפי $\Psi(g) : (xH) \mapsto (gx)H$, מגדירה הומומורפיזם $G \to S_{G/H}$.

תרגיל 9.1.12 (**) הראה ש־ $\mathrm{Ker}(\Psi) = \mathrm{Core}_G(H)$ (ראה תרגיל 5.3.13).

משפט 9.1.13 (העידון של משפט קיילי) *אם G חבורה ו־H תת־חבורה שלה מאינדקס n, אז יש שיכון $G/\mathrm{Core}_G(H) \hookrightarrow S_n$.*

תרגיל 9.1.14 (**) הוכח את המשפט. **הדרכה**. תרגילים 9.1.11, 9.1.12.

תרגיל 9.1.15 (-*)** אם יש ל־G תת־חבורה H מאינדקס n, אז יש לה תת־חבורה נורמלית מאינדקס המחלק את $n!$ (המוכלת ב־H).

חבורה שאין לה תת־חבורות נורמליות נקראת **פשוטה**.

תרגיל 9.1.16 (**) כל חבורה פשוטה עם תת־חבורה מאינדקס n היא תת־חבורה של S_n.

תרגיל 9.1.17 (**) אם יש לחבורה G תת־חבורה מאינדקס n אבל הסדר של G אינו מחלק את $n!$, אז G אינה פשוטה.

תרגיל 9.1.18 (-*)** תהי $G \leq H$ תת־חבורה מאינדקס p, כאשר p הראשוני הקטן ביותר המחלק את $|G|$. הוכח ש־$H \triangleleft G$.

תרגיל 9.1.19 (-*)** G חבורה סופית פשוטה עם תת־חבורה H. הוכח ש־ $\log|G| \leq [G:H]^2$. מצא את החסם על $[G:H]$ אם $|G| = 2^{30}$.

9.2 הסימן של תמורה

תהי $\sigma \in S_n$ תמורה. נאמר שהזוג (i,j) **מפר־סדר** אם $i < j$ ו־$\sigma i > \sigma j$.

הגדרה 9.2.1 הסימן *של $\sigma \in S_n$ מוגדר לפי הזוגיות של מספר הפרות הסדר ביחס ל־σ:* $\mathrm{sgn}(\sigma) = (-1)^{|\{i,j:\ i<j, \sigma i > \sigma j\}|}$.

טענה 9.2.2 העתקת הסימן $\mathrm{sgn}: S_n \to \{\pm 1\}$ היא הומומורפיזם.

תרגיל 9.2.3 (+)** הוכח את טענה 9.2.2, כלומר, הראה ש־$\mathrm{sgn}(\sigma\tau) = \mathrm{sgn}(\sigma)\mathrm{sgn}(\tau)$.
הדרכה. חלק את הזוגות (i,j) שבהם $i < j$ לארבע קבוצות, לפי התכונות $\tau(i) < \tau(j)$ ו־$\sigma\tau(i) < \sigma\tau(j)$, וחשב את התרומה של כל זוג לכל אחד מהסימנים.

תרגיל 9.2.4 (**) יהי $\tau = (ab)$ חילוף. הוכח ש־ $\mathrm{sgn}(\tau) = -1$. בפרט, sgn היא על, לכל $n \geq 2$.

9.2.1 הסימן והדיסקרימיננטה

נתבונן בפולינום $\Delta(x_1,\dots,x_n) = \prod_{1\leq i<j\leq n}(x_i - x_j)$ במשתנים $x_1,\dots,x_n$.

תרגיל 9.2.5 (*+) כתוב את $\Delta_3(x,y,z)$ כסכום של מונומים. השווה את התוצאה ל־ $\Delta_3(x,z,y)$.

תרגיל 9.2.6 (**) הראה שלכל $\sigma \in S_n$, $\Delta(x_{\sigma(1)},\dots,x_{\sigma(n)}) = \pm\Delta(x_1,\dots,x_n)$.
הדרכה. חשוב על הגורמים $(x_i - x_j)$.

תרגיל 9.2.7 (**) $\Delta(x_{\sigma(1)},\dots,x_{\sigma(n)}) = \mathrm{sgn}(\sigma)\Delta(x_1,\dots,x_n)$.

תרגיל 9.2.8 (+)** הוכח את טענה 9.2.2 מתרגיל 9.2.7.

9.2.2 חבורת התמורות הזוגיות

בתרגיל 4.1.19 ראינו שכל תמורה אפשר לכתוב כמכפלה של חילופים.

טענה 9.2.9 הזוגיות של מספר החילופים בהצגה של תמורה σ היא קבועה. כלומר, אם $\sigma = \tau_1\cdots\tau_k = \nu_1\cdots\nu_t$ (כאשר τ_i, ν_j חילופים), אז $k \equiv t \pmod 2$.

תרגיל 9.2.10 (+)** הוכח את הטענה. **הדרכה.** $sgn(\sigma) = (-1)^k = (-1)^t$.

תרגיל 9.2.11 (*) מצא את הסימן של המכפלה $(1\ 2\ 3)(2\ 4\ 5)(1\ 4\ 3\ 5)$.

תרגיל 9.2.12 (*) כתוב את המחזור $(a_1a_2\cdots a_t)$ כמכפלה של חילופים ומצא את הסימן שלו.

כעת אפשר להגדיר את תת־החבורה החשובה ביותר של חבורת הסימטריות:

הגדרה 9.2.13 $A_n = \mathrm{Ker}(\mathrm{sgn})$ *היא* **חבורת התמורות הזוגיות.** התמורות נקראות כך על־שם מספר החילופים בהצגות שלהן.

תרגיל 9.2.14 (*) $A_2 = 1$, $A_3 = \langle(123)\rangle$.

תרגיל 9.2.15 (*) $[S_n : A_n] = 2$.

תרגיל 9.2.16 (**) תן שלושה נימוקים לכך ש־$A_n \lhd S_n$. **הדרכה.** האינדקס שלה הוא 2; היא גרעין של הומומורפיזם; וכן ישירות מן ההגדרה.

תרגיל 9.2.17 (**) חשב את $\langle(1234),(13)\rangle \cap A_4$.

תרגיל 9.2.18 (**) אם G תת־חבורה של S_n שאינה מוכלת ב־A_n, אז $A_nG = S_n$ ו־$[G:A_n \cap G] = 2$.

תרגיל 9.2.19 (*) מה גודלה של מחלקת הצמידות של $(123)(45)$ ב־ A_5?

תרגיל 9.2.20 (**) האם כל שני אברים מסדר 7 ב־ A_7 הם צמודים? מה בדבר כל שני אברים מסדר 2? כל שני אברים מסדר 3?

תרגיל 9.2.21 (-*)** הראה שכל האברים מהצורה $(ab)(cd)$ צמודים זה לזה ב־A_n.
הדרכה. בדוק שתמורות σ,σ' בעלות מבנה המחזורים הזה הן צמודות כאשר התומכים שווים, וכאשר הם נבדלים בנקודה אחת. הסבר מדוע זה מספיק.

תרגיל 9.2.22 (***) נניח $n \geq 5$. הראה שכל המחזורים מהצורה (abc) צמודים זה לזה ב־A_n. **הדרכה**. נראה שמחלקת הצמידות של (123) ב־A_n כוללת את כל המחזורים באורך 3. $(145) = (123)^{(24)(35)}$ מראה שאפשר לעבור למחזור נתון לכל מחזור עם נקודה משותפת אחת, ואז $(214),(124) \sim (345) \sim (123)$. לכן גם $(132) \sim (124) \sim (123)$ ו־$(456) \sim (124) \sim (123)$.

השווה לתרגיל 7.3.43, והסבר מדוע הנימוק של תרגיל 9.2.22 אינו תקף שם.

תרגיל 9.2.23 (-)** במחלקת הצמידות של $(ab)(cd)$ ב־A_n יש $\frac{n(n-1)(n-2)(n-3)}{8}$ אברים. **הדרכה**. תרגיל 9.2.21 מעביר את הבעיה למחלקות ב־S_n.

תרגיל 9.2.24 (**) מצא שיכון של S_n ב־ A_{n+2}.

תת־חבורה של חבורה סופית G שהסדר שלה שווה לחזקה המקסימלית של 2 המחלקת את $|G|$ נקראת חבורת 2־סילו של G (לפי משפטי סילו, תמיד יש תת־חבורות כאלה, אבל לא נוכיח זאת כאן).

תרגיל 9.2.25 (***) הוכח שהשיכון $G \hookrightarrow S_n$ שמספק משפט קיילי הוא למעשה לתוך A_n אם ורק אם אין ל־G חבורה 2־סילו ציקלית.

תרגיל 9.2.26 (***) נניח שלחבורה G יש חבורת 2־סילו ציקלית.

1. הוכח שיש ל־G תת־חבורה מאינדקס 2.
2. הראה שגם לתת־חבורה זו יש חבורת 2־סילו ציקלית.
3. הסק שיש שרשרת של תת־חבורות $G = G_0 \rhd G_1 \rhd \cdots \rhd G_t$ כך שהאינדקסים $[G_i:G_{i+1}] = 2$ ו־$|G_t|$ אי־זוגי.

9.2.3 יוצרים של A_n

הזכר בתת־סעיף **??**.

תרגיל 9.2.27 (*) תהי $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 5 & 3 & 6 & 1 & 4 & 7 & 2 \end{pmatrix}$. כתוב את σ כמכפלה של חילופים מהצורה $(1\,i)$, וקבע אם σ זוגית או אי־זוגית.

תרגיל 9.2.28 (**) הוכח מן ההגדרה ש־A_n נוצרת על־ידי כל התמורות עם מבנה המחזורים של $(12)(34)$, (123).

תרגיל 9.2.29 (**) $(5 \le n)$ A_n נוצרת על־ידי כל התמורות מהצורה $(ij)(kl)$, i,j,k,l שונים.

תרגיל 9.2.30 (***) A_n נוצרת על־ידי כל המחזורים מאורך 3. **הדרכה**. חשב את $(ijk)(jkt)$.

9.2.4 A_n חבורה פשוטה

תרגיל 9.2.31 (**+) הראה שמחלקות הצמידות ב־ A_5 הן בגדלים $1, 10, 10, 15, 24$, והסק שהיא פשוטה.

תרגיל 9.2.32 (***) תת־החבורה הנורמלית היחידה של S_5 היא A_5. **הדרכה**. תת־חבורה נורמלית היא איחוד של מחלקות צמידות.

שני המשפטים הבאים קרובים ברוחם זה לזה, ואכן אפשר, במאמץ מסויים, להסיק אותם זה מזה (הראשון מעט קשה יותר, משום שהוא מאפשר להצמיד רק בתמורות זוגיות). אנו מספקים לשניהם גם הוכחות ישירות.

משפט 9.2.33 *A_n פשוטה לכל* $n \ge 5$.

תרגיל 9.2.34 (***+) נניח $n \ge 5$. כל תת־חבורה נורמלית לא־טריוויאלית של A_n כוללת מחזור באורך 3. **הדרכה**. יחד עם כל איבר $\sigma \in N$, N כוללת גם כל איבר מהצורה $[\sigma, \tau] = \sigma\tau\sigma^{-1}\tau^{-1}$ $(\tau \in A_n)$. נבחר תמיד τ שאינו נוגע במחזורים ה'אחרים', כך שהם יעלמו בקומוטטור. אם יש ל־N $\sigma \in N$ מחזור $(12\ldots m)$, $m \ge 4$, חשב את $(12\ldots m)(213\ldots m)^{-1}$. אם $\sigma = (123)(456)\cdots$, $[\sigma, (243)] = (15243)$. אם $\sigma = (12)(34)(5)\cdots$, $[\sigma, (254)] = (13425)$. אם $\sigma = (123)(45)\cdots$, $[\sigma, (345)] = (15)(34)(2)$. ואם $\sigma = (12)(34)(56)\cdots$ אז $[\sigma, (264)] = (135)(264)$.

תרגיל 9.2.35 (**) הוכח את משפט 9.2.33. **פתרון**. אם $1 \ne N \lhd A_n$ אז לפי תרגיל 9.2.34 יש ב־N מחזור באורך 3. לפי תרגיל 9.2.22 N כוללת את כל המחזורים באורך 3, ולפי תרגיל 9.2.30, $N = A_n$.

משפט 9.2.36 *נניח* $5 \le n$. *תת־החבורה הנורמלית היחידה של* S_n *היא* A_n.

תרגיל 9.2.37 (***+) הוכח את המשפט. **הדרכה**. תהי $N \lhd S_n$. נתבונן באברים של N שאורך המחזור המקסימלי שלהם d הוא הקטן ביותר, ומביניהם ניקח איבר σ עם מספר מחזורים (לא־טריוויאליים) קטן ביותר. נניח, בשלילה, ש־ $d > 2$. קח σ' צמוד ל־ σ שבו מחזור σ_0 באורך d השווה לזה של σ', וכל שאר המחזורים הפוכים (כתמורות). אז $\sigma\sigma' = \sigma_0^2$; אם d זוגי

אז σ_0^2 תמורה עם שני מחזורים באורך $d/2$, בסתירה למינימליות של d. לכן d איזוגי, וב־ σ_0^2 יש מחזור אחד באורך d. החישוב $(a_1a_3a_2) = (a_1a_2a_3\cdots a_d)(a_da_{d-1}\cdots a_3a_1a_2)$ מאפשר להניח $d=3$, אבל המחזורים באורך 3 יוצרים את A_n (תרגיל 9.2.30). לכן $d=2$. הראה שב־ σ יש שני חילופים, והסק ש־ $N=A_n$. היכן נכשלת ההוכחה במקרה $n=4$?

תרגיל 9.2.38 (**) ל־A_n אין תת־חבורות שהן נורמליות ב־S_n. **הדרכה**. מיידי ממשפט 9.2.36.

תרגיל 9.2.39 (***) לחבורה G יש תת־חבורה נורמלית יחידה, $N \lhd G$, מאינדקס 2. נניח ש־N אינה פשוטה. הראה שהיא איזומורפית לחבורה מהצורה $K\times K$. **הדרכה**. תהי $K \lhd N$, $1 \neq K \neq N$. הראה שיש ל־ K תת־חבורה צמודה אחת, K_1, ב־ G. הראה ש־ $N \supseteq K\cap K_1$. הראה ש־ KK_1 ו־$K\cap K_1$ תת־חבורות נורמליות של G (ראה סעיף 6.2). הסק: $N\cong K\times K_1$.

תרגיל 9.2.40 (***־) הראה כיצד להסיק את משפט 9.2.33 מתוך משפט 9.2.36, אם מניחים ש־A_n אינה איזומורפית לחבורה מהצורה $N\times N$. **הדרכה**. הפעל את תרגיל 9.2.39 על $G=S_n$ ו־$N=A_n$.

תרגיל 9.2.41 (***־) תהי G_0 חבורה פשוטה, שהיא תת־חבורה מאינדקס 2 של חבורה G שהמרכז שלה טריוויאלי. הוכח שאין ל־G תת־חבורות נורמליות לא טריוויאליות פרט ל־G_0. **הדרכה**. תהי $N \lhd G$. אם $N \subseteq G_0$ סיימנו, ולכן $N\cap G_0 = 1$ ו־$NG_0 = G$. אבל אז $N\cong N/(N\cap G_0)\cong NG_0/G_0 = G/G_0$; והרי תת־חבורה נורמלית מסדר 2 היא מרכזית (תרגיל 7.1.5), בסתירה להנחה.

תרגיל 9.2.42 (**) הסק את משפט 9.2.36 ממשפט 9.2.33. **הדרכה**. לפי תרגיל 7.1.28 אפשר להפעיל את תרגיל 9.2.41.

תרגיל 9.2.43 (**) נניח $5\leq n$.

א. ל־ A_n אין תת־חבורות מאינדקס קטן מ־ n.

ב. אם $H\leq S_n$ מאינדקס $[S_n\!:\!H]\leq n$, אז $H=A_n$ או $[S_n\!:\!H]=n$.

תרגיל 9.2.44 (***) תהי G_0 חבורה פשוטה, שהיא תת־חבורה של חבורה G. אם יש ל־G תת־חבורה נורמלית לא טריוויאלית פרט ל־G_0, אז $G\cong G_0\times G/G_0$. **הדרכה**. תהי $N \lhd G$ שאינה מוכלת ב־G_0. אז $N\cap G_0 = 1$ ו־$NG_0 = G$, ולפי משפט האיזומורפיזם השני $N\cong N/(N\cap G_0)\cong NG_0/G_0 = G/G_0$. מכאן ש־$G\cong G_0\times N\cong G_0\times G/G_0$.

9.3 תמורות מקריות

תלמידי 89-214 מוזמנים לדלג על הסעיף.

השאלות בסעיף זה מנוסחות בשפה הסתברותית, אבל אפשר לתרגם אותן בקלות לחישובי ממוצעים, ולתת להן גוון קומבינטורי.

תרגיל 9.3.1 (*) בוחרים באקראי $\sigma\in S_{12}$. מה הסיכוי ש־ $\sigma(1)=3$?

תרגיל 9.3.2 (+*) מה הסיכוי לכך ש־ $\sigma(1)=3$ וגם $\sigma(2)=3$?

נסמן ב־ $X(\sigma)$ את מספר נקודות השבת של σ : $X(\sigma)=|\{x : \sigma(x)=x\}|$.

תרגיל 9.3.3 (**) חשב את התוחלת של $X(\sigma)$ (כאשר $\sigma \in S_n$ מקרית).

תרגיל 9.3.4 (**) חשב את הסיכוי לכך שהנקודה 1 תשתייך למחזור באורך k, כאשר $1 \le k \le n$.

תרגיל 9.3.5 (+**) מה תוחלת מספר המחזורים באורך k של תמורה מקרית $\sigma \in S_n$?
הדרכה. ספור נקודות השייכות למחזורים באורך k.

תרגיל 9.3.6 (**) מה תוחלת מספר המחזורים של תמורה מקרית σ?

תרגיל 9.3.7 (***) חשב את ההתפלגות של $X(\sigma)$. מה קורה כאשר $n \to \infty$?

9.3.1 הלמה של Burnside

תהי G חבורה של תמורות על קבוצה סופית Ω.
הנקודות $x, y \in \Omega$ שייכות לאותו **מסלול** אם קיים $g \in G$ כך ש- $y = g(x)$.

תרגיל 9.3.8 (*) הוכח שהתכונה 'להיות באותו מסלול' היא יחס שקילות על Ω.

משפט 9.3.9 (הלמה של Burnside) *מספר המסלולים של G ב- Ω שווה למספר נקודות השבת הממוצע* $\frac{1}{|G|} \sum_{\sigma \in G} X(\sigma)$.

תרגיל 9.3.10 (***) הוכח את הלמה. **הדרכה**. חשב את $\sum_{x \in \Omega, \sigma \in G} \delta_{x,\sigma(x)}$ בשתי דרכים.

תרגיל 9.3.11 (*) חשב באמצעות הלמה של Burnside את מספר נקודות השבת הממוצע של תמורות מ- S_n.

תרגיל 9.3.12 (**) כמה דרכים יש לצבוע קודקודים של ריבוע, אם אפשר להשתמש בששה צבעים ?

תרגיל 9.3.13 (***) במאגר יש מספר גדול של כדורים בכל אחד מעשרה צבעים. השתמש בלמה של Burnside כדי לספור כמה אפשרויות יש לבחור ארבעה כדורים.

פרק 10

חבורות אבליות

בפרק זה נשתמש בכלים שבנינו עד כאן, ובעוד כמה פטנטים המיוחדים לחבורות אבליות, על־מנת לתת מיון שלם של החבורות האבליות הסופיות.

מושגים: תת־חבורת הקומוטטורים. משפט קושי. אקספוננט. פירוק פרימרי. צורה קנונית של חבורה אבלית סופית. פיתול וחוסר פיצול. בסיס של חבורה אבלית.

10.1 תת־חבורת הקומוטטורים

הגדרה 10.1.1 *תהי G חבורה.* **תת־חבורת הקומוטטורים** *של G היא תת־החבורה הנוצרת על־ידי הקומוטטורים; את תת־חבורת הקומוטטורים מסמנים G'.*

תרגיל 10.1.2 (*) $[x,y]^{-1} = [y,x]$.

תרגיל 10.1.3 (+*) הוכח: $(ab)^2 = (ba)^2$ אם ורק אם $[a,b]\cdot[a^{-1},b^{-1}] = 1$.

תרגיל 10.1.4 (*) בחבורת מנה G/N, $[xN,yN] = [x,y]N$.

משפט 10.1.5 *G/G' היא המנה האבלית המקסימלית של G. ביתר פירוט:*

א. $G' \lhd G$.

ב. G/G' *חבורה אבלית.*

ג. לכל תת־חבורה $N \lhd G$, G/N קומוטטיבית אם ורק אם $G' \subseteq N$ (ואז G/N חבורת מנה של G/G').

תרגיל 10.1.6 (+)** הוכח את המשפט.

תרגיל 10.1.7 (**) אם $N \lhd G$, אז $(G/N)' = G'N/N$.

תרגיל 10.1.8 (**) אם $N, M \lhd G$ נחתכות באופן טריוויאלי ו־$G' \subseteq N$, אז $M \subseteq \mathrm{Z}(G)$.

תרגיל 10.1.9 (+*)** תהי N תת־חבורה נורמלית של מכפלה $A = A_1 \times A_2$. נסמן ב־$\pi_i : A \to A_i$ את ההיטלים. הוכח ש־

$$[A_1, \pi_1(N)] \times [A_2, \pi_2(N)] \subseteq N \subseteq \pi_1(N) \times \pi_2(N).$$

תרגיל 10.1.10 (**) אם $K \subseteq A, B$ תת־חבורות נורמליות של חבורה G, אז בחבורת המנה G/K, $[A/K, B/K] = [A, B]K/K$.

אם $N, K \leq G$, נסמן $N^{[K]} = \{x \in G : [x, K] \subseteq N\}$, במין היפוך של הפעולה $N \mapsto [N, K]$.

תרגיל 10.1.11 (**) א. $N^{[G]} \leq G$.
ב. אם $N \lhd G$ נורמלית אז גם $N^{[G]} \lhd G$, ובמקרה זה $N \subseteq N^{[G]}$.
ג. אם $N_1 \subseteq N_2$ אז $N_1^{[G]} \subseteq N_2^{[G]}$.

תרגיל 10.1.12 (**) אם $N \lhd G$ אז $N^{[K]} \leq G$.

תרגיל 10.1.13 (**) $[N^{[K]}, K] \subseteq N$.

תרגיל 10.1.14 (**) אם $K \subseteq H \leq G$, $K \lhd G$, אז $\mathrm{C}_{G/K}(H/K) = K^{[H]}/K$.

תרגיל 10.1.15 (**) חשב את S_3', את D_4', ואת A_4'.

תרגיל 10.1.16 (-***) $n \geq 5$. בלי להעזר בעובדה ש־ A_n פשוטה, הוכח ש־
א. $S_n' = A_n$.
ב. $A_n' = A_n$.

10.1.1 יוצרים של חבורות קומוטטורים

תלמידי 89-214 מוזמנים לדלג על הסעיף.

נסמן $x^y = y^{-1}xy$. אם $A, B \subseteq G$ נסמן $\langle A \rangle^B = \langle b^{-1}ab : a \in A, b \in B \rangle$ - **הסגור הנורמלי** של A ב־ $\langle A, B \rangle$.

תרגיל 10.1.17 (*) $(xy)^z = x^z y^z$, $x^{yz} = (x^y)^z$.

תרגיל 10.1.18 (*) $[x, yz] = [x, y][x, z]^{y^{-1}}$ ו־ $[x, y^{-1}] = [y, x]^{y^{-1}}$.

הגדרה 10.1.19 *תהי $B \leq G$. אם $a \in G$, $[a, B]$ היא תת־החבורה הנוצרת על־ידי הקומוטטורים $[a, b]$, $b \in B$.*

תרגיל 10.1.20 (*) אם $A, B \lhd G$, אז $[A, B] \lhd G$.

תרגיל 10.1.21 (**) אם A ו־B נורמליות אז $[A, B] \subseteq A \cap B$.

תרגיל 10.1.22 (**) א. הוכח את הזהות $[xy, z] = [y, z]^{x^{-1}}[x, z]$.
ב. לכל שתי קבוצות $S, T \subseteq G$, $[\langle S \rangle, \langle T \rangle] = \langle [a, b] : a \in S, b \in T \rangle^{S \cup T}$.

תרגיל 10.1.23 (*) א. הוכח את הזהות $[b_1 a b_1^{-1}, b] = [b_1, a][a, bb_1]$.
ב. לכל שתי קבוצות $S, T \subseteq G$, $[\langle S \rangle^T, \langle T \rangle] = [\langle S \rangle, \langle T \rangle]$.

תרגיל 10.1.24 (+***) הוכח ש־ $[G, [G, x]] \subseteq [G, x]$. **הדרכה.** מצא a, b, c מתאימים, כך שיתקיים $[g, [h, x]] = [a, x][b, x]^{-1}[c, x]^{-1}$.

תרגיל 10.1.25 (זהות Hall)** נסמן $\langle a,b,c\rangle = [[a^{-1},b],c]^a$. הוכח את הזהות

$$\langle a,b,c\rangle\langle c,a,b\rangle\langle b,c,a\rangle = 1.$$

תרגיל 10.1.26 (* למת השלוש)** אם $A,B,C \lhd G$, אז $[[A,B],C] \subseteq [[B,C],A]\cdot[[C,A],B]$.
הדרכה. תרגיל 10.1.25.

תרגיל 10.1.27 (**) הראה שלכל $A,B \lhd G$, $[[A,A],B] \subseteq [[A,B],A]$.

תרגיל 10.1.28 (*) $[axa^{-1},byb^{-1}] = [a,x][x,[b,y]][b,y][x,y][x,a][[a,x],y][y,b]$.

תרגיל 10.1.29 (**) תהי $G = F/R^F$, כאשר $F = \langle s_1,\dots,s_n\rangle$ ו־$R = \langle r_1,\dots,r_m\rangle$.
הוכח ש־ $[R,F] = [\langle r_j\rangle^S, \langle S\rangle] = [\{r_j\},S] = \langle [\{r_j\},\{s_i\}]\rangle^S = \langle s_{i'}[r_j,s_i]s_{i'}^{-1}\rangle$.

10.2 משפט קושי

ידוע שהסדר של כל איבר מחלק את סדר החבורה בה הוא נמצא. מאידך, לא כל מחלק של סדר החבורה הוא סדר של איבר שם (תרגיל 4.3.16).

משפט 10.2.1 *יהי p ראשוני המחלק את הסדר של חבורה G. אז יש ב־G איבר מסדר p.*

תרגיל 10.2.2 (*) לכל d, אם C ציקלית מסדר המתחלק ב־ d, אז יש ב־ C איבר מסדר d. **הדרכה**. תרגיל 4.6.13.

תרגיל 10.2.3 (-*)** הוכח את משפט קושי לחבורות אבליות. **הדרכה**. תהי A אבלית מסדר המתחלק ב־p ויהי $x \in A$ $x \neq 1$. אם p מחלק את $|\langle x\rangle|$ אז יש ב־$\langle x\rangle$ איבר מסדר p. אחרת $p \,|\, |A/\langle x\rangle|$, ובאינדוקציה יש איבר $y \in A$ כך ש־ $y \notin \langle x\rangle$, $y^p \in \langle x\rangle$. אבל אז p מחלק את $|\langle y\rangle|$.

תרגיל 10.2.4 (***) הוכח את משפט קושי. **הדרכה**. אם p מחלק את הגודל של כל מחלקת צמידות לא מרכזית ב־G, אז p מחלק את $|\mathrm{Z}(G)|$ לפי שוויון המחלקות, וסיימנו לפי תרגיל 10.2.3. אחרת יש $x \in G$ לא מרכזי, כך ש־ $[G:\mathrm{C}_G(x)]$ זר ל־p, ואז p מחלק את $|\mathrm{C}_G(x)|$, ושם יש איבר מסדר p באינדוקציה על הסדר.

תרגיל 10.2.5 (***) הוכח את משפט קושי לחבורה סופית G כלשהי באמצעות פעולת הסיבוב על $X = \{(g_1,\dots,g_p) \in G^p :\, g_1\cdots g_p = 1\}$. **הדרכה**. ראשית, $|X| = |G|^{p-1}$ מתחלק ב־p. וקטור אינו משתנה תחת סיבוב בדיוק כאשר $g_1 = \cdots = g_p$ ו־$g_1^p = 1$, ומספר הוקטורים האלה מוכרח להתחלק ב־p.

תרגיל 10.2.6 (***) יש חבורה לא אבלית מסדר p^3 שכל האברים (השונים מ־1) בה מסדר p. **הדרכה**. הראה שהחבורה $G = \{\alpha^i x^j y^k :\, i,j,k = 0,\dots,p-1\}$, שבה מוגדר הכפל לפי הכללים $\alpha^p = x^p = y^p = 1$, $[y,x] = \alpha$, $[\alpha,x] = [\alpha,y] = 1$, עונה על הדרישות.

תרגיל 10.2.7 (***) (המשך תרגיל 7.4.8) לפי משפט קושי יש ב־G איבר y מסדר p, ואיבר x מסדר q.
א. $G = \left\{x^i y^j : 0 \leq i < q, 0 \leq j < q\right\}$.
ב. קיים $\theta \in \mathbb{Z}_q$ כך ש־ $yxy^{-1} = x^\theta$.
ג. כתוב את $x^i y^j \cdot x^{i'} y^{j'}$ בצורה $x^{i''} y^{j''}$.
ד. $\theta^p \equiv 1 \pmod q$, ו־$\theta \not\equiv 1$. כלומר־ θ איבר מסדר p בחבורה U_q.
ה. כל החבורות הלא־אבליות מסדר pq הן איזומורפיות זו לזו.

אם $\phi \in \operatorname{Aut}(G)$ אוטומורפיזם מסדר סופי n, נגדיר את הנורמה ביחס ל־ϕ לפי $N_\phi(x) = x\phi(x)\phi^2(x)\cdots\phi^{n-1}(x)$.

תרגיל 10.2.8 (**) עבור $\gamma_g \in \operatorname{Aut}(G)$, חשב ש־$N_{\gamma_g}(x) = (xg)^n g^{-n}$.

תרגיל 10.2.9 (***) הוכח: אם $|G|$ מתחלק ב־p ו־$\phi \in \operatorname{Aut}(G)$ אוטומורפיזם מסדר p, אז יש בחבורה איברים $x \neq 1$ עם $N_\phi(x) = 1$. **הדרכה**. הכלל את הפתרון לתרגיל 10.2.5.

תרגיל 10.2.10 (***) תהי G חבורה שהסדר שלה מתחלק בראשוני p. נניח ש־ϕ, ψ אוטומורפיזמים מתחלפים של G, ושניהם מסדר p. אז יש איברים $x \neq 1$ כך ש־ $N_\phi(x) = N_\psi(x) = 1$. הכלל את הטענה לכל מספר סופי של אוטומורפיזמים. **הדרכה**. כבתרגיל 10.2.9, עם פעולה של $\mathbb{Z}_p^2$ על אוסף המטריצות (g_{ij}) שבהן המכפלה של כל שורה ועמודה היא 1.

תרגיל 10.2.11 (***) אם p מחלק את $|G|$ ו־$\phi \in \operatorname{Aut}(G)$ מסדר p, אז קיים x מסדר p כך ש־$x\phi^i(x)\phi^{2i}(x)\cdots\phi^{(p-1)i}(x) = 1$ לכל i. **הדרכה**. קח $1, \phi, \phi^2, \cdots, \phi^{p-1}$ בתרגיל 10.2.10.

תרגיל 10.2.12 (***) נניח ש־$|G|$ מתחלק ב־3, ו־$\phi \in \operatorname{Aut}(G)$ אוטומורפיזם מסדר 3. אז יש איבר x כך ש־ $\langle x, \phi(x)\rangle$ איזומורפית ל־$\mathbb{Z}_3$ או ל־$\mathbb{Z}_3 \times \mathbb{Z}_3$. **הדרכה**. מתרגיל 10.2.11 נובע ש־$x\phi(x)\phi^2(x) = x\phi^2(x)\phi(x) = 1$ עבור x מתאים.

10.3 האקספוננט

הגדרה 10.3.1 ***האקספוננט*** *של חבורה G הוא המספר הקטן ביותר N כך ש־ $a^N = 1$ לכל $a \in G$ (ראו תרגיל 4.3.6). מסמנים מספר זה ב־*$\exp(G)$.

תרגיל 10.3.2 (*) האקספוננט של G הוא הכפולה המשותפת המינימלית של סדרי האיברים בה.

תרגיל 10.3.3 (*) $\exp(\mathbb{Z}/n\mathbb{Z}) = n$.

תרגיל 10.3.4 (+**) חשב את $\exp(S_6)$, $\exp(S_7)$. הוכח שלכל n, האקספוננט של S_n הוא $\operatorname{lcm}\{1, \ldots, n\}$.

תרגיל 10.3.5 (+*) הראה שהאקספוננט של החבורה מתרגיל 10.2.6 הוא p.

תרגיל 10.3.6 (+*) $\exp(G)$ מחלק את $|G|$.

תרגיל 10.3.7 (**) ל־$\exp(G)$ יש אותם גורמים ראשוניים כמו ל־$|G|$.

תרגיל 10.3.8 (⁻**) $\exp(A\times B)=[\exp(A),\exp(B)]$ (ראה הגדרה 1.3.32).

תרגיל 10.3.9 (+**) אם G חבורה אבלית עם $\exp(G)=|G|$, אז היא ציקלית. **הדרכה.** פרק את $|G|$ לגורמים והפעל את תרגיל 4.3.8.

תרגיל 10.3.10 (**) תן דוגמא לחבורה לא ציקלית עם $\exp(G)=|G|$.

תרגיל 10.3.11 (**) (השווה לתרגיל 4.6.16) תהי G חבורה סופית מסדר n. אם לכל $d|n$ יש לכל היותר d פתרונות למשוואה $x^d=1$, אז החבורה ציקלית. **הדרכה.** קח $d=\exp(G)$ והפעל את תרגיל 10.3.9.

תרגיל 10.3.12 (**) תן הוכחה קצרה למשפט 4.6.20. **הדרכה.** לכיוון אחד חשב את האקספוננט וסיים לפי תרגיל 10.3.9. לכיוון השני הצג את $\mathbb{Z}_{nm}$ כמכפלה ישרה פנימית.

תרגיל 10.3.13 (**) אם G אבלית אז יש שיכון $\operatorname{Aut}(G)\hookrightarrow U_{\exp(G)}$. הראה שהתמונה נורמלית ב־$\operatorname{Aut}(G)$.

10.4 הפירוק הפרימרי

הזכר בהגדרה 8.1.29: אם A חבורה אבלית, $\mu_n\colon A\to A$ המוגדרת לפי $\mu_n(a)=a^n$ היא הומומורפיזם.

הגדרה 10.4.1 *תהי A חבורה אבלית ויהי $\mu_n\colon A\to A$ ההומומורפיזם של העלאה בחזקה. נסמן* $A^n=\operatorname{Im}(\mu_n)=\{a^n:\ a\in A\}$ *ו־* $A_n=\operatorname{Ker}(\mu_n)=\{a\in A:\ a^n=1\}$. אין קשר בין הסימון A_n לחבורת התמורות הזוגיות של הגדרה 9.2.13.

תרגיל 10.4.2 (⁻**) אם $(n,|A|)=1$, אז $A^n=A$ ו־$A_n=1$.

תרגיל 10.4.3 (**) תהי $A=\mathbb{Z}_n$. הראה שלכל $d\,|\,n$, $A_d\cong\mathbb{Z}_d$ ו־$A^d\cong\mathbb{Z}_{n/d}$. חשב את A_m ואת A^m עבור m כלשהו.

תרגיל 10.4.4 (+**) $\exp(A_n)\,|\,n$.

תרגיל 10.4.5 (**) נניח ש־ $\exp(A)\,|\,nm$. אז $A^n\subseteq A_m$.

תרגיל 10.4.6 (**) אם $\exp(A)=nm$ ו־n,m זרים, אז $A^n=A_m$.

משפט 10.4.7 *אם $\exp A=nm$ כאשר n,m זרים, אז $A\cong A_n\times A_m$.*

תרגיל 10.4.8 (⁻***) הוכח את המשפט. **הדרכה.** כתוב $1=\alpha n+\beta m$ והראה ש־ $A_n\cap A_m=1$ וש־$A\subseteq A^mA^n\subseteq A_nA_m$.

תרגיל 10.4.9 (+***) נניח ש־$A=B\times C$ כאשר $n=\exp(B)$ ו־$m=\exp(C)$ זרים. הראה ש־ $B\cong A^m$ ו־$C\cong A^n$. בפרט, הפירוק לחבורות עם אקספוננטים (זרים) נתונים הוא יחיד.

הגדרה 10.4.10 *חבורה שהסדר של כל איבר בה הוא חזקה של אותו ראשוני p, נקראת* ***חבורת־p***.

תרגיל 10.4.11 (+)** חבורה סופית היא חבורת־p אם ורק אם הסדר שלה הוא חזקה של p, אם ורק אם האקספוננט שלה חזקת־p.

משפט 10.4.12 ***כל חבורה אבלית סופית היא מכפלה ישרה של חבורות־p, שהן יחידות עד־כדי איזומורפיזם.***

תרגיל 10.4.13 (**) הוכח את המשפט. **הדרכה**. קיום הפירוק באינדוקציה על משפט 10.4.7, לפי תרגיל 10.4.4. היחידות לפי תרגיל 10.4.9.

תרגיל 10.4.14 (**) פרק למכפלה ישרה פנימית של תת־חבורות, שהן חבורות־p, את $\mathbb{Z}_{24}$ ואת U_{126}.

תרגיל 10.4.15 (**) אם m מחלק את $|A|$, אז μ_m אינו חד־חד־ערכי.

10.5 חבורות־p אבליות

ראו סעיף **??**.

טענה 10.5.1 בחבורת־p יש איבר שסדרו שווה לאקספוננט.

תרגיל 10.5.2 (**) הוכח את הטענה. **הדרכה**. אחרת הסדר של כל האברים מחלק את $\exp(A)/p$.

בסעיפים 3.5 ו־6.2 עסקנו במכפלות ישרות של מספר סופי של מרכיבים. אפשר להגדיר מכפלות ישרות של מספר כלשהו של מרכיבים, וגם סכומים ישרים; באופן כללי יש הבדל (גדול) בין שני המושגים, אבל עבור מספר סופי של מחוברים, הם מתלכדים. כשמדובר בחבורות אבליות, מעדיפים להשתמש בסכום ישר (כמו למשל במרחבים וקטוריים), וכך נעשה גם כאן.

את **הסכום הישר** של החבורות B,C מסמנים $B\oplus C$. נבהיר שוב ש־ $B\oplus C=B\times C$, ואנו משתמשים בסימון החיבורי משום שהחבורות אבליות.

תת־חבורה $H\leq A$ נקראת **מחובר ישר**, אם יש תת־חבורה H_1 כך ש־A הוא סכום ישר של H ו־H_1. ראה תרגיל 6.2.9.

משפט 10.5.3 ***אם g הוא איבר מסדר השווה לאקספוננט בחבורת־p אבלית A, אז תת־החבורה הציקלית שהוא יוצר היא מחובר ישר ב־A.***

תרגיל 10.5.4 (***) הוכח את המשפט. **הדרכה**. באינדוקציה. נניח ש־ $A\neq\langle g\rangle=H$. ראשית, קיים מחוץ ל־ H איבר x מסדר p, לפי משפט קושי על A/H והשוואת $x^p=g^i$. כעת $Q=\langle x\rangle$ מקיים $Q\cap H=1$ ו־$\exp(A/Q)=\exp(A)$ כי $H\cong HQ/Q$. באינדוקציה קיים $A\leq K\subseteq Q$ כך ש־ $A/Q=(HQ/Q)\oplus K/Q$ מכפלה ישרה, ואז $HK=HQK=A$, ו־$H\cap K\subseteq H\cap Q=1$.

תרגיל 10.5.5 (***) תהי $G=\mathbb{Z}_{p^{\alpha_1}}\oplus\cdots\oplus\mathbb{Z}_{p^{\alpha_t}}$. הראה ש־ $[p^{m-1}G:p^mG]=p^{|\{i:\alpha_i=m\}|}$. בפרט, אפשר לקרוא את קבוצת הערכים $\alpha_1,\dots,\alpha_t$ מתוך G.

משפט 10.5.6 ***לכל חבורת־p אבלית סופית יש פירוק יחיד לסכום ישר של חבורות ציקליות, $G=\mathbb{Z}_{p^{\alpha_1}}\oplus\cdots\oplus\mathbb{Z}_{p^{\alpha_t}}$ כאשר $\alpha_1\leq\cdots\leq\alpha_t$.***

תרגיל 10.5.7 (**) הוכח את המשפט. **הדרכה.** הקיום באינדוקציה לפי משפט 10.5.3, והיחידות היא תרגיל 10.5.5.

תרגיל 10.5.8 (**) מצא כמה אברים מכל סדר יש בחבורות $\mathbb{Z}_p$, $\mathbb{Z}_{p^2} \oplus \mathbb{Z}_p$, $\mathbb{Z}_{p^3}$ ו־$\mathbb{Z}_p \oplus \mathbb{Z}_p \oplus \mathbb{Z}_p$.

תרגיל 10.5.9 (**) בחבורת־p אבלית לא ציקלית יש תת־חבורה מסדר p^2 שאינה ציקלית.

תרגיל 10.5.10 (**) האם קיימת חבורה אבלית G, כך ש־ $\exp(G) = 4$, $|G| = 32$, ו־$[G : G^2] = 4$?

תרגיל 10.5.11 (**) מצא את כל החבורות האבליות A מסדר 3^{13} ומאקספוננט 3^5 כך ש־$3A/9A \cong \mathbb{Z}_9$.

10.6 משפט המיון לחבורות אבליות סופיות

משפט 10.6.1 *כל חבורה אבלית סופית אפשר להציג באופן יחיד בצורה*

$$\mathbb{Z}_{d_1} \oplus \cdots \oplus \mathbb{Z}_{d_t},$$

כאשר $d_1 \mid \cdots \mid d_t$.

צורה זו של החבורה נקראת **הצורה הקנונית**.

תרגיל 10.6.2 (***) הוכח את המשפט. **הדרכה.** קיום: פרק את החבורה למכפלה של חבורות־p לפי משפט 10.4.12, ופרק כל אחת מאלה לסכום של t חבורות ציקליות לפי משפט 10.5.6. אסוף ל־$\mathbb{Z}_{d_t}$ (תרגיל 4.6.20) את המרכיב הגדול ביותר בכל קבוצה, וכן הלאה. יחידות: הראה ש־$t = \max|A/pA|$, כאשר המקסימום על־פני כל הראשוניים המחלקים את $|A|$; הראה ש־ $p^\ell \mid d_1$ אם ורק אם $\log_p |p^{\ell-1}A/p^\ell A| = t$.

תרגיל 10.6.3 (**) הראה ש־$m\mathbb{Z}_n \cong \mathbb{Z}_{\frac{n}{(n,m)}}$.

תרגיל 10.6.4 (**) הראה שאם $A = \mathbb{Z}_{d_1} \oplus \cdots \oplus \mathbb{Z}_{d_t}$, אז לכל m, הצורה הקנונית של mA היא $\mathbb{Z}_{\frac{d_1}{(d_1,m)}} \oplus \cdots \oplus \mathbb{Z}_{\frac{d_t}{(d_t,m)}}$. (העזר בתרגיל 1.3.30).

תרגיל 10.6.5 (***) הוכח את יחידות ההצגה באינדוקציה על הסדר. **פתרון.** *תהי A חבורה אבלית, עם הצגה קנונית $\mathbb{Z}_{d_1} \oplus \cdots \oplus \mathbb{Z}_{d_t}$ (שאולי אינה יחידה). נניח, באינדוקציה, שמספר המרכיבים $\ell(B)$ בהצגה הקנונית של B מוגדר היטב לכל חבורה B מסדר קטן משל A. הראה (בעזרת תרגיל 10.6.4) ש־d_1 הוא הערך הקטן ביותר של m שעבורו $mA \subset A$ ו־$\ell(mA) < t$. נניח שיש שתי הצגה קנונית נוספת $\mathbb{Z}_{d'_1} \oplus \cdots \oplus \mathbb{Z}_{d'_{t'}}$ עם $t' \leq t$, אז $d'_1 \mid d_1$, ולכן המספרים $d_1/d'_1, \dots, d_t/d'_1$ ו־ $d'_2/d'_1, \dots, d'_{t'}/d'_1$ (בניכוי ה־1־ים) שווים. מכאן שבשתי ההצגות יש אותו מספר של מספרים הגדולים מ־d'_1, ואלו שווים זה לזה בהתאמה; מכיוון שבשני המקרים לחבורה אותו סדר, גם מספר הערכים השווים ל־d'_1 שווה, ומכאן שההצגות שוות.*

תרגיל 10.6.6 (-***) לחבורה אבלית סופית יש איבר מכל סדר המחלק את סדר החבורה. (השווה לתרגיל 7.3.10).

תרגיל 10.6.7 (**) הראה שאם $A=\mathbb{Z}_{d_1}\oplus\cdots\oplus\mathbb{Z}_{d_t}$, כאשר $d_1\mid\cdots\mid d_t$, אז לכל i, $d_i=\exp(A)/\exp(A^{d_i})$. בפרט $\exp(A)=d_t$. (הסבר מדוע תרגיל זה אינו מסייע בהוכחת היחידות).

תרגיל 10.6.8 (**) מיין, עד כדי איזומורפיזם, את החבורות האבליות מהסדרים הבאים: $560, 320, 625, 210$.

תרגיל 10.6.9 (**) מיין, עד כדי איזומורפיזם, את החבורות האבליות מהסדרים הבאים: $8085, 2^2 3^2 5$.

תרגיל 10.6.10 (***) מצא את הצורה הקנונית של $\mathbb{Z}_{12}\oplus\mathbb{Z}_{40}\oplus\mathbb{Z}_{15}$.

תרגיל 10.6.11 (+**) כתוב איזומורפיזם מפורש $\mathbb{Z}_{40}\oplus\mathbb{Z}_{30}\oplus\mathbb{Z}_4\cong\mathbb{Z}_2\oplus\mathbb{Z}_{20}\oplus\mathbb{Z}_{120}$.

תרגיל 10.6.12 (**) מצא את החבורות האבליות מסדר 324 ואקספוננט 18.

תרגיל 10.6.13 (**) מצא איבר מסדר 33 ב־ $\mathbb{Z}_{15}\oplus\mathbb{Z}_{55}$.

תרגיל 10.6.14 (+*) הוכח ש־ $\mathbb{Z}_{200}\oplus\mathbb{Z}_{20}\cong\mathbb{Z}_{100}\oplus\mathbb{Z}_{40}$.

תרגיל 10.6.15 (+*) הוכח או הפרך - $\mathbb{Z}_4\oplus\mathbb{Z}_{15}\cong\mathbb{Z}_3\oplus\mathbb{Z}_{20}$, $\mathbb{Z}_{12}\oplus\mathbb{Z}_{12}\oplus\mathbb{Z}_{20}\cong\mathbb{Z}_{30}\oplus\mathbb{Z}_6\oplus\mathbb{Z}_{16}$.

תרגיל 10.6.16 (***) תהי $G=\mathbb{Z}_{ab}\oplus\mathbb{Z}_{bc}$ עם תת החבורה $H=\langle(a,b)\rangle$. מצא r,s כך ש־ $G/H\cong\mathbb{Z}_r\oplus\mathbb{Z}_s$. **הדרכה**. ראשית מצא איזומורפיזם $\phi\colon G\to\mathbb{Z}_b\oplus\mathbb{Z}_{abc}$. מהי התמונה של H תחת ϕ?

10.6.1 חבורות אוילר

תלמידי 89-214 מוזמנים לדלג על הסעיף.

הטלות ופירוק

תרגיל 10.6.17 (**) נניח $m|n$. ההעתקה $[a]_n\mapsto[a]_m$ היא הומומורפיזם $U_n\to U_m$.

תרגיל 10.6.18 (***) אם $(n,m)=1$ אז $U_{nm}\cong U_n\oplus U_m$. **הדרכה**. ההעתקה $U_{nm}\to U_n\oplus U_m$ היא חד־חד־ערכית, ולפי תרגיל 4.4.14 היא גם על. לחילופין, העזר בכך ש־ $U(M\oplus N)=U(M)\oplus U(N)$ ובמשפט 4.6.20.

תרגיל 10.6.19 (**) הסק מתרגיל 10.6.18 שאם $(m,n/m)=1$, אז ההעתקה $U_n\to U_m$ לפי $[a]_n\mapsto[a]_m$ היא על.

תרגיל 10.6.20 (***) הוכח שההעתקה $U_n\to U_m$ לפי $[a]_n\mapsto[a]_m$ (כאשר $m\mid n$) היא על. **הדרכה**. הדרכה. יהי $[a]_m\in U_m$, כלומר, $(a,m)=1$. צריך להראות שקיים $b\equiv a\pmod{m}$ כך ש־ $(b,n)=1$. כתוב $b=a+mx$, ובחר $x\equiv 1\pmod{p}$ לכל $p|n$ כך ש־ $(p,m)=1$. סיים לפי משפט השאריות הסיני.

תרגיל 10.6.21 (**) חשב את הגרעין של ההעתקה $U_{30}\to U_6$. מה המבנה של הגרעין ?

תרגיל 10.6.22 (**) הוכח שהגרעין של ההעתקה $U_{p^2}\to U_p$ איזומורפי ל־ $\mathbb{Z}_p$.

שיכונים

תרגיל 10.6.23 (**) הוכח שקיים שיכון $U_p \to U_{p^2}$.

תרגיל 10.6.24 (**) מצא שיכון מפורש $U_5 \to U_{25}$.

תרגיל 10.6.25 (+**) הוכח שקיימים שיכונים $U_{p^\alpha} \to U_{p^{\alpha+1}}$ לכל $1 < \alpha$.

תרגיל 10.6.26 (***) אם $m|n$ אז קיים שיכון $U_m \to U_n$.

חבורות אוילר ציקליות

תרגיל 10.6.27 (-***) U_p חבורה ציקלית לכל p ראשוני. **הדרכה.** U_p היא חבורת האיברים ההפיכים בשדה $\mathbb{Z}_p$; הפעל את תרגיל 10.3.11.

תרגיל 10.6.28 (**) לכל p ראשוני, $\exp(U_p) = p-1$. **הדרכה.** תרגיל 10.6.27.

תרגיל 10.6.29 (***) אם p ראשוני אי־זוגי אז $\exp(U_{p^n}) = (p-1)p^{n-1}$, ולכן U_{p^n} ציקלית מסדר $\phi(p^n) = (p-1)p^{n-1}$. **הדרכה.** לפי תרגיל 10.6.28 והאפימורפיזם $U_{p^n} \to U_p$ של תרגיל 10.6.20, $(p-1) \mid \exp(U_{p^n})$. נשאר לחשב שהסדר של $p+1$ בחבורה הוא p^{n-1}.

תרגיל 10.6.30 (***) $\exp(U_{2^n}) = 2^{n-2}$ ולכן $U_{2^n} \cong \mathbb{Z}_2 \oplus \mathbb{Z}_{2^{n-2}}$. **הדרכה.** חשב את הסדר של 5 מודולו 2^n, וחשוב על $\langle 5 \rangle \cap \langle -1 \rangle$.

תרגיל 10.6.31 (+***) הוכח ש־ U_n ציקלית אם ורק אם n שווה ל־1, 2, 4, או הוא מהצורה p^α או $2p^\alpha$ עבור p אי־זוגי.

תרגיל 10.6.32 (**) מצא יוצר לחבורת אוילר U_{49}.

תרגיל 10.6.33 (**) הראה ש־$\exp(U_{p^t}) = (p-1)p^{t-1^*}$, כאשר $1^* = 1$ אם p אי־זוגי, ו־$1^* = 2$ עבור $p = 2$. **הדרכה.** תרגילים 10.6.29 ו־10.6.30.

פירוק קנוני

תרגיל 10.6.34 (**) כתוב את U_{144} כמכפלת חבורות ציקליות בצורה מפורשת.

תרגיל 10.6.35 (**) כתוב את U_{1800} כסכום ישר של חבורות ציקליות. **פתרון.** $1800 = 8 \cdot 9 \cdot 25$ ולכן $U_{1800} \cong U_8 \oplus U_9 \oplus U_{25} \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_6 \oplus \mathbb{Z}_{20} \cong \mathbb{Z}_2^3 \oplus \mathbb{Z}_{60}$.

תרגיל 10.6.36 (**) כתוב את U_{100} כסכום ישר של חבורות ציקליות.

תרגיל 10.6.37 (**) כתוב את החבורות הבאות כסכום ישר של חבורות ציקליות: U_8, U_{15}, U_{30}, U_{504}.

תרגיל 10.6.38 (**) מצא את הקוסטים של $\langle 13, 27 \rangle$ בחבורה U_{56}, והצג את חבורת המנה כמכפלה ישרה של חבורות ציקליות.

האקספוננט של חבורת אוילר

מסמנים $\lambda(n) = \exp(U_n)$.

תרגיל 10.6.39 (*) $\lambda(n) \,|\, \varphi(n)$.

תרגיל 10.6.40 (+*) הוכח את העידון הבא של משפט אוילר (4.4.9): לכל a זר ל־n, $a^{\lambda(n)} \equiv 1 \pmod{n}$.

תרגיל 10.6.41 (**) אם $n = \prod p_i^{t_i}$, $\lambda(n) = \mathrm{lcm}_i((p_i - 1)p_i^{t_i - 1^*})$, כאשר $1^* = 2$ אם $p_i = 2$ ו־$1^* = 1$ אחרת. **הדרכה**. תרגילים 10.6.18 ו־10.6.33.

תרגיל 10.6.42 (***)

1. מצא את כל ה־n־ים עבורם $\exp(U_n) = 2$ (ראה גם תרגיל 4.4.17).
2. מיין את החבורות U_n המתקבלות, עד כדי איזומורפיזם.
3. הראה שלא קיימת חבורת אוילר $U_n \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$. **הדרכה**. נניח $\exp(U_n) = 2$. אם $p|n$ אז $U_p \subseteq U_n$ ולכן $\exp(U_p)|2$ - הסק ש־ $(5, n) = 1$ וש־ $n|24$.

תרגיל 10.6.43 (***)

1. אם $(a, 30) = 1$, אז $240|(a^4 - 1)$.
2. לא ניתן להגדיל את המספר 240 בסעיף 1.
3. מצא את המספר הגדול ביותר m המקיים $m|(a^6 - 1)$ לכל a זר ל־m.

תרגיל 10.6.44 (**) מספר n שהוא פסאודו־ראשוני ביחס לכל $a \in U_n$ (ראה סעיף 4.4.3) נקרא **מספר קרמייקל** [ידוע שיש אינסוף מספרי קרמייקל.]

1. n הוא מספר קרמייקל אם ורק אם $\lambda(n) \,|\, n - 1$.
2. 561 הוא מספר קרמייקל.
3. אם $6k + 1, 12k + 1, 18k + 1$ כולם ראשוניים, אז מכפלתם היא מספר קרמייקל. מצא את הדוגמא הקטנה ביותר מסוג זה.
4. למספר קרמייקל יש לפחות שלושה גורמים ראשוניים שונים.

10.7 חבורות אבליות אינסופיות

תלמידי 89-214 מוזמנים לדלג על הסעיף.

הגדרה 10.7.1 *חבורה* **נוצרת סופית** *היא חבורה שיש לה קבוצת יוצרים (הגדרה 4.1.7) סופית.*

תרגיל 10.7.2 (**) אם A נוצרת סופית, אז כל חבורת מנה שלה נוצרת סופית.

הגדרה 10.7.3 *חבורה היא* **מפותלת** *אם לכל איבר בה יש סדר סופי,* **וחסרת פיתול** *אם לכל האיברים (פרט לאיבר היחידה) סדר אינסופי.*

תרגיל 10.7.4 (**) האוסף Ω של חבורות אבליות מפותלות סגור לתת־חבורות, לחבורות מנה, ולהרחבות. כלומר:
א. אם $B \leq A \in \Omega$ אז $B, A/B \in \Omega$.
ב. אם $B, A/B \in \Omega$ אז גם $A \in \Omega$.

תרגיל 10.7.5 (*) אם $F, T \leq A$ כאשר T מפותלת ו־A חסרת פיתול, אז $F \cap T = 0$.

תרגיל 10.7.6 (+)** חבורה אבלית מפותלת נוצרת סופית - היא סופית. **הדרכה**. הראה שהאקספוננט e סופי, ושהחבורה מנה של $\mathbb{Z}_e^n$ ל־n מתאים.

הבעיה הכללית - האם חבורה מפותלת נוצרת סופית היא בהכרח סופית - ידועה בשם 'בעיית Burnside'; זוהי אחת הבעיות הפתוחות המפורסמות בתורת החבורות.

תרגיל 10.7.7 (**) תן דוגמא מפורטת לחבורה מפותלת שאינה סופית.

תרגיל 10.7.8 (-*)** אוסף האברים מסדר אינסופי בחבורה אבלית (יחד עם איבר היחידה) אינו בהכרח תת־חבורה. **הצעה**. $A = \prod_{i \in \mathbb{N}} \mathbb{Z}_{2^i}$.

הגדרה 10.7.9 *אוסף האיברים מסדר סופי בחבורה G נקרא **חבורת הפיתול** של G, ומסומן ב־$t(G)$.*

תרגיל 10.7.10 (*) G מפותלת אם ורק אם $t(G) = G$, וחסרת פיתול אם ורק אם $t(G) = 0$.

תרגיל 10.7.11 (-)** אם G אבלית, $t(G)$ תת־חבורה של G.

תרגיל 10.7.12 (-)** $t(A \oplus B) = t(A) \oplus t(B)$.

תרגיל 10.7.13 (**) $G/t(G)$ חבורה חסרת פיתול.

משפט 10.7.14 *כל חבורה אבלית נוצרת סופית וחסרת פיתול היא מהצורה $\mathbb{Z}^n$ עבור איזשהו n.*

קבוצת יוצרים $x_1, \dots, x_n$ של חבורה אבלית נקראת **בסיס** אם מהשוויון $\sum a_i x_i = 0$ נובע $a_1 = \dots = a_n = 0$.

תרגיל 10.7.15 (-)** ל־$\mathbb{Z}^n$ יש בסיס בגודל n.

תרגיל 10.7.16 (**) אם $\mathbb{Z}^m \cong \mathbb{Z}^n$ אז $n = m$. **הדרכה**. חשוב על A/A^2.

תרגיל 10.7.17 (**) חבורה אבלית שיש לה בסיס בן n אברים איזומורפית ל־$\mathbb{Z}^n$.

תרגיל 10.7.18 (***) קבוצת יוצרים בגודל מינימלי של חבורה אבלית חסרת פיתול היא בסיס. **הדרכה**. נאמר שה**משקל** של יחס $\sum a_i x_i = 0$ הוא $\sum |a_i|$. נוכיח את הטענה באינדוקציה על המשקל מינימלי של יחס שהיוצרים מקיימים. לא יתכן שכל ה־a_i השונים מאפס בעלי אותו ערך מוחלט, משום שאז אפשר לצמצם ולקבל $a_i = 1$, בסתירה למינימליות. מכיוון שהחבורה חסרת פיתול, לא יתכן גם שביחס משתתף יוצר יחיד. לכן יש i, j כך ש־$|a_i| < |a_j|$; נציב $x_i = x_i' + x_j$ או $x_i = x_i' - x_j$ בהתאם לסימן של $a_i a_j$. היוצרים $x_1, \dots, x_{i-1}, x_i', x_{i+1}, \dots, x_n$ מקיימים יחס שבו a_j מוחלף ב־$a_j + a_i$ או ב־$a_j - a_i$, שמשקלו קטן יותר, ולפי הנחת האינדוקציה, הם מהווים בסיס; לכן גם $x_1, \dots, x_n$ בסיס.

תרגיל 10.7.19 (***) הוכח את המשפט. **הדרכה.** קבוצת יוצרים בגודל מינימלי היא בסיס לפי תרגיל 10.7.18, והטענה נובעת מתרגיל 10.7.17.

תרגיל 10.7.20 (**+) תהי A חבורה אבלית עם אברים $x_1,\dots,x_n$. אם הקוסטים $x_1+N,\cdots,x_n+N$ מהווים בסיס של חבורת מנה A/N, אז $x_1,\dots,x_n$ בסיס של תת־החבורה שהם יוצרים ב־A.

משפט 10.7.21 ***חבורה אבלית נוצרת סופית היא סכום ישר של חבורה מפותלת וחבורה חסרת פיתול.***

תרגיל 10.7.22 (***) הוכח את המשפט. **הדרכה.** תהי A אבלית נוצרת סופית. לפי תרגילים 10.7.2 ו־10.7.13, $A/t(A)$ נוצרת סופית וחבאת פיתול. לפי משפט 10.7.14, ל־$A/t(A)$ יש בסיס, שלפי תרגיל 10.7.20 כל הרמה שלו יוצרת תת־חבורה חסרת פיתול, A_0. לפי תרגיל 10.7.5, $A_0\cap t(A)=0$. הוכח ש־$A=A_0+t(A)$ והסק שהחבורות משלימות, ו־A הוא סכום ישר לפי תרגיל 6.2.9.

תרגיל 10.7.23 (**) אם $T_1\oplus A_1\cong T_2\oplus A_2$ כאשר T_i מפותלות ו־A_i חסרות פיתול, אז $T_1\cong T_2$.

משפט 10.7.24 ***ההצגה של חבורה כסכום ישר של חבורה מפותלת עם אקספוננט סופי וחבורה חסרת פיתול נוצרת סופית, אם קיימת כזו, היא יחידה.***

תרגיל 10.7.25 (***) הוכח את המשפט. **הדרכה.** נניח ש־$G=T\oplus A$ הוא פירוק כנ"ל. לפי תרגיל 10.7.23, T נקבעת על־ידי G. קח $e=\exp(T)$. לפי משפט 10.7.14 $A=\mathbb{Z}^n$ עבור n מתאים, ולכן $G^e\cong A^e\cong A$; סיים לפי תרגיל 10.7.16.

משפט 10.7.26 ***כל חבורה אבלית נוצרת סופית אפשר להציג באופן יחיד בצורה $\mathbb{Z}_{d_1}\oplus\cdots\oplus\mathbb{Z}_{d_t}$, כאשר $d_1\mid\cdots\mid d_t$; מותרים $d_{s+1}=\cdots=d_t=0$ (כאן $\mathbb{Z}_0=\mathbb{Z}$).***

תרגיל 10.7.27 (-***) הראה שאם $A\oplus B\cong\mathbb{Z}\oplus\mathbb{Z}$, $A,B\neq 0$, אז $A,B\cong\mathbb{Z}$.

10.7.1 חבורות שאינן נוצרות סופית

תרגיל 10.7.28 (**+) החבורה החיבורית $(\mathbb{Q},+)$ חסרת פיתול, ואינה איזומורפית לשום חזקה של $\mathbb{Z}$.

תרגיל 10.7.29 (***) תן דוגמא לחבורה מסדר אינסופי שכל האיברים שלה מסדר המחלק את n.

תרגיל 10.7.30 (***) תן דוגמא לחבורה אבלית אינסופית, כך ש־ A_n סופית לכל n.

תרגיל 10.7.31 (**) הוכח שכל תת־חבורה נוצרת סופית של $\mathbb{Q}^+$ היא ציקלית

תרגיל 10.7.32 (**) הוכח שהחבורות האבליות $\mathbb{Q}^+$, $\mathbb{Q}^\times$ אינן נוצרות סופית.

תרגיל 10.7.33 (**) הוכח שהחבורות $\mathbb{Q}^+$, $\mathbb{Q}^\times$, ${\mathbb{Q}^\times}^+$ אינן איזומורפיות.

פרק 11

מבוא לחוגים

בפרק זה נעשה צעדים ראשונים להבנת מערכת אלגברית שיש בה שתי פעולות: החוג. מן הדוגמאות הרבות לחוגין נתמקד בחוגים של פולינומים במשתנה אחד, משום שאלו החוגים הנחוצים לנו לבניה של שדות, בפרק האחרון.

מושגים: חוג, חוג קומוטטיבי, אידיאל שמאלי וימני, אידיאל. הומומורפיזם של חוגים, חוג מנה, משפט האיזומורפיזם הראשון. שדה, חוג פשוט. אידיאל ראשוני, אידיאל מקסימלי. מחלק אפס, תחום שלמות, שדה שברים. יחס החלוקה, חברות. איבר אי־פריק ואיבר ראשוני. אידיאל ראשי, חוג ראשי. חוג אוקלידי, חוג פולינומים.

11.1 חוגים, תת־חוגים ואידיאלים

הגדרה 11.1.1 חוג (*עם יחידה*) ***הוא מבנה אלגברי הכולל קבוצה*** R ***עם פעולות חיבור וכפל, כך ש־*** $\langle R,+,0\rangle$ ***חבורה אבלית,*** $\langle R,\cdot,1\rangle$ ***מונויד, ו־*** $a(b+c)=ab+ac$, $(a+b)c=ac+bc$.

תרגיל 11.1.2 (**) הוכח, מן האקסיומות בלבד, שבכל חוג R, $0\cdot a=0$ לכל $a\in R$. הוכח ש־$-a=(-1)\cdot a$.

אם R חוג, אז $\langle R,+,0\rangle$ נקראת **החבורה החיבורית** של החוג, ו־$\langle R,\cdot,1\rangle$ **המונויד הכפלי** של החוג.

תרגיל 11.1.3 (*) בדוק שאוסף המטריצות $\mathrm{M}_n(F)$ מעל שדה F הוא חוג.

תרגיל 11.1.4 (*) אוסף הפולינומים מעל שדה, $F[x]$, הוא חוג.

תרגיל 11.1.5 (*) $\mathbb{Z}$ ו־$\mathbb{Z}_n$ (לכל n טבעי) הם חוגים.

תרגיל 11.1.6 (**) אם R,S חוגים, ה**מכפלה הישרה** $R\oplus S$, שהיא המכפלה הקרטזית עם חיבור וכפל לפי רכיבים, היא חוג.

תרגיל 11.1.7 (**) (ראה תרגיל 5.2.7) תהי A חבורה אבלית. הראה שאוסף האנדומורפיזמים $\mathrm{End}(A)$ הוא חוג, ביחס לפעולות החיבור לפי רכיבים והרכבת הפונקציות.

תרגיל 11.1.8 (**) תהי X קבוצה. הראה שקבוצת החזקה $P(X)$ היא חוג ביחס לפעולות ההפרש הסימטרי (כחיבור) והחיתוך (ככפל).

הגדרה 11.1.9 *חוג הוא **קומוטטיבי** אם הכפל קומוטטיבי, כלומר $ab = ba$ לכל $a, b \in R$.*

תרגיל 11.1.10 (־***) נניח שבחוג R מתקיים $x^2 = x$ לכל x. הראה ש־R קומוטטיבי. השווה לחוג $P(X)$ של תרגיל 11.1.8.

תרגיל 11.1.11 (**) חוג המטריצות $\mathrm{M}_n(F)$ אינו קומוטטיבי לכל שדה F ולכל $n \geq 2$.

תת־קבוצה של R שהיא תת־חבורה ביחס לפעולת החיבור (כלומר, סגורה לחיבור ולפעולת הנגדי), נקראת **תת־חבורה חיבורית**.

תרגיל 11.1.12 (**) אם החבורה החיבורית של חוג היא ציקלית, אז החוג קומוטטיבי.

הגדרה 11.1.13 *תת־חבורה חיבורית $S \subseteq R$ הכוללת את איבר היחידה וסגורה לכפל, נקראת **תת־חוג**.*

תרגיל 11.1.14 (־**) הראה שאוסף המטריצות $\left\{\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} : a \in \mathbb{R}\right\}$ הוא חוג, אבל אינו תת־חוג של חוג המטריצות $\mathrm{M}_2(\mathbb{R})$.

חיבור של תת־קבוצות בחוג מוגדר כרגיל: $A + B = \{a + b \colon a \in A, b \in B\}$. בכפל המצב מסובך יותר:

תרגיל 11.1.15 (־***) הראה ש־$\mathbb{Q}[x], \mathbb{Q}[y]$ הם תת־חוגים של $\mathbb{Q}[x,y]$, אבל אוסף המכפלות $\{fg \colon f \in \mathbb{Q}[x], g \in \mathbb{Q}[y]\}$ אינו סגור לחיבור.

הגדרה 11.1.16 *המכפלה של תת־קבוצות $A, B \subseteq R$ מוגדרת כאוסף כל הסכומים הסופיים $A \cdot B = \{a_1b_1 + \cdots + a_nb_n \colon a_1, \dots, a_n \in A, b_1, \dots, b_n \in B\}$.*

הגדרה 11.1.17 *תת־חבורה חיבורית $L \subset R$ היא **אידיאל שמאלי** אם $RL \subseteq L$, **ואידיאל ימני** אם $LR \subseteq L$. תת־קבוצה שהיא אידיאל שמאלי וימני נקראת **אידיאל**. מסמנים, בהתאמה, $L \leq_\ell R$, $L \leq_r R$, ו־$L \triangleleft R$.*

החוג עצמו, למרות שהוא מקיים את דרישת הסגירות לכפל מבחוץ, אינו נחשב לאידיאל.
בחוג קומוטטיבי, המושגים אידיאל, אידיאל שמאלי ואידיאל ימני - מתלכדים.

תרגיל 11.1.18 (*) כל אידיאל שמאלי הוא תת־חוג.

תרגיל 11.1.19 (*) בכל חוג R, הקבוצה $\{0\}$ (שנסמן בדרך כלל בקיצור, 0), הוא אידיאל. (הנקרא **האידיאל הטריוויאלי**).

תרגיל 11.1.20 (*) תת־חבורה חיבורית $L \subset R$ היא אידיאל שמאלי אם ורק אם היא סגורה ל'כפל שמאלי מבחוץ', כלומר, לכל $a \in R$ ו־ $x \in L$, $ax \in L$. נסח תנאי דואלי לאידיאלים ימניים.

תרגיל 11.1.21 (־**) לכל $a \in R$, $Ra = \{xa \colon x \in R\}$ הוא אידיאל שמאלי (או החוג R כולו).

תרגיל 11.1.22 (**) אם $I, J \triangleleft R$, אז $I + J \triangleleft R$ (או $I + J = R$), $IJ \triangleleft R$ ו־ $I \cap J \triangleleft R$.

תרגיל 11.1.23 (-**) $IJ \subset I \cap J$.

תרגיל 11.1.24 (**) אם $L \leq_\ell R$ ו־$R \leq_r T$, אז $LT \lhd R$.

תרגיל 11.1.25 (+**) תן דוגמא לחוג R עם תת־חוג S ואידיאל $I \lhd S$, כך ש־I אינו אידיאל של R.

תרגיל 11.1.26 (+**) תהי $I_1 \subseteq I_2 \subseteq \cdots$ שרשרת עולה של אידיאלים בחוג R. הראה שהאיחוד $\cup I_i$ הוא אידיאל. שים לב לתפקידה של היחידה במניעת האיחוד מלהיות שווה לחוג כולו.

תרגיל 11.1.27 (+**) הראה שהחיתוך של משפחה כלשהי של אידיאלים היא אידיאל.

תרגיל 11.1.28 (**) כל אידיאל של מכפלה ישרה $R_1 \oplus R_2$ הוא מהצורה $I_1 \oplus I_2$ כאשר $I_i \lhd R_i$.

11.2 הומומורפיזמים וחוגי מנה

לכל תת־חבורה חיבורית $S \subseteq R$, מוגדרת חבורת המנה R/S ביחס לפעולת החיבור.

תרגיל 11.2.1 (**) (השווה לתרגיל 5.4.2) פעולת הכפל על R/I מוגדרת היטב אם ורק אם $I \lhd R$ (או $I = R$).

הגדרה 11.2.2 *אם $I \lhd R$, החוג R/I ביחס לפעולות החיבור והכפל של קוסטים, נקרא* **חוג המנה** *ביחס ל־I.*

תרגיל 11.2.3 (*) $n\mathbb{Z} \lhd \mathbb{Z}$, ו־ $\mathbb{Z}_n \cong \mathbb{Z}/n\mathbb{Z}$ כחוגים. (השווה לתרגיל 5.5.4).

הגדרה 11.2.4 *פונקציה $\phi: R \to S$ היא* **הומומורפיזם** *(של חוגים) אם $\phi(1_R) = 1_S$, $\phi(x+y) = \phi(x) + \phi(y)$, ו־$\phi(xy) = \phi(x)\phi(y)$.*

איזומורפיזם, מונומורפיזם, אפימורפיזם, אנדומורפיזם ואוטומורפיזם של חוגים מוגדרים באותו אופן שהם מוגדרים לחבורות.

הגדרה 11.2.5 *ה***תמונה** *של הומומורפיזם ϕ היא תת־הקבוצה $\operatorname{Im}(\phi) = \{\phi(x) \colon x \in R\}$.* **הגרעין** *הוא תת־הקבוצה $\operatorname{Ker}(\phi) = \{x \in R \colon \phi(x) = 0\}$.*

אלו הם למעשה התמונה והגרעין של ההומומורפיזם, כהומומורפיזם בין החבורות החיבוריות

תרגיל 11.2.6 (*) $\operatorname{Im}(\phi)$ הוא תת־חוג של S, ו־$\operatorname{Ker}(\phi)$ הוא אידיאל של R (שים לב ש־$\operatorname{Ker}(\phi) \neq R$).

משפט 11.2.7 (משפט האיזומורפיזם הראשון) *יהיו R, S חוגים, ו־$\phi: R \to S$ הומומורפיזם. אז $R/\operatorname{Ker}(\phi) \cong \operatorname{Im}(\phi)$.*

השווה כמובן למשפט 5.5.1.

תרגיל 11.2.8 (**) יהי $\phi: R \to S$ הומומורפיזם. אם $J \lhd S$ אז $\phi^{-1}(J) \lhd R$.

תרגיל 11.2.9 (+**) הראה שהתמונה $\phi(J)$ של אידיאל אינה בהכרח אידיאל.

תרגיל 11.2.10 (**) אם $\phi: R \to S$ על, אז לכל אידיאל $J \lhd R$, $\phi(J) \lhd S$.

תרגיל 11.2.11 (***) נסח גרסאות של משפטי האיזומורפיזם השני והשלישי לחוגים.

11.3 אידיאלים בחוג קומוטטיבי

11.3.1 שדות

איבר a של חוג R הוא **הפיך** אם הוא הפיך במונויד הכפלי, כלומר, קיים $b \in R$ כך ש־$ab = ba = 1$.

תרגיל 11.3.1 (*) העזר ביחס הסדר הרגיל על $\mathbb{Z}$ ('גדול מ־') כדי להוכיח שהאיברים ההפיכים של $\mathbb{Z}$ הם בדיוק $1, -1$.

תרגיל 11.3.2 (**) השאלה אם איבר הפיך תלויה בחוג: תן דוגמא לחוג R עם תת־חוג S ולאיבר $x \in S$ שהוא הפיך ב־R ואינו הפיך ב־S.

תרגיל 11.3.3 (*) אם איבר הפיך בתת־חוג הוא הפיך גם בחוג עצמו.

הגדרה 11.3.4 ***שדה*** *הוא חוג קומוטטיבי, שבו כל האיברים השונים מאפס הפיכים.*

תרגיל 11.3.5 (**) הראה שאידיאל אינו יכול לכלול איברים הפיכים.

הגדרה 11.3.6 *חוג* ***פשוט*** *הוא חוג שאין לו אידיאלים לא טריוויאליים.*

תרגיל 11.3.7 (**) שדה הוא חוג פשוט.

תרגיל 11.3.8 (**) חוג קומוטטיבי פשוט הוא שדה.

תרגיל 11.3.9 (**) אם $\phi : D \to S$ הוא הומומורפיזם של חוגים ו־D פשוט, אז ϕ חד־חד־ערכי.

11.3.2 אידיאל ראשוני ומקסימלי

הגדרה 11.3.10 *אידיאל $M \lhd R$ הוא* ***מקסימלי*** *אם אין אידיאלים $M' \lhd R$ $M \subset$.*

תרגיל 11.3.11 (*) 0 אידיאל מקסימלי אם ורק אם R חוג פשוט.

משפט 11.3.12 *$M \lhd R$ מקסימלי אם ורק אם חוג המנה R/M פשוט.*

תרגיל 11.3.13 (**+) הוכח את המשפט.

טענה 11.3.14 בחוג קומוטטיבי, $M \lhd R$ מקסימלי אם ורק אם R/M שדה.

תרגיל 11.3.15 (**) הוכח את הטענה.

הגדרה 11.3.16 *יהי R חוג קומוטטיבי. אידיאל $P \lhd R$ הוא* ***ראשוני*** *אם לכל $A, B \lhd R$, אם $AB \subseteq P$ אז $A \subseteq P$ או $B \subseteq P$.*

תרגיל 11.3.17 (-***) P ראשוני אם ורק אם לכל $a, b \in R$, אם $ab \in P$ אז $a \in P$ או $b \in P$.

תרגיל 11.3.18 (**+) נניח ש־ $A, B \lhd R$ ו־$A \cap B$ הוא אידיאל ראשוני. הראה ש־ $A \cap B$ שווה ל־A או ל־B.

תרגיל 11.3.19 (+**) תהי $P_1 \subseteq P_2 \subseteq \cdots$ שרשרת עולה של אידיאלים ראשוניים בחוג R. הראה שהאיחוד $\cup P_i$ הוא אידיאל ראשוני.

תרגיל 11.3.20 (**) P אידיאל ראשוני אם ורק אם $R-P$ סגור לכפל.

הגדרה 11.3.21 *איבר $0 \neq a \in R$ נקרא **מחלק אפס** אם קיים $b \neq 0$ כך ש־ $ab = 0$.*

תרגיל 11.3.22 (**) אידיאל האפס הוא אידיאל ראשוני בחוג, אם ורק אם אין בו מחלקי אפס.

הגדרה 11.3.23 *חוג קומוטטיבי ללא מחלקי אפס נקרא **תחום שלמות**.*

תרגיל 11.3.24 (*) כל שדה הוא תחום שלמות.

תרגיל 11.3.25 (**) כל תת־חוג של תחום שלמות הוא תחום שלמות.

משפט 11.3.26 *יהי R חוג קומוטטיבי. $P \triangleleft R$ הוא ראשוני אם ורק אם R/P תחום שלמות.*

תרגיל 11.3.27 (**) כל אידיאל מקסימלי הוא ראשוני.

הגדרה 11.3.28 *בחוג קומוטטיבי, מגדירים את **הרדיקל** של אידיאל I להיות האידיאל $\sqrt{I} = \{x \in R \colon \exists n : x^n \in I\}$.*

תרגיל 11.3.29 (**) הראה ש־ $\sqrt{I} \triangleleft R$; כמובן $I \subseteq \sqrt{I}$.

תרגיל 11.3.30 (**) $\sqrt{\sqrt{I}} = \sqrt{I}$.

תרגיל 11.3.31 (**) חשב את $\sqrt{12\mathbb{Z}}$ בחוג $\mathbb{Z}$. תן נוסחה כללית ל־$\sqrt{n\mathbb{Z}}$, אם $n = p_1^{a_1} \cdots p_t^{a_t}$.

11.3.3 אידיאלים ראשיים

הגדרה 11.3.32 *אידיאל מהצורה Ra של חוג קומוטטיבי R נקרא **אידיאל ראשי**. במקרה זה, a הוא **יוצר** של האידיאל.*

למרות הדמיון בשמות אין קשר בין ראשוניות וראשיות של אידיאלים.

לפעמים מסמנים את Ra בסימון $\langle a \rangle$. בעקבות תרגיל 11.1.27 ובדומה לתרגיל 4.1.5, מסמנים ב־$\langle S \rangle$ את האידיאל הקטן ביותר המכיל את הקבוצה S.

משפט 11.3.33 *כל האידיאלים של $\mathbb{Z}$ הם ראשיים.*

תרגיל 11.3.34 (**) הוכח את המשפט. **הדרכה**. תרגיל 4.6.10.

תרגיל 11.3.35 (**) $n\mathbb{Z}$ אידיאל ראשוני אם ורק אם $n\mathbb{Z}$ מקסימלי, אם ורק אם n ראשוני.

תרגיל 11.3.36 (-***) יהי $\phi \colon R \to S$ הומומורפיזם של חוגים קומוטטיביים. הראה שאם $P \triangleleft S$ ראשוני, אז גם $\phi^{-1}(P) \triangleleft R$ הוא ראשוני.

תרגיל 11.3.37 (-***) תן דוגמא המראה שאם $M \triangleleft S$ מקסימלי, $\phi^{-1}(P) \triangleleft R$ אינו בהכרח מקסימלי.

תרגיל 11.3.38 (-***) יהי $\phi \colon R \to S$ אפימורפיזם של חוגים קומוטטיביים. הראה שאם $M \triangleleft R$ מקסימלי, אז $\phi(M) \subset S$ (שהוא אידיאל לפי תרגיל 11.2.10) הוא מקסימלי.

תרגיל 11.3.39 (-***) תן דוגמא המראה שתמונת אידיאל ראשוני תחת אפימורפיזם אינה בהכרח אידיאל ראשוני.

11.4 תחומי שלמות

11.4.1 שדה השברים

בתרגיל 11.3.25 הראינו שכל תת־חוג של שדה הוא תחום שלמות.

משפט 11.4.1 *כל תחום שלמות הוא תת־חוג של שדה.*

תרגיל 11.4.2 (**) יהי D תחום שלמות. הוכח שהיחס $(a,b)\sim(a',b')$ אם ורק אם $ab'=ba'$ הוא יחס שלמות על הקבוצה $\{(a,b):\ a,b\in D, b\neq 0\}$.

את מחלקות השקילות של תרגיל 11.4.2 נסמן $a/b=[(a,b)]$. **שדה השברים** של D הוא קבוצת מחלקות השיקלות, שאותה מסמנים ב־$\mathrm{q}(D)$.

תרגיל 11.4.3 (+)** בסימונים אלה, הראה שהפעולות $a/b\cdot c/d=ac/bd$ ו־$a/b+c/d=(ad+bc)/(bd)$ מוגדרות היטב.

תרגיל 11.4.4 (***) הוכח את המשפט. **הדרכה**. הראה ש־$\mathrm{q}(D)$ הוא שדה, וש־$a\mapsto a/1$ הוא שיכון של חוגים $D\to\mathrm{q}(D)$.

תרגיל 11.4.5 (**) הסבר מדוע $\mathbb{Q}=\mathrm{q}(\mathbb{Z})$.

תרגיל 11.4.6 (**) אם F שדה אז $\mathrm{q}(F)\cong F$.

תרגיל 11.4.7 (*) לכל תחום שלמות, $\mathrm{q}(\mathrm{q}(D))\cong\mathrm{q}(D)$.

תרגיל 11.4.8 (*-)** כל הומומורפיזם $\phi\colon D\to D'$ של תחומי שלמות אפשר להרחיב באופן יחיד להומומורפיזם $\mathrm{q}(D)\to\mathrm{q}(D')$.

תרגיל 11.4.9 (+)** יהי F שדה. תאר את שדה השברים של חוג הפולינומים $F[x]$.

11.4.2 איברים בתחומי שלמות

נקבע תחום שלמות R.

תרגיל 11.4.10 (*) a הפיך אם ורק אם $Ra=R$.

הגדרה 11.4.11 *אומרים ש־*$a\,|\,b$ *(*a ***מחלק את*** b*) אם קיים* $c\in R$ *כך ש־* $b=ac$*. (השווה להגדרה 1.1.1).*

תרגיל 11.4.12 (**) יחס החלוקה תלוי בחוג. כלומר, יתכן ש־ $a,b\in S\subset R$, כאשר a מחלק את b ב־R אבל לא ב־S.

תרגיל 11.4.13 (*) $a\,|\,b$ ב־R אם ורק אם $Rb\subseteq Ra$.

הגדרה 11.4.14 a *ו־*b ***חברים*** *אם* $a\,|\,b$ *ו־*$b\,|\,a$*.*

תרגיל 11.4.15 (*) $a\,|\,b$ ב־R אם ורק אם $Rb=Ra$.

תרגיל 11.4.16 (**) הוכח שיחס החברות הוא יחס שקילות על האיברים השונים מאפס ב־R.

תרגיל 11.4.17 (**) הוכח שיחס החלוקה הוא יחס סדר חלש על מחלקות החבורות.

כל איבר $a \in R$ אפשר לפרק $a = au^{-1} \cdot u$, כאשר u הפיך. פירוק כזה, שבו אחד הגורמים הפיך, נקרא **פירוק טריוויאלי**.

הגדרה 11.4.18 *איבר $p \in R$ (שאינו אפס ואינו הפיך) נקרא* ***אי־פריק*** *אם אין לו פירוקים לא־טריוויאליים.*

הגדרה 11.4.19 *איבר $p \in R$ (שאינו אפס ואינו הפיך) הוא* ***ראשוני*** *אם מ־$p \mid ab$ נובע ש־$p \mid a$ או $p \mid b$.*

תרגיל 11.4.20 (+**) כל איבר ראשוני הוא אי־פריק.

תרגיל 11.4.21 (**) האיבר p ראשוני אם ורק אם האידיאל Rp ראשוני.

תרגיל 11.4.22 (+**) האיבר p אי־פריק אם ורק אם Rp הוא מקסימלי בקבוצת האידיאלים הראשיים.

לסיכום נושא זה:

Rp מקסימלי $\Longleftarrow$

Rp ראשוני $\Longleftrightarrow$ p ראשוני $\Longleftarrow$

p אי־פריק $\Longleftrightarrow$ Rp מקסימלי בקבוצת האידיאלים הראשיים.

טענה 11.4.23 אם יש לאיבר a בחוג R פירוק לגורמים ראשוניים, אז זהו הפירוק היחיד בין כל הפירוקים שלו לגורמים אי־פריקים.

תרגיל 11.4.24 (-***) הוכח את הטענה. כלומר: נניח ש־$a = x_1 \cdots x_n = y_1 \cdots y_m$ הם שני פירוקים של a לגורמים אי־פריקים בחוג R. אם כל הגורמים x_i ראשוניים, הראה ש־$m = n$ ושעד כדי סדר, כל y_i הוא חבר של x_i. **הדרכה.** x_n מחלק מכפלה, ולכן את אחד הגורמים שלה, נניח y_m; אבל y_m אי־פריק ולכן $x_n \sim y_m$. צמצם והמשך באינדוקציה על n.

תרגיל 11.4.25 (**) נניח שעל תחום השלמות R מוגדרת פונקציה שומרת כפל $d : R \to \mathbb{Z}$. הראה שאם $d(a)$ ראשוני אז a אי־פריק.

תרגיל 11.4.26 (***) הראה שהפונקציה $N(a+b\sqrt{5}) = a^2 - 5b^2$ על החוג $\mathbb{Z}[\sqrt{5}]$ היא שומרת כפל. העזר בה כדי להוכיח ש־$4 + \sqrt{5}$ אי־פריק. האם הוא ראשוני?

11.4.3 חוגים ראשיים

הגדרה 11.4.27 *תחום שלמות שבו כל האידיאלים ראשיים נקרא* ***חוג ראשי***.

תרגיל 11.4.28 (*) $\mathbb{Z}$ הוא חוג ראשי.

תרגיל 11.4.29 (**) מצא את כל האידיאלים הראשוניים והמקסימליים של $\mathbb{Z} \oplus \mathbb{Z}$.

תרגיל 11.4.30 (+**) חוג הפולינומים $\mathbb{Z}[x]$ אינו ראשי.

תרגיל 11.4.31 (+**) חוג הפולינומים בשני משתנים $\mathbb{Q}[x,y]$ אינו ראשי.

טענה 11.4.32 בחוג ראשי, אם a אי־פריק אז הוא ראשוני.

תרגיל 11.4.33 (⁻***) הוכח את הטענה. **הדרכה**. אם a אי־פריק אז Ra מקסימלי בקבוצת האידיאלים הראשיים לפי תרגיל 11.4.22; אבל מכיוון שהחוג ראשי, Ra מקסימלי, ולפי תרגיל 11.4.21 הוא ראשוני. לפי תרגיל 11.3.27, a ראשוני.

משפט 11.4.34 *בחוג ראשי, כל איבר (שונה מאפס, לא הפיך) אפשר לפרק למכפלה של איברים אי־פריקים.*

תרגיל 11.4.35 (***) הוכח את המשפט. **הדרכה**. נסמן ב־P את קבוצת האברים שהם מכפלות של איברים אי־פריקים; כך P סגורה לכפל. נניח, בשלילה, שקיים $a_0 \neq 0$ לא הפיך שאינו ב־P. בנה באינדוקציה סדרה $a_{n+1} \,|\, a_n$ (מחלק ממש) של איברים שאינם ב־P. אז $Ra_0 \subset Ra_1 \subset Ra_2 \subset \cdots$. אבל $I = \cup_{i=1,\dots} Ra_i$ אידיאל לפי תרגיל 11.1.26, ולכן קיים $d \in R$ כך ש־$I = Rd$. קיים n כך ש־$d \in Ra_n$ ואז $Ra_{n+1} \subseteq I = Rd \subseteq Ra_n$, בסתירה לכך ש־$Ra_{n+1} \subsetneq Ra_n$.

משפט 11.4.36 *בחוג ראשי, כל איבר (שונה מאפס, לא הפיך) מתפרק לגורמים אי־פריקים באופן יחיד.*

תרגיל 11.4.37 (**) הוכח את המשפט. **הדרכה**. משפט 11.4.34 וטענה 11.4.23.

11.4.4 חוגים אוקלידיים

גם אם תכונת פירוק היחיד לגורמים, המתקיימת בכל חוג ראשי, מוצאת חן בעינינו מאד, נותרה לנו בעיה קשה: כיצד להוכיח שחוג מסויים הוא ראשי?

הגדרה 11.4.38 *יהי R תחום שלמות. פונקציה $d\colon R \to \mathbb{N} \cup \{-\infty\}$ המקיימת $d(0) < d(x)$ לכל $x \neq 0$ נקראת* **פונקציה אוקלידית** *אם*

(E1) $d(a) \leq d(b)$ *לכל* $a \,|\, b$, *וכן*

(E2) *לכל* $b \neq 0$ *ולכל* a *קיימים* q, r *כך ש־* $a = qb + r$ *ו־* $d(r) < d(b)$.

תחום שלמות שמוגדרת עליו פונקצייה אוקלידית נקרא **תחום אוקלידי**.

תרגיל 11.4.39 (*) $d\colon R \to \mathbb{N} \cup \{-\infty\}$ 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 11.4.40 (*) בחוג אוקלידי, $d(1) \leq d(x)$ לכל $x \neq 0$.

תרגיל 11.4.41 (⁻**) בחוג אוקלידי, a הפיך אם ורק אם $d(a) = d(1)$.

תרגיל 11.4.42 (**) $\mathbb{Z}$ עם הפונקציה $d(n) = |n|$ הוא חוג אוקלידי. **הדרכה**. משפט 1.2.1.

תרגיל 11.4.43 (⁻***) כל חוג אוקלידי הוא ראשי. **הדרכה**. העזר בהוכחה של משפט 1.3.7: אם $0 \neq I \lhd R$ אידיאל, אז $0 \neq a \in I$ עם $d(a)$ מינימלי הוא יוצר של I.

תרגיל 11.4.44 (***) נניח שהפוקנציה $d\colon R \to \mathbb{N} \cup \{-\infty\}$ 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.

נניח ש־R תחום שלמות. נגדיר $R_0^* = \{0\}$, ולכל $n \geq 0$ נגדיר באינדוקציה $R_{n+1}^* = \{a \in R\colon\ R = Ra + R_n^*\} \cup R_n^*$. אם R תחום אוקלידי עם פונקציה אוקלידית d המקבלת את הערכים $d_0 < d_1 < \dots$, נגדיר $R_n(d) = \{a \in R\colon\ d(a) \leq d_n\}$. לפי ההנחה $R_0(d) = R_0^*$, ולפי תרגיל 11.4.41, $R_1(d) = R_1^*$.

תרגיל 11.4.45 (**) תהי d פונקציה אוקלידית על תחום שלמות R. הראה ש־$R_n(d) \subseteq R_n^*$ לכל n.

תרגיל 11.4.46 (***) נגדיר $d^*(a) = \min_n \{a \in R_n^*\}$. בדוק ש־$R_n(d^*) = R_n^*$. הראה שאם $\cup_n R_n^* = R$, אז d^* פונקציה אוקלידית על R.

תרגיל 11.4.47 (***) הוכח: תחום שלמות R הוא אוקלידי אם ורק אם $\cup_n R_n^* = R$.

תרגיל 11.4.48 (***) הראה שלכל פונקציה אוקלידית על R, $d(a) \geq d^*(a)$, כלומר, d^* היא הפונקציה האוקלידית האיטית ביותר על R. **הדרכה**. תרגיל 11.4.45.

תרגיל 11.4.49 (**) 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 11.4.50 (**) בהמשך לתרגיל 11.4.57, הראה שעבור חוג הפולינומים $R = F[x]$, $d^* = \deg$.

11.4.5 פולינומים מעל שדה

הגדרה 11.4.51 *יהי R חוג קומוטטיבי. החוג $R[x] = \{a_0 + \cdots + a_n x^n :\ a_0, \dots, a_n \in R\}$, עם הפעולות הרגילות, נקרא* ***חוג הפולינומים מעל*** *R.*

תרגיל 11.4.52 (**־) $R[x]$ הוא אכן חוג, המכיל עותק של R.

מגדירים את **הדרגה** $\deg : R[x] - \{0\} \to \mathbb{N}$ כמקובל, $\deg(a_0 + \cdots + a_n x^n) = n$ אם $a_n \neq 0$.

תרגיל 11.4.53 (**+) אם R תחום שלמות, אז $\deg(fg) = \deg(f) + \deg(g)$ לכל $f, g \in R[x]$.

תרגיל 11.4.54 (**) אם R תחום שלמות אז גם $R[x]$ הוא תחום שלמות.

תרגיל 11.4.55 (**) האברים ההפיכים ב־$R[x]$ הם אלו ההפיכים כבר ב־R.

משפט 11.4.56 *יהי F שדה. אז חוג הפולינומים $F[x]$ הוא חוג אוקלידי.*

תרגיל 11.4.57 (***־) הוכח את המשפט. **הדרכה**. הצע אלגוריתם לחילוק עם שארית.

תרגיל 11.4.58 (*) לכל שדה F, $F[x]$ הוא תחום ראשי.

תרגיל 11.4.59 (***) אם $R[x]$ תחום ראשי אז R שדה.

משפט 11.4.60 *כל פולינום מעל שדה F מתפרק לגורמים אי־פריקים באופן יחיד.*

תרגיל 11.4.61 **(**)** הוכח את המשפט. **הדרכה**. $F[x]$ ראשי לפי תרגיל 11.4.58, ולכן הטענה הראשונה נובעת מתרגיל 11.4.36.

משפט 11.4.62 ***אם*** $f \in F[x]$ ***פולינום אי־פריק, אז*** $F[x]/\langle f\rangle$ ***הוא שדה.***

תרגיל 11.4.63 **(**)** הוכח את המשפט. **הדרכה**. $\langle f\rangle$ מקסימלי בקבוצת האידיאלים הראשיים לפי תרגיל 11.4.22; אבל מכיוון שהחוג ראשי, Rf מקסימלי, ולכן חוג המנה ביחס אליו הוא שדה, משפט 11.3.14.

תרגיל 11.4.64 **(**)** לכל פולינום $f \in F[x]$, $F[x]/\langle f\rangle$ מכיל עותק של F, והוא מרחב וקטורי מעליו, ממימד $\deg(f)$.

פרק 12

מבוא לשדות סופיים

מושגים: שורש של פולינום. גזירה פורמלית. תת־שדה. פולינום מינימלי. מאפיין של שדה.

12.1 שורשים של פולינומים

יהי F שדה. אם $f = \sum_{i=0}^{n} a_i x^i \in F[x]$ ו־$a \in F$, אז $f(a) = \sum_{i=0}^{n} a_i a^i$.

הגדרה 12.1.1 ***איבר*** $a \in F$ ***הוא שורש כל*** $f \in F[x]$ ***אם*** $f(a) = 0$.

תרגיל 12.1.2 (*) אם $(x-a)\,|\,f(x)$, אז a הוא שורש של f.

תרגיל 12.1.3 (-*)** a הוא שורש של f אם ורק אם $(x-a)\,|\,f(x)$. **הדרכה.** חילוק עם שארית: כתוב $f(x) = (x-a)q(x) + r(x)$; $\deg(r) < \deg(x-a) = 1$ ולכן $r(x) \in F$. הצב $x = a$ וקבל $r = 0$.

משפט 12.1.4 ***לפולינום ממעלה n מעל שדה יש לכל היותר n שורשים.***

תרגיל 12.1.5 (+)** הוכח את המשפט. **הדרכה.** לפולינום יש פירוק יחיד לגורמים. יש שורש יחיד לכל גורם $x-a$ בפירוק הזה, ומספרם של אלו אינו עולה על n לפי תרגיל 11.4.53.

תרגיל 12.1.6 (**) פולינום ממעלה $1 <$ שיש לו שורש הוא פריק.

תרגיל 12.1.7 (**) לפולינום פריק ממעלה $3 \leq$ יש שורש.

תרגיל 12.1.8 (**) תן דוגמא לפולינום פריק מעל $\mathbb{Q}$ שאין לו שורש שם.

תרגיל 12.1.9 (+)** תת־חבורה כפלית סופית של שדה היא ציקלית. **הדרכה.** תרגיל 10.3.11.

הגדרה 12.1.10 ***מגדירים גזירה פורמלית של פולינומים, לפי*** $(\sum a_i x^i)' = \sum i a_i x^{i-1}$.

תרגיל 12.1.11 (**) הראה ש־ $(f+g)' = f' + g'$ ו־ $(fg)' = fg' + f'g$.

תרגיל 12.1.12 (**) אם $g^2\,|\,f$ אז $g\,|\,f'$.

תרגיל 12.1.13 (**) אם $f' = 1$, אז כל השורשים של f שונים זה מזה.

תרגיל 12.1.14 (**) תן דוגמא לפולינום f מעל שדה, כך ש־$\deg(f') < \deg(f) - 1$. **רמז.** נסה $F = \mathbb{Z}_p$.

12.2 שדות

הגדרה 12.2.1 *תת־חוג F של שדה K הוא* **תת־שדה** *אם F סגור (בנוסף לחיבור, לחיסור וכפל, גם ל)חילוק.*

תרגיל 12.2.2 (*) אם $K \subseteq F$ תת־שדה, אז K הוא מרחב וקטורי מעל F.

את הממד של K מעל תת־השדה F מסמנים ב־$[K:F]$.

תרגיל 12.2.3 (**) יהי F תת־שדה של K, ויהי $a \in K$. אז $\Phi_a : F[x] \to K$ המוגדר לפי $\Phi_a(f) = f(a)$ הוא הומומורפיזם של חוגים.

תרגיל 12.2.4 (**) אם $[K:F] < \infty$ אז Φ_a כנ"ל אינו חד־חד־ערכי.

הגדרה 12.2.5 *יהיו $F \subseteq K$ שדות ו־$a \in K$.* **הפולינום המינימלי** *של a מעל F הוא הפולינום בעל המעלה הקטנה ביותר מעל F המאפס את a, אם קיים כזה.*

תרגיל 12.2.6 (**) אם F, K, a כנ"ל, אז הפולינום המינימלי h הוא מינימלי גם לגבי יחס החילוק, כלומר, הוא מחלק כל פולינום מעל F המאפס את a. **הדרכה**. $\mathrm{Ker}(\Phi_a) = \langle h \rangle$.

תרגיל 12.2.7 (**+) אם F, K, a כנ"ל, אז h אי־פריק ו־$F[a] = \mathrm{Im}(\Phi_a)$ שדה. **הדרכה**. $F[x]/\langle h \rangle \cong \mathrm{Im}(\Phi_a) \subseteq K$, ולכן הוא תחום שלמות; לפי h ראשוני, אבל מכיוון ש־$F[x]$ ראשי, $\langle h \rangle$ מקסימלי, ולכן חוג המנה הוא שדה.

תרגיל 12.2.8 (**) $[F[a]:F] = \deg(h)$.

12.2.1 שורשים ופיצול

משפט 12.2.9 *יהי $p \in F[x]$ פולינום אי־פריק. אז קיים שדה המכיל את F, ממימד $\deg(p)$ מעליו, שבו יש שורש ל־p.*

תרגיל 12.2.10 (-***) הוכח את המשפט. **הדרכה**. קח $K = F[x]/\langle f \rangle$. הוא מכיל עותק של F וממדו מעליו $\deg(p)$ לפי תרגיל 11.4.64; הקוסט $x+\langle f \rangle$ מקיים $f(x+\langle f \rangle) = f(x)+\langle f \rangle = \langle f \rangle$ שהוא איבר האפס של K, ולכן $x + \langle f \rangle \in K$ שורש.

הגדרה 12.2.11 *אומרים ששדה K* **מפצל את** *$f \in F[x]$, אם הפירוק של f בחוג $K[x]$ הוא לגורמים ליניאריים.*

משפט 12.2.12 *לכל פולינום מעל שדה F יש שדה מפצל.*

תרגיל 12.2.13 (***) הוכח את המשפט. **הדרכה**. באינדוקציה על המעלה. קח גורם אי־פריק p של הפולינום; לפי משפט 12.2.9 יש שדה $F \subseteq K$ ובו שורש של p, ולכן של f. מעל K אפשר לכתוב $f(x) = (x-\alpha)f_1(x)$ עם $\deg(f_1) < \deg(f)$, ולפי הנחת האינדוקציה יש שדה $K \subseteq K_1$ המפצל את f_1, ולכן גם את f.

12.2.2 המאפיין של שדה

הגדרה 12.2.14 ***המאפיין*** *של חוג R הוא המספר הקטן ביותר n כך שהסכום $1+1+\cdots+1$ של n עותקים של היחידה, שווה לאפס - אם יש כזה, ואפס אחרת.*

תרגיל 12.2.15 (**) לכל חוג R יש הומומורפיזם $\phi:\mathbb{Z}\to R$ המוגדר היטב על־ידי ההנחה $1\mapsto 1_R$.

תרגיל 12.2.16 (**) המאפיין של R הוא יוצר של הגרעין של ϕ של תרגיל 12.2.15.

תרגיל 12.2.17 (+*)** הראה שהמאפיין של החוג R מתרגיל 11.1.10 הוא 2.

תרגיל 12.2.18 (**) המאפיין של תחום שלמות (ובכלל זה שדה) הוא ראשוני, או אפס.

תרגיל 12.2.19 (**) כל שדה ממאפיין p מכיל עותק של $\mathbb{Z}_p$.

תרגיל 12.2.20 (**) כל שדה ממאפיין 0 מכיל עותק של הרציונליים $\mathbb{Q}$.

תרגיל 12.2.21 (+*)** בשדה ממאפיין p ראשוני, $(a+b)^p=a^p+b^p$. **הדרכה**. הבינום של ניוטון.

תרגיל 12.2.22 (**) בשדה ממאפיין p ראשוני, $(a+b)^{p^n}=a^{p^n}+b^{p^n}$. **הדרכה**. אינדוקציה.

תרגיל 12.2.23 (-*)** בשדה ממאפיין p ראשוני, $x\mapsto x^p$ הוא אוטומורפיזם. **הדרכה**. זהו הומומורפיזם לפי תרגיל 12.2.21, והגרעין טריוויאלי כי $x^p=0$ גורר $x=0$.

12.3 שדות סופיים

תרגיל 12.3.1 (*) לשדה סופי יש מאפיין חיובי.

תרגיל 12.3.2 (-*)** כל שדה סופי הוא מסדר p^n עבור p ראשוני ו־n מתאים. ***הדרכה***. יהי F שדה סופי. לפי תרגיל 12.3.1 המאפיין שלו הוא ראשוני p, ולפי תרגיל 12.2.19 הוא מכיל עותק של $\mathbb{Z}_p$. לפי תרגיל 12.2.2 F הוא מרחב וקטורי מעל $\mathbb{Z}_p$, וממדו כמובן סופי. לכן $F\cong\mathbb{Z}_p^n$ כמרחבים וקטוריים, ומכאן ש־$|F|=p^n$.

משפט 12.3.3 *יש שדה מסדר $q=p^n$.*

תרגיל 12.3.4 (***) הוכח את המשפט. **הדרכה**. לפולינום $f=x^q-x$ יש שדה מפצל L לפי משפט 12.2.12. אוסף השורשים $L_0=\{a\in L:\ a^q=a\}$ סגור לחיבור וכפל לפי תרגיל 12.2.22, ולחילוק לפי $a^{-1}=a^{q-2}$. לכן L_0 שדה. הוא מפצל את f כי כל שורשי f נמצאים בו. לבסוף, $|L_0|=q$ לפי תרגיל 12.1.13.

משפט 12.3.5 *השדה מסדר q הוא יחיד עד־כדי איזומורפיזם.*

כדי להוכיח את המשפט הזה, יש להראות ש'שדה פיצול', שהוא שדה מפצל מינימלי, הוא יחיד עד־כדי איזומורפיזם.

משפט 12.3.6 *יש פולינום אי־פריק מכל מעלה מעל $\mathbb{F}_p$.*

תרגיל 12.3.7 (-***) הוכח את המשפט. **הדרכה.** נניח $q = p^n$. אם $F_q^\times = \langle\alpha\rangle$ לפי תרגיל 12.1.9, אז $\mathbb{F}_q = F_p[\alpha]$ ולכן המעלה של הפולינום המינימלי של α מעל $\mathbb{F}_p$ היא $[\mathbb{F}_q : \mathbb{F}_p] = n$ (תרגיל 12.2.8), והרי הפולינום הזה אי־פריק.

תרגיל 12.3.8 (**) בנה את לוח הכפל של השדה בגודל 4.

תרגיל 12.3.9 (**) בנה את לוח הכפל של השדה בגודל 9.

תרגיל 12.3.10 (+***) בנה את לוח הכפל של השדה בגודל 8.

תרגיל 12.3.11 (+***) פרק את $x^8 - x$ לגורמים אי־פריקים מעל $\mathbb{F}_2$.