מבוא לתורת החבורות

עוזי וישנה

12 בפברואר 2017

מבוא לתורת החבורות

מהדורה 3.931

הקדמה. חוברת זו ערוכה ומסודרת לפי תוכנית הלימודים בקורס "אלגברה מופשטת 1" לתלמידי מתמטיקה, 88-211, באוניברסיטת בר־אילן. הקורס (בהיקף של שלוש שעות הרצאה ושעתיים תרגיל, לאורך סמסטר אחד) הוא קורס ראשון באלגברה מודרנית (אחרי קורס שנתי באלגברה לינארית), והוא מכסה את היסודות של תורת החבורות.

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

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

המבואות בראשי הפרקים אמורים לתת סקירה ממצה של תוכן הפרק; מי שאינו מתכוון לצלוח יותר ממאה וחמישים עמודים של תרגילים עשוי להסתפק בקריאת ראשי הפרקים האלו.

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

עוזי וישנה, 7.2012

תוכן עניינים

פרק 1

חבורות למחצה, מונוידים וחבורות

הקורס עוסק בחבורות, שהן מערכות אלגבריות בעלות פעולה אחת, המקיימת כמה אקסיומות. בפרק הראשון נכיר את המערכות שהן פרימיטיביות עוד יותר מחבורות - אלו שהפעולה שלהן מקיימת רק חלק מן האקסיומות שמקיימות חבורות.

תכונת האסוציאטיביות של הרכבת פונקציות מובילה אותנו לאמץ את האסוציאטיביות כאקסיומה בכל המערכות שנלמד בקורס הזה. הגישה כאן היא אקסיומטית: לומדים את התכונות האבסטרקטיות הנובעות מהנחות יסוד, שאת העניין בהן מצדיקות דוגמאות חשובות.

המושגים העיקריים בפרק זה: פעולה בינארית המקיימת את האקסיומה $a(bc) = (ab)c$ היא **פעולה אסוציאטיבית**. קבוצה שמוגדרת עליה פעולה אסוציאטיבית נקראת **חבורה למחצה**. בחבורה למחצה עשויים להיות אברים מיוחדים: יחידות מימין, יחידות משמאל ויחידות דו־צדדיות; אברי אפס מימין, אפס משמאל, אברי אפס דו־צדדיים. אם יש לחבורה למחצה איבר יחידה (דו־צדדי), היא נעשית **מונויד**. איבר של מונויד עשוי להיות הפיך מימין, הפיך משמאל, או הפיך משני הצדדים (ואז הוא **הפיך**). מונויד שבו כל האברים הפיכים נעשה **חבורה**, וזה האובייקט המרכזי של הקורס. המשפט המרכזי בחלק זה (משפט 1.3.11) קובע שמונויד סופי המקיים את תכונת הצמצום הוא בהכרח חבורה.

הפרק מציג את המכפלה הישרה, שהיא דרך קלה לשילוב מבנים אלגבריים; ואת המושגים הכלליים **תת־חבורה** ו**הומומורפיזם**, שמשחקים תפקיד מרכזי בכל תאוריה אלגברית.

1.1 חבורות למחצה

נפתח בהצגת **חבורות למחצה**, שהן מבנים עם פעולה אסוציאטיבית אחת. תכונות של אברים מיוחדים בחבורה למחצה מובילות בהדרגה להגדרת החבורה.

פעולה בינרית על קבוצה A היא פונקציה $* : A \times A \to A$. *כל פעולה "מוגדרת היטב", כלומר, לכל שני אברים $x, y \in A$ יש ערך יחיד $x * y$, השייך ל־A; אחרת זו אינה פעולה.*
פעולה $*$ היא **אסוציאטיבית** אם לכל $a, b, c \in A$ מתקיים $a * (b * c) = (a * b) * c$.

הגדרה 1.1.1 ***חבורה למחצה*** *היא מערכת הכוללת קבוצה S* ***עם פעולה אסוציאטיבית*** *$*$.*

אומרים ש־S חבורה למחצה (ביחס לפעולה הנתונה), או, כדי להדגיש את תפקידה של הפעולה, שהזוג הסדור $(S, *)$ הוא חבורה למחצה. בדרך כלל קוראים לפעולה בחבורה "כפל", גם אם יש לה בהקשר המקורי שם אחר (כמו "חיבור" או "הרכבה"). במקרים רבים מקובל להשמיט את סימן הכפל, ולכתוב ab במקום $a * b$.

תרגיל 1.1.2 (*) תהי X קבוצה. הראה שהאוסף $S = X^X$ של פונקציות $X \to X$, עם פעולת ההרכבה, הוא חבורה למחצה.

תרגיל 1.1.3 (+)** בחבורה למחצה נגדיר באינדוקציה, לכל איבר x, את החזקות $x^1 = x$, $x^n = x * x^{n-1}$. הוכח ש־$x^{n+m} = x^n * x^m$. **הדרכה**. אינדוקציה כפולה. היכן משתמשים באסוציאטיביות?

תרגיל 1.1.4 (*) תהי S קבוצה. נגדיר $a*b=b$. הוכח ש־$(S,*)$ חבורה למחצה.

תרגיל 1.1.5 (**) בדוק אילו מהמערכות הבאות הן חבורות למחצה.

1. קבוצת המספרים הזוגיים עם פעולת הכפל.
2. קבוצת המטריצות ההפיכות בגודל 3×3 מעל $\mathbb{R}$, ביחס לחיבור.
3. קבוצת המספרים הממשיים, עם הפעולה $a*b=\frac{1}{2}(a^2+b^2)$.

תרגיל 1.1.6 (**) נניח שבחבורה למחצה A אפשר לשחזר את הגורמים a,b מתוך המכפלה ab, כלומר, מ־$ab=cd$ נובע $a=c$ ו־$b=d$. הוכח ש־$|A|=1$. **הדרכה.** לכל $a,b\in A$, $(aa)b=a(ab)$.

הגדרה 1.1.7 ***איזומורפיזם*** *של חבורות למחצה $(X,*)$ ו־$(Y,\star)$ הוא פונקציה חד־חד־ערכית ועל $f:X\to Y$ המקיימת את התנאי $f(x*x')=f(x)\star f(x')$ (לכל $x,x'\in X$).*
אם קיים איזומורפיזם בין שתי חבורות למחצה, אומרים שהן ***איזומורפיות*** *ומסמנים $X\cong Y$.*

תרגיל 1.1.8 (*) אם $f:X\to X'$ איזומורפיזם, אז $f^{-1}:X'\to X$ גם הוא איזומורפיזם.

תרגיל 1.1.9 (**) איזומורפיות היא תכונה רפלקסיבית, סימטרית וטרנזיטיבית. אינננו אומרים שאיזומורפיות היא יחס שקילות, משום שמחלקת החבורות למחצה גדולה מכדי להיות קבוצה, ולא אפשר להגדיר עליה יחסים.

תרגיל 1.1.10 (**) יש בדיוק 5 חבורות למחצה בנות 2 אברים עד־כדי איזומורפיזם. כלומר, יש 5 חבורות למחצה עם שני אברים, שאינן איזומורפיות זו לזו, וכך שכל חבורה למחצה בת שני אברים איזומורפית לאחת מהן. **הדרכה.** מיינו את האפשרויות לפי מספר הפתרונות למשוואה $x*x=x$.

הערה 1.1.11 מספר החבורות למחצה בגודל n גדל במהירות כפונקציה של n: יש 5, 24, 188, 1915, 28634, 1627672, 3684030417, 105978177936292 חבורות למחצה לא איזומורפיות מסדר $3,4,\ldots,9$ [סדרה *A027851* באנציקלופדיה לסדרות של מספרים טבעיים של *N. J. A. Sloane*]. (השווה להערה 1.2.14).

תרגיל 1.1.12 (-*)** (בעיה A-1 מתחרות Putnam ה־62, 2001) פעולה בינארית (לאו דווקא אסוציאטיבית) $*:S\times S\to S$ מקיימת את החוק $a*(b*a)=b$; הוכח שהיא מקיימת גם $(a*b)*a=b$.

1.1.1 איברי יחידה

יש הרבה חבורות למחצה. כדי לבנות מסגרת שתאפשר לנתח את המבנה שלהן, עלינו לזהות איברים בעלי תכונות מיוחדות.

הגדרה 1.1.13 *תהי $(S,*)$ חבורה למחצה. איבר $e\in S$ נקרא* ***יחידה מימין*** *אם לכל $b\in S$ מתקיים $be=b$,* ***ויחידה משמאל*** *אם לכל $b\in S$ מתקיים $eb=b$.* יחידה מימין היא איבר הפועל כיחידה כאשר כופלים בו מימין, וכן משמאל.
איבר שהוא יחידה מימין ומשמאל נקרא ***איבר יחידה****.*

תרגיל 1.1.14 (*) אם בחבורה למחצה יש יחידה מימין e ויחידה משמאל e', אז $e=e'$ (וזהו כמובן איבר יחידה).

תרגיל 1.1.15 (*) בחבורה למחצה S יש שבע יחידות משמאל. כמה יחידות מימין יש בה?

תרגיל 1.1.16 (**) קבע, לגבי כל אחת מהחבורות למחצה של תרגיל 1.1.10, מיהם אברי היחידה מימין ומשמאל.

תרגיל 1.1.17 (**) 1. $M = \left\{\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} : a, b \in \mathbb{R}\right\}$ היא חבורה למחצה (ביחס לכפל מטריצות).

2. ב־M אין יחידה מימין, אבל יש אינסוף יחידות משמאל.

3. מצא דוגמה לחבורה למחצה בלי יחידות משמאל ועם אינסוף יחידות מימין.

1.1.2 אידמפוטנטים ואברים מיוחדים אחרים

הגדרה 1.1.18 *איבר e בחבורה למחצה נקרא* ***אידמפוטנט*** *אם $e^2 = e$ (כזכור $e^2 = e * e$).*

תרגיל 1.1.19 (*) כל איבר יחידה, מימין או משמאל, הוא אידמפוטנט.

הגדרה 1.1.20 *איברים $a, b \in S$ נקראים* ***הפוכים*** *(****באופן חלש****) זה לזה, אם $a = aba$ ו־$b = bab$.*

תרגיל 1.1.21 (**) נניח ש־a, b הפוכים זה לזה. הוכח ש־ab ו־ba אידמפוטנטים.

תרגיל 1.1.22 (**) אם b ו־b' שניהם הפוכים ל־a, אז ab' ו־ab הפוכים זה לזה (וכך גם $ba, b'a$).

תרגיל 1.1.23 (**) אם b ו־b' שניהם הפוכים ל־a, אז כך גם bab' ו־$b'ab$.

תרגיל 1.1.24 (**) נתון ש־b' הפוך ל־a, a הפוך ל־b, ו־b הפוך ל־a'. הוכח ש־bab' הפוך ל־aba'.

תרגיל 1.1.25 (**) e, e' הם שני אידמפוטנטים הפוכים זה לזה. כתוב את לוח הכפל של הקבוצה $\{e, e', ee', e'e\}$.

תרגיל 1.1.26 (**) חבורה למחצה היא **מגבילה** (restrictive) אם כל איבריה אידמפוטנטים, והיא מקיימת את החוק $xyz = yxz$. (חבורות למחצה אלו הוגדרו על־ידי V. V. Wagner, 1962, שהראה שהן מתקבלות ממערכות של העתקות עם פעולת צמצום הדדית שלא נתאר כאן במלואה.) מיין את כל החבורות למחצה המגבילות עם שלושה אברים.

תרגיל 1.1.27 (**) חבורה למחצה היא **רצועה רגולרית שמאלית** אם היא מקיימת את החוקים $x^2 = x$ ו־$xyx = xy$ לכל x, y. על אוסף המלים בקבוצת האותיות S, שבהן כל אות מופיעה לכל היותר פעם אחת, נגדיר פעולה באופן הבא: $u * v$ היא המלה המתקבלת מקריאת המלה uv משמאל לימין, ומחיקת כל אות שכבר הופיעה. הראה שמתקבלת רצועה שמאלית רגולרית. כתוב את לוח הכפל במקרה $|S| = 2$.

הגדרה 1.1.28 *איבר $z \in S$ המקיים $za = z$ לכל $a \in S$ נקרא* ***אפס משמאל****. אם $az = z$ לכל $a \in S$ אז z נקרא* ***אפס מימין****. אפס מימין ומשמאל נקרא* ***אפס*** *של החבורה למחצה S.*

תרגיל 1.1.29 (*) אם בחבורה למחצה יש אפס מימין ואפס משמאל, אז הם שווים. מכאן שאם יש איבר אפס, אז הוא יחיד. (השווה לתרגיל 1.1.14.)

תרגיל 1.1.30 (**) תן דוגמה לחבורה למחצה שיש בה איבר אפס, ולחבורה למחצה בלי איבר כזה.

תרגיל 1.1.31 (**) איזומורפיזם של חבורות למחצה מעביר יחידה משמאל ליחידה משמאל, יחידה ליחידה, אידמפוטנט לאידמפוטנט ואפסים לאפסים.

תרגיל 1.1.32 (+)** נסמן $x \star y = \frac{x+y}{1+xy}$ (זוהי הנוסחה היחסותית לחיבור מהירויות, ביחידות של מהירות האור). הראה שהקטע $[0,1]$ הוא מונויד ביחס לפעולה $\star$, ובו 0 הוא איבר יחידה, ו־1 הוא איבר אפס. תן נוסחה מפורשת למכפלה $x \star \cdots \star x$ (n פעמים). הראה ש־$([0,1],\star)$ איזומורפי ל־$([0,\infty],+)$. **הדרכה.** קח $f:[0,\infty]\to[0,1]$ לפי $f(t)=\frac{e^t-e^{-t}}{e^t+e^{-t}}$.

תרגיל 1.1.33 (+)** נסמן $x \star y = \frac{x+y}{1-xy}$, ו־$x \star \infty = \infty \star x = -\frac{1}{x}$. הראה ש־$(\mathbb{R}\cup\{\infty\},\star)$ הוא מונויד, כש־0 הוא איבר היחידה.

תרגיל 1.1.34 (***) יהי $\lambda > -1$ מספר ממשי. נגדיר $x \circ y = \frac{xy+\lambda}{x+y+2}$.

1. הוכח שהקטע $I=(-1,\infty)$ הוא חבורה למחצה ביחס לפעולה $\circ$.
2. נניח ש־$e^2+2e=\lambda$ עבור $e\in I$ (בדוק ש־e יחיד). הוכח ש־e איבר אפס של הפעולה.
3. נרחיב את $\circ$ לקטע המוכלל $[-1,\infty]$ על־ידי מעבר לגבול:
$$a\circ(-1)=(-1)\circ a=\lim_{x\to(-1)^+} x\circ a, \qquad a\circ\infty=\infty\circ a=\lim_{x\to\infty} x\circ a;$$
וכן הלאה עבור $(-1)\circ(-1)$, $(-1)\circ\infty=\infty\circ(-1)$ ו־$\infty\circ\infty$. בדוק ש־$(-1)\circ(-1)=\infty$, וש־∞ הוא איבר יחידה בקטע החדש.
4. נסמן $a^*=(-1)\circ a$. 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. הוכח שלכל $a\in I$, $\lim_{n\to\infty}a^n=e$. **רמז.** פרק לגורמים את $a\circ b-e$.

(ראה גם תרגיל 1.4.3)

תרגיל 1.1.35 (+)** ב**משחק קומבינטורי** לשני משתתפים עם מידע מלא, כל שחקן מבצע מהלך בתורו, עד שאחד השחקנים נותר ללא מהלך חוקי והוא מוכרז כמפסיד. המשחק **סופי** אם כל סדרת מהלכים מוכרחה להסתיים בהפסד של אחד השחקנים. נניח שהמשחק סופי. מצב **מפסיד** הוא מצב שבו השחקן אינו יכול לנוע, או שכל מהלך מוביל למצב **זוכה**; ומצב זוכה הוא מצב שבו קיים מהלך המוביל למצב מפסיד.

1. הוכח שהמושגים 'מפסיד' ו'זוכה' מוגדרים היטב, באינדוקציה (למרות שההגדרה נדמית מעגלית), ושכל משחק סופי הוא או מפסיד או זוכה.
2. ה**סכום** $\alpha+\beta$ של שני משחקים α,β הוא המשחק שמהלך חוקי שלו מחזיר את $\alpha+\beta'$ כאשר β' מתקבל ממהלך חוקי ב־β, או את $\alpha'+\beta$ כאשר α' מתקבל במהלך חוקי מ־α.

   הראה שאם α,β שניהם זוכים או שניהם מפסידים, אז $\alpha+\beta$ זוכה; ואם α זוכה ו־β מפסיד או להיפך, אז $\alpha+\beta$ מפסיד.
3. נסמן ב־$s(\alpha)\in\{W,L\}$ את סוג המשחק α, זוכה (W) או מפסיד (L). הצע פעולה $+$ על הקבוצה $\{L,W\}$ כך ש־$s(\alpha+\beta)=s(\alpha)+s(\beta)$.
4. פקודות מטכ"ל אוסרות על חיילים לנוע בגפם. לקצינים מותר לפצל קבוצת חיילים רק בתנאי ששני החלקים מצייתים לפקודה. שני קצינים משחקים בפיצול חוזר של פלוגת חיילים: הראשון שאינו יכול לפצל, מפסיד. הראה שאם בפלוגה יותר משבעה חיילים, הקצין הראשון יכול לנצח.

1.2 מונוידים

הגדרה 1.2.1 *חבורה למחצה M שיש בה איבר יחידה נקראת מונויד.*

במלים אחרות, מונויד הוא מערכת הכוללת קבוצה, פעולה אסוציאטיבית, ואיבר יחידה. כשמדובר במונויד אבסטרקטי, מקובל להקצות את הסימון 1 לאיבר היחידה (יש ספרים המעדיפים את הסימון e למטרה זו, כדי להתאים למקרים שבהם איבר היחידה כבר זכה לסימון משלו). כדי להדגיש את הנחיצות של המרכיבים השונים, מציגים את המונויד לפעמים גם כשלשה סדורה, $(M,\cdot,1)$. כשאיבר היחידה ידוע אפשר להשמיט אותו מהסימון.

תרגיל 1.2.2 (**) תהי A קבוצה. הוכח ש־$M=A^A=\{f:A\to A\}$ עם פעולת ההרכבה הוא מונויד.

תרגיל 1.2.3 (**) יהי V מרחב וקטורי מעל שדה F. הוכח שאוסף ההעתקות הלינאריות $\mathrm{Hom}_F(V)=\{T:V\to V\}$, עם פעולת ההרכבה, הוא מונויד.

תרגיל 1.2.4 (+*) כתוב את לוחות הכפל של כל שבעת המונוידים בעלי 3 אברים. (המיון הוא עד־כדי איזומורפיזם, כמובן.)

תרגיל 1.2.5 (**) אם $S\cong S'$ חבורות למחצה איזומורפיות, ו־S היא מונויד, אז גם S' הוא מונויד (ראה תרגיל 1.1.31).

תרגיל 1.2.6 (*) קבע לגבי כל אחת מהמערכות הבאות האם היא חבורה למחצה והאם היא מונויד.

1. $\mathbb{R}_{>0}=\{x:\ x>0\}$ עם פעולת הכפל.
2. אוסף המטריצות $\mathrm{M}_n(F)$ עם פעולת הכפל.
3. $\mathbb{Z}$ עם פעולת החיסור.
4. אוסף המספרים הרציונליים עם הכפל הרגיל.

תרגיל 1.2.7 (+*) קבע לגבי כל אחת מהמערכות הבאות האם היא מונויד. הפעולה היא בכל מקרה כפל נקודתי, $(f*g)(t)=f(t)\cdot g(t)$.

1. אוסף הפונקציות הרציפות $[0,1]\to\mathbb{R}$.
2. אוסף הפונקציות הרציפות שאינן מתאפסות זהותית בקטע $[0,1]$.
3. אוסף הפוקנציות הרציפות שאינן מתאפסות זהותית באף תת־קטע פתוח של $[0,1]$.

תרגיל 1.2.8 (**) השלם את לוח הכפל של מונויד $M=\{1,a,b,c\}$ שבו 1 איבר יחידה, $ab=c$, $bc=a$ ו־$ca=b$.

תרגיל 1.2.9 (**) הראה שכל חבורה למחצה S אפשר להרחיב למונויד $S'=S\cup\{e\}$, אם נגדיר את e להיות איבר היחידה במבנה החדש.

תרגיל 1.2.10 (**) תאר את המונויד המתקבל לאחר חזרה n פעמים על הבניה של תרגיל 1.2.9, כשמתחילים ממונויד האפס $M=\{0\}$.

תרגיל 1.2.11 (**) 1. M מונויד. נקבע $z\notin M$, ונרחיב את הפעולה לפי $zm=mz=z$. הוכח ש־$M\cup\{z\}$ מונויד, שבו z הוא איבר האפס.

2. נניח ש־$M=\{0\}$. תאר את המונויד המתקבל אחרי n הפעלות של התהליך הזה. הראה שהוא איזומורפי למונויד של תרגיל 1.2.10.

תרגיל 1.2.12 (**) נאמר שפולינום $f(x)$ ממעלה n הוא **פולינדרום** אם $f(x)=x^nf(x^{-1})$ (בדוק שהגדרה זו שקולה לכך שהפולינום הוא מהצורה $a_0+a_1x+a_2x^2+\cdots+a_2x^{n-2}+a_1x^{n-1}+a_0x^n$). הראה שאוסף הפולינומים הפולינדרומיים הוא מונויד ביחס לכפל. הוכח שכל פולינום פולינדרומי הוא מהצורה $x^mg(x+x^{-1})$ כאשר g פולינום ממעלה m.

תרגיל 1.2.13 (**) מיין, עד כדי איזומורפיזם, את על המונוידים מסדר 4 שכל איבריהם מקיימים את הזהות $x^2=x$.

הערה 1.2.14 מספר המונוידים בגודל n גדל במהירות כפונקציה של n: יש 7, 35, 228, 2237, 31559, 1668997 מונוידים לא איזומורפיים מסדר $3,4,\dots,8$ [סדרה *A058129* באנציקלופדיה לסדרות של מספרים טבעיים של *N. J. A. Sloane*]. (השווה להערה 1.1.11; תרגיל 1.2.9 מסביר את הקשר בין הסדרות.)

1.2.1 איברים הפיכים מימין ומשמאל

כמו במקרה של חבורות למחצה, איברים מיוחדים הם הצעד הראשון לפענוח המבנה של מונוידים.

הגדרה 1.2.15 *יהי M מונויד.*
*איבר $a\in M$ **הוא הפיך מימין** אם קיים $b\in M$ כך ש־$ab=1$, **והפיך משמאל** אם קיים $b\in M$ כך ש־$ba=1$.*
*האיבר a **הוא הפיך** אם קיים $b\in M$ כך ש־$ab=ba=1$.*

תרגיל 1.2.16 (+*) אם a הפיך מימין ומשמאל אז הוא הפיך. מה יש כאן להוכיח?

תרגיל 1.2.17 (**) אם a הפיך אז האיבר b המקיים $ab=1$ הוא יחיד; מסמנים אותו בסימון a^{-1}.

תרגיל 1.2.18 (**) הראה שאם a הפיך אז a^{-1} הפיך ו־$(a^{-1})^{-1}=a$.

תרגיל 1.2.19 (**) אם a,b הפיכים אז ab הפיך ו־$(ab)^{-1}=b^{-1}a^{-1}$.

תרגיל 1.2.20 (**) אם a הפיך אז לכל $n>0$, $(a^n)^{-1}=(a^{-1})^n$.

תרגיל 1.2.21 (+*)** הוכח את כללי החזקות $a^na^m=a^{n+m}$, $(a^n)^m=a^{nm}$, לכל $n,m\in\mathbb{Z}$.
הדרכה. ראשית הוכח את הטענות באינדוקציה כפולה עבור $n,m\in\mathbb{N}$ ואז הוכח לערכים שלמים כלשהם בעזרת תרגיל 1.2.20.

תרגיל 1.2.22 (**) אם aba הפיך אז גם a,b הפיכים.

תרגיל 1.2.23 (**) קבע אילו איברים של המונויד A^A מתרגיל 1.2.2 הם הפיכים מימין או משמאל. חזור על השאלה עבור המונויד $\mathrm{Hom}_F(V)$ מתרגיל 1.2.3.

תרגיל 1.2.24 (**) נתבונן בקבוצה $X=\mathbb{N}^{\mathbb{N}}$ של פונקציות $\mathbb{N}\to\mathbb{N}$. נסמן ב־u,d את הפונקציות $u(n)=n+1$, $d(n)=\max\{n-1,0\}$ (הפונקציה $n\mapsto n-1$ אינה מוגדרת). חשב את ההרכבות du ו־ud. הסק ש־d הפיך מימין ו־u הפיך משמאל, אבל שניהם לא הפיכים.

תרגיל 1.2.25 (**) יהי F שדה ו־$V=F^{\aleph_0}$ מרחב הסדרות מעל F. נתבונן בהעתקות $U:(x_1,x_2,\dots)\mapsto(0,x_1,x_2,\dots)$, $D:(x_1,x_2,\dots)\mapsto(x_2,x_3,\dots)$ השייכות ל־$\mathrm{Hom}_F(V)$. חשב את UD ואת DU במונויד $\mathrm{Hom}_F(V)$. הסק ש־D הפיך מימין ו־U הפיך משמאל, אבל שניהם לא הפיכים.

תרגיל 1.2.26 (**) אם במונויד מתקיים $aba = a$ ו־$ab^2a = 1$, אז $a = b^{-1}$.

תרגיל 1.2.27 (**) M מונויד סופי, ו־ $a \in M$ הפיך מימין. הוכח ש־a הפיך.

תרגיל 1.2.28 (**) 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. הראה שאם $(M, *)$ מונויד, אז הוא איזומורפי ל־$(M, \bullet)$.

תרגיל 1.2.29 (**) הראה שאוסף הפולינומים (מעל שדה נתון) הוא מונויד ביחס להרכבה. מהם האברים ההפיכים מימין? ומשמאל?

1.3 חבורות

הגדרה 1.3.1 ***מוניד שבו כל האברים הפיכים נקרא חבורה.***

במלים אחרות, חבורה היא קבוצה G עם פעולה אסוציאטיבית, איבר יחידה 1, ולכל x קיים y כך ש־$xy = yx = 1$. כמו במונוידים, אומרים לפעמים ש־$(G, \cdot, 1_G)$ היא חבורה.

תרגיל 1.3.2 (*–)** נניח שבחבורה למחצה S יש יחידה משמאל e, והופכי משמאל לכל איבר (כלומר לכל a יש a' כך ש־$a'a = e$; לא ידוע ש־a' הנ"ל הוא יחיד). אז S חבורה. **הדרכה.** מכיוון ש־$aa' = aea' = a(a'a)a' = (aa')(aa')$, קיבלנו $e = (aa')'(aa') = (aa')'(aa')(aa') = e(aa') = aa'$. לכן גם $a = ae = aa'a = ae$, ומכאן ש־e יחידה מימין ו־a' ההפכי של a.

תרגיל 1.3.3 (*) באוסף המטריצות $\left\{\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} : a, b \in F, a \neq 0\right\}$ יש יחידה משמאל, וכל האברים ניתנים לצמצום מימין, אבל זו לא חבורה.

תרגיל 1.3.4 (***) אם בחבורה למחצה S יש פתרון לכל משוואה מהצורה $ax = b$ או $xa = b$, אז זו חבורה. **הדרכה.** יהי $a \in S$. לפי ההנחה יש $e \in S$ (התלוי ב־a) כך ש־$ae = a$. לכל $c \in S$ קיים x כך ש־$xa = c$, ואז $ce = xae = xa = c$; מכאן ש־e יחידה מימין. באותו אופן יש יחידה משמאל, ונותר לבחור $b = e$.

הגדרה 1.3.5 ***אומרים שבחבורה למחצה S יש צמצום משמאל אם לכל $a, x, y \in S$, $ax = ay \implies x = y$, וצמצום מימין אם $xa = ya \implies x = y$.***

תרגיל 1.3.6 (*+) כל מונויד המוכל בחבורה (עם אותה פעולה) הוא בעל צמצום מימין ומשמאל.

תרגיל 1.3.7 (***) חבורה למחצה סופית S עם צמצום מימין ומשמאל היא מונויד. **הדרכה.** נבחר $a \in S$. על־ידי צמצום משמאל, הפונקציה $\ell_a : x \mapsto ax$ חד־חד־ערכית, ומכיוון ש־S סופית ℓ_a גם על, ולכן יש $e \in S$ כך ש־$ae = a$ (אולי e תלוי ב־a). לכל $x \in S$, $aex = ax$, ועל־ידי צמצום משמאל נובע $ex = x$, כלומר e יחידה משמאל. בפרט $ee = e$, ולכל $x \in S$ מתקיים $xee = xe$. על־ידי צמצום מימין מתקבל $xe = x$, כלומר e איבר יחידה.

תרגיל 1.3.8 (**) S חבורה למחצה סופית, ו־$Sa = aS = S$ לכל $a \in S$. הוכח ש־S מונויד.

תרגיל 1.3.9 (**) מונויד שבו כל האברים הפיכים מימין הוא חבורה.

תרגיל 1.3.10 (**+)** האם מונויד שבו כל איבר הפיך מימין או משמאל הוא בהכרח חבורה?

משפט 1.3.11 ***מוניד סופי עם צמצום משמאל הוא חבורה.***

זה המשפט המרכזי על מונוידים.

תרגיל 1.3.12 (+)** הוכח את משפט 1.3.11. **הדרכה.** יהי $(M, 1)$ מונויד סופי עם צמצום משמאל. לכל $a \in M$, הפונקציה $\ell_a : x \mapsto ax$ חד־חד־ערכית ולכן על; לכן קיים a' כך ש־$aa' = 1$, כלומר a הפיך מימין. סיימנו לפי תרגיל 1.2.27, או בעזרת העובדה שגם a' הפיך מימין.

תרגיל 1.3.13 (+)** תן דוגמה למונויד (אינסופי) עם צמצום משמאל שאינו חבורה.

תרגיל 1.3.14 (**) הוכח שהמערכות הבאות הן חבורות:

1. $\left\{\begin{pmatrix} x & y \\ -y & x \end{pmatrix} : x,y \in \mathbb{R},\ (x,y) \neq (0,0)\right\}$, עם כפל המטריצות הרגיל.
2. $\mathbb{R}^* = \mathbb{R} \cup \{\infty\}$ עם הפעולה $a*b = \frac{a+b}{1-ab}$ אם $a,b \neq \infty$ ו־$ab \neq 1$; $a * \frac{1}{a} = \infty$; $\infty * a = a * \infty = -\frac{1}{a}$ ל־$a \neq 0$; $\infty * 0 = 0 * \infty = \infty$; $\infty * \infty = 0$.

תרגיל 1.3.15 (**) תהי G חבורה עם $a,b \in G$. הוכח: למשוואה $xax = b$ יש פתרון אם ורק אם ab הוא ריבוע ב־G. **הדרכה.** אם $xax = b$ אז $(ax)^2 = ab$.

תרגיל 1.3.16 (***) תהי G חבורה עם $a \in G$. הוכח: למשוואה $x^2ax = a^{-1}$ יש פתרון אם ורק אם a הוא חזקה שלישית ב־G. **הדרכה.** אם $ax^2ax = 1$ אז $x = (ax^2)^2$, ומכאן $x(ax^2) = (ax^2)x$ ו־$ax = xa^{-1}$.

תרגיל 1.3.17 (**) נתבונן בפונקציות הממשיות $f_a \colon x \mapsto \frac{x}{\sqrt{1+ax^2}}$. הוכח ש־$\{f_a \colon a \in \mathbb{R}\}$ היא חבורה ביחס להרכבת פונקציות. נסו להמציא דוגמאות משלכם.

תרגיל 1.3.18 (**) כתוב את לוח הכפל של חבורה בגודל 6, שבה יש איברים σ, τ המקיימים $\sigma\tau \neq \tau\sigma$, $\sigma^3 = 1$, $\tau^2 = 1$. **הדרכה.** איברי החבורה הם $1,\sigma,\sigma^2,\tau,\sigma\tau,\sigma^2\tau$; הוכח שכל אלה שונים זה מזה, ומצא את $\tau\sigma$, שמוכרח להיות איבר באותה רשימה.

תרגיל 1.3.19 (**) תהי $(S,*)$ חבורה למחצה. מסמנים ב־S^{op} את החבורה למחצה $(S,\bar{*})$ כאשר $a \bar{*} b = b * a$.

1. אם M מונויד אז M^{op} מונויד; אם G חבורה אז G^{op} חבורה.
2. הראה שלכל חבורה G, $G \cong G^{\mathrm{op}}$.
3. תן דוגמה לחבורה למחצה S כך ש־$S \not\cong S^{\mathrm{op}}$.

1.4 תת־מבנים

המפתח לתורת המבנה של החבורות (וגם של מונוידים וחבורות למחצה, שבקורס הזה משחקות תפקיד משנה בלבד) הוא בקשרים בינן לבין תת־חבורות שלהן.

1.4.1 תת־חבורה למחצה

הגדרה 1.4.1 *תהי S חבורה למחצה. תת־קבוצה $S' \subseteq S$ נקראת תת־חבורה־למחצה אם היא תת־חבורה למחצה ביחס לפעולה המושרית מ־S.*

הפעולה המושרית היא הפעולה של S, כשמיישמים אותה לאברי S' בלבד. פעולה בינארית היא פונקציה $S \times S \to S$, כלומר, פורמלית, האוסף $\{(a,b,a*b)\}$ של שלשות סדורות ב־$S \times S \times S$. הפעולה המושרית היא החיתוך של הפעולה עם $S' \times S' \times S'$. אם $a*b \notin S'$, הפעולה החדשה אינה מוגדרת היטב, משום שאין בה שלשה מהצורה (a,b,x).

תרגיל 1.4.2 (*) תת־קבוצה לא ריקה של חבורה למחצה S היא תת־חבורה למחצה אם ורק אם היא סגורה לכפל.

תרגיל 1.4.3 (-*)** בתרגיל 1.1.34, מצא את כל תת־החבורות־למחצה מהצורה (a,b), $(a,b]$, $[a,b)$ או $[a,b]$ של $[-1,\infty]$. **הערה.** אלו הן תת־החבורות הקשירות. התוכל למצוא תת־חבורה שאינה קשירה?

תרגיל 1.4.4 (**) תהי S חבורה למחצה. אם $e \in S$ אידמפוטנט, אז $eSe = \{exe \colon x \in S\}$ תת־חבורה־למחצה שהיא מונויד, עם איבר היחידה e (מדוע $e \in eSe$?)

1.4.2 תת־מונויד

הגדרה 1.4.5 *יהי M מונויד עם יחידה 1_M. תת־קבוצה $M' \subseteq M$ היא **תת־מונויד** אם היא סגורה לכפל ו־ $1_M \in M'$.*

אם $M' \subseteq M$ הוא תת־מונויד מקובל לסמן $M' \leq M$.

תרגיל 1.4.6 (+*) יהי V מרחב וקטורי. אז $\mathrm{Hom}_F(V)$ הוא תת־מונויד של V^V ביחס לפעולת ההרכבה.

תרגיל 1.4.7 (**) תהי I קבוצה של אינדקסים, ויהיו $M_i \leq M$ $(i \in I)$ תת־מונוידים. הוכח ש־$\bigcap M_i$ תת־מונויד. *מדובר בחיתוך כלשהו, לאו דווקא סופי או בן־מניה.*

הגדרה 1.4.8 *קבוצה סדורה חלקית I נקראת **קבוצה מכוונת** אם לכל $i, j \in I$ יש $k \in I$ כך ש־ $k > i, j$.*

תרגיל 1.4.9 (**) תהי I קבוצה מכוונת. מערכת של מונוידים $\{M_i\}_{i \in I}$ נקראת **רשת עולה** אם לכל $i < j$ מתקיים $M_i \subseteq M_j$. הוכח שבמקרה זה $\bigcup M_i$ הוא מונויד. (מדוע נדרשנו להניח ש־I מכוונת? ומדוע נדרשת ההנחה שזו רשת עולה?)
בפרט: אם $M_1 \subseteq M_2 \subseteq \cdots$ מונוידים, גם איחוד השרשרת $\bigcup M_i$ הוא מונויד.

1.4.3 תת־חבורה

הגדרה 1.4.10 *תהי G חבורה. תת־קבוצה $H \subseteq G$ היא **תת־חבורה** אם היא מהווה חבורה ביחס לפעולה המושרית מ־G.*

גם כאן, הסימון $H \leq G$ מיוחד לתת־חבורות.

תרגיל 1.4.11 (**) תת־קבוצה לא ריקה H של חבורה G היא תת־חבורה אם ורק אם היא כוללת את איבר היחידה, סגורה לכפל, וסגורה להיפוך (כלומר לכל $x \in H$ מתקיים $x^{-1} \in H$).

תרגיל 1.4.12 (**) תהי H תת־קבוצה לא ריקה של חבורה G. אם לכל $x, y \in H$ מתקיים $xy^{-1} \in H$, אז $H \leq G$.

תרגיל 1.4.13 (**) אם G חבורה סופית ו־$\emptyset \neq H \subseteq G$ סגורה לכפל, אז H תת־חבורה. **הדרכה.** משפט 1.3.11

תרגיל 1.4.14 (*) בכל חבורה G, הקבוצה $\{1_G\}$ היא תת־חבורה, הנקראת **תת־החבורה הטריוויאלית**. בדרך כלל נשמיט את סימון הקבוצה, ונדבר על תת־החבורה 1.

תרגיל 1.4.15 (*) אם $N \leq H$ ו־$H \leq G$, אז $N \leq G$.

תרגיל 1.4.16 (*) תהיינה H, G_1, G_2 תת־חבורות של G. אם $H \subseteq G_1 \cup G_2$ אז $H \subseteq G_1$ או $H \subseteq G_2$. בפרט איחוד של שתי תת־חבורות אינו יכול להיות תת־חבורה, אלא אם הוא שווה לאחת מהן. (ראה גם תרגיל 1.5.5.)

הגדרה 1.4.17 *יהי M מונויד. מסמנים ב־$U(M)$ את קבוצת האברים ההפיכים ב־M.*

תרגיל 1.4.18 (*) לכל מונויד M, $U(M)$ היא חבורה. (איננו קוראים ל־$U(M)$ "תת־חבורה" של M, משום ש־M אינה חבורה.) **הדרכה.** תרגיל 1.2.19

תרגיל 1.4.19 (*) אם G חבורה אז $U(G) = G$.

תרגיל 1.4.20 (**) 1. החיתוך של משפחה כלשהי של תת־חבורות הוא תת־חבורה (השווה לתרגיל 1.4.7).

2. האיחוד על־פני רשת עולה של תת־חבורות (ראה תרגיל 1.4.9) הוא חבורה.

3. האיחוד של שרשרת של חבורות הוא חבורה.

הגדרה 1.4.21 *תהי S קבוצה של אברים בחבורה G. מסמנים ב־$\langle S\rangle$ את חיתוך כל תת־החבורות של G המכילות את S.*

זוהי תת־חבורה לפי תרגיל 1.4.20. לפי ההגדרה, $\langle S\rangle$ היא תת־החבורה הקטנה ביותר של G המכילה את S. קוראים לה **תת־החבורה הנוצרת** על־ידי S. אם $G=\langle S\rangle$, אומרים ש־S **יוצרת** את G. את אותה חבורה אפשר ליצור על־ידי קבוצות רבות. אין משמעות לביטוי "הקבוצה היוצרת", או "האיבר היוצר", בהא הידיעה.

תרגיל 1.4.22 (**) לכל חבורה G ואיבר $x\in G$, האברים של תת־החבורה $\langle x\rangle$ הם החזקות של x.

הגדרה 1.4.23 *חבורה **נוצרת סופית** היא חבורה שיש לה קבוצת יוצרים סופית.*

תרגיל 1.4.24 (**) תהי G חבורה, ויהיו $x_1,\dots,x_n\in G$. תת־החבורה $\langle x_1,\dots,x_n\rangle$ שווה לקבוצת כל האברים מהצורה $x_{i_1}^{\epsilon_1}\cdots x_{i_m}^{\epsilon_m}$ כאשר $m\in\mathbb{N}$, $i_j\in\{1,\dots,n\}$, ו־$\epsilon_j\in\{\pm1\}$. (בהחלט יתכן שאפשר להציג את אותו איבר בדרכים שונות.)

תרגיל 1.4.25 (+*)** תן דוגמה לחבורה שאינה נוצרת סופית. **הדרכה.** אם אינך רואה דוגמא בשלב זה, העזר בתרגיל 1.5.15.

1.5 מכפלה ישרה חיצונית

כהכנה לפרק הבא, שבו נפגוש כמה דוגמאות סטנדרטיות לחבורות, נציג כאן בניה פשוטה היוצרת חבורה חדשה מחבורות נתונות.

הגדרה 1.5.1 *תהיינה G_1,G_2 חבורות. **המכפלה הישרה החיצונית** שלהן היא המכפלה הקרטזית $G_1\times G_2$ עם הפעולה לפי רכיבים, כלומר $(g_1,g_2)(g_1',g_2')=(g_1g_1',g_2g_2')$.*

תרגיל 1.5.2 (*) תהיינה G_1,G_2 חבורות. המכפלה $G_1\times G_2$ היא חבורה, עם איבר היחידה $(1_{G_1},1_{G_2})$, ונוסחת ההיפוך $(x,y)^{-1}=(x^{-1},y^{-1})$.

תרגיל 1.5.3 (*) ה"קומוטטיביות" וה"אסוציאטיביות" של מכפלה ישרה חיצונית: לכל שלוש חבורות G,H,K מתקיים:

1. $G\times H\cong H\times G$.

2. $(G\times H)\times K\cong G\times(H\times K)$.

תרגיל 1.5.4 (**) 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 דוגמה לחבורה $G\times H$ עם תת־חבורה שאינה מתקבלת בצורה זו.

תרגיל 1.5.5 (−*)** בהמשך לתרגיל 1.4.16, מצא דוגמה 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 $G = \mathbb{Z}_2 \times \mathbb{Z}_2$, כאשר $\mathbb{Z}_2 = \{0,1\}$ עם פעולת החיבור מודולו 2.

תרגיל 1.5.6 (**) $G \times \{1\}$ ו־$\{1\} \times H$ הן תת־חבורות של $G \times H$. המכפלה $G \times H$ נוצרת על־ידי האיחוד שלהן (אבל איננה שווה לו).

תרגיל 1.5.7 (**) הגדר את המכפלה הישרה של שתי חבורות למחצה, והראה שהיא חבורה למחצה. כך גם עבור מונוידים.

תרגיל 1.5.8 (−)** יהיו M_1, M_2 מונוידים. הראה ש־$U(M_1 \times M_2) = U(M_1) \times U(M_2)$ (ראה הגדרה 1.4.17).

הגדרנו לעיל מכפלה ישרה של שתי חבורות, ומכאן באינדוקציה מכפלה ישרה של מספר סופי כלשהו. אפשר להכליל את אותה הגדרה למכפלה של משפחה כללית:

הגדרה 1.5.9 *תהי Λ קבוצת אינדקסים כך שלכל $\lambda \in \Lambda$ מתאימה חבורה G_λ.* ***פונקציית בחירה*** *היא פונקציה $f : \Lambda \to \cup G_\lambda$ כך שלכל $\lambda \in \Lambda$, $f(\lambda) \in G_\lambda$.* ***המכפלה הישרה*** *$\prod_{\lambda \in \Lambda} G_\lambda$ מוגדרת כאוסף פונקציות הבחירה, עם הפעולה $(fg)(\lambda) = f(\lambda)g(\lambda)$.*

תרגיל 1.5.10 (**) המכפלה הישרה של חבורות היא חבורה.

תרגיל 1.5.11 (+)** **אקסיומת הבחירה** היא האקסיומה הקובעת שהמכפלה הישרה של משפחת קבוצות כלשהי אינה ריקה. הסבר מדוע אין צורך באקסיומת הבחירה כדי להוכיח שהמכפלה הישרה של משפחת חבורות כלשהי אינה ריקה.

תרגיל 1.5.12 (**) אם $\Lambda = \{1,2\}$, הגדרה 1.5.9 חוזרת על הגדרה 1.5.1.

הגדרה 1.5.13 *תהי Λ קבוצת אינדקסים כך שלכל $\lambda \in \Lambda$ מתאימה חבורה G_λ.* ***הסכום הישר*** *$\bigoplus_{\lambda \in \Lambda} G_\lambda$ מוגדר כאוסף פונקציות הבחירה f שעבורן $\{\lambda : f(\lambda) \neq 1_{G_\lambda}\}$ סופית, עם אותה פעולה כמו במכפלה הישרה.*

תרגיל 1.5.14 (**) $\bigoplus_{\lambda \in \Lambda} G_\lambda$ היא תת־חבורה של $\prod_{\lambda \in \Lambda} G_\lambda$, והחבורות מתלכדות אם Λ סופית.

תרגיל 1.5.15 (**) חשב את העוצמה של שתי החבורות $\bigoplus_{n \in \mathbb{Z}} \mathbb{Z}$ ו־$\prod_{n \in \mathbb{Z}} \mathbb{Z}$.

תרגיל 1.5.16 (+*)** הראה שלחבורה $\bigoplus_{n \in \mathbb{Z}} \mathbb{Z}_2$, שהיא בת־מניה, יש א תת־חבורות.

1.6 הומומורפיזמים

הגדרה 1.6.1 *תהיינה A, B חבורות למחצה. העתקה $\varphi : A \to B$ המקיימת את התנאי $\varphi(xy) = \varphi(x)\varphi(y)$ לכל $x, y \in A$ נקראת* ***הומומורפיזם של חבורות למחצה****. אם A, B מונוידים ובנוסף מתקיים $\varphi(1_A) = 1_B$ אז φ* ***הומומורפיזם של מונוידים****.*

תרגיל 1.6.2 (*) יהיו M, N, K מונוידים. אם $\varphi_1 : M \to N$, ו־$\varphi_2 : N \to K$ הומומורפיזמים של מונוידים, אז ההרכבה $\varphi_2 \circ \varphi_1 : M \to K$ היא הומומורפיזם (של מונוידים).

תרגיל 1.6.3 (**) מצא מונוידים M, N והומומורפיזם של חבורות למחצה $\varphi : M \to N$, שאינו הומומורפיזם של מונוידים (כלומר, φ שומר על כפל אבל לא על איבר היחידה). **הצעה.** קח $M = N = \mathbb{Z} \times \mathbb{Z}$ עם $\varphi(x,y) = (x,0)$.

תרגיל 1.6.4 (*) יהיו M, N מונוידים, ו־$\varphi\colon M \to N$ הומומורפיזם של חבורות למחצה. אם φ על, אז φ הומומורפיזם של מונוידים.

תרגיל 1.6.5 (**) אם A, B חבורות ו־$\varphi\colon A{\to}B$ הומומורפיזם של חבורות למחצה, אז $\varphi(1_A) = 1_B$ ו־$\varphi(a^{-1}) = \varphi(a)^{-1}$ לכל $a \in A$.

הגדרה 1.6.6 *תהיינה G, H חבורות. כל פונקציה שומרת כפל $\varphi\colon G{\to}H$ נקראת **הומומורפיזם של חבורות**, או סתם **הומומורפיזם**.*

לאור תרגיל 1.6.5, כל הומומורפיזם של חבורות שומר על איברי היחידה ועל פעולת ההפכי.

הגדרה 1.6.7 *יהי $\varphi\colon G \to H$ הומומורפיזם של חבורות. הקבוצה $\mathrm{Im}(\varphi) = \{\varphi(x)\colon\ x \in G\}$ **היא התמונה של** φ. הקבוצה $\mathrm{Ker}(\varphi) = \{x \in G\colon\ \varphi(x) = 1\}$ **היא הגרעין של** φ.*

(להומומורפיזם בין מונוידים מגדירים $\mathrm{Ker}(\varphi) = \{(x, y)\colon\ \varphi(x) = \varphi(y)\} \subseteq M \times M$, ולא $\{x\colon\ \varphi(x) = 1_M\}$. קבוצה זו של זוגות סדורים היא יחס שקילות על M, הנשמר תחת פעולת הכפל. יחס כזה נקרא **קונגרואנציה**, והוא התחליף של חבורות למחצה למושג החשוב של תת־חבורה נורמלית, שנלמד בהמשך. לא נזדקק להגדרה זו בהמשך הקורס.)

תרגיל 1.6.8 (*) הוכח: $\mathrm{Im}(\varphi)$ הוא תת־חבורה של H.

תרגיל 1.6.9 (**) הוכח: $K = \mathrm{Ker}(\varphi)$ הוא תת־חבורה של G.

תרגיל 1.6.10 (+)** $\varphi\colon G{\to}H$ חד־חד־ערכית אם ורק אם $\mathrm{Ker}(\varphi) = 1$.

תרגיל 1.6.11 (**) יהי $\varphi\colon G_1{\to}G_2$ הומומורפיזם של חבורות. הראה שלכל תת־חבורה $H \leq G_1$, $\varphi(H) = \{\varphi(x)\colon\ x \in H\}$ היא תת־חבורה של G_2. (היינו, התמונה של תת־חבורה היא תת־חבורה.)

תרגיל 1.6.12 (**) תהי G חבורה הנוצרת על־ידי קבוצה S. אם $\varphi, \varphi'\colon G{\to}H$ מסכימים על איברי S, אז הם שווים.

הגדרה 1.6.13 *הומומורפיזם שהוא חד־חד־ערכי נקרא **מונומורפיזם** או **שיכון**. הומומורפיזם שהוא על נקרא **אפימורפיזם**.*

כבר ראינו שהומומורפיזם חד־חד־ערכי ועל נקרא איזומורפיזם.

תרגיל 1.6.14 (***) עבור פונקציה $f\colon \mathbb{N}{\to}\mathbb{Q}$, נסמן

$$H(f) = \liminf_{n\to\infty} \frac{1}{n^2}|\{(i, j)\colon\ 1 \leq i, j \leq n,\ f(i) + f(j) = f(i + j)\}|.$$

(זו המידה שבה f שומרת חיבור). מצא פונקציה חד־חד־ערכית ועל f שעבורה $H(f) = 1$.

פרק 2

דוגמאות לחבורות

בפרק הזה נכיר את הדוגמאות הבסיסיות לחבורות. המחלקה הראשונה היא של חבורות אבליות, שהן החבורות המקיימות את החוק $ab = ba$. הדוגמא הפשוטה ביותר לחבורה אבלית (ולחבורה בכלל) היא חבורה ציקלית, שהיא חבורה שכל אבריה הם חזקות של איבר קבוע.

כדי להבין את החבורות הציקליות על בוריין, נלמד מבוא מזורז לתורת המספרים, המפתח בעזרת רעיון החליוק עם שארית של אוקלידס את מושג המחלק המשותף המקסימלי. מכאן נובע בקלות יחסית המשפט היסודי של האריתמטיקה, על פירוק יחיד לגורמים. הרעיונות מתורת המספרים מאפשרים להציג משפחה נוספת של חבורות אבליות: חבורות אוילר, המאפשרות (כפי שנראה בפרק הבא) להסיק ממשפטים בתורת המספרים את המשפטים הקלאסיים של פרמה ואוילר. נוכיח גם את התכונה העיקרית של חבורות ציקליות (משפט 2.3.12): כל תת־חבורה של חבורה ציקלית היא בעצמה ציקלית. את רשימת החבורות האבליות בפרק הזה משלימות החבורות המופיעות באופן טבעי בשדה, שהן חבורות אבליות אינסופיות.

בסעיפים האחרונים מוצגות החבורות הסימטריות, שהן אולי הדוגמא החשובה ביותר לחבורה לא אבלית סופית, ואחריהן חבורות של מטריצות, שהן דוגמא מרכזית לחבורות לא אבליות אינסופיות. הסעיף האחרון מציג משפחה נוספת של חבורות לא אבליות סופיות: החבורות הדיהדרליות.

2.1 חבורות אבליות

אברים $x, y \in G$ **מתחלפים** זה עם זה, אם מתקיים $xy = yx$.

תרגיל 2.1.1 (*) יהי $\varphi\colon G_1 \to G_2$ הומומורפיזם. הוכח: אם x, y מתחלפים ב־G_1, אז $\varphi(x), \varphi(y)$ מתחלפים ב־G_2.

תרגיל 2.1.2 (*) יהי $\varphi\colon G_1 \to G_2$ איזומורפיזם. הוכח: x, y מתחלפים ב־G_1, אם ורק אם $\varphi(x), \varphi(y)$ מתחלפים ב־G_2.

הגדרה 2.1.3 *חבורה שבה כל שני אברים מתחלפים זה עם זה נקראת **חבורה אבלית**.* (*החבורות נקראות כך על־שם המתמטיקאי הנורבגי* Niels Henrik Abel.)

תרגיל 2.1.4 (*) קבוצת המספרים השלמים $\mathbb{Z}$, ביחס לפעולת החיבור, היא חבורה אבלית.

תרגיל 2.1.5 (*) המכפלה $G_1 \times G_2$ אבלית אם ורק אם שני המרכיבים G_1, G_2 אבליים.

הגדרה 2.1.6 *תהי G חבורה. **המרְכָּז** של G הוא תת־החבורה $\mathrm{Z}(G) = \{x \in G\colon (\forall g) gx = xg\}$ הכוללת את האברים המתחלפים עם כל איבר של G.*

תרגיל 2.1.7 (*) $\mathrm{Z}(G)$ היא תת־חבורה אבלית של G, השווה לה אם ורק אם G עצמה אבלית.

הגדרה 2.1.8 *יהי F שדה; מסמנים $F^{\times} = F - \{0\}$ עם פעולת הכפל.*

תרגיל 2.1.9 (+*)** יהי F שדה. אז $(F, +, 0)$ חבורה, $(F, \cdot, 1)$ מונויד, ו־$(F^{\times}, \cdot, 1)$ חבורה. למעשה, קבוצה $(F, +, \cdot, 0, 1)$ היא שדה אם ורק אם $(F, +, 0)$ ו־$(F - \{0\}, \cdot, 1)$ חבורות אבליות, ומתקיימת אקסיומת הדיסטריבוטיביות $(a + b)c = ab + ac$.

אומרים שאיבר x הוא בעל **סדר** 2 אם $x^2 = 1$ אבל $x \neq 1$. הכללה של מושג זה תשרת אותנו רבות בהמשך; ראו הגדרה 2.3.16.

תרגיל 2.1.10 (**) בחבורה מתקיים $x^2 = 1$ לכל איבר. הוכח שהחבורה אבלית. (ראה הכללה בתרגיל 4.8.12.)

תרגיל 2.1.11 (+*)** בחבורה סופית A מתקיים $x^2 = 1$ לכל איבר. הראה ש־$|A|$ הוא חזקה של 2. **הדרכה.** A הוא מרחב וקטורי מעל $\mathbb{F}_2$.

תרגיל 2.1.12 (-*)** תהי $G = \{a_1, \ldots, a_n\}$ חבורה אבלית סופית. נסמן $b = a_1 a_2 \cdots a_n$. (איבר זה מוגדר היטב משום שסדר הגורמים אינו חשוב).

1. הוכח: $b^2 = 1$.
2. אם יש איבר יחיד מסדר 2, הוא שווה ל־b.
3. אם יש יותר מאיבר אחד מסדר 2, אז $b = 1$. **הדרכה.** נסמן ב־A את אוסף האיברים מסדר 2 עם איבר היחידה; העזר בתרגיל 2.1.11.

תרגיל 2.1.13 (**) נסמן ב־$m_2(G)$ את מספר הפתרונות למשוואה $x^2 = 1$ בחבורה G.

1. הראה שבכל חבורה סופית G, $m_2(G) \equiv |G| \pmod 2$. **הדרכה.** נגדיר על G יחס שקילות: $x \equiv y$ אם $x = y$ או $xy = 1$. האברים שריבועם אינו 1 שייכים למחלקות שקילות בגודל 2.
2. בכל חבורה עם מספר זוגי של איברים יש איבר מסדר 2.

תרגיל 2.1.14 (**) תהי G חבורה אבלית. הראה שאוסף האברים מסדר 2, עם איבר היחידה, הוא תת־חבורה. הסק מתרגילים 2.1.11 ו־2.1.13 שבחבורה אבלית שגודלה אי־זוגי אין אברים מסדר 2.

תרגיל 2.1.15 (**) תהי G חבורה. הראה שאם g הוא מכפלה של שני אברים מסדר 2, אז גם g^k כזה לכל k.

תרגיל 2.1.16 (***) 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. הוכח:

1. $\Phi_n \Leftrightarrow \Phi_{1-n}$.
2. החבורה אבלית אם ורק אם מתקיים Φ_2.
3. אם Φ_n אז לכל x, y מתקיים $x^n y^{n-1} = y^{n-1} x^n$.
4. אם Φ_n אז לכל x, $x^{n(n-1)} \in \mathrm{Z}(G)$.
5. אם $\Phi_n \wedge \Phi_{n+1}$ אז לכל x, $x^n \in \mathrm{Z}(G)$.
6. אם $\Phi_n \wedge \Phi_{n+1} \wedge \Phi_{n+2}$ אז החבורה אבלית.

7. אם $\Phi_n \wedge \Phi_{n+1} \wedge \Phi_{n+m} \wedge \Phi_{n+m+1}$ עבור n, m זרים כלשהם, אז החבורה אבלית.

(ראה גם תרגילים 3.3.23 ו־8.4.67.)

תרגיל 2.1.17 (***) בהמשך לתרגיל 2.1.16, נניח שבחבורה מתקיים $x^2y = yx^2$ לכל x, y. הוכח שלכל n זוגי, $\Phi_n \Leftrightarrow \Phi_{n+1}$ ו־$\Phi_n \Leftrightarrow \Phi_{n-4}$. הסק שכל התכונות Φ_{4k}, Φ_{4k+1} מתקיימות, וכל התכונות Φ_{4k-1}, Φ_{4k-2} שקולות לאבליות של החבורה. תן דוגמא לחבורה לא אבלית שבה $x^2y = yx^2$.

תרגיל 2.1.18 (**) תהי G חבורה כלשהי. אם A אבלית, אז האוסף $\mathrm{Hom}(G, A)$ של ההומומורפיזמים $G \to A$, ביחס לכפל לפי רכיבים $(\phi \cdot \phi')(g) = \phi(g)\phi'(g)$, הוא חבורה אבלית.

2.2 מבוא לתורת המספרים

בסעיף זה נאסוף כמה תכונות חיוניות של המספרים השלמים. לשם כך עלינו להכיר את קבוצת המספרים השלמים $\mathbb{Z}$, עם פעולות החיבור והכפל ויחס הסדר, עם האקסיומות הסטנדרטיות שאלה מקיימים, ועם התכונה הידועה כ**אקסיומת האינדוקציה**: אם $P \subseteq \mathbb{Z}$ היא קבוצה של מספרים טבעיים כך ש־$0 \in P$ ולכל $n > 0$ אם $n \in P$ אז $n + 1 \in P$, אז כל מספר חיובי שייך ל־P.

תרגיל 2.2.1 (**) הוכח את **אקסיומת האינדוקציה השלמה**: אם $P \subseteq \mathbb{Z}$ היא קבוצה של מספרים טבעיים המקיימת את שתי התכונות (1) $0 \in P$; (2) לכל $n > 0$, אם לכל $0 \leq m < n$ מתקיים $m \in P$, אז $n \in P$; אז כל מספר חיובי שייך ל־P.

2.2.1 יחס החילוק

הגדרה 2.2.2 *נגדיר יחס על קבוצת המספרים השלמים:* $a \,|\, b$ *("a מחלק את b") אם קיים* $c \in$ *כך ש־*$b = ac$.

ביחס לפעולת הכפל, $\mathbb{Z}$ מהווה מונויד (אבל לא חבורה). האברים ההפיכים של המונויד הזה הם $U(\mathbb{Z}) = \{\pm 1\}$.

תרגיל 2.2.3 (*) $a \,|\, b$ אם ורק אם $a \,|\, (-b)$ אם ורק אם $(-a) \,|\, b$ אם ורק אם $(-a) \,|\, (-b)$.

תרגיל 2.2.4 (*) לכל n, $1 \,|\, n$ ו־$n \,|\, 0$. מאידך, המחלקים היחידים של 1 הם ± 1, והמספר היחיד המתחלק ב־0 הוא 0 עצמו.

תרגיל 2.2.5 (**) היחס 'מחלק' הוא רפלקסיבי וטרנזיטיבי, אבל לא אנטי־סימטרי.

2.2.2 המחלק המשותף המקסימלי

משפט 2.2.6 (האוקלידיות של $\mathbb{Z}$) *לכל* $n \in \mathbb{Z}$ *ולכל* $d \neq 0$ *קיימים* q, r *כך ש־*$n = qd + r$ *ו־*$0 \leq r < |d|$.

הדרכה. אינדוקציה עבור $n \geq 0$; *ואם* $n = qd + r$ *אז* $-n = (-q-1)d + (d-r)$.

הגדרה 2.2.7 ***המחלק המשותף המקסימלי*** *של* $n, m \in \mathbb{Z}$, *כפי שמתבקש משמו, הוא המספר* $(n, m) = \max_{d \in \mathbb{Z}} \{d :\, d \,|\, n, d \,|\, m\}$.

תרגיל 2.2.8 (*) המחלק המשותף המקסימלי $(\pm n, \pm m)$ אינו תלוי בסימנים.

תרגיל 2.2.9 (*) $(n, m) = (m, n)$.

תרגיל 2.2.10 (*) אם $n = qm + r$ אז $(n, m) = (m, r)$.

אלגוריתם 2.2.11 (אלגוריתם אוקלידס לחישוב מחלק משותף מקסימלי) יהיו $n, m \in \mathbb{Z}$. אפשר להניח ש־$0 \leq m < n$. אם $m = 0$ אז $(n,m) = n$. אחרת אפשר לכתוב $n = qm + r$ כאשר $0 \leq r < m$, ואז $(n,m) = (m,r)$, שכבר חושב באינדוקציה.

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

תרגיל 2.2.12 (*) מצא את $(5614, 1260)$ ואת $(7821, 6429)$.

משפט יסודי ושימושי בתורת המספרים האלמנטרית.

משפט 2.2.13 *לכל $n, m \in \mathbb{Z}$, קיימים $\alpha, \beta \in \mathbb{Z}$ כך ש־$(n,m) = \alpha n + \beta m$.*

תרגיל 2.2.14 (***) הוכח את המשפט. **הדרכה.** נסמן $d = \min\{\alpha n + \beta m > 0\}$, $c = (a,b)$. מכיוון ש־$c \,|\, a, b$, ברור ש־$c \,|\, d$. כתוב $a = qd + r$, והראה ש־$r = 0$; לכן $d \,|\, a$ ובדומה $d \,|\, b$, כך ש־$d \leq c$.

תרגיל 2.2.15 (***) נסח את **אלגוריתם אוקלידס המוכלל** לחישוב מחלק משותף מקסימלי עם מקדמים. **הדרכה.** נסמן $d = (n,m)$. אם $n = qm + r$ ו־$\alpha m + \beta r = d$ (את המקדמים האלו אפשר לחשב לפי הנחת האינדוקציה) אז $\beta n + (\alpha - \beta q)m = d$.

דוגמא 2.2.16 $(234, 61) = (61, 51) = (51, 10) = (10, 1) = (1, 0) = 1$. לצורך חישוב המקדמים, נבחין ש־$(1) \cdot 1 + (0)0 = 1$; לכן $(0) \cdot 10 + (1) \cdot 1 = 1$; לכן $(1) \cdot 51 - (5) \cdot 10 = 1$; לכן $(-5) \cdot 61 + (6)51 = 1$; ולבסוף $(6)234 + (-23) \cdot 61 = 1$.

תרגיל 2.2.17 (**) מצא $\alpha, \beta \in \mathbb{Z}$ כך ש־$1525\alpha + 927\beta = 1$.

הגדרה 2.2.18 *אומרים ש־n, m **זרים** אם $(n,m) = 1$.*

תרגיל 2.2.19 (**) יהיו $n, m \in \mathbb{Z}$, ונסמן $d = (n,m)$. אז $(\frac{n}{d}, \frac{m}{d}) = 1$.

תרגיל 2.2.20 (**) אם $(m,k) = 1$, אז $(n, mk) = (n,m) \cdot (n,k)$.

תרגיל 2.2.21 (**) הוכח: $(n, mm') \,|\, (n,m) \cdot (n,m')$ **הדרכה.** כתוב $an + bm = (n,m), a'n + b'm' = (n,m')$.

תרגיל 2.2.22 (**) אם $(n,m) = 1$, אז $(n, mk) = (n,k)$.

תרגיל 2.2.23 (**) אם $d \,|\, d'$ אז לכל m, $\frac{d}{(d,m)} \,|\, \frac{d'}{(d',m)}$.

הגדרה 2.2.24 *הכפולה המשותפת המינימלית של n ו־m היא* $[n,m] = \min_{s \in \mathbb{N}} \{s :\, n \,|\, s, m \,|\, s\}$.

תרגיל 2.2.25 (***) הוכח: $(n,m)[n,m] = nm$.

תרגיל 2.2.26 (**) $\mathbb{Z}$ עם יחס החלוקה הוא סריג (ראה הגדרה 4.4.1), שבו החסם העליון והתחתון הם $n \wedge m = (n,m)$, $n \vee m = [n,m]$.

תרגיל 2.2.27 (**) $(\mathbb{N}, |)$ **סריג דיסטריבוטיבי**, כלומר - $n \wedge (m \vee k) = (n \wedge m) \vee (n \wedge k)$.

תרגיל 2.2.28 (-*)** הוכח שלכל $a > 1$ ולכל n, m, $(a^n - 1, \frac{a^{nm}-1}{a^n-1})$ מחלק את m. הסק שהמספרים $a^n - 1$ ו־$\frac{a^{n \cdot a}-1}{a^n-1}$ זרים.

תרגיל 2.2.29 (-*)** יהיו n, m מספרים שלמים.

1. הוכח שקיימים $a \,|\, a'$ ו־$b \,|\, b'$ כך ש־$n = ab'$, $m = a'b$ ו־$(a', b') = 1$.
2. הראה שאם $n \neq m$ אז a, b, a', b' כנ"ל הם יחידים. **הדרכה.** חשב את $(\frac{n}{(n,m)}^n, m)$.

2.2.3 שקילות מודולו n

הגדרה 2.2.30 *יהי $n \in \mathbb{Z}$ קבוע. נגדיר יחס על המספרים השלמים: a* ***שקול ל־b מודולו n*** *(כותבים $a \equiv b \pmod n$) אם $n \,|\, (a-b)$.*

תרגיל 2.2.31 (*) היחס "שקילות מודולו n" הוא יחס שקילות.

תרגיל 2.2.32 (+)** נניח $a \equiv a' \pmod n$ ו־$b \equiv b' \pmod n$. אז $a+b \equiv a'+b' \pmod n$ ו־$ab \equiv a'b' \pmod n$. במלים אחרות, פעולות החיבור והכפל של מחלקות שקילות מוגדרות היטב.

תרגיל 2.2.33 (**) הוכח ש־$10^{10^{10}}+1$ אינו ראשוני. **הדרכה.** מצא מספר $n < 10^{10^{10}}$ כך ש־$10^{10^{10}} \equiv -1 \pmod n$.

2.2.4 פירוק לראשוניים

הגדרה 2.2.34 *מספר לא הפיך p הוא* ***ראשוני*** *אם בכל פירוק שלו $p = xy$, אחד הגורמים הפיך.*

תרגיל 2.2.35 (**) כל מספר טבעי הוא מכפלה של ראשוניים. **הדרכה.** תרגיל 2.2.1.

תרגיל 2.2.36 (*) מצא את הפירוק לראשוניים של המספרים הבאים: 5720, 12960, 8888, 4096.

תרגיל 2.2.37 (*) אם p ראשוני, אז לכל n, $p \,|\, n$ או $(p,n)=1$.

טענה 2.2.38 אם a זר ל־b ו־$a \,|\, bc$, אז $a \,|\, c$.

תרגיל 2.2.39 (**) הוכח את הטענה. **הדרכה.** כתוב $\alpha a + \beta b = 1$.

תרגיל 2.2.40 (*) הראה שטענה 2.2.38 אינה תקפה אם מוותרים על הדרישה ש־a,b יהיו זרים.

תרגיל 2.2.41 (**) אם p ראשוני ו־$p \,|\, ab$ אז $p \,|\, a$ או $p \,|\, b$. **הדרכה.** אם $p \nmid a$ אז $(p,a)=1$ לפי תרגיל 2.2.37, ואז $p \,|\, b$ לפי טענה 2.2.38.

משפט 2.2.42 *הפירוק של מספר טבעי לגורמים ראשוניים הוא יחיד עד־כדי סדר.*

הוכחה. נניח ש־$p_1 \cdots p_t = p'_1 \cdots p'_{t'}$, כאשר p_i ו־p'_i כולם ראשוניים. לפי תרגיל 2.2.41 $p_t \,|\, p'_i$ לאיזשהו i; לפי ההגדרה $p'_i = \pm p_t$, ואז אפשר לצמצם ולהמשיך באינדוקציה על t. □

אינסוף ראשוניים

משפט 2.2.43 (משפט אוקלידס) *יש אינסוף מספרים ראשוניים.*

תרגיל 2.2.44 (−*)** הוכח את המשפט. **הדרכה.** נניח שהראשוניים הם $p_1, p_2, \dots, p_n$ בלבד. התבונן ב־$P = p_1 \dots p_n + 1$.

תרגיל 2.2.45 (**) הוכח שיש אינסוף ראשוניים מהצורה $4n-1$. **הדרכה.** אחרת תהי $Q = p_1 \dots p_n$ מכפלת כל הראשוניים מצורה זו; התבונן ב־$4Q-1$.

תרגיל 2.2.46 (***) הוכח שיש אינסוף ראשוניים מהצורה $4n+1$. **הדרכה.** אחרת תהי $Q = p_1 \dots p_n$ מכפלת כל הראשוניים מצורה זו; התבונן ב־$4Q^2+1$ והעזר בתרגיל 3.2.7.

תרגיל 2.2.47 (**) הוכח שיש אינסוף ראשוניים מהצורה $6n-1$. **הדרכה.** אחרת תהי $Q = p_1 \dots p_n$ מכפלת כל הראשוניים מצורה זו; התבונן ב־$6Q-1$.

2.2.5 משפט ההיפוך של מביוס

ניתן לדלג בקריאה ראשונה.

הגדרה 2.2.48 *הקונוולוציה של פונקציות* $f,g\colon\mathbb{N}\to\mathbb{R}$ *מוגדרת כפונקציה* $f*g\colon\mathbb{N}\to\mathbb{R}$*, שערכיה הם* $(f*g)(n)=\sum_{n_1n_2=n}f(n_1)g(n_2)$. (*למשל,* $(f*g)(4)=f(1)g(4)+f(2)g(2)+f(4)g(1)$.)

הגדרה 2.2.49 *הפונקציות* $\delta_1, J\colon\mathbb{N}\to\mathbb{R}$ *מוגדרות לפי* $\delta_1(n)=\left\{\begin{array}{ll}1 & n=1\\ 0 & n>1\end{array}\right.$, $J(n)=1$.

תרגיל 2.2.50 (**) $(\mathbb{R}^{\mathbb{N}},*,\delta_1)$ מונויד קומוטטיבי.

הגדרה 2.2.51 פונקצית מביוס $\mu\colon\mathbb{N}\to\mathbb{R}$ מוגדרת לפי
$$\mu(n)=\left\{\begin{array}{ll}(-1)^s & n=p_1\cdots p_s\\ 0 & \exists p: p^2\,|\,n\\ 1 & n=1\end{array}\right.$$

תרגיל 2.2.52 (*) חשב את $\mu(1),\mu(2),\dots,\mu(24)$.

תרגיל 2.2.53 (**) $\mu(nm)=\mu(n)\mu(m)$ לכל $(n,m)=1$.

תרגיל 2.2.54 (**) $J*\mu=\delta_1$ (כלומר לכל $n>1$, $\sum_{d\,|\,n}\mu(d)=0$.)

משפט 2.2.55 (משפט ההיפוך של מביוס) נניח שפונקציה F מוגדרת לפי $F(n)=\sum_{d\,|\,n}f(d)$. אז מתקיים $f(n)=\sum_{d\,|\,n}\mu(\frac{n}{d})F(d)$.

הוכחה. נתון ש־$F=J*f$, ולכן $\mu*F=\mu*(J*f)=(\mu*J)*f=\delta_1*f=f$. □

תרגיל 2.2.56 (*) בדוק את הנוסחה ל־$f(n)$ ישירות עבור $n=1,p,p^2,6,12$.

תרגיל 2.2.57 (**) נסמן ב־$d(n)$ את מספר המחלקים של n (למשל $d(9)=|\{1,3,9\}|=3$). הוכח: $d=J*J$. הסק: $\sum_{d|n}\mu(\frac{n}{d})d(d)=(d*\mu)(n)=J(n)=1$ לכל n. בדוק את הנוסחה עבור $n=18$.

היזכר בפונקציות מהגדרה 2.2.49. נוסיף להן: הפונקציה $\mathrm{Id}\colon\mathbb{N}\to\mathbb{R}$ מוגדרת לפי $\mathrm{Id}(n)=n$.

תרגיל 2.2.58 (**) משפחה של קבוצות $\{F_m\}$ היא בעלת התכונות הבאות:

1. $|F_m|=q^m$ (עבור קבוע q).
2. $F_m\cap F_{m'}=F_{(m,m')}$.

כתוב את מספר האברים ב־$F_n-\bigcup_{i<n}F_i$.

2.3 חבורות ציקליות

הגדרה 2.3.1 *חבורה הנוצרת על־ידי איבר בודד נקראת* ***חבורה ציקלית****. במלים אחרות, חבורה ציקלית היא חבורה שיש בה איבר* $x\in G$ *כך שכל האברים של* G *הם חזקות (חיוביות או שליליות) של* x.

תרגיל 2.3.2 (*) כל חבורה ציקלית היא אבלית (תרגיל 1.1.3).

תרגיל 2.3.3 (+)** החבורה $\mathbb{Z}$ היא ציקלית אינסופית. כל איבר שלה, פרט לאיבר היחידה, יוצר תת־חבורה איזומורפית.

הגדרה 2.3.4 *יהי $n \geq 1$. נגדיר $\mathbb{Z}_n = \{[0], \ldots, [n-1]\}$, אוסף מחלקות השקילות מודולו n, עם פעולת החיבור (של מחלקות), $[a]+[b]=[a+b]$.*

כשמגדירים העתקה מקבוצה לקבוצה (ופעולה בינרית בכלל זה), עולה לפעמים צורך להוכיח שהפעולה מוגדרת היטב. ישנם שני מצבים שכיחים. בראשון, כדי להגדיר פונקציה $f: A \to B$, מגדירים את $f(\alpha)$ באופן מסויים, וצריך לוודא שאכן $f(\alpha) \in B$. 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 "תהיינה α, β מחלקות; נבחר נציגים $x \in \alpha$ ו־$y \in \beta$; נגדיר $\alpha+\beta=[x+y]$". אכן, בתרגיל 2.2.32 בדקנו שבחירת כל שני נציגים x', y' מאותן מחלקות תביא לאותה תוצאה, ולכן פעולת החיבור בין מחלקות (על־ידי חיבור נציגים) מוגדרת היטב.

להבא נשמיט את סימון הסוגריים מן המחלקות. כשנכתוב למשל $3 \in \mathbb{Z}_7$, נתכוון למחלקה של כל המספרים המשאירים שארית 3 בחלוקה ל־7. בחבורה זו, $10=3=-4$.

תרגיל 2.3.5 (**) הראה ש־$\mathbb{Z}_n$ (הגדרה 2.3.4) היא חבורה, שאיבר היחידה שלה הוא (המחלקה של) 0, וההפכי ניתן בה על־ידי הנוסחה $-[a]=[-a]$. בדוק שהחבורה אבלית.

תרגיל 2.3.6 (**) $\mathbb{Z}_n$ נוצרת על־ידי המחלקה 1, ולכן היא חבורה ציקלית.

הגדרה 2.3.7 *מספר האברים בחבורה G נקרא **הסדר** של החבורה; מסמנים אותו ב־$|G|$.*

הסדר של חבורה הוא הנתון הראשון בתעודת הזהות שלה.

משפט 2.3.8 *כל חבורה ציקלית איזומורפית לאחת החבורות $\mathbb{Z}_n$, או ל־$\mathbb{Z}$. בפרט, כל שתי חבורות ציקליות מאותו סדר הן איזומורפיות זו לזו.*

תרגיל 2.3.9 (**) השתמש בכלל הצמצום בחבורה (הגדרה 1.3.5) כדי להוכיח שכל חבורה מסדר 2, 3 או 5 היא ציקלית. **הדרכה**. בחבורה מסדר 5, אם $a \neq 1$, הראה שלא יתכן ש־$a^2=1$, $a^3=1$ או $a^4=1$. לכן האברים $\{1, a, a^{-1}, a^2, a^{-2}\}$ כולם שונים, ו־$a^5=1$.

תרגיל 2.3.10 (**) 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 2.3.11 (**) יהי $x \in G$. לכל $a, b \in \mathbb{Z}$, $\langle x^a, x^b \rangle = \langle x^{(a,b)} \rangle$. **הדרכה**. משפט 2.2.13.

משפט 2.3.12 *כל תת־חבורה של חבורה ציקלית היא ציקלית.*

תרגיל 2.3.13 (**) הוכח את המשפט. **הדרכה**. בחר $x^a \in H$ עם $a > 0$ מינימלי. לכל $x^b \in H$, הסק מתרגיל 2.3.11 ש־$x^b \in \langle x^a \rangle$.

תרגיל 2.3.14 (**) מונויד M הוא **ציקלי** אם קיים $a \in M$ כך ש־$M = \{1, a, a^2, \ldots\}$. מצא דוגמה למונויד ציקלי בגודל 4 שאינו חבורה. כמה אפשרויות יש, עד כדי איזומורפיזם? לעומת זאת הראה שמונויד שבו כל איבר הוא מהצורה a^n עבור $n > 0$ הוא חבורה.

תרגיל 2.3.15 (***) נניח ש־$m \,|\, n$. מצא מונומורפיזם $\varphi: \mathbb{Z}_m \to \mathbb{Z}_n$ ואפימורפיזם $\psi: \mathbb{Z}_n \to \mathbb{Z}_m$ (כמה אפשרויות יש בכל מקרה?). חשב את $\varphi \circ \psi$ ואת $\psi \circ \varphi$. הראה שהתמונה $\operatorname{Im}(\varphi)$ והגרעין $\operatorname{Ker}(\psi)$ אינם תלויים בבחירת ההעתקות.

2.3.1 סדר של אברים

הגדרה 2.3.16 *יהי $x \in G$. המספר $m > 0$ הקטן ביותר כך ש־$x^m = 1$, אם קיים כזה, נקרא הסדר של x; אחרת אומרים ש־x בעל סדר אינסופי. את הסדר של x מסמנים ב־$\operatorname{ord}(x)$.*

תרגיל 2.3.17 (**) הסדר של $x \in G$ שווה לסדר של תת־החבורה (הציקלית) הנוצרת $\langle x \rangle$.

תרגיל 2.3.18 (*+) בחבורה סופית לכל איבר יש סדר סופי.

טענה 2.3.19 יהי $x \in G$. לכל $m \in \mathbb{Z}$, $x^m = 1$ אם ורק אם $\operatorname{ord}(x) \mid m$.

הוכחה. נסמן $e = \operatorname{ord}(x)$. אם $e \mid m$ אז ברור ש־$x^m = (x^e)^{m/e} = 1^{m/e} = 1$. נניח ש־$x^m = 1$, ונכתוב $(e,m) = \alpha e + \beta m$ עבור $\alpha, \beta \in \mathbb{Z}$. אז $x^{(e,m)} = x^{\alpha e + \beta m} = (x^e)^\alpha (x^m)^\beta = 1$, ולפי המינימליות של הסדר, $e = (e,m) \mid m$. □

תרגיל 2.3.20 (**) יהי $\varphi : G_1 \to G_2$ הומומורפיזם.

1. הראה ש־$\operatorname{ord}(\varphi(x)) \mid \operatorname{ord}(x)$ לכל $x \in G_1$.
2. אם φ מונומורפיזם אז $\operatorname{ord}(\varphi(x)) = \operatorname{ord}(x)$.

תרגיל 2.3.21 (*) הסדר של כל איבר ב־$\mathbb{Z}_n$ מחלק את n.

טענה 2.3.22 יהי x איבר מסדר n. אז הסדר של x^d הוא $\frac{n}{(n,d)}$.

הוכחה. $(x^d)^{\frac{n}{(n,d)}} = (x^n)^{\frac{d}{(n,d)}} = 1$, ולפי טענה 2.3.19 נובע מכך ש־$e = \operatorname{ord}(x^d) \mid \frac{n}{(n,d)}$. מאידך $(x^d)^e = x^{de} = 1$, אז מאותה סיבה $n \mid de$ ולכן $\frac{n}{(n,d)} \mid \frac{d}{(n,d)} e$. אלא שלפי תרגיל 2.2.19 $(\frac{n}{(n,d)}, \frac{d}{(n,d)}) = 1$, ולפי טענה 2.2.38 נובע מכך ש־$\frac{n}{(n,d)} \mid e$. □

תרגיל 2.3.23 (**) האיבר x^a יוצר את החבורה הציקלית $\langle x \rangle$ מסדר n אם ורק אם $(a,n) = 1$.

תרגיל 2.3.24 (**) נניח שלחבורה $G \neq 1$ אין תת־חבורות פרט ל־$G, 1$. הוכח ש־G ציקלית מסדר ראשוני.

משפט 2.3.25 *תהי $G = \langle x \rangle$ חבורה ציקלית מסדר n. יהי $d \mid n$. ל־G יש תת־חבורה יחידה מסדר n/d, והיא $\langle x^d \rangle$.*

הוכחה. לפי תרגיל 2.3.11 כל תת־חבורה של G היא ציקלית, ויתרה מזו אם היא נוצרת על־ידי x^k אז היא שווה ל־$\langle x^{(k,n)} \rangle$, והרי $\langle x^k \rangle = \langle x^k, x^n \rangle = \langle x^{(k,n)} \rangle$, $(k,n) \mid n$. לכן החבורה נוצרת על־ידי איבר מהצורה x^d עם $d \mid n$, ובחבורה זו יש n/d אברים לפי ספירה. □

זהו המשפט המרכזי על חבורות ציקליות.

תרגיל 2.3.26 (*) לחבורה ציקלית מסדר n יש תת־חבורה אחת מכל סדר המחלק את n.

הדרכה. משפט 2.3.25.

תרגיל 2.3.27 (**) אם $x, y \in G$ מתחלפים ו־$(\operatorname{ord}(x), \operatorname{ord}(y)) = 1$, אז $o(xy) = \operatorname{ord}(x)\operatorname{ord}(y)$.

הדרכה. הראה שתמיד $\operatorname{ord}(xy) \mid \operatorname{ord}(x)\operatorname{ord}(y)$, והראה ש־$x, y \in \langle xy \rangle$ כדי להוכיח $\operatorname{ord}(x), \operatorname{ord}(y) \mid \operatorname{ord}(xy)$.

תרגיל 2.3.28 (**) הסדר של (g,h) בחבורה $G \times H$ הוא הכפולה המשותפת המינימלית $[\operatorname{ord}(g), \operatorname{ord}(h)]$.

משפט 2.3.29 $\mathbb{Z}_{nm} \cong \mathbb{Z}_m \times \mathbb{Z}_n$ *אם ורק אם* $(n,m)=1$.

(זוהי גרסה של **משפט השאריות הסיני**.)

הוכחה. לפי תרגילים 2.3.21 ו־2.3.28, הסדר של כל איבר ב־$\mathbb{Z}_n \times \mathbb{Z}_m$ מחלק את $[n,m]$; אם $\mathbb{Z}_{nm} \cong \mathbb{Z}_m \times \mathbb{Z}_n$ אז יש באגף שמאל איבר מסדר nm ולכן $nm \,|\, [n,m] = \frac{nm}{(n,m)}$. בכיוון ההפוך, $\varphi\colon [x]_{nm} \mapsto ([x]_n,[x]_m)$ הוא הומומורפיזם, ואם $\varphi([x]_{nm})=0$ אז $n,m \,|\, x$ ולכן $nm=[n,m] \,|\, x$ כי $(n,m)=1$, ו־$[x]_{nm}=0$. $\square$

תרגיל 2.3.30 (**) אם $(n,m)=1$, אז לכל a,b קיים x כך ש־$x \equiv a \pmod n$ ו־$x \equiv b \pmod m$. פתרון זה הוא יחיד מודולו nm. **הדרכה.** משפט 2.3.29.

תרגיל 2.3.31 (*+)** [שאלה 1 מאולימפיאדת גיליס של שנת 2013] מצא את שתי הספרות האחרונות של המכפלה

$$(101^2-100^2)(102^2-101^2)\cdots(200^2-199^2).$$

2.4 חבורות אוילר

ראינו בסעיף הקודם שהקבוצה $\mathbb{Z}_n$ של מחלקות שקילות מודולו n היא חבורה ציקלית ביחס לחיבור. לפי תרגיל 2.2.32, גם פעולת הכפל מוגדרת היטב, ואכן:

תרגיל 2.4.1 (**) הראה ש־$\mathbb{Z}_n$ הוא מונויד ביחס לכפל, שאיבר היחידה שלו הוא (המחלקה של) 1. הראה שהוא קומוטטיבי.

תרגיל 2.4.2 (**) מצא תת־חבורה למחצה של $\mathbb{Z}_{12}$ ביחס לכפל, שאינה תת־מונויד.

תרגיל 2.4.3 (**) $[a] \in \mathbb{Z}_n$ הפיך (ביחס לכפל) אם ורק אם a זר ל־n.

תרגיל 2.4.4 (**) אם m,k זרים ל־n, אז גם mk זר ל־n.

הגדרה 2.4.5 *חבורת האברים ההפיכים ביחס לכפל ב־$\mathbb{Z}_n$ נקראת **חבורת אוילר** ה־n־ית. לפי תרגיל 2.4.3, אבריה הם* $U_n = \{[x] : 1 \leq x \leq n, (n,x)=1\}$.

תרגיל 2.4.6 (*) כתוב את לוח הכפל של החבורות U_n, עבור $n=2,3,4,5,6,7,8,9$, $10,12$.

תרגיל 2.4.7 (**) הוכח ש־U_9, U_{11} ציקליות, וש־U_{12}, U_{16} אינן ציקליות.

תרגיל 2.4.8 (***) הוכח שלחבורה U_{60} אין קבוצת יוצרים של שני אברים, ומצא קבוצת יוצרים עם שלושה אברים.

תרגיל 2.4.9 (***) בכל תת־חבורה לא טריוויאלית של U_{p^n} (p ראשוני), סכום האיברים מתחלק ב־p^n.

תרגיל 2.4.10 (*-)** נניח ש־p ראשוני. האיבר היחיד מסדר 2 ב־U_p הוא -1.

2.4.1 פונקציית אוילר

הגדרה 2.4.11 *את מספר האברים של U_n נסמן ב־$\phi(n)$. הפונקציה ϕ, המוגדרת לפי*

$$\phi(n) = |\{1 \leq a \leq n \colon\ (a,n) = 1\}|,$$

*נקראת **פונקצית אוילר** (על־שם המתמטיקאי לאונרד אוילר).*

תרגיל 2.4.12 (+*) אם p ראשוני, אז $\phi(p^a) = p^{a-1}(p-1)$.

תרגיל 2.4.13 (***) אם n, m זרים אז $\phi(nm) = \phi(n)\phi(m)$. **הדרכה.** משפט 2.3.29 ותרגיל 1.5.8. פתרון נוסף: משפט השאריות הסיני. המספרים הזרים ל־nm הם אלו שזרים ל־n ול־m, תרגיל 2.2.21.

משני התרגילים האחרונים מתקבלת הנוסחה

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

תרגיל 2.4.14 (*) חשב את $\phi(1000), \phi(480), \phi(540)$.

תרגיל 2.4.15 (**) אם $m \,|\, n$ אז $\phi(n) \,|\, \phi(m)$.

תרגיל 2.4.16 (+)** נניח $n \,|\, m$, ויהיו $a \in U_{nm}$, ו־a הנציג של a ב־U_n. נסמן ב־e את הסדר של a ב־U_n, וב־e' את הסדר של a ב־U_{nm}. הוכח ש־$e' \,|\, me$.

תרגיל 2.4.17 (***) מצא את כל הערכים של n המקיימים $\phi(n) \leq 6$ בשתי דרכים: (1) לפי הנוסחה ל־$\phi(n)$. (2) הראה בעזרת תרגיל 2.4.15 שאם $p \,|\, n$ אז $p-1 \leq 6$. הסק שהמספרים $11,13,17,19,23,29,31 \in U_n$ ולכן $n \leq 20$.

תרגיל 2.4.18 (***) הוכח ש־$\liminf_{n\to\infty} \frac{\phi(n)}{n} = 0$. **הדרכה.** נניח ש־$\phi(n) \leq m$, אז כל הגורמים הראשוניים של n קטנים מ־ .... מכיוון שיש אינסוף ראשוניים, ...

תרגיל 2.4.19 (**) לכל $d \,|\, n$, יש בדיוק $\phi(d)$ אברים מסדר d ב־$\mathbb{Z}_n$. בפרט, יש בה $\phi(n)$ יוצרים. **הדרכה.** טענה 2.3.22.

תרגיל 2.4.20 (-*)** לכל n, $\sum_{d\,|\,n} \phi(d) = n$. **הדרכה.** תרגיל 2.4.19.

תרגיל 2.4.21 (+)** בחבורה ציקלית מסדר המתחלק ב־d יש בדיוק d פתרונות למשוואה $x^d = 1$. **הדרכה.** שלב את תרגיל 2.4.19 וטענה 2.3.19 עם תרגיל 2.4.20 (קח d במקום n).

תרגיל 2.4.22 (***) במונחי תת־סעיף 2.2.5, הראה ש־$\phi * J = \mathrm{Id}$, ולכן $\phi = \mathrm{Id} * \mu$, כלומר, $\phi(n) = \sum_{d|n} \mu(\frac{n}{d})d$. בדוק את הנוסחה עבור $d = 12, 16, 24$.

תרגיל 2.4.23 (+)** תן הוכחה נוספת למשפט 2.3.25. **פתרון.** תהי H תת־חבורה מסדר d. מכיוון שהיא ציקלית, יש בה לפי תרגיל 2.4.19 $\phi(d)$ אברים מסדר d, וזה מספרם בחבורה כולה.

תרגיל 2.4.24 (**) כמה אברים בחבורה $\mathbb{Z}_{1200}$ יוצרים אותה (כל אחד לבדו)? **הדרכה.** תרגיל 2.3.23.

2.5 החבורה החיבורית והכפלית של שדה

הגדרה 2.5.1 *יהי F שדה. החבורה $(F,+,0)$ נקראת* ***החבורה החיבורית*** *של F, והחבורה $F^\times = F - \{0\}$ (מהגדרה 2.1.8), עם פעולת הכפל, היא* ***החבורה הכפלית*** *של F.*

נסמן ב־$\mathbb{R}$ את שדה המספרים הממשיים, וב־$\mathbb{C}$ את שדה המספרים המרוכבים, המכיל אותו. נסמן $\mathbb{R}_{>0} = \{x \in \mathbb{R} \colon x > 0\}$. נסמן $S^1 = \{z \in \mathbb{C} \colon |z| = 1\}$. השדות המוכרים לנו מציעים מיד כמה חבורות אינסופיות מעניינות: $(\mathbb{Q},+)$, $(\mathbb{R},+)$, $(\mathbb{C},+)$, $\mathbb{Q}^\times$, $\mathbb{R}^\times$, $\mathbb{C}^\times$.

תרגיל 2.5.2 (**) הראה שאף אחת מהחבורות $(\mathbb{Q},+)$, $(\mathbb{R},+)$, $(\mathbb{C},+)$, $\mathbb{Q}^\times$, $\mathbb{R}^\times$, $\mathbb{C}^\times$ אינה ציקלית.

תרגיל 2.5.3 (**) הראה שהחבורות $(\mathbb{Q},+)$ ו־$\mathbb{Q}^\times$ אינן איזומורפיות.

תרגיל 2.5.4 (**) הראה שהחבורות $(\mathbb{Q},+)$ ו־$(\mathbb{R},+)$ אינן איזומורפיות.

תרגיל 2.5.5 (**) פונקציית האקספוננט היא איזומורפיזם $\exp : (\mathbb{R},+) \to (\mathbb{R}_{>0},\cdot)$.

תרגיל 2.5.6 (**) איבר בעל סדר סופי ב־$\mathbb{C}$ נקרא **שורש יחידה**. הראה שקבוצת שורשי היחידה ב־$\mathbb{C}$ היא תת־חבורה של S^1.

תרגיל 2.5.7 (+)** הראה שכל אחת מהחבורות $\mathbb{Z}_n$ איזומורפית לתת־חבורה של S^1.

תרגיל 2.5.8 (***) החבורות $(\mathbb{R},+), (\mathbb{C},+)$ איזומורפיות: שתיהן סכום ישר של $\aleph$ עותקים של $(\mathbb{Q},+)$ (הגדרה 1.5.13). **הדרכה.** יהיה עליך להשתמש בקיומו של **הבסיס של האמל**, שהוא בסיס למרחב הוקטורי $\mathbb{R}$ מעל השדה $\mathbb{Q}$.

תרגיל 2.5.9 (***) $S^1 \cong S^1 \times (\mathbb{R},+) \cong S^1 \times (\mathbb{R}_{>0},\cdot) \cong \mathbb{C}^\times$.

תרגיל 2.5.10 (*) הוכח שההעתקה $\nu \colon \mathbb{C}^\times \to \mathbb{R}^\times$ המוגדרת לפי $\nu(z) = z\bar{z}$ היא הומומורפיזם. מה הגרעין שלו?

תרגיל 2.5.11 (+)** כל תת־חבורה נוצרת סופית של $(\mathbb{Q},+)$ היא ציקלית.

תרגיל 2.5.12 (**) מצא שרשרת עולה של תת־חבורות ציקליות $C_1 \subset C_2 \subset C_3 \subset \cdots$ של $(\mathbb{Q},+)$, שהאיחוד שלה שווה ל־$\mathbb{Q}$ כולו. הראה ש־$\mathbb{R}$ אינה איחוד של שרשרת (מעוצמה כלשהי) של תת־חבורות ציקליות.

תרגיל 2.5.13 (***) מצא בחבורה $(\mathbb{Q},+)$ שרשרת עולה ממש של תת־חבורות ציקליות, שעוצמתה $\aleph$. **הדרכה.** ראשית מצא שרשרת עולה ממש $\{I_\alpha\}$ מאותה עוצמה. (**רמז.** $\{r \colon r < \alpha\}$). כעת קבע התאמה חד־חד־ערכית ועל $\pi \colon \mathbb{Q} \to P$ כאשר P היא קבוצת הראשוניים ב־$\mathbb{Z}$. התבונן בחבורות $C_\alpha = \sum_{p \in \pi(I_\alpha)} \mathbb{Z}\frac{1}{p}$.

תרגיל 2.5.14 (**) יהי F שדה. הראה ש־
$$G = \left\{ \begin{pmatrix} 1 & a & b & \frac{a^2+b^2}{2} \\ 0 & 1 & 0 & a \\ 0 & 0 & 1 & b \\ 0 & 0 & 0 & 1 \end{pmatrix} \,:\, a,b \in F \right\}$$
חבורה, וש־$(F^2,+) \cong G$. (G היא תת־חבורה של $H(\diamondsuit)$ מתרגיל 3.5.23.)

תרגיל 2.5.15 (*) חשב את הגרעין עבור ההעתקות הבאות.

1. $\varphi \colon (\mathbb{Z},+) \to (\mathbb{Z},+)$, $\varphi(x) = 4x$.
2. $\varphi \colon \mathbb{R}^\times \to \mathbb{R}^\times$, $\varphi(x) = x^4$.
3. $\varphi \colon \mathbb{C}^\times \to \mathbb{C}^\times$, $\varphi(x) = x^4$.

2.6 החבורות הסימטריות

כל החבורות שפגשנו עד כה היו אבליות. בסעיף זה נגדיר משפחה חשובה של דוגמאות לא אבליות, שבה נעיין שוב בפרק 5.

הגדרה 2.6.1 *יהי $n \geq 1$. **חבורת הסימטריות על n אברים** היא החבורה S_n של כל הפונקציות החד־חד־ערכיות ועל $\{1,\dots,n\}\to\{1,\dots,n\}$, עם פעולת ההרכבה. אברי S_n נקראים **תמורות**.*

אנו מכפילים תמורות מימין לשמאל, כמו הרכבת פונקציות: $(\sigma\tau)(a) = \sigma(\tau(a))$.

יש ספרים שבהם מקובל ההיפך; אבל ראו תרגיל 1.3.19.

תרגיל 2.6.2 (**) בדוק ש־S_n אכן חבורה, מסדר $n!$, שאיבר היחידה שלה היא פונקציית הזהות.

את הגדרה 2.6.1 אפשר להכליל בקלות:

תרגיל 2.6.3 (**) תהי X קבוצה כלשהי. הראה שקבוצת הפונקציות החד־חד־ערכיות ועל $X\to X$ היא חבורה. חבורה זו מסמנים ב־S_X.

תרגיל 2.6.4 (**) אם $|X| = |Y|$ אז $S_X \cong S_Y$.

הגדרה 2.6.5 *כל תמורה $\sigma : \{1,\dots,n\} \to \{1,\dots,n\}$ אפשר להציג כמטריצה $2 \times n$, כך:*

$$\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix}.$$

בשיטה זו, הערך i נמצא בשורה השניה בעמודה ה־$\sigma^{-1}(i)$.

כדי להקל על החישובים, נחוץ לנו סימון חסכוני יותר.

הגדרה 2.6.6 *תמורה $\sigma \in S_n$ המעבירה $r_1 \mapsto r_2 \mapsto \cdots \mapsto r_t \mapsto r_1$ (וקובעת את שאר האברים) נקראת **מחזור**. מסמנים תמורה זו בסימון $\sigma = (r_1\, r_2\, \cdots\, r_t)$. מחזור באורך 2 נקרא **חילוף**. שני מחזורים הם **זרים** אם הם פועלים על איברים שונים.*

טענה 2.6.7 כל תמורה ב־S_n אפשר לכתוב כמכפלה של מחזורים זרים, באופן יחיד עד כדי סדר.

בעקבות טענה 2.6.7, כשמבקשים "לחשב" תמורה מתכוונים בדרך כלל להצגתה כמכפלה של מחזורים זרים.

תרגיל 2.6.8 (*) כתוב כמכפלת מחזורים זרים את התמורות הבאות:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 5 & 3 & 9 & 10 & 1 & 6 & 8 & 7 & 2 & 4 \end{pmatrix}, \qquad \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 4 & 7 & 1 & 3 & 2 & 5 & 6 \end{pmatrix}.$$

תרגיל 2.6.9 (*) כתוב בצורה $\begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix}$ 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 2.6.10 (*) חשב את $(4\,6\,1\,3\,4)(3\,2\,4)(1\,2\,4\,7)$, $(1\,2)(1\,3)\cdots(1\,n)$.

תרגיל 2.6.11 (*) כל שני מחזורים זרים מתחלפים זה עם זה.

תרגיל 2.6.12 (**) אם שני מחזורים שאינם זרים מתחלפים זה עם זה, אז כל אחד מהם הוא חזקה של השני. **הדרכה.** יהיו σ, τ מחזורים מתחלפים שאינם זרים. ראשית הראה ש־$\mathrm{supp}(\tau) = \mathrm{supp}(\sigma)$. נניח ש־$\sigma = (1\,2\,\cdots\,n)$, ו־$\tau(1) = 1+k$; הראה ש־$\tau = \sigma^k$.

תרגיל 2.6.13 (*) רשום את לוח הכפל של החבורה S_3. מצא את הסדר של כל איבר.

תרגיל 2.6.14 (**) מצא את הסדר של המחזור $(r_1\,\cdots\,r_t)$ ואת הסדר של σ, אם τ_i הם מחזורים זרים מאורכים n_i ו־$\sigma = \tau_1 \cdots \tau_u$.

תרגיל 2.6.15 (**) מצא ב־S_7 איברים מסדר $5, 6, 7, 10$. למה אין אף איבר מסדר 8?

תרגיל 2.6.16 (**) הראה שאם τ_1, τ_2 מחזורים זרים, $\alpha \neq \tau_1(\alpha)$ ו־$\beta \neq \tau_2(\beta)$, אז $\tau_2\tau_1(\alpha\beta)$ מחזור באורך $\mathrm{ord}(\tau_1) + \mathrm{ord}(\tau_2)$.

תרגיל 2.6.17 (*−)** כל תמורה אפשר להציג כמכפלה של שתי תמורות מסדר 2.

תרגיל 2.6.18 (***) כל תמורה אפשר להציג כמכפלה של שני מחזורים.

תרגיל 2.6.19 (**) הוכח שתת־החבורה $K_4 = \langle (12)(34), (13)(24) \rangle \leq S_4$ איזומורפית ל־U_8.

תרגיל 2.6.20 (**) מצא את אברי תת־החבורה של S_6 הנוצרת על־ידי $(145)(263)$ ו־$(36)(15)$.

תרגיל 2.6.21 (*+)** מצא את הסדר של תת־החבורה $\langle (1324)(5768), (1526)(3847) \rangle$ של S_8.

תרגיל 2.6.22 (**) הראה ש־$H = \langle (1234567), (124)(365) \rangle$ היא חבורה מסדר 21. **הערה.** זו תת־החבורה היחידה מסדר 21 של S_8, עד כדי הצמדה (הצמדה תוגדר בסעיף 6.4.)

2.7 חבורות של מטריצות

יהי F שדה.

הגדרה 2.7.1 *לקבוצה $\mathrm{GL}_n(F)$ של המטריצות ההפיכות בגודל $n \times n$ מעל F קוראים **החבורה הלינארית הכללית**. לקבוצה $\mathrm{SL}_n(F)$ של איברי $\mathrm{GL}_n(F)$ בעלי דטרמיננטה 1 קוראים **החבורה הלינארית המיוחדת**.*

תרגיל 2.7.2 (*+)** הראה ש־$\mathrm{GL}_n(F)$ חבורה, וש־$\mathrm{SL}_n(F)$ תת־חבורה שלה, השווה לגרעין של ההומומורפיזם $\det : \mathrm{GL}_n(F) \to F^\times$.

תרגיל 2.7.3 (*−)** יהי $\mathbb{F}_2 = \{0, 1\}$ השדה בן שני אברים (עם פעולות החיבור והכפל מודולו 2). הסבר מדוע $\mathrm{SL}_n(\mathbb{F}_2) = \mathrm{GL}_n(\mathbb{F}_2)$ (מעל כל שדה אחר החבורות שונות). כתוב במפורש את כל אברי $\mathrm{GL}_2(\mathbb{F}_2)$, והראה ש־$\mathrm{GL}_2(\mathbb{F}_2) \cong S_3$.

תרגיל 2.7.4 (*−)** הראה ש־$\mathrm{SL}_2(\mathbb{Z})$ נוצרת על־ידי המטריצות $S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ ו־$T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. **הדרכה.** הראה שעל־ידי הפעלת המטריצה S והחזקות T^q אפשר להגיע מכל עמודה $\begin{pmatrix} a \\ b \end{pmatrix}$ של מספרים זרים, לעמודה $\begin{pmatrix} 1 \\ 0 \end{pmatrix}$. הפעל זאת על העמודה השמאלית של מטריצה נתונה.

תרגיל 2.7.5 (**) תהי $\mathrm{B}_n(F)$ **חבורת בורל**, הכוללת, לפי ההגדרה, את המטריצות ההפיכות המשולשיות עליונות בגודל $n \times n$. הראה שאם $2 \leq n$ החבורה אינה אבלית. (להרחבה ראה תרגיל 3.5.20.)

תרגיל 2.7.6 (*) הוכח ש־ $\mathrm{GL}_2(\mathbb{R}) \cap \left\{\begin{pmatrix} a & b \\ -b & a \end{pmatrix} : a,b \in \mathbb{R}\right\} \cong \mathbb{C}^\times$.

את ההגדרה של $\mathrm{GL}_n(F)$, המגדירה בפרט את החבורות $\mathrm{GL}_n(\mathbb{Z}_p)$, אפשר להכליל לפעולות מודולו מספרים אחרים.

תרגיל 2.7.7 (***) הוכח, באינדוקציה על t, ש־$\left|\mathrm{SL}_2(\mathbb{Z}_{p^t})\right| = (1-p^{-2})p^{3t}$ (זוהי חבורת המטריצות 2×2 שאבריהן מספרים שלמים מודולו p^t, עם דטרמיננטה 1).

תרגיל 2.7.8 (**) עבור הזוגות הבאים של מטריצות, מצא כמה אברים יש בחבורה הנוצרת על־ידיהן. תן את לוח הכפל של החבורה, או לחילופין, רשום את אברי החבורה ותאר כיצד להכפיל שני אברים זה בזה (כך שהמכפלה תהיה גם היא איבר ברשימה).

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

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

תרגיל 2.7.9 (***) כנ"ל עבור $A = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$ ו־$B = \begin{pmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$; A ו־ $C = \begin{pmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix}$.

תרגיל 2.7.10 (***) יהי F שדה. נניח ש־$n_1 \geq \cdots \geq n_d$. יהי $M = \{(f_{ij})\}$ אוסף המטריצות שרכיביהן $f_{ij} \in F[t]$ מקיימים $f_{ij} = 0$ אם $n_i < n_j$ ו־$\deg(f_{ij}) \leq n_i - n_j$ אחרת. הוכח שזו חבורה, ומצא את הסדר שלה אם F סופי.

2.8 החבורות הדיהדרליות

נקבע $n \geq 1$, ו־$\alpha = \frac{2\pi}{n}$. נסמן $\sigma = \begin{pmatrix} \cos(\alpha) & \sin(\alpha) \\ -\sin(\alpha) & \cos(\alpha) \end{pmatrix}$ (שהיא מטריצה אורתוגונלית) ו־ $\tau = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$.

הגדרה 2.8.1 *תת־החבורה* $\langle \sigma, \tau \rangle \leq \mathrm{GL}_2(\mathbb{R})$ *נקראת* ***החבורה הדיהדרלית*** *ה־n־ית, ומסמנים אותה ב־D_n.*

תרגיל 2.8.2 (+)** יהי $\rho = \exp(i\alpha) \in \mathbb{C}$ שורש יחידה מסדר n. נסמן $X = \left\{1, \rho, \rho^2, \ldots, \rho^{n-1}\right\}$. הראה שלכל $T \in \mathrm{M}_2(\mathbb{R})$, $T(X) \subseteq X$ אם ורק אם $T \in D_n$.

תרגיל 2.8.3 (*) האברים σ, τ מקיימים $\sigma^n = \tau^2 = 1$, $\tau\sigma\tau^{-1} = \sigma^{-1}$. הסדר של σ בחבורה הוא n.

תרגיל 2.8.4 (**) כל איבר של D_n אפשר להציג באופן יחיד בצורה $\sigma^i\tau^j$ כאשר $i = 0,1,\ldots,n-1$ ו־$j = 0,1$. בפרט $|D_n| = 2n$. הסק מתרגיל 2.8.3 את נוסחת הכפל $\sigma^i\tau^j \cdot \sigma^{i'}\tau^{j'} = \sigma^{i+(-1)^j i' \pmod{n}}\tau^{j+j' \pmod{2}}$.

תרגיל 2.8.5 (*) $D_1 \cong \mathbb{Z}_2$, $D_2 \cong \mathbb{Z}_2 \times \mathbb{Z}_2$, $D_3 \cong S_3$. החבורה D_n אינה אבלית כאשר $n \geq 3$.

תרגיל 2.8.6 (***) הוכח שתת־החבורה $\langle (1234), (13) \rangle$ של S_4 איזומורפית ל־D_4.

תרגיל 2.8.7 (**) D_n איזומורפית לתת־החבורה של S_n הנוצרת על־ידי התמורות $(1\,2\,\dots\,n)$, ו־$(1,\,n)(2,\,n-1)(3,\,n-2)\dots$.

תרגיל 2.8.8 (-*)** הוכח ש־$\mathrm{Z}(D_{2n+1}) = 1$ ו־$\mathrm{Z}(D_{2n}) = \langle \sigma^n \rangle$.

תרגיל 2.8.9 (**) קבע כמה אברים מסדר 2 יש ב־D_n.

תרגיל 2.8.10 (**) כמה אפימורפיזמים $\varphi\colon D_n \to \mathbb{Z}_2$ יש?

תרגיל 2.8.11 (***) נניח ש־$m \mid n$. הראה שקיימים אפימורפיזם $\alpha\colon D_n \to D_m$, ומונומורפיזם $\beta\colon D_m \to D_n$. חשב את $\alpha \circ \beta$ ואת $\beta \circ \alpha$. (השווה לתרגיל 2.3.15.)

תרגיל 2.8.12 (***) כל תת־חבורה של החבורה הדיהדרלית D_n איזומורפית לאחת מהחבורות הבאות: $\mathbb{Z}_2$, $\mathbb{Z}_2 \times \mathbb{Z}_2$, חבורה ציקלית מסדר m או חבורה דיהדרליות מסדר m, כאשר $m \mid n$.

תרגיל 2.8.13 (**) כל חבורה הנוצרת על־ידי שני אברים מסדר 2 היא דיהדרלית.

פרק 3

חבורות מנה

משפט לגרנז', הקובע שהסדר של תת־חבורה מחלק את סדר החבורה, מגביל את הסדרים האפשריים של תת־חבורות, ומהווה כלי עבודה בסיסי להבנת המבנה של חבורות. בהנתן תת־חבורה H של חבורה G, פירוק G לקוסטים של H מראה ש־$|G|$ מתחלק ב־$|H|$, ולכן גם הסדר של איבר מחלק תמיד את סדר החבורה.

הפרק מציג את המושג של **תת־חבורה נורמלית**, שבלעדיו אי אפשר לתאר חבורות. אם N תת־חבורה נורמלית של G, אז הכפל ב־G משרה מבנה של **חבורת מנה** על מרחב הקוסטים G/N. **משפט האיזומורפיזם הראשון** הוא כלי עבודה חשוב, המאפשר לזהות חבורות בקלות. המשפט מוליך לתאור של חבורות באמצעות **יוצרים** ו**יחסים**.

3.1 קוסטים של תת־חבורה

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 3.1.1 *הקבוצות Hx נקראות **קוסטים שמאליים** של H, והקבוצות xH - **קוסטים ימניים** של H. נגדיר יחס **שקילות** על החבורה G: $x \equiv y \pmod{H}$ **אם** $xy^{-1} \in H$.*

תרגיל 3.1.2 (+*) $x \equiv y \pmod{H}$ אם ורק אם $Hx = Hy$.

תרגיל 3.1.3 (*) הוכח שהיחס $\pmod{H}\ \equiv$ הוא יחס שקילות.

תרגיל 3.1.4 (*) מחלקות השקילות של היחס $\pmod{H}\ \equiv$ הן מהצורה Hx. הסק: שתי מחלקות Hx, Hy הן או שוות או נחתכות באופן ריק (קל להוכיח זאת גם באופן ישיר).

תרגיל 3.1.5 (+*) Hy היא קבוצת האיברים $x \in G$ שעבורם $y \in Hx$.

הגדרה 3.1.6 *תהי $H \leq G$ תת־חבורה. את קבוצת הקוסטים הימניים מסמנים $G/H = \{xH \colon x \in G\}$. בדומה לזה מסמנים את קבוצת הקוסטים השמאליים ב־$H\backslash G = \{Hx \colon x \in G\}$.*

תרגיל 3.1.7 (*) אם $A, B \leq G$ הן תת־חבורות שונות של G, אז $(G/A) \cap (G/B) = \emptyset$.

תרגיל 3.1.8 (**) לכל $x, y \in G$, $|Hy| = |Hx|$, ובפרט $|Hx| = |H|$.

תרגיל 3.1.9 (*) אם G אבלית, אז $Hg = gH$ לכל איבר $g \in G$ ותת־חבורה $H \leq G$.

הגדרה 3.1.10 ***האינדקס** (השמאלי) של H ב־G הוא מספר הקוסטים השמאליים של H בחבורה. את האינדקס מסמנים ב־$[G \colon H]$.*

לכן אין צורך להבדיל בין אינדקס ימני ושמאלי.

תרגיל 3.1.11 (+*)** 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 $Hx \mapsto xH$?)

תרגיל 3.1.12 (-)** 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 3.1.13 (**) רשום את הקוסטים הימניים והשמאליים של תת־החבורות $H = \langle (12) \rangle$ ו־$K = \langle (123) \rangle$ בחבורה S_3.

תרגיל 3.1.14 (**) מצא את הקוסטים של $H = \langle 41, 49, 31 \rangle$ בחבורה U_{120}. (מה האינדקס של H?)

תרגיל 3.1.15 (**) כתוב את כל הקוסטים של תת־החבורה $\{0, 4, 8\} = \langle 4 \rangle$ של $\mathbb{Z}_{12}$.

תרגיל 3.1.16 (+*)** נסמן ב־A_4 את תת־החבורה של S_4 הכוללת, מלבד הזהות, את התמורות שיש להן נקודת שבת אחת, ואת אלו המחליפות שני זוגות זרים של ערכים. הוכח שזו אכן תת־חבורה. מה האינדקס שלה?

תרגיל 3.1.17 (**) נסמן ב־K_4 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. הראה שקבוצת האברים מהצורה $(ij)(k\ell)$, יחד עם איבר היחידה, אינה תת־חבורה של S_5.

3.2 משפט לגרנז'

משפט לגרנז' הוא משפט המבנה הראשון על חבורות. הוא מדגים מוטיב חוזר: הסדר של חבורה (סופית) הוא אחד המאפיינים החשובים ביותר שלה.

משפט 3.2.1 (משפט לגרנז') *לכל שתי חבורות סופיות $H \leq G$, $|H|$ מחלק את $|G|$.*

תרגיל 3.2.2 (**) הראה ש־$[G:H] \cdot |H| = |G|$, והסק את משפט לגרנז'.

מסקנה 3.2.3 לכל איבר בחבורה סופית, סדר האיבר מחלק את סדר החבורה. **הדרכה.** תרגיל 2.3.17.

תרגיל 3.2.4 (*) לכל איבר $x \in G$ בחבורה סופית מתקיים $x^{|G|} = 1$.

שניים מהמשפטים המפורסמים בתורת המספרים האלמנטרית מתקבלים כמקרים פרטיים:

משפט 3.2.5 (המשפט הקטן של פרמה) לכל ראשוני p ומספרי $a \in \mathbb{Z}$ שאינו מתחלק ב־p, $a^{p-1} \equiv 1 \pmod p$.

משפט 3.2.6 (משפט אוילר) לכל שלם n ולכל מספר a הזר ל־n, $a^{\phi(n)} \equiv 1 \pmod n$.

תרגיל 3.2.7 (**) אם $p \equiv -1 \pmod 4$ אז לא קיים x כך ש־$x^2 \equiv -1 \pmod p$.

תרגיל 3.2.8 (+*)** לא קיים פתרון למשוואה $x^3 \equiv 2 \pmod{151}$.

תרגיל 3.2.9 (-*)** לכל שני מספרים a, n, מתקיים $n \,|\, \phi(a^n - 1)$.

תרגיל 3.2.10 (-*)** אברים $g, g' \in G$ הם **צמודים** אם קיים $x \in G$ כך ש־$g' = xgx^{-1}$ (זו הגדרה 5.2.1). הראה שבחבורה מסדר אי־זוגי אף איבר, פרט לאיבר היחידה, אינו צמוד להפכי שלו.

3.3 תת־חבורות נורמליות

תרגיל 3.3.1 (*) אם H תת־חבורה של G, אז לכל $g \in G$ גם gHg^{-1} תת־חבורה.

משפט 3.3.2 *התכונות הבאות של תת־חבורה $H \leq G$ שקולות זו לזו:*

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

הגדרה 3.3.3 *תת־חבורה $H \leq G$ המקיימת את התכונות שבמשפט, נקראת **תת־חבורה נורמלית**. במקרה זה מסמנים $H \lhd G$.*

תרגיל 3.3.4 (*) כתוב בשפה המתייחסת לאברים בלבד את התנאים "H תת־חבורה נורמלית של G" ו־"H תת־חבורה אבלית של G". **פתרון**. למשל, H נורמלית = $(\forall a \in H \forall g \in G, \exists a' \in H \colon ga = a'g)$. H אבלית = $(\forall a \in H \forall a' \in H \colon a'a = aa')$. ראה תרגיל 3.3.8 כדי להשתכנע שהתנאים אינם שקולים זה לזה.

תרגיל 3.3.5 (*) $N \lhd G$ אם ורק אם $G/N = N\backslash G$ (ראה הגדרה 3.1.6).

תרגיל 3.3.6 (*) בכל חבורה G, תת־החבורות הטריוויאליות $1, G$ הן נורמליות.

תרגיל 3.3.7 (*) בחבורה אבלית, כל תת־חבורה היא נורמלית.

תרגיל 3.3.8 (**) תן דוגמה לתת־חבורה נורמלית שאינה אבלית (**הצעה**. $H \leq G = \mathbb{Z}_2 \times S_3$) ולתת־חבורה אבלית שאינה נורמלית (**הצעה**. $H \leq G = S_3$).

תרגיל 3.3.9 (*) לכל חבורה G, $Z(G) \lhd G$.

תרגיל 3.3.10 (+*)** אם $N \lhd G$, אז גם $Z(N) \lhd G$.

תרגיל 3.3.11 (+*)** 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 3.3.2.

תרגיל 3.3.12 (**) הגרעין של כל הומומורפיזם $G \to H$ הוא תת־חבורה נורמלית של G (ראה משפט 3.4.5).

תרגיל 3.3.13 (**) אם $[G:H] = 2$ אז H נורמלית ב־G (ראה ההכללה בתרגיל 6.3.28).

תרגיל 3.3.14 (*) (נורמליות היא תורשתית). אם $N \leq K \leq G$ ו־N נורמלית ב־G, אז N נורמלית ב־K.

תרגיל 3.3.15 (**) (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־$N = \langle (12)(34) \rangle$. **הערה**. השווה לתרגיל 7.2.51.

תרגיל 3.3.16 (**) תת־החבורה הנוצרת על־ידי ריבועי האברים היא נורמלית.

תרגיל 3.3.17 (-*)** בכל חבורה לא־אבלית מסדר 8 יש תת־חבורה ציקלית נורמלית מסדר 4. **הדרכה.** תרגיל 2.1.10

תרגיל 3.3.18 (**) חיתוך משפחה כלשהי של תת־חבורות נורמליות הוא תת־חבורה נורמלית (זהו המשך לתרגיל 1.4.20).

תרגיל 3.3.19 (**) נניח ש־$N_1 \subseteq N_2 \subseteq N_3 \subseteq \cdots$ כולן תת־חבורות נורמליות של חבורה G. הוכח שגם $N = \bigcup N_i$ נורמלית. **הערה.** ראה תרגיל 1.4.9.

תרגיל 3.3.20 (**) תהי $A \subseteq G$ תת־קבוצה. נסמן $A^G = \{gag^{-1}: g \in G, a \in A\}$. הוכח ש־$\langle A^G \rangle$ היא תת־החבורה הנורמלית המינימלית של G המכילה את A.

הגדרה 3.3.21 *תהי $H \leq G$ תת־חבורה. החיתוך $\mathrm{Core}_G(H) = \bigcap_{g \in G} gHg^{-1}$ נקרא **הליבה של** H.*

תרגיל 3.3.22 (**) לכל תת־חבורה $H \leq G$, הליבה $\mathrm{Core}_G(H)$ היא תת־חבורה נורמלית של G. זוהי תת־החבורה הנורמלית הגדולה ביותר של G המוכלת ב־H (וראה תרגיל 4.5.3).

תרגיל 3.3.23 (+*)** נניח שבחבורה מתקיים, עבור n קבוע, $(ab)^n = a^n b^n$ לכל a, b (השווה לתרגיל 2.1.16). נסמן $G^m = \{g^m : g \in G\}$.

1. הוכח כי G^n, G^{n-1} הן תת־חבורות נורמליות של G.
2. כל אברי G^n מתחלפים עם כל אברי G^{n-1}.
3. לכל a, b ב־G, $(aba^{-1}b^{-1})^{n(n-1)} = 1$.

תרגיל 3.3.24 (-*)** אם $A, B \leq G$ תת־חבורות אבליות של G, אז $A \cap B$ נורמלית ב־$\langle A, B \rangle$.

תרגיל 3.3.25 (-)** תהיינה $H_1, H_2 \leq G$.

1. אם H_1 או H_2 נורמלית, אז $H_1 H_2 \leq G$. זו תוצאה שימושית.
2. אם $H_1, H_2 \lhd G$, אז $H_1 H_2 \lhd G$.

תרגיל 3.3.26 (**) מצא דוגמה נגדית לטענה השגויה הבאה: 'אם אחת מהחבורות H_1, H_2 נורמלית, אז $H_1 H_2$ תת־חבורה נורמלית'.

תרגיל 3.3.27 (**) הראה ש־$\{\sigma \in S_5 : \sigma(2) = 2\}$ היא תת־חבורה של S_5. האם היא נורמלית?

3.4 חבורת מנה

כפל של קוסטים מוגדר כפי שמוגדר בסעיף 4.2 כפל של כל שתי תת־קבוצות.

טענה 3.4.1 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 3.3.11. □

תרגיל 3.4.2 **(-***)** תת־חבורה $H \leq G$ היא נורמלית אם ורק אם הפעולה הבינרית $(Ha, Hb) \mapsto Hab$ על קבוצת הקוסטים השמאליים מוגדרת היטב.

תרגיל 3.4.3 **(**)** 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 3.4.4 *אם $N \lhd G$, החבורה G/N נקראת **חבורת המנה**, או "G מודולו N".*

משפט 3.4.5 *תת־חבורה $H \leq G$ היא נורמלית אם ורק אם היא גרעין של הומומורפיזם מ־G לחבורה כלשהי.*

תרגיל 3.4.6 **(**)** הוכח את המשפט. **הדרכה.** N היא הגרעין של ההטלה $G \to G/N$ המוגדרת על־ידי $a \mapsto Na$. [זוהי **ההטלה הקנונית** מ־G ל־G/N.]

תרגיל 3.4.7 **(**)** תהיינה $A_0 \lhd A$, $B_0 \lhd B$ חבורות ותת־חבורות שלהן. הוכח ש־$A_0 \times B_0$ היא תת־חבורה נורמלית של $A \times B$, וש־$(A \times B)/(A_0 \times B_0) \cong (A/A_0) \times (B/B_0)$.

תרגיל 3.4.8 **(*)** בדוק את הדוגמה הבא: $H = \{1, 11, 29, 39\}$ היא תת־חבורה של U_{40}, ואברי חבורת המנה הם הקוסטים I, A, B, C כאשר $I = H$, $A = \{3, 7, 33, 37\}$, $B = \{9, 19, 21, 31\}$, $C = \{13, 17, 23, 27\}$. למעשה, $U_{40}/H \cong \mathbb{Z}_4$ עם יוצר A.

תרגיל 3.4.9 **(**)** הראה שתת־החבורה $K_4 = \langle (12)(34), (13)(24) \rangle$ של S_4 (הנקראת **חבורת הארבעה של קליין**) היא נורמלית, ומצא איזומורפיזם $S_4/K_4 \cong S_3$ (תרגיל 6.1.8 מסביר את האיזומורפיזם האחרון).

תרגיל 3.4.10 **(**)** תן דוגמה נגדית לטענה השגויה: "אם $A, B \lhd G$ ו־$G/A \cong B$, אז $G/B \cong A$".
הצעה. קח $G = U_{15}$.

תרגיל 3.4.11 **(**)** האם יתכן ש־N ו־G/N שתיהן אבליות, אבל G איננה כזו?

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

תרגיל 3.4.12 **(**)** 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־$\mathbb{Z}_2$? (ראה תרגיל 7.3.10.)

תרגיל 3.4.13 **(**)** תן דוגמה 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 $G_1 = \mathbb{Z}_{p^4}$ עם תת־החבורה $N_1 = \langle p^2 \rangle \subseteq G_1$; ו־$G_2 = \mathbb{Z}_{p^3} \times \mathbb{Z}_p$ עם תת־החבורה $N_2 = \langle (p, 1) \rangle \subseteq G_2$.

תרגיל 3.4.14 **(**)** תהי G חבורה, $H \lhd G$ מאינדקס n. הוכח כי $g^n \in H$ לכל $g \in G$.

תרגיל 3.4.15 **(+***)** הוכח ש־$D_{2n}/\mathrm{Z}(D_{2n}) \cong D_n$.

את הבניה של חבורת מנה אפשר להכליל במידת־מה:

תרגיל 3.4.16 **(**)** נניח ש־M מונויד, ו־$G \leq M$ תת־חבורה נורמלית, כלומר תת־מונויד שהוא חבורה המקיימת $aG = Ga$ לכל $a \in M$. הראה שאוסף הקוסטים $M/G = \{Ga \colon a \in M\}$ הוא מונויד.

3.5 משפט האיזומורפיזם הראשון

תרגיל 3.5.1 (**) יהי $\varphi\colon G\to H$ הומומורפיזם של חבורות. תהי $K\lhd G$ תת־חבורה נורמלית. הראה שהפונקציה $\bar{\varphi}(gK)=\varphi(g)$ מוגדרת היטב $\bar{\varphi}\colon G/K\to H$, אם ורק אם $K\subseteq \mathrm{Ker}(\varphi)$; ובמקרה זה, זהו תמיד הומומורפיזם.

משפט 3.5.2 (משפט האיזומורפיזם הראשון) *יהי* $\varphi\colon G\to H$ *הומומורפיזם של חבורות. אז* $G/\mathrm{Ker}(\varphi)\cong \mathrm{Im}(\varphi)$.

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 3.5.3 (+)** הוכח את המשפט.

תרגיל 3.5.4 (*) אם $\varphi\colon G\to H$ על, אז $H\cong G/\mathrm{Ker}(\varphi)$, כלומר: H (איזומורפית ל־) חבורת מנה של G.

תרגיל 3.5.5 (*) $\mathbb{Z}_n\cong\mathbb{Z}/n\mathbb{Z}$.

תרגיל 3.5.6 (**) יהי $\varphi\colon G\to H$ הומומורפיזם, ותהיינה $H_2\le H_1\le H$ תת־חבורות כך ש־$H_2\lhd H_1$. אז $\varphi^{-1}(H_2)\lhd\varphi^{-1}(H_1)$ ו־$\varphi^{-1}(H_1)/\varphi^{-1}(H_2)\cong H_1/H_2$. **הערה**. המקרה $H_2=1$ הוא משפט האיזומורפיזם הראשון.

תרגיל 3.5.7 (**) הוכח ש־$S_4/K_4\cong S_3$ (זהו תרגיל 3.4.9; הפעם העזר במשפט האיזומורפיזם הראשון; ראה תרגיל 6.1.8 להוכחה אינפורמטיבית יותר).

תרגיל 3.5.8 (**) פתור את תרגיל 3.4.15 בעזרת משפט האיזומורפיזם הראשון.

תרגיל 3.5.9 (**) $K\lhd G$, $G/K\cong\mathbb{Z}$. הוכח שלכל n קיימת ב־G תת־חבורה מאינדקס n.

3.5.1 סדרות ודיאגרמות

סדרות ודיאגרמות הן דרך נוחה להציג ולארגן מידע על כמה אובייקטים (למשל חבורות) וכמה הומומורפיזמים ביניהם. למשל, אם נתונים ההומומורפיזמים $f\colon A\to B$ ו־$g\colon B\to C$, אפשר להציג אותן יחד בסדרה

$$A \xrightarrow{f} B \xrightarrow{g} C\ ,$$

שממנה ברור שאפשר לחשב את ההרכבה $g\circ f\colon A\to C$. באותו אופן אפשר לארגן סדרות ארוכות יותר, מהצורה

$$A_0 \xrightarrow{f_0} A_1 \xrightarrow{f_1} \cdots \xrightarrow{f_{n-2}} A_{n-1} \xrightarrow{f_{n-1}} A_n\ . \tag{3.1}$$

בהקשר זה, נוח לסמן ב־0 את ההומומורפיזם הטריוויאלי $A\to B$ השולח כל איבר אל היחידה.

הגדרה 3.5.10 ***הסדרה (3.1) נקראת קומפלקס אם לכל i מתקיים $\mathrm{Im}(f_{i-1})\subseteq\mathrm{Ker}(f_i)$, כלומר $f_i\circ f_{i-1}=0$. הסדרה מדוייקת ברכיב A_i אם $\mathrm{Im}(f_{i-1})=\mathrm{Ker}(f_i)$, ומדוייקת אם היא מדוייקת בכל רכיביה.***

תרגיל 3.5.11 (*+) הומומורפיזם $f\colon A\to B$ הוא חד־חד־ערכי אם ורק אם $1\longrightarrow A\xrightarrow{f} B$ מדוייקת.

תרגיל 3.5.12 **(+*)** הומומורפיזם $f:A\to B$ הוא על אם ורק אם $A \xrightarrow{f} B \longrightarrow 1$ מדוייקת.

תרגיל 3.5.13 **(+*)** הומומורפיזם $f:A\to B$ הוא איזומורפיזם אם ורק אם $1 \longrightarrow A \xrightarrow{f} B \longrightarrow 1$ מדוייקת.

סדרה מדוייקת מהצורה $1 \longrightarrow K \longrightarrow G \xrightarrow{\varphi} Q \longrightarrow 1$ נקראת **סדרה מדוייקת קצרה**.

תרגיל 3.5.14 **(**)** בהנתן סדרה מדוייקת קצרה כמוצג לעיל, $K = \mathrm{Ker}(\varphi)$, $Q = \mathrm{Im}(\varphi)$, ומשפט האיזומורפיזם הראשון קובע ש־$Q \cong G/K$. היינו, G הרחבה של Q על־ידי K (ראה הגדרה 7.4.18).

דיאגרמה היא גרף מכוון שהקודקודים שלו הם חבורות (או אובייקטים אחרים) והחצים שלו הם הומומורפיזמים. למשל,

$$\begin{tikzcd} A \arrow[r, "f"] \arrow[d, "g"] & A' \arrow[d, "g'"] \\ B \arrow[r, "f'"] & B' \end{tikzcd}$$

הדיאגרמה היא **קומוטטיבית** אם הרכבת הפונקציות לאורך מסלול תלויה רק בנקודות הקצה. בדוגמא, הריבוע הוא דיאגרמה מדוייקת אם $g' \circ f = f' \circ g$.

תרגיל 3.5.15 **(+**)** נתונה דיאגרמה קומוטטיבית

$$\begin{tikzcd} 1 \arrow[r] & K \arrow[r] \arrow[d] & G \arrow[r] \arrow[d, "f"] & Q \arrow[r] \arrow[d, dotted] & 1 \\ 1 \arrow[r] & K' \arrow[r] & G' \arrow[r] & Q' \arrow[r] & 1 \end{tikzcd}$$

שבה השורות מדוייקות (הקו המרוסק אינו נתון). הראה שיש הומומורפיזם יחיד לאורך הקו המרוסק, המשלים את הדיאגרמה באופן קומוטטיבי.

תרגם את התוצאה לשפה הבסיסית של תורת החבורות. **הדרכה.** נתון הומומורפיזם $f:G\to G'$ כך ש־$f(K) \subseteq K'$. אז f משרה הומומורפיזם $f:G/K\to G'/K'$.

תרגיל 3.5.16 **(+**)** חזור על שאלה 3.5.15 עבור הדיאגרמה

$$\begin{tikzcd} 1 \arrow[r] & K \arrow[r] \arrow[d, dotted] & G \arrow[r] \arrow[d, "f"] & Q \arrow[r] \arrow[d] & 1 \\ 1 \arrow[r] & K' \arrow[r] & G' \arrow[r] & Q' \arrow[r] & 1 \end{tikzcd}$$

תרגם את התוצאה לשפה הבסיסית של תורת החבורות. **הדרכה.** נתון הומומורפיזם $f:G\to G'$ המשרה הומומורפיזם $f:G/K\to G'/K'$. אז $f(K) \subseteq K'$.

הגדרה 3.5.17 *ההומומורפיזם $f:A\to B$ מפצל את $f_1:A\to B_1$ אם אפשר להשלים את הדיאגרמה הבאה כך שתתחלף:*

$$\begin{tikzcd} A \arrow[r, "f"] \arrow[dr, "f_1"'] & B \arrow[d, dotted] \\ & B_1 \end{tikzcd}$$

כלומר, קיים $g:B\to B_1$ כך ש־$f_1 = g \circ f$.

3.5.2 עוד על שדות ומטריצות

תרגיל 3.5.18 (**) $\mathbb{R}/\mathbb{Z}\cong S^1$.

תרגיל 3.5.19 (-**) $\mathbb{C}^*/S^1\cong\mathbb{R}_{>0}$.

תרגיל 3.5.20 (**) יהי F שדה. נסמן ב־$\mathrm{B}_n(F)$ את חבורת המטריצות המשולשיות־עליונות ההפיכות מעל F, ב־$\mathrm{U}_n(F)$ את החבורה של מטריצות ב־$\mathrm{B}_n(F)$ שרכיבי האלכסון שלהן כולם 1 ("**הרדיקל היוניפוטנטי**"), וב־$T_n(F)$ את אוסף המטריצות הסקלריות ההפיכות. הוכח ש־$\mathrm{U}_n(F)\lhd\mathrm{B}_n(F)$, $T_n(F)\leq\mathrm{B}_n(F)$, $\mathrm{U}_n(F)T_n(F)=\mathrm{B}_n(F)$ ו־$\mathrm{B}_n(F)/\mathrm{U}_n(F)\cong T_n(F)$.

תרגיל 3.5.21 (*) בהמשך לתרגיל 3.5.20, הראה ש־$\mathrm{Z}(U_n(F))=1+Fe_{1n}$. **הדרכה.** חשב את המרכז של $1+e_{ab}$ כאשר $a<b$.

תרגיל 3.5.22 (+*) יהיו A,B,C יחסי סדר חזקים על קבוצה X.

1. הראה ש־$A(BC)=(AB)C$, כאשר $AB=\{(a,c)\colon\ \exists b\in X:(a,b)\in A,(b,c)\in B\}$.
2. אם $B\subseteq A$ או $A\subseteq B$ אז AB הוא יחס סדר חזק.
3. נגדיר $B^1=B$ ו־$B^n=B^{n-1}B$. הראה ש־$\cdots B^3\subseteq B^2\subseteq B$.
4. אם $B\subseteq A$, נאמר ש־A **נורמלי** ב־B (ונסמן $A\lhd B$) אם $AB,BA\subseteq A$. הראה ש־$\emptyset,B\lhd B$. מצא יחס סדר חזק שאין לו תת־יחסים נורמליים פרט לאלה.

תרגיל 3.5.23 (***) (חבורות הייזנברג מוכללות)

1. יהי A יחס בינארי אי־רפלקסיבי על המספרים $\{1,\dots,n\}$. הראה ש־
$$H(A)=1+\sum_{(i,j)\in A}Fe_{ij}$$
היא תת־חבורה של $\mathrm{GL}_n(F)$ אם ורק אם A הוא יחס סדר חזק.
2. יהי $\prec$ יחס סדר על המספרים $\{1,\dots,n\}$. הראה ש**חבורת הייזברג המוכללת** $H(\prec)$ נוצרת על־ידי האברים $1+e_{ij}$, $i\prec j$.
3. הראה שהמרכז של $H(\prec)$ הוא $H(\prec_0)$, כאשר $i\prec_0 j$ אם ורק אם i מינימלי ו־j מקסימלי ביחס ל־$\prec$. (זו הכללה של תרגיל 3.5.21.)
4. $H(\prec)$ אבלית אם ורק אם אין $i\prec j\prec k$, כלומר $\prec^2=\emptyset$.
5. יהיו $\prec'\subseteq\prec$ יחסי סדר חזקים. הראה ש־$H(\prec')\lhd H(\prec)$ אם ורק אם $\prec'\lhd\prec$.
6. עבור יחסי סדר חזקים $\prec'\subseteq\prec$, נסמן
$$\prec'*\prec=\prec\cap[\prec'\cup\{(i,j)\colon\ \forall x((x\prec i\rightarrow x\prec' j)\wedge(j\prec x\rightarrow i\prec' x))\}].$$
   (א) הראה שזהו יחס סדר חזק, המקיים $\prec\supseteq(\prec'*\prec)\supseteq\prec'$.
   (ב) הראה ש־$\prec_0=(\emptyset*\prec)$.
   (ג) אם היחסים מוגדרים על קבוצה סופית ו־$\prec'\subset\prec$, הראה ש־$(\prec'*\prec)\supset\prec'$.

(ד) הפעולה $*$ מונוטונית ברכיב הראשון (אם $\prec''\subseteq\prec'$ אז $(\prec''*\prec)\subseteq(\prec'*\prec)$) אבל לא בשני.

7. נניח ש־$\prec\lhd\prec'$. אז $\mathrm{Z}(H(\prec)/H(\prec'))=H(\prec'*\prec)/H(\prec')$.

8. אם $\prec'\subseteq\prec^k$ אז $(\prec'*\prec)\subseteq(\prec^k*\prec)\subseteq\prec^{k-1}$.

9. נניח ש־$\prec\lhd\prec'$. אז $H(\prec)/H(\prec')$ אבלית אם ורק אם $\prec=\prec*\prec'$, אם ורק אם $\prec^2\subseteq\prec'$.

(ראה גם תרגיל 10.3.23).

תרגיל 3.5.24 (**) על הקבוצה $G=\{(a,b)\colon a,b\in\mathbb{R},\,a\neq0\}$ מגדירים פעולה לפי $(a,b)(c,d)=(ac,ad+b)$. הוכח ש־G חבורה. הראה ש־$K=\{(1,b)\colon b\in\mathbb{R}\}$ נורמלית ב־G, וש־$G/K\cong\mathbb{R}^\times$. מצא תת־חבורה של $\mathrm{GL}_2(\mathbb{R})$ שהיא איזומורפית ל־G. **הערה**. ראה גם תרגיל 7.3.22.

תרגיל 3.5.25 (**) הוכח ש־$\mathrm{SL}_n(\mathbb{R})\lhd\mathrm{GL}_n(\mathbb{R})$ וש־$\mathrm{GL}_n(\mathbb{R})/\mathrm{SL}_n(\mathbb{R})\cong\mathbb{R}^\times$.

הגדרה 3.5.26 *יהי F שדה. $\mathrm{O}_n(F)$ היא **חבורת המטריצות האורתוגונליות**, כלומר*

$$\mathrm{O}_n(F)=\left\{A\in\mathrm{M}_n(F)\colon\ AA^{\mathrm{t}}=I\right\}.$$

תרגיל 3.5.27 (**) הראה ש־$\mathrm{O}_n(F)\leq\mathrm{GL}_n(F)$.

הגדרה 3.5.28 *יהי F שדה, ויהי $n\geq1$. 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־

$$\mathrm{PSO}_n(F)=\mathrm{SO}_n(F)/\{aI\in\mathrm{SO}_n(F)\}.$$

תרגיל 3.5.29 (*) מצא את המטריצות הסקלריות ב־$\mathrm{O}_n(\mathbb{R})$ וב־$\mathrm{SO}_n(\mathbb{R})$.

תרגיל 3.5.30 (*+)** זהה במפורש את החבורות $\mathrm{O}_2(\mathbb{R})$, $\mathrm{PO}_2(\mathbb{R})$, $\mathrm{SO}_2(\mathbb{R})$, $\mathrm{PSO}_2(\mathbb{R})$. הוכח ש־$\mathrm{PO}_2(\mathbb{R})\cong\mathrm{O}_2(\mathbb{R})\cong S^1\times\{\pm1\}$, וש־$\mathrm{PSO}_2(\mathbb{R})=\mathrm{SO}_2(\mathbb{R})\cong S^1$. בדוק שהאיזומורפיזם $\mathrm{PSO}_2(\mathbb{R})\to\mathrm{PO}_2(\mathbb{R})$ מוגדר לפי $\pm a\mapsto a^2$.

תרגיל 3.5.31 (*+)** אם n אי־זוגי, $\mathrm{PO}_n(\mathbb{R})\cong\mathrm{SO}_n(\mathbb{R})=\mathrm{PSO}_n(\mathbb{R})$.

תרגיל 3.5.32 (**) הראה שכל איבר מסדר 2, 3, 4, 6 ב־$\mathrm{GL}_2(\mathbb{R})$ צמוד למטריצה $\begin{pmatrix}1&0\\0&-1\end{pmatrix}$, $\begin{pmatrix}0&-1\\1&-1\end{pmatrix}$, $\begin{pmatrix}0&1\\-1&0\end{pmatrix}$, $\begin{pmatrix}0&-1\\1&1\end{pmatrix}$, בהתאמה.

3.6 ייצוג בעזרת יוצרים ויחסים

הגדרה 3.6.1 *תהי X קבוצה כלשהי.* ***החבורה החופשית על X*** *היא אוסף כל המלים הסופיות באותיות x, x^{-1} עבור $x \in X$, שאין בהן רצף מהצורה xx^{-1} או $x^{-1}x$. פעולת הכפל היא הדבקה של מלים ומחיקת הרצפים האסורים לפי הצורך. את החבורה החופשית מסמנים $\mathrm{Free}(X)$ או $\mathbb{F}_X$. כל חבורה כזו נקראת* ***חבורה חופשית****.*

תרגיל 3.6.2 (+)** אשר ש־$\mathrm{Free}(X)$ היא אכן חבורה, שאיבר היחידה שלה הוא המלה הריקה. (מהו ההפכי של $x_1 \cdots x_n$?)

תרגיל 3.6.3 (**) הקבוצה X יוצרת את $\mathrm{Free}(X)$.

כמו במקרה של החבורה הסימטרית (תרגיל 2.6.4), אם $|X| = |X'|$ אז $\mathrm{Free}(X) \cong \mathrm{Free}(X')$. את החבורה החופשית על קבוצה סופית בגודל n מסמנים $\mathbb{F}_n$.

תרגיל 3.6.4 (**) הסבר מדוע $\mathrm{Free}(\emptyset) = \{1\}$.

תרגיל 3.6.5 (**) $\mathbb{F}_1 \cong \mathbb{Z}$.

כדוגמה נוספת: $\mathbb{F}_2 \cong \mathrm{Free}(\{x, y\})$ כוללת מלים כמו x, xy, $x^{-1}yx^5$, $yxy^{-1}x^{-1}$, וכן הלאה. האברים xyx^{-1} ו־y שונים זה מזה. זו אינה חבורה אבלית.

תרגיל 3.6.6 (-*)** נסמן ב־x, y את היוצרים של $\mathbb{F}_2$. הוכח שתת־החבורה $\langle x^2, xy \rangle$ היא חופשית.

תרגיל 3.6.7 (***) מצא תת־חבורה חופשית עם $\aleph_0$ יוצרים של $\mathbb{F}_2 = \langle x, y \rangle$.

תכונת **האוניברסליות** של החבורות החופשיות מתבטאת בעובדה הבאה:

טענה 3.6.8 תהי G חבורה ותהי X קבוצה. אז לכל פונקציה $f : X \to G$ קיים הומומורפיזם יחיד $\hat{f} : \mathrm{Free}(X) \to G$ המתלכד עם f על אברי X.

במלים אחרות, כדי להגדיר הומומורפיזם $\mathrm{Free}(X) \to G$, די לקבוע את התמונות של קבוצת היוצרים X. שלא כמו במקרה הכללי, בחבורה חופשית כל בחירה של תמונות ליוצרים מגדירה הומומורפיזם.

תרגיל 3.6.9 (+)** תהי G חבורה עם מנה חופשית: $G/N \cong F$. הוכח ש־F איזומורפית לתת־חבורה של G.

תרגיל 3.6.10 (**) כל חבורה G אפשר להציג בצורה F/K כאשר F חופשית. הדרכה. תהי X קבוצת יוצרים של G. אז יש התאמה $\theta : \mathrm{Free}(X) \to G$ השולחת את אברי X לעצמם. לפי משפט האיזומורפיזם הראשון, $G \cong \mathrm{Free}(X)/\mathrm{Ker}(\theta)$.

הבחן בין תת־החבורה הנוצרת על־ידי קבוצה R, לתת־החבורה הנורמלית הנוצרת על־ידי R.

נמשיך את תרגיל 3.6.10. אם $\mathrm{Ker}(\theta)$ היא תת־החבורה הנורמלית הנוצרת על־ידי אברים $r_1, \ldots, r_m$ (תרגיל 3.3.20), אומרים שאלו **יחסים** המגדירים את החבורה, וכותבים $G \cong \langle X \mid r_1, \ldots, r_m \rangle$. בכיוון ההפוך:

הגדרה 3.6.11 *תהיינה $r_1, \ldots, r_m \in \mathrm{Free}(x_1, \ldots, x_n)$ מלים. תהי K תת־החבורה הנורמלית הנוצרת על־ידי $r_1, \ldots, r_m$, כלומר, תת־החבורה של $\mathrm{Free}(x_1, \ldots, x_n)$ הנוצרת על־ידי האברים מהצורה gr_ig^{-1}. אז*

$$\langle x_1, \ldots, x_n \mid r_1, \ldots, r_m \rangle,$$

נקראת ***ייצוג בעזרת יוצרים ויחסים*** *של חבורת המנה $\mathrm{Free}(x_1, \ldots, x_n)/K$. לפעמים כותבים גם*

$$\langle x_1, \ldots, x_n \mid r_1 = \cdots = r_m = 1 \rangle$$

עבור אותה חבורה. אפשר לקצר ולכתוב $\langle X | R \rangle$ כאשר $X = \{x_1, \ldots, x_n\}$ ו־$R = \{r_1, \ldots, r_m\}$.

דוגמא 3.6.12 $\langle x \mid x^n = 1\rangle \cong \mathbb{Z}_n$. בדומה לזה

$$\langle x, y \mid x^n = y^m = 1,\, yx = xy\rangle \cong \mathbb{Z}_n \times \mathbb{Z}_m;$$

שימו לב שהשמטת היחס $xy = yx$ מגדירה חבורה אחרת לגמרי.

דוגמא 3.6.13 החבורה הדיהדרלית D_n מוגדרת (בהגדרה 2.8.1) כחבורה הנוצרת על־ידי יוצרים σ, τ, המקיימים יחסים כגון $\sigma^n = \tau^2 = (\sigma\tau)^2 = 1$. לכן האברים $\sigma^n, \tau^2, (\sigma\tau)^2$ נמצאים בגרעין של ההטלה $\mathrm{Free}(\sigma,\tau) \to D_n$, ומכיוון שהם יוצרים את הגרעין (כתת־חבורה נורמלית),

$$D_n \cong \langle \sigma, \tau \mid \sigma^n = \tau^2 = (\sigma\tau)^2 = 1\rangle.$$

כידוע, הומומורפיזם נקבע על־ידי הערכים שלו על קבוצת יוצרים; אבל לא כל בחירה של תמונות אכן מגדירה הומומורפיזם. לדוגמא, אין הומומורפיזם $\mathbb{Z}_4 \to \mathbb{Z}_{12}$ השולח $1 \mapsto 1$. התרגיל הבא מראה מתי בחירת התמונות של קבוצת היוצרים אכן מגדירה הומומורפיזם.

תרגיל 3.6.14 (+**) יהי $\langle X|R\rangle$ ייצוג של חבורה, ותהי G חבורה כלשהי. תהי $f\colon X \to G$ פונקציה כזו שלכל $r = x_{i_1}^{\epsilon_1} \cdots x_{i_n}^{\epsilon_n} \in R$ מתקיים $f(x_{i_1})^{\epsilon_1} \cdots f(x_{i_n})^{\epsilon_n} = 1$ (במלים אחרות, ההצבה f שולחת את היחסים לאיבר היחידה). אז יש הומומורפיזם $\varphi\colon \langle X|R\rangle \to G$ כך ש־$\varphi(x) = f(x)$ לכל $x \in X$. **הדרכה.** זה תרגיל 3.5.1.

תרגיל 3.6.15 (**) תהי X קבוצת יוצרים, ותהיינה $R, R' \subseteq \mathrm{Free}(X)$ שתי קבוצות של יחסים. אז יש אפימורפיזם $\langle X|R\rangle \to \langle X|R \cup R'\rangle$ המוגדר לפי $x \mapsto x$ לכל $x \in X$; בפרט, $\langle X|R \cup R'\rangle$ היא חבורת מנה של $\langle X|R\rangle$. **הדרכה.** תרגיל 3.6.14.

תרגיל 3.6.16 (***) יהי $\langle X|R\rangle$ ייצוג של חבורה, כאשר $X = \{x_1, \ldots, x_n\}$. נניח ש־$X' = \{x_1', \ldots, x_n'\}$ הם אברים של $\mathrm{Free}(X)$, כך שגם $X \subseteq \mathrm{Free}(X')$. אז החבורה $\langle X'|R'\rangle$ המתקבלת מהחלפת כל יוצר ביחסים $r \in R$ במלה המתאימה באותיות X', היא חבורה איזומורפית ל־$\langle X|R\rangle$.

הדרך לחשב את $\langle X|R\rangle$ היא לכתוב מלים ביוצרים X, ולהחליף כל מלה המופיעה ב־R במלה הריקה. כדי לבצע את ההחלפות בצורה מסודרת, אפשר להתחיל במלה הריקה וליצור גרף שבו מלה w מחוברת ל־wx ב"צבע" x, עבור כל $x \in \Sigma$. אם w מכילה תת־מלה ששייכת ל־R, מחליפים את הקודקוד w בקודקוד המתקבל מהסרתה. (הגרף נקרא **גרף קיילי** של החבורה). קיימת שיטה של Todd-Coxeter (1935) לחישוב האינדקס של תת־חבורה $\langle Y\rangle$ ב־$\langle X|R\rangle$, כאשר $Y \subseteq \langle X|R\rangle$. עם זאת הבעיה אינה ניתנת לחישוב באופן כללי: לא קיים אלגוריתם המכריע האם שתי הצגות סופיות מייצגות חבורות איזומורפיות, או אפילו האם ייצוג סופי $\langle X|R\rangle$ מייצג את החבורה הטריוויאלית.

במקום לכתוב את היחסים כאיברים באגף ימין, $\langle x, y \mid \ldots, w, \ldots\rangle$, מקובל לכתוב משוואות מהצורה $w = 1$ או אפילו $w = w'$ במקום $w'w^{-1} = 1$.

תרגיל 3.6.17 (**) חשב את אברי החבורה $\langle x, y \mid x^3 = y^2 = (xy)^2 = 1\rangle$.

תרגיל 3.6.18 (**) חשב את אברי החבורה $\langle x, y \mid x^3 = y^2 = xyx^{-1}y^{-1} = 1\rangle$.

תרגיל 3.6.19 (***) צייר את גרף קיילי של $\langle x, y \mid x^3, y^3, (xy)^2\rangle$ (ראו להלן: החבורה היא A_4).

תרגיל 3.6.20 (***) צייר חלק מספיק גדול של גרף קיילי של

$$G = \langle x, y, z \mid x^2 = y^2 = z^2 = (xy)^3 = (yz)^3 = (zx)^3 = 1\rangle,$$

על־מנת להשתכנע שהחבורה אינסופית. מצא הטלה $\varphi\colon G \to S_3$. הוכח שהגרעין נוצר על־ידי $a = zxyx$, $b = xyzy$ ו־$c = yxzx$. הראה שהם מקיימים $abc = 1$ ו־$ab = ba$.

תרגיל 3.6.21 (+)** אברים a,b בחבורה מקיימים $a^2=1$ ו־$b^3=ab^2a^{-1}$. הוכח ש־$b^5=1$. הוכח ש־$\langle a,b\rangle$ היא חבורת מנה של D_5.

תרגיל 3.6.22 (**) מצא תת־חבורה נורמלית של $G=\langle a,b\,|\,(ab)^4=(ba)^4,\,a^2b^2=1\rangle$ כך שהמנה ציקלית אינסופית. **הדרכה.** הצב $c=ba$.

תרגיל 3.6.23 (***) אשר את ההצגות הבאות של כמה חבורות קלאסיות:

$$\begin{aligned}
\langle x,y\,|\,x^3=y^3=(xy)^2=1\rangle &\cong A_4;\\
\langle x,y\,|\,x^3=y^4=(xy)^2=1\rangle &\cong S_4;\\
\langle x,y\,|\,x^3=y^5=(xy)^2=1\rangle &\cong A_5;\\
\langle x,y\,|\,x^4=y^6=(xy)^2=(x^{-1}y)^3=1\rangle &\cong S_5;\\
\langle x,y\,|\,x^4=y^5=(xy)^2=(x^{-1}y)^5=1\rangle &\cong A_6;\\
\langle x,y\,|\,x^8=y^3=(xy)^2=[x^4,y]=1\rangle &\cong \mathrm{GL}_2(\mathbb{F}_3);\\
\langle x,y\,|\,x^3=y^3=(xy)^4=(xy^{-1})^4=1\rangle &\cong \mathrm{PSL}_2(\mathbb{F}_7);\\
\langle x,y\,|\,x^3=y^2=(xy)^7=[x,y]^4=1\rangle &\cong \mathrm{PSL}_2(\mathbb{F}_7).
\end{aligned}$$

תרגיל 3.6.24 (**) הגדר סדרה קצרה מדוייקת $1\longrightarrow A_4\hookrightarrow S_4\longrightarrow\{\pm1\}\longrightarrow 1$ בהתאמה להצגות הנתונות בתרגיל 3.6.23. **הדרכה.** השיכון לפי $x\mapsto x,\ y\mapsto yxy^{-1}$, וההטלה לפי $x\mapsto 1,\ y\mapsto -1$.

תרגיל 3.6.25 (*-)** הראה שהחבורה $\mathrm{SL}_2(\mathbb{F}_3)$, שסדרה 24, איזומורפית ל־

$$\langle x,y,z\,|\,x^3=y^3=1,\,(xy)^2=z,\,xz=zx,\,yz=zy\rangle.$$

מצא שיכון של חבורת הקווטרניונים Q_8 (סעיף 3.6.1) כתת־חבורה נורמלית ב־$\mathrm{SL}_2(\mathbb{F}_3)$.
הדרכה. לחלק השני: $\alpha=xy$ ו־$\beta=yx^{-1}$ מקיימים $\alpha^2=\beta^2=z$, וגם $(\alpha\beta)^2=xyyxxyyx=x^{-1}x^{-1}y^{-1}x^{-1}y^{-1}x=x^{-1}(yxyx)^{-1}x=x^{-1}\beta^2x=z$, ולכן $\beta\alpha=\beta^2(\alpha\beta)^{-1}\alpha^2=z\alpha\beta$; מכאן ש־$\langle\alpha,\beta\rangle\cong Q$. נוסף לזה $x\beta x^{-1}=\alpha$, $x\alpha x^{-1}=\alpha\beta$, ומכאן הנורמליות.

תרגיל 3.6.26 (**) נסמן $\Delta_{n,m,k}=\langle x,y\,|\,x^n=y^m=(xy)^k=1\rangle$ (נקראת גם **חבורת המשולש** של (n,m,k).) מצא בסעיף זה כמה דוגמאות שבהן חושבה החבורה $\Delta_{n,m,k}$, והראה שבכולן סדר החבורה הוא $|\Delta_{n,m,k}|=\frac{2}{\kappa}$ כאשר $\kappa=\frac{1}{n}+\frac{1}{m}+\frac{1}{k}-1$ היא ה"עקמומיות" של החבורה. (לעובדה זו יש הסבר גאומטרי שלא נציג כאן.) מצא את כל חבורות המשולש עם עקמומיות חיובית.

תרגיל 3.6.27 (*-)** נסמן $G_{n,m,k}=\langle a,b,c\,|\,a^2=b^2=c^2=(ab)^n=(ac)^m=(bc)^k=1\rangle$ (זוהי דוגמא ל**חבורת** Coxeter). הראה שיש שיכון $\Delta_{n,m,k}\hookrightarrow G_{n,m,k}$ שהתמונה שלו מאינדקס 2.
הדרכה. הראה ש־$G_{n,m,k}=\langle a,x,y:\ a^2=(xa)^2=(ay)^2=x^n=y^m=(xy)^k=1\rangle$, ושעם יוצרים אלה $\langle x,y\rangle$ מאינדקס 2.

תרגיל 3.6.28 (*-)** נתבונן בחבורה

$$G=\langle x,y\,|\,x^4=y^4=(xy)^2=(x^{-1}y)^n=1\rangle.$$

הראה ש־$a=x^{-1}y$, $b=yx^{-1}$ מתחלפים ומקיימים $a^n=b^n=1$. בנוסף, $xax^{-1}=b$, $xbx^{-1}=a^{-1}$, ולכן $\langle a,b\rangle\lhd G$, עם מנה $G/\langle a,b\rangle=\langle x\,|\,x^4=1\rangle\cong\mathbb{Z}_4$. לכן $|G|=4n^2$.

הערה 3.6.29 לחבורה G יכולים להיות ייצוגים רבים בצורה $G\cong F/N$, כאשר F חופשית. היינץ הופף (*Heintz Hopf*) הוכיח שהמנה $M(G)=(N\cap[F,F])/[F,N]$, הנקראת **כופל שור** של החבורה (על־שם ישי שור) אינה תלויה בייצוג.

3.6.1 חבורת הקווטרניונים

הגדרה 3.6.30 ***חבורת הקווטרניונים הכללית מוגדרת על־פי הייצוג***

$$Q_{4n} = \left\langle i, j \mid i^n = j^2, j^4 = 1, jij^{-1} = i^{-1} \right\rangle.$$

את Q_8 מסמנים לפעמים באות Q, והיא נקראת סתם חבורת הקווטרניונים.

תרגיל 3.6.31 (**) כל איבר של Q_{4n} אפשר לכתוב בצורה $i^a j^b$ ולכן

$$Q_{4n} = \left\{ i^a j^b : \ a = 0, \dots, n-1, \ b = 0, 1, 2, 3 \right\}.$$

בפרט $|Q_{4n}| = 4n$ (ולכן $|Q_8| = 8$).

תרגיל 3.6.32 (**) המרכז של Q_{4n} הוא $\langle j^2 \rangle$, ו־$Q_{4n}/\mathrm{Z}(Q_{4n}) \cong D_n$.

תרגיל 3.6.33 (***) מצא את תת־החבורות של Q_8 והראה שכולן אבליות ונורמליות.

תרגיל 3.6.34 (**) הראה ש־$D_4 \not\cong Q_8$. **הדרכה.** תרגיל 2.8.9.

תרגיל 3.6.35 (**) בחבורה Q_8, סמן $k = ij$, ו־$-1 = i^2 = j^2$. הראה ש־$Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}$, כאשר -1 יוצר את המרכז ו־$(-1)^2 = 1$.

תרגיל 3.6.36 (*) באלגברת המטריצות $\mathrm{M}_2(\mathbb{C})$, נסמן $\hat{i} = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$, $\hat{j} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$. בדוק ש־$\hat{j}\hat{i} = -\hat{i}\hat{j}$ ו־$\hat{i}^2 = \hat{j}^2 = -1$. הראה ש־$\left\langle \hat{i}, \hat{j} \right\rangle \cong Q_8$.

תרגיל 3.6.37 (***) נסמן ב־$\mathcal{H}$ את חבורת כל המטריצות מהצורה $x + y\hat{i} + z\hat{j} + u\hat{i}\hat{j}$, כאשר

$$x, y, z, u \in \frac{1}{2}\mathbb{Z}, \qquad x^2 + y^2 + z^2 + u^2 = 1.$$

הראה ש־$|\mathcal{H}| = 24$, ו־$Q_8 \triangleleft \mathcal{H}$. הראה ש־$\mathcal{H}/\langle -1 \rangle \cong A_4$. הראה ש־$\mathcal{H} \cong \mathrm{SL}_2(\mathbb{F}_3)$ (השווה לתרגיל 3.6.25).

תרגיל 3.6.38 (***) נסמן ב־$\mathcal{B}$ את חבורת כל המטריצות מהצורה $x + y\hat{i} + z\hat{j} + u\hat{i}\hat{j}$, כאשר x, y, z, u מקיימים את התנאים של תרגיל 3.6.37, או ש־(x, y, z, u) מתקבל מתמורה זוגית של הווקטור $(0, \frac{1}{2}, \frac{\varphi^{-1}}{2}, \frac{\varphi}{2})$, ו־$\varphi = \frac{1+\sqrt{5}}{2}$. בפרט הראה ש־$\mathcal{H} < \mathcal{B}$. הראה ש־$|\mathcal{B}| = 120$. חבורה זו נקראת **חבורת האיקוסהדרון הכפולה**. הראה ש־$\mathcal{B} \cong \mathrm{SL}_2(\mathbb{F}_5)$.

תרגיל 3.6.39 (-*)** הראה שהחבורה $\mathrm{SL}_2(\mathbb{F}_5)$, שסדרה 120, איזומורפית ל־

$$\left\langle x, y \mid x^3 = y^5 = (xy)^4 = 1, \ (xy)^2 = (yx)^2 \right\rangle;$$

וגם ל־

$$\left\langle a, b, c \mid a^2 = b^3 = c^5 = abc \right\rangle;$$

ול־

$$\left\langle \alpha, \beta \mid (\alpha\beta)^2 = \alpha^3 = \beta^5 \right\rangle.$$

מצא שיכון של חבורת הקווטרניונים Q_8 כתת־חבורה ב־$\mathrm{SL}_2(\mathbb{F}_5)$ (ראה תרגיל 10.2.9).

תרגיל 3.6.40 (**) נתבונן בחבורה G שהיוצרים שלה $x_1, \dots, x_{n-1}$ מקיימים את היחסים $x_i^2 = -1$, $x_j x_i = -x_i x_j$ (לכל $i \neq j$), כאשר -1 הוא איבר מרכזי מסדר 2. הראה ש־$|G| = 2^n$, וש־$\mathrm{Z}(G) = 1$. עבור $n = 3$, $G \cong Q_8$. **הערה.** חבורה זו מופיעה בהוכחה של משפט Hurwitz, 1898, הקובע שלא קיימת נוסחת מכפלה לסכומי ריבועים אלא עבור סכומים של $2, 4, 8$ ריבועים בלבד.

פרק 4

סריג תת־החבורות

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

הפעולות הבסיסיות בין תת־חבורות הן חיתוך (החיתוך של שתי תת־חבורות הוא תמיד תת־חבורה, והחיתוך של תת־חבורות נורמליות הוא תמיד תת־חבורה נורמלית), ומכפלה (המכפלה של תת־חבורות היא תת־חבורה אם ורק אם הן מתחלפות, כקבוצות). מתברר שאוסף תת־החבורות הנורמליות של חבורה (שהוא **סריג**) מקיים את תכונת ה**מודולריות**. חבורות מנה המערבות את החיתוך והמכפלה מופיעות ב**משפט האיזומורפיזם השני** ו**משפט האיזומורפיזם השלישי**. את סריג תת־החבורות של חבורת מנה מתאר **משפט ההתאמה**. סעיף 4.7 עוסק בכמה תכונות של המרְכָּז.

אם תת־חבורות A,B נחתכות באופן טריוויאלי ומכפלתן היא החבורה כולה, אז הן **משלימות**. תכונה זו מופיעה ב**מכפלה ישרה פנימית**, וגם במכפלה ישרה למחצה שנפגוש בעתיד. כל חבורה שהיא מכפלה ישרה פנימית מתפרקת גם כמכפלה ישרה חיצונית (ולהיפך).

תת־חבורת הקומוטטורים G' מודדת עד כמה החבורה G רחוקה מאבליות. המנה G/G' היא המנה האבלית הגדולה ביותר של G. סעיף 4.9, שהוא מתקדם יותר, מציג את הרעיון של תת־חבורה מקסימלית וחבורת מנה מקסימלית בעלות תכונות מסויימות, באופן אבסטרקטי.

4.1 חיתוך של תת־חבורות

תרגיל 4.1.1 (**) *נורמליות מתחלפת:* אם $H \leq G$ ו־$N \lhd G$, אז $N \cap H \lhd H$. מצא דוגמה נגדית המראה שלא בהכרח $N \cap H \lhd N$.

תרגיל 4.1.2 (**) אם $N_1, N_2 \lhd G$, אז גם $N_1 \cap N_2 \lhd G$.

תרגיל 4.1.3 (**) אם $A \lhd A_1, B \lhd B_1$ תת־חבורות של G, אז $A \cap B \lhd A_1 \cap B_1$.

הגדרה 4.1.4 *חבורה G היא **פשוטה** אם אין לה תת־חבורות נורמליות.*

תרגיל 4.1.5 (**) תהי $\{G_\lambda \colon \lambda \in \Lambda\}$ שרשרת של חבורות פשוטות. הוכח שגם האיחוד $G = \bigcup_\lambda G_\lambda$ חבורה פשוטה.

4.2 כפל תת־חבורות

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

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

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

תרגיל 4.2.1 (*) הוכח את התכונות

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

תרגיל 4.2.2 (*) אוסף תת־הקבוצות הלא ריקות $P'(S)$ של חבורה־למחצה S הוא חבורה למחצה ביחס לפעולת הכפל של קבוצות, ו־S איבר אפס. אם $1 \in S$ הוא איבר יחידה, אז $\{1\}$ הוא איבר היחידה.

(**בעיית** Tamura שואלת האם האיזומורפיזם $P'(S_1) \cong P'(S_2)$ גורר $S_1 \cong S_2$. נמצאו לכך דוגמאות נגדיות, אבל השאלה עבור חבורות למחצה סופיות עודנה פתוחה.)

תרגיל 4.2.3 (+*) תת־קבוצה לא ריקה $A \subseteq G$ היא תת־חבורה אם ורק אם $AA = A$ ו־$A^{-1} = A$.

תרגיל 4.2.4 (+)** תהיינה $A, B \subseteq G$ תת־קבוצות לא ריקות כך ש־$|G| < |A| + |B|$. הראה ש־$AB = G$.

תרגיל 4.2.5 (**) נניח ש־$H \subseteq G$ תת־קבוצה, ונגדיר $\equiv_H$ כבסעיף 3.1. הוכח שאם $\equiv_H$ יחס שקילות, אז H תת־חבורה.

בפרק 4 נתבונן באוסף תת־החבורות כבסריג. מנקודת מבט זו חשוב לזהות את תת־החבורה הגדולה ביותר המוכלת בשתי תת־חבורות, שהיא כמובן החיתוך $H_1 \cap H_2$, ואת תת־החבורה הקטנה ביותר המכילה את שתיהן, שהיא תת־החבורה הנוצרת על־ידי האיחוד, $\langle H_1 \cup H_2 \rangle = \langle H_1, H_2 \rangle$. א־פריורי, האברים בתת־החבורה הנוצרת עשויים להיות מאד מסובכים (למשל, $xyx'y'x''$ כאשר $x, x', x'' \in H_1$, $y, y' \in H_2$). המקרה הפשוט ביותר הוא כאשר המכפלה H_1H_2, שהאברים שלה פשוטים ומובנים, היא חבורה בעצמה.

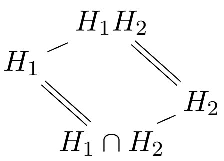
משפט 4.2.6 ***המכפלה H_1H_2 של תת־החבורות H_1, H_2 היא תת־חבורה אם ורק אם $H_1H_2 = H_2H_1$.***

תרגיל 4.2.7 (**) הוכח את המשפט. **הדרכה.** תרגיל 4.2.3.

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 4.2.8 (+)** 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.

תרגיל 4.2.9 (**) (*דוגמה נגדית ל"מכפלת תת־חבורות היא תמיד תת־חבורה"*): מצא תת־חבורות של S_3 שאינן מתחלפות.



טענה 4.2.10 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 4.2.11 (***-) הוכח את הטענה. **הדרכה.** הגדר פונקציה $f : H_1 \times H_2 \to H_1H_2$.

תרגיל 4.2.12 (**) תהיינה N, H תת־חבורות של G, כאשר N נורמלית. אז:

1. $NH \leq G$,
2. $N \lhd NH$,
3. ו־$N \cap H \lhd H$.

משפט 4.2.13 (משפט האיזומורפיזם השני) *תהי G חבורה עם תת־חבורה H ותת־חבורה נורמלית N. אז* $NH/N \cong H/N \cap H$.

תרגיל 4.2.14 (**) הוכח את המשפט. **הדרכה.** הגדר $\varphi : H \to NH/N$ לפי $\varphi(h) = hN$.

תרגיל 4.2.15 (**) תהי G חבורה עם תת־חבורה נורמלית N. נגדיר $\theta : G \to G/N$ לפי $\theta(g) = gN$. תהי $H \leq G$. בדוק שמשפט האיזומורפיזם השני אינו אלא הטענה ש־$H/\mathrm{Ker}(\theta|_H) \cong \mathrm{Im}(\theta|_H)$.

תרגיל 4.2.16 (**) 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 שההעתקה חד־חד־ערכית אם ורק אם $N = H_1 \cap H_2$, ועל אם ורק אם $G = H_1H_2$.

תרגיל 4.2.17 (**) תהי G חבורה עם תת־חבורה H ותת־חבורות נורמליות N, N'. הוכח: אם $N \cap H = N' \cap H$, אז $(HN)/N \cong (HN')/N'$.

תרגיל 4.2.18 (**) תהי G חבורה עם תת־חבורה H ותת־חבורות נורמליות N, N'. הוכח: אם $HN = HN'$, אז $N/(H \cap N) \cong N'/(H \cap N')$.

תרגיל 4.2.19 (**) לכל $N \lhd G$, $\mathrm{Z}(G)N/N \subseteq \mathrm{Z}(G/N)$.

תרגיל 4.2.20 (***) 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־$\mathrm{Im}(f) = \mathrm{Ker}(g)$ בסדרה הבאה:

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

תרגיל 4.2.21 (**) $N \lhd G$ ו־$N, G/N$ אבליות. H תת־חבורה של G. הוכח שקיימת $K \lhd H$, כך ש־$K, H/K$ אבליות.

תרגיל 4.2.22 (***) 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־$\varphi$ חד־חד־ערכית, אבל $\tilde{\varphi}$ אינה כזו.

תרגיל 4.2.23 (+)** באופן אנלוגי לטענה 2.2.38 אפשר לשאול עבור תת־חבורות $A, B, C \leq G$: נניח ש־$A \subseteq BC$ ו־A, B "זרות", האם בהכרח $A \subseteq C$?

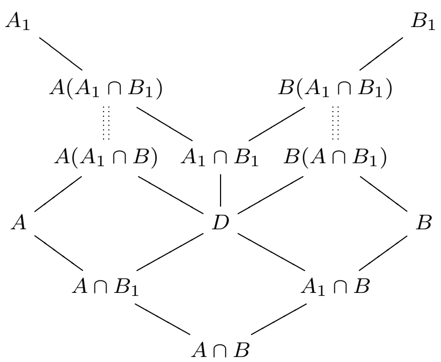
1. נניח ש־$A \subseteq BC$. אם $C \lhd G$ ו־$(|A|, |B|) = 1$, אז $A \subseteq C$.
2. הנחת הנורמליות של C בסעיף הראשון הכרחית: תן דוגמה שבה $1 \neq A \subseteq BC$, $B \lhd G$ ו־$(|A|, |B|) = 1$, אבל $A \cap C = 1$.
3. ההנחה ש־$(|A|, |B|) = 1$ בסעיף הראשון הכרחית: תן דוגמה שבה $1 \neq A \subseteq BC$, $B, C \lhd G$, $A \cap B = 1$ ובכל זאת $A \cap C = 1$.

תרגיל 4.2.24 (***) (הלמה של זסנהאוס) תהיינה $A \lhd A_1$, $B \lhd B_1$, תת־חבורות של G. הוכח:

א. $A_1 \cap B \lhd A_1 \cap B_1$.

ב. $A(A_1 \cap B) \lhd A(A_1 \cap B_1)$.

ג. $\frac{B(A_1 \cap B_1)}{B(A \cap B_1)} \cong \frac{A(A_1 \cap B_1)}{A(A_1 \cap B)}$. **הדרכה.** התבונן ב־$D = (A_1 \cap B)(A \cap B_1)$, והעזר בדיאגרמה:



4.3 מכפלה ישרה פנימית

הגדרה 4.3.1 *תת־חבורות* $H, K \leq G$ *הן משלימות אם* $H \cap K = 1$ *ו־*$HK = G$.

תרגיל 4.3.2 (*) הראה שאם H, K משלימות אז $HK = KH$.

תרגיל 4.3.3 (*) 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 4.3.4 (*−)** אם A, B תת־חבורות משלימות של G ו־$A \subseteq A_1 \leq G$, אז $[A_1 : A] = |A_1 \cap B|$.

תרגיל 4.3.5 (+)** תן דוגמה נגדית לטענה הבאה: אם A, B תת־חבורות משלימות של G ו־$A_0 \lhd A$, אז A_0B היא חבורה. **הצעה.** קח $G = A_4$, $A = K_4$.

הגדרה 4.3.6 G *היא מכפלה ישרה פנימית של תת־חבורות* H, K *אם* H, K *נורמליות ומשלימות.*

תרגיל 4.3.7 (*) אם G אבלית ו־H, K משלימות, אז G היא מכפלה ישרה שלהן.

אברים מתחלפים = commuting elements.

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

הגדרה 4.3.9 *תהיינה $A,B\leq G$. $[A,B]$ היא תת־החבורה של G הנוצרת על־ידי הקומוטטורים $[a,b]$ עבור $a\in A, b\in B$. (הבדילו בין הסימון הזה לסימון האינדקס $[G\colon H]$. נעסוק בתת־חבורת הקומוטטורים שוב בסעיף 4.8.)*

תרגיל 4.3.10 (*) $[A,B]=1$ אם ורק אם כל איבר $a\in A$ מתחלף עם כל איבר $b\in B$.

תרגיל 4.3.11 (**) תהיינה H,K תת־חבורות משלימות. הוכח: $H,K\lhd G$ אם ורק אם $[H,K]=1$. קריטריון חשוב למכפלה ישרה.

תרגיל 4.3.12 (+)** 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 4.3.13 (-)** 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 4.3.14 *אם G מכפלה ישרה פנימית של H,K, אז $G\cong H\times K$.*

תרגיל 4.3.15 (**) הוכח את המשפט. **הדרכה**. הגדר $\varphi\colon H\times K\to G$ לפי $\varphi(h,k)=hk$.

תרגיל 4.3.16 (+)** $\mathbb{Z}_4$ אינה מכפלה פנימית ישרה של תת־חבורות.

תרגיל 4.3.17 (**) תהיינה $A,B\lhd G$. מצא שיכון $G/(A\cap B)\hookrightarrow G/A\times G/B$.

תרגיל 4.3.18 (**) נניח ש־$A,B\lhd G$. הראה שהמנה $AB/(A\cap B)$ היא מכפלה ישרה.

תרגיל 4.3.19 (***) H,K תת־חבורות נורמליות של G, שהמנות ביחס אליהן אבליות. הוכח ש־$G/H\cap K$ אבלית. **הדרכה**. תרגיל 4.3.17. **הערה**. מתרגיל זה אפשר להסיק את קיומן של מנות מקסימליות מטיפוס מסויים, ראה תרגיל 4.9.6.

תרגיל 4.3.20 (**) 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_1K/K ו־H_2K/K.

תרגיל 4.3.21 (***) נניח ש־G מכפלה ישרה פנימית של $\langle\epsilon\,|\,\epsilon^2=1\rangle\cong\mathbb{Z}_2$ ו־G_0. הוכח שכל תת־חבורה של G שאינה מכילה את ϵ, איזומורפית לתת־חבורה של G_0. **הדרכה**. אם $H\not\subseteq G_0$, נפרק $H=H_0\cup H_1$ כאשר $H_0=H\cap G_0$ ו־$H_1=H-H_0$. הראה ש־$H\cong H_0\cup\epsilon H_1\leq G_0$.

תרגיל 4.3.22 (**) תהי G חבורה עם תת־חבורה G_0 מאינדקס 2. נניח שיש אפימורפיזם $\varphi\colon G\to G_0$ כך ש־$\mathrm{Ker}(\varphi)\not\subseteq G_0$. אז $G\cong G_0\times\mathbb{Z}_2$.

4.3.1 מכפלה ישרה של כמה תת־חבורות

הגדרה 4.3.23 *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. *$H_1\cdots H_t=G$.*

תרגיל 4.3.24 (**) אשר שהגדרה 4.3.23, עבור $t=2$, מסכימה עם הגדרה 4.3.6.

משפט 4.3.25 *אם G מכפלה ישרה פנימית של $H_1, \dots, H_t$, אז $G \cong H_1 \times \cdots \times H_t$.*

הוכחה. באינדוקציה על t. אם $t = 2$ זהו משפט **4.3.14**. נסמן $H = H_1 \cdots H_{t-1}$, שהיא תת־חבורה נורמלית של G כי $H_1, \dots, H_{t-1}$ נורמליות. לפי הנחת האינדוקציה, $H \cong H_1 \times \cdots \times H_{t-1}$. אבל לפי ההנחה $HH_t = G$ ו־$H \cap H_t = 1$, ולכן $H \cong H \times H_t \cong H_1 \times \cdots \times H_{t-1} \times H_t$. $\square$

תרגיל 4.3.26 (*-)** תן דוגמה לחבורה G עם 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 מכפלה ישרה פנימית של H_1, H_2, H_3.

תרגיל 4.3.27 (*+)** נניח ש־$H_i \lhd G$, $G = H_1H_2H_3$. אם $H_1 \cap H_2H_3 = H_2 \cap H_3 = 1$ אז G מכפלה ישרה פנימית של H_1, H_2, H_3.

4.4 סריג תת־החבורות

4.4.1 סריגים

הגדרה 4.4.1 *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 4.4.2 (**) הוכח את התכונות הבאות: $a \wedge b \leq a \leq a \vee b$; הפעולות $\wedge, \vee$ הן סימטריות ואסוציאטיביות.

זו הגדרה נוחה לשימוש של החסם העליון והחסם התחתון בסריג.

תרגיל 4.4.3 (*+) לכל a, b בסריג, $x \leq a, b$ אם ורק אם $x \leq a \wedge b$; ו־$a, b \leq x$ אם ורק אם $a \vee b \leq x$.

היזכר בתרגיל 2.2.26. להלן דוגמה נוספת:

תרגיל 4.4.4 (**) 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 4.4.5 (**) תן דוגמה לתת־קבוצה של $P(X)$ שאיננה סריג.

4.4.2 הסריג של תת־החבורות

טענה 4.4.6 אוסף תת־החבורות של חבורה, עם יחס ההכלה, הוא סריג.

תרגיל 4.4.7 (**) 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 4.4.8 (*) אם H_1H_2 תת־חבורה, אז $H_1H_2 = \langle H_1, H_2 \rangle$. אבל אם לא, H_1H_2 אינה נמצאת בסריג תת־החבורות, ולכן אינה יכולה לשמש בעצמה כחסם עליון.

4.4.3 מודולריות

תרגיל 4.4.9 (־)** הראה שבכל סריג, אם $A \leq C$ אז $(A \wedge B) \vee C \leq A \wedge (B \vee C)$.

הגדרה 4.4.10 ***סריג הוא מודולרי אם לכל $A \leq C$ ולכל B, מתקיים*** $(A \wedge B) \vee C = A \wedge (B \vee C)$.

בסריג מודולרי, אם $A \leq C$, מותר לכתוב $A \wedge B \vee C$ ללא חשש של דו־משמעות.

תרגיל 4.4.11 (**) הראה שסריג תת־הקבוצות $P(X)$ הוא מודולרי (כלומר, לכל שלוש קבוצות A, B, C, אם $A \subseteq C$ אז $(A \cap B) \cup C = A \cap (B \cup C)$).

תרגיל 4.4.12 (**) אם A, B, C תת־חבורות של G ו־$A \subseteq C$, אז $(A \cap B) \cdot C = A \cap (B \cdot C)$ (אלו אינן בהכרח תת־חבורות!).

תרגיל 4.4.13 (***) אוסף תת־החבורות הנורמליות של חבורה G הוא סריג מודולרי.

תרגיל 4.4.14 (***) הראה שהסריג של כל תת־החבורות אינו בהכרח מודולרי. **הצעה.** קח $G = S_4$, $C = \langle (12) \rangle$,$A = \langle (12), (34) \rangle$.

תרגיל 4.4.15 (**) תהיינה A, B, C תת־חבורות, כך ש־$CA = CB$, $B \cap C = A \cap C$, ו־$A \subseteq B$. הוכח $A = B$.

תרגיל 4.4.16 (**) 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 $A = B$.

תרגיל 4.4.17 (***) תהי H תת־חבורה של G, עם הומומורפיזם $\psi : G \to H$ כך ש־$\operatorname{Ker}(\psi) \cap H = 1$. אז $H = \operatorname{Im}(\psi)$. **הדרכה.** יישם מודולריות לחבורות $H, \operatorname{Ker}(\psi), \operatorname{Im}(\psi)$. **הערה.** ראה גם תרגיל 7.3.13.

תרגיל 4.4.18 (*) בכל סריג מתקיים $A \vee (B \wedge C) \leq (A \vee B) \wedge (A \vee C)$.

הגדרה 4.4.19 ***סריג הוא דיסטריבוטיבי אם לכל A, B, C מתקיים השוויון***

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

תרגיל 4.4.20 (+*) סריג תת־הקבוצות $P(X)$ הוא דיסטריבוטיבי.

תרגיל 4.4.21 (־*)** כל סריג דיסטריבוטיבי הוא מודולרי.

תרגיל 4.4.22 (**) סריג תת־החבורות הנורמליות אינו בהכרח דיסטריבוטיבי. **הדרכה.** יש להראות שלפעמים $A(B \cap C) \supset (AB) \cap (AC)$. בחר $G = \mathbb{Z}_2 \times \mathbb{Z}_2$.

4.5 אינדקס של תת־חבורות

תרגיל 4.5.1 (+*)** תהיינה $A, B \leq G$ תת־חבורות. נניח ש־$[G : A \cap B]$ סופי.

1. $[AB : B] = [A : A \cap B]$ (איננו מניחים כאן ש־AB היא תת־חבורה.) **הדרכה.** הפונקציה $\{a(A \cap B) :\ a \in A\} \to \{aB :\ a \in A\}$ לפי $a(A \cap B) \mapsto aB$ היא חד־חד־ערכית ועל.
2. $[A : A \cap B] \leq [G : B]$, ויש שוויון אם ורק אם $G = AB$.
3. הסק ש־$[G : A \cap B] \leq [G : A] \cdot [G : B]$, עם שוויון אם ורק אם $G = AB$. (זו טענה 4.2.10.)

תרגיל 4.5.2 (**) תהיינה $A, B \leq G$. אם $[G:A], [G:B]$ זרים, אז $G = AB$. **הדרכה.** תרגיל 4.5.1.

תרגיל 4.5.3 (+)** תהי $H \leq G$ תת־חבורה מאינדקס $[G:H] = n$.

1. הוכח ש־H מכילה תת־חבורה נורמלית מאינדקס $[G:N] \leq n^n$. **הדרכה.** הראה ש־$[G:\mathrm{Core}_G(H)] \leq [G:H]^{[G:H]}$. את $\mathrm{Core}_G(H)$ הגדרנו ב־3.3.21.

תרגיל 6.3.22 מספק תוצאה טובה יותר.

2. נניח ש־$H \leq T \triangleleft G$ עם $[G:T] = m$. הראה ש־H מכילה תת־חבורה נורמלית N מאינדקס $[G:N] \leq m \cdot (n/m)^n$.

בדוק דוגמאות מספריות כדי להתרשם מהשיפור שמספקת תת־חבורת ביניים.

4.6 משפט ההתאמה

משפט 4.6.1 (משפט האיזומורפיזם השלישי) *תהיינה $K \leq N$ תת־חבורות נורמליות של חבורה G.* ***אז*** *$(G/K)/(N/K) \cong G/N$.*

תרגיל 4.6.2 (**) הוכח את המשפט. **הדרכה.** הגדר $\varphi : G/K \to G/N$ לפי $\varphi(gK) = gN$.

תרגיל 4.6.3 (**) תהיינה $A, B, C \triangleleft G$, כך ש־$B \subseteq A$. הוכח ש־AC/BC היא חבורת מנה של A/B.

זו עובדה חשובה ביותר על חבורות מנה.

תרגיל 4.6.4 (**) תהי $N \triangleleft G$. כל תת־חבורה של G/N היא מהצורה H/N עבור $N \subseteq H \leq G$.

משפט 4.6.5 *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 $\mathrm{Im}\varphi$. שני אלו סריגים.*
אז *קיימת התאמה חד־חד־ערכית ועל $\alpha : \mathcal{L}_G \to \mathcal{L}_H$, המקיימת:*

1. *(מונוטוניות) עבור $G_1, G_2 \in \mathcal{L}_G$, $G_1 \leq G_2$* ***אם ורק אם*** *$\alpha(G_1) \leq \alpha(G_2)$.* ולכן α הוא איזומורפיזם של סריגים.
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*** *$G_2 \subseteq G_1$,* ***אז*** *$[G_1 : G_2] = [\alpha(G_1) : \alpha(G_2)]$.*
5. *(שמירה על נורמליות) לכל $N, H \in \mathcal{L}_G$, $N \triangleleft H$* ***אם ורק אם*** *$\alpha(N) \triangleleft \alpha(H)$.*
6. *(שמירה על מנות)* ***אם*** *$N, H \in \mathcal{L}_1$ מקיימות $N \triangleleft H$,* ***אז*** *$H/N \cong \alpha(H)/\alpha(N)$.*

תרגיל 4.6.6 (***) 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, $\alpha \circ \beta = \mathrm{id}_{\mathcal{L}_H}$ ו־$\beta \circ \alpha = \mathrm{id}_{\mathcal{L}_1}$.

תרגיל 4.6.7 (+)** נסח את המשפט במקרה ש־$\varphi : G \to G/K$ הוא הומומורפיזם ההטלה, $g \mapsto gN$. **הערה.** מתקבלת התאמה בין תת־החבורות של G המכילות את K, לבין תת־החבורות של G/K.

תרגיל 4.6.8 (*) נניח ש־$K \triangleleft G$ ו־$K \leq H \leq G$. אז $H/K \triangleleft G/K$ אם ורק אם $H \triangleleft G$.

תרגיל 4.6.9 (+)** מצא את כל תת־חבורה מאינדקס 3 של S_4, והראה שהן אינן נורמליות. **הדרכה.** $K_4 = \langle (12)(34), (13)(24) \rangle$ היא תת־חבורה נורמלית מסדר 4. הראה שהיא מוכלת בכל תת־חבורה מסדר 8 של S_4, ומצא את החבורות האלה בעזרת משפט ההתאמה מן העובדה ש־$S_4/K_4 \cong S_3$.

4.7 המרְכָּז

את המרְכָּז של חבורה הגדרנו בהגדרה 2.1.6.

תרגיל 4.7.1 (*) כל תת־חבורה נורמלית מסדר 2 היא מרכזית.

תרגיל 4.7.2 (**) $H \leq G$. הראה ש־$H \cap \mathrm{Z}(G) \subseteq \mathrm{Z}(H)$, ותן דוגמא שבה זו הכלה אמיתית.

תרגיל 4.7.3 (***) תן דוגמה לחבורה G עם תת־חבורות H המדגימות את כל האפשרויות הבאות:

1. $\mathrm{Z}(H) \subset \mathrm{Z}(G)$,
2. $\mathrm{Z}(G) \subset \mathrm{Z}(H)$,
3. $\mathrm{Z}(H)$ אינו מוכל ב־$\mathrm{Z}(G)$ ואינו מכיל אותו.

תרגיל 4.7.4 (+*)** אם $H \leq G$ ו־$N \lhd G$, אז $\mathrm{Z}(H)N/N \subseteq \mathrm{Z}(HN/N)$.

תרגיל 4.7.5 (**) אם $G/\mathrm{Z}(G)$ חבורה ציקלית, אז G אבלית.

תרגיל 4.7.6 (-*)** תהי H חבורה עם קבוצת יוצרים $x_1, \ldots, x_m$ כך ש־$\langle x_1 \rangle \cap \cdots \cap \langle x_m \rangle \neq 1$. הראה ש־$H$ אינה יכולה להיות מהצורה $G/\mathrm{Z}(G)$. הסק: חבורת הקווטרניונים אינה מהצורה $G/\mathrm{Z}(G)$. **הערה**. תרגיל זה מכליל את תרגיל 4.7.5.

תרגיל 4.7.7 (+**)** הראה שחבורת־p אבלית $\mathbb{Z}_{p^{d_1}} \oplus \mathbb{Z}_{p^{d_2}} \oplus \cdots \oplus \mathbb{Z}_{p^{d_t}}$ יכולה להיות מהצורה $G/\mathrm{Z}(G)$ אם ורק אם $d_t = d_{t-1}$.

תרגיל 4.7.8 (+*) הראה שהמרכז של $\mathrm{GL}_n(F)$ שווה לאוסף המטריצות הסקלריות (מטריצות מהצורה aI).

בתרגיל 5.3.18 נראה שהמרְכָּז של S_n טריוויאלי (כאשר $n \geq 3$).

תרגיל 4.7.9 (***) תהי $G_1 \subseteq G_2 \subseteq G_3 \subseteq \cdots$ שרשרת עולה של חבורות. (בתרגיל 1.4.20 ראינו ש־$\bigcup G_n$ היא חבורה). הוכח ש־$\mathrm{Z}(\bigcup G_n) = \bigcup_m \bigcap_{n \geq m} \mathrm{Z}(G_n)$. (ראה גם תרגיל 6.4.24.)

4.8 תת־חבורת הקומוטטורים

הגדרה 4.8.1 *יהיו $x, y \in G$ אברים של חבורה. האיבר $[x, y] = xyx^{-1}y^{-1}$ **נקרא הקומוטטור** של x, y.*

תרגיל 4.8.2 (*) x, y מתחלפים אם ורק אם $[x, y] = 1$.

תרגיל 4.8.3 (*) $[x, y]^{-1} = [y, x]$.

תרגיל 4.8.4 (*) בחבורת מנה G/N, $[xN, yN] = [x, y]N$.

הגדרה 4.8.5 *תהי G חבורה. **תת־חבורת הקומוטטורים** של G היא תת־החבורה G' הנוצרת על־ידי הקומוטטורים $[x, y]$, $x, y \in G$.*

משפט 4.8.6 *G/G' היא המנה האבלית המקסימלית של G (ונקראת **האבליזציה** של G). ביתר פירוט:*

1. $G' \lhd G$.

2. *G/G' חבורה אבלית.*

3. *לכל תת־חבורה $N \lhd G$, G/N קומוטטיבית אם ורק אם $G' \subseteq N$ (ואז G/N חבורת מנה של G/G').*

תרגיל 4.8.7 (+)** הוכח את המשפט.

תרגיל 4.8.8 (**) אם $N \lhd G$, אז $(G/N)' = G'N/N$.

תרגיל 4.8.9 (**) חשב את S_3', את D_4', ואת A_4'.

תרגיל 4.8.10 (+)** אם $N, M \lhd G$ נחתכות באופן טריוויאלי ו־$G' \subseteq N$, אז $M \subseteq \mathrm{Z}(G)$.

תרגיל 4.8.11 (*) אם $G' \leq N \leq G$ אז $N \lhd G$.

תרגיל 4.8.12 (**) תהי $N \leq G$ תת־חבורה כך ש־$x^2 \in N$ לכל $x \in G$. הוכח ש־$N \lhd G$. **הדרכה.** הראה ש־$G' \subseteq N$.

תרגיל 4.8.13 (***) (בהמשך לתרגיל 1.5.5) נניח ש־$G = G_1 \cup G_2 \cup G_3$, כאשר $G_i \leq G$ תת־חבורות אמיתיות. נסמן $N = G_1 \cap G_2 \cap G_3$. הוכח ש־$[G:N] = 4$. **הדרכה.** הראה ש־$G_i \cap G_j = N$ לכל $i \neq j$. הראה ש־$x^2 \in N$ לכל $x \in G$, והסק ש־$N \lhd G$ (תרגיל 4.8.12). על־ידי מעבר לחבורת המנה G/N, הראה שאפשר להניח ש־$G_i \cap G_j = 1$ לכל $i \neq j$. הראה שלכל $y, y' \in G_j - G_i$ מתקיים $y = y'$, ולכן $[G_j : N] = 2$.

תרגיל 4.8.14 (-*)** תהי $G = \Delta_{(3,3,3)} = \langle x, y \mid x^3 = y^3 = (xy)^3 = 1 \rangle$ חבורת המשולש של $(3,3,3)$.

1. הראה ש־$G' \cong \mathbb{Z} \times \mathbb{Z}$, וחשב את חבורת המנה. **הדרכה.** קח $a = [x,y]$ ו־$b = [x^{-1}, y^{-1}]$. הראה ש־$b = xax^{-1} = yay^{-1}$ ו־$a^{-1}b^{-1} = yby^{-1} = xbx^{-1}$, בעוד ש־$[a,b] = 1$.

2. הראה שהמרכז של x הוא $\langle x \rangle$, והסק ש־$\mathrm{Z}(G) = 1$. **הדרכה.** כל איבר של G אפשר לכתוב כ־$x^i y^j \gamma$ כאשר $\gamma \in G'$; הראה שמ־$y^j \gamma = (xyx^{-1})^j (x\gamma x^{-1})$ נובע $j = 0$ ו־$\gamma = 1$.

3. הראה שכל מנה אמיתית של G היא סופית. **הדרכה.** נניח ש־$N \lhd G$ ו־G/N אינסופית. הראה ש־$N \cap G' = 1$. מכך ש־G אינה אבלית, הסק ש־N מסדר 3. הראה שהיא מרכזית ולכן טריוויאלית.

4. מצא את הסדר של $\langle x, y \mid x^3 = y^3 = (xy)^3 = (xy^{-1})^{3n} = 1 \rangle$. **הדרכה.** ב־$\Delta_{(3,3,3)}$, $(xy^{-1})^3 = a^2 b$; ראה שהסדר של חבורת המנה $G/\langle a^{2n} b^n \rangle^G$ הוא $27n^2$.

תרגיל 4.8.15 (-*)** חזור על תרגיל 4.8.14 (סעיפים 1-3) עבור חבורות המשולש עם עקמומיות אפס, $G = \Delta_{(2,3,6)}$ ו־$\Delta_{(2,4,4)}$ (ראה תרגיל 3.6.26).

הגדרה 4.8.16 *אם $A, B \subseteq G$ תת־קבוצות, מסמנים ב־$[A,B]$ את תת־החבורה הנוצרת על־ידי האברים $[a,b]$ כאשר $a \in A$, $b \in B$. למשל $G' = [G,G]$.*

תרגיל 4.8.17 (*) אם $A, B \lhd G$, אז $[A,B] \lhd G$.

תרגיל 4.8.18 (**) אם A ו־B נורמליות אז $[A,B] \subseteq A \cap B$.

תרגיל 4.8.19 (**) אם $K \subseteq A, B$ תת־חבורות נורמליות של חבורה G, אז בחבורת המנה G/K מתקיים $[A/K, B/K] = [A,B]K/K$.

תרגיל 4.8.20 (-*)** נניח ש־$A \lhd G$ עם G/A ציקלית. הראה ש־$[G,G] = [G,A]$.

תרגיל 4.8.21 (**) (זהות Hall) נסמן $(a,b,c)=[[a^{-1},b],c]^a$. הוכח את הזהות
$$(a,b,c)(c,a,b)(b,c,a)=1.$$

תרגיל 4.8.22 (***) (למת השלוש) אם $A,B,C\lhd G$, אז $[[A,B],C]\subseteq[[B,C],A]\cdot[[C,A],B]$.
הדרכה. תרגיל 4.8.21.

תרגיל 4.8.23 (**) הראה שלכל $A,B\lhd G$, $[[A,A],B]\subseteq[[A,B],A]$.

תרגיל 4.8.24 (*+)** 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־
$$[A_1,\pi_1(N)]\times[A_2,\pi_2(N)]\subseteq N\subseteq\pi_1(N)\times\pi_2(N).$$

נסמן $x^y=y^{-1}xy$. אם $A,B\subseteq G$ תת־קבוצות, **הסגור הנורמלי** של A ב־ $\langle A,B\rangle$ הוא $\langle A\rangle^B=\langle a^b:\ a\in A,b\in B\rangle$.

תרגיל 4.8.25 (*) $(xy)^z=x^zy^z$, $x^{yz}=(x^y)^z$.

תרגיל 4.8.26 (*) $[x,yz]=[x,y][x,z]^{y^{-1}}$ ו־$[x,y^{-1}]=[y,x]^{y-1}$.

תרגיל 4.8.27 (**) 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 4.8.28 (*) 1. הוכח את הזהות $[b_1ab_1^{-1},b]=[b_1,a][a,bb_1]$.

2. לכל שתי קבוצות $S,T\subseteq G$, $[\langle S\rangle^T,\langle T\rangle]=[\langle S\rangle,\langle T\rangle]$.

תרגיל 4.8.29 (*+)** הוכח ש־ $[G,[G,x]]\subseteq[G,x]$. **הדרכה.** מצא $a,b,c\in\langle g,x\rangle$ מתאימים, כך שיתקיים $[g,[h,x]]=[a,x][b,x]^{-1}[c,x]^{-1}$.

תרגיל 4.8.30 (*) $[axa^{-1},byb^{-1}]=[a,x][x,[b,y]][b,y][x,y][x,a][[a,x],y][y,b]$.

תרגיל 4.8.31 (**) יהי $G=F/R^F$ ייצוג על־ידי יוצרים ויחסים, כאשר $F=\langle s_1,\dots,s_n\rangle$ חבורה חופשית, ו־$R=\langle r_1,\dots,r_m\rangle^F$ היא חבורת היחסים. הוכח ש־ $[R,F]=[\langle r_j\rangle^S,\langle S\rangle]=\langle s_{i'}[r_j,s_i]s_{i'}^{-1}\rangle=\langle[\{r_j\},\{s_i\}]\rangle^S=[\{r_j\},S]$, ובפרט אם F,R נוצרות סופית אז גם $[R,F]$ נוצרת סופית.

תרגיל 4.8.32 (**) מצא איבר $1\neq w\in\mathrm{Free}(x_1,x_2)$ כך שלכל i, ההטלה $x_i\mapsto 1$ שולחת $w\mapsto 1$.

תרגיל 4.8.33 (**) נאמר ש־$w\in\mathbb{F}_k=\mathrm{Free}(x_1,\dots,x_k)$ היא r**־שבירה**, אם כל הטלה של r מבין היוצרים $x_1,\dots,x_k$ שולחת את w לאיבר היחידה, אבל אף הטלה של פחות מ־r יוצרים אינה עושה זאת. מצא איבר 1־שביר של $\mathbb{F}_k$.

תרגיל 4.8.34 (**+)** מצא איבר r־שביר של $\mathbb{F}_k$ $(1<r<k)$.

תרגיל 4.8.35 (**+)** נתונה משפחה F של תת־קבוצות של $S=\{x_1,\dots,x_k\}$ הסגורה להגדלה. מצא מלה w_F כך שלכל קבוצה $A\in F$, הטלת כל אברי A אל היחידה שולחת את w_F לאיבר היחידה, ואילו הטלת כל האברים של קבוצה שאינה ב־A אינה עושה זאת.

4.9 משפחות של חבורות

הגדרה 4.9.1 *תהי $\mathcal{L}$ משפחה של חבורות. נסמן את התכונות האפשריות הבאות:*

1. *(סגירות לתת־חבורות) **אם** $G \in \mathcal{L}$ **אז לכל** $A \leq G$, $A \in \mathcal{L}$;*
2. *(סגירות לתמונות הומומורפיות) **אם** $G \in \mathcal{L}$ **אז לכל** $A \lhd G$, $G/A \in \mathcal{L}$;*

3^*. *(סגירות למכפלה ישרה) **אם** $A_\lambda \in \mathcal{L}$ **לכל** $\lambda \in \Lambda$ **אז** $\prod A_\lambda \in \mathcal{L}$;*

3. *(סגירות למכפלה ישרה סופית) **אם** $A, B \in \mathcal{L}$ **אז** $A \times B \in \mathcal{L}$;*

$3'$. *(סגירות למכפלה נורמלית) **אם** $A, B \lhd G$ **ו־** $A, B \in \mathcal{L}$, **אז** $AB \in \mathcal{L}$;*

$3''$. *(סגירות למכפלה) **אם** $A, B \leq G$, $AB = BA$ **ו־** $A, B \in \mathcal{L}$, **אז** $AB \in \mathcal{L}$;*

$3'''$. *(סגירות למכפלה תת־ישרה) **אם** $A, B \lhd G$, $A \cap B = 1$ **ו־**, $G/A, G/B \in \mathcal{L}$, **אז** $G \in \mathcal{L}$;*

4°. *(סגירות להרחבות מרכזיות) **אם** $N \subseteq \mathrm{Z}(G)$ **ו־** $N, G/N \in \mathcal{L}$, **אז** $G \in \mathcal{L}$;*

4. *(סגירות להרחבות) **אם** $N \lhd G$ **ו־** $N, G/N \in \mathcal{L}$, **אז** $G \in \mathcal{L}$.*
5. *(סגירות לאיחוד שרשראות) **אם** G_λ $(\lambda \in \Lambda)$ **שרשרת עולה של חבורות וכל** $G_\lambda \in \mathcal{L}$, **גם האיחוד** $\bigcup G_\lambda \in \mathcal{L}$.*

משפחה הסגורה לתת־חבורות, לתמונות הומומורפיות ולמכפלה ישרה נקראת **יריעה** (variety). משפחה הסגורה למכפלה תת־ישרה ולתמונות הומומורפיות נקראת **מבנה** (formation).

הערה 4.9.2 (משפט בירקהוף, 1935) כל יריעה אפשר להגדיר על־ידי זהויות (כלומר קיימת קבוצת זהויות, כדוגמת $[x_1, x_2]^2 = 1$, כך שחבורה שייכת ליריעה אם ורק אם היא מקיימת את כל הזהויות בקבוצה (הבחן בין זהויות, החלות על כל אברי החבורה, לבין יחסים בין יוצרים)).

$3'''{\to}3''{\to}3'{\to}3$ **תרגיל 4.9.3 (**)** סגירות למכפלה תת־ישרה גוררת סגירות למכפלה. סגירות למכפלה גוררת סגירות למכפלה נורמלית. סגירות למכפלה נורמלית גוררת סגירות למכפלה ישרה סופית.

$4 \to 3, 4^\circ$ **תרגיל 4.9.4 (**-)** סגירות להרחבות גוררת סגירות להרחבות מרכזיות; כמו־כן, סגירות להרחבות גוררת סגירות למכפלה ישרה סופית.

$2 + 4 \to 3'$ **תרגיל 4.9.5 (**)** סגירות לתמונות הומומורפיות ולהרחבות גוררת סגירות למכפלה נורמלית.

$1 + 3 \to 3'''$ **תרגיל 4.9.6 (+**)** תהי $\mathcal{L}$ משפחה הסגורה לתת־חבורות ולמכפלות ישרות סופיות. נניח ש־ $A, B \lhd G$. הראה שאם $G/A, G/B \in \mathcal{L}$, אז גם $G/(A \cap B) \in \mathcal{L}$. **הדרכה**. תרגיל 4.3.17. הסק ש־$\mathcal{L}$ סגורה למכפלה תת־ישרה.

$$\begin{tikzcd}
 & 1+3 \arrow[d] & \\
 & 3''' \arrow[d] & \\
 & 3'' \arrow[d] & 2+4 \arrow[dl] \arrow[d] \\
3^* \arrow[dr] & 3' \arrow[d] & 4 \arrow[dl] \arrow[d] \\
 & 3 & 4^\circ
\end{tikzcd}$$

תרגיל 4.9.7 (+*)** מצא גרירות נוספות לדיאגרמה משמאל, המתייחסת לתכונות של משפחות, לרבות קבוצות נוספות של תכונות כגון $3 + 4^\circ + 5$. הראה שבכל מקום שאין חץ, הגרירה אינה נכונה.

תרגיל 4.9.8 (***) תהי $\mathcal{L}$ משפחה הסגורה לתת־חבורות ולמכפלות ישרות סופיות. תהי G חבורה סופית. הראה שבין תת־החבורות הנורמליות N שעבורן $G/N \in \mathcal{L}$, יש תת־חבורה מינימלית יחידה. במלים אחרות, לכל חבורה סופית G יש מנה מקסימלית ב־$\mathcal{L}$.

תרגיל 4.9.9 (**) הראה שהאוסף $\mathfrak{Ab}$ של החבורות האבליות סגור לתת־חבורות, לתמונות הומומורפיות ולמכפלה ישרה (הוא מוגדר על־ידי הזהות $[x_1, x_2] = 1$; ראה הערה 4.9.2). הסק מתרגיל 4.9.8 את קיומה של תת־חבורה מינימלית יחידה $K \lhd G$ שעבורה G/K אבלית (לפי משפט 4.8.6, $K = G'$).

תרגיל 4.9.10 (**) תהי $\mathcal{L}$ משפחה הסגורה למכפלה נורמלית. אז לכל חבורה סופית G יש תת־חבורה נורמלית גדולה ביותר השייכת ל־$\mathcal{L}$ (היינו, היא מכילה כל תת־חבורה נורמלית בחבורה השייכת ל־$\mathcal{L}$). **הדרכה.** התבונן במכפלה של כל תת־החבורות הנורמליות של G השייכות ל־$\mathcal{L}$.

תרגיל 4.9.11 (**) תהי $\mathcal{L}$ משפחה הסגורה למכפלה נורמלית ולאיחוד שרשראות. אז לכל חבורה G יש תת־חבורה נורמלית גדולה ביותר השייכת ל־$\mathcal{L}$. **הדרכה.** הסגירות לאיחוד שרשאות מאפשרת להפעיל את הלמה של צורן. אם N תת־חבורה נורמלית מקסימלית השייכת ל־$\mathcal{L}$, אז לכל תת־חבורה נורמלית $K \in \mathcal{L}$, $NK \in \mathcal{L}$ ולכן $N \subseteq NK$, $K \subseteq N$.

פרק 5

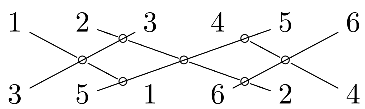
חבורות של תמורות

בפרק זה נלמד את החבורות הסימטריות שהגדרנו בסעיף 2.6. חבורות של תמורות הן אחת הדוגמאות החשובות ביותר לחבורות סופיות, גם מבחינה תאורטית וגם בשימושים של תורת החבורות הסופיות. שאלות רבות בקומבינטוריקה ובאלגוריתמים הקשורים במבנים קומבינטוריים אפשר לתרגם לשפה של החבורות הסימטריות.

חבורת התמורות הזוגיות A_n היא תת־חבורה מאינדקס 2 בחבורת התמורות S_n, הכוללת את התמורות ש**הסימן** שלהן חיובי. מבנה המחזורים של תמורות ב־A_n מאפשר להוכיח שהיא **חבורה פשוטה**.

5.1 הסימן של תמורה

תהי $\sigma \in S_n$ תמורה. נאמר שזוג המספרים $i<j$ **מפר־סדר** אם $\sigma^{-1}i > \sigma^{-1}j$. כפי שצוין בהגדרה 2.6.5, בהצגת התמורה בשתי שורות הערך i עובר למקום ה־$\sigma^{-1}i$, ולכן $i<j$ מפר סדר אם ורק אם הקו הישר המחבר את שתי ההופעות של i נחתך עם הקו הישר המחבר את שתי ההופעות של j. בדוגמה הבאה כל מעגל מסמן הפרת סדר אחת.



הגדרה 5.1.1 ***הסימן של*** $\sigma \in S_n$ ***מוגדר לפי הזוגיות של מספר הפרות הסדר ביחס ל־σ:*** $\operatorname{sgn}(\sigma) = (-1)^{\left|\{i,j:\ i<j,\, \sigma^{-1}i>\sigma^{-1}j\}\right|}$.

טענה 5.1.2 העתקת הסימן $\operatorname{sgn}: S_n \to \{\pm 1\}$ היא הומומורפיזם.

תרגיל 5.1.3 (+)** הוכח את טענה 5.1.2, כלומר, הראה ש־$\operatorname{sgn}(\sigma\tau) = \operatorname{sgn}(\sigma)\operatorname{sgn}(\tau)$. הדרכה. חלק את הזוגות $i<j$ לארבע קבוצות, לפי יחס הסדר בין $\sigma^{-1}i, \sigma^{-1}j$ ו־$\tau^{-1}\sigma^{-1}i, \tau^{-1}\sigma^{-1}j$, וחשב את התרומה של כל זוג לכל אחד מהסימנים.

תרגיל 5.1.4 (**) יהי $\tau = (ab)$ חילוף. הוכח ש־$\operatorname{sgn}(\tau) = -1$. בפרט, לכל $n \geq 2$, sgn היא על.

5.1.1 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 5.1.5 (+*) כתוב את $\Delta_3(x_1,x_2,x_3)$ כסכום של מונומים. השווה את התוצאה ל־$\Delta_3(x_1,x_3,x_2)$.

תרגיל 5.1.6 (**) $\Delta(x_{\sigma(1)},\ldots,x_{\sigma(n)})=\operatorname{sgn}(\sigma)\Delta(x_1,\ldots,x_n)$. **הדרכה.** חשוב על הגורמים (x_i-x_j).

תרגיל 5.1.7 (+)** השתמש בתרגיל 5.1.6 כדי לתת הוכחה נוספת לטענה 5.1.2.

5.1.2 חבורת התמורות הזוגיות

תרגיל 5.1.8 (*) כתוב את המחזור $(a_1a_2\cdots a_t)$ כמכפלה של חילופים ומצא את הסימן שלו. **הדרכה.** $(a_1\ldots a_t)=(a_1a_t)\ldots(a_1a_2)$.

לפי טענה 2.6.7, כל תמורה היא מכפלה של מחזורים (זרים). תרגיל 5.1.8 מראה שכל תמורה אפשר לכתוב כמכפלה של חילופים.

טענה 5.1.9 בכל הדרכים להציג תמורה כמכפלה של חילופים, הזוגיות של מספר החילופים 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 5.1.10 (+)** הוכח את הטענה. **הדרכה.** $\operatorname{sgn}(\sigma)=(-1)^k=(-1)^t$.

תרגיל 5.1.11 (*) כתוב כמה תמורות באקראי, וקבע את הסימן של כל אחת מהן.

כעת אפשר להגדיר את תת־החבורה החשובה ביותר של חבורת הסימטריות:

הגדרה 5.1.12 $A_n=\operatorname{Ker}(\operatorname{sgn})$ ***היא חבורת התמורות הזוגיות.*** *התמורות נקראות כך על־שם מספר החילופים בהצגות שלהן.*

תרגיל 5.1.13 (*) $A_2=1$, $A_3=\langle(123)\rangle$.

תרגיל 5.1.14 (*) $[S_n:A_n]=2$.

תרגיל 5.1.15 (**) תן שלושה נימוקים לכך ש־$A_n\lhd S_n$. **הדרכה.** האינדקס שלה הוא 2 (תרגיל 3.3.13); היא גרעין של הומומורפיזם; וכן ישירות מן ההגדרה.

תרגיל 5.1.16 (**) חשב את $A_4\cap\langle(1234),(13)\rangle$.

תרגיל 5.1.17 (**) אם G תת־חבורה של S_n שאינה מוכלת ב־A_n, אז $A_nG=S_n$ ו־$[G:A_n\cap G]=2$. **הדרכה.** תרגיל 4.5.1.

תרגיל 5.1.18 (**) מצא שיכון של S_n ב־A_{n+2}.

תרגיל 5.1.19 (***) המשחק ב־15 הוא שמה של חידה שפרסם החידונאי סם לויד ב־1880. בחידה זו מסודרות לוחיות ממוספרות מ־1 עד 15 בלוח בגודל 4×4, כך שמשבצת אחת נותרת ריקה. הלוחיות מונחות במקומן, למעט הלוחיות 14 ו־15 המוחלפות זו עם זו. לויד הציע פרס כספי למי שיסדר את הלוחיות בחזרה על־ידי הזזת לוחית אחת בכל פעם למשבצת הריקה. הראה שהבעיה אינה ניתנת לפתרון. **הדרכה.** נסמן את הלוחית הריקה ב־0, כך שמיקום הלוחיות הוא תמורה ב־$S_{\{0,\ldots,15\}}=S_{16}$. נסמן ב־$\chi(\sigma)$ את הערך $(-1)^{i+j}$ כאשר σ ממקמת את המשבצת הריקה במקום ה־(i,j). הראה ש־$\operatorname{sgn}(\sigma)\chi(\sigma)$ אינו משתנה במהלך המשחק.

5.2 אברים צמודים ב־S_n

הגדרה 5.2.1 *תהי G חבורה. אומרים שאברים $g, h \in G$* ***הם צמודים*** *אם קיים $x \in G$ כך ש־$g = xhx^{-1}$. (נחזור לנושא זה בתת־סעיף 6.4.1).*

תרגיל 5.2.2 (**) הראה שהיותם של אברים צמודים זה לזה הוא יחס שקילות.

תרגיל 5.2.3 (**) חשב את כל התמורות ב־S_4 הצמודות ל־$(1\,2\,3)$.

כל תמורה ב־S_n אפשר לכתוב כמכפלה של מחזורים זרים באופן יחיד.

הגדרה 5.2.4 *אם $\sigma \in S_n$ היא מכפלה של מחזורים זרים מאורכים $n_1, \dots, n_t$ (כאשר $n_1 + \cdots + n_t = n$), אז* ***מבנה המחזורים*** *של σ הוא הרשימה הלא־מסודרת $[n_1, \dots, n_t]$.*

לדוגמא, מבנה המחזורים של הזהות הוא $[1, \dots, 1]$; אפשר לקצר ולכתוב $[1^n]$. מבנה המחזורים של $(1234)(56)(78) \in S_9$ הוא $[4, 2^2, 1]$. לפעמים משמיטים את נקודות השבת מן הסימון.

תרגיל 5.2.5 (**) כתוב את כל מבני המחזורים האפשריים לתמורה ב־S_4 וב־S_5. **הערה.** הפונקציה הסופרת כמה מבני מחזורים יש ב־S_n נקרא **פונקציית החלוקה**, ומסמנים אותה ב־$p(n)$. קצב הגידול שלה ידוע: $p(n) \sim \frac{1}{4\sqrt{3}n} e^{\pi\sqrt{2n/3}}$.

משפט 5.2.6 *שתי תמורות ב־S_n הן צמודות אם ורק אם יש להן אותו מבנה מחזורים.*

תרגיל 5.2.7 (***) הוכח את המשפט. **הדרכה.** לכיוון הראשון חשב את הצמוד של מחזור באורך t באופן כללי. לכיוון ההפוך, בהנתן של־τ, σ יש אותו מבנה מחזורים, כתוב אותן זו מעל זו.

תרגיל 5.2.8 (**) מצא $\sigma \in S_6$ כך ש־$(14)(35) = \sigma(12)(34)\sigma^{-1}$.

תרגיל 5.2.9 (**) כמה תמורות $\sigma \in S_8$ יש כך ש־$(1246)(378) = \sigma(1234)(567)\sigma^{-1}$?

תרגיל 5.2.10 (*) מחלקות הצמידות של S_3 הן $[1^3], [2, 1], [3]$. מה הגודל של כל מחלקה?

תרגיל 5.2.11 (**) מצא את כל המחלקות ב־S_4 ואת הגודל של כל מחלקה.

תרגיל 5.2.12 (+)** מצא את כל המחלקות ב־S_5 ואת הגודל של כל מחלקה.

תרגיל 5.2.13 (+)** מצא ארבעה זוגות של מחלקות צמידות מאותו גודל ב־S_6.

תרגיל 5.2.14 (**) כמה מחזורים מאורך r יש ב־S_n?

תרגיל 5.2.15 (**) כמה צמודים יש ל־$(123)(45)$ ב־S_n?

תרגיל 5.2.16 (-)** כמה אברים של S_5 מתחלפים עם $(12)(34)$?

תרגיל 5.2.17 (**) כמה דרכים יש להושיב שבעה אנשים סביב שולחנות עגולים שבאחד מהם יש שלושה מקומות ובשני ארבעה?

תרגיל 5.2.18 (+)** יהי $[1^{a_1} 2^{a_2} \dots n^{a_n}]$ מבנה מחזורים של תמורות ב־S_n; כך $\sum k a_k = n$. הראה שמספר התמורות בעלות מבנה זה הוא $n! \left(\prod k^{a_k} \prod a_k!\right)^{-1}$.

תרגיל 5.2.19 (+)** מצא שתי תת־חבורות אמיתיות H_1, H_2 של S_6, כך שכל איבר של S_6 צמוד לאיבר של אחת מהן. **הצעה.** קח $H_1 = S_5$ ו־$H_2 = \mathrm{Aut}(K_{3,3})$ (ראה תרגיל 6.4.71).

5.2.1 מחלקות צמידות ב־A_n

תרגיל 5.2.20 (**) הראה שהתמורות $(123),(132)$, שיש להן אותו מבנה מחזורים, אינן צמודות ב־A_4. הראה שהן כן צמודות ב־A_5.

תרגיל 5.2.21 (*-)** 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 5.2.22 (***) נניח $n \geq 5$. הראה שכל המחזורים מהצורה (abc) צמודים זה לזה ב־A_n. **הדרכה.** נסמן $x \sim y$ אם x,y צמודים ב־A_n. נראה שמחלקת הצמידות של (123) כוללת את כל המחזורים באורך 3. $(145) = (24)(35)(123)(35)(24)$ מראה שאפשר לעבור ממחזור 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 6.4.31, והסבר מדוע הנימוק של תרגיל 5.2.22 אינו תקף שם.

תרגיל 5.2.23 (-)** במחלקת הצמידות של $(ab)(cd)$ ב־A_n יש $\frac{n(n-1)(n-2)(n-3)}{8}$ אברים. **הדרכה.** תרגיל 5.2.21 מעביר את הבעיה למחלקות ב־S_n.

תרגיל 5.2.24 (*-)** מהי הצורה הכללית של תמורה המתחלפת עם $(1\,2\cdots r)$ ב־S_n?

5.3 קבוצות יוצרים

בסעיף זה נכיר כמה קבוצות יוצרים סטנדרטיות של S_n ושל A_n.

תרגיל 5.3.1 (*) S_n נוצרת על־ידי כל החילופים (ij).

תרגיל 5.3.2 (**) S_n נוצרת על־ידי כל החילופים $(1j)$.

תרגיל 5.3.3 (*-)** S_n נוצרת על־ידי החילוף $\tau = (12)$ והמחזור $\sigma = (123\dots n)$. **הדרכה.** חשב את $\sigma^k\tau\sigma^{-k}$. חשב את $\sigma^j(\tau\sigma^{-1})^{j-i}\tau(\sigma\tau)^{i-j}\sigma^{-j}$.

תרגיל 5.3.4 (*-)** S_n נוצרת על־ידי החילוף $\tau = (1n)$ והמחזור $\sigma = (123\dots n-1)$.

תרגיל 5.3.5 (*+)** S_n נוצרת על־ידי החילופים $\tau_i = (i\,i+1)$, $i = 1,\dots,n-1$. יוצרים אלה מקיימים את היחסים $\tau_i^2 = 1$, $\tau_i\tau_j = \tau_j\tau_i$ אם $|i-j| > 1$, $\tau_i\tau_j\tau_i = \tau_j\tau_i\tau_j$ אם $|i-j| = 1$.
הערה. יחסים אלו מגדירים את **הצגת קוקסטר** של S_n, כחבורה

$$\left\langle x_1,\dots,x_{n-1} \mid x_i^2 = 1,\, x_ix_j = x_jx_i\ (|i-j|>1),\, x_ix_jx_i = x_jx_ix_j\ (|i-j|=1)\right\rangle.$$

תרגיל 5.3.6 (*) 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 5.3.7 (*-)** יהי p ראשוני. אם σ איבר מסדר p ו־τ חילוף, אז הם יוצרים את S_p כולה.

תרגיל 5.3.8 (***) הפרך את הטענה הבאה: אם p ראשוני, S_p נוצרת על־ידי איבר כלשהו מסדר p ואיבר כלשהו מסדר 2.

תרגיל 5.3.9 (**) מצא את תת־החבורה של S_4 הנוצרת על־ידי כל המחזורים מהצורה (abc), a,b,c שונים.

תרגיל 5.3.10 (**) מצא את תת־החבורה של S_4 הנוצרת על־ידי כל התמורות מהצורה $(ab)(cd)$, a,b,c,d שונים.

תרגיל 5.3.11 (**) מצא את הגודל של חבורות התמורות הבאות:

1. $\langle(12),(23)(45)\rangle \subseteq S_5$.
2. $\langle(12),(345)\rangle \subseteq S_5$
3. $\langle(12),(123456)\rangle \subseteq S_6$.

תרגיל 5.3.12 (**) הוכח מההגדרה ש־A_n נוצרת על־ידי כל התמורות עם מבני המחזורים של (123), $(12)(34)$.

תרגיל 5.3.13 (**) נניח ש־$n \geq 5$. החבורה A_n נוצרת על־ידי כל התמורות מהצורה $(ij)(kl)$, i,j,k,l שונים.

תרגיל 5.3.14 (***) A_n נוצרת על־ידי כל המחזורים מאורך 3. **הדרכה.** $(ij)(kt) = (ijk)(jkt)$.

תרגיל 5.3.15 (-)** נניח ש־a,b הם מחזורים באורך 3. הראה שהסדר של $[a,b] = aba^{-1}b^{-1}$ קובע כמה נקודות משותפות יש ל־a,b.

תרגיל 5.3.16 (*-)** יהי T עץ על הקודקודים $1,2,\dots,m$ (**עץ** הוא גרף קשיר ללא מעגלים). לקשת המחברת את הקודקודים i,j מתאימים את החילוף (i,j). הוכח שמכפלת הקשתות על העץ, בכל סדר שיהיה, היא מחזור באורך m.

תרגיל 5.3.17 (**) מה הצורה הכללית של תמורה המתחלפת עם (ij)?

תרגיל 5.3.18 (*-)** $\mathrm{Z}(S_n) = 1$ לכל $3 \leq n$.

תרגיל 5.3.19 (**) מה הצורה הכללית של תמורה המתחלפת עם (ijk)?

תרגיל 5.3.20 (*-)** $\mathrm{Z}(A_n) = 1$ לכל $4 \leq n$.

תרגיל 5.3.21 (*-)** $5 \leq n$. הוכח ש־

1. $S_n' = A_n$. **הדרכה.** כל קומוטטור הוא תמורה זוגית. מאידך, $[(ij),(ik)] = (ijk)$ וסיימנו לפי תרגיל 5.3.14.
2. $A_n' = A_n$.

תרגיל 5.3.22 (***)

1. צפה בפרק ה־10 של העונה ה־6 בסדרה פיוצ'רמה.
2. רשום את 20 החילופים המתבצעים בפרק, ובדוק שמכפלתם היא תמורת הזהות. **הדרכה.** היה עקבי: רשום בכל מקרה את הגופים המחליפים זהויות; או את הזהויות המחליפות גופים.
3. נאמר שסדרת חילופים היא **נאותה** אם אף חילוף אינו מופיע בה פעמיים. הפרופסור מצהיר על המשפט הבא: כל סדרה נאותה של חילופים על n עצמים אפשר להמשיך לסדרה נאותה של חילופים על n העצמים ועוד שניים, כך שמכפלת כל החילופים היא הזהות. תן דוגמא נגדית למשפט זה, אם מסתפקים ב־n העצמים ועוד אחד.
4. הוכח את המשפט.

5.4 A_n חבורה פשוטה

תרגיל 5.4.1 (**) מחלקות הצמידות ב־A_4 הן בגדלים $1,3,4,4$. מצא כמה תת־חבורות נורמליות יש לה.

תרגיל 5.4.2 (**) לחבורה S_4 יש מחלקות צמידות בגדלים $1,3,6,6,8$. מצא נציג מכל מחלקה. מהן תת־החבורות הנורמליות של S_4?

תרגיל 5.4.3 (*−)** תת־החבורה הנורמלית היחידה של S_5 היא A_5. **הדרכה**. תת־חבורה נורמלית כוללת יחד עם כל איבר גם את כל האברים הצמודים אליו; ראה תרגיל 5.2.12 ותרגיל 6.4.6.

תרגיל 5.4.4 (*−)** הוכח ש־A_5 פשוטה מתוך הגדלים של מחלקות הצמידות שלה. **הדרכה**. מחלקות הצמידות הן בגודל $1,12,12,15,20$ (העזר בתרגיל 6.4.34).

שני המשפטים הבאים קרובים ברוחם זה לזה, ואכן אפשר, במאמץ מסויים, להסיק אותם זה מזה (הראשון מעט קשה יותר, טכנית, משום שהוא מאפשר להצמיד רק בתמורות זוגיות). אנו מספקים לשניהם גם הוכחות ישירות. ראה גם תרגיל 6.6.90, המציג הוכחה אלגנטית למשפט 5.4.5 מן התאוריה של פעולת חבורה על קבוצה.

משפט 5.4.5 *A_n פשוטה לכל $5 \leq n$.*

תרגיל 5.4.6 (***) כל תת־חבורה נורמלית לא־טריוויאלית של A_n כוללת מחזור באורך 3. תן לכך שתי הוכחות:

1. הוכחה ישירה. **הדרכה**. יחד עם כל איבר $\sigma \in N$, N כוללת גם כל איבר מהצורה $[\sigma,\tau] = \sigma \cdot \tau\sigma^{-1}\tau^{-1}$ ($\tau \in A_n$). נבחר תמיד τ שאינו נוגע במחזורים ה'אחרים', כך שהם יעלמו בקומוטטור. אם יש ל־$\sigma \in N$ מחזור $(12\dots m)$, $m \geq 4$, חשב את $[(12\dots m),(123)]$ שהוא מחזור באורך 3; כך אפשר להניח שכל המחזורים של σ באורך 1, 2 או 3. אם $\sigma = (123)(456)\cdots$, $[\sigma,(243)] = (15243)$; ואם $\sigma = (123)(45)\cdots$, $[\sigma,(234)] = (123)(45)(234)(132)(45)(243) = (15324)$. לכן, אם יש ל־$\sigma$ מחזור באורך 3, אין מחזורים נוספים והטענה מוכחת. מכאן אפשר להניח ש־σ הוא מכפלה של חילופים. אם $\sigma = (12)(34)(5)\cdots$ אז $[\sigma,(254)] = (13425)$ (נקודת השבת קיימת כי $n \geq 5$), ואם $\sigma = (12)(34)(56)\cdots$ אז $[\sigma,(264)] = (135)(264)$. לכן יש ל־$\sigma$ חילוף בודד לכל היותר, אבל מכיוון שהיא זוגית נובע $\sigma = 1$.

2. בעזרת העובדה ש־A_5 פשוטה. **הדרכה**. תהי $1 \neq \sigma \in N \triangleleft A_n$. קח i כך ש־$i \neq \sigma i = j$. קח $\ell \neq i,j,\sigma j$. נסמן $X = \{i,j,\ell,\sigma j,\sigma\ell\}$. אז σ אינו מתחלף עם $(i\,j\,\ell)$ (כי $\sigma(i\,j\,\ell)i = \sigma j$ ו־$(i\,j\,\ell)\sigma i = \ell$). לכן $1 \neq \omega = [\sigma,(i\,j\,\ell)] = \sigma(i\,j\,\ell)\sigma^{-1} \cdot (i\,j\,\ell)^{-1} = (j\,\sigma j\,\sigma\ell)(i\,\ell\,j) \in N \cap A_X \triangleleft A_X \cong A_5$, ולפי תרגיל 5.4.4, $N \cap A_X = A_X$ ו־$A_X \subseteq N$; מכאן שיש ב־N מחזורים באורך 3.

תרגיל 5.4.7 (**) הוכח את משפט 5.4.5. **פתרון**. אם $1 \neq N \triangleleft A_n$ אז לפי תרגיל 5.4.6 יש ב־N מחזור באורך 3. לפי תרגיל 5.2.22 (מדוע משפט 5.2.6 אינו מספיק?) N כוללת את כל המחזורים באורך 3, ולפי תרגיל 5.3.14, $N = A_n$.

תרגיל 5.4.8 (*+)** הוכח באינדוקציה ש־A_n פשוטה לכל $5 \leq n$. **הדרכה**. תרגיל 5.4.4 מראה ש־A_5 פשוטה. נניח ש־$n \geq 6$. לכל i, נסמן $G_i = \{\sigma \in A_n : \sigma(i) = i\}$. מכיוון ש־$G_i \cong A_{n-1}$, לפי הנחת האינדוקציה כל תת־החבורות האלה פשוטות. כעת תהי $N \triangleleft A_n$ תת־חבורה נורמלית. לפי תרגיל 4.2.12 $N \cap G_i \triangleleft G_i$, ולכן יש שתי אפשרויות: $G_i \subseteq N$ או $N \cap G_i = 1$. אם $G_i \subseteq N$, אז יש ב־N מחזורים באורך 3, וסיימנו לפי תרגיל 5.3.14. מכאן ש־$N \cap G_i = 1$ לכל i, כלומר שלאף איבר לא טריוויאלי ב־N אין נקודות שבת. נניח שיש $1 \neq \sigma \in N$. קבע i כלשהו, וקח $j \neq i, \sigma i, \sigma^{-1} i$. אז המחזור $\tau = (i\,\sigma i\,j)$ מוגדר, ו־$\sigma\tau\sigma^{-1}\tau^{-1} = (\sigma i\,\sigma^2 i\,\sigma j)(i\,j\,\sigma i)$ הוא איבר של N, אינו הזהות משום ש־$\sigma i \mapsto \sigma j$, ויש לו נקודות שבת משום שבחישוב משתתפים רק חמישה ערכים. זו סתירה לכך שאין לאברי N נקודות שבת. **הערה**. הוכחה זו היא וריאציה על תרגיל 5.4.6.(2).

משפט 5.4.9 *נניח $5 \leq n$. תת־החבורה הנורמלית היחידה של S_n היא A_n.*

תרגיל 5.4.10 (***) הוכח את המשפט. **הדרכה.** תהי $N \lhd S_n$. נתבונן באברים של N שאורך המחזור המקסימלי שלהם d הוא הקטן ביותר, ומביניהם ניקח איבר $\sigma \neq 1$ 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 $(a_1a_2a_3\cdots a_d)(a_da_{d-1}\cdots a_3a_1a_2) = (a_1a_3a_2)$ מאפשר להניח $d = 3$ או $d = 2$. במקרה הראשון סיימנו כי המחזורים באורך 3 יוצרים את A_n (תרגיל 5.3.14). במקרה השני, הראה שב־σ יש שני חילופים, והסק ש־$N = A_n$. [היכן נכשלת ההוכחה במקרה $n = 4$?]

תרגיל 5.4.11 (**) ל־A_n אין תת־חבורות שהן נורמליות ב־S_n. **הדרכה.** מיידי ממשפט 5.4.9.

תרגיל 5.4.12 (***) 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־$K \cap K_1 \subseteq N$. הראה ש־KK_1 ו־$K \cap K_1$ תת־חבורות נורמליות של G (ראה סעיף 4.3). הסק: $N \cong K \times K_1$.

תרגיל 5.4.13 (*-)** הראה כיצד להסיק את משפט 5.4.5 ממשפט 5.4.9, אם מניחים ש־A_n אינה איזומורפית לחבורה מהצורה $N \times N$ (עובדה זו נובעת למשל מן הלמה של ברטרנד, לפיה יש מספר ראשוני ברווח $n < p < 2n$ לכל $n > 1$, משום ש־p כזה מחלק את $n!$ בדיוק פעם אחת). **הדרכה.** הפעל את תרגיל 5.4.12 על $G = S_n$ ו־$N = A_n$.

תרגיל 5.4.14 (*-)** 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 4.7.1), בסתירה להנחה.

תרגיל 5.4.15 (**) הסק את משפט 5.4.9 ממשפט 5.4.5. **הדרכה.** לפי תרגיל 5.3.18 אפשר להפעיל את תרגיל 5.4.14.

תרגיל 5.4.16 (***) תהי G_0 חבורה פשוטה, שהיא תת־חבורה מקסימלית 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־$G \cong G_0 \times N \cong G_0 \times G/G_0$.

תרגיל 5.4.17 (*+)**
1. נסמן ב־S_∞ את חבורת התמורות של $\mathbb{N}$ בעלות תומך סופי (התומך של $\sigma : \mathbb{N} \to \mathbb{N}$ הוא $\{x :\ \sigma(x) \neq x\}$). הראה ש־$S_\infty$ היא תת־חבורה נורמלית של חבורת כל התמורות $S_{\mathbb{N}}$. הראה ש־$|S_\infty| = \aleph_0$ בעוד ש־$|S_{\mathbb{N}}| = א$.
2. נסמן ב־A_∞ את תת־החבורה של S_∞ הכוללת תמורות זוגיות. הראה ש־A_∞ פשוטה. **הדרכה.** תרגיל 4.1.5.

תרגיל 5.4.18 (*+)** תן דוגמא לשתי תת־חבורות פשוטות שהחיתוך שלהן אינו פשוט. **הדרכה.** בחר שני עותקים של A_5 ב־S_6 שהחיתוך שלהן איזומורפי ל־A_4.

תרגיל 5.4.19 (*-)** תן דוגמא לשרשרת של חבורות פשוטות, שהחיתוך שלה אינו פשוט. השווה לתרגיל 4.1.5. **הדרכה.** קח $G_n = (A_\infty)_{5,6,\dots,n}$, כלומר המייצב ב־$A_\infty$ של הנקודות $5, 6, \dots, n$. אז $G_n \cong A_\infty$ כולן פשוטות, ו־$\bigcap G_n \cong A_4$.

5.5 תמורות מקריות

ניתן לדלג בקריאה ראשונה.

השאלות בסעיף זה מנוסחות בשפה הסתברותית, אבל אפשר לתרגם אותן בקלות לחישובי ממוצעים, ולתת להן גוון קומבינטורי.

תרגיל 5.5.1 (*) בוחרים באקראי (ובהתפלגות אחידה) $\sigma \in S_n$. מה הסיכוי ש־$\sigma(1) = 3$?

תרגיל 5.5.2 (*+) מה הסיכוי לכך ש־$\sigma(1) = 3$ וגם $\sigma(2) = 3$?

תרגיל 5.5.3 (**) חשב את הסיכוי לכך שהנקודה 1 תשתייך למחזור באורך k, כאשר $1 \leq k \leq n$.

תרגיל 5.5.4 (**) מה הסיכויים לכך שהנקודות $1, 2, \ldots, k$ שייכות כולן לאותו מחזור של תמורה אקראית $\sigma \in S_n$? **הדרכה.** אפשר לבנות באופן אקראי את המחזור המתחיל ב־1 על־ידי הגרלת תמונה אקראית לכל ערך שפגשנו. מכיוון ש־1 אינה תמונה (עדיין), הסדר שבו פוגשים את הנקודות $1, \ldots, k$ הוא אקראי, והנקודות הרצויות תשתתפנה באותו מחזור אם ורק אם האחרונה מבין כולן היא הנקודה 1. לחילופין, פתרון ישיר ומסורבל: $1/k = \sum_{i=1}^{n} \frac{(n-k)!(i-1)!}{n!(i-k)!}$.

תרגיל 5.5.5 (+)** מה תוחלת מספר המחזורים באורך k של תמורה מקרית $\sigma \in S_n$? **הדרכה.** ספור נקודות השייכות למחזורים באורך k.

תרגיל 5.5.6 (**) מה תוחלת מספר המחזורים של תמורה מקרית σ?

תרגיל 5.5.7 (+)** מה הסיכוי שלתמורה אקראית $\sigma \in S_n$ יש מחזור באורך k, כאשר $k > n/2$?

תרגיל 5.5.8 (*-)** חשב את ההתפלגות של מספר נקודות השבת X של תמורה אקראית $\sigma \in S_n$. מה קורה כאשר $n \to \infty$?

פרק 6

פעולה של חבורה על קבוצה

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

חבורות הן בין האובייקטים המרכזיים בכל תחומי המתמטיקה. הסיבה לכך היא שהן יכולות לפעול על מבנים אחרים. מעבר לזה, האפשרות לתאר חבורה לפי הפעולה שלה על קבוצות שונות מוסיפה עומק גם לתורת החבורות עצמה.

פעולה של חבורה היא **נאמנה** אם איבר נקבע על־ידי הפעולה שלו. נקודה במרחב עשויה להיות **נקודת שבת** (אם כל החבורה פועלת עליה באופן טריוויאלי). באופן כללי יותר, לכל נקודה במרחב יש **מייצב**, שהוא תת־החבורה הכוללת את אברי החבורה שאינם מזיזים את הנקודה. הפעולה מפרקת את המרחב ל**מסלולים**, שהגודל של כל אחד מהם שווה לאינדקס של המייצב של נקודות מתוכו, ולכן מחלק את סדר החבורה.

משפט קיילי משתמש בכך שכל חבורה פועלת על עצמה (על־ידי כפל משמאל), כדי להראות שכל חבורה סופית היא תת־חבורה של חבורת תמורות S_n. הפעולה של G על מרחב הקוסטים G/H מוליכה ל**עידון של משפט קיילי**, המספק בין השאר תת־חבורה נורמלית המוכלת ב־H.

פעולה טבעית אחרת של חבורה היא פעולת ההצמדה. תחת פעולה זו, המסלולים הופכים ל**מחלקות צמידות**, והמייצבים הם **מרכְּזים** של איברים. לצד העיסוק במרכזים של אברים, הקדשנו תת־סעיפים גם למרכזים ולמנרמלים של תת־חבורות. המנרמלים מהווים מייצבים בפעולה טבעית אחרת: פעולת ההצמדה של החבורה על אוסף תת־החבורות של עצמה.

הלמה של ברנסייד (סעיף 6.5) סופרת את המסלולים בפעולת חבורה בעזרת מספר נקודות השבת של אברי החבורה. לשיטה הזו יש שימושים קומבינטוריים נרחבים (בעיקר דרך "תורת פוליה" שלא נעסוק בה כאן). סעיף 6.6 עוסק ב**פעולה טרנזיטיבית**, שהיא פעולה שבה כל המרחב מהווה מסלול אחד. למושג חשוב זה יש כמה הכללות, וביניהם רנזיטביות מרובה ו**פעולה רגולרית**. טיפוס אחר, שאנו מציגים רק על קצה המזלג, היא **פעולה פרימיטיבית**, שתחתיה בלתי אפשרי לפרק את המרחב לבלוקים. סעיף 6.6.2 מוקדש כולו לפעולות טבעיות של החבורות הלינאריות, ובעיקר $\mathrm{GL}_2(F)$ כאשר F שדה סופי. אנו מציגים בעזרת הפעולה כמה זוגות מפתיעים של חבורות איזומורפיות. הסעיף האחרון מדגים פעולה של חבורה על אובייקט נוסף: גרפים.

6.1 הפעולה

הגדרה 6.1.1 ***פעולה של חבורה*** *G על קבוצה X היא הומומורפיזם $\Phi\colon G \to S_X$ כאשר S_X היא חבורת התמורות על X.*

הגדרה 6.1.2 ***פעולה של חבורה*** *G על קבוצה X היא פונקציה $\Phi\colon G \times X \to X$ כך ש־$\Phi(gh,x) = \Phi(g,\Phi(h,x))$ לכל $g,h \in G$ ו־$x \in X$.*

תרגיל 6.1.3 (*) הראה ששתי ההגדרות שקולות. **הדרכה.** אם Φ פעולה לפי ההגדרה הראשונה אז $\Phi(g,x) = \Phi(g)(x)$ פעולה לפי ההגדרה השניה, ולהיפך.

הפעולה של G על X מפרשת כל איבר של G כתמורה $\Phi(g)$ (לפי ההגדרה הראשונה, $\Phi(g,\cdot)$ לפי השניה) של אברי הקבוצה X. את תוצאת הפעולה של $g \in G$ על $x \in X$ (כלומר $\Phi(g)(x)$ או $\Phi(g,x)$, בהתאמה) מסמנים ב־$g(x)$, $g \cdot x$ או סתם gx. לפי ההנחה מתקיים $(gh)x = g(hx)$ לכל $g,h \in G$ ו־$x \in X$.

תרגיל 6.1.4 (*) בכל פעולה של חבורה על קבוצה, איבר היחידה פועל באופן טריוויאלי, כלומר $1_G(x) = x$ לכל נקודה x.

תרגיל 6.1.5 (+*) בכל פעולה, כל הפונקציות $x \mapsto g(x)$ הן חד־חד־ערכיות ועל.

6.1.1 דוגמאות ופעולות מושרות

דוגמא 6.1.6 כל חבורה G יכולה לפעול **פעולה טריוויאלית** על כל קבוצה X, אם נגדיר $gx = x$ לכל $g \in G$ ולכל $x \in X$.

דוגמא 6.1.7 חבורת הסימטריות S_n פועלת על הקבוצה $\{1,\dots,n\}$, לפי $\sigma \cdot n = \sigma(n)$. זוהי **הפעולה הטבעית** של S_n.

פעולה של חבורה G על קבוצה X מגדירה באופן טבעי פעולה של כל תת־חבורה של G על אותה קבוצה. אם G פועלת על שתי קבוצות, X ו־Y, **הפעולה האלכסונית** של G על $X \times Y$ מוגדרת לפי $g(x,y) = (gx, gy)$.

תרגיל 6.1.8 (**) הראה שהפעולה הטבעית של S_4 על קבוצת החלוקות $\{12|34, 13|24, 14|23\}$ משרה הומומורפיזם $S_4 \twoheadrightarrow S_3$ שהגרעין שלו הוא K_4 (זהו תרגיל 3.5.7).

תרגיל 6.1.9 (**) מצא שלושה עותקים של D_4 בתוך S_4. **הדרכה.** D_4 פועלת על ארבעת קודקודי הריבוע; ראה גם תרגיל 4.6.9.

6.1.2 פעולה נאמנה

הגדרה 6.1.10 ***פעולת חבורה G על קבוצה X היא נאמנה אם רק איבר היחידה פועל באופן טריוויאלי. במלים אחרות, לכל $1 \neq g \in G$ יש $x \in X$ כך ש־$gx \neq x$.***

תרגיל 6.1.11 (*) נסמן $G_0 = \{g \in G \colon (\forall x \in X) gx = x\}$ את גרעין ההומומורפיזם $G \to S_X$ שמגדירה הפעולה לפי הגדרה 6.1.1. הפעולה נאמנה אם ורק אם $G_0 = 1$.

תרגיל 6.1.12 (*) הפעולה של G על X נאמנה אם ורק אם ההומומורפיזם $G \to S_X$ המתאים לפעולה, $g \mapsto (x \mapsto gx)$, הוא שיכון.

תרגיל 6.1.13 (*) הראה שיש פעולה נאמנה של G על קבוצה בגודל n אם ורק אם יש שיכון $G \hookrightarrow S_n$.

תרגיל 6.1.14 (**) תהי $N \lhd G$, כאשר G פועלת על קבוצה X, ותהי G_0 החבורה המוגדרת בתרגיל 6.1.11. הראה שהנוסחא $(gN)\cdot x = g \cdot x$ מגדירה פעולה של G/N על X, אם ורק אם $N \subseteq G_0$.

תרגיל 6.1.15 (**) תן דוגמה לפעולה נאמנה של $\mathbb{Z}_p \times \mathbb{Z}_p$ על הקבוצה $\mathbb{Z}_2 \times \mathbb{Z}_p$ (כאשר $p > 2$).

6.2 מסלולים ומייצבים

הגדרה 6.2.1 *תהי G חבורה הפועלת על קבוצה X. **המסלול** של $x \in X$ הוא הקבוצה $G\cdot x = \{g \cdot x :\ g \in G\}$.*

תרגיל 6.2.2 (*) היחס "$x \sim y$ אם ורק אם קיים $g \in G$ כך ש־$y = gx$" הוא יחס שקילות, שמחלקות השקילות שלו הן המסלולים של הפעולה.

תרגיל 6.2.3 (*) $x \sim y$ אם ורק אם $x \in G \cdot y$ אם ורק אם $y \in G \cdot x$.

הגדרה 6.2.4 *את קבוצת המסלולים של G בפעולה על X מסמנים ב־$X \backslash G$.*

תרגיל 6.2.5 (*) תהי $H \leq G$ תת־חבורה. הראה ששני הפירושים לסימון G/H, כאוסף הקוסטים השמאליים של H וכאוסף המסלולים בפעולת H על G לפי כפל מימין, מתלכדים.

תרגיל 6.2.6 (**) תהי G חבורה הפועלת על קבוצה X, ותהי $N \triangleleft G$ תת־חבורה נורמלית. הראה שהפעולה של G על X/N, לפי $g(N \cdot x) = N \cdot (gx)$, מוגדרת היטב. הראה ש־$(X/N)/G = X/G$. תן דוגמה שבה, אם $H \leq G$ ואינה נורמלית, G אינה פועלת על X/H.

תרגיל 6.2.7 (**) תאר את המסלולים בפעולת הכפל של S^1 על $\mathbb{C}$.

הגדרה 6.2.8 *המייצב של נקודה $x \in X$ הוא הקבוצה $G_x = \{g \in G :\ gx = x\}$. לכל $g \in G_x$, x נקרא **נקודת שֶבֶת** של g.*

תרגיל 6.2.9 (*) כל מייצב הוא תת־חבורה של G.

תרגיל 6.2.10 (*) תן דוגמה לפעולה נאמנה של חבורה G על קבוצה X עם איבר $x \in G$ כך ש־$G_x = G$.

תרגיל 6.2.11 (**) $G_{gx} = gG_xg^{-1}$ (הזכר בתרגיל 3.3.1).

תרגיל 6.2.12 (**) $G = S_n$ פועלת באופן טבעי על $\{1, \cdots, n\}$. תאר את הקוסטים הימניים והשמאליים של המייצב של הנקודה n.

תרגיל 6.2.13 (**) החבורה S_3 פועלת על האוסף $\mathbb{C}[x_1, x_2, x_3]$ של פולינומים במשתנים x_1, x_2, x_3. מצא את המייצב של הפולינומים הבאים: x_1, $x_1 + x_2 + x_3$, $x_1x_2 + x_3$, $(x_1 - x_2)(x_2 - x_3)(x_3 - x_1)$. (עבור הפולינום האחרון, ראה תת־סעיף 5.1.1).

משפט 6.2.14 *האינדקס של המייצב של $x \in X$ שווה לגודל המסלול $G \cdot x$.*

הוכחה. נגדיר פונקציה $f : G \to X$ לפי $f(g) = g \cdot x$. אפשר לחשב ש־$f(g) = f(g')$ אם ורק אם $g \cdot x = g' \cdot x$ אם ורק אם $g^{-1}g' \in G_x$, אם ורק אם $gG_x = g'G_x$. לכן ההתאמה $gG_x \mapsto gx$ היא התאמה חד־חד־ערכית ועל בין קוסטים של G_x ואברים במסלול של x. □

קבוצה X שפועלת עליה חבורה G נקראת **מרחב־G**. אפשר ללמוד על החבורה מן המרחבים שלה, אבל עוד יותר מזה אפשר ללמוד מן הקשרים בין המרחבים האלה (שאפשר לקודד ב'קטגוריה של מרחבי־G').

הגדרה 6.2.15 *יהיו X, Y מרחבי־G. פונקציה $f : X \to Y$ היא **הומומורפיזם של מרחבי־G**, אם לכל $\sigma \in G$ ולכל $x \in X$ מתקיים $f(\sigma \cdot x) = \sigma \cdot f(x)$. כרגיל, הומומורפיזם הפיך הוא **איזומורפיזם**. אם יש בין X ל־Y איזומורפיזם של מרחבי־G, אומרים שהמרחבים איזומורפיים.*

$$\begin{tikzcd} G \times X \arrow[r] \arrow[d, "\mathrm{id}_G \times f"'] & X \arrow[d, "f"] \\ G \times Y \arrow[r] & Y \end{tikzcd}$$

תרגיל 6.2.16 (**) $G/G_x \cong G\cdot x$ כמרחבי־G. **הדרכה**. הפונקציה ממשפט 6.2.14 היא איזומורפיזם של מרחבי־G.

תרגיל 6.2.17 (+)** תהי G חבורה הפועלת על קבוצה X. הראה שאם $A \leq G$ תת־חבורה כך ש־$A \cdot x = G \cdot x$, אז $G = AG_x$. **הדרכה**. לכל $g \in G$ קיים $a \in A$ כך ש־$ax = gx$, ואז $a^{-1}g \in G_x$.

תרגיל 6.2.18 (*+) בכל פעולה של G, הגודל של כל מסלול מחלק את $|G|$.

תרגיל 6.2.19 (**) חבורה G פועלת על קבוצה X. לכל $g \in G$, נסמן ב־$X_g =$ $\{x \in X:\ g \cdot x = x\}$ את אוסף נקודות השבת של g. הראה ש־$X_{gg'g^{-1}} = g(X_{g'})$. הראה שאם $g \in \mathrm{Z}(G)$, אז אפשר לצמצם את הפעולה של G על X לפעולה על X_g.

תרגיל 6.2.20 (+)** בהמשך לתרגיל 6.2.19, נקבע $\sigma \in \mathrm{Z}(G)$ ומספר $d \geq 1$. הראה ש־G פועלת על קבוצת המסלולים בגודל d של $\langle\sigma\rangle$.

תרגיל 6.2.21 (*) נסמן ב־$f: \mathbb{C}^\times \to \mathrm{GL}_2(\mathbb{R})$ את ההומומורפיזם מתרגיל 2.7.6 וב־$\varphi: \mathbb{C} \to \mathbb{R}^2$ את האיזומורפיזם הקנוני של מרחבים וקטוריים מעל $\mathbb{R}$, $\varphi(a+bi) = \begin{pmatrix} a \\ b \end{pmatrix}$. יש פעולות טבעיות, של $\mathbb{C}^\times$ על $\mathbb{C}$ ושל $\mathrm{GL}_2(\mathbb{R})$ על $\mathbb{R}^2$. הראה ש־$\varphi(\alpha \cdot z) = f(\alpha) \cdot \varphi(z)$.

פעולת חבורה G על קבוצה X היא **פעולה חופשית** אם כל המייצבים הם טריוויאליים. כלומר, לכל נקודה x, אם $g \cdot x = x$ אז $g = 1$.

תרגיל 6.2.22 (+)** תהיינה F, G חבורות. נסמן ב־$\mathrm{Epi}(F,G)$ את כל האפימורפיזמים $\phi: F \to G$. לכל אפימורפיזם כזה, $G \cong F/\mathrm{Ker}(\phi)$. הראה ש־$\mathrm{Aut}(G)$ פועלת (חופשית) על $\mathrm{Epi}(F,G)$ על־ידי הרכבה משמאל, ושיש התאמה חד־חד־ערכית ועל בין המסלולים של הפעולה, לבין תת־החבורות הנורמליות $K \lhd F$ שעבורן $G \cong F/K$.

6.3 פעולת הכפל של חבורה על עצמה

תהי G חבורה. החבורה **פועלת על עצמה על־ידי כפל משמאל**, לפי $g \cdot x \mapsto gx$. החבורה **פועלת על עצמה על־ידי כפל מימין** על־ידי $g \cdot x \mapsto xg^{-1}$.

תרגיל 6.3.1 (**) בדוק שפעולות החבורה על עצמה על־ידי כפל משמאל ומימין הן אכן פעולות. (אבל פעולת הכפל משמאל $g \cdot x \mapsto xg$, ללא ההיפוך, אינה פעולה של G אלא אם G אבלית.)

6.3.1 משפט קיילי

בתת־סעיף זה נעזר בפעולה הטבעית של כל חבורה על עצמה, כדי להראות שכל חבורה סופית היא תת־חבורה של אחת החבורות הסימטריות.

תרגיל 6.3.2 (**) מצא הצגה של D_4 כחבורת תמורות (חשוב על פינות הריבוע).

משפט 6.3.3 (משפט קיילי) *כל חבורה G איזומורפית לתת־חבורה של החבורה הסימטרית S_G.*

תרגיל 6.3.4 (**) הוכח את המשפט. **הדרכה**. לפי תרגיל 6.1.12 מספיק למצוא פעולה נאמנה של G על עצמה; פעולה כזו היא פעולת הכפל משמאל, $g: x \mapsto gx$. ההומומורפיזם המתאים לה הוא $\Psi: G \to S_G$ לפי $\Psi(g): x \mapsto gx$. הראה ש־$\Psi(gh) = \Psi(g)\Psi(h)$ והסק ש־Ψ מוגדרת היטב *כלומר, בהקשר הנוכחי, היא מחזירה תמורות ולא סתם פונקציות* $G \to G$. פעולה זו של G על עצמה נקראת **הפעולה הרגולרית**.

זכור (תרגיל 2.6.4) שאם G חבורה סופית, מסדר n, אז $S_G \cong S_n$. כלומר, המשפט נותן שיכון $G \hookrightarrow S_n$, כאשר $n = |G|$. זהו שיכון בזבזני למדי, שהרי $|S_G| = n!$.

תרגיל 6.3.5 (*) הצג את החבורות $\mathbb{Z}_4$ ו־U_8 כתת־חבורות של S_4.

תרגיל 6.3.6 (**) הצג את U_9 כתת־חבורה של S_6.

תרגיל 6.3.7 (**) הצג את S_3 כתת־חבורה של S_6, כך שלאף איבר מלבד הזהות אין נקודות שבת.

תרגיל 6.3.8 (***) הצג את חבורת הקווטרניונים Q_8 (מהגדרה 3.6.30) כתת־חבורה של S_8, והראה שהיא אינה ניתנת לשיכון ב־S_7. **הדרכה.** כדי להגדיר שיכון $Q_8 \hookrightarrow S_8$ די לתאר את תמונות היוצרים i, j. לחלק השני, פתור את המשוואה $x^2 = y^2$ עבור $x, y \in S_7$ מסדר 4, והראה שלא יתכן ש־$yxy^{-1} = x^{-1}$. ראה פתרון אחר לחלק זה בתרגיל 8.3.19.

תרגיל 6.3.9 (*-)** 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 תרגיל 1.6.10 אינו חל במקרה הכללי.) **הדרכה.** העזר בשיכון של G לחבורת תמורות.

תרגיל 6.3.10 (***) מצא את כל החבורות G שעבורן התמונה של שיכון קיילי ב־S_G היא תת־חבורה נורמלית. **הדרכה.** התמונה נורמלית אם ורק אם $\forall\sigma\forall a\exists b : \sigma\ell_a = \ell_b\sigma$, כלומר $\forall\sigma\forall a\exists b\forall x : \sigma(ax) = b\sigma(x)$; הראה שזה שקול לכך ש־$\forall\sigma\forall a\forall x : \sigma(ax) = \sigma(a)\sigma(1)^{-1}\sigma(x)$ (ולכן $h_\sigma(x) = \sigma(1)^{-1}\sigma(x)$ היא הומומורפיזם). בחר $\sigma = (1t)$ כאשר $t \neq 1$; בחר $a \neq 1, t$, אז $G \subseteq \{1, t, a^{-1}, a^{-1}t\}$, ובפרט $|G| \leq 4$; עובדה זו נובעת כמובן גם ממשפט 5.4.9.

להצגה של חבורה נתונה כחבורת מטריצות יש שימושים תאורטיים מרחיקי לכת, הרבה מעבר למשפט קיילי. מעל שדה מתאים, כל הצגה אפשר לפרק באופן יחיד לסכום ישר של "הצגות אי־פריקות".

תרגיל 6.3.11 (**) לכל שדה F, כל חבורה סופית G היא תת־חבורה של $\mathrm{GL}_n(F)$ עבור n מתאים. **הדרכה.** לפי משפט קיילי די להראות ש־$S_n \subseteq \mathrm{GL}_n(F)$; התבונן במטריצות התמורה $p_\sigma = \sum e_{\sigma(i),i}$.

תרגיל 6.3.12 (*-)** מצא שיכון $S_n \hookrightarrow \mathrm{GL}_{n-1}(F)$. **הדרכה.** קח $V_0 = \mathrm{span}\{v_i - v_j\} \subset \mathrm{span}\{e_1, \ldots, e_n\}$, והגדר פעולה של S_n על V_0 לפי $\sigma(v_i - v_j) = v_{\sigma(i)} - v_{\sigma(j)}$. (ובמפורש: $\sigma \mapsto \sum_{j=1}^{n-1}(\sum_{i<\sigma(j+1)} e_{ij} - \sum_{i<\sigma(j)} e_{ij})$.)

6.3.2 העידון של משפט קיילי

נסמן ב־G/H את אוסף הקוסטים $\{xH : x \in G\}$ (אם H נורמלית, המכפלה של קוסטים היא קוסט; אבל הסימון תקף בכל מקרה).

תרגיל 6.3.13 (*+)** הראה ש־G פועלת על G/H לפי $g : (xH) \mapsto (gx)H$. זוהי **פעולת הכפל משמאל על מרחב הקוסטים**.

תרגיל 6.3.14 (*+)** אם H_1, H_2 תת־חבורות צמודות של G, אז המרחבים G/H_1 ו־G/H_2 איזומורפיים (כמרחבי־G, ראה הגדרה 6.2.15).

הגדרה 6.3.15 *חבורה של תמורות היא **מאוזנת** אם כל איבר שלה הוא מכפלה של מחזורים זרים שכולם מאותו אורך. (נקודות השבת נכללות בדיון: התמורה $(12)(34)(56)$ מאוזנת ב־S_6 **אבל לא** ב־S_8.)*

תרגיל 6.3.16 (**) תהי $H \leq S_n$ תת־חבורה. נניח שלאף איבר לא טריוויאלי ב־H אין נקודות שבת. הוכח ש־H מאוזנת.

תרגיל 6.3.17 (**) הראה שהתמונה של ההומומורפיזם $\Psi : G \to S_{S/H}$, המוגדר על־ידי הפעולה שבתרגיל 6.3.13, היא מאוזנת.

תרגיל 6.3.18 (**) עבור הפעולה שמשרה תרגיל 6.3.13 וההומומורפיזם $\Psi : G \to S_{G/H}$ המתאים לה, הראה שהמייצב של הקוסט xH הוא $x^{-1}Hx$ וש־$\mathrm{Ker}(\Psi) = \mathrm{Core}_G(H)$ (ראה תרגיל 3.3.22).

אם G חבורה גדולה, משפט קיילי המספק שיכון שלה ל־$S_{|G|}$ אינו נוח ואינו יעיל. מידע נוסף על החבורה יכול לשפר את ההצגה בצורה דרמטית.

משפט 6.3.19 (העידון של משפט קיילי) *תהי G חבורה ותהי H תת־חבורה מאינדקס $n = [G:H]$. אז יש שיכון $G/\mathrm{Core}_G(H) \hookrightarrow S_n$.*

תרגיל 6.3.20 (**) הוכח את המשפט. **הדרכה**. תרגילים 6.3.13, 6.3.18.

תרגיל 6.3.21 (**) המייצב של הנקודה $H \in G/H$ בפעולת G על המרחב G/H הוא H עצמה.

תרגיל 6.3.22 (*-)** אם יש ל־G תת־חבורה H מאינדקס n, אז יש לה תת־חבורה נורמלית מאינדקס המחלק את $n!$ (המוכלת ב־H).

כזכור חבורה שאין לה תת־חבורות נורמליות נקראת **פשוטה** (הגדרה 4.1.4).

תרגיל 6.3.23 (**) כל חבורה פשוטה עם תת־חבורה מאינדקס n היא תת־חבורה של S_n (ראו תרגיל 6.3.24.)

תרגיל 6.3.24 (**) תהי G תת־חבורה פשוטה של S_n. אם $|G| > 2$ אז $G \subseteq A_n$. **הדרכה**. תרגיל 5.1.17; השווה לתרגיל 6.3.23.

תרגיל 6.3.25 (**) אם לחבורה פשוטה $G \neq \mathbb{Z}_2$ יש תת־חבורה מאינדקס n, אז $G \hookrightarrow A_n$ ובפרט $|G|$ מחלק את $\frac{1}{2}n!$. **הדרכה**. תרגיל 6.3.24.

תרגיל 6.3.26 (**) נניח $5 \leq n$.

1. ל־A_n אין תת־חבורות מאינדקס קטן מ־n.
2. תת־החבורה היחידה של S_n שהאינדקס שלה קטן מ־n היא A_n.

תרגיל 6.3.27 (+)** הראה שאין שיכון של S_n ב־A_{n+1} ($n \geq 2$; השווה לתרגיל 5.1.18.)

תרגיל 6.3.28 (*-)** תהי $H \leq G$ תת־חבורה מאינדקס p, כאשר p הראשוני הקטן ביותר המחלק את $|G|$. הוכח ש־$H \triangleleft G$. **הערה**. זוהי הכללה של תרגיל 3.3.13.

תרגיל 6.3.29 (*-)** G חבורה סופית פשוטה עם תת־חבורה H. הוכח ש־$\log|G| \leq [G:H]^2$. מצא את החסם על $[G:H]$ אם $|G| = 2^{30}$.

תרגיל 6.3.30 (*-)** לחבורה נוצרת סופית (הגדרה 1.4.23) יש מספר סופי של תת־חבורות מאינדקס n. **הדרכה**. תת־חבורה $H \leq G$ מאינדקס n משרה פעולה של G על קבוצת הקוסטים של H, וניתנת לשחזור מן הפעולה כמייצב של עצמה. לכן מספר החבורות אינו עולה על מספר ההומומורפיזמים $G \to S_n$.

6.4 פעולת ההצמדה

בסעיף הקודם עסקנו בפעולה של חבורה G על עצמה ועל הקוסטים של תת־חבורה לפי כפל. בסעיף זה נבחן פעולה חדשה: הצמדה.

הגדרה 6.4.1 *הפעולה של חבורה G על עצמה לפי $g: x \mapsto gxg^{-1}$ נקראת הצמדה. נגדיר $\gamma_g: G \to G$ לפי $\gamma_g(x) = gxg^{-1}$; פעולת ההצמדה מתאימה איבר g לפעולה γ_g.*

תרגיל 6.4.2 (**) קבע מתי $g: x \mapsto g^{-1}xg$ מגדיר פעולה של G על עצמה.

6.4.1 מחלקות צמידות

הגדרה 6.4.3 *שני אברים $x, y \in G$ הם צמודים אם קיים $g \in G$ כך ש־$y = gxg^{-1}$. לפעמים מסמנים $x \approx y$.*

תרגיל 6.4.4 (*) הראה שיחס הצמידות הוא יחס שקילות. **הדרכה.** אברים הם צמודים אם ורק אם הם שייכים לאותו מסלול של פעולת ההצמדה; אפשר גם להוכיח ישירות.

תרגיל 6.4.5 (*) $x \in \mathrm{Z}(G)$ אם ורק אם מחלקת הצמידות של x היא היחידון $[x] = \{x\}$.

תרגיל 6.4.6 (*) תת־חבורה היא נורמלית אם ורק אם היא מהווה איחוד של מחלקות צמידות (אבל איחוד של מחלקות צמידות הוא תת־חבורה נורמלית רק אם הוא סגור לכפל).

תרגיל 6.4.7 (*) חשב את מחלקת הצמידות של $(g,h) \in G \times H$.

תרגיל 6.4.8 (***) הוכח שבחבורה $\mathrm{GL}_2(\mathbb{Z})$, כל איבר מסדר 2 צמוד לאחת מן המטריצות $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$, $\begin{pmatrix} 1 & 1 \\ 0 & -1 \end{pmatrix}$ ו־$\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$.

תרגיל 6.4.9 (**) מחלקות הצמידות בחבורה הדיהדרלית D_n הן:

- אם n זוגי, $n/2+3$ המחלקות

$$\{1\}, \{\sigma, \sigma^{-1}\}, \dots, \left\{s^{n/2-1}, \sigma^{n/2+1}\right\}, \left\{\sigma^{n/2}\right\}, \{\tau, \sigma^2\tau, \sigma^4\tau, \dots, \sigma^{n-2}\tau\}, \{\sigma\tau, \sigma^3\tau, \sigma^5\tau, \dots, \sigma^{n-1}\tau\}.$$

- ואם n איזוגי, $(n+3)/2$ המחלקות

$$\{1\}, \{\sigma, \sigma^{-1}\}, \{\sigma^2, \sigma^{-2}\}, \dots, \left\{\sigma^{(n-1)/2}, \sigma^{(n+1)/2}\right\}, \{\tau, \sigma\tau, \sigma^2\tau, \dots, \sigma^{n-1}\tau\}.$$

6.4.2 מרכְּזים

הגדרה 6.4.10 *תהי G חבורה, ויהי $a \in G$. המרכֵּז של a הוא קבוצת האברים*

$$\mathrm{C}_G(a) = \left\{x \in G \colon\ xax^{-1} = a\right\}.$$

המרכֵּז הוא המייצב של a בפעולת ההצמדה של G על עצמה.

תרגיל 6.4.11 (*) המרכז של איבר הוא תת־חבורה של G.

תרגיל 6.4.12 (*) $\mathrm{C}_G(gag^{-1}) = g\mathrm{C}_G(a)g^{-1}$.

תרגיל 6.4.13 (**) אם $\varphi\colon G \to H$ איזומורפיזם, אז $C_H(\varphi(x)) = \varphi(\mathrm{C}_G(x))$.

תרגיל 6.4.14 (+*) מספר האברים במחלקת הצמידות של $a \in G$ שווה לאינדקס $[G : \mathrm{C}_G(a)]$. בפרט, מספר האברים במחלקת הצמידות מחלק את סדר החבורה.

תרגיל 6.4.15 (*) מחלקת הצמידות של איבר a בחבורה היא בגודל 2. הוכח: יש לחבורה תת־חבורה נורמלית לא טריוויאלית.

תרגיל 6.4.16 (***) תהי G חבורה סופית. מגרילים $g, g' \in G$ באקראי לפי התפלגות אחידה.

1. חשב את תוחלת מספר הפתרונות למשוואה $xgx^{-1} = g'$.
2. חשב את תוחלת מספר הפתרונות למשוואה $xgx^{-1} = g'gg'^{-1}$.

תרגיל 6.4.17 (*) רשום את אברי המרכז של (123) ב-S_3.

תרגיל 6.4.18 (**) רשום את אברי המרכז של $(12)(34)$ ב-S_4.

תרגיל 6.4.19 (**) מצא את המרכז של $(12)(34)$ בחבורה S_5. כמה אברים יש במחלקה $[(12)(34)]$?

תרגיל 6.4.20 (**) מצא את $\mathrm{C}_{S_n}(\sigma)$ כאשר $\sigma = (123\dots n)$. **הדרכה.** חשב את $|[\sigma]|$.

תרגיל 6.4.21 (*) מה גודלה של מחלקת הצמידות של $(123)(45)$ ב-A_5?

תרגיל 6.4.22 (**) רשום את אברי המרכז של (123) ב-A_4.

תרגיל 6.4.23 (***) החבורה $G = \mathrm{SL}_2(\mathbb{Z}_3)$ של מטריצות 2×2 מעל $\mathbb{Z}_3$ מדטרמיננטה 1, היא מסדר 24.

1. מצא איבר לא טריוויאלי במרכז של G.
2. חשב את המרכז $\mathrm{C}_G(\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix})$, וזהה את החבורה עד כדי איזומורפיזם.
3. הסק - כמה מטריצות צמודות ל-$\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$ בחבורה הזו?

תרגיל 6.4.24 (***) נניח ש-$G = \bigcup G_n$, כאשר $G_1 \subseteq G_2 \subseteq G_3 \subseteq \cdots$. תהי $H \leq G$. הוכח ש-$\mathrm{C}_G(H) = \bigcup_m \bigcap_{n \geq m} \mathrm{C}_{G_n}(H \cap G_n)$. (הסק את תרגיל 4.7.9 כמקרה פרטי).

תרגיל 6.4.25 (**) תהי G חבורה (אינסופית). נסמן ב-$\Delta(G)$ את קבוצת האברים שמחלקת הצמידות שלהם סופית. הראה ש-$\Delta(G)$ היא תת־חבורה נורמלית של G.

תרגיל 6.4.26 (*-)** בהמשך לתרגיל 6.4.25, נסמן ב-$\Delta^+(G)$ את קבוצת האברים מסדר סופי ב-$\Delta(G)$. הוכח ש-$\Delta(G)/\Delta^+(G)$ היא חבורה אבלית חסרת פיתול (למושג האחרון, ראה הגדרה 9.5.2).

תרגיל 6.4.27 (*-)** לכל תת־חבורה נוצרת סופית $H \subseteq \Delta(G)$, $[H, H]$ היא חבורה מפותלת (ראו הגדרה 9.5.2).

תרגיל 6.4.28 (*+)** $\Delta(G)$ אבלית חסרת פיתול אם ורק אם אין ל-G תת־חבורות נורמליות סופיות.

6.4.3 מחלקות צמידות בתת־חבורה

ניתן לדלג בקריאה ראשונה.

בסעיף זה נלמד מה קורה למחלקות צמידות כאשר יורדים לתת־חבורה. תהי G חבורה עם תת־חבורה נורמלית N, ותהי Γ מחלקת צמידות של G, המוכלת ב־N. (דוגמה חשובה במיוחד: $G = S_n$ ו־$N = A_n$).

תרגיל 6.4.29 (*) Γ היא איחוד של מחלקות צמידות ב־N (כלומר: אם g_1, g_2 צמודים ב־N, הם צמודים ב־G).

תרגיל 6.4.30 (*+)** אם $\Gamma = \Gamma_1 \cup \cdots \cup \Gamma_s$ כאשר Γ_i מחלקות של N, אז Γ_i שווי־גודל ו־$|\Gamma| = s \cdot \Gamma_1$ עבור s מתאים.

תרגיל 6.4.31 (**) הראה ש־$(123), (124)$ צמודים ב־S_4 אבל אינם צמודים ב־A_4.

תרגיל 6.4.32 (**) הראה ש־$A = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ ו־$-A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ צמודות ב־$\mathrm{GL}_2(\mathbb{R})$ אבל אינן צמודות ב־$\mathrm{SL}_2(\mathbb{R})$. הראה שכל מטריצה הצמודה ל־A ב־$\mathrm{GL}_2(\mathbb{R})$ צמודה לאחת המטריצות $A, -A$ ב־$\mathrm{SL}_2(\mathbb{R})$.

כדי לבדוק האם מחלקה Γ היא מחלקת צמידות של N, נשווה את המרכְּזים. נבחר $g \in \Gamma$.

תרגיל 6.4.33 (*) $\mathrm{C}_N(g) = N \cap \mathrm{C}_G(g)$.

תרגיל 6.4.34 (**) Γ מתפצלת ל־$\frac{[G:N]}{[\mathrm{C}_G(g):\mathrm{C}_N(g)]}$ מחלקות צמידות של N. בפרט:

1. Γ מחלקת צמידות של N אם ורק אם $[G:N] = [\mathrm{C}_G(g):\mathrm{C}_N(g)]$.
2. Γ מתפצל ל־$[G:N]$ מחלקות לכל היותר. Γ מתפצל ל־$[G:N]$ מחלקות אם ורק אם $C_G(g) \subseteq N$.

תרגיל 6.4.35 (**) נסח את תוצאות התרגיל האחרון במקרה $[G:N] = 2$.

תרגיל 6.4.36 (**) מצא את מחלקות הצמידות ב־A_4.

תרגיל 6.4.37 (**) האם כל שני אברים מסדר 7 ב־A_7 הם צמודים? מה בדבר כל שני אברים מסדר 2? כל שני אברים מסדר 3?

תרגיל 6.4.38 (*-)** מצא את מחלקת הצמידות היחידה של S_6 המוכלת ב־A_6 ומתפצלת שם לשתי מחלקות.

6.4.4 מרכְּזים של תת־חבורות.

הגדרה 6.4.39 *תהי $H \leq G$ תת־חבורה. **המרכְּז** של H הוא קבוצה האברים*

$$\mathrm{C}_G(H) = \left\{x \in G \colon \forall a \in H : xax^{-1} = a\right\}.$$

זוהי הכללה של המרכֵּז של איבר (הגדרה 6.4.10) משום ש־$\mathrm{C}_G(\langle g \rangle) = \mathrm{C}_G(g)$.

תרגיל 6.4.40 (*) $\mathrm{C}_G(H)$ תת־חבורה של G.

תרגיל 6.4.41 **(*)** $H \subseteq \mathrm{C}_G(H)$ אם ורק אם H אבלית.

תרגיל 6.4.42 **(*)** אם H אבלית, אז $S = \mathrm{C}_G(H)$ היא תת־החבורה המקסימלית כך ש־$H \subseteq$ $\mathrm{Z}(S)$.

תרגיל 6.4.43 **(*)** $\mathrm{Z}(H) = H \cap \mathrm{C}_G(H)$.

תרגיל 6.4.44 **(*)** $\mathrm{Z}(G) = \mathrm{C}_G(G)$.

תרגיל 6.4.45 **(+*)** $\mathrm{C}_G(xHx^{-1}) = x\mathrm{C}_G(H)x^{-1}$. לכן, אם $H \lhd G$ אז $\mathrm{C}_G(H) \lhd G$.

תרגיל 6.4.46 **(*)** אם $A \subseteq B$ אז $\mathrm{C}_G(B) \subseteq \mathrm{C}_G(A)$.

תרגיל 6.4.47 **(**)** $A, B \leq G$ תת־חבורות. הראה ש־$\mathrm{C}_G(AB) = \mathrm{C}_G(A) \cap \mathrm{C}_G(B)$.

תרגיל 6.4.48 **(**)** לכל תת־חבורה H, $H \subseteq \mathrm{C}_G(\mathrm{C}_G(H))$.

תרגיל 6.4.49 **(-***)** יהי $\Psi : \mathcal{L} \to \mathcal{L}$ אופרטור מקבוצה סדורה לעצמה, המקיים את שני התנאים

1. אם $A \leq B$ אז $\Psi(A) \geq \Psi(B)$,
2. לכל $A \in \mathcal{L}$, $A \leq \Psi^2(A)$;

אז $\Psi^3 = \Psi$, כלומר, $\Psi(\Psi(\Psi(A))) = \Psi(A)$ לכל A.

תרגיל 6.4.50 **(-***)** לכל תת־חבורה $H \leq G$ מתקיים $\mathrm{C}_G(\mathrm{C}_G(\mathrm{C}_G(H))) = \mathrm{C}_G(H)$ הדרכה. תרגיל 6.4.49.

תרגיל 6.4.51 **(+**)** תהיינה $H \leq G$ חבורות, אז $\mathrm{Z}(H) \cdot \mathrm{Z}(G) = H \cdot \mathrm{Z}(G) \cap \mathrm{C}_G(H)$.

תרגיל 6.4.52 **(***)** תהי G חבורה שבה $\mathrm{C}_G(x) = \langle x \rangle$ לכל $x \neq 1$. הוכח שלכל איבר ב־G יש סדר ראשוני. תן דוגמה לחבורה כזו שאינה מסדר p^n.

תרגיל 6.4.53 **(*)** חשב את $\mathrm{C}_{G\times H}(G \times 1)$ ואת $\mathrm{Z}(G \times H)$.

6.4.5 מנרמלים

יהי $\mathcal{S}$ אוסף כל תת־החבורות של G.

תרגיל 6.4.54 **(**)** הנוסחה $g : H \mapsto gHg^{-1}$ מגדירה פעולה של G על האוסף $\mathcal{S}$.

הגדרה 6.4.55 *תהי $H \leq G$ תת־חבורה. **המנרמל** של H ב־G הוא הקבוצה*

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

כלומר, כמקודם, זהו המייצב של H בפעולת ההצמדה על $\mathcal{S}$.

תרגיל 6.4.56 **(**)** הראה שהקבוצה $\left\{x \in G :\ xHx^{-1} \subseteq H\right\}$ אינה בהכרח תת־חבורה. הדרכה. קח $G = \begin{pmatrix} \mathbb{Q}^\times & \mathbb{Q} \\ 0 & 1 \end{pmatrix}$ ו־$H = \begin{pmatrix} 1 & \mathbb{Z} \\ 0 & 1 \end{pmatrix}$.

תרגיל 6.4.57 **(*)** המנרמל $\mathrm{N}_G(H)$ הוא תת־חבורה של G, המכילה את המרכז $\mathrm{C}_G(H)$.

תרגיל 6.4.58 (*) $H\lhd \mathrm{N}_G(H)$, ולמעשה $\mathrm{N}_G(H)$ היא תת־החבורה הגדולה ביותר של G שבה H נורמלית: לכל $H \le K \le G$, $H\lhd K$, אז ורק אם $K \subseteq \mathrm{N}_G(H)$.

תרגיל 6.4.59 (*) $\mathrm{N}_G(H) = G$ אם ורק אם $H\lhd G$.

תרגיל 6.4.60 (*) $\mathrm{N}_G(xHx^{-1}) = x\mathrm{N}_G(H)x^{-1}$.

תרגיל 6.4.61 (*) $H \cdot \mathrm{C}_G(H)$ היא תת־חבורה נורמלית של $\mathrm{N}_G(H)$.

תרגיל 6.4.62 (*) אם $H \subseteq K \subseteq G$, אז $\mathrm{N}_K(H) = \mathrm{N}_G(H) \cap K$.

תרגיל 6.4.63 (**) נניח ש־$K \subseteq H \le G$, $K\lhd G$. אז $\mathrm{N}_{G/K}(H/K) = \mathrm{N}_G(H)/K$.

הגדרה 6.4.64 ***שתי תת־חבורות H, H' של G הן צמודות אם קיים $g \in G$ כך ש־$H' = gHg^{-1}$.***

תרגיל 6.4.65 (*) אם H_1, H_2 צמודות, אז הן איזומורפיות. תן דוגמא המראה שההיפך אינו נכון.

תרגיל 6.4.66 (***) מספר תת־החבורות הצמודות ל־H שווה ל־$[G{:}\mathrm{N}_G(H)]$.

תרגיל 6.4.67 (**) נניח ש־X, Y הם מרחבי־G איזומורפיים (הגדרה 6.2.15). הראה שלתמורה המתאימה לאיבר $g \in G$ בפעולה שלו על X יש אותו מבנה מחזורים כמו בפעולה שלו על Y.

תרגיל 6.4.68 (***) תהי $H \le G$ תת־חבורה. הראה שקבוצת הקוסטים של המנרמל $G/\mathrm{N}_G(H)$, עם פעולת הכפל של G משמאל, איזומורפית (כמרחב־G) לקבוצת תת־החבורות הצמודות ל־H, שהוגדרה בתרגיל 6.3.13. בפרט, הראה שמספר נקודות השבת בפעולה של $g \in G$ שווה למספר הצמודים של $\mathrm{N}_G(H)$ שאליהם g שייך.

תרגיל 6.4.69 (***) תהי $H \le G$ תת־חבורה. הפעולה של G על תת־החבורות הצמודות ל־H, על־ידי הצמדה, משרה פעולת הצמדה של כל תת־חבורה $K \le G$. הראה שאם יש בפעולה של K נקודת שבת משותפת, אז $\mathrm{N}_G(H)$ מכיל תת־חבורה הצמודה ל־K.

תרגיל 6.4.70 (***) תהי $G = \mathrm{GL}_n(F)$, ו־$T = T_n(F)$, כפי שהוגדרו בתרגיל 3.5.20. מצא את המנרמל $\mathrm{N}_G(T)$ והוכח ש־$\mathrm{N}_G(T)/T \cong S_n$.

תרגיל 6.4.71 (**) תהי G חבורה סופית עם תת־חבורה אמיתית H. הוכח שיש ב־G איברים שאף צמוד שלהם אינו שייך ל־H. **הדרכה.** הראה ש־$|\bigcup_{x\in G} xHx^{-1}| < \frac{|G|}{[\mathrm{N}_G(H):H]}$.

תרגיל 6.4.72 (***) תהי G חבורה פשוטה סופית, שאינה ציקלית.

1. נניח שכל תת־חבורה אמיתית של G היא אבלית.

(א) החיתוך של שתי תת־חבורות מקסימליות הוא טריוויאלי. **הדרכה.** תהיינה H_1, H_2 תת־חבורות מקסימליות, ונסמן $K = H_1 \cap H_2$. מכיוון ש־$K\lhd H_i$, $\mathrm{N}_G(K) \supseteq H_1, H_2$ ולכן $\mathrm{N}_G(K) = G$ ו־$K\lhd G$, אבל G פשוטה.

(ב) תהי H תת־חבורה מקסימלית. נסמן $V(H) = \bigcup_x xHx^{-1} - \{1\}$. אז $|V(H)| \ge \frac{1}{2}|G|$. **הדרכה.** $|V(H)| = |G| - [G{:}H]$ לפי סעיף (א).

(ג) תהי H תת־חבורה מקסימלית. אז יש תת־חבורה מקסימלית שאינה צמודה ל־H. **הדרכה.** לפי תרגיל 6.4.71 יש איבר של G שאינו באף צמוד של H.

(ד) תהיינה H_1, H_2 תת־חבורות מקסימליות שאינן צמודות, אז $|G| \le |V(H_1) \cup V(H_2)|$, וזו סתירה לכך ש־$1 \notin V(H_i)$.

2. יש ל־G תת־חבורה לא אבלית.

6.5 הלמה של ברנסייד

דוגמא 6.5.1 בונים ריבועים ממוטות עץ בשלושה צבעים. שני ריבועים שאפשר לקבל אחד מהם מן השני על־ידי סיבוב או שיקוף הם שקולים. כמה ריבועים לא שקולים אפשר לבנות?

בשאלה זו יש חבורה (D_4) הפועלת על אוסף הריבועים הבנויים, כלומר 3^4 הרביעיות הסדורות של מוטות משלושה צבעים. הלמה של ברנסייד מאפשרת לספור כמה מסלולים יש בפעולה הזו.

הגדרה 6.5.2 *תהי G חבורה הפועלת על X. לכל $\sigma \in G$, נסמן ב־$\mathrm{fp}(\sigma) = |\{x \colon \sigma(x) = x\}|$ את מספר נקודות השבת של σ (**f**ixed **p**oints).*

משפט 6.5.3 (הלמה של ברנסייד) *מספר המסלולים בפעולה של חבורה G על קבוצה X שווה לערך הממוצע של מספר נקודות השבת:*

$$|X/G| = \frac{1}{|G|} \sum_{\sigma \in G} \mathrm{fp}(\sigma).$$

הוכחה. מצד אחד, $\sum_{\sigma \in G} \mathrm{fp}(\sigma) = \sum_{\sigma \in G} \sum_{x \in X} \delta_{x,\sigma(x)}$. מצד שני אותו סכום שווה ל־$\sum_{x \in X} \sum_{\sigma \in G} \delta_{x,\sigma(x)} = \sum_{x \in X} |G_x| = \sum_{x \in X} \frac{|G|}{|[x]|} = |G| \cdot \sum_O \sum_{x \in O} \frac{1}{|O|} = |G| \cdot \sum_O 1$, כאשר הסכום $\sum_O$ מחושב על־פני המסלולים $O \subseteq X$. $\square$

תרגיל 6.5.4 (+)** תהי G חבורה הפועלת על קבוצה X. אם $\sigma, \sigma' \in G$ צמודות אז $|\mathrm{fp}(\sigma')| = |\mathrm{fp}(\sigma)|$. לכן

$$|X/G| = \frac{1}{|G|} \sum_{C \subseteq G} |C| \cdot \mathrm{fp}(C)$$

כאשר $\mathrm{fp}(C)$ הוא מספר נקודות השבת של איבר כלשהו ממחלקת הצמידות C.

תרגיל 6.5.5 (*) חשב באמצעות הלמה של ברנסייד את מספר נקודות השבת הממוצע של תמורות מ־S_n.

תרגיל 6.5.6 (-*)** תהי G חבורה סופית. הראה שההסתברות לכך ששני אברים מקריים יתחלפו, שווה למספר מחלקות הצמידות חלקי סדר החבורה. **הדרכה.** ההסתברות היא $\frac{1}{|G|^2} \sum_{g \in G} |\mathrm{C}_G(g)|$; יישם את הלמה של ברנסייד לפעולת ההצמדה של החבורה על עצמה.

תרגיל 6.5.7 (+)** יהי p מספר ראשוני. החבורה הדיהדרלית D_p פועלת על מצולע משוכלל בן p צלעות. כמה משולשים יש במצולע, עד כדי שקילות?

מתי שתי צביעות של קודקודי ריבוע נחשבות שקולות זו לזו?

הלמה של ברנסייד מאפשרת לספור את הדרכים השונות לצבוע קבוצה X, באופן הבא. תהי B קבוצת הצבעים. **צביעה** של X היא פונקציה $f \colon X \to B$. נניח שחבורה G פועלת על X; החבורה פועלת גם על קבוצת הצביעות B^X לפי הנוסחה $(\sigma(f))(x) = f(\sigma(x))$.

תרגיל 6.5.8 (**) מספר נקודות השבת של $\sigma \in G$ בפעולה על B^X שווה ל־$|B|^{\mathrm{c}(\sigma)}$ כאשר $\mathrm{c}(\sigma)$ הוא מספר המחזורים של σ כאיבר של S_X. לכן מספר הצביעות השונות הוא $\frac{1}{|G|} \sum_{\sigma \in G} |B|^{\mathrm{c}(\sigma)}$.

תרגיל 6.5.9 (**) בכמה דרכים שונות עקרונית אפשר לצבוע קודקודים של ריבוע, אם אפשר להשתמש בששה צבעים? (שתי צביעות הן שקולות אם אפשר לסובב ולשקף את הריבוע הצבוע באחת מהן אל השניה.)

תרגיל 6.5.10 (***) במאגר יש מספר גדול של כדורים בכל אחד מעשרה צבעים. השתמש בלמה של ברנסייד כדי לספור כמה אפשרויות יש לבחור קבוצה בת ארבעה כדורים.

תרגיל 6.5.11 (+*)** בכמה דרכים שונות אפשר לצבוע את הקודקודים של פירמידה משוכללת, כשמשתמשים בחמישה צבעים? (כתבו מהי החבורה הפועלת על מרחב הצביעות).

תרגיל 6.5.12 (+*)** כמה מחרוזות באורך n אפשר ליצור מחרוזים בשני צבעים? **הדרכה.** בפעולה של σ^i יש $2^{(n,i)}$ נקודות שבת.

תרגיל 6.5.13 (**) חבורה G פועלת על־ידי כפל משמאל על זוגות לא סדורים של אברים של עצמה. כמה מסלולים יש? **הדרכה.** נסמן ב־n את גודל החבורה. נסמן ב־d_2 את מספר האברים מסדר 2 בחבורה; לכל איבר מסדר 2 יש $\frac{n}{2}$ נקודות שבת, ולאיברים שאינם מקיימים $g^2=1$ אין נקודות שבת. לכן מספר המסלולים הוא $\frac{1}{2}(n-1+d_2)$. ספור את המסלולים ישירות תוך שימוש בעובדה שכל זוג שקול לזוג מהצורה $\{1,g\}$ (השווה לתרגיל 2.1.13).

תרגיל 6.5.14 (***) הראה שלכל n,k, $\binom{n+k-1}{n} = \frac{1}{n!}\sum_{\sigma\in S_n} k^{\ell(\sigma)}$, כאשר $\ell(\sigma)$ הוא מספר המחזורים בתמורה σ. **הדרכה.** זהו מספר הדרכים לצבוע n חרוזים ב־k צבעים, כאשר סדר החרוזים אינו משנה. כאן S_n פועלת על מרחב הצביעות k^n.

תרגיל 6.5.15 (**) ריבוע סודוקו מסדר 2 הוא ריבוע של 4×4 משבצות, שבכל שורה ובכל עמודה שלו כתובים המספרים $1,2,3,4$, וכך שבכל רבע של הריבוע מופיעים כל ארבעת המספרים. הגדר שלוש פעולות שונות של D_4 על האוסף Σ של כל ריבועי סודוקו מסדר 2. הגדר פעולה טבעית של S_4. כמה ריבועי סודוקו מסדר 2 יש, עד כדי הפעולה המשותפת של כל החבורות האלה?

6.6 טרנזיטיביות

הגדרה 6.6.1 ***הפעולה של G על X היא פעולה טרנזיטיבית אם לכל $x,y\in X$ קיים $g\in G$ כך ש־$y=g(x)$. כלומר, X היא מסלול יחיד תחת הפעולה.***

תרגיל 6.6.2 (*) בהמשך לתרגיל 6.3.13, הפעולה של G על מרחב הקוסטים G/H (כאשר $H\leq G$ תת־חבורה) היא טרנזיטיבית.

תרגיל 6.6.3 (**) לחבורה יש פעולה טרנזיטיבית על קבוצה בגודל n אם ורק אם יש לה תת־חבורה מאינדקס n.

תרגיל 6.6.4 (**) כל קבוצה X שעליה פועלת החבורה G באופן טרנזיטיבי, איזומורפית כמרחב־G (הגדרה 6.2.15) למרחב קוסטים G/H. **הדרכה.** קח $H=G_x$, כאשר $x\in X$. הראה ש־$gG_x\mapsto g(x)$ מגדיר איזומורפיזם $G/G_x \to X$.

תרגיל 6.6.5 (**) אם G פועלת טרנזיטיבית אז כל המייצבים G_x צמודים זה לזה. (**הדרכה.** תרגיל 6.2.11) הסק ש־$\mathrm{Core}_G(G_x)=1$, ולכן המייצב של נקודה אינו מכיל אף תת־חבורה נורמלית של G.

תרגיל 6.6.6 (**) החבורה $\mathrm{GL}_n(F)$ פועלת על המרחב $V=F^n$ בדרך הרגילה, $A\colon x\mapsto Ax$. כמה מסלולים יש בפעולה הזו? (ראה תרגיל 6.7.8.)

תרגיל 6.6.7 (**) אם G פועלת על X ויש נקודה $x\in X$ כך ש־$|X|=[G\colon G_x]$ אז הפעולה טרנזיטיבית.

6.6.1 טרנזיטיביות מרובה

הגדרה 6.6.8 *פעולה על מרחב X שיש בו לפחות k נקודות נקראת k-**טרנזיטיבית** אם לכל $x_1, \dots, x_k$ שונים, ולכל $y_1, \dots, y_k$ שונים, קיים $g \in G$ כך ש-$g(x_i) = y_i$. (פעולה 1-טרנזיטיבית נקראת, כפי שהוגדר לעיל, סתם "טרנזיטיבית".)*

תרגיל 6.6.9 (*) כל פעולה k-טרנזיטיבית היא בפרט $(k-1)$-טרנזיטיבית.

תרגיל 6.6.10 (*) אם G פועלת k-טרנזיטיבית על X, אז G_x פועלת $(k-1)$-טרנזיטיבית על הקבוצה $X - \{x\}$.

תרגיל 6.6.11 (*-)** נניח ש-G פועלת טרנזיטיבית. אם G_x פועלת $(k-1)$-טרנזיטיבית על הקבוצה $X - \{x\}$, אז G היא k-טרנזיטיבית.

הגדרה 6.6.12 *תהי X קבוצה. נסמן ב-$X^{[d]}$ את קבוצת הוקטורים $(x_1, \dots, x_d) \in X^d$ שכל רכיביהם שונים זה מזה; וב-$\binom{X}{d}$ את קבוצת תת-הקבוצות בנות d אברים של X. נסמן גם $n(n-1)\cdots(n-d+1) = \frac{n!}{(n-d)!} = n^{[d]}$.*

תרגיל 6.6.13 (*) הראה ש- $\left||X|^{[d]}\right| = |X|^{[d]}$ וש-$\left|\binom{X}{d}\right| = \binom{|X|}{d}$.

תרגיל 6.6.14 (**) אם G פועלת k-טרנזיטיבית על קבוצה בגודל n, אז $|G|$ מתחלק ב-$n^{[k]}$.

תרגיל 6.6.15 (**) תהי G חבורה הפועלת על קבוצה X, ויהי $d \in \mathbb{N}$ כלשהו. הגדר פעולה של G על הקבוצות $X^{[d]}$ ו-$\binom{X}{d}$.

תרגיל 6.6.16 (**) החבורה הדיהדרלית D_n פועלת באופן טבעי על קודקודי המצולע בן n צלעות. כתוב את המסלולים של פעולת D_8 על הזוגות של קודקודי המתומן; על האלכסונים; על שלשות לא סדורות של קודקודים.

תרגיל 6.6.17 (**) G פועלת d-טרנזיטיבית על X אם ורק אם היא פועלת טרנזיטיבית על $X^{[d]}$ (הגדרה 6.6.12).

תרגיל 6.6.18 (***) יהיו n, k מספרים זרים. הוכח ש-$n \mid \binom{n}{k}$. **הדרכה**. תהי G חבורה כלשהי מסדר n. התבונן בפעולה של G על $X = \binom{G}{k}$ על-ידי כפל משמאל. הראה שהמייצב של כל $A \in X$ הוא טריוויאלי. לכן X מתפרק לאיחוד זר של מסלולים שגודל כל אחד ואחד מהם הוא n. הסק מכאן שגם $k \mid \binom{n-1}{k-1}$.

תרגיל 6.6.19 (*) הפעולה של A_n על $\{1, \dots, n\}$ היא $(n-2)$-טרנזיטיבית.

תרגיל 6.6.20 (**) כל תת-חבורה של S_n הפועלת n-טרנזיטיבית על $X = \{1, \dots, n\}$, שווה ל-S_n. כל תת-חבורה שהיא $(n-2)$-טרנזיטיבית מכילה את A_n (שהיא תת-החבורה היחידה של S_n מאינדקס 2, ראו הגדרה 5.1.12).

תרגיל 6.6.21 (***) תהי G חבורה. נתבונן בפעולה של $\mathrm{Aut}(G)$ (להגדרה ראה סעיף 7.1) על $G^{\#} = G - \{1\}$.

1. אם הפעולה טרנזיטיבית אז כל האברים ב-G מאותו סדר, שהוא ראשוני p.
2. אם הפעולה 2-טרנזיטיבית אז $G = \mathbb{Z}_3$ או ש-$p = 2$ (ו-G אבלית לפי תרגיל 2.1.10).
3. אם הפעולה 3-טרנזיטיבית אז $G = \mathbb{Z}_2 \times \mathbb{Z}_2$.
4. הפעולה אינה יכולה להיות 4-טרנזיטיבית.

הדרכה. פעולת החבורה שומרת על סדר של אברים. אם הפעולה 2־טרנזיטיבית ו־$g \neq g^{-1}$ אז יש אוטומורפיזם המעביר $g \mapsto g$ ו־$g^{-1} \mapsto h \neq g, g^{-1}$, אלא אם $G = \{1, g, g^{-1}\}$. נניח שהפעולה 3־טרנזיטיבית וניקח $a \neq b$ ב־G; אם יש $c \notin \{1, a, b, ab\}$ אז יש אוטומורפיזם המעביר $a \mapsto a$, $b \mapsto b$ ו־$ab \mapsto c$, בסתירה לשמירה על הכפל. לכן $|G^{\#}| = 3$ וזה מוכיח את הסעיף האחרון.

תרגיל 6.6.22 (**) מספר נקודות השבת של $g \in G$ בפעולה על $X^{[d]}$ הוא $\mathrm{fp}(g)^{[d]}$.

המומנטים של מספר נקודות השבת אינם תלויים בחבורה, אלא במידת הטרנזיטיביות שבה היא פועלת.

תרגיל 6.6.23 (***) נסמן ב־$Y = \mathrm{fp}(g)$ את המשתנה המקרי השווה למספר נקודות השבת של איבר g הנבחר באקראי ובהתפלגות אחידה מן החבורה G. (הלמה של ברנסייד קובעת שאם הפעולה טרנזיטיבית אז $\mathbf{E}(Y) = 1$.) הראה שלכל d, אם הפעולה d־טרנזיטיבית אז $\mathbf{E}(Y^{[d]}) = 1$. בפרט אם הפעולה 2־טרנזיטיבית אז $\mathbf{V}(Y) = 1$. **הדרכה**. השתמש בלמה של ברנסייד עבור הפעולה של G על $X^{[d]}$.

תרגיל 6.6.24 (***) תהי G חבורה הפועלת d־טרנזיטיבית על קבוצה X. מספר המסלולים בפעולה של G על $X^{[d+1]}$, שאותו נסמן ב־m, שווה למספר המסלולים בפעולה של $G_{x_1,\dots,x_d}$ על $X - \{x_1, \dots, x_d\}$. הראה ש־$\mathbf{E}(Y^{[d+1]}) = m$.

פעולה 2־טרנזיטיבית

תרגיל 6.6.25 (**) נניח ש־G פועלת 2־טרנזיטיבית על קבוצה X בגודל > 2. אז מייצבי הנקודות (שהם צמודים זה לזה לפי תרגיל 6.6.5) יוצרים את G. **הדרכה**. יהי $\sigma \in G$. קח $a \in X$ ו־$b \neq a, \sigma a$. יש $\sigma' \in G$ כך ש־$\sigma'\sigma a = \sigma a$ ו־$\sigma' b = \sigma b$, ואז $\sigma = \sigma'(\sigma'^{-1}\sigma) \in G_{\sigma a} G_b$.

תרגיל 6.6.26 (**) תהי G חבורה הפועלת 2־טרנזיטיבית על קבוצה X. אז לכל $x \in X$, $\mathrm{N}_G(G_x) = G_x$.

תרגיל 6.6.27 (**) בעידון של משפט קיילי (תרגיל 6.3.13) G פועלת על אוסף הקוסטים G/H על־ידי כפל משמאל. הראה שפעולה זו 2־טרנזיטיבית אם ורק אם כל קוסט ימני של H חותך כל קוסט שמאלי.

תרגיל 6.6.28 (**) תהי G חבורה הפועלת 2־טרנזיטיבית על X. אז כל תת־חבורה נורמלית לא־טריוויאלית שלה פועלת טרנזיטיבית. **הדרכה**. תהי $H \lhd G$ עם $1 \neq h \in H$. אז יש $a \in X$ כך ש־$h(a) \neq a$. יהיו $x, y \in X$, אז קיים $\sigma \in G$ כך ש־$\sigma a = x$ ו־$\sigma h a = y$; כך $\sigma h \sigma^{-1} \in H$ מקיים $\sigma h \sigma^{-1} x = \sigma h a = y$.

הערה 6.6.29 לפי **משפט ברנסייד**, כל תת־חבורה טרנזיטיבית של S_p (p ראשוני) שאינה 2־טרנזיטיבית, מוכלת (לאחר מספור מתאים) בחבורת ההעתקות האפיניות $\{x \mapsto ax + b :\ a \in \mathbb{F}_p^{\times}, b \in \mathbb{F}_p\}$.

קוסטים כפולים

הגדרה 6.6.30 *תהיינה $A, B \leq G$ תת־חבורות. הקוסטים הכפולים של A, B הם הקבוצות מהצורה AgB, $g \in G$. את מרחב הקוסטים הכפולים מסמנים ב־$A \backslash G / B$.*

תרגיל 6.6.31 (*) קוסטים כפולים שונים של G הם זרים.

תרגיל 6.6.32 (*-)** $|HgK| = \frac{|H| \cdot |K|}{|gHg^{-1} \cap K|}$. **הערה**. שים לב במיוחד למקרה $g = 1$.

תרגיל 6.6.33 (**) חשב את הקוסטים הכפולים של $\langle (123) \rangle, \langle (124) \rangle$ בחבורה A_4.

תרגיל 6.6.34 (*) הקוסטים הכפולים הם המסלולים של פעולת A משמאל על מרחב הקוסטים הימניים G/B; וגם של פעולת B מימין על מרחב הקוסטים השמאליים $A \backslash G$.

תרגיל 6.6.35 **(**+)** תהי G חבורה עם תת־חבורות A, B. הראה שמספר הקוסטים הכפולים $A\backslash G/B$ שווה למספר המסלולים של G בפעולת הכפל משמאל על $G/A \times G/B$. **הדרכה**. יש איזומורפיזם של קבוצות $G\backslash(G/A \times G/B) \to A\backslash G/B$ המוגדר לפי $G(xA, yB) \mapsto Ax^{-1}yB$.

תרגיל 6.6.36 **(**+)** תהיינה $A, B \leq G$ תת־חבורות. נסמן ב־P את קבוצת החיתוכים של תת־חבורה הצמודה ל־A עם תת־חבורה הצמודה ל־B. החבורה A פועלת על P על־ידי הצמדה. הראה ש־$[A \cap gBg^{-1}] \mapsto AgB$ היא פונקציה מוגדרת היטב מ־$A\backslash G/B$ ל־P/A.

תרגיל 6.6.37 **(**+)** $|A\backslash G/B| = \frac{1}{|A|}\sum_{g\in G/B}\left|A \cap gBg^{-1}\right|$. **הדרכה**. הלמה של ברנסייד (משפט 6.5.3).

תרגיל 6.6.38 **(**)** תהי $H \leq G$. $|H\backslash G/H| = \frac{|G|}{|H|^2}\sum_{C\subseteq G}\frac{|H\cap C|^2}{|C|}$, כאשר הסכום על פני מחלקות הצמידות $C \subseteq G$. **הדרכה**. מספר נקודות השבת של $H \times H$ הוא $(x, y) \in H \times H$ הוא $|C_G(x)|$ אם x, y צמודים ב־G, ואפס אחרת.

תרגיל 6.6.39 **(**+)** בתרגיל 6.6.36, נניח ש־G פועלת על קבוצה X ו־$B = G_x$ היא המייצב של נקודה. כך פועלת A על X. הראה שהפונקציה המתוארת שם מתאימה מסלול ב־X תחת פעולת A, למייצב של נקודה במסלול (תחת פעולת A) עד כדי הצמדה.

תרגיל 6.6.40 **(**)** נניח שחבורות A, B פועלות על מרחב X. הפעולות **מתחלפות** אם לכל $a \in A$ ו־$b \in B$, ולכל $x \in X$, מתקיים $a(b(x)) = b(a(x))$. במקרה זה החבורה $A \times B$ פועלת על X לפי $(a, b)x = a(b(x))$.

תרגיל 6.6.41 **(**)** תהיינה $A, B \leq G$ תת־חבורות; אז A פועלת על G על־ידי כפל משמאל, ו־B פועלת על־ידי כפל מימין ($b\colon x \mapsto xb^{-1}$). הראה שהפעולות מתחלפות, כך ש־$A \times B$ פועלת על G, לפי $(a, b)\colon x \mapsto axb^{-1}$. הראה שמסלולי הפעולה הזו הם הקוסטים הכפולים $A\backslash G/B$.

תרגיל 6.6.42 **(**)** החבורה G פועלת על $G \times G$ מימין ומשמאל. מצא התאמה חד־חד־ערכית בין קבוצת המסלולים $G\backslash(G \times G)/G$ לקבוצת מחלקות הצמידות של G.

תרגיל 6.6.43 **(**)** תהי G חבורה הפועלת 2־טרנזיטיבית על קבוצה X, ויהי $a \in X$. הראה שלכל $x \notin G_a$, $G = G_a \cup G_axG_a$. **הדרכה**. זו גרסה של תרגיל 6.6.44.

תרגיל 6.6.44 **(***)** לכל תת־חבורה $B \leq G$, הפעולה של G על מרחב הקוסטים G/B היא טרנזיטיבית. הפעולה של B, לעומת זאת, אינה טרנזיטיבית. הוכח שהפעולה של G על G/B היא 2־טרנזיטיבית, אם ורק אם בפעולה של B יש שני מסלולים, כלומר קיים $x \notin B$ (שקול לזה: לכל $x \notin B$), כך ש־$G = B \cup BxB$. (השווה לתרגיל 6.6.86.)

פעולה סימטרית

הגדרה 6.6.45 ***פעולת חבורה G על קבוצה X היא סימטרית אם לכל $x, y \in X$ יש $g \in G$ כך ש־$gx = y$ ו־$gy = x$.***

הגדרה 6.6.46 ***פעולת חבורה G על קבוצה X היא 2־טרנזיטיבית חלש אם היא טרנזיטיבית על אוסף הזוגות הלא סדורים $\{\{x, y\} : x, y \in X,\ x \neq y\}$. כלומר, לכל $x \neq x'$ ולכל $y \neq y'$ קיים $g \in G$ כך ש־$gx = y$ ו־$gx' = y'$, או ש־$gx = y'$ ו־$gx' = y$.***

תרגיל 6.6.47 **(*)** פעולת G על X היא 2־טרנזיטיבית אם ורק אם היא 2־טרנזיטיבית חלש וסימטרית.

תרגיל 6.6.48 (**) כל פעולה סימטרית היא טרנזיטיבית.

תרגיל 6.6.49 (**) כל פעולה 2־טרנזיטיבית חלש היא פרימיטיבית. **הדרכה.** נניח ש־$B \subset X$ הוא בלוק עם יותר מנקודה אחת, וניקח $x, y \in B$ ו־$y' \not\in B$. לפי ההנחה אפשר להזיז את $\{x, y\}$ ל־$\{x, y'\}$, וזה שובר את הבלוק.

תרגיל 6.6.50 (**) תנאי הכרחי ומספיק לכך שכל פעולה טרנזיטיבית של G תהיה סימטרית, הוא ש־$g^2 = 1$ לכל $g \in G$. **הדרכה.** הפעולה הרגולרית.

תרגיל 6.6.51 (**) הראה שפעולת $\mathbb{Z}_n$ על עצמה היא תמיד טרנזיטיבית, פרימיטיבית לכל p ראשוני, 2־טרנזיטיבית חלש רק אם $n = 2, 3$, ו־2־טרנזיטיבית רק אם $n = 2$.

תרגיל 6.6.52 (**) בעידון של משפט קיילי (תרגיל 6.3.13) G פועלת על אוסף הקוסטים G/H על־ידי כפל משמאל. הראה שפעולה זו סימטרית אם ורק אם בכל קוסט zH יש שני אברים הפוכים זה לזה.

6.6.2 פעולה פרימיטיבית

ניתן לדלג בקריאה ראשונה.

הגדרה 6.6.53 ***אומרים שחלוקה $X = X_1 \cup \cdots \cup X_t$ נשמרת על־ידי הפעולה של חבורה G אם לכל $g \in G$ ולכל i, $g(X_i) = X_j$ לאיזשהו j. חלוקה שיש בה רק בלוק אחד, או שכל הבלוקים שלה הם יחידונים, היא חלוקה טריוויאלית (כל פעולה שומרת על כל חלוקה טריוויאלית). הפעולה של חבורה G על קבוצה X אינה פרימיטיבית אם היא שומרת חלוקה לא טריוויאלית כלשהי; כלומר, הפעולה פרימיטיבית אם אינה שומרת אף חלוקה לא־טריוויאלית.***

תרגיל 6.6.54 (+*) כל פעולה על קבוצה בגודל 1 או 2 היא פרימיטיבית. לכל קבוצה בגודל > 2, מצא פעולה עליה שאינה פרימיטיבית.

תרגיל 6.6.55 (***) כל פעולה 2־טרנזיטיבית היא פרימיטיבית.

תרגיל 6.6.56 (-*)** כל פעולה פרימיטיבית היא טרנזיטיבית (למעט פעולת החבורה הטריוויאלית על קבוצה בגודל 2).

תרגיל 6.6.57 (***) כל תת־חבורה נורמלית של חבורה הפועלת פרימיטיבית, פועלת בעצמה באופן טרנזיטיבי. (זו הכללה של תרגיל 6.6.56, ולפי תרגיל 6.6.55 גם של תרגיל 6.6.28.)

תרגיל 6.6.58 (***) תהי G חבורה הפועלת טרנזיטיבית. הפעולה פרימיטיבית אם ורק אם המייצב של נקודה, G_x, הוא תת־חבורה מקסימלית.

הגדרה 6.6.59 ***חבורה G היא מכפלה תת־ישרה של החבורות H_α אם $G \hookrightarrow \prod H_\alpha$ באופן כזה שההטלה על כל רכיב היא על.***

תרגיל 6.6.60 (***) חבורה הפועלת נאמנה באופן לא פרימיטיבי היא מכפלה תת־ישרה של חבורות הפועלות באופן פרימיטיבי.

משפט 6.6.61 (משפט Wielandt) תת־החבורות הפרימיטיביות היחידות של S_∞ מתרגיל 5.4.17 הן S_∞ ו־A_∞.

6.6.3 תת־חבורות של S_n

תרגיל 6.6.62 (**) החבורה $S_n \times \mathbb{Z}_2$ פועלת על מרחב הזוגות $\{(i,j) \colon 1 \leq i \neq j \leq n\}$ על־ידי $\sigma(i,j) = (\sigma i, \sigma j)$ לכל $\sigma \in S_n$, כאשר $\omega(i,j) = (j,i)$ יוצר את המרכיב מסדר 2. הראה שפעולה זו היא פרימיטיבית.

תרגיל 6.6.63 (**) מצא את כל תת־החבורות של S_4 הפועלות באופן 2־טרנזיטיבי. **הדרכה.** מצא את הגודל של תת־חבורה שכזו, והראה שהיא נורמלית. העזר במבנה מחלקות הצמידות של S_4.

תרגיל 6.6.64 (-*)** מה יכול להיות הסדר של תת־חבורה 2־טרנזיטיבית של S_5? **הדרכה.** תרגיל 6.6.14.

תרגיל 6.6.65 (***) נתאר את תת־החבורות מסדר 20 של S_5 (לחבורות אלה תפקיד חשוב בתרגיל 7.2.33).

1. (א) מצא (כלומר: רשום יוצרים של) תת־חבורה G מסדר 20 של S_5. **הדרכה.** חבורה מסדר 20 חייבת להכיל איבר σ מסדר 5. הראה ש־$\langle\sigma\rangle \lhd G$, ולכן $G \subseteq \mathrm{N}_{S_5}(\sigma)$.
   (ב) הראה שחבורת 2־סילו של G היא ציקלית. כמה תת־חבורות מסדר 4 יש ל־G?
   (ג) חשב (בלי לספור) כמה איברים מסדר 5 יש ב־G. כמה מסדר 4? ומסדר 2?
   (ד) הסק שהחיתוך של כל שתי תת־חבורות ציקליות של G הוא טריוויאלי.
   (ה) הוכח של־G יש תת־חבורה יחידה מסדר 10 (ושהיא איזומורפית ל־D_5).
   (ו) יש בדיוק 6 דרכים לפרק את הגרף השלם K_5 לאיחוד זר של שני מחומשים.
   (ז) יש התאמה בין הפירוקים של K_5 למחומשים לבין עותקים צמודים של G.
   הדרכה. הפירוק $K_5 = P \cup P'$ מתאים לחבורת התמורות השומרות על הפירוק.
2. כל 6 תת־החבורות מסדר 20 של S_5 צמודות זו לזו.
3. החיתוך של כל שתי תת־חבורות מסדר 20 איזומורפי ל־$\mathbb{Z}_4$. יש 15 עותקים של $\mathbb{Z}_4$ ב־S_5. כל אחד מהם מוכל בדיוק בשתי תת־חהובורת מסדר 20. החיתוך של כל שלוש תת־החבורות מסדר 20 הוא טריוויאלי.
4. הראה שתת־חבורה מסדר 20 של S_5 היא 2־טרנזיטיבית.

תרגיל 6.6.66 (***)
1. הוכח שכל תת־חבורה 2־טרנזיטיבית של S_n המכילה חילוף היא החבורה כולה.
2. נתבונן בתת־החבורות $A = \mathrm{Aut}(\triangle\triangle)$ ו־$B = \mathrm{Aut}(||||)$ של S_6, המוגדרות כחבורות אוטומורפיזמים של הגרפים הנתונים על 6 נקודות. הראה ש־$|A| = 72$ ו־$|B| = 48$. נסמן ב־B_0 את תת־החבורה של B הפועלת באופן זוגי על שלושת הזוגות; כך $|B_0| = 24$. הראה שאפשר לבחור את המספור כך ש־$A = \langle(13),(123456)\rangle$; $B_0 = \langle(14),(123456)\rangle$.
3. הראה ש־A, B_0 טרנזיטיביות אבל אינן פרימיטיביות (פרימיטיביות מוגדרת בתת־סעיף 6.6.2. בתרגיל 10.2.6 אנו מוכיחים תכונה מעניינת נוספת של תת־החבורות האלו).
4. כל תת־חבורה טרנזיטיבית של S_6 המכילה חילוף מכילה עותק צמוד של A או של B_0.
5. נסמן ב־A^+, B^+, B_0^+ את החיתוך של A_6 עם A, B, B_0 בהתאמה (שהוא מאינדקס 2 בכל המקרים). הראה שכל תת־חבורה טרנזיטיבית של A_6 מכילה עותק צמוד של A^+ או של B_0^+. הראה ש־$B_0^+ \cong A_4$. הראה ש־A^+ מקסימלית ב־A_6, ושיש בדיוק שתי תת־חבורות אמיתיות של A_6 (עד כדי הצמדה) המכילות את B_0^+: B^+ ועותק לא סטנדרטי של A_5 (ראה תרגיל 7.2.33).

6. כל תת־חבורה טרנזיטיבית של S_6 מכילה עותק צמוד של A^+ או של B_0^+.

תרגיל 6.6.67 (***) הראה שיש שני טיפוסי איזומורפיזם של תת־חבורות מסדר 12 של S_5: A_4 ו־$S_3 \times \mathbb{Z}_2$. הראה שכל שתי תת־חבורות איזומורפיות הן צמודות. כמה יש מכל סוג? **הדרכה.** מבני המחזורים האפשריים לאברי תת־החבורה הם $[41], [32], [311], [221], [2111], [11111]$. כתוב את המשוואות הנובעות מן הלמה של ברנסייד בפעולת החבורה על נקודות, על זוגות סדורים, על זוגות סדורים, על שלשות סדורות ועל זוגות לא סדורים. הסק שיש שמונה אברים עם מבנה $[311]$ ושלושה עם מבנה $[221]$. לכן יש שני מסלולים בפעולה על נקודות.

תרגיל 6.6.68 (***) נראה כיצד מסייעת הלמה של ברנסייד למצוא את התפלגות מבני המחזורים בתת־חבורה של A_6.

1. מבני המחזורים של אברים ב־A_6 הם $[51], [42], [33], [3111], [2211], [111111]$.
2. הראה שמספר נקודות השבת בפעולה הטבעית של S_6 על $X = \{1, 2, \ldots, 6\}$, בהתאמה לרשימת מבני המחזורים, הוא $6, 2, 3, 0, 0, 1$. באותו אופן יש $30, 2, 6, 0, 0, 0$ נקודות שבת בפעולה על זוגות סדורים (של אברים שונים); $120, 0, 6, 0, 0, 0$ נקודות שבת בפעולה על שלשות סדורות (של אברים שונים); ו־$15, 3, 3, 0, 1, 0$ נקודות שבת בפעולה על זוגות לא סדורים.
3. בחבורה $G \leq A_6$, נסמן ב־k_2, k_3, k_3', k_4, k_5 את מספרי האברים מן המחלקות השונות, בהתאמה, פרט לאיבר היחידה. אז $1 + k_2 + k_3 + k_3' + k_4 + k_5 = n$, ו־$n$ מחלק את $6 + 2k_2 + 3k_3 + k_5$, $30 + 2k_2 + 6k_3$, $120 + 6k_3$ ו־$15 + 3k_2 + k_3 + k_4$. **הדרכה.** הלמה של ברנסייד.
4. תהי $G \leq A_6$ תת־חבורה מסדר $n = 40$. אז יש לה 5 אברים מסדר 2, 10 מסדר 4 ו־24 מסדר 5. **הדרכה.** פתור (או תן למחשב לפתור) את המשוואות $n = 1 + k_5 + \cdots + k_2$, $6 + 2k_2 + 3k_3 + k_5 = \alpha n$, $30 + 2k_2 + 6k_3 = \beta n$, $120 + 6k_3 = \gamma n$, $15 + 3k_2 + k_3 + k_4 = \delta n$, לכל הערכים האפשריים של $\alpha, \beta, \gamma, \delta$.
5. לכל תת־חבורה $G \leq A_6$ מסדר 18 יש תשעה אברים מסדר 2, וארבעה אברים מכל אחת משתי מחלקות הצמידות של אברים מסדר 3. פעולת G על X אינה טרנזיטיבית. הסק ש־$G \cong \mathbb{Z}_3 \times S_3$. **הדרכה.** לפני פתרון המשוואות יש להציב $k_4 = k_5 = 0$, שהרי $4, 5$ אינם מחלקים את 18.
6. אין ל־A_6 תת־חבורות מסדר 30. **הדרכה.** בשני הפתרונות היחידים למערכת, אין אברים מסדר 2, וזו סתירה לתרגיל 2.1.13.

סגור וילנד

הגדרה 6.6.69 ***תהי G חבורה הפועלת על קבוצה X. אומרים שתמורה $\sigma \in S_X$ k־מסכימה עם G, אם לכל $x_1, \ldots, x_k \in X$ יש $g \in G$ כך ש־$\sigma(x_i) = g(x_i)$ לכל i. סְגור וילנד ה־k של G הוא החבורה $W_k(G)$ של כל התמורות ש־k־מסכימות עם G. (הפעולה נקראת על־שם Helmut Wielandt, 1910-2001).***

תרגיל 6.6.70 (*) הוכח ש־$W_k(G)$ היא חבורה.

תרגיל 6.6.71 (+*) $W_k(G) = \bigcap_{x_1,\ldots,x_k} (G \cdot S_{X-\{x_1,\ldots,x_k\}})$.

תרגיל 6.6.72 (**) הראה ש־$W_1(G) \supseteq W_2(G) \supseteq \cdots \supseteq G$.

תרגיל 6.6.73 (*) אם $G \subseteq H$ אז לכל k, $W_k(H) \subseteq W_k(G)$.

תרגיל 6.6.74 (**) לכל k, k', $W_k(W_{k'}(G)) = W_{\min\{k,k'\}}(G)$. **הדרכה.** הוכח ש־$W_k(W_k(G)) = W_k(G)$, וחלק למקרים.

תרגיל 6.6.75 (-)** פעולת G k־טרנזיטיבית אם ורק אם $W_k(G) = S_X$.

תרגיל 6.6.76 (-)** הראה ש־$W_1(G)$ אינה אלא מכפלה ישרה של חבורות סימטריות $S_{m_1} \times \cdots \times S_{m_t}$, כאשר m_i הם גדלי המסלולים בפעולה.

תרגיל 6.6.77 (-*)** לכל $x \in X$, $W_k(G)_x = W_{k-1}(G_x)$.

תרגיל 6.6.78 (**) נניח ש־G טרנזיטיבית. הראה ש־$W_k(G) = G$ אם ורק אם $W_{k-1}(G_x) = G_x$.

תרגיל 6.6.79 (**) מצא את $W_k(G)$ לכל k, כאשר $G = D_8$ עם הפעולה הרגילה על קודקודי המתומן.

6.6.4 פעולה רגולרית

ניתן לדלג בקריאה ראשונה.

הגדרה 6.6.80 ***הפעולה של G על X היא רגולרית** (נקראת גם **טרנזיטיבית חדה**) **אם לכל x, y יש איבר יחיד $g \in G$ כך ש־$g(x) = y$.***

תרגיל 6.6.81 (*) אם G פועלת רגולרית על X אז $|X| = |G|$.

תרגיל 6.6.82 (**) הפעולה הרגולרית של G על עצמה (על־ידי כפל משמאל, ראה תרגיל 6.3.4) היא אכן רגולרית.

תרגיל 6.6.83 (-)** פעולה טרנזיטיבית היא רגולרית אם ורק אם לאף איבר $g \neq 1$ אין נקודות שבת. כלומר, $G_x = 1$ לכל $x \in X$.

תרגיל 6.6.84 (+)** ("חוק השלישי חינם") תהי G חבורה סופית הפועלת על קבוצה X. כל שתיים משלוש התכונות הבאות גוררת את השלישית: (1) הפעולה טרנזיטיבית, (2) הפעולה רגולרית, (3) $|X| = |G|$.

תרגיל 6.6.85 (**) תהי G חבורה הפועלת על קבוצה X, ותהי $H \leq G$ תת־חבורה טרנזיטיבית. אז הפעולה של H רגולרית אם ורק אם $H \cap G_x = 1$ לכל $x \in X$.

תרגיל 6.6.86 (**) תהיינה $A, B \leq G$. הפעולה של A על G/B, לפי כפל משמאל, היא טרנזיטיבית אם ורק אם $AB = G$, ורגולרית אם ורק אם A, B משלימות.

תרגיל 6.6.87 (**) תהי G חבורה הפועלת על קבוצה X, ותהי $H \lhd G$ תת־חבורה נורמלית רגולרית. יהי $x \in X$. הראה שהפעולה של G_x על $X-\{x\}$ איזומורפית לפעולת ההצמדה של G_x על $H^\# = H-\{1\}$. **הדרכה.** נתאים $h \mapsto h(x)$, אז לכל $\sigma \in G_x$, $\sigma(hx) \mapsto \sigma h \sigma^{-1}$.

תרגיל 6.6.88 (***) תהי G חבורה הפועלת באופן 4־טרנזיטיבי על קבוצה X. אם יש לה תת־חבורה נורמלית רגולרית אז $G = S_4$. **הדרכה.** נקבע $x \in X$, ותהי $H \lhd G$ נורמלית רגולרית. לפי תרגיל 6.6.87, פעולת ההצמדה של G_x על $H^\# = H-\{1\}$ איזומורפית לפעולה של G_x על $X-\{1\}$, שהיא 3־טרנזיטיבית לפי תרגיל 6.6.10. מקל וחומר, גם פעולת $\mathrm{Aut}(H)$ על $H^\#$ היא 3־טרנזיטיבית, ולפי תרגיל 6.6.21, $H = \mathbb{Z}_2 \times \mathbb{Z}_2$. אבל אז $|X| = 4$ (תרגיל 6.6.81) ו־$G = S_4$ לפי ההנחה.

משפט 6.6.89 ***תהי G חבורה הפועלת באופן 4־טרנזיטיבי על קבוצה X. אם ל־G יש מייצב פשוט, אז G פשוטה.***

הוכחה. נקבע $x \in X$. תהי $H \lhd G$, אז $H \cap G_x \lhd G_x$, ולפי ההנחה יש שתי אפשרויות: או ש־$G_x \leq H$, ואז $H = G$ לפי תרגיל 6.6.25, או ש־$G_x \cap H = 1$. אם $H = 1$ סיימנו, ואחרת H טרנזיטיבית לפי תרגיל 6.6.28, ורגולרית (תרגיל 6.6.85). מתרגיל 6.6.88 יוצא ש־$G = S_4$, אבל אז $G_x = S_3$ שאינה פשוטה, בסתירה להנחה. $\square$

תרגיל 6.6.90 (**) הוכח ממשפט 6.6.89 ש־A_n פשוטה לכל $n \geq 5$. **הדרכה.** באינדוקציה על n, כשהבסיס $n=5$ הוא תרגיל 5.4.4. לכל $n \geq 6$, A_n היא $(n-2)$־טרנזיטיבית לפי תרגיל 6.6.19 ולכן 4־טרנזיטיבית, והמשפט חל משום שהמייצב של הנקודה n הוא A_{n-1}. **הערה.** להוכחה ישירה, ראה 5.4.5.

תרגיל 6.6.91 (***־) תהי G חבורה הפועלת על קבוצה X, יש לה תת־חבורה נורמלית רגולרית.

1. אם הפעולה 2־טרנזיטיבית אז $|X|$ הוא חזקת ראשוני.
2. אם הפעולה 3־טרנזיטיבית אז $|X| = 3$ או $|X| = 2^n$.

הדרכה. הוכחת תרגיל 6.6.88 תקפה, עד לשורה האחרונה.

תרגיל 6.6.92 (**+) כל חבורה אבלית הפועלת טרנזיטיבית, היא רגולרית. **הדרכה.** אחרת יש $x \in G$ עם $x(a) = a$ ו־$x(b) \neq b$. קח y כך ש־$y(a) = b$, אז $xy(a) = x(b)$ בעוד ש־$yx(a) = y(a) = b$.

תרגיל 6.6.93 (**) תת־חבורה אמיתית של חבורה רגולרית אינה יכולה להיות רגולרית.

תרגיל 6.6.94 (***־) תהי G חבורה הפועלת רגולרית. הראה ש־$G = W_2(G)$ (ראה הגדרה 6.6.69). **הדרכה.** $W_2(G)_x = W_1(G_x) = W_1(1) = 1$ לפי תרגיל 6.6.77, ולפי תרגיל 6.6.85, $W_2(G)$ רגולרית. סיים בעזרת תרגיל 6.6.93.

תרגיל 6.6.95 (**+) תהי $A \leq S_X$ חבורה אבלית הפועלת רגולרית. אז $\mathrm{C}_{S_X}(A) = A$. **הדרכה.** אם x מרכז את A אז $\langle A, x\rangle$ רגולרית לפי תרגיל 6.6.92; הפעל את תרגיל 6.6.93.

הגדרה 6.6.96 *פעולה היא k־טרנזיטיבית חדה אם לכל $x_1, \dots, x_k$ שונים ולכל $y_1, \dots, y_k$ שונים, יש $g \in G$ יחיד כך ש־$g(x_i) = y_i$.*

תרגיל 6.6.97 (**) אם G פועלת k־טרנזיטיבית בחדות על קבוצה X, אז $|G| = |X|^{[d]}$.

תרגיל 6.6.98 (**) נניח ש־G פועלת 2־טרנזיטיבית בחדות על קבוצה X, $|X| > 1$. הראה שיש לה אברים מסדר 2. הראה שכולם צמודים זה לזה. **הדרכה.** אם t, t' מסדר 2, קח $x \in X$ ובחר $s \in G$ כך ש־$s \cdot x = x$ ו־$t' \cdot x = s \cdot (t \cdot x)$.

6.7 החבורות הלינאריות

ניתן לדלג בקריאה ראשונה.

הגדרה 6.7.1 *נסמן ב־$F^\times I$ את חבורת המטריצות הסקלריות ב־$\mathrm{GL}_n(F)$.*

תרגיל 6.7.2 *(**)* $\mathrm{Z}(\mathrm{GL}_n(F)) = F^\times I$.

מגדירים $\mathrm{PGL}_n(F) = \mathrm{GL}_n(F)/F^\times I$ ו־$\mathrm{PSL}_n(F) = \mathrm{SL}_n(F)/(\mathrm{SL}_n(F) \cap F^\times I)$.

תרגיל 6.7.3 (*) מעל השדה $F = \mathbb{F}_2$, $\mathrm{GL}_n(F) = \mathrm{SL}_n(F) \cong \mathrm{PGL}_n(F) = \mathrm{PSL}_n(F)$.

תרגיל 6.7.4 (**) הראה שכל מטריצה לא סקלרית ב־$\mathrm{GL}_2(F)$ צמודה למטריצה יחידה מהצורה $\begin{pmatrix} 0 & * \\ 1 & * \end{pmatrix}$. **הדרכה.** הצמד את $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ במטריצה הפיכה מהצורה $P = \begin{pmatrix} -\Delta x & -\Delta y \\ ax+cy & bx+dy \end{pmatrix}$, כאשר $\Delta = \det(A)$. היחידות לפי הדטרמיננטה והעקבה.

תרגיל 6.7.5 (*+)** 1. כל מטריצה לא סקלרית ב־$\mathrm{SL}_2(F)$ שקולה, תחת פעולת ההצמדה של $\mathrm{GL}_2(F)$, למטריצה יחידה מהצורה $\begin{pmatrix} 0 & -1 \\ 1 & t \end{pmatrix}$

2. עם זאת, המטריצה $\begin{pmatrix} 0 & 1 \\ -1 & 1 \end{pmatrix}$ אינה צמודה ב־$\mathrm{SL}_2(\mathbb{F}_3)$ לאף מטריצה מהצורה $\begin{pmatrix} 0 & -1 \\ 1 & t \end{pmatrix}$.

3. הסדר של $\begin{pmatrix} 0 & -1 \\ 1 & t \end{pmatrix}$ (בהנחה שהוא סופי) שווה ל־n המינימלי כך ש־$(x^2-tx+1) \mid (x^n-1)$.

תרגיל 6.7.6 (**) $\mathrm{PGL}_2(F)/\mathrm{PSL}_2(F) \cong F^\times/F^{\times 2}$. בפרט, כאשר F שדה סופי, $\mathrm{PSL}_2(F) = \mathrm{PGL}_2(F)$ עבור שדות ממאפיין 2, ו־$[\mathrm{PGL}_2(F) : \mathrm{PSL}_2(F)] = 2$ במאפיין אי־זוגי.

תרגיל 6.7.7 (*+)** כל איבר לא טריוויאלי ב־$\mathrm{PSL}_2(F)$ שקול תחת פעולת $\mathrm{PGL}_2(F)$ לאיבר מהצורה $\begin{pmatrix} 0 & -1 \\ 1 & t \end{pmatrix}$, כאשר $t \in F$ יחיד עד־כדי סימן. הסדר של $\begin{pmatrix} 0 & -1 \\ 1 & t \end{pmatrix}$ (בהנחה שהוא סופי) שווה ל־n המינימלי כך ש־$(x^2-tx+1) \mid (x^n \pm 1)$.

תרגיל 6.7.8 (**) יהי F שדה, ו־$V = F^n$ המרחב הוקטורי ה־n־ממדי מעליו.

1. הפעולה הטבעית של $G = \mathrm{GL}_n(F)$ על V היא טרנזיטיבית על $V - \{0\}$.
2. הפעולה היא 2־טרנזיטיבית אם ורק אם $|F| = 2$.
3. הפעולה היא 3־טרנזיטיבית אם ורק אם $|F| = 2$ ו־$n \leq 2$.

(השווה לתרגיל 6.6.21.)

תרגיל 6.7.9 (**) הפעולה הטבעית של $\mathrm{GL}_n(F)$ על F^n מגדירה פעולה נאמנה של $\mathrm{PGL}_n(F)$ (הגדרה 6.7.1) על אוסף תת־המרחבים החד־ממדיים של F^n, לפי $[A] : Fx \mapsto F(Ax)$.

1. פעולה זו של $\mathrm{PGL}_n(F)$ היא תמיד 2־טרנזיטיבית.
2. הפעולה של $\mathrm{PGL}_n(F)$ אינה 3־טרנזיטיבית כאשר $n > 2$.

תרגיל 6.7.10 (**) נתבונן בפעולה של $\mathrm{PGL}_2(F)$ שהוגדרה בתרגיל 6.7.9. נזהה את תת־המרחב $F\begin{pmatrix} z \\ 1 \end{pmatrix}$ עם $z \in F$ ואת תת־המרחב $F\begin{pmatrix} 1 \\ 0 \end{pmatrix}$ עם ∞, כך שמתקבלת פעולה של $\mathrm{PGL}_2(F)$ על $F \cup \{\infty\}$. הראה שפעולה זו מוגדרת על־ידי $\begin{pmatrix} a & b \\ c & d \end{pmatrix} z = \frac{az+b}{cz+d}$, כאשר הערך של שבר שהמכנה שלו הוא 0 הוא ∞, ו־$\frac{a\infty+b}{c\infty+d} = \frac{a}{c}$.

תרגיל 6.7.11 (**) הראה שפעולת $\mathrm{PGL}_2(F)$ על $F \cup \{\infty\}$ היא 3־טרנזיטיבית (בחדות). **הדרכה.** הראה שלכל x, y, z שונים יש איבר (יחיד) המעביר $x \mapsto 0$, $y \mapsto 1$, $z \mapsto \infty$.

תרגיל 6.7.12 (*-)** הראה שהחבורה $\mathrm{PGL}_2(F)$ נוצרת על־ידי הפעולות $z \mapsto -1/z$, $z \mapsto z+a$ ו־$z \mapsto \alpha z$ ($a \in F$, $\alpha \in F^\times$).

תרגיל 6.7.13 (−*)** הראה שהחבורה $\mathrm{PSL}_2(F)$ נוצרת על־ידי הפעולות $z \mapsto -1/z$, $z \mapsto z+a$ ($a \in F$). **הדרכה.** העזר בתרגיל 6.7.12 כדי להראות שהחבורה נוצרת על־ידי הפעולות $z \mapsto -1/z$, $z \mapsto z+a$ ו־$z \mapsto \alpha^2 z$; בנוסף $\alpha^2 z = \alpha - \frac{1}{\alpha^{-1} - \frac{1}{\alpha - \frac{1}{z}}}$.

תרגיל 6.7.14 (+)** ל־$a,b,c \in F \cup \{\infty\}$ שונים, נסמן $\Delta(a,b,c) = (a-b)(b-c)(a-c)$ (כאשר $\Delta(\infty,a,b) = \Delta(b,\infty,a) = \Delta(a,b,\infty) = a-b$). הראה ש־$\sigma = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$ מקיימת

$$\Delta(\sigma a, \sigma b, \sigma c) = \det(\sigma)^3 (\gamma a+\delta)^{-2}(\gamma b+\delta)^{-2}(\gamma c+\delta)^{-2}\Delta(a,b,c).$$

מגדירים את **הסימן** של שלשה a,b,c להיות הקוסט של $\Delta(a,b,c)$ בחבורת המנה $F^\times/F^{\times 2}$.

1. הפעולה $\sigma \in \mathrm{PGL}_2(F)$ המוגדרת על־ידי $\sigma: 0 \mapsto a, 1 \mapsto b, \infty \mapsto c$, שייכת ל־$\mathrm{PSL}_2(F)$ אם ורק אם $\Delta(a,b,c) = \Delta(0,1,\infty)$.
2. פעולת $\mathrm{PSL}_2(F)$ שומרת על הסימן.
3. הפעולה של $\mathrm{PSL}_2(F)$ היא טרנזיטיבית (בחדות) על קבוצת השלשות מאותו סימן.

תרגיל 6.7.15 (**) בפעולה של $G = \mathrm{PGL}_2(F)$ על $F \cup \{\infty\}$, המייצב של נקודה איזומורפי ל־$F^\times \ltimes F^+$ (ראה תרגיל 7.3.8), והמייצב של שתי נקודות איזומורפי ל־$F^\times$. הסק שהפעולה נאמנה. **הדרכה.** חשב את G_∞ ואת $G_{\infty,0}$.

משפט 6.7.16 (לא נוכיח כאן) כל החבורות $\mathrm{PSL}_n(F)$ פשוטות, **למעט** $\mathrm{PSL}_2(\mathbb{F}_2)$ ו־$\mathrm{PSL}_2(\mathbb{F}_3)$.

תרגיל 6.7.17 (+**)** לכל n, האפימורפיזם $\mathbb{Z}\to\mathbb{Z}_n$ משרה אפימורפיזם $\mathrm{GL}_2(\mathbb{Z})\to\mathrm{GL}_2(\mathbb{Z}_n)$. מסמנים את הגרעין ב־$\Gamma(n)$. כל תת־חבורה של $\mathrm{GL}_2(\mathbb{Z})$ המכילה איזשהו $\Gamma(n)$ נקראת **תת־חבורת קונגרואנציה**. הראה ש־$H = \left\langle \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix} \right\rangle$ מקיימת $\Gamma(4) \subseteq H \subseteq \Gamma(2)$. הוכח ש־$H \cong \mathbb{F}_2$. העזר בכך כדי להגדיר הטלה $H\to\mathbb{Z}_p^2$. הראה שגרעין ההטלה הזו אינו תת־חבורת קונגרואנציה.

6.7.1 איזומורפיזמים יוצאי דופן

בסעיף זה נוכיח כמה איזומורפיזמים יוצאי דופן בין חבורות פשוטות.

הגדרה 6.7.18 *עבור q שהוא חזקת ראשוני, נסמן ב־$\mathbb{F}_q$ את השדה היחיד מסדר q.*

ידוע ש־$\mathbb{F}_q^\times$ ציקלית (הוכחה בתרגיל 9.1.13) ולכן, אם q אי־זוגי, $\mathbb{F}_q^\times/\mathbb{F}_q^{\times 2} \cong \mathbb{Z}_2$.
להמשך הסעיף יש להכיר את תת־החבורה $A_n \leq S_n$ מהגדרה 5.1.12.

תרגיל 6.7.19 (**) בדוק ש־$|\mathrm{PGL}_2(\mathbb{F}_q)| = (q-1)q(q+1)$. והסק מן השיכון $\mathrm{PGL}_2(\mathbb{F}_q) \hookrightarrow S_{q+1}$ של תרגיל 6.7.10, על־ידי השוואת סדרים, ש־

$$\mathrm{GL}_2(\mathbb{F}_2) = \mathrm{PGL}_2(\mathbb{F}_2) \cong S_3, \qquad \mathrm{PGL}_2(\mathbb{F}_3) \cong S_4, \qquad \mathrm{PGL}_2(\mathbb{F}_4) \cong A_5.$$

תרגיל 6.7.20 (**) בהמשך לתרגילים 6.7.6 ו־6.7.19, הראה ש־

$$\mathrm{PSL}_2(\mathbb{F}_3) \cong A_4.$$

תרגיל 6.7.21 (**) **היחס הכפול** של רביעיה סדורה של אברים שונים $x_1,x_2,x_3,x_4 \in F\cup\{\infty\}$ מוגדר לפי $[x_1,x_2;x_3,x_4]=\frac{x_1-x_3}{x_1-x_4}/\frac{x_2-x_3}{x_2-x_4}=\frac{x_3-x_1}{x_3-x_2}/\frac{x_4-x_1}{x_4-x_2}$, כאשר מגדירים $\frac{\infty-a}{\infty-b}=1$. הראה ש־$[x_1,x_2;x_3,x_4]\in F^\times-\{1\}$, ויכול לקבל כל ערך שם. הראה ש־$\mathrm{PGL}_2(F)$ שומרת על היחס הכפול, כלומר, לכל $\sigma\in\mathrm{PGL}_2(F)$, $[\sigma x_1,\sigma x_2;\sigma x_3,\sigma x_4]=[x_1,x_2;x_3,x_4]$.

תרגיל 6.7.22 (**) בהמשך לתרגיל 6.7.11 ולתרגיל 6.7.21, הראה ששמירת היחס הכפול מגדירה את הפעולה של $\mathrm{PGL}_2(F)$ על $F\cup\{\infty\}$, במובן הבא: לכל x_1,x_2,x_3 שונים קיים $\sigma\in\mathrm{PGL}_2(F)$ יחיד כך ש־$\sigma(x_1)=0$, $\sigma(x_2)=1$, $\sigma(x_3)=\infty$. איבר זה מוגדר לכל $y\neq x_1,x_2,x_3$ לפי הנוסחה $[x_1,x_2;x_3,y]=[0,1;\infty,\sigma(y)]$.

תרגיל 6.7.23 (**) בהמשך לתרגיל 6.7.21, הראה שבפעולה של S_4 על הביטויים מהצורה $[x_i,x_j;x_k,x_\ell]$, על־ידי החלפת המשתנים, היוצרים $(12),(23),(34)$ פועלים על $\lambda=[x_1,x_2;x_3,x_4]$ לפי $(12),(34)\colon\lambda\mapsto\lambda^{-1}$, $(23)\colon\lambda\mapsto 1-\lambda$. בפרט, הפעולה של חבורת הארבעה של קליין $K\subseteq S_4$ היא טריוויאלית: $[x_2,x_1;x_4,x_3]=[x_4,x_3;x_2,x_1]=[x_1,x_2;x_3,x_4]$. בדוק שהערך של $\frac{(\lambda^3-3\lambda+1)(\lambda^3-3\lambda^2+1)}{\lambda^2(1-\lambda)^2}$ אינו תלוי בסדר המשתנים.

תרגיל 6.7.24 (**) יהיו F שדה ו־$\lambda\in F^\times-\{1\}$. הראה שהמסלול של λ תחת הפעולה של S_4 (מתרגיל 6.7.23) נופל לאחד המקרים הבאים:

1. במסלול יש איבר בודד, $\{-1\}$, ו־$\mathrm{char}F=3$;
2. המסלול בן שני אברים, $\{\lambda,1-\lambda\}$, כאשר $\lambda+\lambda^{-1}=1$ ו־$\mathrm{char}F\neq 3$;
3. המסלול בן שלושה אברים, $\{-1,2,1/2\}$, כאשר $\mathrm{char}F\neq 3$;
4. המסלול בן 6 אברים שונים בכל מקרה אחר.

תרגיל 6.7.25 (**) נניח שהמאפיין של F הוא 3. נאמר שרביעיה לא סדורה $\{x_1,x_2,x_3,x_4\}$ היא **סימטרית** אם $[x_1,x_2;x_3,x_4]=-1$. (לפי תרגיל 6.7.24 התנאי אינו תלוי בסדר הנקודות; אבל אין זה כך מעל שדה ממאפיין אחר, או אם מחליפים את -1 בערך אחר.) נסמן ב־Θ את קבוצת הרביעיות הסימטריות.

1. בדוק ש־$[x_1,x_2;x_3,x_4]=-1$ אם ורק אם $s_2(x_1,\dots,x_4)=0$, כאשר $s_2(x_1,\dots,x_4)=\sum_{i<j}x_ix_j$ לערכים ב־F ו־$s_2(x_1,x_2,x_3,\infty)=\sum x_i$.
2. לכל $\{x_1,x_2,x_3\}$ יש השלמה יחידה לרביעיה סימטרית. לכן $\mathrm{PGL}_2(F)$ פועלת טרנזיטיבית על הרביעיות הסימטריות.
3. מעל שדה מסדר q (חזקה של 3), מספר הרביעיות הסימטריות הוא $|\Theta|=\frac{q(q^2-1)}{24}$; דרך כל נקודה עוברות $\frac{q(q-1)}{6}$ רביעיות (**הדרכה.** לפי הטרנזיטיביות, די לבדוק זאת עבור $\{0,\infty\}$) ; ודרך כל זוג נקודות עוברות $\frac{q-1}{2}$ רביעיות.

(משפחה של תת־קבוצות בגודל k של קבוצה Ω נקראת **תכנון בלוקים** אם לכל $x_1,x_2\in\Omega$ שונים יש מספר קבוע, λ, של $\theta\in\Theta$ כך ש־$x_1,x_2\in\theta$. לפיכך, Θ הוא תכנון בלוקים בעל הפרמטרים $|\Omega|=q+1,\ k=4,\ \lambda=\frac{q-1}{2}$.)

תרגיל 6.7.26 (*+)** בהמשך לתרגיל 6.7.25: נניח ש־$-1\in F^{\times 2}$ (בפרט, אם F שדה מסדר סופי q, אז q הוא חזקה של 9). הראה שהסימן $\Delta(x_1,x_2,x_3)$ של רביעיה סימטרית (כפי שהוגדר בתרגיל 6.7.14), מוגדר היטב כאיבר של $F^\times/F^{\times 2}$, ואינו תלוי בבחירת השלשה. **הדרכה.** $[x_1,x_2;x_3,x_4]=\frac{\Delta(x_1,x_3,x_4)}{\Delta(x_2,x_3,x_4)}$.

1. הראה ש־$\mathrm{PSL}_2(F)$ פועלת טרנזיטיבית על הרביעיות הסימטריות מאותו סימן.

2. נאמר שרביעיה סימטרית היא **חיובית** אם הסימן שלה הוא $+1$. נסמן ב־Θ^+ את קבוצת הרביעיות הסימטריות החיוביות. הראה ש־$|\Theta^+| = \frac{q(q^2-1)}{48}$. דרך כל נקודה עוברות $\frac{q(q-1)}{12}$ רביעיות חיוביות. דרך כל זוג נקודות עוברות $\frac{q-1}{4}$ רביעיות חיוביות. (לכן Θ^+ היא תכנון בלוקים עם $\lambda = \frac{q-1}{4}$.)

תרגיל 6.7.27 (***) נוכיח ש־$\mathrm{PSL}_2(\mathbb{F}_9) \cong A_6$. כלומר, נמצא פעולה של $\mathrm{PSL}_2(\mathbb{F}_9)$ על קבוצה בגודל 6 (של חמישיות של רביעיות של נקודות), המושרית מן הפעולה שלה על עשרת הנקודות של $\hat{\mathbb{F}}_9 = \mathbb{F}_9 \cup \{\infty\}$.
בהמשך לתרגיל 6.7.26, יהי $F = \mathbb{F}_9$ השדה מסדר 9 (-1 אינו ריבוע ב־$\mathbb{F}_3$, ולכן $\mathbb{F}_9 = \mathbb{F}_3[i]$ כאשר $i^2 = -1$).

1. נסמן ב־Θ^+ את קבוצת הרביעיות הסימטריות החיוביות. הראה ש־$|\Theta^+| = 15$. (אברי Θ^+ הם $\begin{matrix}0158, 0247, 0378, \infty012, \infty036\\ 0456, 1236, 1357, \infty147, \infty258\\ 1468, 2348, 2567, \infty345, \infty678\end{matrix}$, כאשר האינדקס $a+3b$ מייצג את האיבר $a+bi$ של השדה; למשל $\infty147$ מייצג את $\{\infty, 1, 1+i, 1-i\}$).

2. דרך כל שתי נקודות של $\hat{\mathbb{F}}_9$ עוברות בדיוק שתי רביעיות $\theta, \theta' \in \Theta^+$. לכן כל רביעיה נחתכת בשתי נקודות עם בדיוק 6 רביעיות אחרות. הראה שהרביעיה נחתכת עם כל אחת מ־8 הרביעיות הנותרות בנקודה אחת.

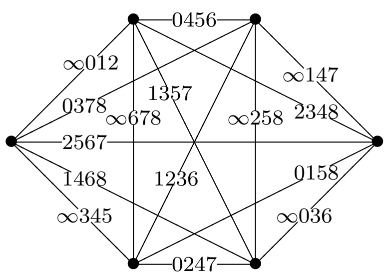
3. הראה ש־$\mathrm{PSL}_2(\mathbb{F}_9)$:

(א) פועלת טרנזיטיבית על הקבוצה $\{(\theta, \theta') : |\theta \cap \theta'| = 2\}$ (שיש בה 90 זוגות). **הדרכה.** המייצב של $(\infty012, \infty036)$ הוא $\langle z \mapsto -z, z \mapsto -1/z \rangle$.

(ב) פועלת טרנזיטיבית על הקבוצה $\{(\theta, \theta') : |\theta \cap \theta'| = 1\}$ (שיש בה 120 זוגות). **הדרכה.** המייצב של $(\infty012, \infty345)$ הוא $\langle z \mapsto z+1 \rangle$.

4. נאמר ש־$\theta_1, \theta_2, \theta_3 \in \Theta$ מהוות **משולש** אם $|\theta_i \cap \theta_j| = 1$ לכל $i \neq j$ ו־$\theta_1 \cap \theta_2 \cap \theta_3 = \emptyset$, ו**משולש חיובי** אם כל $\theta_i \in \Theta^+$. הראה שיש 60 משולשים. הראה ש־$\mathrm{PSL}_2(\mathbb{F}_9)$ פועלת טרנזיטיבית בחדות על קבוצת 360 המשולשים החיוביים הסדורים. (**הדרכה.** המייצב של $(\infty012, \infty345, 0378)$ טריוויאלי.)

5. תת־קבוצה $F \subseteq \Theta^+$ שיש בה חמש רביעיות היא **מניפה**, אם כל $\theta, \theta', \theta'' \in F$ שונות מהוות משולש. הראה שכל משולש מוכל במניפה יחידה. (**הדרכה.** לפי הסעיף הקודם די להוכיח טענה זו עבור משולש אחד.) הראה שיש בדיוק שש מניפות. (**הדרכה.** כל מניפה מכילה 10 משולשים.)



6. הראה שכל שתי מניפות נפגשות ברביעיה משותפת אחת. התבונן בגרף השלם (המופיע באיור משמאל) שקודקודיו הם המניפות, וכל צלע שלו מתוייגת ברביעיה היחידה המשותפת לשני הקודקודים. הראה שהתגיות של כל שתי קשתות זרות נחתכות בשתי נקודות (התגיות של קשתות בעלות קודקוד משותף נחתכות בנקודה אחת לפי הגדרת המניפות.)
הראה שלכל נקודה $\omega \in \hat{\mathbb{F}}_9$, הקשתות שהתגית שלהן כוללת את ω מהוות חלוקה של הגרף לזוג משולשים זרים, ושכל חלוקה מתאימה לנקודה אחת ויחידה.

7. הראה שפעולת $\mathrm{PSL}_2(\mathbb{F}_9)$ על $\hat{\mathbb{F}}_9 = \mathbb{F}_9 \cup \{\infty\}$ משרה פעולה נאמנה על הגרף, ודרך כך איזומורפיזם $\mathrm{PSL}_2(\mathbb{F}_9) \cong A_6$.

8. הראה שבפעולת $\mathrm{PSL}_2(\mathbb{F}_3) \subseteq \mathrm{PSL}_2(\mathbb{F}_9)$ על הגרף, תת־החבורה שווה למייצב של שני קודקודי הקשת $\hat{\mathbb{F}_3} = \infty 012$. **הדרכה**. נסמן את קודקודי הגרף ב־a, b, c, d, e, f, החל בקודקוד השמאלי ונגד כיוון השעון; אז $(cde) = (z \mapsto z+1)$ ו־$(be)(cd) = (z \mapsto -1/z)$. האיבר הנוסף $(abf) = (z \mapsto z+i)$ יוצר איתם את החבורה כולה.

תרגיל 6.7.28 (***) נראה שהאיזומורפיזם $\mathrm{PSL}_2(\mathbb{F}_9) \cong A_6$ של תרגיל 6.7.27 אינו ניתן להמשכה לאיזומורפיזם של חבורות האם $\mathrm{PGL}_2(\mathbb{F}_9) \to S_6$. ל־$A_6$ יש שבע מחלקות שקילות. המסלולים תחת פעולת S_6 מאופיינים במבנה המחזורים, והפעולה מאחדת שתי מחלקות (תרגיל 6.4.38). לצד זה, המסלולים של $\mathrm{PSL}_2(\mathbb{F}_9)$ תחת פעולת ההצמדה של $\mathrm{PGL}_2(\mathbb{F}_9)$ (פרט לזה של איבר היחידה) מאופיינים על־ידי העקבה, עד־כדי סימן (תרגיל 6.7.7); פעולה זו מאחדת שתי מחלקות אחרות. תכונותיהן של המחלקות מסוכמות בטבלה להלן.

סדר האברים	גודל המחלקה	מסלולי S_6: מבנה מחזורים	נציגים של מחלקות הצמידות ב־$\mathrm{PSL}_2(\mathbb{F}_9)$	מסלולי $\mathrm{PGL}_2(\mathbb{F}_9)$: עקבה	מבנה מחזורים בפעולה על $\hat{\mathbb{F}_9}$
5	72	$\left.\begin{matrix}\\ \\ \end{matrix}\right\}$ $[51]$	$\frac{-1}{z+1+i}$	$\pm(1+i)$	$[5^2]$
5	72		$\frac{-1}{z+1-i}$	$\pm(1-i)$	$[5^2]$
4	90	$[42]$	iz	$\pm i$	$[4^2 1^2]$
3	40	$[3^2]$	$z+1+i$	± 1	$[3^3 1]$
3	40	$[31^3]$	$z+1$		
2	45	$[2^2 1^2]$	$-\frac{1}{z}$	0	$[2^4 1^2]$
1	1	$[1^6]$	z		$[1^{10}]$

תרגיל 6.7.29 (***) נסמן ב־$\phi \colon \mathbb{F}_9 \mapsto \mathbb{F}_9$ את **אוטומורפיזם פרובניוס**, המוגדר לפי $\phi(x) = x^3$; הפעולה מורחבת באופן טבעי לתמורה על $\mathbb{F}_9 \cup \{\infty\}$. לחבורה $\langle \mathrm{PGL}_2(\mathbb{F}_9), \phi \rangle$ יש שלוש תת־חבורות המכילות את $\mathrm{PSL}_2(\mathbb{F}_9)$, והן $\mathrm{PGL}_2(\mathbb{F}_9) = \langle \mathrm{PSL}_2(\mathbb{F}_9), z \mapsto -z \rangle$, $\langle \mathrm{PSL}_2(\mathbb{F}_9), \phi \rangle$ ו־$M_{10} = \langle \mathrm{PSL}_2(\mathbb{F}_9), -\phi \rangle$ (האחרונה היא הקטנה מחמש **חבורות מתיו**). בתרגיל 6.7.27 ראינו ש־$A_6 \cong \mathrm{PSL}_2(\mathbb{F}_9)$. הראה שפעולת M_{10} על מחלקות הצמידות של A_6 מאחדת אותן מחלקות כמו הפעולה של S_6. (בתרגיל 8.4.46 אנו מראים ש־$M_{10} \not\cong S_6$).

תרגיל 6.7.30 (***) 1. יהי F שדה ממאפיין $\neq 2$. נאמר ששני זוגות זרים $\{\alpha, \beta\}$, $\{\alpha', \beta'\}$ הם שכנים אם $[\alpha, \beta; \alpha', \beta'] = -1$. הראה שיחס השכנות מוגדר היטב (כלומר, אינו מושפע מהחלפת α ו־β או α' ו־β') וסימטרי.

2. הראה שלכל $a \neq b$, קיים $\tau_{a,b} \in \mathrm{PGL}_2(F)$ (מסדר 2, עם נקודות שבת a, b בלבד), כך ש־$\{x, y\}$ שכן של $\{a, b\}$ אם ורק אם $y = \tau_{a,b} x$ (ולכן אם $|F| = q$ אז לכל זוג יש בדיוק $\frac{q-1}{2}$ שכנים). עבור $\{a, b\} = \{0, \infty\}$, $\tau_{0,\infty} x = -x$.

תרגיל 6.7.31 (***) בהמשך לתרגיל 6.7.30, נניח ש־$F = \mathbb{F}_5$.

1. הראה שיחס השכנות על 15 הזוגות של אברים ב־$F \cup \{\infty\}$ הוא יחס שקילות. (**הדרכה**. בדוק את הטענה עבור השכנים של $\{0, \infty\}$ והעזר ב־2־טרנזיטיביות; אשר שתכונה זו מיוחדת לשדה $\mathbb{F}_5$.) הראה שכל מחלקת שקילות מהווה חלוקה של $F \cup \{\infty\}$ לשלושה זוגות זרים.

2. הראה ש־$\mathrm{PGL}_2(\mathbb{F}_5)$ פועלת נאמנה על חמש מחלקות השקילות. הסק, מהשוואת סדרים, ש־$\mathrm{PGL}_2(\mathbb{F}_5) \cong S_5$. הסק מכאן ש־$\mathrm{PSL}_2(\mathbb{F}_5) \cong A_5$.

3. לפי תרגיל 6.7.10, $\mathrm{PGL}_2(\mathbb{F}_5) \hookrightarrow S_6$, דרך הפעולה על $F \cup \{\infty\}$. הראה שהתמונה היא עותק לא סטנדרטי של S_5 (ראה תרגיל 7.2.33).

תרגיל 6.7.32 (***) נוכיח ש־$\mathrm{PSL}_2(\mathbb{F}_7) \cong \mathrm{GL}_3(\mathbb{F}_2)$ (זוהי החבורה הפשוטה היחידה מסדר 168, ראה תרגיל 8.5.61). לשם כך נמצא פעולה של $\mathrm{PSL}_2(\mathbb{F}_7)$ על מרחב וקטורי תלת־ממדי מעל $\mathbb{F}_2$.

1. תהיינה $x_1, \dots, x_4 \in \hat{F} = \mathbb{F}_7 \cup \{\infty\}$ נקודות שונות. נסמן $\lambda = [x_1, x_2; x_3, x_4]$. הראה (בעזרת תרגיל 6.7.24) שהתכונה $\lambda + \lambda^{-1} = 1$ אינה תלויה בסדר הנקודות. נאמר שרביעיה בעלת תכונה זו היא **מאוזנת**.
2. הראה שבפירוק של $\hat{F}$ לאיחוד של שתי רביעיות, אם אחת מהן מאוזנת, כך גם השניה. (אינני מכיר הוכחה מחוכמת לטענה זו.)
3. יש $14 = \frac{2\cdot 8\cdot 7\cdot 6}{2\cdot 24}$ חלוקות של $\hat{F}$ לרביעיות מאוזנות. הראה ש־$\mathrm{PGL}_2(\mathbb{F}_7)$ פועלת נאמנה על קבוצת החלוקות המאוזנות. הראה שהפעולה טרנזיטיבית, ושבפעולת $\mathrm{PSL}_2(\mathbb{F}_7)$ יש שני מסלולים.
4. המסלולים של $\mathrm{PSL}_2(\mathbb{F}_7)$ מן הסעיף הקודם, שנסמן ב־X, X' בהתאמה, הם המסלולים של $\{0124|\infty356\}$ ושל $\{0356|\infty124\}$ תחת הפעולה $z \mapsto z+1$ ($1,2,4$ הם הריבועים בשדה $\mathbb{F}_7$).
5. הראה שלכל שתי חלוקות $(a|b), (a'|b') \in X$, $|a \cap a'| = 2$, ולכן הפעולה $(a|b) + (a'|b') = (a\Delta a'|b\Delta b')$ (כאשר Δ הוא ההפרש הסימטרי) מוגדרת היטב. הראה שהיא אסוציאטיבית.
6. נסמן ב־V את המרחב הוקטורי $X \cup \{0\}$ מעל $\mathbb{F}_2$, שממדו 3. הראה שפעולת $\mathrm{PSL}_2(\mathbb{F}_7)$ על V היא לינארית, והסק את האיזומורפיזם הדרוש.

בספרות מופיעות כמה וכמה הוכחות לכך ש־$\mathrm{GL}_4(\mathbb{F}_2) \cong A_8$ (כמה מהן מוצגות בפירוט בעמודים הבאים).

1. על־ידי שיכון $\mathrm{Aff}_3(\mathbb{F}_2) = \mathrm{GL}_3(\mathbb{F}_2) \ltimes \mathbb{F}_2^3$ כתת־חבורה (מאינדקס 15) ב־A_8.

זו ההוכחה הראשונה לאיזומורפיזם, והיא ניתנה על־ידי Camile Jordan, בסעיף 516 של Traite des substitutions et des equations algebraiques, 1870.

2. על־ידי השוואת השיכונים השונים של $\mathbb{Z}_2^3$ ב־A_8.

את ההוכחה הזו הציע J.H. Conway, סעיף 1.4 ב־Three Lectures on exceptional groups (הרצאות אלה הן פרק ב־"Finite Simple Groups", M.B.Powell and G.Higman, eds., Academic Press, 1971; וגם פרק 10 ב־Sphere Packings, Lattices and Groups, J.H. Conway ו־N.J.A. Sloane). גרסה מורחבת מציג John Murray, The alternating group A_8 and the general linear group $\mathrm{GL}_4(2)$, Math Proc Royal Irish Acad, **99A**(2), 123–132, 1999.

3. על־ידי הפעולה של $\mathrm{GL}_4(\mathbb{F}_2)$ על שמונת ה"הפטאדים". מטריצה $A \in \mathrm{M}_4(\mathbb{F}_2)$ היא **א־סימטרית** אם $A + A^{\mathrm{t}} = 0$; מטריצה א־סימטרית הפיכה נקראת **בורג** (screw; יש 28 כאלה); שני ברגים הם **בלתי־מתואמים** (azygetic) אם סכומם הוא בורג (כל בורג הוא בלתי־מתואם עם 12 אחרים); **הפטאד** הוא קבוצה של שבעה ברגים שהם בלתי־מתואמים בזוגות (ו־$\mathrm{GL}_4(\mathbb{F}_2)$ פועלת על ההפטאדים על־ידי כפל משמאל). [זו ההוכחה הדומה ביותר לתרגיל 6.7.27.] מתברר שכל בורג מוכל בדיוק בשני הפטאדים; שכל ששה ברגים בהפטאד הם בלתי־תלויים לינארית, ולכן סכום כל השבעה הוא אפס; ומכאן ש־21 הברגים שמחוץ להפטאד הם סכומי הזוגות של ברגים בהפטאד. לברגים וההפטאדים יש פירוש גאומטרי: כל בורג מתאים ל־15 מבין 35 המישורים (אלו הם המישורים האיזוטרופיים ביחס לבורג); כל מישור ב־$\mathbb{F}_2^4$ מתאים לחלוקה יחידה של ההפטאדים לרביעיות (שני הפטאדים נמצאים באותו חלק אם המישור שייך לבורג

המשותף שלהם); ומישורים נחתכים אם החלוקות שלהם מתקבלות מהחלפת זוג הפטאדים. כל שני ברגים בלתי־מתואמים נחתכים בחמישה מישורים, המכסים את כל הנקודות במרחב; אם σ, σ' ברגים בלתי־מתואמים, אז גם $\sigma'' = \sigma + \sigma'$ מכיל את אותם מישורים; וכל חמישיה מוכלת בשלשה יחידה של ברגים בלתי־מתואמים.

ההוכחה מתוארת בהרחבה אצל W.L. Edge, *The Geometry of the Linear Fractional Group* LF$(4,2)$, London Math Soc **4**(3), 1954; היא מבוססת על E.H. Moore, Math. Annalen **51**, 417–444, 1899.

4. על־ידי שיכון $A_7 \hookrightarrow \mathrm{GL}_4(\mathbb{F}_2)$ בעזרת שיכון $\mathrm{GL}_3(\mathbb{F}_2) \hookrightarrow A_7$ (תרגיל **6.7.33**).

הוכחה זו, של נעם אלקיס, לקוחה מ־`http://www.math.harvard.edu/~elkies/Misc/A8.pdf`.

5. על־ידי שיכון A_8 ו־$\mathrm{GL}_4(\mathbb{F}_2)$ בתת־החבורה $\Omega_6^+(2)$ של $\mathrm{GL}_6(\mathbb{F}_2)$, שהיא חבורת האוטומורפיזמים של תבנית ריבועית היפרבולית (תרגילים **6.7.36-6.7.38**).

   על־פי Robert A. Wilson, "The Finite Simple Groups", 2009, סעיף 3.12.1.

6. על־ידי שיכון $\mathrm{GL}_4(\mathbb{F}_2)$ בחבורת מתיו M_{24} (תרגיל **6.7.39**).

   מתוך J.J. Rotman, "Introduction to the Theory of Groups", משפט 9.71.

7. בעזרת התכונות של חבורת מתיו M_{24}, המוגדרת (כאן) כתת־חבורה של S_{24} המכילה את $\mathrm{PSL}_2(\mathbb{F}_{23})$; ההוכחה מבוססת על כך ש־$M_{24}$ היא חבורת האוטומורפיזמים של קוד Golay הבינארי ממימד 12.

   את ההוכחה הזו, גם היא של קונווי, אפשר למצוא במשפט 10 (סעיף 2.2) של ה־Three Lectures on exceptional groups.

תרגיל 6.7.33 (***) נוכיח ש־$\mathrm{GL}_4(\mathbb{F}_2) \cong A_8$.

1. בדוק ש־$|\mathrm{GL}_4(\mathbb{F}_2)| = |A_8| = 20160$.
2. אם ל־$\mathrm{GL}_4(\mathbb{F}_2)$ יש תת־חבורה מאינדקס 8 אז סיימנו. **הדרכה.** העידון של משפט קיילי.
3. הסבר כיצד הפעולה של $H = \mathrm{GL}_3(\mathbb{F}_2)$ על הנקודות במישור פאנו, משרה שיכון $\mathrm{GL}_3(\mathbb{F}_2) \hookrightarrow A_7$ (ההוכחה שדווקא לתמורות הזוגיות: לפי יוצרים). לפי חישוב הסדרים, $[A_7 : H] = 15$.
4. הגדר פעולת חיבור על $V = \{0\} \cup (A_7/H)$, ההופכת את הקבוצה הזו למרחב וקטורי ארבעה־ממדי מעל $\mathbb{F}_2$. לשם כך מזהים את S_7/H עם אוסף הדרכים לשיים שבע נקודות במישור פאנו, ואז $X = A_7/H \subseteq S_7/H$ הם השיומים שהתקבלו מהפעלת תמורה זוגית על השיום הסטנדרטי. לכל $P, P' \in X$ יש ישר משותף יחיד (על־ידי ספירה: כל ישר אפשר להמשיך לשיום זוגי ב־3 דרכים בדיוק).
5. החיבור ב־$X \cup \{0\}$ מוגדר כך ש־$P + P' + P'' = 0$ אם יש להם ישר משותף. מכיוון ש־A_7 פועל טרנזיטיבית על $\frac{1}{2}7! = 15 \cdot 14 \cdot 12$ השלשות P, Q, R שאין להם ישר משותף, די לבדוק את האסוציאטיביות $(P+Q)+R = P+(Q+R)$ פעם אחת.
6. הראה שהפעולה הטבעית של A_7 על V שומרת על החיבור שהוגדר בסעיף הקודם.
7. ממילא מתקבל שיכון $A_7 \hookrightarrow \mathrm{GL}_4(\mathbb{F}_2)$, והאינדקס הוא 8. לפי סעיף 2, $\mathrm{GL}_4(\mathbb{F}_2) \cong A_8$.
8. נסמן ב־$\theta : \mathrm{GL}_4(\mathbb{F}_2) \to \mathrm{GL}_4(\mathbb{F}_2)$ את האוטומורפיזם $\theta(x) = (x^{\mathrm{t}})^{-1}$. אז $S_8 \cong \langle \mathrm{GL}_4(\mathbb{F}_2), \theta \rangle$.

שני התרגילים הבאים עוסקים במשפחה של חבורות אורתוגונליות.

תרגיל 6.7.34 (***) נסמן ב־$b_m(x,y) = x_1y_2 + \cdots + x_{2m-1}y_{2m}$ את התבנית הבילינארית ההיפרבולית על המרחב $\mathbb{F}_2^{2m}$, ו־$q_m(x) = b_m(x,x)$.

1. וקטור $x \in \mathbb{F}_2^{2m}$ הוא **איזוטרופי** אם $q(x) = 0$. הראה שיש במרחב $(2^m-1)(2^{m-1}+1)$ וקטורים איזוטרופיים. **הדרכה.** אם $X \sim b(p)$, $X' \sim b(p')$ משתנים מקריים בלתי תלויים בעלי התפלגות ברנולי, אז "$q-p$" של $X \oplus X'$ שווה ל־$(q-p)(q'-p')$.
2. תת־מרחב $U' \subseteq \mathbb{F}_2^m$ הוא **איזוטרופי לחלוטין** אם כל הווקטורים שלו איזוטרופיים. כל תת־מרחב איזוטרופי לחלוטין מקסימלי הוא מממד m. הראה של־U יש $\prod_{i=0}^{m-1}(2^i+1)$ תת־מרחבים איזוטרופיים מקסימליים. (זהו פעמיים מספר זוגי.)

תרגיל 6.7.35 (***) בהמשך לתרגיל 6.7.34, נסמן $f_m(x,y) = b_m(x,y) + b_m(y,x)$.

1. נסמן ב־$\mathrm{GO}_{2m}^+(2) = \{T \in \mathrm{GL}_{2m}(\mathbb{F}_2) :\ q_m(Tx) = q_m(x)\}$ את חבורת האוטומורפיזמים של המרחב הריבועי $(\mathbb{F}_2^{2m}, q_m)$. הראה ש־$\mathrm{GO}_{2m}^+(2)$ פועל טרנזיטיבית על קבוצת הווקטורים האיזוטרופיים. על־ידי חישוב המייצב, הראה ש־
$$\left|\mathrm{GO}_{2m}^+(2)\right| = 2 \cdot 2^{m(m-1)}(2^2-1)\cdots(2^{2m-2}-1)(2^m-1).$$
2. נסמן ב־$t_x : y \mapsto y + f_m(x,y)x$ את העתקת ההסטה, כאשר $q_m(x) = 1$. הראה ש־$t_x \in \mathrm{GO}_{2m}^+(2)$, וש־$t_x^2 = 1$. **הערה.** $\mathrm{GO}_{2m}^+(2)$ נוצרת על־ידי ההסטות.
3. נסמן ב־M את קבוצת תת־המרחבים האיזוטרופיים המקסימליים. הראה שלכל $U' \in M$, $t_x(U') \neq U'$. לכן, בפעולה על M, כל t_x הוא מכפלה של חילופים ללא נקודות שבת (ולפי סעיף 2 של תרגיל 6.7.34 זו תמורה אי־זוגית).
4. נסמן ב־$\Omega_{2m}^+(2)$ את תת־החבורה מאינדקס 2 של $\mathrm{GO}_{2m}^+(2)$ שאבריה פועלים כתמורות זוגיות על M. אז $\left|\Omega_{2m}^+(2)\right| = \frac{1}{2}\left|\mathrm{GO}_{2m}^+(2)\right|$.

שלושת התרגילים הבאים מציעים הוכחה נוספת לכך ש־$A_8 \cong \mathrm{GL}_4(\mathbb{F}_2)$.

תרגיל 6.7.36 (**) בהמשך לתרגיל 6.7.35, הראה ש־$\left|\Omega_6^+(2)\right| = 20160$.

תרגיל 6.7.37 (***) שיכון של $\mathrm{GL}_4(\mathbb{F}_2)$ ב־$\Omega_6^+(2)$:

1. נקבע בסיס $\{e_1,e_2,e_3,e_4\}$ למרחב $V = \mathbb{F}_2^4$. נסמן ב־$V \otimes V$ את המרחב עם הבסיס $\{e_i \otimes e_j :\ i,j = 1,\dots,4\}$. נסמן ב־$v \wedge w$ את התמונה של $v \otimes w$ במרחב המנה $V \wedge V = V \otimes V / \mathrm{span}\{v \otimes v :\ v \in V\}$. כך, הוקטורים $e_i \wedge e_j$ $(i \neq j)$ מהווים בסיס של $V \wedge V$. לכן $\dim(V \wedge V) = 6$.
2. כל העתקה לינארית $T : V \to V$ משרה העתקה $x \wedge y \mapsto T(x) \wedge T(y)$ על $V \wedge V$. כך מתקבל שיכון $\mathrm{PGL}_4(\mathbb{F}_2) \hookrightarrow \mathrm{GL}_6(\mathbb{F}_2)$.
3. נגדיר תבנית ריבועית על $V \wedge V$ לפי $q(\sum \alpha_{ij} \cdot e_i \wedge e_j) = \sum_{ij|k\ell} \alpha_{ij}\alpha_{k\ell}$ כאשר הסכום באגף ימין הוא על כל החלוקות של $\{1,2,3,4\}$. התבנית q היא היפרבולית.
4. השיכון $T \mapsto T \wedge T$ משכן את $\mathrm{GL}_4(\mathbb{F}_2)$ בתוך $\mathrm{GO}_6^+(2)$. **הדרכה.** מספיק לבדוק את הטענה על קבוצת יוצרים של $\mathrm{GL}_4(\mathbb{F}_2)$.
5. $\mathrm{GL}_4(\mathbb{F}_2) \hookrightarrow \Omega_6^+(2)$ (**הדרכה.** $\Omega_6^+(2)$ פשוטה), וזהו איזומורפיזם לפי השוואת הסדרים.

תרגיל 6.7.38 **(***)** שיכון של A_8 ב־$\Omega_6^+(2)$:

1. נגדיר על המרחב $W = \mathbb{F}_2^8$ תבנית בילינארית לפי $(x,y) = \sum x_i y_i$. נסמן $j = (1,1,1,1,1,1,1,1)$. המרחב $j^\perp/\langle j \rangle$ הוא ממימד 6, והתבנית הריבועית המושרית עליו מ־W היא היפרבולית.
2. יש פעולה טבעית של S_8 על W, השומרת על j, ולכן משרה פעולה על $j^\perp/\langle j \rangle$.
3. פעולת S_8 על $j^\perp/\langle j \rangle$ שומרת על התבנית, ולכן מהווה שיכון $S_8 \subseteq \mathrm{GO}(j^\perp/\langle j \rangle, q)$ המשכן גם $A_8 \subseteq \Omega_6^+(2)$. לפי השוואת סדרים, החבורות שוות.

תרגיל 6.7.39 **(***+)** (סקירה של הוכחה שלישית לאיזומורפיזם $A_8 \cong \mathrm{PSL}_4(\mathbb{F}_2)$) משפחה של תת־קבוצות בגודל t של קבוצה X בגודל n נקראת **מערכת שטיינר** $S(k,t,n)$, אם כל תת־קבוצה בגודל k של X מוכלת באיבר יחיד של המשפחה.

1. קיימת מערכת שטיינר (יחידה) עם הפרמטרים $S(5,8,24)$, שהמרחב עליו היא בנויה הוא המישור הפרויקטיבי $\mathbb{P}^2\mathbb{F}_4$ ועוד שלוש נקודות.
2. חבורת האוטומורפיזמים של $S(5,8,24)$ היא תת־חבורה (פשוטה ו־5־טרנזיטיבית) של S_{24}, המכילה את $\mathrm{PSL}_3(\mathbb{F}_4)$, והיא מסדר $48 \cdot \frac{24!}{19!}$. זוהי **חבורת מתיו** M_{24}.
3. נסמן ב־H את המייצב של חמש נקודות ב־M_{24} (לכן $|H| = 48$); מתברר ש־H מכילה את $U = \left\{ \begin{pmatrix} 1 & 0 & \alpha \\ 0 & 1 & \beta \\ 0 & 0 & 1 \end{pmatrix} : \alpha, \beta \in \mathbb{F}_4 \right\}$, שהיא איזומורפית ל־$\mathbb{Z}_2^4$, ולכן $N \hookrightarrow \mathrm{Aut}(U) \cong \mathrm{GL}_4(\mathbb{F}_2)$.
4. ל־U יש שמונה נקודות שבת משותפות; המנרמל $N = \mathrm{N}_G(U)$ פועל על שמונה הנקודות האלה, ולכן יש לו שיכון ב־S_8; והוא איזומורפי ל־A_8. מכאן ש־$A_8 \cong \mathrm{Aut}(U)$.

בתרגיל 8.4.47 נוכיח שהחבורות A_8 ו־$\mathrm{PSL}_3(\mathbb{F}_4)$ אינן איזומורפיות (למרות ששתיהן פשוטות ובעלות אותו סדר!)

פרק 7

אוטומורפיזמים

בפעולה על קבוצה נטולת מבנה, הדרישה היחידה היא שאברי החבורה הפועלת יהיו הפיכים. אם לקבוצה יש מבנה נוסף, הגיוני לדרוש שהפעולה תשמור על המבנה הזה. לדוגמא, בפעולות על הישר הממשי $\mathbb{R}$ נצפה שאברי החבורה יהיו פונקציות רציפות הפיכות, ולא סתם פונקציות הפיכות. בפרק זה נבדוק בעיקר את הפעולות על קבוצה שהיא בעצמה חבורה.

בעוד שהפרק הקודם עוסק בפעולה של G על מרחבים מתאימים, חבורת האוטומורפיזמים של G היא החבורה הגדולה ביותר הפועלת על G עצמה, תוך שמירה על פעולת הכפל שלה. בנייה של אוטומורפיזמים עשויה להיות אתגר לא פשוט; אנו מסתפקים ברעיון הבסיסי של אוטומורפיזמים פנימיים. הפאשרות של חבורה אחת לפעול על חבורה אחרת (כחבורת אוטומורפיזמים) מוליך לבניה של **מכפלה ישרה למחצה**, המכליל את המכפלה הישרה. כמו במכפלה ישרה, המושגים של מכפלה ישרה למחצה **חיצונית** ו**פנימית** מתלכדים. סעיף 7.4, שבדרך כלל אינו שייך לקורס ראשון בתורת החבורות, מראה כיצד אפשר לארגן את כל המכפלות הישרות למחצה, ואת כל ההרחבות מודולו המכפלות הישרות למחצה, במבנה של חבורות אבליות.

7.1 חבורת האוטומורפיזמים

הגדרה 7.1.1 *תהי G חבורה. איזומורפיזם $G \to G$ נקרא* ***אוטומורפיזם****. אוסף האוטומורפיזמים הוא* ***חבורת האוטומורפיזמים*** *של G, ומסמנים אותו ב־$\mathrm{Aut}(G)$.*

תרגיל 7.1.2 (+*) הראה ש־$\mathrm{Aut}(G)$ פועלת על G, ולכן היא תת־חבורה של חבורת התמורות S_G.

(ידוע שאם G חבורה סופית אז הסדר של כל $\sigma \in \mathrm{Aut}(G)$ קטן מ־$|G|$. משפט זה אינו נובע מן התרגיל, כמובן; זהו משפט 2 ב־M.V. Horosevskii, "On Automorphisms of finite groups", Mat. Sbornik **22**(4), (1974); ההוכחה מבוססת על שימוש ברדיקל הפתיר, המוגדר בתרגיל 10.3.64.)

תרגיל 7.1.3 (**) תהי G חבורה הנוצרת על־ידי אברים $g_1, \dots, g_t$. אם $\varphi, \psi \in \mathrm{Aut}(G)$ ו־$\varphi(g_i) = \psi(g_i)$, אז $\varphi = \psi$. כלומר, כדי להגדיר אוטומורפיזמים, די להגדיר אותו על קבוצת יוצרים (בדומה ל'משפט ההגדרה' על העתקות לינאריות).

תרגיל 7.1.4 (**) הוכח ש־$U_n \cong \mathrm{Aut}(\mathbb{Z}_n)$. **הדרכה.** הגדר $\Phi : \mathrm{Aut}(\mathbb{Z}_n) \to U_n$ לפי $\Phi(\phi) = \phi(1)$.

תרגיל 7.1.5 (**) $\mathrm{Aut}(\mathbb{Z}_2 \times \mathbb{Z}_2) \cong S_3$. (ראה תרגיל 6.7.19.)

תרגיל 7.1.6 (**) $\mathrm{Aut}(\mathbb{Z}) \cong \mathbb{Z}_2$.

תרגיל 7.1.7 (**) הוכח ש־$\mathrm{Aut}(S_3) \cong S_3$.

תרגיל 7.1.8 (+)** חבורת האוטומורפיזמים של $\mathbb{Z}_p^n = \mathbb{Z}_p \times \cdots \times \mathbb{Z}_p$ היא חבורת המטריצות $\mathrm{GL}_n(\mathbb{F}_p)$. **הדרכה.** זו בעיה באלגברה לינארית.

תרגיל 7.1.9 (+)** הראה שהסדר של $\mathrm{Aut}(\mathbb{Z}_4 \times \mathbb{Z}_4)$ הוא 96. **הדרכה.** מצא התאמה $\mathrm{Aut}(\mathbb{Z}_4^2) \to \mathrm{M}_2(\mathbb{Z}_4)$.

תרגיל 7.1.10 (-)**
1. לכל G, H יש שיכון $\mathrm{Aut}(G) \times \mathrm{Aut}(H) \hookrightarrow \mathrm{Aut}(G \times H)$.
2. כאשר $(|G|, |H|) = 1$, השיכון הזה הוא איזומורפיזם, ולכן $\mathrm{Aut}(G \times H) \cong \mathrm{Aut}(G) \times \mathrm{Aut}(H)$.

תרגיל 7.1.11 (-*)** תהי G חבורה סופית, ו־$\varphi \in \mathrm{Aut}(G)$ אוטומורפיזם שנקודת השבת היחידה שלו היא איבר היחידה.

1. הוכח: לכל g קיים x כך ש $g = x^{-1}\varphi(x)$.
2. אם $\varphi \circ \varphi = I_G$, אז G אבלית.

תרגיל 7.1.12 (-*)** הוכח ש־$\mathrm{Aut}(Q_8) \cong S_4$. **הדרכה.** כתוב את האברים $i, -i$, $j, -j$, $k, -k$ על הפאות המנוגדות של קוביה C, והראה שיש שיכון $\mathrm{Aut}(Q_8) \to \mathrm{Aut}(C) \cong S_4$ (בתרגיל 7.5.8). הראה ש־$i \leftrightarrow j,\ k \mapsto -k$ הוא אוטומורפיזם המחליף שני אלכסונים בקוביה, ולכן השיכון הוא על.

תרגיל 7.1.13 (***) חשב את $\mathrm{Aut}(\mathbb{Z}_2 \times \mathbb{Z}_4)$.

תרגיל 7.1.14 (+)** הוכח ש־$\mathrm{Aut}(\mathbb{Z}_2 \times \mathbb{Z}) \cong \mathbb{Z}_2 \times \mathbb{Z}_2$. **הדרכה.** מהם האיברים מסדר 2 של $\mathbb{Z}_2 \times \mathbb{Z}$?

נזכיר ש־$\mathbb{F}_n$ היא החבורה החופשית על n יוצרים.

תרגיל 7.1.15 (***) הוכח שלכל $1 \neq w \in \mathbb{F}_n$, $\mathrm{C}_{\mathbb{F}_n}(w) \cong \mathbb{Z}$.

תרגיל 7.1.16 (+**)** הוכח ש־$\mathrm{Aut}(\mathbb{F}_n \times \mathbb{F}_n)$, $n > 1$, נוצרת על־ידי האוטומורפיזמים על שני המרכיבים ועל־ידי האוטומורפיזם $(x, y) \mapsto (y, x)$. **הדרכה.** המרכז של איבר $(a, b) \neq (1, 1)$ איזומורפי ל־$\mathbb{Z} \times \mathbb{F}_n$ אם $a = 1$ או $b = 1$, ול־$\mathbb{Z} \times \mathbb{Z}$ אם $a, b \neq 1$. תת־החבורות המקסימליות של $\{x :\ \mathrm{C}_x(x)' \neq 1\}$ הן שני הגורמים הקנוניים $\mathbb{F}_n \times 1$ ו־$1 \times \mathbb{F}_n$.

הגדרה 7.1.17 ***תהי G חבורה. נסמן ב־$\mu_m : G \to G$ את פעולת ההעלאה בחזקה*** $\mu_m : g \mapsto g^m$.

תרגיל 7.1.18 (**) אם G אבלית ו־$(m, |G|) = 1$, אז μ_m הוא אוטומורפיזם.

הגדרה 7.1.19 ***תהי G חבורה אבלית. נסמן ב־$\exp(G)$ את הכפולה המשותפת המינימלית של כל הסדרים של אברים ב־G. (נחזור לנושא זה בסעיף 9.1).***

תרגיל 7.1.20 (**) אם G אבלית סופית אז יש שיכון $U_{\exp(G)} \hookrightarrow \mathrm{Aut}(G)$. הראה שהתמונה נורמלית ב־$\mathrm{Aut}(G)$.

תרגיל 7.1.21 (+*) $\mathrm{Inv} : g \mapsto g^{-1}$ הוא אוטומורפיזם אם ורק אם G אבלית, ואם G אבלית סופית הוא מהצורה μ_m עבור m מתאים.

7.2 אוטומורפיזמים פנימיים

בסעיף זה נכיר את אחת הדרכים הקלות לבנות אוטומורפיזמים של חבורה נתונה: הלא החבורה פועלת על עצמה בהצמדה, כפי שראינו בסעיף 6.4.

הגדרה 7.2.1 *תהי G חבורה. לכל איבר $g \in G$, נגדיר **אוטומורפיזם** $\gamma_g : G \to G$ לפי $\gamma_g(h) = ghg^{-1}$. כל אוטומורפיזם כזה נקרא **אוטומורפיזם פנימי**. האוסף $\mathrm{Inn}(G) = \{\gamma_g : \ g \in G\}$ הוא **חבורת האוטומורפיזמים הפנימיים** של G.*

תרגיל 7.2.2 (*) $\gamma_g \circ \gamma_h = \gamma_{gh}$.

תרגיל 7.2.3 (*) הוכח: $\gamma_g \in \mathrm{Aut}(G)$.

תרגיל 7.2.4 (**) נגדיר $\Gamma : G \to \mathrm{Aut}(G)$ לפי $\Gamma(g) = \gamma_g$.

1. הוכח ש־Γ הומומורפיזם (זהו תרגיל 7.2.2).
2. הראה ש־$\mathrm{Ker}(\Gamma) = \mathrm{Z}(G)$, והסק ש־$\mathrm{Inn}(G) \cong G/\mathrm{Z}(G)$.

תרגיל 7.2.5 (*-)** הוכח ש־$\mathrm{Aut}(S_4) \cong S_4$.

תרגיל 7.2.6 (*-)** הוכח ש־$\mathrm{Aut}(A_4) \cong S_4$.

תרגיל 7.2.7 (***) לאף חבורה סופית G לא יתכן ש־$\mathrm{Aut}(G) \cong \mathbb{Z}_3$.

תרגיל 7.2.8 (**) לכל G, H, $\mathrm{Inn}(G \times H) \cong \mathrm{Inn}(G) \times \mathrm{Inn}(H)$.

תרגיל 7.2.9 (**) נסמן $H = \langle (123), (456) \rangle \leq S_6$. תאר את $\mathrm{N}_{S_6}(H)$ ואת $\mathrm{C}_{S_6}(H)$, והוכיח ש־$\mathrm{N}_{S_6}(H)/\mathrm{C}_{S_6}(H) \cong D_4$.

משפט 7.2.10 (משפט N/C) *תהי $H \leq G$ תת־חבורה. אז קיים שיכון $\mathrm{N}_G(H)/\mathrm{C}_G(H) \hookrightarrow \mathrm{Aut}(H)$.*

תרגיל 7.2.11 (**) הוכח את המשפט. **הדרכה.** ההצמדה ב־$g \in G$ משרה אוטומורפיזם של H אם ורק אם $g \in \mathrm{N}_G(H)$. הגדר $\varphi : \mathrm{N}_G(H) \to \mathrm{Aut}(H)$ לפי $\varphi : g \mapsto \gamma_g|_N$. חשב את הגרעין של ההעתקה.

תרגיל 7.2.12 (*) נסח את משפט N/C במקרה $H = G$.

תרגיל 7.2.13 (**) תהי G חבורה (אינסופית), ו־$N \triangleleft G$ תת־חבורה נורמלית סופית. הראה ש־$\mathrm{C}_G(N)$ מאינדקס סופי ב־G.

תרגיל 7.2.14 (**) הראה ש־$\mathrm{Inn}(G) \triangleleft \mathrm{Aut}(G)$. **הדרכה.** $\varphi \circ \gamma_g \circ \varphi^{-1} = \gamma_{\varphi(g)}$ לכל $\varphi \in \mathrm{Aut}(G)$ ו־$g \in G$.

את חבורת המנה מסמנים ב־$\mathrm{Out}(G) = \mathrm{Aut}(G)/\mathrm{Inn}(G)$, והיא נקראת **חבורת האוטומורפיזמים החיצוניים** של G (למרות שאבריה אינם אוטומורפיזמים).

תרגיל 7.2.15 (**) הראה שיש העתקה $\mathrm{Out}(G) {\to} \mathrm{Aut}(\mathrm{Z}(G))$ המוגדרת על־ידי $[\sigma] \mapsto \sigma|_{\mathrm{Z}(G)}$.

תרגיל 7.2.16 (+)** לכל G, H יש שיכון $\mathrm{Out}(G) \times \mathrm{Out}(H) \hookrightarrow \mathrm{Out}(G \times H)$. **הדרכה.** תרגילים 7.1.10 ו־7.2.8.

תרגיל 7.2.17 (+)** בהמשך לתרגיל 7.1.12, הראה ש־$\mathrm{Out}(Q_8) \cong S_3$. על איזו קבוצה בגודל 3 פועלת החבורה הזו?

אם G חסרת מרכז, גם $\mathrm{Aut}(G)$ חסרת מרכז.

תרגיל 7.2.18 (**) נניח ש־$\mathrm{Z}(G) = 1$. הוכח ש־$\mathrm{C}_{\mathrm{Aut}(G)}(\mathrm{Inn}(G)) = 1$, ובפרט גם $\mathrm{Z}(\mathrm{Aut}(G)) = 1$.

תרגיל 7.2.19 (+)** $\sigma \in \mathrm{C}_{\mathrm{Aut}(G)}(\mathrm{Inn}(G))$ אם ורק אם $\alpha(g) = \sigma(g)g^{-1}$ הוא הומומורפיזם $\alpha\colon G \to \mathrm{Z}(G)$. (זו הכללה של תרגיל 7.2.18.)

תרגיל 7.2.20 (**) אם קיים g כך ש $gxg^{-1} = x^{-1}$ לכל x, אז G אבלית.

תרגיל 7.2.21 (***) נניח שבחבורה סופית G יש אוטומורפיזם $\sigma \in \mathrm{Aut}(G)$ כך שההסתברות ל־$\sigma(x) = x^{-1}$ (אם בוחרים את x בהתפלגות אחידה מן החבורה) גדולה מ־$3/4$. הראה ש־G אבלית ו־$\sigma = 1$. **הערה**. בחבורות $G = D_4 \times \mathbb{Z}_2^n$, עם $\sigma = 1$, ההסתברות שווה $3/4$.

תרגיל 7.2.22 (-*)** לכל חבורה אבלית A מסדר 3 או יותר, $\mathrm{Out}(A) = \mathrm{Aut}(A) \neq 1$. **הדרכה**. אם $x \mapsto x^{-1}$ טריוויאלי, אז A מרחב וקטורי מעל $\mathbb{F}_2$.

תרגיל 7.2.23 (-*)** לכל חבורה, פרט ל־$\{1\}$ ול־$\mathbb{Z}_2$, יש אוטומורפיזם לא טריוויאלי. **הדרכה**. אחרת $\mathrm{Inn}(G) = 1$ והחבורה אבלית; תרגיל 7.2.22.

הערה 7.2.24 ממשפט המיון לחבורות פשוטות סופיות נובע שלכל חבורה פשוטה סופית S, $\mathrm{Out}(S)$ היא חבורה פתירה (ראה הגדרה 10.2.1).

תרגיל 7.2.25 (+**)** (משפט נילסן) ההטלה $\mathbb{F}_2 \to \mathbb{Z}^2$ מגדירה אפימורפיזם $\mathrm{Aut}(\mathbb{F}_2) \to \mathrm{Aut}(\mathbb{Z}^2) = \mathrm{GL}_2(\mathbb{Z})$, שממנו נובע ש־$\mathrm{Out}(\mathbb{F}_2) \cong \mathrm{GL}_2(\mathbb{Z})$.

הגדרה 7.2.26 ***תהי G חבורה. אוטומורפיזם $\sigma \in \mathrm{Aut}(G)$ הוא שומר מחלקות צמידות אם לכל $g \in G$ יש $x \in G$ כך ש־$\sigma(g) = xgx^{-1}$. את אוסף האוטומורפיזמים האלה מסמנים ב־$\mathrm{Aut}_c(G)$.***

תרגיל 7.2.27 (*) $\sigma \in \mathrm{Aut}_c(G)$ אם ורק אם לכל מחלקת צמידות $[g] \subseteq G$ מתקיים $\sigma([g]) = [g]$.

תרגיל 7.2.28 (+)** הראה ש־$\mathrm{Inn}(G) \lhd \mathrm{Aut}_c(G) \lhd \mathrm{Aut}(G)$.

לאור תרגיל זה, אפשר לסמן $\mathrm{Out}_c(G) = \mathrm{Aut}_c(G)/\mathrm{Inn}(G)$. ידוע שיש חבורות־$p$ שעבורן $\mathrm{Out}_c(G)$ אינה אבלית. לא ידוע האם $\mathrm{Out}_c(G)$ פתירה (הגדרה 10.2.1) לכל חבורה סופית G.

תרגיל 7.2.29 (***) יהי $n = 2^t$ חזקת־2 כאשר $3 \leq t$. נתבונן בחבורה $G = \left\{\begin{pmatrix} a & x \\ 0 & 1 \end{pmatrix} : a \in U_n,\, x \in \mathbb{Z}_n\right\}$ שהיא מכפלה ישרה למחצה $\mathbb{Z}_n \rtimes U_n$, כאשר U_n משוכנת בפינה השמאלית העליונה (השווה לתרגיל 7.3.22). נסמן ב־$\phi\colon U_n \to \mathbb{Z}_n$ את ההטלה שהגרעין שלה הוא $\langle -1, U_n^2 \rangle$ (כך שהתמונה היא $\frac{n}{2}\mathbb{Z}_n$; ראה תרגיל 9.4.31). נגדיר $\sigma \in \mathrm{Aut}(G)$ לפי $\sigma\colon \begin{pmatrix} a & x \\ 0 & 1 \end{pmatrix} \mapsto \begin{pmatrix} a & x + \phi(a) \\ 0 & 1 \end{pmatrix}$.

1. הראה ש־σ אוטומורפיזם של G.
2. הראה ש־σ אינו פנימי.
3. הראה ש־σ שומר על מחלקות הצמידות של G. (זהו חלק מפתרון של Wall, 1947 לשאלה של ברנסייד מ־1911: האם יתכן אוטומורפיזם שאינו פנימי ושומר על מחלקות צמידות; ברנסייד מצא לכך דוגמא נגדית ב־1913.)
4. הראה ש־σ הוא האוטומורפיזם היחיד מודולו $\mathrm{Inn}(G)$ השומר על מחלקות צמידות. **הדרכה**. הראה ש־
$$G = \left\langle \alpha, \beta, \gamma \mid \alpha^2 = 1,\, \beta^{n/4} = 1,\, \gamma^n = 1,\, \alpha\beta = \beta\alpha,\, \alpha\gamma\alpha^{-1} = \gamma^{-1},\, \beta\gamma\beta^{-1} = \gamma^5 \right\rangle.$$
מחלקת הצמידות של γ היא $\{\gamma^a : a \in U_n\}$. הראה שמחלקות הצמידות של α, β הן $\{\alpha\gamma^{2i}\}$ ו־$\{\beta\gamma^{4j}\}$ בהתאמה, והראה ש־$\alpha\gamma^{2i}\beta\gamma^{4j} = \beta\gamma^{4j}\alpha\gamma^{2i}$ אם ורק אם $8j = -8i$. הראה שאם $4j = -4i$ אז האוטומורפיזם פנימי.

7.2.1 האוטומורפיזמים של S_n

תרגיל 7.2.30 (**) 1. הוכח שלכל $k \geq 2$ ו־$a \geq 1$, $(ka)! > k^a a!$.

2. יש יותר תמורות בעלות מבנה מחזורים $[1^{d+ak} \cdots k^0 \cdots]$ מאשר בעלות מבנה מחזורים $[1^d \cdots k^a \cdots]$. **הדרכה.** תרגיל 5.2.18.

3. אם $ka > 6$ אז $2(ka-2)! > k^a a!$. **הדרכה.** $k^a a^1 = (ka)(ka-k)(ka-2k) \cdots$. פרט לראשון, כל הגורמים האלה משתתפים במכפלה $(ka-2)(ka-1) \cdots$ שבאגף שמאל; וכשמצמצמים אותם נותר לפחות אחד הגורמים $(ka-2)$ או $(ka-3)$. אבל $2(ka-3) > ka$.

4. מחלקת הצמידות הכוללת את החילופים היא הקטנה ביותר ב־S_n מלבד המחלקה של תמורת היחידה, פרט ליוצאי הדופן הבאים: $[3^1]$ ב־S_3; $[4^1], [2^2]$ ב־S_4; $[3^2], [2^3]$ ב־S_6.

5. לכל $n \neq 6$, מחלקת הצמידות של החילופים שונה בגודלה מכל מחלקת צמידות אחרת של איברים מסדר 2.

בתרגיל 7.2.32 נגזור מעובדה זו מסקנה מעניינת.

6. ב־S_6 יש 15 חברים במחלקה של (12), ו־15 איברים במחלקה של $(12)(34)(56)$.

תרגיל 7.2.31 (**) הראה שכל אוטומורפיזם של S_n השומר את מחלקת הצמידות של החילופים, הוא פנימי. **הדרכה.** נקרא לקבוצת חילופים **כוכב** אם היא מהצורה $\{(1i), (2i), (3i), \dots\}$ לאיזשהו i, ו**קדם־כוכב** אם אף שניים מאיבריה אינם מתחלפים זה עם זה. הראה שכל קדם־כוכב מקסימלי ביחס להכלה, עם יותר משלושה חילופים, הוא כוכב. הסק שהאוטומורפיזם הנתון פועל על קבוצת הכוכבים, ולכן פועל על $\{1, \dots, n\}$.

תרגיל 7.2.32 (**) לכל $n \neq 6$, כל אוטומורפיזם של S_n הוא פנימי. **הדרכה.** תרגילים 7.2.30 ו־7.2.31.

בפעולה הטבעית של S_6 על קבוצה בגודל 6, המייצב של נקודה נקרא **עותק סטנדרטי** של S_5; שיכון $S_5 \hookrightarrow S_6$ שאינו מייצב נקודה נקרא **עותק לא סטנדרטי**.

תרגיל 7.2.33 (**) תהי H תת־חבורה מסדר 20 של S_5 (ראה תרגיל 6.6.65). הראה שפעולת S_5 על S_5/H, בהתאם לעידון של משפט קיילי, משרה שיכון $S_5 \to S_6$, שהתמונה שלו היא עותק לא סטנדרטי. **הדרכה.** נסמן ב־$\tilde{S}_5$ את תמונת S_5 ב־$G = S_6$ המוגדרת על־ידי הפעולה. נסמן ב־G_0 את המייצב של הנקודה H תחת הפעולה של S_6 על המרחב S_5/H (זה בוודאי עותק סטנדרטי); לפי תרגיל 6.3.21, המייצב של הנקודה תחת הפעולה של $\tilde{S}_5$ הוא H, כלומר $G_0 \cap \tilde{S}_5 = H$. אבל החיתוך של כל שני עותקים סטנדרטיים איזומורפי ל־S_4.

תרגיל 7.2.34 (***) יהי $S_5 \cong \tilde{S}_5 \leq S_6$ עותק לא סטנדרטי. הראה שפעולת S_6 על הקוסטים $S_6/\tilde{S}_5$ משרה שיכון $S_6 \hookrightarrow S_6$. הראה שהשיכון הזה הוא אוטומורפיזם שאינו פנימי, ובפרט $\mathrm{Out}(S_6) \neq 1$. **הדרכה.** הראה שהשיכון מעביר חילוף למכפלה של שלושה חילופים. הסק מתרגילים 7.2.31 ו־(6)7.2.30 ש־$\mathrm{Out}(S_6) \cong \mathbb{Z}_2$.

תרגיל 7.2.35 (+*)** יהי $S_5 \cong \tilde{S}_5 \leq S_6$ עותק לא סטנדרטי. הראה שהוא פועל 3־טרנזיטיבית בחדות על החלוקות של K_5 לזוגות זרים של מחומשים (תרגיל 6.6.65). לכן $\tilde{S}_5$ פועלת טרנזיטיבית על 10 החלוקות של המרחב בגודל 6 לשלשות זרות. עובדה זו מגדירה שיכון לא סטנדרטי $S_5 \hookrightarrow S_{10}$.

תרגיל 7.2.36 (+*)** מצא קשר בין תרגיל 6.7.27 (שם מצאנו לחבורה $\mathrm{PSL}_2(\mathbb{F}_9)$ הפועלת באופן טבעי על 10 נקודות פעולה על קבוצה בגודל 6) לבין תרגיל 7.2.35 (המתאר פעולה של תת־חבורה של S_6 על קבוצה בגודל 10).

7.2.2 אוטומורפיזמים יחסיים

ניתן לדלג בקריאה ראשונה.

הגדרה 7.2.37 *תהי $H \leq G$ תת־חבורה. נסמן*

$$\mathrm{Aut}(G,H) = \{\phi \in \mathrm{Aut}(G) \colon \ \phi(H) = H\}$$

ו־

$$\mathrm{Aut}^1(G,H) = \{\phi \in \mathrm{Aut}(G) \colon \ \forall h \in H, \phi(h) = h\}.$$

בהמשך לזה, נגדיר גם

$$\mathrm{Inn}(G,H) = \mathrm{Aut}(G,H) \cap \mathrm{Inn}(G),$$

$$\mathrm{Inn}^1(G,H) = \mathrm{Aut}^1(G,H) \cap \mathrm{Inn}(G).$$

$$\begin{tikzcd}
 & & \mathrm{Aut}(G) \arrow[dl, dash] \arrow[dd, dash] \\
G/\mathrm{Z}(G) \arrow[r, equal] & \mathrm{Inn}(G) \arrow[dd, dash] & \\
 & & \mathrm{Aut}(G,H) \arrow[dl, dash] \arrow[dd, dash] \\
\mathrm{N}_G(H)/\mathrm{Z}(G) \arrow[r, equal] & \mathrm{Inn}(G,H) \arrow[dd, dash] & \\
 & & \mathrm{Aut}^1(G,H) \arrow[dl, dash] \\
\mathrm{C}_G(H)/\mathrm{Z}(G) \arrow[r, equal] & \mathrm{Inn}^1(G,H) &
\end{tikzcd}$$

תרגיל 7.2.38 (**) נסמן ב־$\Gamma \colon G \to \mathrm{Inn}(G)$ את ההטלה הסטנדרטית, המוגדרת לפי $g \mapsto \gamma_g$. הוכח ש־$\mathrm{Aut}(G,H) \cap \mathrm{Inn}(G) = \Gamma(\mathrm{N}_G(H))$ ו־$\mathrm{Aut}^1(G,H) \cap \mathrm{Inn}(G) = \Gamma(\mathrm{C}_G(H))$.

תרגיל 7.2.39 (**) הוכח: $\mathrm{Aut}^1(G,H) \lhd \mathrm{Aut}(G,H)$.

תרגיל 7.2.40 (***) הוכח את ההכללה הבאה של משפט N/C (משפט 7.2.10): לכל $H \leq G$, $\mathrm{N}_G(H)/\mathrm{C}_G(H) \hookrightarrow \mathrm{Aut}(G,H)/\mathrm{Aut}^1(G,H) \hookrightarrow \mathrm{Aut}(H)$.

תרגיל 7.2.41 (-*)** הראה שבשיכון של תרגיל 7.2.40 לעיל, $\mathrm{N}_G(H)/\mathrm{C}_G(H) \lhd \mathrm{Aut}(G,H)/\mathrm{Aut}^1(G,H)$.

7.2.3 תת־חבורות אופייניות

הגדרה 7.2.42 *תת־חבורה $H \leq G$ נקראת **תת־חבורה אופיינית** אם לכל $\varphi \in \mathrm{Aut}(G)$, $\varphi(H) = H$. נסמן $H \sqsubseteq G$ (הסימון המקובל בספרות הוא $K \mathrm{char} G$).*

תרגיל 7.2.43 (*) כל תת־חבורה אופיינית היא נורמלית.

תרגיל 7.2.44 (*) אם $H \leq G$ ואין עוד תת־חבורות מאותו סדר, אז H אופיינית ב־G.

תרגיל 7.2.45 (**) כל תת־החבורות של חבורה ציקלית הן אופייניות.

תרגיל 7.2.46 (*) המרכז הוא תת־חבורה אופיינית.

תרגיל 7.2.47 (***) תהי G חבורה שאין לה תת־חבורות אופייניות לא טריוויאליות. הוכח ש־G מכפלה ישרה של עותקים איזומורפיים של אותה חבורה פשוטה. **הדרכה**. התבונן באוסף תת־החבורות הנורמליות המינימליות של G. **הערה**. האנלוגיה המשווה בין חבורות פשוטות למספרים הראשוניים (שיש להודות שאינה חזקה במיוחד) מתאימה לפי התרגיל הזה חבורות ללא תת־חבורות אופייניות לחזקות של מספרים ראשוניים.

תרגיל 7.2.48 (**) אופייניות אינה תורשתית: יהיו $N \leq K \leq G$ תת־חבורות. מ־$N \sqsubseteq G$ לא נובע $N \sqsubseteq K$ (השווה לתרגיל 3.3.14) **הצעה**. $G = D_4$, $N = \mathrm{Z}(D_4)$.

תרגיל 7.2.49 (**) (נורמליות אינה טרנזיטיבית) מ־ $G \sqsubseteq K \lhd N$ לא נובע $N \lhd G$. (השווה לתרגיל 3.3.15) **הצעה**. $G = A_4$, $K = \langle (12)(34), (13)(24) \rangle$, $N = \langle (12)(34) \rangle$.

תרגיל 7.2.50 (**) (אופייניות היא טרנזיטיבית) נניח $N \sqsubseteq K \leq G$.

1. אם $K \lhd G$ אז $N \lhd G$.
2. אם $K \sqsubseteq G$ אז $N \sqsubseteq G$.

תרגיל 7.2.51 (+)** תת־חבורה של תת־חבורה ציקלית נורמלית, גם היא נורמלית.

תרגיל 7.2.52 (**) נניח ש־$K \leq H \leq G$, ו־K אופיינית ב־H. הראה ש־$\mathrm{N}_G(H) \subseteq \mathrm{N}_G(K)$.

הגדרה 7.2.53 ***התשתית של חבורה G היא תת־החבורה $\mathrm{soc}(G)$ הנוצרת על־ידי תת־החבורות הפשוטות המינימליות.***

תרגיל 7.2.54 (**) התשתית היא תת־חבורה אופיינית.

תרגיל 7.2.55 (*-)** בחבורה סופית, התשתית היא מכפלה ישרה של תת־חבורות נורמליות פשוטות.

7.3 מכפלה ישרה למחצה

7.3.1 מכפלה ישרה למחצה פנימית

כשהגדרנו מכפלה ישרה (פנימית) בסעיף 4.3, קראנו לתת־חבורות $K, Q \leq G$ **משלימות** אם $K \cap Q = 1$ ו־$KQ = G$. לפי תרגיל 4.3.3, נובע מכאן שכל איבר של G אפשר להציג באופן יחיד כאיבר במכפלה KQ.

הגדרה 7.3.1 ***אם $K, Q \leq G$ משלימות ו־$K \lhd G$, אומרים ש־G היא מכפלה ישרה למחצה (פנימית) של K ב־Q.***

כדי לציין ש־G מכפלה ישרה למחצה של K ב־Q, כותבים $G = K \rtimes Q$ (הצד הפתוח של הסימן $\rtimes$ מופנה כלפי תת־החבורה הנורמלית). כפי שנראה בהמשך, ידיעת K, Q (עד כדי איזומורפיזם) לא מספיקה כדי להגדיר מהי בדיוק החבורה $G = K \rtimes Q$.

תרגיל 7.3.2 (*) כל מכפלה ישרה היא בפרט ישרה למחצה.

תרגיל 7.3.3 (*) נניח ש־$G = K \rtimes Q$. אם $Q \lhd G$ אז $G \cong K \times Q$.

תרגיל 7.3.4 (**) נניח ש־$G = K \rtimes Q$. הוכח ש־$G/K \cong Q$. **הדרכה**. התבונן בתמונת Q תחת $g \mapsto Kg$ (העזר במשפט האיזומורפיזם השני).

תרגיל 7.3.5 (**) תהי $K \lhd G$, ונניח שיש תת־חבורה סופית $Q \leq G$ כך ש־$Q \cap K = 1$ ו־$G/K \cong Q$. הוכח ש־$G = K \rtimes Q$. **הערה**. חשוב: האם חיוני להניח ש־Q סופית?

תרגיל 7.3.6 (-*)** נניח ש־$G = K \rtimes Q$. אז $q \mapsto \gamma_q|_K$ מגדיר הומומורפיזם $Q{\to}\mathrm{Aut}(K)$.

תרגיל 7.3.7 (**) בתרגיל 7.3.5, אם מוותרים על ההנחה $Q \cap K = 1$, יתכן ש־G אינה מכפלה ישרה למחצה של K באף תת־חבורה. **הצעה.** $G = \mathbb{Z}_4$.

תרגיל 7.3.8 (**) חבורת המטריצות $\left\{\begin{pmatrix}\alpha & x\\ 0 & 1\end{pmatrix} :\ \alpha \in F^\times, x \in F\right\}$ היא מכפלה ישרה למחצה $F^\times \ltimes F^+$, כאשר F^+ היא החבורה החיבורית של השדה, ו־$F^\times$ פועלת על F^+ באופן הטבעי.

תרגיל 7.3.9 (*) S_n היא מכפלה פנימית ישרה למחצה של A_n ב־$\langle(12)\rangle$.

תרגיל 7.3.10 (**) גם $\mathbb{Z}_6$ וגם S_3 הן מכפלות ישרות למחצה של (תת־חבורה איזומורפית ל־)$\mathbb{Z}_3$ ב(תת־חבורה איזומורפית ל־)$\mathbb{Z}_2$. עם זאת, S_3 אינה מכפלה ישרה־למחצה של $\mathbb{Z}_2$ ב־$\mathbb{Z}_3$.

תרגיל 7.3.11 (**) נניח ש־$\varphi : H \to G$, $\psi : G \to H$ הומומורפיזמים כך ש־$\psi \circ \varphi = \mathrm{id}_H$.

1. φ חד־חד־ערכית, ψ על.
2. $G = \mathrm{Ker}(\psi) \rtimes \mathrm{Im}(\varphi)$.

תרגיל 7.3.12 (**) [הכיוון ההפוך לתרגיל 7.3.11] נניח ש־$G = K \rtimes Q$. הראה שקיימים הומומורפיזמים $\varphi : Q \to G$, $\psi : G \to Q$ המקיימים $\psi \circ \varphi = \mathrm{id}_Q$, כך ש־ $K = \mathrm{Ker}\psi$ ו־$Q = \mathrm{Im}\varphi$.

תרגיל 7.3.13 (-*)** תהי G חבורה סופית, ויהי $\psi : G{\to}G$ הומומורפיזם. אם $\mathrm{Ker}(\psi) \cap \mathrm{Im}(\psi) = 1$, אז $G = \mathrm{Ker}(\psi)\mathrm{Im}(\psi)$ ולכן $G = \mathrm{Ker}(\psi) \rtimes \mathrm{Im}(\psi)$. **הדרכה.** הראה ש־$\mathrm{Im}(\psi)\mathrm{Ker}(\psi)/\mathrm{Ker}(\psi) = G/\mathrm{Ker}(\psi)$.

תרגיל 7.3.14 (-*)** תהי G חבורה, ותהי $\psi : G{\to}G$ **הטלה**, כלומר הומומורפיזם המקיים $\psi{\circ}\psi = \psi$.

1. $\mathrm{Ker}(\psi) \cap \mathrm{Im}(\psi) = 1$.
2. $G = \mathrm{Ker}(\psi)\mathrm{Im}(\psi)$.
3. $G = \mathrm{Ker}(\psi) \rtimes \mathrm{Im}(\psi)$.

תרגיל 7.3.15 (**) תהי $\psi : G{\to}G$ הטלה.

1. הוכח ש־$\mathrm{Ker}(\psi) = \left\{x \cdot \psi(x)^{-1} :\ g \in G\right\}$ (השווה לתרגיל 7.1.11).
2. נניח ש־$G = \langle g_1, \ldots, g_n\rangle$. הוכח ש־$\mathrm{Ker}(\psi)$ היא תת־החבורה הנורמלית הנוצרת על־ידי האיברים $g_i \cdot \psi(g_i)^{-1}$.

תרגיל 7.3.16 (**) הצגה נוספת של S_4 כמכפלה ישרה למחצה:

1. הראה ש־$S = \{\sigma : \sigma(4) = 4\}$ הוא עותק של S_3 בתוך S_4.
2. הראה ש $-$ $K_4 = \langle(12)(34), (13)(24)\rangle$ תת־חבורה נורמלית של S_4.
3. הראה ש־S_4 מכפלה פנימית ישרה למחצה של K ב־S.

7.3.2 מכפלה ישרה למחצה חיצונית

תהיינה K,Q חבורות. בסעיף זה נבנה מכפלות ישרות למחצה של K ב־Q. לפי תרגיל 7.3.6, כל מכפלה ישרה למחצה מגדירה הומומורפיזם $\theta:Q\to\mathrm{Aut}(K)$ (שנסמן $\theta:q\mapsto\theta_q$), כך ש־$qk=\theta_q(k)q$.

המצרכים בבניית מכפלה ישרה למחצה: גרעין K, חבורת מנה Q, ופעולה θ של Q של K.

הגדרה 7.3.17 *יהי $\theta:Q\to\mathrm{Aut}(K)$ הומומורפיזם.* ***המכפלה הישרה למחצה*** *(**החיצונית**) של K ב־Q, ביחס ל־θ, היא הקבוצה $K\times Q$ עם פעולת הכפל $(k,q)(k',q')=(k\cdot\theta_q(k'),qq')$. את החבורה שהגדרנו מסמנים $K\rtimes_\theta Q$. לשם הבהירות, נכתוב את האברים בצורה kq במקום (k,q); ההצגה יחידה לפי ההגדרה.*

תרגיל 7.3.18 (**) הוכח ש־$K\rtimes_\theta Q$ חבורה.

תרגיל 7.3.19 (*) ההטלה $\gamma:K\rtimes_\theta Q\to Q$ המוגדרת לפי $\gamma(kq)=q$ היא הומומורפיזם, שהגרעין שלו הוא K.

תרגיל 7.3.20 (***) נתבונן בתת־החבורות $Q^*=Q\times 1$ ו־$K^*=1\times K$ של $G=K\rtimes_\theta Q$; כמובן $Q\cong Q^*$ ו־$K\cong K^*$. הראה ש־$G=K^*\rtimes Q^*$, כלומר (הגדרה 7.3.1): $K^*\cap Q^*=1$, $K^*Q^*=G$, $K^*\lhd G$. במלים אחרות, מכפלה ישרה למחצה חיצונית היא גם מכפלה ישרה למחצה פנימית של אותן חבורות.

תרגיל 7.3.21 (***) תהי $G=K\rtimes Q$ מכפלה ישרה למחצה פנימית של K ב־Q. נגדיר הומומורפיזם $\theta:Q\to\mathrm{Aut}(K)$ לפי תרגיל 7.3.6. הראה ש־$G\cong K\rtimes_\theta Q$; כלומר, כל מכפלה ישרה פנימית היא גם מכפלה ישרה למחצה חיצונית של אותן חבורות.

תרגיל 7.3.22 (**) יהי R **חוג** (קבוצה עם פעולות חיבור וכפל, שהיא חבורה אבלית ביחס לחיבור ומונויד ביחס לכפל המקיימת את חוקי מימין ומשמאל). יהי K **אידיאל שמאלי** של R (תת־חבורה ביחס לחיבור, הסגורה לכפל משמאל בכל איבר), ותהי $Q\leq R^\times$ תת־חבורה ביחס לכפל של חבורת האברים ההפיכים. הראה שחבורת המטריצות $\left\{\begin{pmatrix} q & k\\ 0 & 1\end{pmatrix}:\ q\in Q,\,k\in K\right\}$ איזומורפית למכפלה הישרה למחצה $K\rtimes Q$ ביחס לפעולה $\theta:Q\to\mathrm{Aut}(K)$ המוגדרת לפי $\theta_q:k\to qk$. קבל את תרגיל 7.3.8 כמקרה פרטי ($R=K=F$ ו־$Q=F^\times$).

תרגיל 7.3.23 (*+)** בכל המקרים הבאים, המכפלה הישרה למחצה $K\rtimes Q$ היא ביחס להומומורפיזם $Q\to\mathrm{Aut}(K)$ שאינו טריוויאלי. הוכח:

1. $D_n\cong\mathbb{Z}_n\rtimes\mathbb{Z}_2$ לכל n (האיבר הלא־טריוויאלי של $\mathbb{Z}_2$ הופך את אברי $\mathbb{Z}_n$).
2. $D_4\cong(\mathbb{Z}_2\times\mathbb{Z}_2)\rtimes\mathbb{Z}_2$.
3. $A_4\cong(\mathbb{Z}_2\times\mathbb{Z}_2)\rtimes\mathbb{Z}_3$ (בדוק שזו החבורה $F^+\rtimes F^\times$ מתרגיל 7.3.8, עם $F=\mathbb{F}_4$, השדה בן ארבעה אברים).

תרגיל 7.3.24 (-*)** תהי $G=K\rtimes_\theta Q$. נסמן $K^Q=\{k\in K:\ (\forall q\in Q)\theta_q(k)=k\}$.

1. $\mathrm{N}_G(Q)=K^QQ$. בפרט, אם פעולת Q על K נאמנה, אז $\mathrm{N}_G(Q)=Q$.
2. $\mathrm{C}_G(Q)=K^Q\mathrm{Z}(Q)$.
3. $\mathrm{N}_G(Q)/\mathrm{C}_G(Q)\cong\mathrm{Inn}(Q)$.

תרגיל 7.3.25 (*) הראה ש־Q נורמלית ב־$K\rtimes_\theta Q$ אם ורק אם θ היא הפעולה הטריוויאלית $\theta_q=\mathrm{id}$ לכל q. במקרה זה $K\rtimes_\theta Q\cong K\times Q$.

תרגיל 7.3.26 (**) נניח ש־Q פועלת על K באמצעות $\theta\colon Q \to \mathrm{Aut}(K)$, ו־$Q_0 = \mathrm{Ker}(\theta)$. אז $Q_0 \lhd (K \rtimes_\theta Q)$ והמנה היא $(K \rtimes_\theta Q)/Q_0 \cong K \rtimes_\theta (Q/Q_0)$.

תרגיל 7.3.27 (**+) נניח ש־$Q = Q_1 \times Q_2$ פועלת באמצעות $\theta\colon Q_1 \times Q_2 \to \mathrm{Aut}(K)$ על K, באופן ש־$\theta(q_2) = 1$ לכל $q_2 \in Q_2$. אז $K \rtimes_\theta (Q_1 \times Q_2) = (K \rtimes_\theta Q_1) \times Q_2$.

תרגיל 7.3.28 (***-) יהיו $\theta', \theta\colon Q \to \mathrm{Aut}(K)$ שני הומומורפיזמים. נבדוק מתי פונקציה $K \rtimes_\theta Q \to K \rtimes_{\theta'} Q$ השומרת את K ו־Q (כקבוצות), היא איזומורפיזם.

1. העתקה $(k,q) \mapsto (\phi k, \sigma q)$ היא איזומורפיזם $K \rtimes_\theta Q \to K \rtimes_{\theta'} Q$ אם ורק אם $\phi \in \mathrm{Aut}(K)$, $\sigma \in \mathrm{Aut}(Q)$, ו־$\theta = \gamma_\phi \circ \theta' \circ \sigma^{-1}$ (γ_ϕ הוא האוטומורפיזם הפנימי ב־$\mathrm{Aut}(K)$ של הצמדה ב־ϕ).
2. יש איזומורפיזם $K \rtimes_\theta Q \to K \rtimes_{\theta'} Q$ הקובע את אברי Q ושומר על K (כקבוצה), אם ורק אם יש $\phi \in \mathrm{Aut}(K)$ קבוע המצמיד כל θ_q ל־θ'_q.
3. נניח שפעולת Q על K היא פעולה נאמנה (כלומר θ חד־חד־ערכית). אז יש שיכון $\mathrm{N}_{\mathrm{Aut}(K)}(\mathrm{Im}\theta) \hookrightarrow \mathrm{Aut}(K \rtimes_\theta Q)$ המתאים ל־$\phi \in \mathrm{Aut}(K)$ את הפונקציה $(k,q) \mapsto (\phi k, (\theta^{-1}\gamma_\phi\theta)q)$.

תרגיל 7.3.29 (**+) 1. המכפלה הישרה למחצה $K \rtimes_\theta \mathbb{Z}_n$ תלויה רק ב־K, n, והאוטומורפיזם $\theta(1) \in \mathrm{Aut}(K)$.

2. יש איזומורפיזם $K \rtimes_\theta \mathbb{Z}_n \cong K \rtimes_{\theta'} \mathbb{Z}_n$ השומר את $K, \mathbb{Z}_n$ כקבוצות אם ורק אם יש $i \in U_n$ כך ש־$\theta(1)$ צמוד ב־$\mathrm{Aut}(K)$ ל־$\theta'(1)^i$. **הדרכה.** זהו תרגיל 7.3.28 כאשר Q ציקלית.

תרגיל 7.3.30 (**+) תהי A חבורה כך ש־$\mathrm{Aut}(A)$ ציקלית מסדר המתחלק ב־p. אז יש בדיוק שתי מכפלות ישרות למחצה $A \rtimes \mathbb{Z}_p$: באחת הפעולה טריוויאלית, ובשניה הפעולה אינה טריוויאלית. **הדרכה.** תרגיל 7.3.29.

תרגיל 7.3.31 (***-) יהיו p ראשוני, V מרחב וקטורי מעל שדה ממאפיין זר ל־p, ו־$T \in \mathrm{End}(V)$ העתקה שהפולינום המינימלי שלה הוא $1 + \lambda + \cdots + \lambda^p$ (בפרט $T^p = 1$). הראה ש־$V \rtimes \mathbb{Z}_p = \{vx^i :\ i \in \mathbb{Z}_p\}$, המוגדרת לפי הפעולה $xv = T(v)x$, היא חבורה מסדר $p|V|$, שיש בה $|V|$ תת־חבורות מסדר p.

תרגיל 7.3.32 (***) יהיו $K = S_3$ ו־$Q = \mathbb{Z}_2 \times \mathbb{Z}_2$. ידוע ש־$\mathrm{Aut}(K) \cong K$ (תרגיל 7.1.7). רשום את כל ההומומורפיזמים $Q \to \mathrm{Aut}(K)$. הראה שיש בדיוק שתי מכפלות ישרות למחצה (חיצוניות) של K ב־Q, ותאר אותן. איזו מהן היא S_4?

תרגיל 7.3.33 (***) 1. נניח ש־$Z(K) = 1$, והפעולה של Q על K היא פנימית, כלומר, $\theta\colon Q \to \mathrm{Inn}(K)$. הוכח ש־$K \rtimes_\theta Q \cong K \times Q$. **הדרכה.** חפש בעזרת תרגיל 7.3.28 איזומורפיזם הקובע את אברי K.

2. הראה, על־ידי דוגמה נגדית, שהתנאי $Z(K) = 1$ בסעיף הקודם הכרחי. **הדרכה.** למשל קח $Q = \mathbb{Z}_2 \times \mathbb{Z}_2$, $K = Q_8$ (חבורת הקווטרניונים מסדר 8), $\theta\colon Q \stackrel{\cong}{\to} K/\langle -1 \rangle$; המרכז של $K \rtimes Q$ בגודל 2, ואילו זה של $K \times Q$ מסדר 8.

תרגיל 7.3.34 (***-) תהי G חבורה. פעולה של G על עצמה מהצורה $\theta\colon G \xrightarrow{\varphi} G \to \mathrm{Inn}G \subseteq \mathrm{Aut}G$, כאשר $G \to \mathrm{Inn}G$ היא ההטלה הסטנדרטית, ו־φ אנדומורפיזם כלשהו, נקראת **פעולת הצמדה מוכללת**. הראה שלכל פעולת הצמדה מוכללת, $G \rtimes_\theta G \cong G \times G$. **הדרכה.** $(a,x) \mapsto (a\varphi(x), x)$.

7.3.3 חבורות שלמות

ניתן לדלג בקריאה ראשונה.

ההולומורף

הגדרה 7.3.35 *תהי G חבורה. העתקת הזהות $\mathrm{Aut}(G) \to \mathrm{Aut}(G)$ מגדירה את הפעולה הטבעית של $\mathrm{Aut}(G)$ על G. המכפלה הישרה למחצה $\mathrm{Hol}(G) = G \rtimes \mathrm{Aut}(G)$ המתאימה לפעולה זו נקראת **ההולומורף** של G.*

תרגיל 7.3.36 (**) $H \times 1$ היא תת־חבורה נורמלית של $\mathrm{Hol}(G)$ אם ורק אם H אופיינית ב־G.

תרגיל 7.3.37 (**) כל אוטומורפיזם של G מושרה על־ידי אוטומורפיזם פנימי של $\mathrm{Hol}(G)$.

תרגיל 7.3.38 (+)** הראה ש־$D_4 \cong \mathrm{Hol}(\mathbb{Z}_4)$. הראה ש־$S_4 \cong \mathrm{Hol}(\mathbb{Z}_2 \times \mathbb{Z}_2)$.

תרגיל 7.3.39 (+)** הראה שלכל $n > 2$, $\mathrm{Hol}(\mathbb{Z}_n) \cong \mathrm{Aut}(D_n)$.

תרגיל 7.3.40 (*-)** נתבונן בחבורה G כתת־חבורה של חבורת הסיטריות S_G, לפי שיכון קיילי. המנרמל שלה הוא $\mathrm{N}_{S_G}(G) = \mathrm{Hol}(G)$.

חבורות שלמות וכמעט שלמות

הגדרה 7.3.41 *חבורה K נקראת **חבורה שלמה** אם $\mathrm{Z}(K) = 1$ ו־$\mathrm{Out}(K) = 1$.*

תרגיל 7.3.42 (*) אם G שלמה אז $G \cong \mathrm{Aut}(G)$.

תרגיל 7.3.43 (**) לכל $n \neq 2, 6$, החבורה הסימטרית S_n היא שלמה. **הדרכה.** תרגילים 5.3.18 ו־7.2.32.

תרגיל 7.3.44 (**) אם K שלמה אז כל מכפלה ישרה למחצה $K \rtimes_\theta Q$ היא מכפלה ישרה. **הדרכה.** תרגיל 7.3.33. **הערה.** תרגיל 7.4.72 מספק תוצאה חזקה עוד יותר.

תרגיל 7.3.45 (**) נאמר ש־G **כמעט שלמה** אם $\mathrm{Out}(G) = 1$ ו־$G = \mathbb{Z}_2 \times X$ כאשר $\mathrm{Z}(X) = 1$. הראה שבמקרה זה X שלמה.

תרגיל 7.3.46 (+)** אם G שלמה או כמעט שלמה אז $\mathrm{Hol}(G) \cong G \times \mathrm{Aut}(G)$. **הדרכה.** תרגיל 7.3.44 כש־G שלמה; מתקבל האיזומורפיזם $(g, \gamma_x) \mapsto (gx, \gamma_x)$ הפועל גם כש־G כמעט שלמה.

תרגיל 7.3.47 (*-)** נניח שיש איזומורפיזם $\mathrm{Hol}(G) \to G \times \mathrm{Aut}(G)$ השומר על אברי G ומשרה את הזהות על המנה $\mathrm{Aut}(G)$. אז G שלמה או כמעט שלמה. **הדרכה.** לפי ההנחה האיזומורפיזם הוא $T : g\varphi \mapsto (gx_\varphi, \varphi)$ כאשר $x_\varphi \in G$. מהשוואת $T(g\varphi) \cdot T(g'\varphi') = (gx_\varphi g' x_{\varphi'}, \varphi\varphi')$ ו־$T(g\varphi \cdot g'\varphi') = (g\varphi(g')x_{\varphi\varphi'}, \varphi\varphi')$ נובע, על־ידי בחירת $g' = 1$ בתחילה, ש־$x_{\varphi\varphi'} = x_\varphi x_{\varphi'}$ ו־$\varphi(g') = x_\varphi g' x_\varphi^{-1}$. בפרט כל $\varphi \in \mathrm{Aut}(G)$ הוא פנימי. נסמן $Z = \mathrm{Z}(G)$ ו־$X = \{x_\varphi\}$. לכל $g \in G$, $gx_{\gamma_g}^{-1} \in Z$, ולכן $G = ZX$. זוהי מכפלה ישרה כי $Z \cap X = 1$ ו־$X \lhd G$. לפי תרגיל 7.2.16, $\mathrm{Out}(Z) \times \mathrm{Out}(X) \hookrightarrow \mathrm{Out}(G) = 1$, ולכן $\mathrm{Out}(X) = 1$. אם $x \in \mathrm{Z}(X) \subseteq \mathrm{Z}(G) = Z$ אז $x = 1$, ומכאן ש־X שלמה. בנוסף $\mathrm{Out}(Z) = 1$ ולפי תרגיל 7.2.22, $Z = 1$ או $Z = \mathbb{Z}_2$.

תרגיל 7.3.48 (***) נניח ש־X שלמה. אז $\mathrm{Out}(\mathbb{Z}_2 \times X) \cong \mathrm{Hom}(X, \mathbb{Z}_2)$. בפרט $\mathbb{Z}_2 \times X$ כמעט שלמה אם ורק אם אין ל־X תת־חבורות מאינדקס 2.

7.3.4 מכפלת זר

הגדרה 7.3.49 *תהיינה A, B חבורות. נסמן ב־A^B את החבורה של פונקציות $f : B \to A$, עם פעולת הכפל לפי רכיבים, כלומר $(fg)(b) = f(b)g(b)$. החבורה B פועלת על A^B לפי $(bf)(b') = f(bb')$. המכפלה הישרה למחצה המתקבלת, $A^B \rtimes B = A \wr B$, נקראת* ***מכפלת זר*** *של A ו־B.*

תרגיל 7.3.50 (*) $|A \wr B| = |A|^{|B|}|B|$.

משפט 7.3.51 *כל הרחבה של B על־ידי A (הגדרה 7.4.18) היא תת־חבורה של $A \wr B$.*

תרגיל 7.3.52 (*) זהה את החבורה $\mathbb{Z}_2 \wr \mathbb{Z}_2$.

תרגיל 7.3.53 (**) האם $S_4 \cong \mathbb{Z}_2 \wr \mathbb{Z}_3$?

תרגיל 7.3.54 (**) תאר פעולה של $S_n \wr \mathbb{Z}_m$ על אוסף המריצות $m \times n$ שערכיהן הם כל המספרים $1, \dots, nm$. הסק ש־$m!n!^m \mid (nm)!$.

7.4 מבוא לקוהומולוגיה

7.4.1 משלימים והקוהומולוגיה הראשונה

ניתן לדלג בקריאה ראשונה.

לאורך כל הסעיף נניח ש־$K \triangleleft G$ היא תת־חבורה נורמלית, עם תת־חבורה משלימה $Q \leq G$ (כלומר $KQ = G$ ו־$K \cap Q = 1$), וכך שהצמדה משרה פעולה $\theta : Q \to \mathrm{Aut}(K)$ של Q על K. כך $G = K \rtimes_\theta Q$ היא מכפלה ישרה למחצה, ולפי תרגיל 7.3.19, $G/K \cong Q$. לשם הקיצור נסמן $(\theta(q))(k) = \theta_q(k) = q(k)$.

1־קו־מעגלים

תרגיל 7.4.1 (**) תהי $Q_1 \leq G$ משלימה כלשהי של K. הראה שקיימת פונקציה $a : Q \to K$ (שאת ערכיה נסמן ב־$a : q \mapsto a_q \in K$) כך ש־$Q_1 = \{a_q q :\ q \in Q\}$.

תרגיל 7.4.2 (**) הראה שקבוצה מהצורה $\{a_q q :\ q \in Q\}$ $(a : Q \to K)$ היא תת־חבורה של G אם ורק אם $a_{qq'} = a_q \cdot q(a_{q'})$ לכל $q, q' \in Q$. (הראה שמנוסחה זו נובע $a_1 = 1$ ו־$q(a_{q^{-1}}) = a_q^{-1}$).

הגדרה 7.4.3 *פונקציות $a : Q \to K$ המקיימות את התנאי $a_{qq'} = a_q \cdot q(a_{q'})$ קרויות (מסיבות שלא נסביר כאן)* ***1־קו־מעגלים****. עבור פעולה נתונה של Q על K, נסמן*

$$\mathrm{Z}^1(Q, K) = \big\{a : Q \to K :\ a_{qq'} = a_q \cdot q(a_{q'})\big\}.$$

לפי תרגיל 7.4.2, יש התאמה חד־חד־ערכית בין $\mathrm{Z}^1(Q, K)$ לבין קבוצת המשלימים של K, כאשר האיבר $1_q = 1$ מתאים ל־Q.

תרגיל 7.4.4 (**) בדומה לתרגיל 1.6.12, אם שני 1־קו־מעגלים מסכימים זה עם זה על קבוצת יוצרים של Q, אז הם שווים.

שקילות של 1־קו־מעגלים

תרגיל 7.4.5 (*) לכל $u \in K$, אם $a \in \mathrm{Z}^1(Q,K)$ אז $a'_q = ua_qq(u)^{-1}$ מגדיר איבר $a' \in \mathrm{Z}^1(Q,K)$. **פתרון.** $a'_{qq'} = ua_{qq'}qq'(u)^{-1} = ua_qq(a_{q'})qq'(u)^{-1} = (ua_qq(u)^{-1})q(ua_{q'}q'(u)^{-1}) = a'_qq(a'_{q'})$.

הגדרה 7.4.6 ***נאמר ששני 1־קו־מעגלים $a, a' : Q \to K$ הם קוהומולוגיים זה לזה אם קיים $u \in K$ (קבוע) כך ש־$a'_q = ua_qq(u)^{-1}$. במקרה זה נסמן $a' \sim a$.***

תרגיל 7.4.7 (**) הראה שיחס הקוהומולוגיות בין 1־קו־מעגלים הוא יחס שקילות.

תרגיל 7.4.8 (*) $a \in \mathrm{Z}^1(Q,K)$ קוהומולוגי לפונקציה הטריוויאלית 1 אם ורק אם קיים $u \in K$ כך ש־$a_q = uq(u)^{-1}$ לכל $q \in Q$.

תרגיל 7.4.9 (*) נניח שפעולת Q על K טריוויאלית, כלומר $q(k) = k$ לכל $q \in Q$ ולכל $k \in K$. אז $\mathrm{Z}^1(Q,K) = \mathrm{Hom}(Q,K)$ היא קבוצת ההומומורפיזמים, ו־$a \sim a'$ אם ורק אם הפונקציות צמודות, כלומר יש $u \in K$ כך ש־$a'_q = ua_qu^{-1}$. בפרט, ה־1־קו־מעגל $1_q = 1$ קוהומולוגי רק לעצמו.

תרגיל 7.4.10 (**) תהי Q_1 תת־חבורה משלימה של K, המתאימה ל־$a \in \mathrm{Z}^1(Q,K)$.

1. יהי $k \in Q$. הראה ש־kQ_1k^{-1} הוא המשלים המתאים ל־$a' \in \mathrm{Z}^1(Q,K)$ המוגדר לפי $a'_q = ka_qq(k)^{-1}$. **הדרכה.** $kQ_1k^{-1} = \{ka_qqk^{-1}\} = \{ka_qq(k)^{-1} \cdot q\}$.
2. יהי $x \in Q$. הראה ש־xQ_1x^{-1} הוא המשלים המתאים ל־$a' \in \mathrm{Z}^1(Q,K)$ המוגדר לפי $a'_q = a_x^{-1}a_qq(a_x)$. **הדרכה.** $xQ_1x^{-1} = \{xa_qqx^{-1}\} = \{x(a_q) \cdot xqx^{-1}\} = \left\{x(a_{x^{-1}qx}) \cdot q\right\} = \left\{a_x^{-1}a_qq(a_x) \cdot q\right\}$.
3. תת־החבורות המשלימות המתאימות ל־$a, a' \in \mathrm{Z}^1(Q,K)$ הן צמודות אם ורק אם a, a' קוהומולוגיות.

לסיכום, יש התאמה בין $\mathrm{Z}^1(Q,K)$ לבין קבוצת תת־החבורות המשלימות את K; והתאמה בין מחלקות הקוהומולוגיה של קו־מעגלים, היינו קבוצת המנה $\mathrm{Z}^1(Q,K)/\sim$, לבין קבוצת תת־החבורות המשלימות עד־כדי הצמדה.

קוהומולוגיה ראשונה עם מקדמים אבליים

נניח ש־K אבלית. במקרה זה, על אף ש־$K \leq G$, מקובל לכתוב את K בכתיב חיבורי, כך ש־

$$\mathrm{Z}^1(Q,K) = \left\{a : Q \to K :\ a_{qq'} = a_q + q(a_{q'})\right\},$$

והאיבר הנייטרלי (המתאים למשלימה Q) הוא קו־מעגל האפס, $0_q = 0$.

תרגיל 7.4.11 (**) נניח ש־K אבלית. הראה ש־$\mathrm{Z}^1(Q,K)$ היא חבורה (אבלית) ביחס לפעולת החיבור לפי רכיבים, $(a+b)_q = a_q + b_q$. הראה שאוסף הפונקציות הקוהומולוגיות ל־1, $\mathrm{B}^1(Q,K) = \{a_q = u - q(u) :\ u \in K\}$, הוא תת־חבורה. הראה ש־$a, a' \in \mathrm{Z}^1(Q,K)$ קוהומולוגיים אם ורק אם הם שייכים לאותו קוסט של $\mathrm{B}^1(Q,K)$. במקרה זה מגדירים

$$\mathrm{H}^1(Q,K) = \mathrm{Z}^1(Q,K)/\mathrm{B}^1(Q,K)$$

- **חבורת הקוהומולוגיה הראשונה של Q עם מקדמים ב־K**; זו קבוצת מחלקות הקוהומולוגיה של 1־קו־מעגלים.

לסיכום: כאשר Q חבורה הפועלת על חבורה אבלית K, יש התאמה בין אברי $\mathrm{H}^1(Q,K)$ לבין מחלקות הצמידות של תת־החבורות המשלימות את K במכפלה הישרה למחצה $K \rtimes Q$. האיבר הטריוויאלי מתאים ל־Q. $\Longrightarrow$

תרגיל 7.4.12 (+)** תהי Q חבורה הפועלת על חבורה אבלית K. כל תת־החבורות של $K \rtimes Q$ המשלימות את K צמודות ל־Q אם ורק אם $\mathrm{H}^1(Q,K)=0$. **הדרכה.** לפי ההתאמה לעיל.

תרגיל 7.4.13 (*+) נניח שפעולת Q על K טריוויאלית, כאשר K אבלית. אז $\mathrm{B}^1(Q,K)=0$ ו־$\mathrm{H}^1(Q,K)=\mathrm{Z}^1(Q,K)=\mathrm{Hom}(Q,K)$.

תרגיל 7.4.14 (*+) $|K|\cdot \mathrm{Z}^1(Q,K)=0$. **הדרכה.** $|K|k=0$ לכל $k\in K$.

תרגיל 7.4.15 (***) נניח ש־K אבלית. אז $|Q|\cdot \mathrm{H}^1(Q,K)=0$. (כלומר, לכל $a\in \mathrm{Z}^1(Q,K)$, הסכום $|Q|\cdot a=a+\cdots+a$ קוהומולוגי לקו־מעגל האפס.) **פתרון**. נסמן $u=\sum_{g\in Q} a_g$. לכל $q\in Q$, $u-q(u)=\sum_g a_g-\sum_g q(a_g)=\sum_g a_g-\sum_g(a_{gq}-a_q)=|Q|a_q$; הראינו ש־$|Q|a$ הומולוגי לאפס.

התרגיל הבא הוא עילת כל המאמץ הטכני שעשינו בסעיף הזה.

תרגיל 7.4.16 (***) נניח ש־$K\lhd G$ אבלית ו־$([G:K],|K|)=1$, ושיש ל־K תת־חבורה משלימה Q. אז כל תת־החבורות של G המשלימות את K צמודות זו לזו. **הדרכה.** כמובן, $|Q|=[G:K]$. מתרגילים 7.4.14 ו־7.4.15 וקיומו של צירוף $\alpha|Q|+\beta|K|=1$, נובע ש־$\mathrm{H}^1(Q,K)=0$. תרגיל 7.4.12 מסיים את המלאכה.

תרגיל 7.4.17 (***) תהי A חבורה אבלית.

1. כל פעולה של $Q=\mathbb{Z}_2=\{1,x\}$ על A מוגדרת לפי אוטומורפיזם $\tau\colon A\to A$ המקיים $\tau^2=\mathrm{id}$.
2. יש איזומורפיזם $A\rtimes_\tau \mathbb{Z}_2\cong A\rtimes_{\tau'}\mathbb{Z}_2$ הקובע את העותקים של $\mathbb{Z}_2$, אם ורק אם $\tau,\tau'\in \mathrm{Aut}(A)$ צמודים. כלומר, יש התאמה בין המכפלות הישרות למחצה של $K=A$ ב־$Q=\mathbb{Z}_2$, עד כדי איזומורפיזם, לבין מחלקות צמידות של אברים מסדר 1 או 2 ב־$\mathrm{Aut}(A)$ (יתכן ששתי מחלקות תתאמנה לחבורות איזומורפיות). **הדרכה.** זהו ניסוח מחדש את תרגיל 7.3.28.
3. נקבע $\tau\in\mathrm{Aut}(A)$ כך ש־$\tau^2=\mathrm{id}$, ו־$G=\langle A,x\rangle$ עם הפעולה $xa=\tau(a)x$, $x^2=1$. אז $\mathrm{C}_G(x)=A^\tau\langle x\rangle$ כאשר $A^\tau=\{a\in A:\ \tau(a)=a\}$. בפרט, $A\rtimes_\tau\mathbb{Z}_2$ אבלית (ושווה למכפלה הישרה $A\times\mathbb{Z}_2$) אם ורק אם $\tau=1$.
4. אפשר לזהות קו־מעגל $a\colon Q=\{1,x\}\to A$ עם הערך a_x (ממילא $a_1=0$). הראה ש־$\mathrm{H}^1(\mathbb{Z}_2,A)=\mathrm{Ker}(1+\tau)/\mathrm{Im}(1-\tau)$, ואשר שזהו מרחב וקטורי מעל $\mathbb{F}_2$. **הדרכה.** $\mathrm{Z}^1(\mathbb{Z}_2,A)=\{a_x:\ \tau(a_x)+a_x=0\}=\mathrm{Ker}(1+\tau)$ ו־$\mathrm{B}^1(\mathbb{Z}_2,K)=\{a_x=u-\tau(u)\}=\mathrm{Im}(1-\tau)$. למשל, אם $\tau=-\mathrm{id}$, אז $\mathrm{H}^1(\mathbb{Z}_2,A)=A/2A$, ואם $\tau=\mathrm{id}$ אז $\mathrm{H}^1(\mathbb{Z}_2,A)=A_2$ היא תת־החבורה של אברים מסדר 2 ב־A.
5. לדוגמא, אם $A=\mathbb{Z}_{2p}$ אז יש שתי פעולות אפשריות, $\tau=\mathrm{id}$ ו־$\tau=-\mathrm{id}$. המכפלה הישרה למחצה היא $\mathbb{Z}_{2p}\times\mathbb{Z}_2$ במקרה הראשון ו־D_{2p} בשני. במקרה האבלי יש למרכיב A משלים בודד (הלוא הוא המרכיב ה), ובמקרה $G=D_{2p}$ יש לתת־החבורה $A=\langle\sigma\rangle$ שני משלימים לא צמודים: $Q=\langle\tau\rangle$ ו־$\langle\sigma\tau\rangle$ (את המרכיב השני, $\{1,a_\tau\tau\}$, אפשר למצוא מן הקו־מעגל הלא טריוויאלי $0\neq a_\tau\in A/2A$).

7.4.2 הרחבות והקוהומולוגיה השניה

ניתן לדלג בקריאה ראשונה.

הגדרה 7.4.18 *נאמר שחבורה G היא הרחבה של Q על־ידי K אם* $K \lhd G$ ו־$G/K \cong Q$.

אפשר לתאר את ההרחבה על־ידי סדרה קצרה מדוייקת (תת־סעיף 3.5.1)

$$1 \longrightarrow K \longrightarrow G \longrightarrow Q \longrightarrow 1.$$

תרגיל 7.4.19 (*) כל מכפלה ישרה למחצה של K ב־Q היא הרחבה של Q על־ידי K.

תרגיל 7.4.20 (*) $\mathbb{Z}_4$ היא הרחבה של $\mathbb{Z}_2$ על־ידי $\mathbb{Z}_2$ שאינה מכפלה ישרה למחצה שלהן.

תרגיל 7.4.21 (***) הרחבה G של Q על־ידי K נקראת **מפוצלת** אם יש הומומורפיזם $p\colon Q \to G$ כך ש־$\pi \circ p = 1$ כאשר $\pi\colon G \to Q$ היא ההטלה הטבעית. הוכח שכל מכפלה ישרה למחצה משרה הרחבה מפוצלת, ושהרחבה מפוצלת היא מכפלה ישרה למחצה של K ו־$p(Q) \cong Q$. מכפלה ישרה למחצה = הרחבה מפוצלת
הדרכה. תרגיל 7.3.11.

נניח מעתה שנתונות חבורה אבלית K וחבורה Q הפועלת עליה. גם כאן נאמץ כתיב חיבורי לאברים של K.

תרגיל 7.4.22 (**) כאשר K אבלית, ההרחבה $1 \longrightarrow K \longrightarrow G \longrightarrow Q \longrightarrow 1$ משרה פעולה של Q על K. **הדרכה.** לכל $q \in Q$ יש מקור $z_q \in G$, שהצמדה בו משרה אוטומורפיזם של K; אוטומורפיזם זה אינו תלוי בבחירת z_q משום ש־K אבלית.

הגדרה 7.4.23 *פונקציה $c\colon Q \times Q \to K$ המקיימת את התנאי $c_{q,q'} + c_{qq',q''} = q(c_{q',q''}) + c_{q,q'q''}$ קרויה 2־קו־מעגל. נסמן*

$$\mathrm{Z}^2(Q,K) = \left\{c\colon Q \times Q \to K:\ c_{q,q'} + c_{qq',q''} = q(c_{q',q''}) + c_{q,q'q''}\right\}.$$

תרגיל 7.4.24 (*) $\mathrm{Z}^2(Q,K)$ היא חבורה (אבלית), ביחס לפעולה $(c+c')_{q,q'} = c_{q,q'} + c'_{q,q'}$, ועם האיבר הנייטרלי $c_{q,q'} = 0$.

תרגיל 7.4.25 (+*) הראה שלכל $c \in \mathrm{Z}^2(Q,K)$, $c_{1,q} = c_{1,1}$ ו־$c_{q,1} = q(c_{1,1})$ לכל q. **הדרכה.** אלו הזהויות הנובעות מהצבת $q = 1$, $q' = 1$ או $q'' = 1$.

תרגיל 7.4.26 (**) תהי G הרחבה של Q על־ידי K (המשרה את הפעולה הנתונה של Q על K). נבחר נציגים $z_q \in G$ (לכל $q \in Q$) כך ש־$G = \cup K z_q$; כלומר, בהטלה $G \to Q$, $z_q \mapsto q$. נסמן $c_{q,q'} = z_q z_{q'} z_{qq'}^{-1}$. הראה ש־$c\colon (q,q') \mapsto c_{q,q'}$ היא 2־קו־מעגל. **הדרכה.** ראשית הראה ש־$c_{q,q'} \in K$. את תנאי הקו־מעגליות הסק משוויון האסוציאטיביות $(z_q z_{q'}) z_{q''} = z_q (z_{q'} z_{q''})$.

תרגיל 7.4.27 (**) בתרגיל 7.4.26, הנציגים $\{z_q :\ q \in Q\}$ מהווים תת־חבורה (איזומורפית ל־Q) של G אם ורק אם $c_{q,q'} = 0$ זהותית. במקרה זה, Q היא תת־חבורה משלימה של K, ו־$G = K \rtimes Q$.

תרגיל 7.4.28 (**) תהי G הרחבה של Q על־ידי החבורה האבלית K, המשרה פעולה טריוויאלית על K. לאחר בחירת נציגים $z_q \in G$ לכל $q \in Q$, נגדיר $c_{q,q'} = z_q z_{q'} z_{qq'}^{-1}$. הראה ש־$\mathrm{Z}(G) = KQ_0$ כאשר $Q_0 = \{q_0 \in Q \,|\, \forall q : c_{q_0,q} = c_{q,q_0}\}$.

הגדרה 7.4.29 ***נאמר ששני 2־קו־מעגלים $c, c' : Q \to K$ הם קוהומולוגיים זה לזה אם יש פונקציה $a : Q \to K$ כך ש־$c'_{q,q'} = a_q + q(a_{q'}) + c_{q,q'} - a_{qq'}$. כמו במקרה של 1־קו־מעגלים, במקרה זה כותבים $c' \sim c$. אוסף המעגלים הקוהומולוגיים לאפס הוא תת־חבורה $\mathrm{B}^2(Q,K) = \left\{c_{q,q'} = a_q + q(a_{q'}) - a_{qq'} : \, a : Q \to K\right\}$. חבורת המנה***

$$\mathrm{H}^2(Q,K) = \mathrm{Z}^2(Q,K)/\mathrm{B}^2(Q,K)$$

היא חבורת הקוהומולוגיה השניה של Q עם מקדמים ב־K.

(שלא כבמקרה של $\mathrm{Z}^1(Q,K)$, ההנחה ש־K אבלית הכרחית על־מנת לקבל יחס שקילות.)

תרגיל 7.4.30 (*) כל 2־קו־מעגל $c \in \mathrm{Z}^2(Q,K)$ קוהומולוגי לקו־מעגל c' שבו $c'_{1,q} = c'_{q,1} = 0$.

הדרכה. בחר $a_1 = c_{1,1}$ ו־$a_q = 0$ לכל $q \neq 1$; העזר בתרגיל 7.4.25.

תרגיל 7.4.31 (**) בתרגיל 7.4.26, החלפת הנציגים z_q בנציגים $z'_q = a_q z_q$ $(a_q \in K)$ מגדירה קו־מעגל $c' = z'_q z'_{q'} z'^{-1}_{qq'}$, שהוא קוהומולוגי ל־$c$.

תרגיל 7.4.32 (***) יהי $[c] \in \mathrm{H}^2(Q,K)$, המוגדר על־ידי פונקציה $c \in \mathrm{Z}^2(Q,K)$. נגדיר על $K \times Q$ פעולת כפל לפי $(k,q)(k',q') = (k + q(k') + c_{q,q'}, qq')$. הראה שמתקבלת חבורה שהיא הרחבה של K על־ידי Q. בחירת $c' \sim c$ מגדירה חבורה איזומורפית.

$\Longrightarrow$ **לסיכום (על־פי תרגילים 7.4.31 ו־7.4.32): תהי Q חבורה הפועלת על חבורה אבלית K. יש התאמה בין אברי החבורה $\mathrm{H}^2(Q,K)$ לבין ההרחבות של Q על־ידי K המשרות את הפעולה הנתונה. האיבר הטריוויאלי מתאים להרחבה $1 \longrightarrow K \longrightarrow K \rtimes Q \longrightarrow Q \longrightarrow 1$.**

תרגיל 7.4.33 (**) הרחבה G של Q על־ידי K היא אבלית אם ורק אם K אבלית, Q אבלית, הפעולה של Q על K טריוויאלית, וה־2־קו־מעגל $c : Q \times Q \to K$ המגדיר את ההרחבה הוא סימטרי (היינו $c_{q,q'} = c_{q',q}$; כאשר הפעולה טריוויאלית, תכונה זו נשמרת תחת קוהומולוגיה.)

תרגיל 7.4.34 (*־)** תהי Q חבורה הפועלת על חבורה אבלית K. כל הרחבה של Q על־ידי K היא מכפלה ישרה למחצה $K \rtimes Q$, אם ורק אם $\mathrm{H}^2(Q,K) = 0$.

תרגיל 7.4.35 (***) יהיו $\theta', \theta : Q \to \mathrm{Aut}(K)$ שני הומומורפיזמים. תהי G ההרחבה של Q על־ידי K ביחס לפעולה θ המוגדרת על־ידי $c \in \mathrm{Z}^2_{\theta}(Q,K)$, ותהי G' ההרחבה של Q על־ידי K ביחס לפעולה θ' המוגדרת על־ידי $c' \in \mathrm{Z}^2_{\theta'}(Q,K)$.

1. העתקה $kz_q \mapsto \phi(k) z'_{\sigma(q)}$ היא איזומורפיזם $G \to G'$ אם ורק אם $\phi \in \mathrm{Aut}(K)$, $\sigma \in \mathrm{Aut}(Q)$, $\theta = \gamma_\phi \circ \theta' \circ \sigma^{-1}$, ו־$c' = \phi \circ c \circ (\sigma^{-1} \times \sigma^{-1})$.
2. נניח ש־$\theta' = \theta$. יש איזומורפיזם $G \to G'$ המשרה את הזהות על Q, אם ורק אם יש $\phi \in \mathrm{C}_{\mathrm{Aut}(K)}(\mathrm{Im}(\theta))$ כך ש־$c'_{q,q'} = \phi(c_{q,q'})$ לכל $q, q' \in Q$.

תרגיל 7.4.36 (***) $|Q| \cdot \mathrm{H}^2(Q,K) = 0$. (כלומר, לכל $a \in \mathrm{Z}^2(Q,K)$, $|Q| \cdot a$ קוהומולוגי לאפס.)

פתרון. נסמן $a_q = \sum_{g \in Q} c_{q,g}$. לכל $q, q' \in Q$, מתקיים $a_q + q(a_{q'}) - a_{qq'} = \sum_g c_{q,g} + \sum_g (q(c_{q',g}) - c_{qq',g}) = \sum_g c_{q,g} + \sum_g (c_{q,q'} - c_{q,q'g}) = |Q| c_{q,q'}$.

גם כאן, פירות המאמץ הם תוצאה חשובה על המבנה של חבורות סופיות.

תרגיל 7.4.37 (***) נניח ש־K אבלית ו־$(|Q|,|K|)=1$. אז כל הרחבה של Q על־ידי K היא מכפלה ישרה למחצה. **הדרכה.** מתרגיל 7.4.36 וקיומו של צירוף $\alpha|Q|+\beta|K|=1$, נובע ש־$\mathrm{H}^2(Q,K)=0$. לכן תקפה מסקנת תרגיל 7.4.34.

בניסוח אחר: לכל תת־חבורה אבלית נורמלית, שהסדר שלה זר לאינדקס, יש משלים. במשפט 8.4.65 נתבסס על התוצאה הזו כדי להסיר את ההנחה ש־K אבלית.

תרגיל 7.4.38 (**) תהי A חבורה אבלית, עם פעולה של $Q=\{1,x\}\cong\mathbb{Z}_2$ לפי $\tau\in\mathrm{Aut}(A)$ המקיים $\tau^2=\mathrm{id}$. הראה ש־$\mathrm{H}^2(\mathbb{Z}_2,A)=\mathrm{Ker}(1-\tau)/\mathrm{Im}(1+\tau)$. **הדרכה.** על־פי תרגיל 7.4.30 אפשר להניח ש־$[c]\in\mathrm{H}^2(Q,A)$ מיוצג על־ידי $c\in\mathrm{Z}^2(Q,A)$ עם $c_{1,1}=c_{1,x}=c_{x,1}=0$, וכך לזהות את c עם $c_{x,x}\in A$. **הערה.** בתרגיל 7.4.17.(4) הראינו ש־$\mathrm{H}^1(\mathbb{Z}_2,A)=\mathrm{Ker}(1+\tau)/\mathrm{Im}(1-\tau)$.

תרגיל 7.4.39 (***) נניח ש־$Q=\mathbb{Z}_n$ פועלת באופן טריוויאלי על החבורה האבלית K. הראה ש־$\mathrm{H}^2(\mathbb{Z}_n,K)=K/nK$.

תרגיל 7.4.40 (**) תהיינה $Q=\mathbb{Z}_2$ ו־$A=\langle y\mid y^4=1\rangle\cong\mathbb{Z}_4$. תאר את החבורות G עם $A\lhd G$ ו־$G/A\cong Q$, שבהן פעולת Q על A טריוויאלית. **הדרכה.** לפי תרגיל 7.4.38, $\mathrm{H}^2(Q,A)=A/2A=\langle y\mid y^2=1\rangle$. לכן יש הרחבה אחת טריוויאלית, $\mathbb{Z}_4\times\mathbb{Z}_2$, ואחת שבה $G=A\cup Az_x$ עם $z_1=1$ ו־$z_x^2=c_{x,x}z_{x^2}=y$; זוהי אם כך החבורה $G=\langle y,x\mid y^4=1,\,xyx^{-1}=y,\,x^2=y\rangle\cong\mathbb{Z}_8$.

תרגיל 7.4.41 (**) חזור על תרגיל 7.4.40 עם הפעולה הלא־טריוויאלית היחידה, $x:y\mapsto y^{-1}$. **הדרכה.** לפי תרגיל 7.4.38, $\mathrm{H}^2(Q,A)=A_2=\langle y^2\rangle$. לכן יש הרחבה אחת טריוויאלית, $\mathbb{Z}_4\rtimes_{-1}\mathbb{Z}_2=\langle y,x:\,y^4=x^2=1,\,xyx^{-1}=y^{-1}\rangle\cong D_4$, ואחת שבה $G=A\cup Az_x$ עם $z_1=1$ ו־$z_x^2=c_{x,x}z_{x^2}=y^2$, היינו $G=\langle y,x\mid y^4=1,\,xyx^{-1}=y^{-1},\,x^2=y^2\rangle\cong Q$.

תרגיל 7.4.42 (**) תהי $K\lhd G$ תת־חבורה נורמלית. הראה ש־$\sigma(gK)=\sigma(g)K$ מגדיר הומומורפיזם $\mathrm{Aut}(G,K)\to\mathrm{Aut}(G/K)$ (ראה הגדרה 7.2.37).

נסיים בבניה הקושרת את החבורות שפגשנו בשני הסעיפים הקודמים, ורומזת לתאוריה כללית הנקראת **קוהומולוגיה של חבורות**.

הגדרה 7.4.43 *תהי Q חבורה הפועלת על חבורה אבלית K. נגדיר פונקציות קיצור $\pi_i:Q^{n+1}\to Q^n$ לפי $\pi_i(q_0,\dots,q_n)=(q_0,\dots,q_{i-1},q_iq_{i+1},q_{i+2},\dots,q_n)$ (כאשר $i=0,\dots,n-1$), ו־$\pi_n(q_0,\dots,q_n)=(q_0,\dots,q_{n-1})$.*
נסמן $C^i(Q,K)=\{f:Q\times\dots\times Q\to K\}$, כאשר המכפלה כוללת i עותקים של Q. בפרט, $C^0(Q,K)=K$. כעת נגדיר

$$C^0(Q,K)\xrightarrow{\partial^0}C^1(Q,K)\xrightarrow{\partial^1}C^2(Q,K)\xrightarrow{\partial^2}C^3(Q,K)\xrightarrow{\partial^3}C^4(Q,K)\longrightarrow\cdots$$

לפי

$$(\partial^n f)(q_0,\dots,q_n)=q_0\cdot f(q_1,\dots,q_n)+\left(\sum_{i=0}^{n}(-1)^{i+1}f\circ\pi_i\right)(q_0,\dots,q_n).$$

בפרט,

$$\begin{aligned}(\partial^0u)_q&=q(u)-u;\\(\partial^1a)_{q,q'}&=q(a_{q'})-a_{qq'}+a_q;\\(\partial^2c)_{q,q',q''}&=q(c_{q',q''})-c_{qq',q''}+c_{q,q'q''}-c_{q,q'}.\end{aligned}$$

תרגיל 7.4.44 (**) הוכח שתמיד $\partial^{n+1}\partial^n=0$ והסק ש־$\mathrm{Im}(\partial^n)\subseteq\mathrm{Ker}(\partial^{n+1})$.

תרגיל 7.4.45 (**) בדוק עבור $n=1,2$ ש־$\mathrm{Z}^n(Q,K)=\mathrm{Ker}(\partial^n)$ ו־$\mathrm{B}^n(Q,K)=\mathrm{Im}(\partial^{n-1})$. לכן $\mathrm{H}^n(Q,K)=\mathrm{Ker}(\partial^n)/\mathrm{Im}(\partial^{n-1})$.

הרחבות מרכזיות

הרחבה G של Q על־ידי K נקראת **מרכזית** אם $K \subseteq \mathrm{Z}(G)$. (זהו בדיוק המקרה שבו פעולת Q על K טריוויאלית.)

תרגיל 7.4.46 (-*)** תהי G הרחבה מרכזית של Q על־ידי חבורה K. נסמן ב־$\mathrm{Aut}(G;K,Q)$ את הגרעין של ההומומורפיזם מתרגיל 7.4.42. הראה ש־$\mathrm{Aut}(G;K,Q) \cong \mathrm{Hom}(Q,K)$. **הדרכה.** בהנתן $\sigma \in \mathrm{Aut}(G;K,Q)$, הגדר $\psi_\sigma : Q \to K$ לפי $\psi_\sigma(gK) = \sigma(g)g^{-1}$; הראה ש־$\psi_\sigma(gK)$ מוגדר היטב, ש־ψ_σ הוא הומומורפיזם, וש־$\Psi : \sigma \mapsto \psi_\sigma$ הומומורפיזם עם גרעין טריוויאלי. הראה שלכל $\psi \in \mathrm{Hom}(Q,K)$, הפונקציה $\sigma : G \to G$ המוגדרת על־ידי $\sigma(g) = \psi(gK)g$ היא אוטומורפיזם, ולכן Ψ על.

תרגיל 7.4.47 (+*) כל הרחבה של Q על־ידי $\mathbb{Z}_2$ היא הרחבה מרכזית. **הדרכה.** תרגיל 4.7.1.

תרגיל 7.4.48 (-*)** הראה שיש שתי הרחבות מרכזיות של $A_4 \cong \mathrm{PSL}_2(\mathbb{F}_3)$ (תרגיל 6.7.20) על־ידי $\mathbb{Z}_2$, והן $A_4 \times \mathbb{Z}_2$ ו־$\mathrm{SL}_2(\mathbb{F}_3)$.
הדרכה. תחילה אשר ש־$A_4 \times \mathbb{Z}_2$ ו־$\mathrm{SL}_2(\mathbb{F}_3)$ הן אכן הרחבות מרכזיות. לפי ההנחה והייצוג מתרגיל 3.6.23 ל־A_4, יש i,j,k כך ש־

$$G = \left\langle x,y,z \mid x^3 = z^i,\ y^3 = z^j,\ (xy)^2 = z^k,\ xz = zx,\ yz = zy,\ z^2 = 1 \right\rangle.$$

החלף את x,y ב־xz^i, yz^j בעזרת תרגיל 3.6.16, והסק שיש לכל היותר שתי הרחבות מרכזיות.

תרגיל 7.4.49 (***) הראה שיש שתי הרחבות מרכזית של $A_5 \cong \mathrm{PSL}_2(\mathbb{F}_5)$ (תרגיל 6.7.31) על־ידי $\mathbb{Z}_2$, והן $A_5 \times \mathbb{Z}_2$ ו־$\mathrm{SL}_2(\mathbb{F}_5)$. **הדרכה.** כמו בתרגיל 7.4.48, יש i,j,k כך ש־

$$G = \left\langle x,y,z \mid x^3 = z^i,\ y^5 = z^k,\ (xy)^2 = z^k,\ xz = zx,\ yz = zy,\ z^2 = 1 \right\rangle.$$

החלף את x,y,z ב־$x^{-1}z^i, y^{-1}z^k, z$ בעזרת תרגיל 3.6.16.

תרגיל 7.4.50 (***) הראה ש־$\mathrm{H}^2(A_5,\mathbb{Z}_2) \cong \mathbb{Z}_2$. **הדרכה.** תרגיל 7.4.49.

תרגיל 7.4.51 (***) הראה שיש ארבע הרחבות מרכזיות של S_4 על־ידי $\mathbb{Z}_2$: $S_4 \times \mathbb{Z}_2$,

$$\begin{aligned}
&\left\langle x,y \mid x^3 = 1,\ y^4 = 1,\ (xy)^4 = 1,\ (xy)^2 = (yx)^2 \right\rangle,\\
&\left\langle x,y \mid x^3 = 1,\ y^8 = 1,\ (xy)^2 = 1,\ [y^4,x] = 1 \right\rangle \cong \mathrm{GL}_2(\mathbb{F}_3),\\
&\left\langle x,y \mid x^3 = 1,\ y^8 = 1,\ (xy)^2 = y^4,\ [y^4,x] = 1 \right\rangle.
\end{aligned}$$

הראה שכולן שונות זו מזו. **הדרכה.** למשל על־ידי חישוב האבליזציה (משפט 4.8.6) וקיומם של איברים מסדר 8.

תרגיל 7.4.52 (**) יהיו F שדה ו־$V = F^n$ מרחב וקטורי ממימד n מעל F. הראה שחבורת המטריצות

$$G = \left\{ \begin{pmatrix} 1 & x^{\mathrm{t}} & y^{\mathrm{t}} & \alpha \\ & I & 0 & y \\ & & I & -x \\ & & & 1 \end{pmatrix} \ :\ x,y \in V, \alpha \in F \right\} \leq \mathrm{SL}_{2n+1}(F).$$

היא הרחבה מרכזית $1 \longrightarrow F \longrightarrow G \longrightarrow V \longrightarrow 1$. חשב את האיבר של $\mathrm{H}^2(V,F)$ המתאים לה.

כיסויים

הרחבה $1 \longrightarrow K \longrightarrow G \longrightarrow Q \longrightarrow 1$ של Q ב־K היא **הרחבת גזע** (stem extension) אם $K \subseteq Z(G) \cap G'$. בפרט, כל הרחבת גזע היא מרכזית. הרחבת גזע של Q נקראת **כיסוי** אם $|G|$ מקסימלי בין הרחבות הגזע של Q (לכל חבורה סופית יש כיסוי, שאינו בהכרח יחיד).

תרגיל 7.4.53 (***) נניח ש־Q נתונה על־ידי ייצוג $Q = F/R$. הראה ש־$G = F/R_1$ היא כיסוי של Q אם ורק אם $[R,F] \subseteq R_1 \subseteq R$, $R \subseteq F'R_1$, ו־$|F/R_1|$ מקסימלית בכפוף לתנאים אלה.

תרגיל 7.4.54 (**) מימוש אלגוריתמי של תרגיל 7.4.53: נניח שהחבורה Q מוצגת כמנה של החבורה החופשית $F = \langle x_1, \dots, x_n \rangle$ מודולו חבורת היחסים $R = \langle r_1, \dots, r_t \rangle^F$. אם $G = F/R_1$ כיסוי של Q, אז יש $\omega_1, \dots, \omega_t \in F' \cap R$ כך ש־$R_1 = \langle \omega_j r_j, [x_i, r_j] \rangle^F$. באופן עוד יותר קונקרטי, נסמן ב־$\hat{Q} = F/[R,F] = \langle x_1, \dots, x_n \mid [x_i, r_j] \rangle$ את ההרחבה המרכזית המקסימלית של Q שבה היחסים r_j מרכזיים. כל כיסוי של Q הוא מהצורה $\hat{Q}/\langle \omega_1 r_1, \dots, \omega_t r_t \rangle$ כאשר $\omega_j \in \hat{Q}' \cap \langle r_1, \dots, r_t \rangle$.

תרגיל 7.4.55 (*־)** הראה שהכיסויים של $\mathbb{Z}_2 \times \mathbb{Z}_2$ הם החבורות הלא אבליות מסדר 8. **הדרכה**. הראה שהחבורות D_4, Q_8 אכן מכסות את $\mathbb{Z}_2 \times \mathbb{Z}_2$.

תרגיל 7.4.56 (*־)** הראה בעזרת תרגיל 7.4.54 שהכיסויים של D_4 הם החבורות הבאות מסדר 16: D_8, Q_{16} ו־ $\mathbb{Z}_8 \rtimes_3 \mathbb{Z}_2 = \left\langle x, y \mid x^8 = 1,\, yxy^{-1} = x^3,\, y^2 = 1 \right\rangle$.
הדרכה. נבחר ייצוג $D_4 = \langle x, y \mid x^4 = y^2 = yxy^{-1}x = 1 \rangle$, ונפעיל את תרגיל 7.4.54. ההרחבה המרכזית היא $\hat{Q} = \langle x, y, \omega \mid \omega^4 = [x, \omega] = 1,\, y\omega y^{-1} = \omega^{-1},\, yx = \omega xy \rangle$; בחבורה הזו $\hat{Q}' = \langle \omega \rangle \cong \mathbb{Z}_4$, ותמונת R היא $\langle x^4, y^2, \omega x^2 \rangle$. לכן $\hat{Q}' \cap R = \langle \omega^2 \rangle$. מכאן שהכיסויים של Q הם מהצורה

$$\left\langle x, y, \omega \mid \omega^4 = [x, \omega] = 1,\, y\omega y^{-1} = \omega^{-1},\, yx = \omega xy,\, \omega^{2i}x^4 = \omega^{2j}y^2 = \omega^{2k+1}x^2 = 1 \right\rangle$$

עבור $i, j, k \in \{0,1\}$. סימטריות משאירות רק חמישה ייצוגים, שאחד מהם, של D_4, אינו מסדר מקסימלי. שאר החבורות הן $\langle x, y \mid x^8 = 1,\, yxy^{-1} = x^{4a-1},\, y^2 = x^{4b} \rangle$ עבור $a, b \in \{0,1\}$ (אם $a = 1$ המקרים $b = 0,1$ איזומורפיים), שכולן הרחבות של D_4 על־ידי $\mathbb{Z}_2$ (וגם הרחבות של $\mathbb{Z}_2$ על־ידי $\mathbb{Z}_8$).

7.4.3 הרחבות בחבורה K שאינה אבלית

כשטיפלנו בהרחבות עם גרעין אבלי, ראינו שההרחבה משרה פעולה של המנה Q על הרגעין K על־ידי הצמדה (מוגדרת היטב) בהרמה של האיבר ל־G. מתברר שאפשר לשמר חלק מן הפעולה הזו גם כאשר K אינה אבלית. להומומורפיזם $Q \to \mathrm{Out}(K)$ נקרא **פעולה חיצונית** של Q על K; זוהי אינה פעולה.

תרגיל 7.4.57 (**) הרחבה G של Q על־ידי חבורה K משרה פעולה חיצונית של Q על K.
הדרכה. הראה שהדיאגרמה הבאה מתחלפת, כאשר ההעתקה $G \to \mathrm{Aut}(K)$ היא פעולת ההצמדה, וההעתקה $\alpha : Q \to \mathrm{Out}(K)$ מוגדרת לפי $(gK) \mapsto \gamma_g|_K \mathrm{Inn}(K)$.

$$\begin{tikzcd}
1 \arrow[r] & K \arrow[r] \arrow[d] & G \arrow[r] \arrow[d] & Q \arrow[r] \arrow[d, "\alpha"] & 1 \\
1 \arrow[r] & \mathrm{Inn}(K) \arrow[r] & \mathrm{Aut}(K) \arrow[r] & \mathrm{Out}(K) \arrow[r] & 1
\end{tikzcd}$$

תרגיל 7.4.58 (*) אם K אבלית, מתקבלת הפעולה מתרגיל 7.4.22. **הדרכה**. במקרה זה $\mathrm{Inn}(K) \cong K/Z(K) = 1$ ולכן $\mathrm{Out}(K) = \mathrm{Aut}(K)$.

תרגיל 7.4.59 (־)** פעולה חיצונית של Q על K משרה פעולה על $Z(K)$. **הדרכה**. תרגיל 7.2.15.

הערה 7.4.60 השלשה $(K, Q, \alpha: Q \to \mathrm{Out}(K))$ משרה איבר של חבורת הקוהומולוגיה $\mathrm{H}^3(Q, \mathrm{Z}(K))$ (ביחס לפעולת Q על $\mathrm{Z}(K)$ המושרית על־ידי α), שהוא טריוויאלי אם ורק אם יש הרחבה של Q על־ידי K המשרה את α. בפרט, אם $\mathrm{H}^3(Q, \mathrm{Z}(K)) = 1$ אז לכל פעולה חיצונית יש הרחבה המשרה אותה. (בדומה לתרגיל 7.4.37, אם $(|Q|, |\mathrm{Z}(K)|) = 1$ מובטח ש־$\mathrm{H}^3(Q, \mathrm{Z}(K)) = 1$.)

הערה 7.4.61 תהי $(K, Q, \alpha: Q \to \mathrm{Out}(K))$ שלשה שאפשר לממש בהרחבה. מתברר ש־$\mathrm{H}^2(Q, \mathrm{Z}(K))$ פועלת באופן רגולרי על אוסף ההרחבות המשרות את α עד כדי שקילות (שאיננו מגדירים כאן). שלא כמו במקרה ש־K אבלית, כאן אין מעמד מיוחד למכפלות ישרות למחצה: יתכן שאין כאלה, ויתכן שיש יותר מאחת (הרי פעולת Q על $\mathrm{Z}(K)$ אינה קובעת פעולה על K כולה). בפרט, אם $\mathrm{H}^2(Q, \mathrm{Z}(K)) = 1$, יש הרחבה יחידה המשרה את α.

תרגיל 7.4.62 (*) תהי K חבורה עם מרכז טריוויאלי. אז לכל חבורה Q ופעולה חיצונית α של Q על K, יש הרחבה יחידה $1 \longrightarrow K \longrightarrow G \longrightarrow Q \longrightarrow 1$ המשרה את α. **הדרכה.** על פי ההערות.

תרגיל 7.4.63 (**) אפשר להמשיך את הדיאגרמה של תרגיל 7.4.57 לדיאגרמה שבה השורות והעמודות מדוייקות, כאשר $Q^0 = \mathrm{Ker}(\alpha)$. הראה ש־$Q^0 \cong K\mathrm{C}_G(K)/K$.

$$\begin{tikzcd}
 & 1 \arrow[d] & 1 \arrow[d] & 1 \arrow[d] & \\
1 \arrow[r] & \mathrm{Z}(K) \arrow[r] \arrow[d] & \mathrm{C}_G(K) \arrow[r] \arrow[d] & Q^0 \arrow[r] \arrow[d] & 1 \\
1 \arrow[r] & K \arrow[r] \arrow[d] & G \arrow[r] \arrow[d] & Q \arrow[r] \arrow[d, "\alpha"] & 1 \\
1 \arrow[r] & \mathrm{Inn}(K) \arrow[r] \arrow[d] & \mathrm{Aut}(K) \arrow[r] & \mathrm{Out}(K) \arrow[r] & 1 \\
 & 1 & & &
\end{tikzcd}$$

הדרכה. שתי השורות התחתונות מדוייקות לפי תרגיל 7.4.57; העמודות מדוייקות לפי תרגיל 7.2.4 והגדרת Q^0. נשאר להראות שהשורה העליונה מדוייקת. אם $g \in \mathrm{C}_G(K)$ אז תמונתו ב־Q שייכת ל־Q^0 משום ש־α מעביר אותה ליחידה. מאידך, לכל $q \in Q^0$ יש $z_q \in G$ כך שההטלה $G \to Q$ שולחת $z_q \mapsto q$. מכיוון שההצמדה ב־z_q משרה על K אוטומורפיזם פנימי לפי ההנחה, אפשר להחליף את z_q בנציג המתחלף עם K; כלומר, $z_q \in \mathrm{C}_G(Q)$, ולכן ההטלה $\mathrm{C}_G(K) \to Q^0$ המושרית מ־$G \to Q$ היא על. גרעין ההטלה הזו הוא $\mathrm{C}_G(K) \cap K = \mathrm{Z}(K)$.

תרגיל 7.4.64 (***) תהי $1 \to K \to G \to Q \to 1$ הרחבה. התכונות הבאות שקולות עבור הדיאגרמה של תרגיל 7.4.57:

1. K אבלית.
2. יש העתקה $Q \to \mathrm{Aut}(K)$ (המסומנת כאן בחץ מקווקו) השומרת על כך שהדיאגרמה תתחלף:

$$\begin{tikzcd}
1 \arrow[r] & K \arrow[r] \arrow[d] & G \arrow[r] \arrow[d] & Q \arrow[r] \arrow[d] \arrow[dl, dashed] & 1 \\
1 \arrow[r] & \mathrm{Inn}(K) \arrow[r] & \mathrm{Aut}(K) \arrow[r] & \mathrm{Out}(K) \arrow[r] & 1
\end{tikzcd}$$

הדרכה. אם K אבלית אין מה להוכיח כי השורה התחתונה היא $1 \to 1 \to \mathrm{Aut}(K) = \mathrm{Aut}(K) \to 1$. נניח שהחץ האלכסוני קיים, אז תמונת איבר של K ב־$\mathrm{Aut}(K)$ עוברת דרך $K \to G \to Q$ ולכן שווה ל־1; לכן גם תמונת K ב־$\mathrm{Inn}(K)$ טריוויאלית.

תרגיל 7.4.65 (+)** תהי $1{\to}K{\to}G{\to}Q{\to}1$ הרחבה. התכונות הבאות שקולות עבור הדיאגרמה של תרגיל 7.4.57:

1. הפעולה $G{\to}\mathrm{Aut}(K)$ טריוויאלית.
2. G הרחבה מרכזית של Q ב־K (ובפרט $K \subseteq \mathrm{Z}(G)$ ולכן K אבלית).
3. K אבלית והפעולה החיצונית $\alpha\colon Q{\to}\mathrm{Out}(K)$ טריוויאלית.
4. יש הומומורפיזמים $Q{\to}\mathrm{Aut}(K)$ ו־$G{\to}\mathrm{Inn}(K)$ (מסומנים בקו מקווקו) שעבורם הדיאגרמה מתחלפת:

$$\begin{tikzcd}
1 \arrow[r] & K \arrow[r] \arrow[d] & G \arrow[r] \arrow[d] \arrow[dl, dashed] & Q \arrow[r] \arrow[d] \arrow[dl, dashed] & 1 \\
1 \arrow[r] & \mathrm{Inn}(K) \arrow[r] & \mathrm{Aut}(K) \arrow[r] & \mathrm{Out}(K) \arrow[r] & 1
\end{tikzcd}$$

הרחבות עם פעולה חיצונית טריוויאלית

תרגיל 7.4.66 (+)** תהי $1{\to}K{\to}G{\to}Q{\to}1$ הרחבה. התכונות הבאות שקולות עבור הדיאגרמה של תרגיל 7.4.57:

1. הפעולה החיצונית $Q{\to}\mathrm{Out}(K)$ טריוויאלית (כלומר $Q^0 = Q$).
2. ההרכבה $G{\to}\mathrm{Aut}(K){\to}\mathrm{Out}(K)$ טריוויאלית.
3. יש העתקה $G{\to}\mathrm{Inn}(K)$ (המסומנת כאן בחץ מקווקו) השומרת על כך שהדיאגרמה תתחלף:

$$\begin{tikzcd}
1 \arrow[r] & K \arrow[r] \arrow[d] & G \arrow[r] \arrow[d] \arrow[dl, dashed] & Q \arrow[r] \arrow[d] & 1 \\
1 \arrow[r] & \mathrm{Inn}(K) \arrow[r] & \mathrm{Aut}(K) \arrow[r] & \mathrm{Out}(K) \arrow[r] & 1
\end{tikzcd}$$

4. $G = K\mathrm{C}_G(K)$.

הדרכה. (2) שקול לכך שההרכבה $G{\to}Q{\to}\mathrm{Out}(K)$ טריוויאלית, וזה שקול ל־(1) מכיוון ש־$G{\to}Q$ על. כמו־כן, (2) שקול לכך שתמונת $G{\to}\mathrm{Aut}(K)$ נמצאת למעשה ב־$\mathrm{Inn}(K)$. השקילות ל־(4) נובעת מכך שההטלה $G{\to}Q$ משרה $K\mathrm{C}_G(K)/K \cong Q^0$.

לסיכום, פגשנו שלושה סוגים מיוחדים של הרחבות:

1. הרחבה היא מרכזית אם ורק אם אפשר לשבור למשולשים את שני הריבועים בדיאגרמה;
2. K אבלית אם ורק אם אפשר לשבור את הריבוע הימני;
3. הפעולה החיצונית טריוויאלית אם ורק אם אפשר לשבור את הריבוע השמאלי.

בסתם הרחבה, יתכן שיש חצים אלכסוניים שעבורם מתחלפים המשולשים החיצוניים - אבל לא הפנימיים - בדיאגרמה, ויתכן שלא. אם $G = K \rtimes Q$ אז פעולת Q על K שוברת את הריבוע הימני לשני משולשים, שהחיצוני ביניהם מתחלף (הפנימי מתחלף אם ורק אם K אבלית).

תרגיל 7.4.67 (**) בהרחבה שבה הפעולה החיצונית טריוויאלית, פעולת Q על $\mathrm{Z}(K)$ גם היא טריוויאלית.

תרגיל 7.4.68 (*) תהי K חבורה עם $\mathrm{Z}(K) = 1$. אז לכל חבורה Q, ההרחבה היחידה של Q על־ידי K המשרה את הפעולה החיצונית הטריוויאלית היא המכפלה הישרה $K \times Q$. **הדרכה.** לפי תרגיל 7.4.62, משום ש־$K \times Q$ אכן משרה את הפעולה החיצונית הטריוויאלית.

תרגיל 7.4.69 (***) תהי $1{\to}K{\to}G{\to}Q{\to}1$ הרחבה כך שהפעולה החיצונית של Q היא טריוויאלית (היינו מתקיימים תנאי תרגיל 7.4.66). אז יש הרחבה $1{\to}\mathrm{Z}(K){\to}\mathrm{C}_G(K){\to}Q{\to}1$ עם דיאגרמה קומוטטיבית

$$\begin{tikzcd}
1 \arrow[r] & \mathrm{Z}(K) \arrow[r] \arrow[d, hook] & \mathrm{C}_G(K) \arrow[r] \arrow[d, hook] & Q \arrow[r] \arrow[d, equal] & 1 \\
1 \arrow[r] & K \arrow[r] & G \arrow[r] & Q \arrow[r] & 1
\end{tikzcd}$$

הדרכה. זהו המקרה $\alpha = 1$ בתרגיל 7.4.63.

תרגיל 7.4.70 (**) אם בדיאגרמה של תרגיל 7.4.69 ההרחבה $1{\to}\mathrm{Z}(K){\to}\mathrm{C}_G(K){\to}Q{\to}1$ מתפצלת, אז $G \cong K \times Q$. **הדרכה.** העתקת הפיצול $Q{\to}\mathrm{C}_G(Q)$ היא גם העתקת פיצול $Q{\to}G$, ולכן $G = K{\rtimes}Q$, אבל מכיוון ש־$Q \subseteq \mathrm{C}_G(K)$, $Q{\lhd}G$ ולכן המכפלה ישרה.

תרגיל 7.4.71 (+*)** תהי $1{\to}K{\to}G{\to}Q{\to}1$ הרחבה המשרה פעולה חיצונית טריוויאלית. אם $\mathrm{H}^2(Q, \mathrm{Z}(K)) = 1$, אז $G \cong K \times Q$.

הדרכה. בהמשך לתרגיל 7.4.69, משתי ההנחות נובע ש־$1{\to}\mathrm{Z}(K){\to}\mathrm{C}_G(K){\to}Q{\to}1$ מתפצלת, והתוצאה נובעת מתרגיל 7.4.70.

תרגיל 7.4.72 (+*)** תהי K חבורה שלמה (הגדרה 7.3.41). כל הרחבה G של חבורה Q על־ידי K איזומורפית ל־$K \times Q$. **הדרכה.** מיידי מתרגיל 7.4.71.

תרגיל 7.4.73 (+*)** אם $\mathrm{Z}(K) = 1$, $\mathrm{Out}(K)$ אבלית ו־Q פשוטה לא אבלית, אז ההרחבה היחידה של Q על־ידי K היא $K \times Q$. **הדרכה.** מיידי מתרגיל 7.4.71; די להניח ש־$\mathrm{Out}(K)$ פתירה (הגדרה 10.2.1).

תרגיל 7.4.74 (+*)** ההרחבה היחידה של חבורה פשוטה סופית לא אבלית אחת בחבורה פשוטה לא אבלית סופית שניה, היא המכפלה הישרה שלהן. **הדרכה.** תרגיל 7.4.73, לפי הערה 7.2.24.

7.5 סימטריות של גרפים

הגדרה 7.5.1 גרף על קבוצת קודקודים V הוא אוסף של זוגות לא סדורים, הקרויים קשתות. סימטריה של הגרף הוא תמורה $\sigma \in S_V$, המעבירה כל קשת לקשת בגרף.

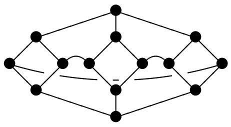
תרגיל 7.5.2 (+*) חבורת הסימטריות של גרף היא החבורה הגדולה ביותר הפועלת עליו בצורה נאמנה.

תרגיל 7.5.3 (*) חבורת הסימטריות של הגרף הריק על n נקודות היא S_n.

תרגיל 7.5.4 (*) חבורת הסימטריות של גרף שווה לחבורת הסימטריות של הגרף המשלים (זה שהקשתות שלו הם הזוגות שאינם מהווים קשתות בגרף המקורי).

תרגיל 7.5.5 (**) חבורת הסימטריות של טבעת עם n קודקודים היא D_n.

תרגיל 7.5.6 (**) שרטט שניים־שלושה גרפים נאים למראה ומצא את חבורות הסימטריות שלהם.



תרגיל 7.5.7 (***) הראה שהגרף משמאל מתאר את 14 הטריאנגולציות של משושה משוכלל, כאשר זוג טריאנגולציות מחובר בקשת אם ניתן לעבור ביניהן על־ידי הזזת קו אחד. הוכח שחבורת הסימטריות של הגרף היא S_3. מצא את חבורת הסימטריות של הגרף המתקבל ממחיקת שלוש הקשתות המעוגלות.

תרגיל 7.5.8 (***) הראה שחבורת הסימטריות $\mathrm{Aut}(C)$ של קוביה קשיחה איזומורפית ל־S_4.
הדרכה. הפעולה על ארבעת האלכסונים הראשיים מגדירה הומומורפיזם $H \to S_4$; הראה ש־$|H| = 24$ וכדי לסיים בדוק למשל שסיבוב ב־$180°$ סביב חתך אלכסוני מחליף שני אלכסונים.

הראה שחבורת הסימטריות של גרף המקצועות של הקוביה היא $S_4 \times \mathbb{Z}_2$ (העזר בתרגיל 4.3.22).

תרגיל 7.5.9 (*-)** הראה שהשיכון $\psi: S_4 \to S_6$ המתקבל מפעולת $\mathrm{Aut}(C)$ של תרגיל 7.5.8 על שש הפאות מוגדר (תחת מספור מתאים) לפי

$$(12) \mapsto (13)(24)(56), \quad (23) \mapsto (12)(36)(45), \quad (34) \mapsto (14)(23)(56).$$

מצא את מבנה המחזורים ב־S_6 של $\psi(\sigma)$ לפי מבנה המחזורים של $\sigma \in S_4$.

תרגיל 7.5.10 (+)** הוכח את נכונות הטענות בטבלה הבאה, עבור הפעולה של S_4 על קוביה קשיחה.

תאור האברים	מספרם	מבנה מחזורים בפעולה על אלכסונים	מבנה מחזורים בפעולה על פאות	מבנה מחזורים בפעולה על קודקודים	מבנה מחזורים בפעולה על צלעות
הזהות	1	$[1^4]$	$[1^6]$	$[1^8]$	$[1^{12}]$
סיבוב סביב חתך אלכסוני	6	$[2^1 1^2]$	$[2^3]$	$[2^4]$	$[1^2 2^5]$
שליש סיבוב סביב פינה	8	$[3^1 1^1]$	$[3^2]$	$[1^2 3^2]$	$[3^4]$
רבע סיבוב של פאה	6	$[4^1]$	$[1^2 4^1]$	$[4^2]$	$[4^3]$
חצי סיבוב של פאה	3	$[2^2]$	$[1^2 2^2]$	$[2^4]$	$[2^6]$

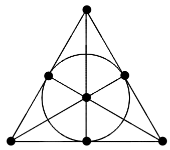
תרגיל 7.5.11 (***) חבורת הסימטריות של האיקוסהדרון (בן עשרים פאות משולשות) היא A_5. נתח באופן דומה לתרגיל 7.5.10 את הפעולות הטבעיות של A_5 על האיקוסהדרון.

תרגיל 7.5.12 (***) הראה ש־A_5 היא גם חבורת הסימטריות של הדודקהדרון (הפאון בן 12 פאות מחומשות). **הדרכה.** האיקוסהדרון והדודקהדרון דואליים זה לזה.

תרגיל 7.5.13 (*-)** קפלר הבחין שיש חמש דרכים לשכן קוביה בדודקהדרון, כך שמקצועותיה הם אלכסונים של הפאות. העזר בעובדה זו כדי לתת הוכחה נוספת לתרגיל 7.5.12.

תרגיל 7.5.14 (*-)** כמה קוביות שונות אפשר ליצור אם צובעים כל פאה באחד מבין n צבעים?
פתרון. $\frac{n^2(n+1)(n^3-n^2+4n+8)}{24}$ קוביות (בפרט יש 10 קוביות בשני צבעים.) **הדרכה.** הפעל את הלמה של ברנסייד מתרגיל 6.5.8 על תרגיל 7.5.9 (או השורה המתאימה מתרגיל 7.5.10).

הגדרה 7.5.15 גאומטריה פרוייקטיבית היא מערכת של נקודות וישרים המקיימת את האקסיומות הבאות: דרך כל שתי נקודות עובר ישר יחיד; כל שני ישרים נפגשים בנקודה; על כל ישר לפחות 3 נקודות; יש ישר ונקודה מחוץ לו.



תרגיל 7.5.16 (**) הראה שהאיור משמאל מתאר גאומטריה פרוייקטיבית, שהיא היחידה עם 7 נקודות. (זהו **מישור פאנו**)

תרגיל 7.5.17 (**) (בניה אלגברית של גאומטריה פרוייקטיבית) יהי F שדה. נתבונן במרחב הוקטורי $V = F^3$; לתת־מרחבים ממימד 1 נקרא **נקודות**, ולתת־מרחבים ממימד 2 נקרא **ישרים**. נאמר שנקודה נמצאת על ישר אם היא מוכלת בו (כלומר, המרחב המתאים לה מוכל במרחב המתאים לו).

1. הראה שהמבנה המתקבל, שאותו נסמן ב־$\mathbb{P}^2F$, הוא אכן גאומטריה פרוייקטיבית.
2. אם $|F| = q$, יש בה q^2+q+1 נקודות וכמספר הזה ישרים; יש $q+1$ נקודות על כל ישר, ו־$q+1$ ישרים דרך כל נקודה.
3. אם $F = \mathbb{F}_2$ מתקבלת הגאומטריה של תרגיל 7.5.16.

תרגיל 7.5.18 (**) **סימטריה** של גאומטריה פרוייקטיבית היא זוג תמורות, σ של הנקודות ו־σ' של הישרים, השומרות על יחס החילה: $\sigma(x) \in \sigma'(\ell)$ אם ורק אם $x \in \ell$. הראה שכל סימטריה של הגאומטריה נקבעת לפי הפעולה שלה על הנקודות.

תרגיל 7.5.19 (+)** 1. החבורה $\mathrm{PGL}_3(F)$ פועלת נאמנה על הגאומטריה $\mathbb{P}^2F$.

2. הפעולה היא טרנזיטיבית בחדות על מרובעים (**מרובע** הוא רביעיה סדורה של נקודות שאף שלוש מהן אינן על ישר אחד).

תרגיל 7.5.20 (+)** עבור $F = \mathbb{F}_2$, $\mathrm{GL}_3(F) = \mathrm{PGL}_3(F)$ הפועלת כבתרגיל 7.5.19, היא חבורת הסימטריות המלאה של $\mathbb{P}^2F$.

גרפי קיילי

ניתן לדלג בקריאה ראשונה.

אם מוגדרים מספר גרפים על אותן נקודות, חבורת הסימטריות של המבנה היא החבורה של תמורות שהן סימטריות של כל אחד ואחד מהגרפים. תהי G חבורה עם יוצרים $g_1, \dots, g_t$. בסעיף 3.6 בנינו t גרפים על הקבוצה G: לכל i, הגרף T_i כולל את הזוגות (x, xg_i). מבנה זה נקרא גרף קיילי של G (ביחס ליוצרים $g_1, \dots, g_t$).

תרגיל 7.5.21 (**) צייר את גרף קיילי של $S_3 = \langle \sigma, \tau \mid \sigma^3 = \tau^2 = (\sigma\tau)^2 = 1 \rangle$ ושל $\mathbb{Z}_6 = \langle \sigma, \tau \mid \sigma^3 = \tau^2 = 1, \sigma\tau = \tau\sigma \rangle$.

תרגיל 7.5.22 (***) הוכח שחבורת האוטומורפיזמים של גרף קיילי פועלת על קבוצת הקודקודים באופן רגולרי והיא איזומורפית ל־G.

פרק 8

משפטי סילו

משפט לגרנז' מראה שהסדר של איברים מחלק תמיד את סדר החבורה. **משפט קושי** הופך את הכיוון, ומראה שאם סדר החבורה מתחלק בראשוני p, אז יש לה איברים מסדר p. ההוכחה מבוססת על **שוויון המחלקות**. משפט קושי מראה שהסדר של חבורה הוא חזקה של ראשוני p אם ורק אם כל האברים שלה הם מסדר חזקה של אותו p; חבורות העונות לתנאי הזה נקראות **חבורות־**p. לחבורות־p יש כמה תכונות מעניינות. המרכז של חבורת־p לעולם אינו טריוויאלי. נובע מכאן שהמנרמל של תת־חבורה תמיד מכיל אותה ממש.

משפטי סילו ממשיכים את הכיוון של משפט קושי, בכך שהם מספקים תת־חבורה מסדר השווה לכל חזקת ראשוני המחלקת את סדר החבורה. סעיף 8.5 מציג בפרוטרוט מספר דרכים להעזר במשפטי סילו, עם משפטים אחרים ובראשם העידון של משפט קיילי, על־מנת לנתח מבנה של חבורה בעלת סדר נתון. היעד העיקרי במקרים רבים הוא להראות שהחבורה אינה פשוטה, משום שאז היא נחשפת לניתוח כהרחבה של שתי חבורות מסדר קטן יותר.

8.1 שוויון המחלקות

סעיף זה מציג את שוויון המחלקות של חבורה סופית. השימושים מופיעים בשני הסעיפים הבאים.

הגדרה 8.1.1 *שוויון המחלקות של חבורה סופית G הוא השוויון*

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

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

חשיבותו של השוויון הזה, המקודד את פירוק החבורה לאיחוד מחלקות הצמידות שלה, היא בכך שלפי תרגיל 6.4.14 המחוברים באגף ימין הם מחלקים אמיתיים (גדולים מ־1) של סדר החבורה.

תרגיל 8.1.2 (*) הוכח את שוויון המחלקות. **הדרכה.** העזר בתרגיל 6.4.5.

תרגיל 8.1.3 (*) אם G אבלית מסדר n, שוויון המחלקות שלה הוא הזהות הטריוויאלית $n = n$.

תרגיל 8.1.4 (**) כתוב את שוויונות המחלקה של S_3, S_4, S_5.

תרגיל 8.1.5 (**) כתוב את שוויונות המחלקה של החבורות הלא אבליות מסדר 8: D_4 והקווטרניונים Q_8.

תרגיל 8.1.6 (**) הראה ששוויון המחלקות של החבורה הדיהדרלית D_6 הוא $12 = 2 + 3 + 3 + 2 + 2$.

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

תרגיל 8.1.7 (**) מצא את כל החבורות שיש להן בדיוק 2 מחלקות צמידות.

תרגיל 8.1.8 (***) 1. הוכח שאם לחבורה יש בדיוק 3 מחלקות צמידות אז $G \cong \mathbb{Z}_3$ או $G \cong S_3$.

2. אם לחבורה G יש בדיוק 4 מחלקות צמידות, אז $|G| \in \{4, 8, 10, 12, 18, 20, 24, 42\}$.

תרגיל 8.1.9 (+*)** תהי G חבורה לא אבלית מסדר pq, $p < q$.

1. $\mathrm{Z}(G) = 1$, ולכן שוויון המחלקות של G (בכתיב מקוצר) הוא $pq = 1 + \alpha p + \beta q$.
2. במחלקות מגודל p יש אברים מסדר q, ולהיפך.
3. (בכל חבורה) מספר האברים מסדר p מתחלק ב־$(p-1)$.
4. $\beta \mid (p-1)$, ולכן $\beta = p-1$. מכאן ש־$\alpha = (q-1)/p$. בפרט $q \equiv 1 \pmod{p}$.
5. ל־G יש תת־חבורה יחידה מסדר q (ו־q תת־חבורות מסדר p).
6. $G \cong \mathbb{Z}_q \rtimes_\theta \mathbb{Z}_p$ עם הומומורפיזם לא טריוויאלי $\theta : \mathbb{Z}_p \to U_q$.

תרגיל 8.1.10 (**) נניח ש־p, q ראשוניים כך ש־$q \equiv 1 \pmod{p}$. אז יש שתי חבורות מסדר pq: $\mathbb{Z}_p \times \mathbb{Z}_p$ ו־ $G \cong \langle x, y :\ x^q = 1, y^p = 1, yxy^{-1} = x^t \rangle$ כאשר $t \in U_q$ איבר (כלשהו) מסדר p.
הדרכה. תרגיל 8.1.9.

תרגיל 8.1.11 (**) יש שתי חבורות לא אבליות מסדר 21: $\mathbb{Z}_3 \times \mathbb{Z}_7$ ו־$\langle x, y \mid x^7 = y^3 = 1,\ yxy^{-1} = x^2 \rangle$.
הדרכה. תרגיל 8.1.10.

תרגיל 8.1.12 (**) (הכללה של שוויון המחלקות) לכל תת־חבורה נורמלית H של G מתקיים $|H| = |\mathrm{Z}(G) \cap H| + \sum |C|$ כשהסכום הוא על מחלקות הצמידות הלא מרכזיות של G המוכלות ב־H (הזכר בתרגיל 6.4.6). כרגיל, אם $C = [x]$ אז $|C| = [G : \mathrm{C}_G(x)]$.

8.2 משפט קושי

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

תרגיל 8.2.1 (*) לכל d, אם G ציקלית מסדר המתחלק ב־d, אז יש ב־G איבר מסדר d.

אבל הוא אינו נכון באופן כללי:

תרגיל 8.2.2 (**) ל־A_4 אין תת־חבורה מסדר 6 (ובפרט אין בה איברים מסדר זה).

משפט קושי (שנוכיח מיד) מראה שהטענה ההפוכה למשפט לגרנז' נכונה בכל־זאת, כשמדובר במחלק ראשוני (הוכחנו זאת עבור $p = 2$ בתרגיל **2.1.13**).

טענה 8.2.3 (משפט קושי לחבורות אבליות) אם ראשוני p מחלק את הסדר של חבורה אבלית A, אז יש ב־A איבר מסדר p.

הוכחה. יהי $1 \neq x \in A$. אם $p \mid e = \mathrm{ord}(x)$ אז $x^{e/p}$ איבר מסדר p. אחרת לפי הנחת האינדוקציה יש קוסט $y\langle x\rangle \in A/\langle x\rangle$ מסדר p, ואז $y^p \in \langle x\rangle$ ו־$p \mid \mathrm{ord}(y)$. □

משפט 8.2.4 (משפט קושי) אם ראשוני p מחלק את הסדר של חבורה G, אז יש ב־G איבר מסדר p.

הוכחה. כתוב את שוויון המחלקות של G: $|G| = |\mathrm{Z}(G)| + \sum [G\colon \mathrm{C}_G(x)]$, כאשר הסכום הוא על נציג x מכל מחלקת צמידות לא מרכזית. אם הסדר של $\mathrm{Z}(G)$ מתחלק ב־p, גמרנו לפי טענה 8.2.3. אחרת יש $x \in G$ שעבורו האינדקס $[G\colon \mathrm{C}_G(x)]$ זר ל־p, ולכן סדר המרכּז $\mathrm{C}_G(x)$ מתחלק ב־p; לפי הנחת האינדוקציה יש ב־$\mathrm{C}_G(x)$ איבר מסדר p. □

תרגיל 8.2.5 (***) הוכח את משפט קושי בעזרת פעולה של $\mathbb{Z}_p$ על קבוצת וקטורים באורך p ב־G. **הדרכה.** התבונן בקבוצה $X = \{(g_0, \dots, g_{p-1})\colon\ g_i \in G,\ g_0g_1\dots g_{p-1} = 1\}$.

1. $\mathbb{Z}_p = \langle\sigma\rangle$ פועלת על X לפי $\sigma(g_0, \dots, g_{p-1}) = (g_1, \dots, g_{p-1}, g_0)$.
2. המסלולים ב־X הם בגודל 1 או p.
3. $|X| = |G|^{p-1}$, ולכן $|X| \equiv 0 \pmod p$.
4. קיים ב־A לפחות מסלול אחד בגודל 1, ולכן קיימים לפחות p כאלה.

תרגיל 8.2.6 (+)** כתוב את ההוכחה שבתרגיל 8.2.5 במקרה $p = 2$, והסבר כיצד היא חוזרת על ההוכחה של תרגיל 2.1.13.

אם $\phi \in \mathrm{Aut}(G)$ 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 8.2.7 (*+) בדוק ש־$N_\phi(\phi(x)) = \phi(N_\phi(x)) = x^{-1}N_\phi(x)x$.

תרגיל 8.2.8 (**) עבור $\gamma_g \in \mathrm{Aut}(G)$, חשב ש־$N_{\gamma_g}(x) = (xg)^n g^{-n}$.

תרגיל 8.2.9 (**) הראה שכל איבר מהצורה $x = t^{-1}\phi(t)$ הוא פתרון למשוואה $N(x) = 1$. (פתרונות אלו הם **טריוויאליים**).

תרגיל 8.2.10 (+)** תהי G חבורה עם אוטומורפיזם ϕ מסדר p. בהמשך להגדרות 7.4.3 ו־7.4.6, הראה שיש התאמה בין 1־קו־מעגלים (אברי $\mathrm{Z}^1(\mathbb{Z}_p, G)$) לפתרונות של המשוואה $N(x) = 1$, כך שה־1־קו־מעגלים השקולים לאיבר היחידה מתאימים לפתרונות הטריוויאליים.

תרגיל 8.2.11 (***) 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.** ראשית הכלל את הפתרון לתרגיל 8.2.5 כדי להראות שאם $|G|$ מתחלק ב־p ו־$\phi \in \mathrm{Aut}(G)$ אוטומורפיזם מסדר p, אז יש בחבורה איברים $x \neq 1$ עם $N_\phi(x) = 1$. (זו טענה שאפשר להוכיח ישירות, על־ידי הפתרונות הטריוויאליים מתרגיל 8.2.9.)

הכלל פתרון זה, עם פעולה של $\mathbb{Z}_p^2$ על אוסף המטריצות (g_{ij}) שבהן המכפלה של כל שורה ועמודה היא 1.

תרגיל 8.2.12 (***) אם p מחלק את $|G|$ ו־$\phi \in \mathrm{Aut}(G)$ 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 8.2.11.

תרגיל 8.2.13 (***) נניח ש־$|G|$ מתחלק ב־3, ו־$\phi \in \mathrm{Aut}(G)$ אוטומורפיזם מסדר 3. אז יש איבר x מסדר 3 כך ש־$[x, \phi(x)] = 1$. **הדרכה.** מתרגיל 8.2.12 נובע ש־$x\phi(x)\phi^2(x) = x\phi^2(x)\phi(x) = 1$ עבור x מתאים.

8.3 חבורות־p

הגדרה 8.3.1 *יהי p ראשוני. חבורה נקראת **חבורת־p** אם הסדר של כל איבר הוא חזקה של p.*

תרגיל 8.3.2 (***) חבורה סופית היא חבורת־p אם ורק אם הסדר שלה הוא חזקה של p. **הדרכה.** כיוון אחד נובע ממשפט לגרנז', והשני ממשפט קושי.

באופן טיפוסי, יש יותר חבורות מסדר p^n מאשר מכל גודל דומה (למשל, יש 2328 חבורות לא איזומורפיות מסדר $2^7 = 128$, ורק 47 מסדר 120). עם זאת, לכל חבורות־p יש מאפיינים משותפים, שנציג בסעיף זה ובסעיפים הבאים.

משפט 8.3.3 לכל חבורת־p סופית יש מֶרְכָּז לא טריוויאלי.

הוכחה. שוויון המחלקות כותב את $|G| = p^t$ כסכום של $|\mathrm{Z}(G)|$ ומחלקים של p^t שהם כולם חזקות p לא טריוויאליות, ולכן מתחלקים ב־p. לכן גם הסדר של $\mathrm{Z}(G)$ מתחלק ב־p.
(M.L. Sylow, *Théorémes sur les groupes de substitutions*, Mathematische Annalen **5**, (1872), Théorème III.) □

תרגיל 8.3.4 (+)** לחבורת־p סופית יש תת־חבורה מרכזית מסדר p.

תרגיל 8.3.5 (**) כל חבורת־p (סופית) פשוטה G היא ציקלית מסדר p. **הדרכה.** אחרת $\mathrm{Z}(G) = G$ ולכל $1 \neq x \in G$, $\langle x \rangle = G$.

תרגיל 8.3.6 (**) תהי G חבורת־p עם תת־חבורה נורמלית H מסדר p. הוכח ש־$H \subseteq \mathrm{Z}(G)$.
הדרכה. משפט N/C.

תרגיל 8.3.7 (***) לכל תת־חבורה אמיתית $H < G$ של חבורת־p, $H < \mathrm{N}_G(H)$. **הדרכה.** באינדוקציה על הסדר. נסמן $Z = \mathrm{Z}(G)$. כמובן, $ZH = HZ$; לכן, אם $H \not\supseteq Z$, אז $H < ZH \leq \mathrm{N}_G(H)$ וסיימנו. נניח אם כן ש־$Z \subseteq H$, ונתבונן בחבורות המנה $H/Z < G/Z$. לפי הנחת האינדוקציה $H/Z < \mathrm{N}_{G/Z}(H/Z) = \mathrm{N}_G(H)/Z$ כשהשתמשנו בתרגיל 6.4.63, ולכן $H < \mathrm{N}_G(H)$.

תרגיל 8.3.8 (*−)** פתור את תרגיל 8.3.7 על־ידי פעולת H על תת־החבורות הצמודות לה.
הדרכה. H פועלת על־ידי הצמדה על הקבוצה Ω של תת־החבורות הצמודות ל־H, שיש בה $[G\!:\!\mathrm{N}_G(H)]$ נקודות. מכיוון ש־H מנרמלת את עצמה, $\{H\}$ מהווה מסלול, ומכיוון שגדלי כל המסלולים מחלקים את $|H|$, יש תת־חבורה צמודה $H_1 = aHa^{-1} \neq H$ שגם היא מהווה מסלול. בפרט $H_1 \lhd HH_1 = H_1H$ ולכן $HaHa^{-1} = HH_1 \leq \mathrm{N}_G(H_1) = a\mathrm{N}_G(H)a^{-1}$ ו־$H < a^{-1}HaH \leq \mathrm{N}_G(H)$.

תרגיל 8.3.9 (**) כל תת־חבורה מאינדקס p של חבורת־p היא נורמלית. **הדרכה.** $H < \mathrm{N}_G(H) \leq G$ לפי תרגיל 8.3.7.

תרגיל 8.3.10 (***) כל תת־חבורה מקסימלית של חבורת־p היא מאינדקס p. **הדרכה.** תהי M תת־חבורה מקסימלית. לפי תרגיל 8.3.7, $M < \mathrm{N}_G(M) \leq G$, ולכן $M \lhd \mathrm{N}_G(M) = G$. יהי $xM \in \mathrm{Z}(G/M)$ איבר מסדר p, אז $M < \langle M, x \rangle$ ולכן $[G\!:\!M] = [\langle M, x \rangle\!:\!M] = p$.

תרגיל 8.3.11 (*−)** כל תת־חבורה נורמלית לא טריוויאלית N של חבורת־p G חותכת את המרכז $\mathrm{Z}(G)$. **הערה.** זו הכללה של משפט 8.3.3. **הדרכה.** שוויון המחלקות המוכלל, תרגיל 8.1.12.

תרגיל 8.3.12 (**) חבורה מסדר p^2 היא אבלית, ואיזומורפית ל־$\mathbb{Z}_{p^2}$ או ל־$\mathbb{Z}_p \times \mathbb{Z}_p$. **הדרכה.** הסק מתרגיל 4.7.5 שהחבורה אבלית. אם אין לה איבר מסדר p^2, אז היא מרחב וקטורי מעל השדה $\mathbb{F}_p$.

תרגיל 8.3.13 (**) G לא אבלית מסדר 2197. זהה את $G/\mathrm{Z}(G)$ עד כדי איזומורפיזם.

תרגיל 8.3.14 (***) תהי G חבורת־p הפועלת על קבוצה X מגודל שאינו מתחלק ב־p. הראה שיש נקודת־שבת המשותפת לכל אברי G. **הדרכה.** הגודל של כל מסלול שאינו נקודת שבת הוא חזקה של p ולכן מתחלק ב־p.

תרגיל 8.3.15 (***) נניח שלחבורה G **יש תת־חבורה מינימלית יחידה**, כלומר, יש תת־חבורה לא טריוויאלית G_0 המוכלת בכל תת־חבורה של G. (תנאי זה שקול לכך שחיתוך כל תת־החבורות הציקליות אינו טריוויאלי).

1. הראה ש־G חבורת־p וש־$G_0 \subseteq \mathrm{Z}(G)$ היא תת־חבורה מסדר p.
2. הראה שכל תת־חבורה אבלית של G היא ציקלית.
3. אם G/G_0 ציקלית אז גם G ציקלית. **הדרכה.** יהי $x \in G$ איבר כך ש־$G/G_0 = \langle G_0x \rangle$, מסדר n; אז $\langle x^n \rangle = G_0 \cap \langle x \rangle = G_0$ ולכן x מסדר pn ו־$G = \langle x \rangle$.
4. נניח ש־p אי־זוגי. הראה שגם ל־G/G_0 יש תת־חבורה מינימלית. **הדרכה.** יהי $z \in G$ איבר כך ש־G_0z מרכזי מסדר p ב־G/G_0. כך $z^p \in G_0$, ו־$\epsilon = z^{p-1}$ הוא יוצר של G_0. יהי $x \in G$ כך ש־$x \notin G_0$. הסדר של $G_0x \in G/G_0$ הוא חזקת־p ולכן מתחלק ב־p; נסמן את הסדר הזה ב־pm. כך $x^{pm} \in G_0$, אבל $x^{pm} \neq 1$ ועל־ידי העלאת x בחזקה זרה ל־p אפשר להניח ש־$x^{pm} = \epsilon$. מכיוון ש־G_0z מרכזי, אפשר לכתוב $zxz^{-1} = \epsilon^j x$, ואז $zx^{-m}z^{-1} = \epsilon^{-jm}x^{-m}$. כעת $(x^{-m}z)^p = \epsilon^{-mj(1+2+\cdots+(p-1))}x^{-mp}z^p = \epsilon^{-pmj(p-1)/2}\epsilon^{-1}\epsilon = 1$ ולכן $x^{-m}z \in G_0$, ומכאן ש־$z \in \langle \epsilon, x^m \rangle \leq \langle G_0, x \rangle$ ו־$G_0z \in \langle G_0x \rangle$.
5. נניח ש־p אי־זוגי. הראה ש־G ציקלית. **הדרכה.** באינדוקציה לפי הסעיף הקודם.
6. מצא חבורה לא ציקלית שיש לה תת־חבורה מינימלית יחידה.

תרגיל 8.3.16 (**) תהי G חבורת־p עם תת־חבורה יחידה מסדר p. הראה שיש לה תת־חבורה מינימלית יחידה (במובן של תרגיל 8.3.15.)

תרגיל 8.3.17 (+)** לחבורה G יש תת־חבורה מינימלית יחידה (תרגיל 8.3.15). הראה ש־G אינה יכולה לפעול נאמנה על קבוצה בגודל $< |G|$.

תרגיל 8.3.18 (**) הראה שמבין החבורות מסדר 8, רק ב־$\mathbb{Z}_8$ ו־Q_8 יש איבר יחיד מסדר 2.

תרגיל 8.3.19 (+)** הראה שאין שיכון $Q_8 \hookrightarrow S_7$. **הדרכה.** תרגיל 8.3.17. ראה גם תרגיל 6.3.8.

תהי G חבורת־p. נסמן ב־$G^p = \langle x^p : x \in G \rangle$ את תת־החבורה הנוצרת על־ידי כל האברים מהצורה x^p.

תרגיל 8.3.20 (**) תהי G חבורת־p. אז $G^p \lhd G$.

תרגיל 8.3.21 (+)** אם $G \neq 1$ חבורת־p, אז $G^p < G$. **הדרכה.** אינדוקציה על $|G|$.

תרגיל 8.3.22 (**) תהי $G = D_8$. חשב את G^2. חשב את G^{2^n} לכל n.

תרגיל 8.3.23 (+)** תהי G חבורת־p שכל תת־החבורות האבליות שלה מסדר p לכל היותר. הוכח ש־$G \cong \mathbb{Z}_p$. **הדרכה.** יהי $z \in \mathrm{Z}(G)$. אם $x \notin \mathrm{Z}(G)$, אז $\langle z, x \rangle$ אבלית.

תרגיל 8.3.24 (***) אם T העתקה לינארית מסדר p של מרחב וקטורי $V \neq 0$ מעל שדה ממאפיין p, אז $V^{\langle T \rangle} = \{v \in V : T(v) = v\} \neq 0$. **הדרכה.** לפי ההנחה $T^p = I$ ולכן T מאפסת את הפולינום $\lambda^p - 1 = (\lambda - 1)^p$. (ראה הכללה בתרגיל 8.3.25)

תרגיל 8.3.25 (***) אם G חבורת־p ו־$A \leq \mathrm{Aut}(G)$ חבורת־p, אז יש נקודת שבת משותפת לא טריוויאלית בפעולה של A על G (היינו $G^A \neq 1$). **הדרכה.** לפי משפט 8.3.3 אפשר להניח ש־G אבלית. המשך באינדוקציה על $|A|$ לפי אותו משפט, והפעל את תרגיל 8.3.24.

תרגיל 8.3.26 (**) יהי p ראשוני. נסמן ב־$U_n(\mathbb{F}_p)$ את חבורת המטריצות המשולשיות עליונות עם אלכסון $\mathrm{diag}(1, 1, \ldots, 1)$ (ראה גם תרגיל 3.5.20). הראה ש־$U_n(\mathbb{F}_p)$ היא חבורת־p (מסדר $p^{\binom{n}{2}}$), ומצא את המרכז שלה.

תרגיל 8.3.27 (***) נסמן $U_\infty(\mathbb{F}_p)$ את האיחוד $\bigcup U_n(\mathbb{F}_p)$ (כאשר $U_n(\mathbb{F}_p)$ הן החבורות מתרגיל 8.3.26), כלומר חבורת המטריצות האינסופיות, עם 1 באלכסון, וכמעט כל איבר אחר שווה לאפס. הראה שזו חבורת־p (אינסופית), עם מרכז טריוויאלי.

תרגיל 8.3.28 (**) הראה שהאוסף $\mathfrak{P}_p$ של חבורות־p סגור לתת־חבורות, לחבורות מנה, למכפלות ולהרחבות (ראה הגדרה 4.9.1). הסק שלכל חבורה יש תת־חבורה נורמלית מינימלית יחידה N ביחס לתכונה ש־G/N היא חבורת־p. **הדרכה.** תרגיל 4.9.8.

8.3.1 משפט מילר

תרגיל 8.3.29 (+)** תהי G חבורת־p עם תת־חבורה נורמלית אבלית $A \lhd G$. אם $A \subset \mathrm{C}_G(A)$ אז יש תת־חבורה נורמלית אבלית $A \subset A_1$ כך ש־$|A| \leq [\mathrm{C}_G(A) : \mathrm{C}_G(A_1)]$ (ואפשר להניח ש־$[A_1 : A] = p$). **הדרכה.** תת־החבורה $H = \mathrm{C}_G(A)$ נורמלית לפי תרגיל 6.4.45. נתבונן במנה G/A. לפי תרגיל 8.3.11 יש איבר לא טריוויאלי $xA \in H/A \cap \mathrm{Z}(G/A)$. נסמן $A_1 = \langle A, x \rangle$ (אפשר להניח ש־$\mathrm{ord}(xA) = p$ ולקבל $[A_1 : A] = p$). כיוון ש־$x \in H$, A_1 אבלית. ההנחה $xA \in \mathrm{Z}(G/A)$ פירושה ש־$[x, G] \subseteq A$, ולכן $gxg^{-1} \in Ax$ לכל $g \in G$ ו־$A_1 \lhd G$. מכיוון ש־$A \subseteq \mathrm{Z}(H)$, לכל $h, h' \in H$ מתקיים $[x, hh'] = [x, h][x, h']$, ולכן $\mathrm{ad}_x : h \mapsto [x, h]$ הוא הומומורפיזם $G \to A$; הגרעין שלו הוא $H_1 = \mathrm{Ker}(\mathrm{ad}_x) = \mathrm{C}_G(A_1)$, ולכן $[H : H_1] \leq |\mathrm{Im}(\mathrm{ad}_x)| \leq |A|$.

תרגיל 8.3.30 (+)** תהי G חבורת־p עם מרכז $Z = \mathrm{Z}(G)$. אם G אינה אבלית, אז יש תת־חבורה $H \lhd G$ כך ש־$\mathrm{Z}(G) \subset \mathrm{Z}(H)$ ו־$|Z| \leq [G : H]$. **הדרכה.** קח $A = \mathrm{Z}(G)$ בתרגיל 8.3.29, ו־$H = \mathrm{C}_G(A_1)$.

תרגיל 8.3.31 (+)** בכל חבורת־p עם מרכז מסדר p^c, שהסדר שלה גדול מ־$p^{\binom{m}{2} - \binom{c}{2}}$, יש תת־חבורה נורמלית אבלית מסדר p^m. **הדרכה.** נוכיח טענה מעט חזקה יותר: בחבורה G כנ"ל יש תת־חבורה נורמלית אבלית מסדר p^m כך ש־$[G : \mathrm{C}_G(A)] \leq p^{\binom{m}{2} - \binom{c}{2}}$. ההוכחה באינדוקציה על m. עבור $m \leq c$ אין מה להוכיח (קח $A \subseteq \mathrm{Z}(G)$). נניח שהטענה נכונה ל־$m - 1$. אז יש תת־חבורה נורמלית אבלית A מסדר p^{m-1} עם $[G : \mathrm{C}_G(A)] \leq p^{\binom{m-1}{2} - \binom{c}{2}}$. לכן $[\mathrm{C}_G(A) : A] \, p^{\binom{m}{2} - \binom{c}{2}} = [G : \mathrm{C}_G(A)][\mathrm{C}_G(A) : A]|A| = |G| < p^{\binom{m}{2} - \binom{c}{2}}$, ו־$A \subset \mathrm{C}_G(A)$. לפי תרגיל 8.3.29, יש תת־חבורה נורמלית אבלית $A_1 \lhd G$ כך ש־$|A_1| = p^{m+1}$ ו־$[G : \mathrm{C}_G(A_1)] \leq [G : \mathrm{C}_G(A)][\mathrm{C}_G(A) : \mathrm{C}_G(A_1)] \leq p^{m + \binom{m}{2} - \binom{c}{2}} = p^{\binom{m+1}{2} - \binom{c}{2}}$.

תרגיל 8.3.32 (***) (משפט מילר) לכל חבורת־p שסדרה גדול ממש מ־$p^{\binom{m}{2}}$ יש תת־חבורה נורמלית אבלית מסדר p^m לפחות. **הדרכה.** תרגיל 8.3.31; הרי $1 \leq c$.

[G.A. Miller, *On an important theorem with respect to the operation groups of order p^α, p being any prime number*, Messenger Math **27**, (1898), p. 120]

תרגיל 8.3.33 (**) לחבורת־p מסדר p^n יש תת־חבורה אבלית מסדר p^m כאשר $n \leq \binom{m+1}{2}$. **הדרכה.** זהו תרגיל 8.3.32.

תרגיל 8.3.34 (+)** נתבונן בחבורה $U_n(\mathbb{F}_p)$ מתרגיל 8.3.26. מצא תת־חבורה נורמלית אבלית מסדר p^{n-1}. **הדרכה.** $A = \langle 1 + e_{1j} : 1 < j \rangle$.

תרגיל 8.3.35 (*+)** הראה שהחסם של משפט מילר (תרגיל 8.3.32) הדוק: לחבורה $U_n(\mathbb{F}_p)$, מסדר $p^{\binom{n}{2}}$, אין תת־חבורה נורמלית אבלית מסדר p^n.

8.3.2 מספר תת־החבורות

ניתן לדלג בקריאה ראשונה.

(על־פי סעיפים 59–61 בספר Theory of groups of finite order, William Burnside, 1897.)

תהי G חבורה מסדר p^n. נסמן ב־$d_i(G)$ את מספר תת־החבורות מסדר p^i ב־G; ולכל תת־חבורה $P \leq G$, נסמן ב־$u_j^G(P)$ את מספר תת־החבורות מסדר p^j של G המכילות את P. בתת־סעיף זה נוכיח שכל המספרים האלה שקולים ל־1 מודולו p.

תרגיל 8.3.36 (־*)** הראה ש־$d_{n-1}(G) \equiv 1 \pmod p$. **הדרכה.** תת־החבורות מאינדקס p הן נורמליות לפי תרגיל 8.3.9. נקבע תת־חבורה כזו, H (קיימת לפי תרגיל 8.3.10). לכל $H \neq H_1 < G$ מאינדקס p, $N = H \cap H_1$ היא נורמלית מאינדקס p^2, עם מנה $G/N \cong \mathbb{Z}_p \times \mathbb{Z}_p$; ל־$G/N$ יש $p+1$ תת־חבורות אמיתיות, ולכן יש בדיוק p תת־חבורות H_1 עם חיתוך השווה ל־N. נפרק את אוסף תת־החבורות מאינדקס p למחלקות לפי החיתוך עם H; אז פרט ל־H, בכל מחלקה יש בדיוק p תת־חבורות.

תרגיל 8.3.37 (־*)** הראה ש־$u_1^G(1) \equiv 1 \pmod p$. **הדרכה.** מכיוון שבמרכז $\mathrm{Z}(G)$ של G יש אברים מסדר p, אוסף הפתרונות למשוואה $x^p = 1$ במרכז הוא תת־חבורה מסדר המתחלק ב־p, ולכן מספרם m של האברים מסדר p שקול ל־-1 מודולו p. האברים מסדר p שאינם במרכז שייכים למחלקות צמידות, שגודל כל אחת מהן מתחלק ב־p. מכיוון ששתי תת־חבורות שונות מסדר p נחתכות באופן טריוויאלי, יש $p-1$ אברים שונים מסדר p בכל חבורה, ולכן $u_1^G(1) \equiv -(p-1)u_1^G(1) = -m \equiv 1 \pmod p$.

תרגיל 8.3.38 (־*)** לכל תת־חבורה $P \neq G$ מסדר p^i, $u_{i+1}^G(P) \equiv 1 \pmod p$. **הדרכה.** נסמן $|P| = p^i$. לפי תרגיל 8.3.9, P נורמלית בכל תת־חבורה P_1 מסדר p^{i+1} המכילה אותה, ולכן כל P_1 כזו מוכלת במנרמל $N = \mathrm{N}_G(P)$. כמובן, $P \lhd N$; לכן יש התאמה בין החבורות P_1 לבין תת־חבורות מסדר p ב־N/P, שמספרן שקול ל־1 מודולו p לפי תרגיל 8.3.37.

תרגיל 8.3.39 (**) כל תת־חבורה מסדר p^i $(0 < i < n)$ מוכלת בתת־חבורה מסדר p^{i+1}, וכל תת־חבורה מסדר p^{i+1} מכילה תת־חבורה מסדר p^i. **הדרכה.** תרגיל 8.3.10 ותרגיל 8.3.38: אפס אינו שקול ל־1 מודולו p.

תרגיל 8.3.40 (־*)** הוכח שלכל $0 \leq i < n$, $d_i(G) \equiv d_{i+1}(G)$. **הדרכה.** נסמן ב־X_0 את אוסף תת־החבורות מסדר p^i, ב־X_1 את אוסף תת־החבורות מסדר p^{i+1}, וב־X את קבוצת הזוגות $(P_0, P_1) \in X_0 \times X_1$ כך ש־$P_0 < P_1$. לפי תרגילים 8.3.36 ו־8.3.38,

$$|P_1| = \sum_{P_1 \in X_1} 1 \equiv \sum_{P_1 \in X_1} d_i(P_1) = |X| = \sum_{P_0 \in X_0} u_{i+1}^G(P_0) \equiv \sum_{P_0 \in X_0} 1 = |P_0| \pmod p.$$

תרגיל 8.3.41 (־)** מספר תת־החבורות מסדר p^i של חבורה מסדר p^n שקול ל־1 מודולו p (כלומר $d_i(G) \equiv 1 \pmod p$). **הדרכה.** אינדוקציה על i בתרגיל 8.3.40.

תרגיל 8.3.42 (**) מספר תת־החבורות הנורמליות מסדר p^i של חבורה מסדר p^n שקול ל־1 מודולו p. **הדרכה.** תת־החבורות מסדר p^i משתייכות למחלקות צמידות, שגודלן 1 עבור תת־החבורות הנורמליות, וחזקת־p אמיתית בשאר המקרים.

תרגיל 8.3.43 (***) מספר תת־החבורות מגודל קבוע המכילות תת־חבורה P של G שקול ל־1 מודולו p. (היינו: נניח ש־$|P| = p^i$ ו־$j \leq n-i$, אז $u_{i+j}^G(P) \equiv 1 \pmod p$). **הדרכה.** בדומה לתרגיל 8.3.40, נסמן ב־N את מספר הזוגות (P_1, Q) כך ש־$P < P_1 < Q < G$, $[P_1 : P] = p$ ו־$[Q : P] = p^j$. ספירת הזוגות בשתי דרכים מראה לפי תרגיל 8.3.41 ש־

$$u_{i+j}^G(P) = \sum_Q 1 \equiv \sum_Q d_{j+i-1}(Q) = N = \sum_{P_1} u_{i+j}^G(P_1) \pmod p.$$

כעת נוכיח את הטענה, באינדוקציה על j. את המקרה $j = 1$ כיסינו בתרגיל 8.3.38. מכיוון ש־$|P_1| = p^{i+1}$, הנחת האינדוקציה נותנת $u_{i+j}^G(P_1) \equiv 1$, ולכן $u_{i+j}^G(P) \equiv \sum_{P_1} u_{i+j}^G(P_1) \equiv \sum_{P_1} 1 = u_{i+1}^G(P) \equiv 1 \pmod p$, שוב לפי תרגיל 8.3.38.

8.4 משפטי סילו

הגדרה 8.4.1 *יהי p ראשוני. נסמן $p^t \parallel n$ אם $p^t \mid n$ אבל $p^{t+1} \nmid n$.*

הגדרה 8.4.2 *יהי p ראשוני, ונניח ש־$|G| = n \parallel p^t$. תת־חבורה של G שהסדר שלה p^t נקראת **תת־חבורת p־סילו** של G.*

תרגיל 8.4.3 (*) תהי $P \leq G$ תת־חבורה שהיא חבורת־p. אז P היא תת־חבורת p־סילו אם ורק אם $[G:P]$ זר ל־p.

8.4.1 קיומן של חבורות p־סילו

תרגיל 8.4.4 (*) אם P תת־חבורת p־סילו של G ו־$P \subseteq H \subseteq G$, אז P היא גם חבורת p־סילו של H.

תרגיל 8.4.5 (**) אם $P \lhd G$ תת־חבורה נורמלית שהיא חבורת־p, ול־G/P יש תת־חבורת p־סילו, אז גם ל־G יש תת־חבורת p־סילו. **הדרכה**. כל תת־חבורה של G/P היא מהצורה B/P עבור $B \leq G$.

תרגיל 8.4.6 (**) הראה שלחבורת הקווטרניונים המוכללת Q_{12} (מסדר 12) יש שלוש תת־חבורות 2־סילו, והחיתוך שלהן הוא תת־חבורה מסדר 2, שהיא מרכז החבורה.

תרגיל 8.4.7 (*−)** תהי A חבורה אבלית מסדר המתחלק ב־p. אז יש לה תת־חבורת p־סילו. **הדרכה**. נניח ש־$|A| = n \parallel p^t$. לפי משפט קושי (לחבורות אבליות) יש ל־A איבר $x \in A$ מסדר p. לפי הנחת האינדוקציה ל־$A/\langle x \rangle$ תת־חבורה מסדר p^{t-1}, וסיימנו לפי תרגיל 8.4.5.

משפט 8.4.8 (משפט סילו הראשון) **לכל חבורה סופית שהסדר שלה מתחלק בראשוני p יש תת־חבורות p־סילו.**

הוכחה. ההוכחה דומה לזו של משפט קושי (משפט 8.2.4). אם יש מרכֵּז לא טריוויאלי שהסדר שלו מתחלק ב־p^t, גמרנו באינדוקציה. אחרת, האינדקסים של כל המרכזים מתחלקים ב־p, ולכן גם הסדר של המרְכָּז מתחלק ב־p, ולפי משפט קושי יש בו איבר x מסדר p. לפי הנחת האינדוקציה ל־$G/\langle x \rangle$ יש תת־חבורת p־סילו, ולפי תרגיל 8.4.5 די בכך. □

תרגיל 8.4.9 (**) יהיו p ראשוני ו־m זר ל־p. הראה ש־$\binom{p^k m}{p^k} \equiv m \pmod p$. **הדרכה**. $\binom{p^k m}{p^k} = \prod_{i=0}^{p^k-1} \frac{p^k m - i}{p^k - i}$; לכל $0 < i < p^k$ (מתחלק ב־p או זר לו), $\frac{p^k m - i}{p^k - i} \equiv 1 \pmod p$.

תרגיל 8.4.10 (+)** יהי $p > 2$ ראשוני. הראה ש־$\binom{2p}{p} \equiv 2 \pmod{p^2}$. **הדרכה**. מצא פעולה של $\mathbb{Z}_p \times \mathbb{Z}_p$ על מרחב תת־הקבוצות בגודל p של $\{1, \dots, 2p\}$, וחשב את גדלי המסלולים.

תרגיל 8.4.11 (***) עבור $p > 3$, $\binom{2p}{p} \equiv 2 \pmod{p^3}$. (השווה לתרגיל 8.4.10.)

תרגיל 8.4.12 (***) תן הוכחה של משפט סילו הראשון המבוססת על פעולה של G על תת־קבוצות. **הדרכה**. (הוכחת Wielandt) יהי $\Omega = \binom{G}{p^t}$ אוסף תת־הקבוצות בגודל p^t של G. החבורה G פועלת על Ω לפי $g : B \mapsto gB$. מכיוון ש־p אינו מחלק את $|\Omega|$ (תרגיל 8.4.9), יש מסלול שגודלו זר ל־p; יהי $B \in \Omega$ איבר בכזה מסלול. יהי H המייצב של B. מחד, $[G:H] = |[B]|$ זר ל־p, ולכן $|H| = s \mid p^t$. מאידך נקבע $b_0 \in B$, אז $Hb_0 \subseteq HB = B$ ולכן $H \subseteq Bb_0^{-1}$ כך ש־$s \leq p^t$. לכן H תת־חבורת p־סילו.

תרגיל 8.4.13 (**) תהי G חבורה, עם חבורת p־סילו P. הראה שהמנה המקסימלית של G שהיא חבורת־p (תרגיל 8.3.28), איזומורפית לחבורת מנה של P. **הדרכה**. נסמן את המנה המקסימלית שהיא חבורת־p ב־G/N_p. אז יש אפימורפיזם $P \twoheadrightarrow P/(P \cap N_p) \cong PN_p/N_p \leq G$. אבל מכיוון שהאינדקס $[G:PN_p]$ מחלק גם את $[G:N_p]$ וגם את $|P|$, $G = PN_p$.

תרגיל 8.4.14 (**) יהי p ראשוני המחלק את סדר החבורה G. אז יש איבר z מסדר p כך ש־$\mathrm{C}_G(z)$ מכיל תת־חבורת P־סילו של G. **הדרכה**. קח איבר השייך למרכז של תת־חבורת p־סילו.

8.4.2 תת־חבורות סילו צמודות זו לזו

תרגיל 8.4.15 **(***)** תהי P תת־חבורת p־סילו של חבורה G. לכל תת־חבורה $N \leq G$ שהיא חבורת־p, אם $NP = PN$ אז $N \leq P$. **הדרכה.** לפי טענה 4.2.10 PN היא חבורת־p, וסדרה אינו יכול לעלות על זה של P.

תרגיל 8.4.16 **(**)** תהי P תת־חבורת p־סילו של G. כל תת־חבורה של המנרמל $\mathrm{N}_G(P)$ שהיא חבורת־p, מוכלת ב־P. **הדרכה.** תרגיל 8.4.15. בפרט, P היא תת־חבורת p־סילו יחידה של $\mathrm{N}_G(P)$.

תרגיל 8.4.17 **(***)** לכל תת־חבורת p־סילו $P \leq G$ מתקיים $\mathrm{N}_G(\mathrm{N}_G(P)) = \mathrm{N}_G(P)$. **הדרכה.** יהי $a \in \mathrm{N}_G(\mathrm{N}_G(P))$. אז $aPa^{-1} \subseteq \mathrm{N}_G(aPa^{-1}) = a\mathrm{N}_G(P)a^{-1} = \mathrm{N}_G(P)$, ולפי תרגיל 8.4.16, $aPa^{-1} \subseteq P$, ולכן $a \in \mathrm{N}_G(P)$.

תרגיל 8.4.18 **(***)** תהי $P \leq G$ תת־חבורת p־סילו, ותהי $N \subseteq \mathrm{Z}(G)$ תת־חבורה מרכזית. אם $PN \lhd G$ אז גם $P \lhd G$. **הדרכה.** (השווה לתרגיל 8.4.15.) מכיוון ש־N מרכזית, $NP \subseteq \mathrm{N}_G(P)$. לפי ההנחה, לכל $x \in G$ מתקיים $xPx^{-1} \subseteq xPNx^{-1} = PN \subseteq \mathrm{N}_G(P)$; אבל $P \lhd \mathrm{N}_G(P)$, ולכן זו חבורת p־סילו יחידה של $\mathrm{N}_G(P)$, ו־$xPx^{-1} = P$.

תרגיל 8.4.19 **(**)** תהי P תת־חבורת p־סילו של חבורה G. הראה שפעולת G לפי הצמדה על המסלול של $\mathrm{N}_G(P)$, איזומורפית לפעולה של G על הקוסטים של $\mathrm{N}_G(P)$. **הדרכה.** תרגילים 6.4.68 ו־8.4.17.

משפט 8.4.20 תהי G חבורה סופית.

1. כל תת־חבורות p־סילו של G צמודות זו לזו. (**משפט סילו השני**)
2. מספרן $n_p \equiv 1 \pmod p$. (**משפט סילו השלישי**)

הוכחה. החבורה G פועלת על־ידי הצמדה על הקבוצה Ω של תת־חבורות p־סילו של G, שאינה ריקה לפי משפט 8.4.8. תהי $Q \in \Omega$. המסלולים תחת פעולת Q על Ω הם בגודל המחלק את $|Q|$, כלומר חזקות של p. אם P נקודת שבת של Q אז $Q \subseteq \mathrm{N}_G(P)$ ולפי תרגיל 8.4.16 נובע מכאן ש־$Q = P$; לכן Ω היא איחוד של מסלולים בגודל המתחלק ב־p עם המסלול $\{Q\}$, ומכאן $n_p \equiv 1 \pmod p$. נימוק זה תקף גם אם נחליף את Ω במסלול $[Q]$ של Q תחת פעולת G. אם $Q' \in \Omega$ אינה שייכת למסלול הזה, אז בפעולתה על $[Q]$ אין נקודות שבת, בסתירה לכך שגודל המסלול זר ל־p; מכאן ש־$Q' \in [Q]$. □

משפט 8.4.21 כל תת־חבורה של G שהיא חבורת־p מוכלת בתת־חבורת p־סילו.

הוכחה. בהמשך להוכחת משפט סילו השני, תהי P תת־חבורת־p של G. בפעולה שלה על Ω יש נקודת שבת Q (תרגיל **8.3.14**), ו־$P \leq Q$ לפי תרגיל **8.4.16**. □

תרגיל 8.4.22 **(**)** תהי P תת־חבורת p־סילו של G. לכל $\mathrm{N}_G(P) \leq H \leq G$ מתקיים היחס $[G\!:\!H] \equiv 1 \pmod p$. **הדרכה.** לפי משפט סילו השני ותרגיל 8.4.4, $[G\!:\!\mathrm{N}_G(P)] \equiv [G\!:\!H] \equiv 1 \pmod p$.

תרגיל 8.4.23 **(***)** מספר תת־החבורות מסדר p^i של G (כאשר $p^i \mid |G|$) שקול ל־1 מודולו p.
הערה. זוהי כמובן הכללה של סעיף 2 במשפט סילו השני, שם $p^i \parallel |G|$. **הדרכה.** תהי Q חבורת p־סילו של G. בדומה להוכחת משפט סילו השני, Q פועלת על האוסף Ω של תת־החבורות מסדר p^i ב־G. כל נקודת שבת היא תת־חבורה P המוכלת ב־Q לפי תרגיל 8.4.15, ומספרן של אלה שקול ל־1 לפי תרגיל 8.3.41. שאר תת־החבורות שייכות למסלולים שגודלם מתחלק ב־p ככל מחלק גדול מ־1 של $|Q|$.

תרגיל 8.4.24 **(**)** תהי Q תת־חבורת p־סילו של G. אם גם P תת־חבורת p־סילו, אז $P \cap \mathrm{N}_G(Q) = P \cap Q$.

תרגיל 8.4.25 (***) (לכל $i \geq 1$) אם $n_p \neq 1$ ו־$n_p \not\equiv 1 \pmod{p^i}$, אז יש תת־חבורות p־סילו שונות P, Q עם $[P : P \cap Q] < p^i$. **הדרכה.** נוכיח את הטענה הקונטרפוזיטיבית: אם לכל שתי תת־חבורות p־סילו P, Q שונות מתקיים $[P : P \cap Q] \geq p^i$, אז $n_p \equiv 1 \pmod{p^i}$. בדומה למשפט 8.4.20, נתבונן בפעולה של תת־חבורת p־סילו P על אוסף תת־חבורות p־סילו, Ω. המייצב של $Q \in \Omega$ הוא $P \cap \mathrm{N}_G(Q) = P \cap Q$, וכך מתקבל הפירוק $n_p = 1 + \sum [P : P \cap Q]$, כאשר הסכום הוא על נציג אחד מכל מסלול מלבד המסלול של P.

תרגיל 8.4.26 (***) תהי $G \leq H$ תת־חבורה המכילה מנרמל של תת־חבורת p־סילו. אז $\mathrm{N}_G(H) = H$. **הדרכה.** (זוהי הכללה של תרגיל 8.4.17.) יהי $t \in \mathrm{N}_G(H)$, אז $tPt^{-1} \subseteq t\mathrm{N}_G(P)t^{-1} \subseteq tHt^{-1} = H$, ולכן tPt^{-1} היא חבורת p־סילו של H. לכן יש $h \in H$ כך ש־$hPh^{-1} = tPt^{-1}$ ואז $h^{-1}t \in \mathrm{N}_G(P)$, ו־$t \in h\mathrm{N}_G(P) \subseteq H$.

כדאי להשוות בין תרגילים 8.3.7 ו־8.4.26: בחבורת־p המנרמל של תת־חבורה תמיד גדול ממנה, ואילו המנרמל של תת־חבורה המכילה תת־חבורת סילו, שווה לה.

תרגיל 8.4.27 (-)** הראה שהאיחוד של כל תת־חבורות p־סילו של G שווה לאוסף האברים מסדר חזקת־p של החבורה.

תרגיל 8.4.28 (*) נניח ש־$|G| = p^t m$ כאשר $(p, m) = 1$. אז $n_p \mid m$. **הדרכה.** מספר תת־חבורות p־סילו של G, $n_p = n_p(G)$, מקיים $n_p \equiv 1 \pmod{p}$ לפי המשפט השני. מאידך $n_p = [G : \mathrm{N}_G(P)]$, ולכן הוא מחלק את $|G|$. אם $|G| = p^t m$ כאשר $p \nmid m$, נובע מכך ש־$n_p \mid m$.

תרגיל 8.4.29 (**) $n_p = 1$ אם ורק אם תת־חבורת p־סילו היא נורמלית.

תרגיל 8.4.30 (**) כל המרכזים של תת־חבורות p־סילו צמודים זה לזה.

תרגיל 8.4.31 (*-)** תהי P חבורת סילו של G. אם $a, b \in \mathrm{C}_G(P)$ צמודים ב־G, אז הם צמודים גם ב־$\mathrm{N}_G(P)$. **הדרכה.** נניח ש־$b = gag^{-1}$, ונתבונן במרכז $H = \mathrm{C}_G(a)$. לפי ההנחה $P \subseteq H$ וגם $P \subseteq \mathrm{C}_G(b) = gHg^{-1}$, כלומר $P, g^{-1}Pg \subseteq H$. לפי משפט סילו, קיים $h \in H$ כך ש־$g^{-1}Pg = h^{-1}Ph$, ואז $gh^{-1} \in \mathrm{N}_G(P)$ ו־$(gh^{-1})a(gh^{-1})^{-1} = b$.

תרגיל 8.4.32 (**) תהי P חבורת סילו אבלית של G. אם $a, b \in P$ צמודים ב־G, אז הם צמודים גם ב־$\mathrm{N}_G(P)$ [משפט זה של ברנסייד הוא תוצאה ראשונה בתחום הקרוי היום Fusion Theory]. **הדרכה.** תרגיל 8.4.31.

תרגיל 8.4.33 (***) תן דוגמה נגדית לתרגיל 8.4.32 ללא ההנחה ש־P אבלית. **הדרכה.** קח $P = D_4$ בתוך $G = S_4$.

תרגיל 8.4.34 (**) נניח ש־$P_1, \dots, P_t$ הן תת־חבורות סילו של G (לראשוניים שונים), וכולן נורמליות. אז $\langle P_1, \dots, P_t \rangle$ היא מכפלה ישרה של החבורות.

תרגיל 8.4.35 (**) נניח שכל תת־חבורות סילו של חבורה סופית G הן נורמליות. אז G היא מכפלה ישרה שלהן.

תרגיל 8.4.36 (+)** נניח ש־$|G| = p^t q^s$ כאשר p, q ראשוניים. תהיינה P, Q תת־חבורת p־סילו ותת־חבורת q־סילו, בהתאמה. אם $P \subseteq \mathrm{Z}(G)$ אז $G \cong P \times Q$. **הדרכה.** לפי ההנחה $G = PQ \rhd Q$.

תרגיל 8.4.37 (***) הוכח שהשיכון $G \hookrightarrow S_n$ שמספק משפט קיילי אינו לתוך A_n, אם ורק אם תת־חבורת 2־סילו של G היא ציקלית ולא טריוויאלית. (ראה גם תרגיל 10.2.19; הכללה ל־$p > 2$ מופיעה בתרגיל 8.4.78.)

תרגיל 8.4.38 (−*)** (דוגמה נגדית למשפטי סילו עבור חבורות אינסופיות) יהי $T:\mathbb{Z}^2 \to \mathbb{Z}^2$ האוטומורפיזם המוגדר לפי $T(x) = y^{-1}$ ו־$T(y) = x^{-1}$ כאשר x, y יוצרים את $\mathbb{Z}^2$. הראה ש־$T^4 = 1$. נגדיר $\theta: \mathbb{Z}_4 \to \mathrm{Aut}(\mathbb{Z}^2)$ לפי $\theta(1) = T$. נתבונן בחבורה $G = \mathbb{Z}^2 \rtimes_\theta \mathbb{Z}_4 = \langle x, y, \sigma \mid xy = yx,\, \sigma x \sigma^{-1} = y^{-1},\, \sigma y \sigma^{-1} = x,\, \sigma^4 = 1 \rangle$. הראה שמחוץ לתת־החבורה הנורמלית $\langle x, y \rangle$, כל איבר של G צמוד בדיוק לאחד מהאברים $\sigma, x\sigma, \sigma^{-1}, x\sigma^{-1}, \sigma^2, x\sigma^2, y\sigma^2, xy\sigma^2$. הראה שתת־חבורות־2 המקסימליות של G שייכות לשלוש מחלקות צמידות (באחת חבורות מסדר 2, ובשתיים חבורות מסדר 4).

תת־חבורות סילו של החבורות הסימטריות

תרגיל 8.4.39 (−*)** 1. ל־S_5 יש 15 חבורות 2־סילו.

2. ל־A_5 יש 5 חבורות 2־סילו.

הדרכה. נסמן $G = S_5$ ו־$a = (12)(34)$. הראה ש־$P = \mathrm{C}_G(a) \subseteq S_4 = S_{\{1,2,3,4\}}$ היא תת־חבורת 2־סילו, וש־$\mathrm{N}_G(P) \subseteq S_4$ ולכן $\mathrm{N}_G(P) = P$. מאידך, עבור $H = A_5$, $\mathrm{N}_H(P \cap H) = A_4$.

תרגיל 8.4.40 (**) זהה את תת־חבורות 2־סילו של S_4. מה החיתוך שלהן? מה האיחוד שלהן?

הדרכה. השווה לתרגיל 6.1.9.

תרגיל 8.4.41 (**) תאר את חבורות 5־סילו של S_{17}.

תרגיל 8.4.42 (−*)** הראה שתת־חבורת 2־סילו של S_6 איזומורפית ל־$\mathbb{Z}_2 \times D_4$, ושתת־חבורת 2־סילו של S_8 איזומורפית ל־$\mathbb{Z}_2 \wr D_4$ (ראה הגדרה 7.3.49).

תרגיל 8.4.43 (+)** מצא למה איזומורפיות תת־חבורות 2־סילו של $\mathrm{SL}_2(\mathbb{F}_5)$. **הדרכה.** תרגיל 3.6.39 נותן פתרון מלא. לחילופין, הראה שב־$\mathrm{SL}_2(\mathbb{F}_5)$ יש איבר יחיד מסדר 2 והשלם את הפתרון בעזרת תרגיל 8.3.18.

תרגיל 8.4.44 (**) כל איבר מסדר 2 ב־A_6 שייך למרכז של איזושהי חבורת 2־סילו.

תרגיל 8.4.45 (**) מצא תת־חבורת 2־סילו P של A_8. מה המרכז שלה, $\mathrm{Z}(P)$? בחר איבר $z \in \mathrm{Z}(P)$ מסדר 2. מה המרכז שלו, $\mathrm{C}_{A_8}(z)$? **הערה.** Brauer ו־Fowler הראו שיש רק מספר סופי של חבורות פשוטות סופיות שהמרכז של איבר מסדר 2 במרכז של תת־חבורת 2 סילו שלהן איזומורפי לחבורה נתונה. "אנליזה מקומית", העוסקת במבנה זה, היא אחת השיטות המרכזיות במשפט המיון לחבורות פשוטות סופיות.

תרגיל 8.4.46 (***) בתרגיל 6.7.29 הגדרנו את חבורת מתיו M_{10}, שהיא מאותו סדר כמו S_6 ואף מכילה את A_6 כתת־חבורה. הראה שלשתי החבורות יש תת־חבורות 2־סילו שונות.

תרגיל 8.4.47 (***) הוכח שהחבורות A_8 ו־$\mathrm{PSL}_3(\mathbb{F}_4)$ אינן איזומורפיות (למרות ששתיהן פשוטות ובעלות אותו סדר!). **הדרכה.** תת־חבורת 2־סילו של A_8 היא $A_8 \cap \langle (15)(26)(37)(48), (13)(24), (12) \rangle = G_1$ וצמודותיה; תת־חבורת 2־סילו של $\mathrm{PSL}_3(\mathbb{F}_4)$ היא $G_2 = \mathrm{U}_3(\mathbb{F}_4)$ וצמודותיה (ראה תרגיל 3.5.20 להגדרת $\mathrm{U}_n(F)$). שתי החבורות מסדר 2^6. הראה ש־$\mathrm{Z}(G_1) = \langle (12)(34)(56)(78) \rangle$ מסדר 2 (ראה תרגיל 8.4.45), ואילו $\mathrm{Z}(G_2) = 1 + \mathbb{F}_4 e_{13}$ מסדר 4.

תת־חבורות סילו של תת־חבורות וחבורות מנה

כדי לנסח בקלות טענות על תת־חבורות p־סילו של חבורות שונות, נסמן ב־$\mathrm{Syl}_p(G)$ את קבוצת תת־חבורות p־סילו של G.

תרגיל 8.4.48 (**) תהי $H \leq G$. לכל $P_0 \in \mathrm{Syl}_p(H)$ יש $P \in \mathrm{Syl}_p(G)$ כך ש־$P_0 = P \cap H$.

הדרכה. תהי $P_0 \leq H$ תת־חבורת p־סילו; זוהי חבורת־p ולכן יש תת־חבורת p־סילו $P \leq G$ כך ש־$P_0 \subseteq P$; אז $P_0 \subseteq P \cap H$, ומכיוון ש־$P \cap H$ היא חבורת־p מתקיים שוויון.

תרגיל 8.4.49 (+)** 1. תהי $H\lhd G$. לכל $P \in \mathrm{Syl}_p(G)$, $P \cap H \in \mathrm{Syl}_p(H)$. **הדרכה.** $[H:P\cap H]=[HP:P] \mid [G:P]$ והאינדקס $[G:P]$ זר ל־p.

2. הנחת הנורמליות בסעיף הקודם - הכרחית. תן דוגמה לתת־חבורה $H \leq G$ שהסדר שלה מתחלק ב־p, עם $P \in \mathrm{Syl}_p(G)$ כך ש־$P \cap H = 1$.

תרגיל 8.4.50 (***) תהי $N\lhd G$. לכל $P \in \mathrm{Syl}_p(G)$, $NP/N \in \mathrm{Syl}_p(G/N)$.

תרגיל 8.4.51 (+)** אם תת־חבורת p־סילו של G מוכלת בתת־חבורה נורמלית N של G, אז כל חבורות p־סילו מוכלות ב־N. בפרט, $n_p(N)=n_p(G)$.

תרגיל 8.4.52 (+)** אם תת־חבורת p־סילו P של G מוכלת בתת־חבורה H של G, אז $n_p(H) \leq n_p(G)$. **הדרכה.** $\mathrm{N}_H(P)=H\cap \mathrm{N}_G(P)$ ולכן $n_p(H)[G:H]=[G:\mathrm{N}_H(P)] \leq [G:H][G:\mathrm{N}_G(P)]$.

תרגיל 8.4.53 (+)** החיתוך של כל תת־חבורות p־סילו הוא תת־חבורת־p נורמלית מקסימלית של G. כלומר: החיתוך נורמלי, וכל תת־חבורת p־סילו נורמלית מוכלת בו.

תרגיל 8.4.54 (**) תן דוגמה נגדית: "אם $P \leq G$ תת־חבורת p־סילו ו־$H \leq G$, אז $H\cap P$ תת־חבורת p־סילו של H." (לפי תרגיל 8.4.50 הטענה נכונה אם H נורמלית).

תרגיל 8.4.55 (***) ("**טיעון פרטיני**") תהי $N\lhd G$ ו־P תת־חבורת סילו של N. אז $G=N\cdot \mathrm{N}_G(P)$. **הדרכה.** לכל $g\in G$ מתקיים $gPg^{-1} \subseteq gNg^{-1}=N$; לכן gPg^{-1} תת־חבורת p־סילו של N, ולכן קיים $x\in N$ כך ש־$xgPg^{-1}x^{-1}=P$. כלומר, $g=x^{-1}(xg) \in N\cdot \mathrm{N}_G(P)$.

תרגיל 8.4.56 (**) אם $H\lhd G$ ו־$P\lhd H$ היא תת־חבורת p־סילו (יחידה) של H, אז $P\lhd G$. **הדרכה.** תרגיל 7.2.50; אכן אצלנו P אופיינית ב־H. (אפשר להוכיח גם בעזרת טיעון פרטיני.)

8.4.3 תת־חבורות הול

ניתן לדלג בקריאה ראשונה.

תהי π קבוצה של ראשוניים. **חבורה שהסדר של כל איבר בה הוא מכפלה של ראשוניים $p\in\pi$** (לאו דווקא שונים) נקראת **חבורת־π**.

תרגיל 8.4.57 (**) האוסף של חבורות־π סגור לתת־חבורות, לחבורות מנה, למכפלה של תת־חבורות נורמליות ולאיחוד שרשראות (ראה הגדרה 4.9.1).

תרגיל 8.4.58 (***) בכל חבורה G יש תת־חבורת־π נורמלית גדולה ביותר (היינו היא מכילה כל תת־חבורת־π נורמלית בחבורה). מסמנים אותה ב־$O_\pi(G)$. **הדרכה.** תרגיל 4.9.11.

תרגיל 8.4.59 (-*)** בכל חבורה סופית G יש תת־חבורה נורמלית מסדר אי־זוגי גדולה ביותר (ככזו). מסמנים אותה ב־$O_{2'}(G)$. **הדרכה.** זהו מקרה פרטי חשוב של תרגיל 8.4.58.

הגדרה 8.4.60 *תת־חבורה שהסדר והאינדקס שלה זרים, נקראת **תת־חבורת הול*** (*על שם* Phillip Hall).

תרגיל 8.4.61 (*) כל תת־חבורת סילו היא תת־חבורת הול.

תרגיל 8.4.62 (**) תהי $N \leq G$ תת־חבורת הול. כל תת־חבורה מסדר $[G:N]$ של G היא תת־חבורה משלימה של N. (ראה הגדרה 4.3.1.)

תרגיל 8.4.63 (+*) לתת־החבורות מסדר 8 של S_5 אין משלים. **הדרכה.** ל־S_5 אין תת־חבורה מסדר 15.

תרגיל 8.4.64 (**) תת־חבורת הול נורמלית N מכילה כל תת־חבורה של G מסדר המחלק את $|N|$. **הדרכה**. תהי N' תת־חבורה מסדר המחלק את $|N|$. אז $NN'/N \cong N'/(N \cap N')$ ולכן $[NN'\!:\!N] = [N'\!:\!N \cap N']$ מחלק גם את $[G\!:\!N]$ וגם את $|N'|$ המחלק את $|N|$; מכאן ש־$NN' = N$ ולכן $N' \subseteq N$.

משפט 8.4.65 (משפט שור־זסנהאוז) *לכל תת־חבורת הול נורמלית יש משלים.*

הוכחה. באינדוקציה על הסדר של G. תהי $N \lhd G$ תת־חבורת הול, כלומר $|N|$ זר ל־$m = [G\!:\!N]$. ראשית נניח ש־N מכילה תת־חבורה $1 < K < N$ שהיא נורמלית ב־G; נתבונן בתת־החבורה N/K של G/K. היא נורמלית, וסדרה $|N/K|$ מחלק את $|N|$ ולכן זר לאינדקס $[G/K\!:\!N/K] = [G\!:\!N]$. לפי הנחת האינדוקציה, יש ב־G/K משלים L/K ל־N/K; כלומר, $NL = G$ ו־$N \cap L = K$. לפי משפט האיזומורפיזם השני $L/K = L/(N \cap L) \cong NL/N = G/N$, ולכן $[L\!:\!K]$ זר ל־$|N|$, ובפרט זר ל־$|K|$. שוב לפי הנחת האינדוקציה יש ב־L משלים ל־K, וזוהי תת־חבורה מסדר m המוכלת ב־G.

מעתה נוכל להניח שאין ל־N תת־חבורות לא טריוויאליות שהן נורמליות ב־G, פרט לעצמה. אם N אבלית, יש לה משלים לפי תרגיל 7.4.37. נניח ש־N אינה אבלית. יהי p ראשוני המחלק את $|N|$, ותהי $P \leq N$ תת־חבורת p־סילו. אם $P = N$ אז N חבורת־p ולכן $\mathrm{Z}(N) \lhd N$ היא תת־חבורה אמיתית לפי ההנחה, לא טריוויאלית לפי משפט 8.3.3, וזו תת־חבורה נורמלית של G לפי תרגיל 3.3.10. זוהי סתירה להנחה שאין ל־N תת־חבורות אמיתיות נורמליות ב־G.

אם כך, $P < N$, ולפי ההנחה P אינה נורמלית ב־G; לכן $\mathrm{N}_G(P) < G$. מכיוון ש־$N \lhd G$, גם $\mathrm{N}_N(P) = N \cap \mathrm{N}_G(P) \lhd \mathrm{N}_G(P)$. לפי טיעון פרטיני (תרגיל 8.4.55), $G = N \cdot \mathrm{N}_G(P)$, ומכיוון ש־$G/N = N \cdot \mathrm{N}_G(P)/N \cong \mathrm{N}_G(P)/\mathrm{N}_N(P)$ מסדר m, $\mathrm{N}_N(P)$ היא תת־חבורת הול של $\mathrm{N}_G(P)$. לפי הנחת האינדוקציה יש לה משלים (מסדר m), שהוא גם תת־חבורה של G. $\square$

תרגיל 8.4.66 (*) הראה שאם n, m אינם זרים, אז לתת־החבורה מסדר n של $\mathbb{Z}_{nm}$ אין משלים.

תרגיל 8.4.67 (***) יהי p ראשוני המחלק את הסדר של חבורה G. נניח שמתקיים החוק $(ab)^p = a^p b^p$ (השווה לתרגיל 2.1.16).

1. הוכח: תת־חבורת p־סילו, P, נורמלית ב־G.
2. הראה שיש ל־P משלים נורמלי (כלומר תת־חבורה נורמלית N כך ש־$P \cap N = e$ ו־$NP = G$).
3. הראה ש־$G \cong P \times N$, ובפרט $\mathrm{Z}(G) \neq e$.

הדרכה. $\varphi : x \mapsto x^p$ הוא הומומורפיזם. חשוב על φ^t כאשר $p^t \parallel n = |G|$.

8.4.4 הטרנספר

ניתן לדלג בקריאה ראשונה.

תהיינה $H \leq G$ חבורה ותת־חבורה. כפי שראינו בסעיף 6.3.2, G פועלת על מרחב הקוסטים G/H על־ידי כפל משמאל. באופן מפורש, אם נבחר $n = [G\!:\!H]$ נציגים $g_1, \dots, g_n \in G$ כך ש־$G = \bigcup g_i H$, אז יש הומומורפיזם $\phi\!: G \to S_n$ כך שלכל $x \in G$, התמורה $\sigma = \phi(x)$ מקיימת $x g_i H = g_{\sigma(i)} H$ לכל i.

הגדרה 8.4.68 *תהי G חבורה עם תת־חבורה H מאינדקס n כמתואר לעיל. מגדירים $T = T_{G/H}\!: G \to H/H'$ לפי $x \mapsto \prod_{i=1}^{n} g_{\sigma i}^{-1} x g_i$ (המכפלה אינה תלויה בסדר משום ש־H/H' אבלית). העתקה זו נקראת **הטרנספר** מ־G ל־H.*

תרגיל 8.4.69 (+)** הראה ש־$T_{G/H}$ מוגדרת היטב (כלומר אינה תלויה בבחירת הנציגים g_i).

תרגיל 8.4.70 (+)** הראה ש־$T\!: G \to H/H'$ הוא הומומורפיזם, והסק שהוא משרה הומומורפיזם $G/G' \to H/H'$.

תרגיל 8.4.71 (***-) נניח ש־$K \subseteq H \subseteq G$. הראה ש־$T_{G/K} = T_{H/K} \circ T_{G/H}$.

תרגיל 8.4.72 (**) אם K תת־חבורה משלימה של H, אז $K \subseteq \mathrm{Ker}(T_{G/H})$. **הדרכה.** לפי ההנחה $G = KH$, ואפשר לבחור את K כקבוצת הנציגים בפירוק $G = \cup g_i H$; כך, לכל $k \in K$, $kg_i = g_{\sigma(i)}$ ו־$T_{G/H}(k)$ היא מכפלה של אברי היחידה.

תרגיל 8.4.73 (**) אם H אבלית והצמצום של $T_{G/H}$ ל־H חד־חד־ערכי, אז $Q = \mathrm{Ker}(T_{G/H})$ הוא משלים נורמלי של H. **הדרכה.** לפי ההנחה $Q \cap H = 1$ ולכן $|QH| = |Q||H|$; הסק $G = QH$.

אומרים שהטרנספר **מעריכי** (או **מעריכי על** H) אם $T_{G/H}(g) = g^{[G:H]}$ לכל $g \in G$ (או לכל $g \in H$). זהו המקרה שבו הטרנספר שימושי במיוחד. נזכיר שאם Q הוא משלים נורמלי של H, אז $G = Q \rtimes H$ ביחס לפעולה מתאימה של H על Q.

תרגיל 8.4.74 (+**) אם H היא תת־חבורת הול (כלומר $(|H|, [G:H]) = 1$) והטרנספר $T_{G/H}$ מעריכי על H, אז הצמצום של $T_{G/H}$ ל־H חד־חד־ערכי (ולפי תרגיל 8.4.73 יש ל־H משלים נורמלי).

משפט 8.4.75 (משפט המשלים הנורמלי של ברנסייד) תהי $P \leq G$ תת־חבורת p־סילו עם $\mathrm{N}_G(P) = \mathrm{C}_G(P)$. אז יש ל־$P$ משלים נורמלי.

הוכחה. נכתוב $G = \cup g_i P$. יהי $x \in P$. לפי ההגדרה, $T_{G/P}(x) = \prod g_{\sigma(i)}^{-1} x g_i = \prod_C g_C^{-1} x^{d(C)} g_C$ כאשר המכפלה השניה היא על המחזורים בפעולת x על G/P, ו־$d(C)$ הוא אורך המחזור C. כמכפלה של אברים ב־P, לכל מחזור C, $g_C^{-1} x^{d(C)} g_C \in P \subseteq \mathrm{N}_G(P) = \mathrm{C}_G(P)$; אבל גם $x^{d(C)} \in \mathrm{C}_G(P)$, ולפי תרגיל 8.4.31, $g_C^{-1} x^{d(C)} g_C$ צמוד ל־$x^{d(C)}$ ב־$\mathrm{N}_G(P)$. מכיוון ש־$x^{d(C)}$ במרכז של $\mathrm{N}_G(P) = \mathrm{C}_G(P)$, הוכחנו למעשה ש־$g_C^{-1} x^{d(C)} g_C = x^{d(C)}$. אם כך $T_{G/P}(x) = \prod_C x^{d(C)} = x^{[G:P]}$, והטרנספר מעריכי על P. סיימנו לפי תרגילים 8.4.74 ו־8.4.73. □

תרגיל 8.4.76 (**) אם קיימת תת־חבורה K כך ש־$G = KH$ ו־$[K, H] = 1$, אז הטרנספר מעריכי. (בפרט הטרנספר מעריכי אם $H \subseteq \mathrm{Z}(G)$, כי אז אפשר לקחת $K = G$.)

תרגיל 8.4.77 (***) תת־חבורת סילו מרכזית היא מחובר ישר. כלומר, אם $P \leq G$ היא תת־חבורת סילו מרכזית, אז $G \cong P \times H$ עבור תת־חבורה $H \lhd G$. **הדרכה.** (זו גרסה חלשה של משפט המשלים הנורמלי של ברנסייד). תרגילים 8.4.74, 8.4.76 ו־7.3.13.

תרגיל 8.4.78 (+***) [לואי פולב] תהי G חבורה ויהי p המחלק הראשוני הקטן ביותר של $|G|$. אם חבורת p־סילו P היא ציקלית, אז יש ל־G תת־חבורה נורמלית מאינדקס p. (השווה לתרגיל 8.4.37). **הדרכה.** לפי ההנחה $P \subseteq \mathrm{C}_G(P) \subseteq \mathrm{N}_G(P)$, אבל $\mathrm{N}_G(P)/\mathrm{C}_G(P) \hookrightarrow \mathrm{Aut}(P) \cong U_{p^t}$ לפי משפט N/C, ו־$[\mathrm{N}_G(P) : \mathrm{C}_G(P)]$ זר ל־$\phi(p^t) = p^{t-1}(p-1)$ לפי ההנחה. לכן $\mathrm{N}_G(P) = \mathrm{C}_G(P)$ ולפי משפט המשלים הנורמלי של ברנסייד, משפט 8.4.75, יש ל־P משלים נורמלי Q, עם $G/Q \cong P$. הרם תת־חבורה מאינדקס p של P. (די להוכיח ש־Q תת־חבורה, משום שהנורמליות נובעת מתרגיל 6.3.28).

תרגיל 8.4.79 (+***) (הכללה של תרגיל 8.4.78) תהי $P \leq G$ תת־חבורת p־סילו.

1. אם P ציקלית ו־$|G|$ זר ל־$(p-1)$ אז יש ל־P משלים נורמלי.
2. אם $|P| = p^2$ ו־$|G|$ זר ל־(p^2-1) אז יש ל־P משלים נורמלי.

8.4.5 מכפלה של תת־חבורות

ניתן לדלג בקריאה ראשונה.

הצגה של G כמכפלה $G = AB$, כאשר $A, B < G$, נקראת **פירוק**. הפירוק $G = (gAg^{-1})(gBg^{-1})$ המתקבל מהצמדה באיבר $g \in G$ נקרא **פירוק צמוד** לפירוק $G = AB$.

כל שני פירוקים לתת־חבורות צמודות, צמודים זה לזה

תרגיל 8.4.80 (−*)** הראה שאם $G = AB$ ו־A', B' צמודות בהתאמה ל־A, B, אז $G = A'B'$ ושני הפירוקים צמודים. **הדרכה**. לפי ההנחה קיימים $x, y \in G$ כך ש־$A' = xAx^{-1}$ ו־$B' = yBy^{-1}$. נכתוב $y = ab$ כאשר $a \in A$ ו־$b \in B$. מכיוון ש־$AB = BA$ (משפט 4.2.6), אפשר גם לכתוב $a^{-1}xa = b_1a_1$ כאשר $a_1 \in A$ ו־$b_1 \in B$. נבחר $g = ab_1$, אז $gAg^{-1} = ab_1Ab_1^{-1}a^{-1} = xAx^{-1} = A'$ ו־$gBg^{-1} = aBa^{-1} = yBy^{-1} = B'$, ולכן $A'B' = g(AB)g^{-1} = G$.

תרגיל 8.4.81 (**) נניח ש־$G = A_1A_2$ הוא פירוק של G כמכפלה של תת־חבורות, ו־$P_i \leq A_i$ הן תת־חבורות p־סילו.

1. אם $P \supseteq P_1P_2$ כאשר P תת־חבורת p־סילו של G, אז $P = P_1P_2$. **הדרכה**. הסדר של P_1P_2 מחלק את $|P_1| \cdot |P_2|$ ולכן הוא חזקת־p. מאידך, $\frac{|G|}{|P_1P_2|} = [A_1A_2 : P_1P_2] = \frac{[A_1:P_1][A_2:P_2]}{[A_1\cap A_2:P_1\cap P_2]}$ זר ל־p, ולכן $P_1P_2 = P$.
2. אם $P = P_1P_2$ היא תת־חבורה של G, אז זוהי חבורת p־סילו ו־$P = (P \cap A_1)(P \cap A_2)$. **הדרכה**. לפי טענה 4.2.10 P היא חבורת־p, והאינדקס שלה $[G : P] = [A_1A_2 : P_1P_2] = \frac{[A_1:P_1][A_2:P_2]}{[A_1\cap A_2:P_1\cap P_2]}$ זר ל־p. השוויון $P = (P \cap A_1)(P \cap A_2)$ מתקבל מהכלה בשני הכיוונים.

פירוק של החבורה משרה פירוק של תת־חבורות p־סילו

תרגיל 8.4.82 (***) נניח ש־$G = A_1A_2$. אז יש תת־חבורות p־סילו $P_1 \leq A_1$ ו־$P_2 \leq A_2$ כך ש־P_1P_2 היא תת־חבורת p־סילו של G. **הדרכה**. נבחר $P_1 \in \mathrm{Syl}_p(A_1)$ ו־$P_2' \in \mathrm{Syl}_p(A_2)$. תהיינה $Q, Q' \in \mathrm{Syl}_p(G)$ כך ש־$P_1 \subseteq Q$ ו־$P_2' \subseteq Q'$ (משפט 8.4.21). מכיוון ש־Q' צמודה ל־Q, יש $x \in G$ כך ש־$Q = xQ'x^{-1}$, ואז $P_2 = xP_2'x^{-1} \subseteq Q$, ו־$P_2$ תת־חבורת p־סילו של xA_2x^{-1}. לפי תרגיל 8.4.80, $G = A_1(xA_2x^{-1})$, ומכיוון ש־$P_1P_2 \subseteq Q$ היא מכפלה של תת־חבורות p־סילו של A_1, xA_2x^{-1} בהתאמה, יש שוויון לפי תרגיל 8.4.81.

תרגיל 8.4.83 (+)** פתור את תרגיל 8.4.82 בהנחה ש־$A_2 \lhd G$. **הדרכה**. תהי $P \in \mathrm{Syl}_p(A_1)$ ותהי $Q \in \mathrm{Syl}_p(G)$ כך ש־$P \subseteq Q$. אז $P_2 = Q \cap A_2 \in \mathrm{Syl}_p(A_2)$ לפי תרגיל 8.4.49 ו־$PP_2 = Q$ לפי תרגיל 8.4.81.

8.5 שימושים במשפטי סילו

אם לחבורה G יש תת־חבורה נורמלית לא טריוויאלית N, אפשר ללמוד אותה דרך N וחבורת המנה G/N (G היא **הרחבה** של G/N על־ידי N). אבני הבנין של תורת החבורות הן, אם כן, החבורות הפשוטות, אלו שאין להן תת־חבורות נורמליות.

8.5.1 נומרולוגיה

תרגיל 8.5.1 (*) החבורות האבליות הפשוטות הן החבורות $\mathbb{Z}_p$ עבור p ראשוני.

תרגיל 8.5.2 (*) חבורה מסדר p^t $(1 < t)$ אינה פשוטה.

תרגיל 8.5.3 (**) אם $|G| = kp^t$ $(k < p)$ אז $n_p = 1$. לדוגמא, חבורות מסדר 18, 42, 44, 51, 54, 98, 162, ... אינן פשוטות.

תרגיל 8.5.4 (**) חבורה מסדר 50 אינה פשוטה.

תרגיל 8.5.5 (***) תהי G חבורה מסדר 75.

1. תת־חבורת 5־סילו של G היא יחידה ולכן נורמלית.
2. אם תת־חבורת 3־סילו של G היא נורמלית, אז G אבלית.
3. אם תת־חבורת 5־סילו היא ציקלית, אז היא מרכזית ו־G אבלית.
4. בנה חבורה מסדר 75 שיש בה 25 תת־חבורות 3־סילו. **הדרכה.** תרגיל 7.3.31.

תרגיל 8.5.6 (**) חבורה מסדר 42 אינה פשוטה.

תרגיל 8.5.7 (**) חבורה מסדר 130 אינה פשוטה. מצא חבורה לא אבלית מסדר זה.

תרגיל 8.5.8 (-)** חבורה מסדר 15 היא ציקלית.

תרגיל 8.5.9 (**) תהי G חבורה מסדר 28.

1. חבורת 7־סילו P_7 היא נורמלית.
2. אם G לא אבלית, אז $|G'| = 7$.
3. אם G לא אבלית ויש לה תת־חבורה נורמלית מסדר 2, אז $G/\mathrm{Z}(G) \cong D_7$.

תרגיל 8.5.10 (**) יהיו $p < q$ ראשוניים כך ש־$q \not\equiv 1 \pmod{p}$. אז כל חבורה מסדר pq היא ציקלית. (בפרט, חבורות מסדר 15, 33, 35, 51, 65, 69, 77, 85, ... הן ציקליות.)

תרגיל 8.5.11 (**) נניח ש־$n = p^t m$, $p^t \parallel n$, ואין אף מחלק של m, פרט ל־1, השקול ל־1 מודולו p. אז תת־חבורת p־סילו של כל חבורה מסדר n היא נורמלית (ולכן חבורה כזו אינה פשוטה). בפרט, החבורות מסדר 40, 45, 63, 70, 84, 135, 140, 165, 175, 195, 200, 225, ... אינן פשוטות. זוהי הכללה של תרגיל 8.5.3.

תרגיל 8.5.12 (-)** חבורה מסדר 45 אינה פשוטה.

תרגיל 8.5.13 (+*) חבורה מסדר 84 אינה פשוטה.

תרגיל 8.5.14 (**) חבורה מסדר $1001 = 7 \cdot 11 \cdot 13$ היא ציקלית.

תרגיל 8.5.15 (-*)** אין חבורות פשוטות מסדר $p^2 q$.

תרגיל 8.5.16 (-*)** יהיו $p < q$ ראשוניים כך ש־$q \not\equiv \pm 1 \pmod{p}$. הראה שכל חבורה מסדר $p^2 q^2$ היא אבלית. **הדרכה.** תרגיל 8.4.35.

תרגיל 8.5.17 (***) נניח ש־$n = p_1 \cdots p_t$ הוא מכפלה של ראשוניים שונים. נניח שלכל מחלק $1 \neq d \,|\, n$ מתקיים $(d-1, n) = 1$. הראה שהחבורה היחידה מסדר n היא $\mathbb{Z}_n$. **הדרכה.** הראה שכל תת־חבורת סילו של G היא נורמלית.

תרגיל 8.5.18 (***) אם $(n, \phi(n)) = 1$, אז החבורה היחידה מסדר n היא ציקלית.

הדרכה. תהי G דוגמא נגדית מינימלית, מסדר n. לכל מחלק אמיתי $m \,|\, n$ מתקיים $(m, \phi(m)) = 1$ ולכן כל תת־חבורה אמיתית של G היא ציקלית. לפי תרגיל 6.4.72, G אינה פשוטה. תהי $N \lhd G$ תת־חבורה נורמלית. לפי הנחת האינדוקציה, N ציקלית ולכן $N \subseteq \mathrm{C}_G(N)$. לפי משפט N/C, $G/\mathrm{C}_G(N) \hookrightarrow \mathrm{Aut}(N)$ שהיא חבורה מסדר $\phi(|N|) \,|\, \phi(n)$. מאידך $|G/\mathrm{C}_G(N)|$ מחלק את n, ולפי ההנחה $G = \mathrm{C}_G(N)$, כלומר $N \subseteq \mathrm{Z}(G)$. מכיוון ש־$G/N$ ציקלית לפי הנחת האינדוקציה, גם $G/\mathrm{Z}(G)$ ציקלית ולכן G אבלית. אבל מהתנאי נובע ש־n מכפלה של ראשוניים שונים, ושכל תת־חבורות סילו של G נורמליות וציקליות. סיים בעזרת תרגיל 8.4.35.

הערה. התנאי על n שקול לכך ש־$n = p_1 \cdots p_t$ הוא מכפלה של ראשוניים שונים, ו־$(p_i, p_j - 1) = 1$ לכל i, j; לכן זו גרסה חזקה של תרגיל 8.5.17.

תרגיל 8.5.19 (**) אם $(n,\phi(n)) > 1$ אז יש חבורה (אבלית) לא ציקלית מסדר n (יחיד עם תרגיל 8.5.18, יש חבורה יחידה מסדר n אם ורק אם $(n,\phi(n)) = 1$.).

תרגיל 8.5.20 (-)** מצא n המקיים את התנאי של תרגיל 8.5.17, אבל לא את זה של תרגיל 8.5.18.

תרגיל 8.5.21 (**) תהי G חבורה מסדר mp, $(p,m) = 1$, עם תת־חבורת p־סילו נורמלית P. נניח ש־$(p-1,m) = 1$. הראה ש־$P \subseteq \mathrm{Z}(G)$. **הדרכה.** משפט N/C.

תרגיל 8.5.22 (**) תהי G חבורה מסדר $385 = 5\cdot 7\cdot 11$.

1. P_7, P_{11} נורמליות ב־G.
2. $P_7 \subseteq \mathrm{Z}(G)$ (תרגיל 8.5.21).
3. $\mathrm{Z}(G) = P_7$ או ש־G ציקלית.

8.5.2 ספירת אברים

גם אם מבחינה נומרית נראה שהערך של n_p עשוי להיות גדול מ־1, לפעמים אפשר לפסול אפשרות זו בעזרת ספירת איברים בחבורה, המראה שהערכים המוצעים ל־n_p גדולים מכדי להיות אפשריים.

תרגיל 8.5.23 (*) אם $P_1, P_2 \leq G$ תת־חבורות שונות מסדר p, אז $P_1 \cap P_2 = 1$.

תרגיל 8.5.24 (*) אם $p \,\|\, n = |G|$ (ראה הגדרה 8.4.1), אז מספר האברים מסדר p שווה ל־$(p-1)n_p$.

תרגיל 8.5.25 (**) חבורה מסדר 56 אינה פשוטה. **הדרכה.** אחרת $n_7 = 8$, ויש 48 אברים מסדר 7. שאר 8 האברים מרכיבים חבורת 2־סילו יחידה.

תרגיל 8.5.26 (***) נראה שיש בדיוק 4 חבורות מסדר 30. תהי G חבורה מסדר זה.

1. לפחות אחת מתת־חבורות סילו P_3, P_5 של G היא נורמלית.
2. ל־G יש תת־חבורה מסדר 15 (שהיא נורמלית לפי האינדקס וציקלית לפי תרגיל 8.5.8).
3. G איזומורפית לאחת מבין החבורות הבאות: $\mathbb{Z}_{30}$, D_{15}, $\mathbb{Z}_5 \times D_3$ או $\mathbb{Z}_3 \times D_5$.
4. הראה שארבע החבורות הללו אינן איזומורפיות זו לזו.

תרגיל 8.5.27 (***) תהי G חבורה מסדר 105. נסמן ב־P_3, P_5, P_7 תת־חבורות סילו מהסדרים המתאימים.

1. לפחות אחת מתת־החבורות P_5 ו־P_7 נורמלית ב־G.
2. $H = P_5P_7$ היא תת־חבורה ציקלית של G, מאינדקס 3. **הדרכה.** תרגילים 4.2.12 ו־8.5.10.
3. $H \lhd G$. **הדרכה.** תרגיל 6.3.28.
4. יהי $x \in H$ איבר מסדר 35, ויהי $y \in G$ איבר מסדר 3. אז $G = \langle x, y\rangle$.
5. $yxy^{-1} \in \left\{x, x^{11}, x^{16}\right\}$. **הדרכה.** $\mathrm{Aut}(H) \cong U_{35} \cong U_5 \times U_7$.
6. $P_5 \subseteq \mathrm{Z}(G)$. **הדרכה.** $P_5 = \langle x^7\rangle$.

7. $N = \langle x^5, y \rangle$ היא תת־חבורה נורמלית מסדר 21 של G.
8. $G \cong \mathbb{Z}_5 \times N$.
9. הראה שיש שתי חבורות מסדר 105, עד כדי איזומורפיזם: $\mathbb{Z}_{105}$ ו־$\mathbb{Z}_5 \times (\mathbb{Z}_7 \rtimes \mathbb{Z}_3)$. **הדרכה.** תרגיל 8.1.11.

תרגיל 8.5.28 (+)** אין חבורות פשוטות מסדר 132.

תרגיל 8.5.29 (***) יהי $p > 2$ ראשוני. נוכיח שיש חבורה מסדר $p(p+1)$ שחבורת p־סילו שלה אינה נורמלית, אם ורק אם p הוא ראשוני מרסן (כלומר $p = 2^r - 1$ עבור r מתאים, שהוא בהכרח ראשוני). **הערה.** במקרה זה $p(p+1)/2$ הוא מספר משוכלל.

1. תהי G חבורה מסדר $p(p+1)$ כאשר $p > 2$ ראשוני, שחבורת p־סילו שלה אינה נורמלית.
   (א) בחבורה יש $p^2 - 1$ אברים מסדר p.
   (ב) לכל חבורת p־סילו P, $P = \mathrm{C}_G(P) = \mathrm{N}_G(P)$. **הדרכה.** $P \subseteq \mathrm{C}_G(P) \subseteq \mathrm{N}_G(P)$ ו־$[G:\mathrm{N}_G(P)] = p+1 = [G:P]$.
   (ג) נסמן ב־X את קבוצת האברים שאינם שייכים לאף חבורת p־סילו. אז $|X| = p$.
   (ד) יהי $x \in X$. אז $[x] \subseteq X$ ו־$\mathrm{C}_G(x) \subseteq \{1\} \cup X$. **הדרכה.** x אינו מרכז אף איבר של חבורת p־סילו.
   (ה) $[x] = X$ ו־$\mathrm{C}_G(x) = X \cup \{1\}$. **הדרכה.** $|\mathrm{C}_G(x)| \cdot |[x]| = |G|$.
   (ו) $H = X \cup \{1\}$ היא תת־חבורה נורמלית מסדר $p+1$, שכל אבריה הלא־טריוויאליים צמודים ב־G.
   (ז) p הוא ראשוני מרסן; ולמעשה $H \cong \mathbb{Z}_2^r$ עבור r מתאים. **הדרכה.** משפט קושי על H.
2. יהי $p = 2^r - 1$ ראשוני מרסן. אז יש חבורה מסדר $p(p+1)$ שבה חבורת p־סילו אינה נורמלית. **הדרכה.** יש $a \in \mathrm{GL}_r(\mathbb{F}_2)$ מסדר p; הגדר $G = \mathbb{Z}_2^r \rtimes \mathbb{Z}_p$ בעזרת a.

תרגיל 8.5.30 (-*)** הראה שמספר השלשות שאפשר לבחור בקבוצה בת m אברים כך ששתי שלשות שונות יש לכל היותר נקודה אחת משותפת, אינו עולה על $(\frac{m-1}{2})^2 - 2$. **הדרכה.** נסמן את המספר המקסימלי ב־$g(m)$. בחר נקודה בקבוצה; יש שני סוגי שלשות - אלו העוברות דרך הנקודה הזו, ואלו שאינן עוברות דרכה. הסק ש־$g(m) \leq \lfloor \frac{m-1}{2} \rfloor + g(m-1)$.

תרגיל 8.5.31 (**) נניח שחבורות 2־סילו של G איזומורפיות ל־$\mathbb{Z}_2 \times \mathbb{Z}_2$. הראה שהקבוצות של אברים לא טריוויאליים בחבורות 2־סילו מהוות שלשות שאין לאף שתיים מהן יותר מנקודה משותפת. הראה שאם יש לחבורה n_2 חבורות סילו, אז מספר האברים מסדר 2 הוא לפחות $1 + 2\sqrt{n_2 + 2}$. **הדרכה.** אם מספר האברים הוא m אז לפי תרגיל 8.5.30, $n_2 \leq (\frac{m-1}{2})^2 - 2$.

8.5.3 פעולה על תת־חבורות

כלי נוסף במלחמה נגד החבורות הפשוטות הוא העידון של משפט קיילי (משפט 6.3.19).

תרגיל 8.5.32 (**) אם $[G:H] = n$ ו־G חבורה פשוטה, אז $G \leq A_n$. **הדרכה.** העידון של משפט קיילי, והחיתוך $G \cap A_n$.

תרגיל 8.5.33 (**) תהי H תת־חבורה מאינדקס p, שהוא הראשוני הקטן ביותר המחלק את הסדר של G. הוכח ש־H נורמלית.

תרגיל 8.5.34 (***) תהי P תת־חבורת p־סילו של G, ונניח שהיא אינה נורמלית. הראה ש־P אינה מוכלת ב־$\mathrm{Core}_G(\mathrm{N}_G(P))$. **הדרכה.** אחרת, לפי תרגיל 8.4.51, $P_1 \subseteq \mathrm{Core}_G(\mathrm{N}_G(P)) \subseteq \mathrm{N}_G(P)$ לכל תת־חבורת p־סילו $P_1 \leq G$, אבל ל־$\mathrm{N}_G(P)$ יש תת־חבורת p־סילו יחידה.

תרגיל 8.5.35 (***) תהי P תת־חבורת p־סילו של G, ונניח שהיא אינה נורמלית. הראה ש־$p \mid [G\colon \mathrm{Core}_G(\mathrm{N}_G(P))]$. **הדרכה.** תרגיל 8.5.34. **הערה.** כידוע $n_p = [G\colon \mathrm{N}_G(P)]$. לפי העידון של משפט קיילי ומכיוון ש־$(p, n_p) = 1$, $pn_p \mid [G\colon \mathrm{Core}_G(\mathrm{N}_G(P))] \mid n_p!$.

תרגיל 8.5.36 (**) לחבורה מסדר 24 יש תת־חבורה נורמלית מסדר 4 או 8.

תרגיל 8.5.37 (**) אם $|G| = p^t m$, $1 = (m, p)$, ו־$|G|$ אינו מחלק את $m!$, אז G אינה פשוטה. בפרט, החבורות מסדר 12, 24, 36, 48, 80, 108, 160, ... אינן פשוטות.

תרגיל 8.5.38 (***) תהי G חבורה מסדר 36. נניח שחבורות 3־סילו של G אינה נורמלית.

1. יש ל־G תת־חבורה נורמלית Q מסדר 3. **הדרכה.** העידון של משפט קיילי.
2. $Q \subseteq \mathrm{Z}(G)$. **הדרכה.** לפי העידון של משפט קיילי $G/Q \cong A_4$ ולכן אין ל־G/Q תת־חבורה מאינדקס 2. הפעל את משפט N/C.
3. חבורת 2־סילו של G נורמלית. **הדרכה.** מכיוון ש־$G/Q \cong A_4$, יש תת־חבורה $Q \subseteq A \lhd G$ כך ש־A/Q מסדר 4. אז $|A| = 12$, ו־$Q \subseteq \mathrm{Z}(A)$. תהי F תת־חבורת 2־סילו של A, אז $F \lhd QF = A$ ולפי תרגיל 8.4.56, $F \lhd G$.
4. ל־G יש תת־חבורה אבלית נורמלית מסדר 12. **הדרכה.** $A = QF$.

תרגיל 8.5.39 (+*) חבורה מסדר 96 אינה פשוטה.

תרגיל 8.5.40 (**) אין חבורה פשוטה מסדר 150.

תרגיל 8.5.41 (**) אין חבורה פשוטה מסדר 216.

תרגיל 8.5.42 (**) חבורה מסדר 108 אינה פשוטה: הראה שיש לה תת־חבורה נורמלית מסדר 9 או 27.

תרגיל 8.5.43 (**) חבורה מסדר $224 = 2^5 \cdot 7$ אינה פשוטה.

תרגיל 8.5.44 (**) אם $|G|$ אינו מחלק את $n_p!$ אז G אינה פשוטה.

תרגיל 8.5.45 (**) תהי G חבורה מסדר $72 = 2^3 \cdot 3^2$. מתקיים אחד הדברים הבאים:

1. ל־G יש תת־חבורה נורמלית מסדר 9.
2. G היא הרחבה של אחת החבורות $\mathbb{Z}_2 \times A_4, \mathrm{SL}_2(\mathbb{F}_3)$ או S_4 על־ידי $\mathbb{Z}_3$.

הדרכה. אם תת־חבורת 3־סילו P היא נורמלית, גמרנו; אחרת האינדקס של המנרמל $\mathrm{N}_G(P)$ הוא 4. לפי העידון של משפט קיילי, הסדר של $K = \mathrm{Core}_G(\mathrm{N}_G(P))$ הוא 3 או 6. אם $|K| = 3$ אז $G/K \cong S_4$. אחרת $G/K \cong A_4$, ול־K יש תת־חבורה יחידה K_1 מסדר 3, שהיא נורמלית לפי תרגיל 7.2.50. כעת $\mathbb{Z}_2 = K/K_1 \longrightarrow G/K_1 \longrightarrow G/K = A_4$ היא הרחבה של A_4 על־ידי $\mathbb{Z}_2$, והתוצאה נובעת מתרגיל 6.7.6.

תרגיל 8.5.46 (**) חבורה מסדר 300 אינה פשוטה. **הדרכה.** תרגיל 8.5.44.

תרגיל 8.5.47 (-*)** אין חבורות פשוטות מסדר 120. **הדרכה.** אחרת $n_5 = 6$, ואז $G \leq S_6$. (השווה לתרגיל 10.2.9.)

תרגיל 8.5.48 (***) חבורה מסדר 90 אינה פשוטה. **הדרכה.** אחרת $n_5 = 6$, ואז $G \leq S_6$. אם $G \leq A_6$ אז $[A_6\colon G] = 4$.

תרגיל 8.5.49 (***) חבורה מסדר 112 אינה פשוטה. **הדרכה.** אחרת $n_2 = 7$ ו־$G \leq S_7$. חשב את $\mathrm{N}_G(P_7)$ (עד כדי איזומורפיזם), והראה שלא יתכן $G \leq A_7$.

תרגיל 8.5.50 (***) נניח ש־2^t היא חזקת 2 המקסימלית המחלקת את $m!$, כאשר m איזוגי. הוכח שחבורה מסדר $2^t m$ אינה פשוטה. **הדרכה.** אם כן, קיים שיכון של G ב־S_m, שאינו מוכל ב־A_m.

תרגיל 8.5.51 (**) תהי G חבורה מסדר p^2m כאשר $(p, m) = 1$. אם יש ל־G שתי תת־חבורות p־סילו P_1, P_2 שהחיתוך שלהן $Q = P_1 \cap P_2 \neq 1$, אז $[G:C] \leq \frac{m}{p+1}$ כאשר $C = \mathrm{C}_G(Q)$. **הדרכה.** מכיוון ש־$P_1, P_2 \subseteq \mathrm{C}_G(Q)$, $[C:P_1] \geq [P_2:Q] = p$ לפי תרגיל 4.5.1.(2), ו־$[C:P_1]$ זר ל־p. למעשה $[C:P_1] \mid [C:\mathrm{N}_C(P_1)] = n_p(C)$, כאשר $n_p(C)$ הוא מספר תת־חבורות p־סילו של C, ו־$n_p(C) > 1$ שהרי $P_2 \subseteq C$. **הערה.** לפי תרגיל 8.4.25, אם $n_p \not\equiv 1 \pmod{p^2}$ אז יש תת־חבורות p־סילו שונות שהחיתוך ביניהן מסדר p.

תרגיל 8.5.52 (**) אם תת־חבורת p־סילו $P \leq G$ היא אבלית, אז הסדר של המנה $\mathrm{N}_G(P)/\mathrm{C}_G(P)$ זר ל־p. **הדרכה.** $P \subseteq \mathrm{C}_G(P) \subseteq \mathrm{N}_G(P)$. זהו עידון של משפט 7.2.10.

תרגיל 8.5.53 (-*)** בהמשך לתרגיל 8.5.51, נניח שתת־חבורות p־סילו של G הן ציקליות, $Q = P_1 \cap P_2$ מסדר p, ו־$C = \mathrm{C}_G(Q)$. אז $[G:C] \leq \frac{p-1}{p+1} n_p(G)$. **הדרכה.** נסמן $C_1 = \mathrm{C}_G(P_1)$. לפי הנתון $\mathrm{Aut}(P) \cong U_{p^2}$ מסדר $p(p-1)$, ולפי תרגיל 8.5.52, $[\mathrm{N}_G(P):C_1]$ מחלק את $p-1$. כמו בתרגיל 8.5.51, $p+1 \leq$ $n_p(C) = [C:\mathrm{N}_C(P)] \mid [C:C_1]$, ולכן $(p+1)[G:C] \leq [G:C] \cdot [C:C_1] = [G:C_1] = n_p(G) \cdot [\mathrm{N}_G(P):C_1] \mid (p-1)n_p(G)$.

תרגיל 8.5.54 (***) תהי G חבורה מסדר 180. נוכיח שהיא אינה פשוטה. נניח שכן.

1. אין ל־G תת־חבורות מאינדקס ≤ 6.
2. $n_3 = 10$ ו־$n_5 = 36$.
3. כל שתי תת־חבורות 3־סילו נחתכות באופן טריוויאלי. **הדרכה.** אחרת יש $Q = P \cap P'$ מסדר 3, והאינדקס של $N = \mathrm{C}_G(Q)$ הוא לכל היותר 5; ראה תרגיל 8.5.51.
4. קבל סתירה על־ידי ספירת אברים.

תרגיל 8.5.55 (***) תהי G חבורה מסדר 400. נוכיח שהיא אינה פשוטה.

1. אם יש יותר מתת־חבורת 5־סילו אחת אז מספרן $n_5 = 16$.
2. אם החיתוך של כל שתי תת־חבורות 5־סילו טריוויאלי, אז חבורת 2־סילו נורמלית.
3. אם Q הוא חיתוך לא טריוויאלי של שתי תת־חבורות 5־סילו אז $Q \subseteq \mathrm{Z}(G)$ או $[G:\mathrm{C}_G(Q)] \leq 2$. **הדרכה.** תרגיל 8.5.51.

תרגיל 8.5.56 (***) תהי G חבורה מסדר 144.

1. אם יש ל־G תת־חבורה H מסדר ≤ 24, אז G אינה פשוטה.
2. נניח ש־$n_3 = 1$. אז יש תת־חבורה נורמלית P מסדר 9. אם P ציקלית, אז $[G:\mathrm{C}_G(P)] \leq 2$.
3. נניח ש־$n_3 = 4$. אז $\mathrm{N}_G(P)$ מסדר 36, עם חבורת 3־סילו יחידה P. הוכח שקיימת תת־חבורה H מסדר 18, $P \subset H \subset \mathrm{N}_G(P)$.
4. נניח ש־$n_3 = 16$.

(א) אם החיתוך של כל שתי תת־חבורות 3־סילו טריוויאלי, אז תת־חבורת 2־סילו היא נורמלית.

(ב) אם $Q = P_1 \cap P_2 \neq 1$ חיתוך של שתי חבורות 3־סילו, אז $|\mathrm{C}_G(Q)| \geq 36$. **הדרכה.** תרגיל 8.5.51.

(ג) הראה שאם לא קיימת תת־חבורה מסדר 72 של G, אז $\mathrm{N}_G(Q) = \mathrm{C}_G(Q)$.

(ד) אם Q אינה במרכז של G, אז $Q \subseteq \mathrm{Z}(\mathrm{N}_G(Q))$, ו־$\mathrm{N}_G(Q)/Q \cong A_4$.

תרגיל 8.5.57 (***) תהי G חבורה מסדר 210.

1. אם $n_7 \neq 15$ או $n_5 \neq 21$ אז יש תת־חבורה נורמלית מסדר 5, 7 או 35.

2. אם $n_3 = 7$, אז $n_5 = 1$. **הדרכה.** נניח ש־$n_3 = 7$; אז $|\mathrm{N}_G(P_3)| = 30$. נסמן $C = \mathrm{Core}_G(\mathrm{N}_G(P_3))$. לפי תרגיל 8.5.34, $C \not\subseteq P_3$, ולכן $|C|$ מחלק את 10. אם $|C| = 5$ סיימנו; אם $|C| = 10$ אז תת־החבורה מסדר 5 היא אופיינית ב־C ושוב סיימנו (תרגיל 7.2.50). נניח ש־$|C| \in \{1,2\}$; לפי העידון של משפט קיילי יש שיכון $G/C \hookrightarrow S_7$, אבל $\mathrm{N}_G(P_3)/C$ מסדר 15 או מכילה תת־חבורה מסדר זה, ולפי תרגיל 8.5.8 יש ב־S_7 איבר מסדר 15, מה שאינו נכון.

3. נניח ש־$n_5 = 21$, $n_7 = 15$. תהי P_3 תת־חבורת 3־סילו של G.

(א) הראה ש־$n_3 \neq 70$. **הדרכה.** ספירת אברים.

(ב) הראה ש־$n_3 \neq 10$. **הדרכה.** אחרת $\mathrm{N}_G(P_3)$ מסדר 21 ויש תת־חבורת 7־סילו P_7 שהיא נורמלית ב־$\mathrm{N}_G(P_3)$, אבל אז $\mathrm{N}_G(P_3) \leq \mathrm{N}_G(P_7)$ בסתירה לסדרים.

(ג) $n_3 \neq 7$. **הדרכה.** סעיף 2.

(ד) הסק ש־$P_3 \triangleleft G$.

(ה) קיימת תת־חבורה $A \leq G$ מסדר 105. **הדרכה.** תת־חבורות סילו של G/P_3.

(ו) הוכח ש־A ציקלית (**הדרכה.** תרגיל 8.5.10 עבור A/P_3).

(ז) יש שמונה חבורות (לא איזומורפיות) מסדר 210 עם תת־חבורה ציקלית מאינדקס 2.

תרגיל 8.5.58 (***) תהי G חבורה מסדר 240. נראה שיש לה תת־חבורה נורמלית מאחד הסדרים $2, 4, 8, 16, 5, 10, 20$.

1. $n_5 \in \{1, 6, 16\}$. אם $n_5 = 1$ אז יש ל־G תת־חבורה נורמלית מסדר 5.

2. אם $n_5 = 6$ אז $|\mathrm{Core}_G(\mathrm{N}_G(P))|$ מחלק את 8. **הדרכה.** תרגיל 8.5.35.

3. אם $n_p = 16$ אז $n_3 \in \{1, 4, 16\}$. **הדרכה.** המנרמל של תת־חבורת סילו מסדר 5 הוא מסדר 15, ומכיל תת־חבורת 3־סילו יחידה. מכיוון שכל אלו צמודות זו לזו, $n_3 \,|\, n_5$.

(א) אם $n_3 = 1$ יש תת־חבורה נורמלית מסדר 9.

(ב) אם $n_3 = 4$ יש תת־חבורה נורמלית מסדר 10 או 20. **הדרכה.** תרגיל 8.5.35.

(ג) אם $n_3 = 16$ אז $n_2 = 1$. **הדרכה.** 16 החבורות מסדר 15 נחתכות באופן טריוויאלי; ספור אברים.

תרגיל 8.5.59 (***) תהי G חבורה מסדר $540 = 2^2 3^3 5$. נראה שהיא אינה פשוטה.

1. כרגיל n_p הוא מספר תת־חבורות p־סילו. אז $n_3 = 1, 4, 10$, ו־$n_5 = 1, 6, 36$.

2. אם $n_3 = 1$ או $n_5 = 1$, אז יש ל־G תת־חבורה נורמלית מאינדקס 3 או 5.

3. אם $n_3 = 4$ או $n_5 = 6$ אז יש ל־G תת־חבורה נורמלית מאינדקס 4, 6, 12, 30 או 60.

4. נניח ש־$n_3 = 10$ ו־$n_5 = 36$. נסמן את הקבוצה של תת־חבורות 3־סילו ב־Ω_3.

(א) תהי P תת־חבורת 5־סילו. אז $T = \mathrm{N}_G(P)$ מסדר 15, ולכן T אינו מוכל במנרמל של אף $Q \in \Omega_3$. הסק שבפעולת ההצמדה של T על Ω_3 יש שני מסלולים בגודל 5. **הדרכה.** לפעולה אין נקודות שבת לפי תרגיל 6.4.69.

(ב) תהי Q_0 תת־חבורת 3־סילו של T (שהיא מסדר 3). פעולת ההצמדה של Q_0 על Ω_3 היא טריוויאלית (**הדרכה.** העלה יוצר של T בחזקת 5), ולכן היא מנרמלת כל $Q \in \Omega_3$. הסק ש־Q_0 מוכלת בכל $Q \in \Omega_3$ (תרגיל 8.4.16).

(ג) ל־G יש תת־חבורה נורמלית מסדר 3 או 9. **הדרכה.** תרגיל 8.4.53.

תרגיל 8.5.60 (+)** אם G חבורה פשוטה מסדר 60, אז $G \cong A_5$. **הדרכה.** לפי תרגילים 6.3.24 ו־6.3.25, אם יש ל־G תת־חבורה מאינדקס 5 אז $G \cong A_5$ וגמרנו, ובכל מקרה אין לה תת־חבורה מאינדקס קטן מ־5. לכן $n_2 = 15$, $n_3 = 10$ ו־$n_5 = 6$ (ולכן $G \subseteq A_6$). מכאן שיש לחבורה 20 אברים מסדר 3 ו־24 מסדר 5. לכן יש לה לכל היותר 15 אברים מסדר חזקת 2, ומכאן שיש חבורות 2־סילו עם חיתוך Q לא טריוויאלי. לפי תרגיל 8.5.51, המרכז $\mathrm{C}_G(Q)$ הוא מאינדקס ≥ 5.

תרגיל 8.5.61 (***) תהי G חבורה פשוטה מסדר $168 = 2^3 \cdot 3 \cdot 7$. נראה ש־$G \cong \mathrm{PSL}_3(\mathbb{F}_2)$.
הערה. הרעיון הוא למצוא מבנה גאומטרי שעליו החבורה פועלת, כפי שעושה $\mathrm{PSL}_3(\mathbb{F}_2)$ לפי תרגיל 7.5.20.

1. לכל תת־חבורה $H < G$ יש סדר $|H| \leq 24$. **הדרכה.** האינדקס $[G:H] \geq 7$.
2. כרגיל נסמן ב־n_p את מספר תת־חבורות p־סילו של G. אז $n_7 = 8$. לכן יש שיכון $G \subseteq A_8$, המוגדר לפי פעולת ההצמדה של G על 8 תת־חבורות 7־סילו.
3. נראה ש־$n_3 = 28$.

(א) $n_3 \in \{7, 28\}$.

(ב) כל תת־חבורה H מסדר 21 של A_8 צמודה לחבורה $\langle(1234567), (235)(476)\rangle$.
הדרכה. אפשר להניח ש־$\sigma = (1234567) \in H$. תת־החבורה מסדר 7 היא נורמלית, אבל H אינה אבלית או שהיה בה איבר מסדר 21, ולפי משפט N/C יש איבר $\tau \in H$ מסדר 3 המקיים $\tau\sigma\tau^{-1} = \sigma^2$.

(ג) G מכילה תת־חבורה מסדר 21, ולכן לכל האברים מסדר 3 ב־G יש מבנה המחזורים $[3^2 1^2]$. **הדרכה.** לטענה הראשונה התבונן במנרמל של תת־חבורת 7־סילו. כל תת־החבורות מסדר 3 צמודות זו לזו.

(ד) $n_3 = 28$. **הדרכה.** כל איבר מסדר 3 מייצב שתי תת־חבורות 7־סילו ולכן שייך לשני מנרמלים. בכל מנרמל יש 14 אברים מסדר 3. לכן מספר הזוגות (איבר מסדר 3, מנרמל של חבורת 7־סילו המכילה אותו) הוא $2n_3 \cdot 2 = 8 \cdot 14$.

4. נראה ש־$n_2 = 21$.

(א) $n_2 \in \{7, 21\}$.

(ב) סדרי האברים בחבורה הם (לכל היותר) $1, 2, 3, 4, 6, 7$.

(ג) יש בחבורה $1, 56, 48$ אברים מסדר $1, 3, 7$, בהתאמה; נסמן ב־k_2, k_4, k_6 את מספר האברים מסדר $2, 4, 6$, בהתאמה. אז $k_2 + k_4 + k_6 = 63$.

(ד) $k_6 = 0$. **הדרכה.** אם $k_6 > 0$ אז יש איבר מסדר 3 שהוא ריבוע, אבל אז כולם כאלה כי הם צמודים ולכן $k_6 \geq 56$; זה משאיר רק $63 - 56 = 7$ אברים מסדר חזקת־2, ותת־חבורת 2־סילו תצטרך להיות אבלית.

(ה) יש 63 אברים מסדר חזקת־2, ואם $n_2 = 7$ יש לכל היותר $7 \cdot (8 - 1) = 49$ אברים כאלה. לכן $n_2 > 7$.

5. נראה שיש תת־חבורות 2־סילו, S, S', עם חיתוך בגודל 4.

(א) יש $S,S' \in \mathrm{Syl}_2(G)$ כך ש־$U = S \cap S' \in \{2,4\}$. **הדרכה.** אחרת יש $21 \cdot (8-1) = 147$ אברים מסדר חזקת 2.

(ב) נניח ש־$|U| = 2$ ונסמן $N = \mathrm{N}_G(U)$. נראה ש־$|N| \in \{8,24\}$.

i. $|N| \in \{8,12,24\}$. **הדרכה.** מחד, $\mathrm{N}_S(U) \leq N$ ולכן $|N|$ מתחלק ב־4, והסדר אינו 4 כי גם $\mathrm{N}_{S'}(U) \leq N$; מאידך $[G:N] \geq 7$.

ii. לא יתכן ש־$|N| = 12$. **הדרכה.** המנרמל של תת־חבורת 3־סילו ב־G הוא מסדר 6, ולכן אין ל־N תת־חבורה נורמלית מסדר 3; מכאן שיש לה תת־חבורה נורמלית מסדר 4, אבל אז מ־$|N \cap S| = |N \cap S'| = 4$ נובע $N \cap S = N \cap S'$ בסתירה להנחה ש־$|U| = 2$.

(ג) אם $|N| = 24$ אז יש תת־חבורות 2־סילו עם חיתוך מסדר 4. **הדרכה.** N אינו יכול להכיל את SS' שיש בה $|S||S'|/|S \cap S'| = 32$ אברים; נניח ש־$S \not\subseteq N$, אז $S \cap N = \mathrm{N}_S(U)$ מסדר 4, ולכן יש $S'' \in \mathrm{Syl}_2(N) \subseteq \mathrm{Syl}_2(G)$ כך ש־$S \cap N \subseteq S''$, ואז $S \cap S''$ מסדר 4.

(ד) אם $|N| = 8$ אז $|N \cap S| = 4$, כפי שרצינו.

6. לכל תת־חבורה $C \leq G$ מסדר 24 יש שבעה צמודים, ויש בה שלוש תת־חבורות 2־סילו וארבע תת־חבורות 3־סילו של G. **הדרכה.** $\mathrm{N}_G(C) = C$ כי C אינה נורמלית ב־G, והיא תת־חבורה מקסימלית. חבורות 2־ או 3־סילו של G אינן יכולות להיות נורמליות ב־C משום שהמנרמלים שלהן ב־G הם מסדר 8 או 6, בהתאמה.

7. נבחר $S,S' \in \mathrm{Syl}_2(G)$ עם $L = S \cap S'$ מסדר 4, ונסמן $A = \mathrm{N}_G(L)$. אז $|A| = 24$.
הדרכה. $S,S' \leq \mathrm{N}_G(L)$ כי $L \lhd S, S'$, אבל $\mathrm{N}_G(L) \neq G$, ולכן $|\mathrm{N}_G(L)|$ מתחלק ב־8, גדול מ־8, ואינו עולה על 24.

8. החיתוך של כל שני צמודים של A הוא מסדר 4. **הדרכה.** יש 28 תת־חבורות 3־סילו, ולפי התכונות של A בסעיף 6, כל אחת מהן שייכת לצמוד אחד בדיוק של A, ומכאן שהחיתוך אינו מכיל חבורה מסדר 3 ולכן הוא חבורת־2. אותו נימוק (יש 21 תת־חבורות 2־סילו של G, וב־A יש שלוש תת־חבורות 2־סילו) מראה שהחיתוך אינו מסדר 8. מצד שני לכל צמוד A', $[A' : A \cap A'] \geq [G:A] = 7$.

9. נבחר A' צמוד ל־A ו־$T = A \cap A'$. אז $B = \mathrm{N}_G(T)$ הוא מסדר 24. לכן T מוכלת בשלוש תת־חבורת 2־סילו של B, ששתיים מהן הן $A \cap B$ ו־$A' \cap B$.

10. נתבונן במערכת שהנקודות שלה הן הצמודים של A, והישרים הם הצמודים של B; נאמר שנקודה נמצאת על ישר אם החיתוך של החבורות המתאימות הוא חבורת 2־סילו של G. הראה שזוהי גאומטריה פרוייקטיבית, שהופיעה בתרגיל 7.5.16.

11. G פועלת על הגאומטריה לפי הצמדה, ומהווה חבורת הסימטריות המלאה שלה.

12. $G \cong \mathrm{PSL}_3(\mathbb{F}_2)$. **הדרכה.** תרגיל 7.5.20.

הערה 8.5.62 הטבלה הבאה מסכמת את הנימוקים לכך שחבורה מסדר n אינה יכולה להיות פשוטה,

כמפורט במקרא (המספרים מציינים סדרים שהנימוקים עבורם לא הושלמו; השלם אותם.)

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
0+			p	p	p^t	p	m	p	p^t	p^t	m	p	c	p	m	m	p^t	p	m	p
20+	m	m	m	p	s	p^t	m	p^t	m	p	c'	p	p^t	m	m	m	s	p	m	m
40+	y	p	m	p	m	y	m	p	s	p^t	m	m	m	p	m	m	c	m	m	p
60+	$*$	p	m	y	p^t	m	m	p	m	m	y	p	s	p	m	m	m	m	m	p
80+	s	p^t	m	p	y	m	m	m	m	p	s'	m	m	m	m	m	s	p	m	m
100+	m	p	m	p	m	c'	m	p	s	p	m	m	s'	p	m	m	m	m	m	m
120+	s'	p^t	m	m	m	p^t	s	p	p^t	m	m	p	c'	m	m	y	m	p	m	p
140+	y	m	m	m	s^+	m	m	m	m	p	s	p	m	m	y	m	m	p	m	m
160+	s	m	m	p	m	y	m	p	$*$	p^t	m	m	m	p	m	y	s	m	m	p
180+	s^+	p	s	m	m	m	m	m	m	s	m	p	s	p	m	y	m	p	y	p
200+	y	m	m	m	m	m	m	m	s	m	n	p	m	m	m	m	s	m	m	m
220+	y	m	m	p	s	y	m	p	m	p	m	s	m	p	y	m	m	m	m	p

p — החבורה ציקלית מסדר ראשוני
p^t — n הוא חזקת ראשוני
m — $n = p^t m$ כאשר $m < p$ ולכן ת"ח p־סילו נורמלית
y — תרגיל 8.5.11: יש ת"ח סילו נורמלית
c — $n = pq^t$ כאשר $\operatorname{ord}(q)$ ב־U_p הוא t; ספירת אברים מסדר p מראה שיש ת"ח נורמלית מסדר p או q^t
c' — ספירת אברים מראה שיש תת־חבורת סילו נורמלית
s — תרגיל 8.5.44: עידון משפט קיילי
s' — עידון משפט קיילי והעדר שיכון לתוך A_n
s^+ — עידון משפט קיילי + ספירת אברים + חיתוך של ת"ח סילו והמרכז שלו
n — תרגיל 8.5.57 על חבורות מסדר 210
$*$ — יש חבורה פשוטה מסדר זה

משפט 8.5.63 אין חבורות פשוטות לא אבליות מסדר ≤ 240 פרט ל־A_5 ו־$\mathrm{PSL}_3(\mathbb{F}_2)$.

הוכחה. ראשית פוסלים את הסדרים הראשוניים ואת אלו שהם חזקת ראשוני. כשתרגילים 8.5.3 או 8.5.11 חלים, הם מוכיחים שיש לחבורה תת־חבורת סילו נורמלית. מן הסדרים הנותרים, תרגיל 8.5.44 מראה שאין חבורות פשוטות מסדר 12, 24, 36, 48, 72, 80, 96, 108, 160, 192 או 224. נותרים הסדרים 30, 56, 90, 105, 112, 120, 132, 144, 150, 180, 210, 216, 240, שכל אחד מהם טופל בתרגיל נפרד במהלך הפרק, והסדרים 60 ו־168 שמהם אכן יש חבורות פשוטות. תרגילים 8.5.60 ו־8.5.61 משלימים את המלאכה. $\square$

החבורות הפשוטות הקטנות ביותר הן $A_5 \cong \mathrm{PSL}_2(\mathbb{F}_5) \cong \mathrm{PSL}_2(\mathbb{F}_4)$ (שהיא מסדר 60; תרגילים 6.7.19, 6.7.20, ו־6.7.31); $\mathrm{PSL}_2(\mathbb{F}_7) \cong \mathrm{GL}_3(\mathbb{F}_2)$ (סדר 168, ראה תרגיל 6.7.32), $A_6 \cong \mathrm{PSL}_2(\mathbb{F}_9)$ (סדר 360, תרגיל 6.7.27); ו־$\mathrm{PSL}_2(\mathbb{F}_{11})$ (סדר 660).

8.6 החבורות הקטנות

בסעיף זה ניתן רשימה של כל החבורות הקטנות, עד כדי איזומורפיזם, לפעמים עם סריגי תת־החבורות שלהן. הרשימה מכסה את הגדלים עד 15.

תרגיל 8.6.1 (*) כל חבורה מסדר p ראשוני היא ציקלית, ואיזומורפית ל־$\mathbb{Z}_p$.

תרגיל 8.6.2 (+)** בחבורה מסדר $2p$ יש איבר מסדר p. **הדרכה**. אין צורך במשפט קושי. אם הטענה אינה נכונה אז לכל איבר לא טריוויאלי יש סדר 2. אבל אז, קח $a \neq b$ מסדר 2, וקבל (בעזרת תרגיל 2.1.10) את הסתירה $4 \mid 2p$.

תרגיל 8.6.3 (***) כל חבורה מסדר $2p$ איזומורפית ל־$\mathbb{Z}_{2p}$ או ל־D_p $(p > 2$ ראשוני). **הדרכה**. לפי תרגיל 8.6.2 יש בחבורה איבר y מסדר p. נסמן $N = \langle y \rangle$, אז $N \lhd G$ לפי תרגיל 3.3.13. 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 2.4.10) $xyx^{-1} = y^{\pm 1}$. אם $xyx^{-1} = y$ אז $o(xy) = 2p$. אחרת, $G \cong D_p$.

תרגיל 8.6.4 (**) כל חבורה מסדר p^2 היא אבלית, ואיזומורפית ל־$\mathbb{Z}_{p^2}$ או ל־$\mathbb{Z}_p^2$. **הדרכה**. משפט 8.3.3 ותרגיל 4.7.5.

תרגיל 8.6.5 (**) חבורה מסדר pq, כאשר $p < q$ ו־$q \not\equiv 1 \pmod p$, היא ציקלית.

תרגיל 8.6.6 (+*)** חבורה מסדר pq, כאשר $q \equiv 1 \pmod p$, היא או ציקלית או איזומורפית ל־$\left\langle x, y\colon\ x^p = y^q = 1,\ xyx^{-1} = y^\theta \right\rangle$ עבור $\theta \in U_q$ מסדר p (כל הבחירות של θ נותנות חבורות איזומורפיות). **הערה**. ראה תרגיל 8.1.9.

תרגיל 8.6.7 (**) יש שלוש חבורות אבליות מסדר 8: $\mathbb{Z}_4 \times \mathbb{Z}_2$, $\mathbb{Z}_8$, $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$.

תרגיל 8.6.8 (**) בחבורה $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ יש 7 תת־חבורות מסדר 2 ו־7 תת־חבורות מסדר 4, כולן איזומורפיות ל־$\mathbb{Z}_2 \times \mathbb{Z}_2$. כל תת־חבורה מסדר 2 מוכלת ב־3 תת־חבורות מסדר 4, וכל תת־חבורה מסדר 4 מכילה 3 תת־חבורות מסדר 2.

תרגיל 8.6.9 (**) תהי G חבורה לא אבלית מסדר 8.

1. קיים איבר $x \in G$ מסדר 4, ולכן תת־חבורה ציקלית נורמלית N מסדר 4.
2. יהי $y \notin N$. אז $yxy^{-1} = x^{-1}$.
3. אם קיים y כנ"ל, כך ש־$y^2 = 1$, אז $G \cong D_4$.
4. אחרת $y^2 = x^2$, ואז $G \cong Q_8$ (חבורת הקווטרניונים).

תרגיל 8.6.10 (-*)** (מיון החבורות מסדר 8 - גישה נוספת.) תהי G חבורה לא אבלית מסדר 8.

1. $G/\mathrm{Z}(G) \cong \mathbb{Z}_2 \times \mathbb{Z}_2$. **הדרכה**. לפי תרגיל 8.3.3, $\mathrm{Z}(G) \neq 1$, ולכן $G/\mathrm{Z}(G)$ מסדר 2 או 4; סיים בעזרת תרגיל 4.7.5.
2. נסמן $Z = \mathrm{Z}(G) = \{1, z\}$, ויהיו $x, y \in G$ אברים כך ש־$G/Z = \{Z, Zx, Zy, Zxy\}$. כל איבר של G אפשר להציג באופן יחיד בצורה $x^iy^jz^k$, $0 \leq i, j, k \leq 1$. בפרט $G = \langle x, y, z \rangle$.
3. $x^2, y^2, yxy^{-1}x^{-1} \in Z$. הראה ש־$yxy^{-1}x^{-1} = z$. **הדרכה**. אחרת $x \in \mathrm{Z}(G)$, בסתירה להנחה.
4. $x^2(xy)^2y^2 = z$, ולכן, על־ידי החלפת משתנים, אפשר להניח ש־$x^2 = z$.
5. אם $y^2 = 1$ אז $G \cong D_4$, ואם $y^2 = z$ אז $G \cong Q$.

תרגיל 8.6.11 (-*)** תהי G חבורה מסדר 12.

1. המספר של תת־חבורות 3־סילו של G הוא 1 או 4.
2. נניח ש־$n_3 = 1$. אז $C = P_3 \lhd G$ היא חבורת 3־סילו יחידה (ונורמלית).
   (א) קיים איבר מסדר 6. **הדרכה.** משפט N/C.
   (ב) יהי $x \in G$ מסדר 6. אם קיים איבר מסדר 2 פרט ל־x^3, אז $G \cong \mathbb{Z}_2 \times \mathbb{Z}_6$ או $G \cong D_6$.
   (ג) נניח שלא קיימים אברים מסדר 2 פרט ל־x^3. הוכח שקיים איבר y מסדר 4, וש־$y^2 = x^3$.
   (ד) $yxy^{-1} = x^{\pm 1}$. אם $yxy^{-1} = x$ אז $G \cong \mathbb{Z}_{12}$, ואם $yxy^{-1} = x^{-1}$ אז $G \cong Q_{12}$ (חבורת הקווטרניונים המוכללת מסדר 12).
3. מקרה שני. יש ארבע חבורות 3־סילו. אז $G \subseteq S_4$ ולכן $G \cong A_4$. **הדרכה.** העידון של משפט קיילי.

תרגיל 8.6.12 (***) תהי G חבורה מסדר $2p^2$.

1. נסמן ב־P את תת־חבורת p־סילו של G. אז $P \lhd G$, ואיזומורפית ל־$\mathbb{Z}_{p^2}$ או ל־$\mathbb{Z}_p \times \mathbb{Z}_p$.
2. אם $P \cong \mathbb{Z}_{p^2}$, אז G איזומורפית ל־$\mathbb{Z}_{p^2}$ או ל־D_{p^2}.
3. אחרת $P \cong \mathbb{Z}_p^2$. יהי $y \in G$ מסדר 2.
4. אם קיים $x \in P$ כך ש־ $yxy^{-1} = x$, אז $G \cong \mathbb{Z}_p \times D_p$.
5. אם קיים $x \in P$ כך ש־$\langle x \rangle$ אינה נורמלית, אז $G \cong \mathbb{Z}_p \times D_p$. **הדרכה.** קח $x_2 = yx_1y^{-1}$ והתבונן ב־$\langle x_1 x_2 \rangle$ וב־$\left\langle y, x_1 x_2^{-1} \right\rangle$.
6. $P \cong \mathbb{Z}_p^2$, ולכל $x \in P$ מתקיים $yxy^{-1} = x^{-1}$. חבורה זו נסמן ב־$\mathrm{Di}(\mathbb{Z}_p \times \mathbb{Z}_p)$.
7. הוכח ש־$\mathrm{Di}(\mathbb{Z}_p \times \mathbb{Z}_p)$ היא חבורת מנה של $D_p \times D_p$.

תרגיל 8.6.13 (***) ל־S_4 יש תת־החבורות הבאות: $\mathbb{Z}_2$ (ששה עותקים צמודים, ועוד שלושה צמודים), $\mathbb{Z}_3$ (ארבעה עותקים צמודים), $\mathbb{Z}_2^2$ (עותק אחד), $\mathbb{Z}_4$ (שלושה עותקים), S_3 (ארבעה עותקים), D_4 (שלושה עותקים), A_4.

תרגיל 8.6.14 (***) יהי p ראשוני אי־זוגי. נראה שיש בדיוק שתי חבורות לא אבליות מסדר p^3. תהי G חבורה כזו. אז $Z = \mathrm{Z}(G) \cong \mathbb{Z}_p$, ו־$G/\mathrm{Z}(G) \cong \mathbb{Z}_p \times \mathbb{Z}_p$. נכתוב $Z = \langle \alpha \rangle$ ונבחר $x, y \in G$ כך ש־$G/Z \cong \langle x, y \rangle$. אז $x^p, y^p, [y,x] \in Z$, ולכן $G = \left\{ \alpha^i x^j y^k : \; i,j,k = 0, \dots, p-1 \right\}$.

1. אם $x^p = y^p = 1$ אז אפשר להניח $[y,x] = \alpha$. במקרה זה
$$G = \langle x, y, \alpha \,|\, x^p = 1,\, y^p = 1,\, \alpha^p = 1,\, [y,x] = \alpha,\, [x,\alpha] = [y,\alpha] = 1 \rangle,$$
ומתקיים $w^p = 1$ לכל $w \in G$.
2. אחרת, על־ידי החלפת x, y, אפשר להניח ש־$y^p \neq 1$. אפשר לבחור $\alpha = y^p$. על־ידי החלפת x באיבר מהצורה xy^{-t} אפשר להניח ש־$x^p = 1$. על־ידי החלפת x בחזקה מתאימה אפשר להניח ש־$[y,x] = \alpha$. כלומר $G = \langle x, y, \alpha \,|\, x^p = 1,\, y^p = \alpha,\, \alpha^p = 1,\, [y,x] = \alpha,\, [x,\alpha] = [y,\alpha] = 1 \rangle$.

פרק 9

חבורות אבליות

בפרק זה נשתמש בכלים שבנינו עד כאן, ובעוד כמה פטנטים המיוחדים לחבורות אבליות, על־מנת לתת מיון שלם של החבורות האבליות הסופיות.

כלי העבודה הבסיסי הוא האקספוננט, שהוא המכפלה המשותפת המינימלית של סדרי האברים בחבורה. האקספוננט מאפשר לפרק כל חבורה **פירוק פרימרי**, שהוא פירוק כמכפלה ישרה של חבורות־p אבליות (לראשוניים p שונים). מכאן אפשר לקבל **הצגה קנונית** יחידה של כל חבורה אבלית סופית. כשלומדים **פיתול** ו**חוסר פיתול**, אפשר להרחיב את הטכניקה כך שתכסה כל חבורה אבלית נוצרת סופית.

9.1 האקספוננט

הגדרה 9.1.1 *__האקספוננט__ של חבורה G הוא המספר החיובי הקטן ביותר N כך ש־ $a^N = 1$ לכל $a \in G$. מסמנים מספר זה ב־$\exp(G)$.*

תרגיל 9.1.2 (*) האקספוננט של G הוא הכפולה המשותפת המינימלית של סדרי האיברים בה.

תרגיל 9.1.3 (+*) $\exp(G)$ מחלק את $|G|$. **הדרכה.** תרגיל 3.2.4

תרגיל 9.1.4 (*) $\exp(\mathbb{Z}/n\mathbb{Z}) = n$.

תרגיל 9.1.5 (+*)** חשב את $\exp(S_6)$, $\exp(S_7)$. הוכח שלכל n, האקספוננט של S_n הוא $\mathrm{lcm}\{1, \dots, n\}$.

תרגיל 9.1.6 (+*) הראה שהאקספוננט של החבורה הראשונה מתרגיל 8.6.14 הוא p.

תרגיל 9.1.7 (**) ל־$\exp(G)$ יש אותם גורמים ראשוניים כמו ל־$|G|$.

תרגיל 9.1.8 (+*)** חבורה סופית היא חבורת־p אם ורק אם הסדר שלה הוא חזקה של p, אם ורק אם האקספוננט שלה חזקת־p.

תרגיל 9.1.9 (-)** $\exp(A \times B) = [\exp(A), \exp(B)]$ (ראה הגדרה 2.2.24).

תרגיל 9.1.10 (+*)** אם G חבורה אבלית עם $\exp(G) = |G|$, אז היא ציקלית. **הדרכה.** פרק את $|G|$ לגורמים והפעל את תרגיל 2.3.27.

תרגיל 9.1.11 (**) תן דוגמה לחבורה לא ציקלית עם $\exp(G) = |G|$.

תרגיל 9.1.12 (**) (השווה לתרגיל 2.4.21) תהי G חבורה סופית מסדר n. אם לכל $d\,|\,n$ יש לכל היותר d פתרונות למשוואה $x^d = 1$, אז החבורה ציקלית. **הדרכה.** הפעל את תרגיל 9.1.10 עם $d = \exp(G)$.

תרגיל 9.1.13 (**) ידוע (ולא נוכיח זאת כאן) שמעל שדה מספר השורשים של פולינום אינו יכול לעלות על המעלה שלו. הראה שתת־חבורה סופית של החבורה הכפלית $F^{\times}$ (ראה הגדרה 2.5.1) היא תמיד ציקלית, ובפרט החבורות הכפליות $\mathbb{F}_q^{\times}$ הן ציקליות לכל שדה סופי $\mathbb{F}_q$.
הדרכה. תרגיל 9.1.12.

תרגיל 9.1.14 (**) תן הוכחה קצרה למשפט 2.3.29. **הדרכה.** לכיוון אחד חשב את האקספוננט וסיים לפי תרגיל 9.1.10. לכיוון השני הצג את $\mathbb{Z}_{nm}$ כמכפלה ישרה פנימית.

תרגיל 9.1.15 (**) אם G אבלית אז יש שיכון $U_{\exp(G)} \hookrightarrow \operatorname{Aut}(G)$. הראה שהתמונה נורמלית ב־$\operatorname{Aut}(G)$.

9.2 הפירוק הפרימרי

הזכר בהגדרה 7.1.17: אם A חבורה אבלית, אז $\mu_n\colon A \to A$ המוגדרת לפי $\mu_n(a) = a^n$ היא הומומורפיזם.

הגדרה 9.2.1 *תהי A חבורה אבלית ויהי $\mu_n : A \to A$ ההומומורפיזם של העלאה בחזקה. נסמן*

$$A^n = \operatorname{Im}(\mu_n) = \{a^n :\ a \in A\},$$

$$A_n = \operatorname{Ker}(\mu_n) = \{a \in A :\ a^n = 1\}.$$

אין קשר בין הסימון A_n לחבורת התמורות הזוגיות של הגדרה 5.1.12.

תרגיל 9.2.2 (-)** אם $(n, |A|) = 1$, אז $A^n = A$ ו־$A_n = 1$.

תרגיל 9.2.3 (**) 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 9.2.4 (+*) $\exp(A_n)\,|\,n$.

תרגיל 9.2.5 (**) נניח ש־ $\exp(A)\,|\,nm$. אז $A^n \subseteq A_m$.

תרגיל 9.2.6 (**) אם $\exp(A) = nm$ ו־n, m זרים, אז $A^n = A_m$.

משפט 9.2.7 *אם $\exp A = nm$ כאשר n, m זרים, אז $A \cong A_n \times A_m$.*

תרגיל 9.2.8 (-*)** הוכח את המשפט. **הדרכה.** כתוב $1 = \alpha n + \beta m$ והראה ש־ $A_n \cap A_m = 1$ וש־$A \subseteq A^m A^n \subseteq A_n A_m$.

תרגיל 9.2.9 (+)** 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.

משפט 9.2.10 *כל חבורה אבלית סופית היא מכפלה ישרה של חבורות־p, שהן יחידות עד־כדי איזומורפיזם.*

תרגיל 9.2.11 (**) הוכח את המשפט. **הדרכה.** אפשר בעזרת חבורות p־סילו, שכולן נורמליות משום שהחבורה אבלית. אפשרות שניה: קיום הפירוק באינדוקציה על משפט 9.2.7, לפי תרגיל 9.2.4. היחידות לפי תרגיל 9.2.9.

תרגיל 9.2.12 (**) פרק למכפלה ישרה פנימית של תת־חבורות־p את $\mathbb{Z}_{24}$ ואת U_{126}.

תרגיל 9.2.13 (**) אם m מחלק את $|A|$, אז μ_m אינו חד־חד־ערכי.

9.3 חבורות־p אבליות

ראו סעיף 8.3.

טענה 9.3.1 בחבורת־p יש איבר שסדרו שווה לאקספוננט.

תרגיל 9.3.2 (**) הוכח את הטענה. **הדרכה.** אחרת הסדר של כל האברים מחלק את $\exp(A)/p$.

בסעיפים 1.5 ו־4.3 עסקנו במכפלות ישרות של מספר סופי של מרכיבים. הגדרנו 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.

הגדרה 9.3.3 *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 (במלים אחרות, יש ל־H משלים נורמלי; אבל כל תת־חבורה של A נורמלית). ראה תרגיל 4.3.7.*

תרגיל 9.3.4 (+)** תהי A חבורה עם תת־חבורות $Q,H,B \lhd A$ כך ש־B ⊇ Q, כלומר $Q \subseteq B$, ו־$Q \cap H = 1$. נניח ש־$A/Q \cong B/Q \oplus QH/Q$. אז $A \cong B \oplus H$. **הדרכה.** לפי ההנחה $HB = HQB = A$, ו־$H \cap B = H \cap QH \cap B = H \cap Q = 1$.

משפט 9.3.5 *יהי g איבר מסדר השווה לאקספוננט בחבורת־p אבלית A. אז תת־החבורה $\langle g \rangle$ היא מחובר ישר ב־A.*

תרגיל 9.3.6 (***) הוכח את המשפט. **הדרכה.** באינדוקציה. נניח ש־ $H = \langle g \rangle \neq A$. ראשית, יהי $xH \in A/H$ איבר מסדר p, אז קיים i כך ש־$x^p = g^i$; אם i זר ל־p אז $\operatorname{ord}(x) = p \cdot \operatorname{ord}(g)$ וזה לא יתכן. לכן אפשר לכתוב $i = pj$ ואז xg^{-j} הוא איבר מסדר p מחוץ ל־H. נחליף את x באיבר הזה. כעת $Q = \langle x \rangle$ מקיים $Q \cap H = 1$ ו־$\exp(A/Q) = \exp(A)$ כי $HQ/Q \cong H$. באינדוקציה קיים $Q \subseteq K \leq A$ כך ש־ $A/Q = (HQ/Q) \oplus K/Q$ סכום ישר, ולפי תרגיל 9.3.4, $A \cong B \oplus H$.

הערה. טענת התרגיל היא שלתת־החבורה $\langle g \rangle$ יש משלים. השווה את ההוכחה למשפט שור־זסנהאוז, משפט 8.4.65.

תרגיל 9.3.7 (-*)** $A = \mathbb{Z}_4 \times \mathbb{Z}_8$. הראה שתת־החבורה הציקלית $H = \langle (0,2) \rangle \leq A$ חותכת כל תת־חבורה מסדר 8 של A, והסק שהיא אינה מחובר ישר. מדוע אין עובדה זו סותרת את משפט 9.3.5?

תרגיל 9.3.8 (***) תהי $G = \mathbb{Z}_{p^{\alpha_1}} \oplus \cdots \oplus \mathbb{Z}_{p^{\alpha_t}}$. הראה ש־$[p^{m-1}G : p^m G] = p^{|\{i : \alpha_i \geq m\}|}$. בפרט, אפשר לקרוא את קבוצת הערכים $\alpha_1, \dots, \alpha_t$ מתוך G.

משפט 9.3.9 *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 9.3.10 (**) הוכח את המשפט. **הדרכה.** הקיום באינדוקציה לפי משפט 9.3.5, והיחידות היא תרגיל 9.3.8.

תרגיל 9.3.11 (**) מצא כמה אברים מכל סדר יש בחבורות $\mathbb{Z}_{p^3}, \mathbb{Z}_{p^2} \oplus \mathbb{Z}_p$ ו־$\mathbb{Z}_p \oplus \mathbb{Z}_p \oplus \mathbb{Z}_p$.

תרגיל 9.3.12 (**) בחבורת־p אבלית לא ציקלית יש תת־חבורה מסדר p^2 שאינה ציקלית.

תרגיל 9.3.13 (**) האם קיימת חבורה אבלית G, כך ש־ $\exp(G) = 4$, $|G| = 32$, ו־$[G : G^2] = 4$?

תרגיל 9.3.14 (**) מצא את כל החבורות האבליות A שהסדר שלהן 3^{10}, האקספוננט שלהן 3^5, וכך ש־$A/9A \cong \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_9 \oplus \mathbb{Z}_9$.

תרגיל 9.3.15 (***) תת־חבורה ציקלית של A היא **ציקלית מקסימלית** אם היא אינה מוכלת באף תת־חבורה ציקלית אחרת. הוכח שאם $A = A_0 \oplus A_1$ היא חבורת־p אבלית אז כל תת־חבורה ציקלית מקסימלית של A_0 היא ציקלית מקסימלית ב־A. **הדרכה**. תהי $\langle a_0 \rangle \subseteq A_0$ תת־חבורה ציקלית מקסימלית של A_0, ונניח ש־$a_0 \in C = \langle b_0 + b_1 \rangle$ כאשר $b_i \in A_i$. לכן אפשר לכתוב $a_0 = n(b_0 + b_1) = nb_0 + nb_1$ ומכיוון שזהו סכום ישר, $nb_1 = 0$ ו־$a_0 \in \langle b_0 \rangle$. לפי המקסימליות n זר ל־p, ולכן $b_1 = 0$. (האם תכונה זו מספיקה כדי להסיק ש־A_0 מחובר ישר ב־A?)

9.4 משפט המיון לחבורות אבליות סופיות

משפט 9.4.1 ***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 9.4.2 (***) הוכח את המשפט. **הדרכה**. קיום: פרק את החבורה למכפלה של חבורות־p לפי משפט 9.2.10, ופרק כל אחת מאלה לסכום של t חבורות ציקליות לפי משפט 9.3.9. אסוף ל־$\mathbb{Z}_{d_t}$ (תרגיל 2.3.29) את המרכיב הגדול ביותר בכל קבוצה, וכן הלאה. יחידות: בחר הצגה קנונית כלשהי של A. הראה ש־$t = \max \log_p |A/pA|$, כאשר המקסימום על־פני כל הראשוניים המחלקים את $|A|$, ולכן האורך $\ell(A) = t$ מוגדר היטב. הראה ש־$\ell(\delta A) = \ell(A)$ לכל $1 < \delta < d_1$, בעוד ש־$\ell(d_1 A) < \ell(A)$, ולכן d_1 מוגדר היטב. סיים באינדוקציה על t.

תרגיל 9.4.3 (**) הראה ש־$m\mathbb{Z}_n \cong \mathbb{Z}_{\frac{n}{(n,m)}}$.

תרגיל 9.4.4 (**) 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 2.2.23).

תרגיל 9.4.5 (***) אם לשתי חבורות אבליות סופיות יש אותו מספר איברים מכל סדר, אז הן איזומורפיות. **הדרכה**. צריך להוכיח שמספר האברים מכל סדר קובע את החבורה. כתוב את החבורה בצורה הקנונית. לכל ראשוני p, מספר האברים מסדר p שווה ל־$p^m - 1$ עבור m מתאים; בחר p עם m מקסימלי; אז $p \mid d_1$, ו־m הוא אורך ההצגה. מספר האברים מכל סדר ב־A קובע את מספר האברים מכל סדר ב־A^p, ובאינדוקציה, את המבנה של A. מהאורך, p ו־A^p אפשר לשחזר את A.

תרגיל 9.4.6 (*-)** לחבורה אבלית סופית יש איבר מכל סדר המחלק את סדר החבורה. (השווה לתרגיל 8.2.2).

תרגיל 9.4.7 (**) הראה שאם $A = \mathbb{Z}_{d_1} \oplus \cdots \oplus \mathbb{Z}_{d_t}$, כאשר $d_1 \mid \cdots \mid d_t$, אז לכל $m \mid d_t$ מתקיים $m = \exp(A)/\exp(A^m)$. בפרט $\exp(A) = d_t$.

תרגיל 9.4.8 (**) מיין, עד כדי איזומורפיזם, את החבורות האבליות מהסדרים הבאים: $560, 320, 625, 210$.

תרגיל 9.4.9 (**) מיין, עד כדי איזומורפיזם, את החבורות האבליות מהסדרים הבאים: $8085, 2^2 3^2 5$.

תרגיל 9.4.10 (+)** מצא את הצורה הקנונית של $\mathbb{Z}_{12} \oplus \mathbb{Z}_{40} \oplus \mathbb{Z}_{15}$.

תרגיל 9.4.11 (**+*) כתוב איזומורפיזם מפורש $\mathbb{Z}_{40}\oplus\mathbb{Z}_{30}\oplus\mathbb{Z}_4\to\mathbb{Z}_2\oplus\mathbb{Z}_{20}\oplus\mathbb{Z}_{120}$.

תרגיל 9.4.12 (**) כתוב איזומורפיזם מפורש $\mathbb{Z}_{12}\oplus\mathbb{Z}_7\to\mathbb{Z}_{14}\oplus\mathbb{Z}_6$.

תרגיל 9.4.13 (**) מצא את כל החבורות האבליות מסדר 324 ואקספוננט 18.

תרגיל 9.4.14 (**) מצא איבר מסדר 33 ב־ $\mathbb{Z}_{15}\oplus\mathbb{Z}_{55}$.

תרגיל 9.4.15 (*+) הוכח ש־ $\mathbb{Z}_{200}\oplus\mathbb{Z}_{20}\cong\mathbb{Z}_{100}\oplus\mathbb{Z}_{40}$.

תרגיל 9.4.16 (*+) 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 9.4.17 (***) 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?

9.4.1 חבורות אוילר

ניתן לדלג בקריאה ראשונה.

הטלות ופירוק

תרגיל 9.4.18 (**) נניח $n\,|\,m$. ההעתקה $[a]_m\mapsto[a]_n$ היא הומומורפיזם $U_n\to U_m$.

תרגיל 9.4.19 (***) אם $(n,m)=1$ אז $U_{nm}\cong U_n\times U_m$. **הדרכה.** ההעתקה $U_{nm}\to U_n\times U_m$ היא חד־חד־ערכית, ולפי תרגיל 2.4.13 היא גם על. לחילופין, העזר במשפט 2.3.29 ובכך שלכל שני מונוידים M,N מתקיים $U(M\times N)=U(M)\times U(N)$.

תרגיל 9.4.20 (**) הסק מתרגיל 9.4.19 שאם $(m,n/m)=1$, אז ההעתקה $U_n\to U_m$ לפי $[a]_n\mapsto[a]_m$ היא על.

תרגיל 9.4.21 (***) הוכח שההעתקה $U_n\to U_m$ לפי $[a]_n\mapsto[a]_m$ (כאשר $m\,|\,n$) היא על. **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 9.4.22 (**) חשב את הגרעין של ההעתקה $U_{30}\to U_6$. מה המבנה של הגרעין?

תרגיל 9.4.23 (**) הוכח שהגרעין של ההעתקה $U_{p^2}\to U_p$ איזומורפי ל־$\mathbb{Z}_p$.

שיכונים

תרגיל 9.4.24 (**) מצא שיכון מפורש $U_5\to U_{25}$.

תרגיל 9.4.25 (**) הוכח שקיים שיכון $U_p\to U_{p^2}$, כאשר p ראשוני.

תרגיל 9.4.26 (**+*) הוכח שקיימים שיכונים $U_{p^{\alpha+1}}\to U_{p^\alpha}$ לכל $1<\alpha$.

תרגיל 9.4.27 (***) אם $m\,|\,n$ אז קיים שיכון $U_m\to U_n$.

חבורות אוילר ציקליות

תרגיל 9.4.28 (−*)** U_p חבורה ציקלית לכל p ראשוני. **הדרכה.** U_p היא חבורת האיברים ההפיכים בשדה $\mathbb{Z}_p$; הפעל את תרגיל 9.1.12.

תרגיל 9.4.29 (**) לכל p ראשוני, $\exp(U_p) = p-1$. **הדרכה.** תרגיל 9.4.28.

תרגיל 9.4.30 (***) אם p ראשוני אי־זוגי אז $\exp(U_{p^n}) = \phi(p^n) = (p-1)p^{n-1}$, ולכן U_{p^n} ציקלית מסדר $(p-1)p^{n-1}$. **הדרכה.** לפי תרגיל 9.4.29 והאפימורפיזם $U_{p^n} \to U_p$ של תרגיל 9.4.21, $(p-1) \mid \exp(U_{p^n})$. נשאר לחשב שהסדר של $p+1$ בחבורה הוא p^{n-1}.

תרגיל 9.4.31 (***) $\exp(U_{2^n}) = 2^{n-2}$ ולכן $U_{2^n} \cong \mathbb{Z}_2 \oplus \mathbb{Z}_{2^{n-2}}$. **הדרכה.** הוכח ש־$U_{2^n}$ נוצרת על־ידי $5, -1$, על־ידי חישוב הסדר של 5 מודולו 2^n, והחיתוך $\langle 5 \rangle \cap \langle -1 \rangle$.

תרגיל 9.4.32 (+*)** 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 9.4.33 (**) מצא יוצר לחבורת אוילר U_{49}.

תרגיל 9.4.34 (**) הראה ש־$\exp(U_{p^t}) = (p-1)p^{t-1^*}$, כאשר $1^* = 1$ אם p איזוגי, ו־$1^* = 2$ עבור $p = 2$. **הדרכה.** תרגילים 9.4.30 ו־9.4.31.

פירוק קנוני

תרגיל 9.4.35 (**) כתוב את U_{144} כמכפלת חבורות ציקליות בצורה מפורשת.

תרגיל 9.4.36 (**) 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 9.4.37 (**) כתוב את U_{100} כסכום ישר של חבורות ציקליות.

תרגיל 9.4.38 (**) כתוב את החבורות הבאות כסכום ישר של חבורות ציקליות: U_8, U_{15}, U_{30}, U_{504}.

תרגיל 9.4.39 (**) 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 9.4.40 (*) $\lambda(n) \mid \phi(n)$.

תרגיל 9.4.41 (+)** הוכח את העידון הבא של משפט אוילר (3.2.6): לכל a זר ל־n, $a^{\lambda(n)} \equiv 1 \pmod{n}$.

תרגיל 9.4.42 (**) 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 9.4.19 ו־9.4.34.

תרגיל 9.4.43 (***)
1. מצא את כל ה־n־ים עבורם $\exp(U_n) = 2$ (ראה גם תרגיל 2.4.17).
2. מיין את החבורות U_n המתקבלות, עד כדי איזומורפיזם.

3. הראה שלא קיימת חבורת אוילר $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \cong U_n$. **הדרכה.** נניח $\exp(U_n) = 2$. אם $p \mid n$ אז $U_p \subseteq U_n$ ולכן $\exp(U_p) \mid 2$ - הסק ש־ $(5, n) = 1$ וש־ $n \mid 24$.

תרגיל 9.4.44 (***) 1. אם $(a, 30) = 1$, אז $240 \mid (a^4 - 1)$.

2. לא ניתן להגדיל את המספר 240 בסעיף 1.

3. מצא את המספר הגדול ביותר m המקיים $m \mid (a^6 - 1)$ לכל a זר ל־m.

תרגיל 9.4.45 (**) מספר n שהוא פסאודו־ראשוני ביחס לכל $a \in U_n$ (כלומר $a^{n-1} \equiv 1 \pmod{n}$) נקרא **מספר קרמייקל** [ידוע שיש אינסוף מספרי קרמייקל.]

1. n הוא מספר קרמייקל אם ורק אם $\lambda(n) \mid n - 1$.

2. 561 הוא מספר קרמייקל.

3. אם $6k + 1, 12k + 1, 18k + 1$ כולם ראשוניים, אז מכפלתם היא מספר קרמייקל. מצא את הדוגמה הקטנה ביותר מסוג זה.

4. למספר קרמייקל יש לפחות שלושה גורמים ראשוניים שונים.

הגדרה 9.4.46 *איבר $a \in U_p$ נקרא **שארית ריבועית** מודולו p אם קיים $x \in U_p$ כך ש־ $a = x^2$. סימן לגרנז' מוגדר כ־ $\left(\frac{a}{p}\right) = +1$ אם a הוא שארית ריבועית, ו־ $\left(\frac{a}{p}\right) = -1$ אחרת.*

תרגיל 9.4.47 (**) $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$.

תרגיל 9.4.48 (**) $\left(\frac{a}{p}\right) = a^{\frac{p-1}{2}}$.

תרגיל 9.4.49 (+)** הראה ש־(-1) הוא שארית ריבועית מודולו $p > 2$ אם ורק אם $p \equiv 1 \pmod{4}$ (ראה תרגיל 3.2.7).

9.5 חבורות אבליות אינסופיות

תרגיל 9.5.1 (**) אם A נוצרת סופית, אז כל חבורת מנה שלה נוצרת סופית.

הגדרה 9.5.2 *חבורה (לאו דווקא אבלית) היא **מפותלת** אם לכל איבר בה יש סדר סופי, **וחסרת פיתול** אם לכל האיברים (פרט לאיבר היחידה) סדר אינסופי.*

תרגיל 9.5.3 (**) האוסף $\mathfrak{Tor}$ של חבורות מפותלות סגור לתת־חבורות, לחבורות מנה ולהרחבות (ראה הגדרה 4.9.1).

תרגיל 9.5.4 (**) האוסף $\mathfrak{Ab}$־$\mathfrak{Tor}$ של חבורות אבליות מפותלות סגור לתת־חבורות ולחבורות מנה (ראה תרגיל 4.9.9). הוא סגור גם להרחבות בתוך אוסף החבורות האבליות, כלומר, אם $B, A/B \in \mathfrak{Ab}$־$\mathfrak{Tor}$ ו־A אבלית, אז $A \in \mathfrak{Ab}$־$\mathfrak{Tor}$.

תרגיל 9.5.5 (*) אם $F, T \leq A$ כאשר T מפותלת ו־F חסרת פיתול, אז $F \cap T = 0$.

תרגיל 9.5.6 (+)** חבורה אבלית מפותלת נוצרת סופית - היא סופית. **הדרכה.** הראה שהאקספוננט e סופי, ושהחבורה היא מנה של $\mathbb{Z}_e^n$ ל־n מתאים.

הבעיה הכללית - האם חבורה מפותלת נוצרת סופית (שאינה אבלית) היא בהכרח סופית - ידועה בשם בעיית Burnside; זוהי אחת הבעיות הפתוחות המפורסמות בתורת החבורות.

תרגיל 9.5.7 (**) תן דוגמה מפורטת לחבורה מפותלת שאינה סופית.

תרגיל 9.5.8 (*-)** אוסף האברים מסדר אינסופי בחבורה אבלית (יחד עם איבר היחידה) אינו בהכרח תת־חבורה. **הצעה.**

הגדרה 9.5.9 *אוסף האיברים מסדר סופי בחבורה G נקרא **חבורת הפיתול** של G, ומסומן ב־$t(G)$.*

תרגיל 9.5.10 (*) G מפותלת אם ורק אם $t(G) = G$, וחסרת פיתול אם ורק אם $t(G) = 0$.

תרגיל 9.5.11 (-)** אם G אבלית, $t(G)$ תת־חבורה של G.

תרגיל 9.5.12 (-)** $t(A \oplus B) = t(A) \oplus t(B)$.

תרגיל 9.5.13 (**) $G/t(G)$ חבורה חסרת פיתול.

תרגיל 9.5.14 (*+)** תאר את $t(A)$ כאשר $A = \prod_{i\in\mathbb{N}} \mathbb{Z}_{2^i}$.

קבוצת יוצרים X של חבורה אבלית נקראת **בסיס** אם מהשוויון $\sum a_i x_i = 0$ עבור $x_1, \dots, x_n \in X$ ומקדמים $a_1, \dots, a_n \in \mathbb{Z}$ נובע ש־$a_i = 0$ לכל i. חבורה אבלית שיש לה בסיס היא **חבורה אבלית חופשית**.

תרגיל 9.5.15 (-)** ל־$\mathbb{Z}^n$ יש בסיס בגודל n.

תרגיל 9.5.16 (**) אם $\mathbb{Z}^n \cong \mathbb{Z}^m$ אז $n = m$. **הדרכה.** חשוב על A/A^2.

תרגיל 9.5.17 (**) חבורה אבלית שיש לה בסיס בן n אברים איזומורפית ל־$\mathbb{Z}^n$.

תרגיל 9.5.18 (***) קבוצת יוצרים בגודל מינימלי של חבורה אבלית חסרת פיתול היא בסיס.
הדרכה. נאמר ש**המשקל** של יחס $\sum a_i x_i = 0$ הוא $\sum |a_i|$. נוכיח את הטענה באינדוקציה על המשקל המינימלי 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־$|a_j| > |a_i| > 0$; 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.

משפט 9.5.19 *כל חבורה אבלית נוצרת סופית וחסרת פיתול היא מהצורה $\mathbb{Z}^n$ עבור איזשהו n.*

תרגיל 9.5.20 (***) הוכח את המשפט. **הדרכה.** קבוצת יוצרים בגודל מינימלי היא בסיס לפי תרגיל 9.5.18, והטענה נובעת מתרגיל 9.5.17.

תרגיל 9.5.21 (**) חבורה אבלית נוצרת סופית חסרת פיתול היא חופשית.

תרגיל 9.5.22 (*+)** 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 9.5.23 *חבורה אבלית נוצרת סופית היא סכום ישר של חבורה מפותלת וחבורה חסרת פיתול.*

תרגיל 9.5.24 **(***)** הוכח את המשפט. **הדרכה.** תהי A אבלית נוצרת סופית. לפי תרגילים 9.5.1 ו־9.5.13, $A/t(A)$ נוצרת סופית וחסרת פיתול. לפי משפט 9.5.19, ל־$A/t(A)$ יש בסיס, שלפי תרגיל 9.5.22 כל הרמה שלו יוצרת תת־חבורה חסרת פיתול, A_0. לפי תרגיל 9.5.5, $A_0 \cap t(A) = 0$. הוכח ש־$A = A_0 + t(A)$ והסק שהחבורות משלימות, ו־A הוא סכום ישר לפי תרגיל 4.3.7.

תרגיל 9.5.25 **(**)** 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 9.5.26 ***ההצגה של חבורה כסכום ישר של חבורה מפותלת עם אקספוננט סופי וחבורה חסרת פיתול נוצרת סופית, אם קיימת כזו, היא יחידה.***

תרגיל 9.5.27 **(***)** הוכח את המשפט. **הדרכה.** נניח ש־$G = T \oplus A$ הוא פירוק כנ"ל. לפי תרגיל 9.5.25, T נקבעת על־ידי G. קח $e = \exp(T)$. לפי משפט 9.5.19 $A = \mathbb{Z}^n$ עבור n מתאים, ולכן $G^e \cong A^e \cong A$; סיים לפי תרגיל 9.5.16.

משפט 9.5.28 ***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 9.5.29 **(***־)** הראה שאם $A \oplus B \cong \mathbb{Z} \oplus \mathbb{Z}$, $A, B \neq 0$, אז $A, B \cong \mathbb{Z}$.

תרגיל 9.5.30 **(**)** הראה ש־$\mathbb{Q}$ אינה חופשית (כחבורה אבלית).

תרגיל 9.5.31 **(**)** הראה שכל תת־חבורה אמיתית של $(\bigcup_{n=0}^{\infty} 5^{-n}\mathbb{Z})/\mathbb{Z}$ היא ציקלית סופית.

9.5.1 חבורות סדורות

הגדרה 9.5.32 ***חבורה (שאינה דווקא אבלית) היא סדורה אם מוגדר עליה יחס סדר לינארי (שלם), כך שאם*** $a < b$ ***אז לכל*** c ***מתקיים*** $ac < bc$ ***ו־***$ca < cb$***. חבורה ניתנת לסידור אם קיים יחס סדר ההופך אותה לחבורה סדורה.***

תרגיל 9.5.33 **(**)** כל חבורה אבלית חופשית (נוצרת סופית) ניתנת לסידור.

תרגיל 9.5.34 **(*)** כל חבורה סדורה היא חסרת פיתול.

9.5.2 חבורות שאינן נוצרות סופית

תרגיל 9.5.35 **(***+)** החבורה החיבורית $(\mathbb{Q}, +)$ חסרת פיתול, ואינה איזומורפית לשום חזקה של $\mathbb{Z}$.

תרגיל 9.5.36 **(***־)** תן דוגמה לחבורה מסדר אינסופי שכל האיברים שלה מסדר המחלק את n.

תרגיל 9.5.37 **(***)** תן דוגמה לחבורה אבלית אינסופית, כך ש־ A_n סופית לכל n.

תרגיל 9.5.38 **(**)** הוכח שכל תת־חבורה נוצרת סופית של $\mathbb{Q}^+$ היא ציקלית

תרגיל 9.5.39 **(**)** הוכח שהחבורות האבליות $\mathbb{Q}^+$, $\mathbb{Q}^\times$ אינן נוצרות סופית.

תרגיל 9.5.40 **(**)** הוכח שהחבורות $\mathbb{Q}^+$, $\mathbb{Q}^\times$, $\mathbb{Q}^\times_{>0}$ אינן איזומורפיות.

תרגיל 9.5.41 **(***+)** תנו דוגמא לחבורה A עם תת־חבורה אמיתית $B < A$ כך ש־$A \cong B$. תנו דוגמא לחבורות $A < B < C$ כך ש־$A \cong C$ אבל $A \not\cong B$.

פרק 10

חבורות פתירות ונילפוטנטיות

הפרק האחרון עוסק ב**סדרות תת־נורמליות** ו**סדרות הרכב**. לפי **משפט ז'ורדן-הולדר**, גורמי ההרכב של חבורה אינם תלויים בסדרת ההרכב. סדרות ההרכב מגדירות את המחלקה החשובה של **חבורות פתירות**, שאותה אפשר לאפיין ישירות גם דרך **הסדרה הנגזרת**. חבורה שיש לה **סדרה מרכזית** נקראת **חבורה נילפוטנטית**. משפט 10.3.56 מאפיין חבורות נילפוטנטיות ככאלו שהן מכפלה ישרה של חבורות־p (ומספק להן אפיונים נוספים).

10.1 סדרות תת־נורמליות וסדרות הרכב

הגדרה 10.1.1 ***סדרה תת־נורמלית*** *של חבורה G היא סדרה*

$$1 = G_n < G_{n-1} < \cdots < G_1 < G_0 = G$$

של תת־חבורות, שבה $G_i \lhd G_{i-1}$ ($i \geq 1$). החבורות G_{i-1}/G_i נקראות ***המנות*** *של הסדרה.*

סדרה תת־נורמלית המתקבלת על־ידי הכנסת תת־חבורה לא טריוויאלית $G_i \lhd G_i^* \lhd G_{i-1}$ (פעם אחת או יותר), נקראת **עידון** של הסדרה המקורית.

תרגיל 10.1.2 (*) G/N פשוטה אם ורק אם N נורמלית מקסימלית (כלומר, אינה מוכלת באף תת־חבורה נורמלית אמיתית).

תרגיל 10.1.3 (**) אם אחת המנות בסדרת הרכב אינה פשוטה, אז אפשר לעדן את הסדרה.

הגדרה 10.1.4 *סדרה תת־נורמלית שכל המנות בה פשוטות, נקראת* ***סדרת הרכב.***

תרגיל 10.1.5 (*) סדרה תת־נורמלית היא סדרת הרכב אם ורק אם כל המנות שלה פשוטות.

תרגיל 10.1.6 (**) לכל חבורה סופית יש סדרת הרכב.

תרגיל 10.1.7 (***) תהי $1 = G_n < \cdots < G_1 < G_0 = G$ סדרת הרכב של G, ותהי $N \lhd G$ תת־חבורה נורמלית.

1. הראה ש־$N_i = G_i \cap N$ (בהשמטת הצעדים השווים) מגדיר סדרת הרכב של N.
2. הראה ש־$T_i = NG_i/N$ (בהשמטת הצעדים השווים) מגדיר סדרת הרכב של G/N.

תרגיל 10.1.8 (+)** בתרגיל 10.1.7, הנחת הנורמליות אינה מיותרת: תן דוגמא לסדרת הרכב $1 = G_n < \cdots < G_1 < G_0 = G$, עם תת־חבורה $H \leq G$, כך ש־$H_i = G_i \cap H$ (בהשמטת הצעדים השווים) אינה סדרת הרכב של H. **הדרכה.** קח G פשוטה.

תרגיל 10.1.9 (-*)** האוסף $\mathfrak{Dec}$ של החבורות שיש להן סדרות הרכב סגור לתת־חבורות נורמליות, לתמונות הומומורפיות ולהרחבות (ראה הגדרה 4.9.1; ותרגיל 10.1.7.) הראה שהוא אינו סגור למכפלה ישרה אינסופית.

תרגיל 10.1.10 (**) מצא סדרת הרכב של S_4 ושל S_5.

תרגיל 10.1.11 (**) מצא את כל סדרות ההרכב של $\mathbb{Z}_{18}$.

תרגיל 10.1.12 (**) מצא את כל סדרות ההרכב של $S_n \times S_n$, כאשר $5 \leq n$; מצא גם את כל סדרות ההרכב של $S_4 \times S_4$.

תרגיל 10.1.13 (**) המנות בסדרת הרכב של חבורת־p סופית הן ציקליות מסדר p. **הדרכה.** תרגיל 8.3.5 או תרגיל 8.3.39.

תרגיל 10.1.14 (**) רשום את כל סדרות ההרכב של החבורות D_4 ו־Q. **הדרכה.** יש 7 ו־3, בהתאמה.

תרגיל 10.1.15 (***) חשב סדרת הרכב מפורשת עבור החבורה $G = \mathrm{GL}_2(\mathbb{F}_3)$. **הדרכה.** נסמן $a = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$, $\sigma = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, $\tau = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$, $c = \begin{pmatrix} -1 & 1 \\ 1 & 1 \end{pmatrix}$. חשב את תת־החבורות $\langle c, \tau, \sigma \rangle \subseteq \langle c, \tau \rangle \subseteq \langle c \rangle$.

תרגיל 10.1.16 (**) מה יכולים להיות גורמי ההרכב של חבורה מסדר 240?

משפט ז'ורדן-הולדר

תרגיל 10.1.17 (-)** נניח ש־$A, B \lhd G$ נורמליות מקסימליות ושונות זו מזו. הראה ש־$G = AB$ וש־$A/(A \cap B)$ פשוטה.

משפט 10.1.18 (משפט ז'ורדן-הולדר) *כל סדרות ההרכב של חבורה G הן באותו אורך, ולכולן אותן מנות הרכב עד כדי סדר.*

הוכחה. נאמר ששתי סדרות הרכב הן **שקולות** אם הן בעלות אותו אורך ויש להן מנות שוות עד כדי סדר (ברור שזה אכן יחס שקילות). ההוכחה היא באינדוקציה על האורך של הקצרה מבין שתי הסדרות.

תהיינה

$$1 = A_n < A_{n-1} < \cdots < A_1 < A_0 = G$$

ו־

$$1 = B_m < B_{m-1} < \cdots < B_1 < B_0 = G$$

שתי סדרות הרכב. אם $A_1 = B_1$ אז הסדרות $1 < \cdots < A_1$ ו־$1 < \cdots < B_1$ שקולות לפי הנחת האינדוקציה. אחרת ניקח $C_2 = A_1 \cap B_1$ ונתבונן בסדרת הרכב

$$1 = C_t < C_{t-1} < \cdots < C_2$$

(סדרה כזו קיימת לפי תרגיל 10.1.7 משום ש־$C_2 \lhd G$). לפי הנחת האינדוקציה, הסדרות $1 = C_t < \cdots < C_2 < A_1$ ו־$1 = A_n < A_{n-1} < \cdots < A_1$ שקולות, והסדרות $1 = C_t < \cdots < C_2 < B_1$ ו־$1 = B_m < B_{m-1} < \cdots < B_1$ שקולות. לפי תרגיל 10.1.17 הסדרות $C_2 < A_1 < G$ ו־$C_2 < B_1 < G$ שקולות ולכן גם הסדרות המקוריות שקולות זו לזו. $\square$

חבורות המנה בסדרת הרכב (כלשהי) של חבורה סופית G הם **גורמי ההרכב** של החבורה.

תרגיל 10.1.19 (+*)** הראה שלחבורות S_6 ו־$\mathrm{PGL}_2(\mathbb{F}_9)$, שאינן איזומורפיות, יש אותם גורמי הרכב (העזר בתרגיל 6.7.27).

10.2 חבורות פתירות

הגדרה 10.2.1 ***חבורה פתירה*** *היא חבורה שיש לה סדרה תת־נורמלית שכל המנות בה אבליות.*

(יש בספרות הגדרות שונות לפתירות, שכולן מתלכדות עבור חבורות סופיות.)

תרגיל 10.2.2 (*) כל חבורה אבלית היא פתירה.

תרגיל 10.2.3 (**) חבורה סופית היא פתירה אם ורק אם גורמי ההרכב שלה הם חבורות ציקליות מסדר ראשוני.

תרגיל 10.2.4 (*) החבורה $G \times H$ פתירה אם ורק אם G, H פתירות.

תרגיל 10.2.5 (**) כל החבורות הדיהדרליות D_n הן פתירות.

תרגיל 10.2.6 (+)** החבורות A, B מתרגיל 6.6.66 פתירות.

תרגיל 10.2.7 (*+) כל חבורה G מסדר 88 היא פתירה.

תרגיל 10.2.8 (*+) כל חבורה מסדר $1089 = 3^2 \cdot 11^2$ היא פתירה.

תרגיל 10.2.9 (***) תהי G חבורה לא פתירה מסדר 120 שתת־חבורת 2־סילו שלה היא חבורת הקווטרניונים Q_8. נוכיח ש־$G \cong \mathrm{SL}_2(\mathbb{F}_5)$.

1. ראשית נראה ש־G היא הרחבה מרכזית של A_5 בחבורה מסדר 2.

(א) כל תת־חבורה נורמלית של G היא מסדר 2 או 60. אין ל־G תת־חבורות מאינדקס 3 או 4. **הדרכה.** משפט 8.5.63.

(ב) ל־G יש 6 תת־חבורות 5־סילו, ולכן 24 איברים מסדר 5.

(ג) נניח שאין ל־G תת־חבורה מאינדקס 5. אז יש לה שתי תת־חבורות 2־סילו הנחתכות באופן לא טריוויאלי. יש להן איבר משותף מסדר 2. איבר זה הוא מרכזי וחבורת המנה ביחס אליו היא A_5.

(ד) נניח שיש ל־G תת־חבורה מאינדקס 5. אז יש הומומורפיזם $G \to S_5$, שאינו יכול להיות שיכון (כי חבורת 2־סילו של S_5 היא דיהדרלית). לכן יש לו גרעין מסדר 2, שהמנה ביחס אליו היא A_5.

2. יש רק שתי הרחבות מרכזיות של A_5 בחבורה מסדר 2 (תרגיל 7.4.49). חבורת 2־סילו של $A_5 \times \mathbb{Z}_2$ היא אבלית, ולכן $G \neq A_5 \times \mathbb{Z}_2$.

3. $G \cong \mathrm{SL}_2(\mathbb{F}_5)$ משום שגם $\mathrm{SL}_2(\mathbb{F}_5)$ אינה פתירה (תרגיל 6.7.31) ותת־חבורת 2־סילו שלה איזומורפית ל־Q_8 (תרגיל 8.4.43).

תרגיל 10.2.10 (**) כל חבורת־p סופית היא פתירה. למעשה, אם $|G| < p^{\binom{m}{2}}$ אז $G^{(m-2)} = 1$.
הדרכה. משפט מילר, 8.3.32.

תרגיל 10.2.11 (+)** תן דוגמה לתת־חבורה של חבורה פתירה, שאינה נורמלית וגם אינה אבלית.

תרגיל 10.2.12 (*) פרובניוס הוכיח שחבורה מסדר $p^a q^b$ לעולם אינה פשוטה. הוכח שכל חבורה כזו היא פתירה.

תרגיל 10.2.13 (+*)** יהי F שדה. הוכח שהחבורה $B_n(F)$ מתרגיל 2.7.5 היא פתירה.

תרגיל 10.2.14 (**) תן דוגמאות (נוספות) לחבורות פתירות אינסופיות שאינן אבליות.

תת־חבורה $A \leq G$ היא **2־קשורה** אם יש סדרה $A = A_0 \leq A_1 \leq \cdots \leq A_t = G$ כך ש־$[A_{i+1} \colon A_i] = 2$ לכל i (המינוח אינו סטנדרטי).

תרגיל 10.2.15 (***) נניח ש־$A, B \leq G$ הן 2־קשורות. הוכח שגם $A \cap B$ 2־קשורה.

תרגיל 10.2.16 (**) תת־חבורה 2־קשורה מינימלית (כלומר, כזו המוכלת בכל תת־חבורה 2־קשורה) היא נורמלית.

תרגיל 10.2.17 (**) לכל חבורה סופית G יש תת־חבורה 2־קשורה מינימלית.

תרגיל 10.2.18 (***) כל תת־חבורה 2־קשורה A של G מכילה תת־חבורה 2־קשורה נורמלית, שהאינדקס שלה ב־G מחלק את $2^{\frac{1}{2}[G:A]}$. **הדרכה.** העזר בעידון של משפט קיילי: $[G \colon \mathrm{Core}_G(A)]$ מחלק את $[G \colon A]!$.

תרגיל 10.2.19 (***) נניח שלחבורה G יש תת־חבורת 2־סילו ציקלית לא טריוויאלית.

1. הוכח שיש ל־G תת־חבורה מאינדקס 2. **הדרכה.** תרגיל 8.4.37.
2. הראה שגם לתת־חבורה זו יש חבורת 2־סילו ציקלית.
3. הסק שיש ל־G תת־חבורה 2־קשורה (מינימלית, ולכן נורמלית) מסדר אי־זוגי.

תרגיל 10.2.20 (**) חבורה מסדר $2m$, כאשר m איזוגי, אינה פשוטה. **הדרכה.** תרגיל 10.2.19.

10.2.1 הסדרה הנגזרת

הגדרה 10.2.21 *תהי G חבורה. מגדירים באינדוקציה $G^{(0)} = G$, $G^{(n+1)} = [G^{(n)}, G^{(n)}]$ (בפרט $G^{(1)} = G'$). הסדרה*

$$\cdots \leq G^{(n)} \leq \cdots \leq G''' \leq G'' \leq G' \leq G$$

*נקראת **הסדרה הנגזרת** של G.*

תרגיל 10.2.22 (**) כל אחת מהחבורות $G^{(n)}$ היא תת־חבורה אופיינית של G (הגדרה 7.2.42).

תרגיל 10.2.23 (**) חשב את הסדרה הנגזרת של S_4.

תרגיל 10.2.24 (+*)** חשב את הסדרה הנגזרת של

$$G = \langle (12)(34)(56)(78), (13)(24)(57)(68), (15)(26)(37)(48) \rangle \leq S_8.$$

טענה 10.2.25 תהי

$$1 = G_n \leq G_{n-1} \leq \cdots \leq G_1 \leq G_0 = G$$

סדרה תת־נורמלית עם מנות אבליות של חבורה (פתירה) G. אז לכל i, $G^{(i)} \subseteq G_i$.

הוכחה. אינדוקציה. עבור $i = 0$ הטענה טריוויאלית, ואם $G^{(i)} \subseteq G_i$ אז $G^{(i+1)} = [G^{(i)}, G^{(i)}] \subseteq [G_i, G_i] \subseteq G_{i+1}$ לפי משפט 4.8.6, כי המנה G_i/G_{i+1} אבלית. □

משפט 10.2.26 ***חבורה סופית G היא פתירה אם ורק אם קיים n כך ש־$G^{(n)} = 1$.***

הוכחה. אם $G^{(n)} = 1$ אז הסדרה הנגזרת היא סדרה תת־נורמלית עם מנות אבליות, ולכן החבורה פתירה. להיפך, אם לחבורה יש סדרה תת־נורמלית $1 = G_n \leq G_{n-1} \leq \cdots \leq G_1 \leq G_0 = G$ עם מנות אבליות, אז $G^{(n)} \subseteq G_n = 1$ לפי הטענה. $\square$

תרגיל 10.2.27 (*–)** האוסף $\mathfrak{Sol}$ של החבורות הפתירות סגור לתת־חבורות, לתמונות הומומורפיות ולהרחבות (ראה הגדרה 4.9.1.) הראה שהוא אינו סגור למכפלה ישרה אינסופית.

הגדרה 10.2.28 ***סדרה נורמלית של חבורה G היא סדרה***

$$1 = G_n < G_{n-1} < \cdots < G_1 < G_0 = G$$

של תת־חבורות, שבה $G_i \lhd G_0$ לכל i.

(סדרת הרכב נורמלית נקראת **סדרה ראשית** של החבורה.)

תרגיל 10.2.29 (*) כל סדרה נורמלית היא גם תת־נורמלית, אבל לא להיפך. **הערה**. המונחים "סדרה תת־נורמלית" ו"סדרה נורמלית" נקראים בספרות גם בשמות אחרים; אצל Scott, למשל, אלו "סדרה נורמלית" ו"סדרה אינווריאנטית".

תרגיל 10.2.30 (***) בחן את התנאים הבאים על חבורה G:

1. יש לחבורה סדרת הרכב עם מנות ציקליות מסדר ראשוני.
2. יש לחבורה סדרה תת־נורמלית עם מנות אבליות ("פתירה").
3. יש לחבורה סדרה תת־נורמלית עם מנות ציקליות ("פוליציקלית").
4. יש לחבורה סדרה תת־נורמלית עם מנות ציקליות מסדר ראשוני.
5. יש לחבורה סדרה נורמלית עם מנות אבליות.
6. יש לחבורה סדרה נורמלית עם מנות ציקליות ("סופר־פתירה").
7. יש לחבורה סדרה נורמלית עם מנות ציקליות מסדר ראשוני.

הראה שאם G סופית, תנאים 1–5 שקולים זה לזה, ושתנאי 7 חזק מתנאי 6, החזק מתנאי 5.

תרגיל 10.2.31 (**) לחבורה פתירה יש תת־חבורה נורמלית אבלית. **הדרכה**. יש n מינימלי כך ש־$G^{(n)} = 1$. (ולכן הטכניקות של הרחבת חבורות, עם גרעין אבלי, תקפות לחבורות פתירות.)

תרגיל 10.2.32 (***) תהי G חבורה פתירה. כל תת־חבורה נורמלית $H \lhd G$ מכילה תת־חבורה אבלית לא־טריוויאלית שהיא נורמלית ב־G. **הדרכה**. הכלל את הפתרון לתרגיל 10.2.31: נניח ש־m מינימלי כך ש־$H \cap G^{(m)} = 1$; אז $H \cap G^{(m-1)} \cong (H \cap G^{(m-1)})G^{(m)}/G^{(m)} \leq G^{(m-1)}/G^{(m)}$ וזו תת־חבורה אבלית ונורמלית.

תרגיל 10.2.33 (***) חבורה G היא **פתירה למעשה** (virtually solvable) אם יש לה תת־חבורה פתירה מאינדקס סופי. הראה שאם $G/N \cong \mathbb{Z}$ ו־N פתירה למעשה, אז גם G פתירה למעשה.

חבורות מושלמות

הגדרה 10.2.34 חבורה H המקיימת את התנאי $H' = H$ נקראת **מושלמת**.

הסדרה הנגזרת של חבורה סופית עוצרת באחת משתי דרכים: או שעבור n מספיק גדול $G^{(n)} = 1$, או ש־$H = G^{(n)} \neq 1$ היא חבורה מושלמת.

תרגיל 10.2.35 (**) כל חבורה פשוטה לא אבלית היא מושלמת.

תרגיל 10.2.36 (*+)** החבורה $\mathrm{SL}_2(\mathbb{F}_5)$ היא מושלמת, אבל אינה פשוטה.

תרגיל 10.2.37 (**) אין חבורת־p מושלמת. **הדרכה**. תרגיל 8.3.10.

תרגיל 10.2.38 (*+)** מכפלה ישרה למחצה $G = K \rtimes Q$ היא מושלמת אם ורק אם Q מושלמת, והקומוטטורים $[q,k] = (qkq^{-1})k^{-1}$ $(k \in K, q \in Q)$ פורשים את חבורת המנה K/K'.

תרגיל 10.2.39 (*+)** מכפלה ישרה למחצה של חבורות מושלמות היא מושלמת.

תרגיל 10.2.40 (**) מכפלה ישרה היא מושלמת אם ורק אם כל רכיביה מושלמים.

תהי G חבורה. הרחבה $H \to G$ נקראת **העתקת כיסוי** אם $Z(H) \leq H'$. העתקת כיסוי $U \to G$ היא **אוניברסלית** אם כל העתקת כיסוי $H \to G$ מפצלת את $U \to G$ (ראה הגדרה 3.5.17).

תרגיל 10.2.41 (**+)** לחבורה סופית מושלמת יש העתקת כיסוי אוניברסלית.

10.2.2 תת־חבורת פרטיני

ניתן לדלג בקריאה ראשונה.

תרגיל 10.2.42 (**) החבורה $\mathbb{Z}_p \times \cdots \times \mathbb{Z}_p = (\mathbb{Z}_p)^n$ נוצרת על־ידי n אברים, ולא פחות מזה. **הדרכה**. זהו מרחב וקטורי מעל השדה $\mathbb{Z}_p$.

הגדרה 10.2.43 *תהי G חבורה. החיתוך של כל תת־החבורות המקסימליות של G נקרא **תת־חבורת פרטיני** של G, ומסומן ב־$\Phi(G)$.*

תרגיל 10.2.44 (+)** $\Phi(G)$ תת־חבורה אופיינית של G. בפרט, $\Phi(G) \lhd G$.

תרגיל 10.2.45 (**) נניח ש־G חבורה סופית. לכל תת־חבורה אמיתית $N < G$, גם $\langle N, \Phi(G) \rangle < G$. **הדרכה**. N מוכלת בתת־חבורה מקסימלית של G.

תרגיל 10.2.46 (*−)** איבר $x \in G$ הוא לא־יוצר אם לכל קבוצת יוצרים A של G, גם $A - \{x\}$ יוצרת את G. הוכח ש־$\Phi(G)$ היא קבוצת האיברים הלא־יוצרים של G.

תרגיל 10.2.47 (***) נניח ש־G חבורת־p.

1. $\Phi(G) = G'G^p$, ולכן $G/\Phi(G) \cong \mathbb{Z}_p^n$ לאיזשהו n.
2. בכל קבוצת יוצרים מינימלית של G יש $\mathrm{rank}(G/\Phi(G))$ אברים.

תרגיל 10.2.48 (*+)** תהי G חבורת 2־סילו של S_6. חשב את $\Phi(G)$ ואת $G/\Phi(G)$.

תרגיל 10.2.49 (*−)** לכל חבורה G, $Z(G) \cap G' \subseteq \Phi(G)$. **הדרכה**. תהי $M < G$ תת־חבורה מקסימלית. נתבונן ב־$M \leq MZ(G) \leq G$. אם $MZ(G) = G$ אז $M \lhd G$, ואז M/G ציקלית מסדר ראשוני ולכן $G' \subseteq M$. אחרת $Z(G) \subseteq M$.

תרגיל 10.2.50 (*−)** תת־חבורה מקסימלית של G (כלומר תת־חבורה אמיתית שאינה מוכלת בשום תת־חבורה אמיתית אחרת) אינה יכולה להכיל גם את G' וגם את $Z(G)$.

10.2.3 חבורות סופר־פתירות

הגדרה 10.2.51 *חבורה היא **סופר־פתירה** אם יש לה סדרה נורמלית עם מנות ציקליות.*

תרגיל 10.2.52 (*−)** מחלקת החבורות הסופר־פתירות סגורה לתת־חבורות, לחבורות מנה, למכפלה תת־ישרה סופית ולהרחבה בחבורה ציקלית (אבל לא להרחבות באופן כללי).

תרגיל 10.2.53 (***) כל חבורה סופר־פתירה היא הרחבה של חבורה אבלית סופית בחבורה נילפוטנטית.

תרגיל 10.2.54 (*+)** כל חבורה סופר־פתירה היא פתירה.

10.2.4 תנאי סופיות

חבורה מקיימת את **תנאי המקסימום** אם בכל קבוצה לא ריקה של תת־חבורות שלה יש איבר מקסימלי.

תרגיל 10.2.55 (+)** לחבורה המקיימת את תנאי המקסימום יש תת־חבורה מקסימלית.

לפי הלמה של צורן, תנאי המקסימום שקול ל**תנאי השרשרת העולה** (ACC), שלפיו כל שרשרת (בת־מניה) עולה חייבת לעצור.

תרגיל 10.2.56 (***) חבורה מקיימת את תנאי המקסימום אם ורק אם כל תת־חבורה שלה נוצרת סופית.

תרגיל 10.2.57 (***) מחלקת החבורות המקיימות ACC סגורה לתת־חבורות, לחבורות מנה ולהרחבות.

תרגיל 10.2.58 (*−)** תהי $H < G$ תת־חבורה ונניח שקיים איבר $x \in G$ כך ש־$G = \langle H, x \rangle$. אז H מוכלת בתת־חבורה מקסימלית של G. **הדרכה**. הלמה של צורן: אוסף תת־החבורות המכילות את H אבל לא את x סגור לאיחוד של שרשראות.

תרגיל 10.2.59 (**) החבורה $\left\{ \begin{pmatrix} 2^n & 2^m k \\ 0 & 2^{-n} \end{pmatrix} : n, m, k \in \mathbb{Z} \right\}$ נוצרת סופית, אבל אינה מקיימת את תנאי המקסימום.

הערה. חבורה פתירה מוצגת סופית אינה חייבת לקיים את תנאי המקסימום אפילו על תת־חבורות נורמליות; ראה [Yu. V. Sosnovskii Finitely presented solvable groups that do not satisfy the maximal condition for normal subgroups Mathematical notes of the Academy of Sciences of the USSR (1984), 577–580, Vol. 36(2)].

חבורות פוליציקליות וחבורות־M

הגדרה 10.2.60 *חבורה נקראת **חבורת־M** אם יש לה סדרה תת־נורמלית שבה כל מנה אינסופית היא ציקלית.*

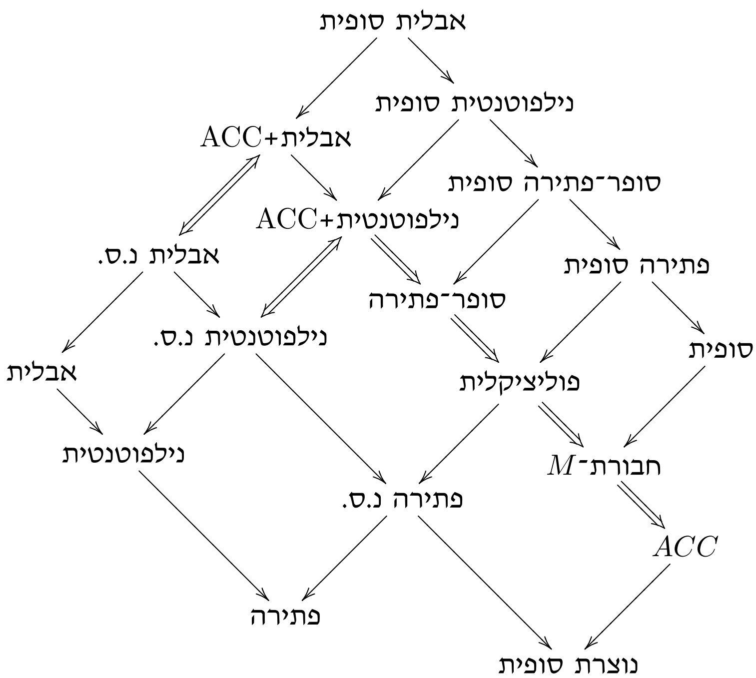
תרגיל 10.2.61 (***) המחלקה של חבורות־M סגורה לתת־חבורות, לחבורות מנה ולהרחבות.

תרגיל 10.2.62 (***) כל חבורה סופר־פתירה היא חבורת־M.

תרגיל 10.2.63 (*−)** חבורת־M מקיימת את תנאי המקסימום.

הגדרה 10.2.64 *חבורה **פוליציקלית** היא חבורה שיש לה סדרה תת־נורמלית עם מנות ציקליות.*

תרגיל 10.2.65 (***) חבורה היא פוליציקלית אם ורק אם היא פתירה ומקיימת את התנאי ACC.



איור 10.1: מחלקות חשובות של חבורות

10.3 סדרות מרכזיות

סדרה תת־נורמלית $G_0 \leq \cdots \leq G_n$ בחבורה G נקראת **סדרה נורמלית** אם $G_i \lhd G$ לכל i. (לשם הכלליות איננו מניחים ש־$G_n = 1$ או ש־$G_0 = G$).

הגדרה 10.3.1 *סדרה נורמלית $G_0 \leq \cdots \leq G_n$ בחבורה G נקראת* ***סדרה מרכזית*** *אם $G_{i-1}/G_i \subseteq \mathrm{Z}(G/G_i)$ לכל $1 \leq i$.*

תרגיל 10.3.2 (*) כל המנות בסדרה מרכזית הן אבליות.

תרגיל 10.3.3 (*) נניח ש־$G_0 \leq \cdots \leq G_n$ מרכזית. אז $G \leq G_0 \leq \cdots \leq G_n$ מרכזית אם ורק אם G/G_0 אבלית, ו־$G_0 \leq \cdots \leq G_n \leq 1$ מרכזית אם ורק אם $G_n \subseteq \mathrm{Z}(G)$.

תרגיל 10.3.4 (+*) תהי $B \leq G$. אז $[G,B] \leq B$ אם ורק אם $B \lhd G$.

תרגיל 10.3.5 (*) סדרה תת־נורמלית היא מרכזית אם ורק אם לכל i, $[G, G_{i-1}] \subseteq G_i$.

תרגיל 10.3.6 (+)** תן דוגמא לסדרה נורמלית שאינה מרכזית.

תרגיל 10.3.7 (+)** אם $G_0 \leq \cdots \leq G_n$ סדרה מרכזית בחבורה G ו־$G_i \leq G_i^* \leq G_{i-1}$, אז גם $G_0 \leq \cdots \leq G_{i-1} \leq G_i^* \leq G_i \leq \cdots \leq G_n$ מרכזית. **הדרכה.** את התנאי $G_{i-1}/G_i \subseteq \mathrm{Z}(G/G_i)$ מחליפים שני התנאים $G_{i-1}/G_i^* \subseteq \mathrm{Z}(G/G_i^*)$ ו־$G_i^*/G_{i-1} \subseteq \mathrm{Z}(G/G_{i-1})$.

תרגיל 10.3.8 (**) כל סדרה מרכזית $G_0 \leq \cdots \leq G_n$ אפשר לעדן לסדרת הרכב (של G_0/G_n). **הדרכה.** תרגיל 10.3.7.

10.3.1 הסדרה המרכזית היורדת

הגדרה 10.3.9 ***הסדרה המרכזית היורדת*** *של G היא הסדרה*

$$\cdots \leq G_{(4)} \leq G_{(3)} \leq G_{(2)} \leq G_{(1)} = G$$

המוגדרת לפי $G_{(n+1)} = [G_{(n)}, G]$. *בפרט* $G_{(2)} = [G,G] = G'$.

סדרה זו יורדת מ־G, אבל אינה מוכרחה להסתיים ב־1.

תרגיל 10.3.10 (**) לכל n, $G_{(n+1)}$ היא תת־החבורה הנורמלית המינימלית של G שעבורה $G_{(n)}/G_{(n+1)}$ מרכזית ב־$G/G_{(n+1)}$.

תרגיל 10.3.11 (**) כל החבורות $G_{(n)}$ הן תת־חבורות אופייניות של G.

תרגיל 10.3.12 (**) הסדרה המרכזית היורדת היא אכן סדרה מרכזית.

תרגיל 10.3.13 (***) אם G/G' ציקלית, אז $G_{(n)} = G'$ לכל $2 < n$. **הדרכה.** הוכח ש־$G/G_{(3)}$ אבלית.

תרגיל 10.3.14 (**) יהי n מינימלי כך ש־$G_{(n)} = 1$ (אם קיים כזה). הוכח ש־$G_{(n-1)} \subseteq \mathrm{Z}(G)$.

תרגיל 10.3.15 (-*)** $[G_{(n)}, G_{(m)}] \subseteq G_{(n+m)}$. **הדרכה.** עבור $m=1$ הטענה נכונה לפי ההגדרה. באינדוקציה, $[G_{(n)}, G_{(m+1)}] = [G_{(n)}, [G, G_{(m)}]] \subseteq [G, [G_{(m)}, G_{(n)}]] \cdot [G_{(m)}, [G_{(n)}, G]] \subseteq [G, G_{(n+m)}] \cdot [G_{(m)}, G_{(n+1)}] \subseteq G_{(n+m+1)} \cdot G_{(n+m+1)} = G_{(n+m+1)}$ בעזרת תרגיל 4.8.22.

תרגיל 10.3.16 (+)** לכל $n,m \geq 1$, $(G_{(n)})_{(m)} \subseteq G_{(nm)}$. **הדרכה.** לפי תרגיל 10.3.15.

תרגיל 10.3.17 (**) $G^{(k)} \subseteq G_{(2^k)}$.

הערה 10.3.18 $Grün$ הוכיח ש־$G_{(n)}$ הוא חיתוך כל הגרעינים של ההומומורפיזמים $G \to U_n(\mathbb{Z})$, כאשר U_n היא החבורה היוניפוטנטית שהוגדרה בתרגיל 3.5.20 [$Deutsche\ Math.$ **1**, 1936].

תרגיל 10.3.19 (+)** לכל $n \geq 1$ ולכל $N \triangleleft G$, $(G/N)_{(n)} = G_{(n)}N/N$.

תרגיל 10.3.20 (**) לכל הומומורפיזם $\varphi : G \to H$, $\varphi(G_{(n)}) \subseteq H_{(n)}$.

תהיינה $A, B \triangleleft G$. מגדירים $[A,_1 B] = [A, B]$ ובאינדוקציה $[A,_{n+1} B] = [[A,_n B], B]$. בפרט $[G,_n G] = G_{(n+1)}$.

תרגיל 10.3.21 (**) נניח ש־$G = HN$ כאשר $H \leq G$ ו־$N \triangleleft G$. אז לכל n, $G_{(n+1)} = H_{(n+1)}[N,_n G]$.

תרגיל 10.3.22 (**) תהי $H \leq G$. אם $G = HG_{(2)}$ אז $G = HG_{(n)}$ לכל n. **הדרכה.** באינדוקציה. נניח ש־$G = HG_{(n)}$, אז $G' = G_{(2)} = H_{(2)}[G_{(n)}, G] = H'G_{(n+1)}$ לפי תרגיל 10.3.21, ולכן $G = HG' = HH'G_{(n+1)} = HG_{(n+1)}$.

תרגיל 10.3.23 (+)** בהמשך לתרגיל 3.5.23 על חבורת הייזנברג המוכללת,

1. נניח ש־$\prec \triangleleft \prec', \prec''$. אז $[H(\prec'), H(\prec'')] = H(\prec'\prec'' \cup \prec''\prec')$.
2. הראה ש־$H(\prec)_{(n)} = H(\prec^n)$.
3. הראה ש־$[H(\prec)_{(n)}, H(\prec)_{(n')}] = H(\prec)_{n+n'}$ (כך שהחסם של תרגיל 10.3.15 עשוי להיות הדוק).

הסדרה המרכזית היורדת ב־p

הגדרה 10.3.24 ***הסדרה המרכזית היורדת ב־p של G, מוגדרת לפי*** $G = G_{(1,p)}$ ו־$G_{(n+1,p)} = G^p_{(n,p)}[G_{(n,p)}, G]$.

בפרט, $G_{(n)} \subseteq G_{(n,p)}$ לכל p.

תרגיל 10.3.25 (**) לכל n, $G_{(n+1,p)}$ היא תת־החבורה הנורמלית המינימלית של G שעבורה $G_{(n,p)}/G_{(n+1,p)}$ מרכזית ב־$G/G_{(n+1,p)}$ ובעלת אקספוננט p. (השווה לתרגיל 10.3.10).

10.3.2 הסדרה המרכזית העולה

הגדרה 10.3.26 ***אם*** $N \leq G$, ***נסמן*** $N^{[G]} = \{x \in G : [x, G] \subseteq N\}$

תרגיל 10.3.27 (**)

1. $N^{[G]} \leq G$.
2. אם $N \triangleleft G$ נורמלית אז גם $N^{[G]} \triangleleft G$, ובמקרה זה $N \subseteq N^{[G]}$.
3. אם $N_1 \subseteq N_2$ אז $N_1^{[G]} \subseteq N_2^{[G]}$.

תרגיל 10.3.28 (**) לכל $N \triangleleft G$, $\mathrm{Z}(G/N) = N^{[G]}/N$.

הגדרה 10.3.29 ***הסדרה המרכזית העולה של G היא הסדרה*** $1 = \zeta_0 G \leq \zeta_1 G \leq \zeta_2 G \leq \cdots$, ***המוגדרת לפי*** $\zeta_{n+1}G = \zeta_n G^{[G]}$.

לפי תרגיל 10.3.28 מתקיים $\zeta_{n+1}G/\zeta_n G = \mathrm{Z}(G/\zeta_n G)$. בפרט $\zeta_1 G = \mathrm{Z}(G)$. סדרה זו עולה מ־$1$, אבל היא אינה מוכרחה להסתיים ב־G.

תרגיל 10.3.30 (*) תת־החבורות $\zeta_n G$ אופייניות ב־G, ובפרט נורמליות.

תרגיל 10.3.31 (+*) $N = \zeta_{n+1}G$ היא תת־החבורה הגדולה ביותר של G המקיימת $[G,N] \subseteq \zeta_n G$.

תרגיל 10.3.32 (**) תהי $H \leq G$. אם $\zeta_n G \subseteq H$ אז $\zeta_{n+1}G \subseteq \mathrm{N}_G(H)$. **הדרכה.** יהיו $x \in \zeta_{n+1}G$ ו־$h \in H$, אז $xhx^{-1} = [x,h]h \in \zeta_n(G)H = H$.

תרגיל 10.3.33 (+)** 1. לכל $N \lhd G$ מתקיים $\zeta_k(G)N/N \leq \zeta_k(G/N)$.

2. $\zeta_n(G/\zeta_k G) = \zeta_{n+k}G/\zeta_k G$.

תרגיל 10.3.34 (**) לכל הומומורפיזם $\varphi : G \to H$, $\varphi(\zeta_n G) \subseteq \zeta_n(H)$.

תרגיל 10.3.35 (-)** $\mathrm{Z}(\mathrm{Inn}(G)) = \Gamma(\zeta_2 G)$. ($\Gamma : G \to \mathrm{Inn}(G)$ הוגדרה בתרגיל 7.2.4.)

תרגיל 10.3.36 (**) נסמן $\mathrm{Inn}^0(G) = G$ ו־$\mathrm{Inn}^{n+1}(G) = \mathrm{Inn}(\mathrm{Inn}^n(G))$. הראה ש־$\mathrm{Inn}^n(G) \cong G/\zeta_n G$.

תרגיל 10.3.37 (**) $[G', \zeta_2 G] = 1$. **הדרכה.** תרגיל 4.8.23.

תרגיל 10.3.38 (**) (הלמה של גרון) אם $G' = G$ אז המרכז של $G/\mathrm{Z}(G)$ טריוויאלי. **הדרכה.** תרגיל 10.3.37.

תרגיל 10.3.39 (-*)** הראה ש־$g \in \zeta_n G$ אם ורק אם $[\cdots[[[g,x_1],x_2],x_3],\dots,x_n] = 1$ לכל $x_1,\dots,x_n \in G$.

תרגיל 10.3.40 (-*)** תהי G חבורה כלשהי. האיחוד $\zeta_\infty G = \bigcup_{n=1}^\infty \zeta_n G$ נקרא **העל־מרכז** (hyper-center) של G. הראה ש־$\mathrm{Z}(G/\zeta_\infty G) = 1$.

תרגיל 10.3.41 (+)** לכל תת־חבורה נורמלית $N \lhd G$, אם $N \cap \zeta_1 G = 1$ אז $N \cap \zeta_n G = 1$ לכל n. **הדרכה.** יהי $x \in N \cap \zeta_n G$, ויהי $g \in G$; אז $[g,x] \in N \cap \zeta_n G = 1$, ולכן $x \in \zeta_1 G \cap N = 1$.

את הגדרה 10.3.26 אפשר להכליל:

הגדרה 10.3.42 ***אם*** $N,K \leq G$***, נסמן*** $N^{[K]} = \{x \in G : [x,K] \subseteq N\}$. ***(זהו מעין היפוך של הפעולה*** $N \mapsto [N,K]$***; באופן כללי*** $N^{[K]}$ ***אינה בהכרח תת־חבורה.)***

תרגיל 10.3.43 (**) $[N^{[K]},K] \subseteq N$.

תרגיל 10.3.44 (**) אם $N \lhd G$ אז $N^{[K]} \leq G$.

תרגיל 10.3.45 (**) אם $K \subseteq H \leq G$, $K \lhd G$, אז $\mathrm{C}_{G/K}(H/K) = K^{[H]}/K$.

10.3.3 חבורות נילפוטנטיות

הגדרה 10.3.46 *חבורה G היא **נילפוטנטית** אם יש סדרה מרכזית המחברת את G ל־1:*

$$1 = G_0 \leq G_1 \leq \cdots \leq G_{n-1} \leq G_n = G$$

האורך המינימלי של סדרה מרכזית כזו נקרא **מחלקת הנילפוטנטיות** של החבורה. כך, רק החבורה הטריוויאלית היא נילפוטנטית ממחלקה 0, והחבורות הנילפוטנטיות ממחלקה 1 הן החבורות האבליות. חבורה היא נילפוטנטית ממחלקה לכל היותר 2 אם $G/\mathrm{Z}(G)$ אבלית.

תרגיל 10.3.47 (*) לחבורה נילפוטנטית יש מרכז לא טריוויאלי.

תרגיל 10.3.48 (**) מכפלה ישרה סופית של חבורות נילפוטנטיות היא נילפוטנטית.

תרגיל 10.3.49 (**) חבורות־p הן נילפוטנטיות.

משפט 10.3.50 *1. לכל סדרה מרכזית $G = H_0 \geq H_1 \geq \cdots$ מתקיים $G_{(i+1)} \leq H_i$ לכל i.*

2. לכל סדרה מרכזית $1 = H_0 \leq H_1 \leq \cdots$ של חבורה G מתקיים $H_i \leq \zeta_i G$ לכל i.

3. תהי $1 = H_0 \leq \cdots \leq H_n = G$ סדרה מרכזית באורך n של חבורה (נילפוטנטית) G. אז לכל i מתקיים $G_{(n+1-i)} \leq H_i \leq \zeta_i G$, ובפרט $G_{(n+1)} = 1$ ו־$\zeta_n G = G$.

הוכחה. 1. $G_{(1)} = H_0 = G$ לפי ההגדרה, ואם $G_{(i+1)} \leq H_i$ אז $G_{(i+2)} = [G_{i+1}, G] \leq [H_i, G] \leq H_{i+1}$ לפי תרגיל 10.3.5.

2. לפי ההגדרה $H_0 = \zeta_0 G = 1$. נניח ש־$H_i \leq \zeta_i G$. מכיוון שהסדרה הנתונה היא מרכזית, $[H_{i+1}, G] \subseteq H_i \subseteq \zeta_i G$; לפי תרגיל 10.3.31, $H_{i+1} \leq \zeta_{i+1} G$.

3. מיידי.

□

תרגיל 10.3.51 (**) G נילפוטנטית אם ורק אם הסדרה המרכזית היורדת מסתיימת ב־1, אם ורק אם הסדרה המרכזית העולה מסתיימת ב־G.

תרגיל 10.3.52 (**) החבורה הדיהדרלית D_n נילפוטנטית אם ורק אם $n = 2^m$.

תרגיל 10.3.53 (*-)** כל חבורה נילפוטנטית חסרת פיתול ניתנת לסידור. (ראה הגדרה 9.5.32)

תרגיל 10.3.54 (**) תהי G נילפוטנטית. לכל תת־חבורה אמיתית H, $H \subset \mathrm{N}_G(H)$. הדרכה. קח n מקסימלי כך ש־$\zeta_n G \subseteq H$, אז לפי תרגיל 10.3.32, $\zeta_{n+1} G \subseteq \mathrm{N}_G(H)$, והרי $\zeta_{n+1} G \not\subseteq H$. הוכחה נוספת: נניח שלא. $H \triangleleft H \cdot \mathrm{Z}(G)$, ולכן $\mathrm{Z}(G) \subseteq H$. עבור למנה $G/\mathrm{Z}(G)$.

תרגיל 10.3.55 (**) בחבורה נילפוטנטית כל תת־חבורה מקסימלית היא נורמלית. הדרכה. לפי תרגיל 10.3.54; השווה לתרגיל 8.3.10.

לסיכום:

משפט 10.3.56 *התנאים הבאים שקולים עבור חבורה סופית G:*

1. G נילפוטנטית;

2. *לכל תת־חבורה אמיתית H מתקיים $H \subset \mathrm{N}_G(H)$;*

3. *כל תת־חבורה מקסימלית היא נורמלית;*

4. *כל תת־חבורת סילו היא נורמלית;*

5. *החבורה היא מכפלה ישרה של חבורות p.*

הוכחה. (1)$\Longleftarrow$(2): תרגיל 10.3.54; (2)$\Longleftarrow$(3): לפי ההנחה $G = \mathrm{N}_G(M) \supset M$; (3)$\Longleftarrow$(4): אחרת יש תת־חבורה מקסימלית M המכילה את $\mathrm{N}_G(P)$, אבל אז $\mathrm{N}_G(M) = M$ לפי תרגיל 8.4.26, בעוד ש־$M \lhd G$ לפי ההנחה; (4)$\Longleftarrow$(5): תרגיל 8.4.35; (5)$\Longleftarrow$(1): תרגילים 10.3.48 ו־10.3.49. $\square$

תרגיל 10.3.57 (**) האוסף $\mathfrak{Nil}$ של החבורות הנילפוטנטיות סגור לתת־חבורות, לחבורות מנה ולהרחבות מרכזיות (ראה הגדרה 4.9.1; השווה לתרגיל 10.2.27.)

תרגיל 10.3.58 (***) $\mathfrak{Nil}$ אינו סגור לאיחוד של שרשראות. **הדרכה.** המחלקה אינה חסומה.

תרגיל 10.3.59 (**) האוסף $\mathfrak{Nil}_n$ של החבורות הנילפוטנטיות ממחלקה לכל היותר n סגור לתת־חבורות, לחבורות מנה ולאיחוד שרשראות, אבל לא להרחבות מרכזיות.

תרגיל 10.3.60 (***) תת־חבורת פרטיני F של כל חבורה סופית G היא נילפוטנטית. **הדרכה.** (ראה הגדרה 10.2.43.) תהי $P \leq F$ תת־חבורת p־סילו של F. לפי טיעון פרטיני 8.4.55, $G = F \cdot \mathrm{N}_G(P)$. לפי תרגיל 10.2.45, $G = \mathrm{N}_G(P)$ ולכן $P \lhd G$ ובפרט $P \lhd F$.

תרגיל 10.3.61 (***) 1. לכל חבורה סופית G יש תת־חבורה נורמלית נילפוטנטית מקסימלית, $\mathrm{Fit}(G)$, הקרויה **תת־חבורת פיטינג** של G. **הדרכה.** תרגיל 4.9.10 (ותרגיל 10.3.59).

2. הראה ש־$\mathrm{Fit}(G/\mathrm{Fit}(G)) = 1$, כלומר, ל־$G/\mathrm{Fit}(G)$ אין תת־חבורות נורמליות נילפוטנטיות.

תרגיל 10.3.62 (***) חבורת פיטינג של חבורה פתירה אינה טריוויאלית. **הדרכה.** תרגיל 10.2.31.

תרגיל 10.3.63 (-***) תהי G חבורה סופית, אז $\mathrm{Fit}(G) = \prod O_p$ עבור הראשוניים p המחלקים את $|G|$, כאשר $O_p = \bigcap \{P \in \mathrm{Syl}_p(G)\}$. **הדרכה.** לכל p, O_p נורמלית כי היא שווה לליבה של כל תת־חבורת p־סילו, ונילפוטנטית כי היא חבורת p. מאידך, אם $Q \in \mathrm{Syl}_p(\mathrm{Fit}(G))$ אז יש $P \in \mathrm{Syl}_p(G)$ כך ש־$Q \subseteq P$, ואז $Q \subseteq \mathrm{Core}_G(P)$ כי $Q \lhd G$.

תרגיל 10.3.64 (***) 1. לכל חבורה סופית G יש תת־חבורה נורמלית פתירה מקסימלית, $\mathrm{rad}(G)$. תת־חבורה זו קרויה **הרדיקל** של G. **הדרכה.** תרגיל 4.9.10 (בעזרת תרגיל 4.9.5 ותרגיל 10.2.27).

2. הראה ש־$\mathrm{rad}(G/\mathrm{rad}(G)) = 1$, כלומר, ל־$G/\mathrm{rad}(G)$ אין תת־חבורות נורמליות פתירות.

תרגיל 10.3.65 (**) $\mathrm{Fit}(G) \subseteq \mathrm{rad}(G)$ לכל חבורה סופית G.