TEL AVIV UNIVERSITY אוניברסיטת תל-אביב
RAYMOND AND BEVERLY SACKLER FACULTY OF EXACT SCIENCES
SCHOOL OF MATHEMATICAL SCIENCES
הפקולטה למדעים מדויקים ע"ש ריימונד ובברלי סאקלר
בית הספר למדעי המתמטיקה

אלגברה ב' 1

מערכי שעור

תשע"ז

נערך על ידי

דן הרן

תוכן העניינים

ספרות מומלצת ii
1. מבנים אלגבריים ופעולות 1
2. משחק המחשבת 5
3. חוגים, שדות 7
4. פריקות בחוג השלמים 10
5. מבנים חלקיים. תת חבורות 13
6. סדר של איבר בחבורה 16
7. תת חבורות נורמליות 20
8. אוטומורפיזמים 26
9. חבורות תמורות 29
10. מכפלות ישרות 33
11. סדרות נורמליות 37
12. חבורות p- 40
13. חבורות סילוב (Sylow) 42
14. החבורות חילופית (חפשיות) נוצרות סופית 47
15. מבנה של חבורות חילופית נוצרות סופית 52
16. חבורות (חילופיות) חופשיות 56
17. חבורות חופשיות 59
18. חבורות נילפוטנטיות 63
19. מכפלות ישרות למחצה 66
20. תרגילים 70
דוגמה של מבחן 80
דוגמה של מבחן עם פתרון 81
משחק המחשבת – פתרון 84

ספרות מומלצת

ככלל מספיק להעזר בסיכומי ההרצאות שילכו ויתפרסמו בהמשך לדף זה. אך מומלץ להציץ גם בספרים:

- D.J.S. Robinson, *A Course in the Theory of Groups*, Springer-Verlag
- J.J. Rotman, *Introduction to the Theory of Groups*, Springer
- *מבנים אלגבריים* של האוניברסיטה הפתוחה.

1. מבנים אלגבריים ופעולות.

הגדרה (לא פורמלית) 1.1: **מבנה אלגברי** הוא מערכת הבנויה משלושה רכיבים:

(א) קבוצה לא ריקה,

(ב) פעולות,

(ג) חוקים שהפעולות מקיימות.

דוגמה 1.2: $\mathbb{R}$ (מספרים ממשיים), עם

פעולת החיבור ופעולת הכפל,

וחוקים: חילופיות של החיבור ושל הכפל, חוק הפילוג, ועוד.

אנו נדון רק במבנים עם פעולות בינאריות (אחת או שתים לכל היותר):

הגדרה 1.3: **פעולה בינארית** על קבוצה S היא העתקה $\pi\colon S\times S\to S$. למשל פעולת החיבור על $\mathbb{R}$ היא ההעתקה $(a,b)\mapsto a+b$ המוגדרת על ידי $\mathbb{R}\times\mathbb{R}\to\mathbb{R}$. **סימון פעולה:** אם π היא פעולה על S, בד"כ במקום $\pi(a,b)=c$ רושמים $a\pi b=c$, כאשר במקום אותיות כגון π בוחרים בסימנים כגון $+,\cdot,\circ$, או אפילו - וכך נעשה בד"כ - בלי סימן, כגון הרישום $ab=c$ בכפל ב-$\mathbb{R}$.

הגדרה 1.4: חוקים. יש הרבה חוקים אפשריים. נדון בחשובים שבהם, שיש להם הרבה ישומים: תהי S קבוצה לא ריקה עם פעולה בינארית (בלי סימן).

חוק החילוף (קומוטטיביות): אם מתקיים $ab=ba$ לכל $a,b\in S$.

חוק הצירוף (אסוציאטיביות): אם מתקיים $(ab)c=a(bc)$ לכל $a,b,c\in S$.

דוגמה 1.5: תהי X קבוצה, ונגדיר פעולה בינארית $\circ$ על הקבוצה $\{f\colon X\to X\}$ על ידי $(f\circ g)(x)=f(g(x))$. פעולה זו (הרכבה) בד"כ אינה חלופית (בדוק!), אך היא אסוציאטיבית:

$$\big((f\circ g)\circ h\big)(x)=(f\circ g)\big(h(x)\big)=f\big(g(h(x))\big),$$
$$\big(f\circ(g\circ h)\big)(x)=f\big((g\circ h)(x)\big)=f\big(g(h(x))\big).$$

טענה 1.5: *אם על S פעולה אסוציאטיבית $\circ$, אז מתקיים על S*

חוק הצירוף המורחב: *יהי $n\geq 2$, $a_1,a_2,\ldots,a_n\in S$, אז סדר בצוע הפעולות בחישוב הביטוי $a_1\circ a_2\circ\cdots\circ a_n$ אינו משנה את התוצאה. (כלומר - היות והסוגריים בסה"כ מורים על סדר בצוע הפעולות - אפשר לוותר על הסוגריים בביטוי זה).*

הוכחה: עבור $n=2$ זה ברור, כי יש רק פעולה אחת. (מקרה $n=3$ הוא חוק הצירוף הרגיל.) נניח באינדוקציה כי הטענה נכונה לגבי ביטויים עם m גורמים, לכל $m<n$. אם נבצע את הפעולות ב-$a_1\circ a_2\circ\cdots\circ a_n$ באפן כזה שהפעולה האחרונה תהיה זו שסימנה בין a_k לבין a_{k+1} באשר $1\leq k<n$ אז נקבל את התוצאה

$(a_1 \circ a_2 \circ \cdots \circ a_k) \circ (a_{k+1} \circ \cdots \circ a_n)$ (לפי הנחת האינדוקציה אין צורך לכתוב סוגריים נוספים). לכן עלינו להוכיח לכל $1 \leq k, l < n$

$$(a_1 \circ a_2 \circ \cdots \circ a_k) \circ (a_{k+1} \circ \cdots \circ a_n) = (a_1 \circ a_2 \circ \cdot \circ a_l) \circ (a_{l+1} \circ \cdots \circ a_n) \quad (1)$$

בה"כ $k < l$, ונסמן $u = a_1 \circ a_2 \circ \cdots \circ a_k, v = a_{k+1} \circ \cdots \circ a_l, w = a_{l+1} \circ \cdots \circ a_n$. לפי הנחת האינדוקציה, (1) שקול ל־ $u \circ (v \circ w) = u \circ (v \circ w)$, וזה נכון לפי חוק הצירוף הרגיל. ∎

הגדרה 1.6: $e \in S$ נקרא **ניטרלי** (גם: **איבר יחידה**) ביחס לפעולה על S אם $ea = ae = a$ לכל $a \in S$. אם הוא קיים, הוא יחיד: אכן, אם גם e' ניטרלי אז $e = ee' = e'$.

דוגמאות 1.7: 1 ניטרלי ביחס לכפל ב־ $\mathbb{R}$ ($\mathbb{N}$), 0 ניטרלי ביחס לחיבור ב־$\mathbb{R}$ ($\mathbb{Z}$), העתקת הזהות ניטרלית ביחס להרכבה ב־$\{f: X \to X\}$.

הגדרה 1.8: תהי S קבוצה עם פעולה בינארית אסוציאטיבית ועם איבר ניטרלי $e \in S$. איבר $a \in S$ נקרא **הפיך** אם קיים $b \in S$ כך ש־$ab = ba = e$. איבר b כזה הוא יחיד (אם גם $ab' = b'a = e$ אז $b = be = bab' = eb' = b'$) והוא ייקרא **ההופכי** של a ויסומן a^{-1}.

דוגמאות 1.9: כל איבר שונה מ־0 ב־$\mathbb{R}$ הפיך ביחס לכפל ב־$\mathbb{R}$. כל איבר ב־$\mathbb{R}$ הפיך ביחס לחיבור ב־$\mathbb{R}$ וההופכי של a הוא $-a$. פונקציה f ב־$\{f: X \to X\}$ הפיכה אמ"ם היא חח"ע ועל.

הגדרה 1.10: **אגודה** (semigroup) היא קבוצה לא ריקה עם פעולה בינארית אסוציאטיבית.

מונואיד היא אגודה עם איבר ניטרלי. **חבורה** (group) היא מונואיד בו כל איבר הפיך.

כלומר, **חבורה** היא קבוצה לא ריקה עם פעולה בינארית אסוציאטיבית, בה יש איבר ניטרלי וכל איבר הוא הפיך. חבורה נקראת **חילופית** (גם: **אַבֶּלית**) אם הפעולה חילופית.

דוגמאות של חבורות 1.11:

(א) $\{1\}, \{\pm 1\}$ עם פעולת הכפל.

(ב) $\mathbb{Z}$ (הפעולה $+$, האיבר הניטרלי 0, ההופכי של n הוא $-n$). אם G חבורה חלופית עם פעולה שמסומנת $+$ אז האיבר הניטרלי נקרא **איבר האפס** (סימון: 0), וההופכי נקרא **הנגדי** (סימון: $-a$).

(ג) החבורה החיבורית F^+ והחבורה הכפלית $F^\times$ של שדה F, למשל, $F = \mathbb{R}$.

(ד) החבורה החיבורית של $\mathbb{Z}/n\mathbb{Z}$ (של השאריות של שלמים לאחר חילוק ב־n). נפרט בפרק הבא.

(ה) חבורת המטריצות ההפיכות מסדר $n \times n$ מעל $\mathbb{R}$, או - באופן כללי יותר - מעל שדה כלשהו F. תסומן $\mathrm{Gl}_n(F)$.

(ו) **חבורת התמורות** של קבוצה X $\{f: X \to X \mid f$ חח"ע ועל$\}$ $S(X) =$ עם פעולת ההרכבה, כלומר: $(\alpha \circ \beta)(x) = \alpha(\beta(x))$.

(ז) **החבורה הסימטרית** S_n: חבורת התמורות של $\{1, \ldots, n\}$.

סימון של תמורה: $\begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ k_1 & k_2 & k_3 & \cdots & k_n \end{pmatrix}$ - מסמן את התמורה $i \mapsto k_i$. כך, למשל, S_3 היא

$$\left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \right\}.$$

ומתקיים

$$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}.$$

חישוב $(a_1 a_2 \dots a_r)$ –באשר $a_1, \dots, a_r \in \{1, \dots, n\}$ שונים זה מזה –היא התמורה שמעתיקה את a_1 ל־a_2, את a_2 ל־a_3, , . . . , את a_{r-1} ל־a_r, את a_r ל־a_1, ואת כל שאר האיברים לעצמם.

(ח) אם G, H שתי חבורות, אז $G \times H$ עם הפעולה לפי הקואורדינטות $(g_1, h_1)(g_2, h_2) = (g_1 g_2, h_1 h_2)$ היא חבורה. בפרט, $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ נקראת **חבורת קליין**.

הגדרה 1.12: יהיו G, H מבנים אלגבריים. העתקה $\varphi: G \to H$ נקראת **הומומורפיזם** אם היא שומרת את הפעולות המתאימות, כלומר (אם הפעולות הן כפל וחיבור)

$$a, b \in G \text{ לכל} \qquad \varphi(ab) = \varphi(a)\varphi(b)$$
$$a, b \in G \text{ לכל} \qquad \varphi(a + b) = \varphi(a) + \varphi(b)$$

הומומורפיזם $\varphi: G \to H$ נקרא **איזומורפיזם** אם הוא חח"ע ועל.

דוגמה 1.13: $\psi: S_2 \to \{\pm 1\}$ הנתונה על ידי $1 \mapsto +1, (12) \mapsto -1$ היא איזומורפיזם חבורות.

$\psi: S_3 \to \{\pm 1\}$ הנתונה על ידי $1 \mapsto +1$, $(123), (132) \mapsto 1$, ו־ $(12), (23), (31) \mapsto -1$ היא הומומורפיזם חבורות.

תרגיל 1.14 (חוק הצמצום): *תהי G חבורה ויהיו $a, b \in G$. אם $ab = ac$ או $ba = ca$ אז $b = c$.*

הוכחה: הכפל את השוויון הנתון ב־ a^{-1} משמאל (מימין).

למה 1.15: *יהי $\varphi: G \to H$ הומומורפיזם חבורות. אזי*

(א) *$\varphi(e_G) = e_H$, באשר $e_G \in G$, $e_H \in H$ הם איברי היחידה.*

(ב) *$\varphi(g^{-1}) = (\varphi(g))^{-1}$ לכל $g \in G$.*

הוכחה:

(א) $\varphi(e_G) = e_H \varphi(e_G) = \varphi(e_G e_G) = \varphi(e_G)\varphi(e_G)$, ולאחר הצמצום $\varphi(e_G) = e_H$.

(ב) $\varphi(g^{-1})\varphi(g) = \varphi(g^{-1}g) = \varphi(e_G) = e_H$, לכן $\varphi(g^{-1}) = (\varphi(g))^{-1}$.

למה 1.16: *יהי $\varphi: G \to H$ איזומורפיזם של מבנים אלגבריים. אזי ההעתקה ההפוכה $\varphi^{-1}: H \to G$ אף היא איזומורפיזם.*

הוכחה: [נזכיר מתורת הקבוצות: ההעתקה ההפוכה $\varphi^{-1}: H \to G$ של העתקת קבוצות $\varphi: G \to H$ מוגדרת כאשר φ חח"ע ועל, וזאת באפן הבא: $\varphi^{-1}(h)$ הוא האיבר היחיד של G המקיים $\varphi(\varphi^{-1}(h)) = h$. מתקיים: $\varphi \circ \varphi^{-1} = 1_H$, $\varphi^{-1} \circ \varphi = 1_G$, באשר $1_G, 1_H$ הן העתקות הזהות של G, H, בהתאמה.]

$$\varphi\big(\varphi^{-1}(h_1)\varphi^{-1}(h_2)\big) = \varphi(\varphi^{-1}(h_1))\varphi(\varphi^{-1}(h_2)) = h_1h_2 = \varphi\big((\varphi^{-1}(h_1h_2)\big),$$

לכן, בגלל ש־φ חח"ע, $\varphi^{-1}(h_1h_2) = \varphi^{-1}(h_1)\varphi^{-1}(h_2)$. ∎

תרגיל 1.17 (תרגיל אתגר***): *תהי G קבוצה לא ריקה עם פעולה בינארית אסוציאטיבית ונניח שלכל $a \in G$ קיים $a' \in G$ יחיד אשר מקיים $aa'a = a$. הוכח ש־G חבורה.*

הדרכה:

(א) הוכח שיש $e \in G$ כך ש־$ee = e$.

(ב) הוכח שלכל $a \in G$ מתקיים $(a')' = a$.

(ג) הוכח שלכל $a \in G$ יש $b \in G$ כך ש־$(ea)' = b = be$.

(ד) יהי $a \in G$. עבור $b = (ea)'$ הוכח כי $b' = ea$ וגם $b' = a$. הסק כי $ae = a$.

(ה) באופן דומה הוכח ש־$ea = a$ לכל $a \in G$. לכן e יחידה ב־G.

2. משחק המחשבת (שעשעון עם חבורת קליין)

משחק המחשבת (peg solitaire, solitary, חפשו באינטרנט) משוחק על ידי שחקן אחד, בעזרת 32 כלי משחק זהים, על גבי לוח עץ בו יש 33 חורים (ראה התרשים למטה בצד **ימין**). במצב ההתחלתי יש כלי בכל חור (מסומן על ידי עיגול מלא) פרט לחור באמצע (מסומן בתרשים על ידי עיגול ריק).

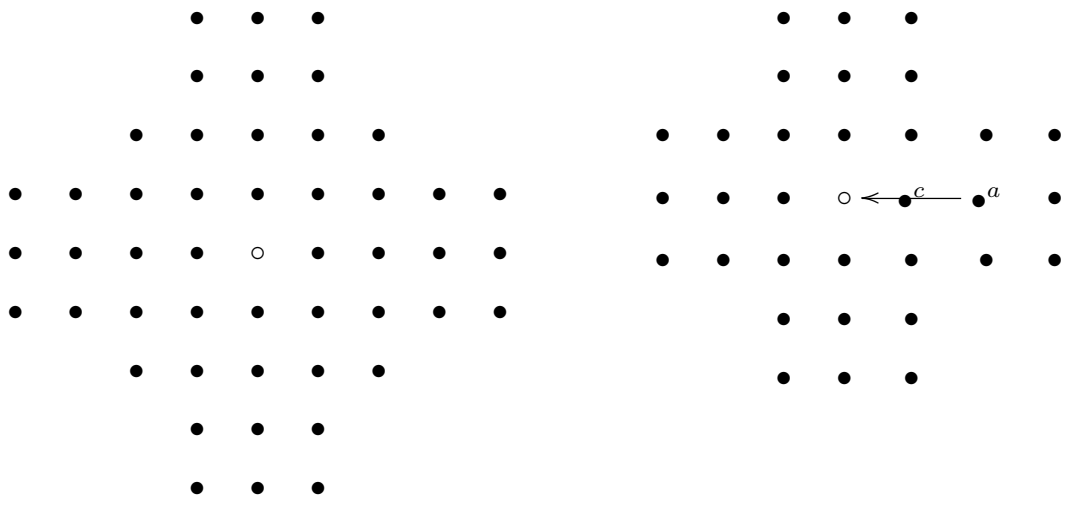
מהלך המשחק: בכל מצב במשחק יכול השחקן להעביר כלי אחד שני חורים ימינה, שמאלה, קדימה או אחורה, בתנאי שהחור החדש פנוי והחור מעליו הכלי עבר — תפוס. מיד לאחר מכן חייב השחקן לסלק מהלוח את הכלי שמעליו הוא עבר. (כך למשל, בהתחלה יכול השחקן להעביר את הכלי המסומן a לחור באמצע ולסלק את הכלי c מהלוח.) בכך קטן מספר הכלים על הלוח ב־1 אחרי כל מהלך.

מטרת המשחק: להגיע לכמה שפחות כלים על הלוח. ציון השחקן הוא, לפי יצרן אחד,

גאון — אם נשאר כלי אחד על גבי הלוח והוא בחור המרכזי,

מצוין — אם נשאר כלי אחד על גבי הלוח, אך לא במרכז,

טוב מאד — אם נשארו שני כלים על גבי הלוח.



המשחק המקורי

הגרסה המשופרת

בשנות השמונים(?) של המאה הקודמת החליט יצרן משחקים מסוים להוציא גרסה חדשה ומתוחכמת יותר של המשחק. היה מדובר באותם הכללים כמו במשחק המקורי, רק שהלוח היה יותר מסובך — ראה התרשים לעיל מצד שמאל.

על החידוש למדתי לראשונה בתכנית הטלויזיה "כלבוטק" (הישנה), שם הופיע אלי אלחדף, מי שהיה אז דוקטורנט (או מסטרנט?) אצלנו והיום הנו פרופסור בטכניון. הוא ניסה להסביר לקהל הצופים מדוע כלל אי אפשר לסיים את המשחק "המשופר" עם כלי אחד, באמצע או לא באמצע!

כיצד הוא הגיע למסקנה זו?

לצורך ההסבר נתבונן בחבורת קליין. זוהי החבורה $K = \{1, a, b, c\}$ מסדר 4 עם לוח הכפל הבא:

$\cdot$	1	a	b	c
1	1	a	b	c
a	a	1	c	b
b	b	c	1	a
c	c	b	a	1

כלומר: K חילופית, $a^2 = b^2 = c^2 = 1$ ומכפלת כל שנים מבין a, b, c נותנת את השלישי. (בדוק ש־K אכן חבורה.)

נסמן את החורים בלוח המשחק באיברי K כדלקמן:

$$
\begin{array}{ccccccccc}
 & & & a & b & c & & & \\
 & & & b & c & a & & & \\
 & & b & c & a & b & c & & \\
a & b & c & a & b & c & a & b & c \\
b & c & a & b & c & a & b & c & a \\
c & a & b & c & a & b & c & a & b \\
 & & c & a & b & c & a & & \\
 & & & b & c & a & & & \\
 & & & c & a & b & & &
\end{array}
$$

(א) מהי המכפלה ב־K של כל החורים התפוסים בתחילת המשחק?

(ב) איך משתנה מכפלה זו אחרי כל מהלך במשחק?

(ג) מהי המכפלה ב־K של כל החורים התפוסים בסוף המשחק?

(ד) מדוע אי אפשר להגיע למצב בו יהיה רק כלי אחד על לוח?

(ה) מביני דבר טוענים שבמשחק *המקורי*, ציונו של מי שסיים עם כלי אחד **שלא** במרכז הלוח צריך להיות "מטומטם" במקום "מצוין". מדוע?

(רמז: היכן בכלל יכול להימצא הכלי האחרון? השתמש גם בסימטריה של הלוח כדי לקבל תשובה מדויקת יותר על שאלה זו.)

פתרון: ראה עמוד 84.

הערה: אחרי שכתבתי פרק זה, נודע לי שידידי פרופ׳ אריה ביאלוסטוצקי כתב מאמר, אשר גם מכיל את הדברים האמורים לעיל (וכנראה עוד פרטים נוספים על משחק המחשבת). ראה

Arie Bialostocki, *An Application of Elementary Group Theory to Central Solitaire*, The College Mathematics Journal **29** (1999), 208–212.

3. חוגים, שדות.

מטרת פרק זה איננה לתת טיפול ממצה בחוגים ושדות, אלא רק מה שנחוץ לנו בשביל ללמוד על חבורות - וקצת מעבר לזה. רוב הדברים (אם לא כולם) בעצם מוכרים מאלגברה לינארית.

הגדרה 3.1: **חוג** הוא קבוצה R עם שתי פעולה בינאריות אסוציאטיביות: חיבור $(+)$ וכפל (בלי סימן), כך ש-R הוא חבורה חלופית ביחס לחיבור ומתקיימים חוקי הפילוג:

$$a,b\in R \text{ לכל } a(b+c)=ab+ac$$

$$.a,b\in R \text{ לכל } (b+c)a=ba+ca$$

חוג נקרא **חילופי** אם הכפל חילופי.

הוא נקרא חוג עם **יחידה** אם יש בו איבר ניטרלי ביחס לכפל.

תחום שלמות הוא חוג חילופי עם יחידה שונה מאפס בו מתקיים: $a\neq 0, b\neq 0 \Leftarrow ab\neq 0$ לכל $a,b\in R$.

שדה F הוא חוג בו $F\setminus\{0\}$ חבורה חלופית ביחס לכפל. כלומר, F חוג חילופי עם יחידה $0\neq 1$, וכל $0\neq a\in F$ הפיך.

הערה 3.2: בכל חוג R מתקים: $a0=0=0a$ לכל $a\in R$.

דוגמאות 3.3: $\mathbb{Z}$ הוא תחום שלמות (בפרט חילופי, עם יחידה);

$\mathbb{Q},\mathbb{R},\mathbb{C}$ הם שדות; כל שדה הוא תחום שלמות;

אסף המטריצות מעל שדה הוא חוג לא חילופי, עם יחידה;

$\mathbb{Q}(\sqrt{2})=\{a+b\sqrt{2}|\ a,b\in\mathbb{Q}\}$ הוא שדה (כי $(a+b\sqrt{2})(a/(a^2-2b^2)-b\sqrt{2}/(a^2-2b^2))=1$);

חוג פולינומים (במשתנה אחד) מעל חוג כלשהו R:

$$R[X]=\left\{f(X)=\sum_{n=0}^{\infty}a_nX^n=a_0+a_1X+a_2X^2+\cdots \;\middle|\; \begin{array}{ll} a_0,a_1,a_2,\ldots\in R & \text{ויש } n \\ a_{n+1}=a_{n+2}=\ldots=0 & \text{כך ש-}\end{array}\right\}.$$

אם $a_n=0$ לכל $n\geq 0$ אז $f(X)$ נקרא **פולינום האפס**.

המעלה של $f(X)=\sum_{n=0}^{\infty}a_nX^n\neq 0$ היא $\deg(f)=\max\{n|\ a_n\neq 0\}$.

חיבור:

$$(a_0+a_1X+a_2X^2+a_3X^3\cdots)+(b_0+b_1X+b_2+X^2+b_3X^3\cdots)=$$
$$(a_0+b_0)+(a_1+b_1)X+(a_2+b_2)X^2+(a_3+b_3)X^3+\cdots$$

כפל:

$$(a_0+a_1X+a_2X^2+a_3X^3\cdots)(b_0+b_1X+b_2+X^2+b_3X^3\cdots)=$$
$$a_0b_0+(a_0b_1+a_1b_0)X+(a_0b_2+a_1b_1+a_2b_0)X^2+(a_0b_3+a_1b_2+a_2b_1+a_3b_0)X^3+\cdots$$

בד"כ כותבים איבר $\sum_{n=0}^{\infty}a_nX^n$ כ-$a_nX_n+\cdots+a_1X+a_0$ אם $a_k=0$ לכל $k>n$.

טענה 3.4: *$R[X]$ הוא חוג והוא מכיל את R. הוא חילופי, אם R חילופי. הוא חוג עם יחידה, אם R חוג עם יחידה. הוא תחום שלמות, אם R תחום שלמות.*

הוכחה: לא נבדוק כאן ש־$R[X]$ חוג ולא נבדוק חילופיות. אם 1 היא היחידה של R, אז $1 = 1+0X+0X^2+\ldots$ היא היחידה של $R[X]$.

נניח כי R תחום שלמות: אם $f(X), g(X) \neq 0$ אז $\deg(fg) = \deg(f) + \deg(g)$, בפרט $fg \neq 0$. לכן גם $R[X]$ תחום שלמות. ∎

דוגמה 3.5: חוג סופי. יהי $n \in \mathbb{N}$. נגדיר יחס שקילות על $\mathbb{Z}$: $a \sim b$ אם $n \big| a-b$. חילוק עם שארית ב־n נותן

$$a = nq_a + r_a, \qquad 0 \leq r_a < n$$

$$b = nq_b + r_b, \qquad 0 \leq r_b < n$$

ובפרט $0 \leq |r_a - r_b| < n$. לכן $r_a = r_b \Leftrightarrow n \big| (r_a - r_b) \Leftrightarrow a \sim b$. נסמן מחלקת השקילות של a ב־$[a]$, ואת קבוצת המנה ב־$\mathbb{Z}/n\mathbb{Z}$. ב־$\mathbb{Z}/n\mathbb{Z}$ יש n איברים: $[0], [1], \ldots, [n-1]$.

היחס $\sim$ שומר על הפעולות על $\mathbb{Z}$: אם $a \sim a', b \sim b'$ אז $ab \sim a'b', a+b \sim a'+b'$. אכן, $ab - a'b' = a(b-b') + (a-a')b'$, $(a+b) - (a'+b') = (a-a') + (b-b')$ ושני הביטויים מתחלקים ב־n. מכאן נובע שאם נגדיר פעולות חיבור וכפל על $\mathbb{Z}/n\mathbb{Z}$ על ידי

$$[a] + [b] = [a+b], \qquad [a][b] = [ab]$$

אז ההגדרה טובה (אינה תלויה במיצגים של מחלקות השקילות).

מזה נקבל בקלות: $\mathbb{Z}/n\mathbb{Z}$ הוא חוג חילופי עם יחידה ($[0]$ האפס, $[1]$ היחידה). נניח מעתה $n \geq 2$.

טענה: *$[k]$ הפיך אם"ם k זר ל־n.*

אכן, $[k]$ הפיך $\Leftrightarrow$ יש $a \in \mathbb{Z}$ כך ש־$[a][k] = [1]$,

$\Leftrightarrow$ יש $a \in \mathbb{Z}$ כך ש־$ak + bn = 1$ עבור איזה $b \in \mathbb{Z}$.

$\Leftrightarrow$ k, n זרים

($\Leftarrow$: אם $d \in \mathbb{N}$ גורם משותף ל־n, k אז $d \big| 1$ ומכאן ש־$d = 1$.

$\Rightarrow$: יוסבר בפרק הבא ש־$\gcd(k,n) = 1$ ולכן יש a, b כאלה.) ∎

מסקנה 3.6: *$\mathbb{Z}/n\mathbb{Z}$ שדה אם"ם $\mathbb{Z}/n\mathbb{Z}$ תחום שלמות אם"ם n ראשוני.*

הוכחה: אם n ראשוני אז:

$$[k] \text{ הפיך } \Leftrightarrow k \text{ זר ל־} n \Rightarrow n \nmid k \Leftrightarrow [k] \neq [0].$$

לכן $\mathbb{Z}/n\mathbb{Z}$ שדה, ובפרט תחום שלמות.

אם n אינו ראשוני אז $n = kl$, באשר $1 < k, l < n$, ואז $[k], [l] \neq [0]$, אך $[k][l] = [n] = [0]$. לכן $\mathbb{Z}/n\mathbb{Z}$ אינו תחום שלמות וודאי לא שדה. ∎

תרגיל 3.7: אם R חוג עם יחידה אז $R^\times = \{r \in R |$ הפיך $r\}$ הוא חבורה (ביחס לכפל ב־R).

(בעיקר יש להראות שהצמצום של הכפל על R ל־$R^\times$ הוא פעולה, כלומר, אם a, b הפיכים אז גם ab הפיך.)

דוגמאות 3.8:

(א) המטריצות ההפיכות מסדר n מעל המרוכבים= $M_n(\mathbb{C})^\times = \mathrm{Gl}_n(\mathbb{C})$.

(ב) $(\mathbb{Z}/n\mathbb{Z})^\times = \{[k] |$ k זר ל־$n\}$.

(ג) אם R תחום שלמות אז $(R[X])^\times = R^\times$.

הגדרנו הומומורפיזם (של מבנים אלגבריים ובפרט) של חוגים. נביא דוגמאות אחדות:

דוגמאות 3.9:

(א) $\psi\colon \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ הנתונה על ידי $\psi(k) = [k]$ היא הומומורפיזם חוגים.

(ב) יהי R חוג חילופי עם יחידה, ויהי $u \in R$. לכל $f = a_1 + a_1X + \cdots + a_nX_n \in R[X]$ נגדיר $f(u) = a_1 + a_1u + \cdots + a_nu^n \in R$. קל לראות ש־$(f+g)(u) = f(u) + g(u), (fg)(u) = f(u)g(u)$, כלומר העתקת ההצבה $f \mapsto f(u)$ היא הומומורפיזם חוגים (שומר יחידה) מ־$R[X]$ לתוך R.

(ג) העתקת האפס בין שני חוגים היא הומומורפיזם.

למה 3.10: יהי $\varphi\colon G \to H$ הומומורפיזם חוגים. אזי

(א) $\varphi(0_G) = 0_H$, באשר $0_G \in G, 0_H \in H$ הם איברי האפס.

(ב) $\varphi(-g) = -\varphi(g)$ לכל $g \in G$.

(ג) נניח כי G, H חוגים עם יחידה ו־$\varphi(1_G) = 1_H$. אז $\varphi(g^{-1}) = (\varphi(g))^{-1}$ לכל $g \in G$ הפיך.

הוכחה: הוכחה (א) ו־(ב) נובעים מלמה דומה עבור חבורות, כי φ הומומורפיזם של החבורות החיבוריות של G, H. ל־(ג) אותה ההוכחה כמו ל־(ב). ∎

הערה 3.11: הפילוסופיה מאחורי מושג האיזומורפיזם היא שאם $\varphi\colon G \to H$ איזומורפיזם אז G ו־H הן כאילו אותו המבנה (בשני כתיבים שונים). "כל דבר" שנוכל לומר על G (איבר $g \in G$, קבוצה $A \subseteq G$) יהיה גם נכון עבור H ($\varphi(G) = H$ איבר $\varphi(g) \in H$, קבוצה $\varphi(A) \subseteq H$).

4. פריקות בחוג השלמים.

הגדרה 4.1: יהיו $a_1, a_2, \ldots, a_k \in \mathbb{Z}$. אם $d \in \mathbb{N}$ מקיים

(א) $d \big| a_i$ לכל i;

(ב) אם $d' \in \mathbb{N}$ כך ש־$d' \big| a_i$ לכל i אז $d' \big| d$;

הוא יקרא **המחלק המשותף הגדול ביותר** של $a_1, \ldots, a_k$ ויסומן $d = \gcd(a_1, \ldots, a_k)$.

אם $m \in \mathbb{N}$ מקיים

(א) $a_i \big| m$ לכל i;

(ב) אם $m' \in \mathbb{N}$ כך ש־$a_i \big| m'$ לכל i אז $m \big| m'$;

הוא יקרא **הכפולה המשותפת הקטנה ביותר** של $a_1, \ldots, a_k$ ויסומן $m = \operatorname{lcm}(a_1, \ldots, a_k)$.

טענה 4.2: *אם* $\gcd(a_1, \ldots, a_k)$ (lcm) *קיים, הוא יחיד.*

הוכחה: אם d_1, d_2 מקיימים את התנאים (א), (ב) של הגדרה 4.1, אז $d_1 \big| d_2$ וגם $d_2 \big| d_1$, לכן $d_1 = d_2$. ∎

למה 4.3: *יהיו* $a_1, \ldots, a_k \in \mathbb{Z}$ *לא כולם* 0. *אז* $d = \gcd(a_1, \ldots, a_k)$ *קיים וקיימים* $c_1, \ldots, c_k \in \mathbb{Z}$ *כך ש־*$d = c_1 a_1 + \cdots + c_k a_k$.

הוכחה: נעיר שאם $q \in \mathbb{Z}$ אז $\gcd(a_1, a_2, \ldots, a_k)$ קיים אם ורק אם $\gcd(a_1 - qa_2, a_2, \ldots, a_k)$ קיים ושניהם שווים. אכן, לכל $d' \in \mathbb{Z}$:

$$d' \big| a_1 - qa_2, a_2, \ldots, a_k \Leftrightarrow d' \big| a_1, a_2, \ldots, a_k.$$

שנית, בלי הגבלת הכלליות $a_1, \ldots, a_k \geq 0$. ואפילו $a_1 \geq \cdots \geq a_k \geq 0$.

הלמה ודאי נכונה אם

$$a_1 \neq 0, a_2 = a_3 = \cdots = a_k = 0. \qquad (*)$$

אכן, אז $d = a_1$ ו־$c_1 = 1, c_2 = \cdots = c_k = 0$.

המשך ההוכחה באינדוקציה על $\sum_i a_i$. אם $\sum_i a_i = 1$, מתקיים $(*)$ ולכן הטענה הוכחה. נניח $\sum_i a_i > 1$. בה"כ $a_1, a_2 \neq 0$, אחרת $(*)$. יש $q, r \in \mathbb{Z}$ כך ש־$a_1 = qa_2 + r$ ו־$0 \leq r < a_2$. כיוון ש־$r < a_2 \leq a_1$, לפי הנחת האינדוקציה $d = \gcd(r, a_2, \ldots, a_k)$ קיים ויש $c_1, \ldots, c_k \in \mathbb{Z}$ כך ש־$d = c_1 r + c_2 a_2 + \cdots + c_k a_k$. לפי ההערה $\gcd(a_1, a_2, \ldots, a_k)$ קיים ושווה ל־d. לכן

$$d = c_1(a_1 - qa_2) + c_2 a_2 + \cdots + c_k a_k = c_1 a_1 + (c_2 - c_1 q)a_2 + c_3 a_3 + \cdots + c_k a_k.$$

∎

דוגמה 4.4: $\gcd(54,70)=2$.

הגדרה 4.5: יהי $1\neq p\in\mathbb{N}$.

(א) p **אי פריק** אם אין $a_1,a_2\in\mathbb{N}$ גדולים מ־1 כך ש־$p=a_1a_2$. במילים אחרות: אם $p=a_1a_2$, באשר $a_1,a_2\in\mathbb{N}$, אז $a_1=1$ (כלומר $a_2=p$) או $a_2=1$ (כלומר $a_1=p$).

(ב) p **ראשוני** אם לכל $a,b\in\mathbb{Z}$ עבורם $p\big|ab$ מתקיים $p\big|a$ או $p\big|b$.

למה 4.6: *p אי פריק אם ורק אם p ראשוני.*

הוכחה: יהי p ראשוני. נניח כי $p=a_1a_2$, באשר $a_1,a_2\in\mathbb{N}$. אז $p\big|a_1a_2$, לכן, למשל, $p\big|a_1$. אבל $a_1\big|p$. לכן $a_1=p$. זה מוכיח ש־p אי פריק.

להיפך, יהי p אי פריק. נניח כי $a,b\in\mathbb{Z}$ וכי $p\big|ab$. עלינו להוכיח כי $p\big|a$ או $p\big|b$. בלי הגבלת הכלליות $a,b\in\mathbb{N}$. נוכל להניח כי $p\nmid b$.

יהי $d=\gcd(p,b)$. אז $d\big|p$ אבל $d\neq p$, כי $d\big|b$ ו־$p\nmid b$. כיוון ש־p אי פריק, $d=1$. לכן יש $c_1,c_2\in\mathbb{Z}$ כך ש־$1=pc_1+bc_2$. מכאן $a=apc_1+abc_2$ ו־p מחלק את אגף ימין, לכן $p\big|a$. ∎

משפט 4.7: *לכל $0\neq a\in\mathbb{Z}$ יש הצגה יחידה*

$$a=up_1p_2\cdots p_r$$

באשר $u\in\{\pm1\}$ ו־$p_1\leq p_2\leq\ldots\leq p_r$ ראשוניים (לא בהכרח שונים זה מזה).

הוכחה: בלי הגבלת הכלליות $a\in\mathbb{N}$ ועלינו להוכיח את המשפט עם $u=1$.

קיום ההצגה: ־ באינדוקציה על a: אם $a=1$, ניקח $r=0$.

נניח $a>1$. אם a אי פריק, אז $a=a$ היא הצגה מבוקשת. אם a פריק, אז $a=a_1a_2$, באשר $1<a_1,a_2$, ולכן $a_1,a_2<a$. לפי הנחת האינדוקציה

$$a_1=p_1\cdots p_r\quad,a_2=p_{r+1}\cdots p_s$$

ואז

$$a=p_1\cdots p_r\cdots p_s.$$

סידור מחדש של הגורמים באגף ימין נותן את ההצגה המבוקשת.

יחידות ההצגה: נניח שיש עוד הצגה $a=p'_1\cdots p'_s$, ונראה שהיא זהה לראשונה. בה"כ $r\geq s$, ההוכחה באינדוקציה על r. אם $r=0$ אז $s=0$ ולכן $a=1$. אם $r\geq1$ אז $p_r\big|a$ ולכן יש i כך ש־$p_r\big|p'_i$. כיוון ש־p'_i אי פריק, נובע ש־$p_r=p'_i$, ולכן (צמצום!) $p_1p_2\cdots p_{r-1}=p'_1\cdots p'_{i-1}p'_{i+1}\cdots p'_s$. לפי הנחת האינדוקציה שתי ההצגות האלה שוות, ומכאן המסקנה. ∎

ניסוח שקול: *לכל* $0 \neq a \in \mathbb{Z}$ *הצגה יחידה* $a = u\prod_{p\in\mathbb{N}\text{ אי פריק}} p^{n_p}$, *באשר* u *הפיך,* $n_p \geq 0$ *וכמעט לכל (=פרט למספר סופי)* $p \in \mathbb{N}$ *אי פריקים:* $n_p = 0$.

תרגיל 4.8: *אם* $a, b \in \mathbb{Z}$ *שונים מ־*0,

$$, a = u \prod_{p\in\mathbb{N}\text{ אי פריק}} p^{m_p} \quad , b = v \prod_{p\in\mathbb{N}\text{ אי פריק}} p^{n_p}$$

באשר $u, v \in \{\pm 1\}$, *אז*

(א) $a \mid b$ *אם"ם* $m_p \leq n_p$ *לכל* p.

(ב) $\gcd(a, b) = \prod_{p\in\mathbb{N}\text{ אי פריק}} p^{\min(m_p,n_p)}$.

(ג) $\operatorname{lcm}(a, b) = \prod_{p\in\mathbb{N}\text{ אי פריק}} p^{\max(m_p,n_p)}$.

הוכחה:

(א) $a \mid b \Leftrightarrow$ קיים $c \in \mathbb{Z}$ כך ש־$b = ac$ (בהכרח $c \neq 0$)

$\Leftrightarrow$ קיימים $w \in \{\pm 1\}$ ו־$k_p \geq 0$ (כמעט כולם 0) כך ש־ [$c = w\prod p^{k_p}$ ו־]

$$v\prod p^{n_p} = u\prod p^{m_p} w\prod p^{k_p} = uw\prod p^{m_p+k_p}$$

$\Leftrightarrow$ קיימים $w \in \{\pm 1\}$ ו־$k_p \geq 0$ (כמעט כולם 0) כך ש־$v = uw, n_p = m_p + k_p$

$\Leftrightarrow m_p \leq n_p$ לכל p. ∎

תרגיל 4.9: *יהיו* $a, b, c \in \mathbb{Z}$ *שונים מאפס. נניח כי* a, b *זרים (כלומר* $\gcd(a, b) = 1$*). הוכח: אם* $a \mid bc$ *אז* $a \mid c$.

הוכחה: לפי למה 4.3, יש $m, n \in \mathbb{Z}$ כך ש־$1 = ma + nb$. מכאן $c = mac + nbc$. אם a מחלק את bc אז a מחלק את אגף ימין של משוואה זו, ולכן גם את c. ∎

5. מבנים חלקיים. תת חבורות

אם $\pi: G \times G \to G$ פעולה בינארית על קבוצה G ו־$H \subseteq G$, נאמר שהצמצום של π ל־H היא פעולה בינארית על H אם $\pi(g_1, g_2) \in H$ לכל $g_1, g_2 \in H$.

הגדרה 5.1: קבוצה חלקית H של מבנה אלגברי G (חבורה, חוג, שדה,...) תקרא מבנה (חבורה, חוג, שדה,...) **חלקי** או **תת מבנה** אם הצמצומים של הפעולות על G ל־H הן פעולות בינאריות על H ו־H מבנה (חבורה, חוג, שדה,...) ביחס לפעולות על G. נסמן $H \leq G$; הסימון $H < G$ פירושו $H \leq G$ וגם $H \neq G$.

למה 5.2: *קבוצה חלקית H של חבורה G היא חבורה חלקית אם ורק אם*

(א) $H \neq \emptyset$ *או: (א')* $1_G \in H$,

(ב) H *סגורה תחת הפעולה על* G: $a, b \in H \Rightarrow ab \in H$,

(ג) $a \in H \Rightarrow a^{-1} \in H$.

הוכחה: הכרחיות: (א), (ב) - ברור. (א'): מתקיים $1_H 1_H = 1_H = 1_G 1_H$, לכן (צמצום ב־G) $1_H = 1_G$.

(ג) ההפכי $b \in H$ של a ב־H הוא גם ההפכי של a ב־G. מהיחידות ההפכי ב־G יוצא $b = a^{-1}$. לכן $a^{-1} \in H$.

מספיקות: לפי (ב) הצמצום של הפעולה ל־H מגדיר פעולה בינארית על H. היא ודאי אסוציאטיבית. לפי (א) יש $a \in H$; לפי (ג) $a^{-1} \in H$; לפי (ב) $1_G = aa^{-1} \in H$; זהו ודאי איבר ניטרלי ביחס לכפל על H. לפי (ג) יש לכל $a \in H$ הפכי ביחס ל־1_G.

מסקנה 5.3: *אם $H \leq G$ חבורות אז $1_H = 1_G$. (אם $H \leq G$ חוגים או שדות אז $0_H = 0_G$.)*

הוכחה: 1_G היא יחידה ב־H. לפי יחידות היחידה, $1_G = 1_H$. ∎

דוגמאות 5.4:

(א) $A_3 = \{(1), (123), (132)\} < S_3$.

(ב) לכל חבורה G מתקים: $\{1_G\} \leq G$.

(ג) $\mathbb{Q} < \mathbb{R} < \mathbb{C}$ (חבורות ביחס לחיבור).

(ד) אם R חוג קומוטטיבי עם יחידה, אז $R \leq R[X]$ (כלומר, $R \cong R_0, R_0 = \{f | \deg f = 0\} \leq R$).

למה 5.5: *אם $\{H_i | i \in I\}$ משפחת חבורות חלקיות של חבורה G אז גם $\bigcap_{i \in I} H_i$ חבורה חלקית.*

סימון: אם G חבורה ו־$A, B \subseteq G, g \in G$ נסמן:

$$AB = \{ab | a \in A, b \in B\},$$
$$Ag = \{ag | \in A\} = A\{g\}, gA = \{ga | \in A\} = \{g\}A,$$
$$A^{-1} = \{a^{-1} | a \in A\}.$$

תרגיל 5.6: תהי G חבורה ויהיו $A, B, C \subseteq G, a, b, g \in G$. יהי e איבר היחידה של G.

(א) $(AB)C = A(BC)$. בפרט, $(ab)C = a(bC)$.

(ב) $eA = A = Ae$.

(ג) $A = B \Leftrightarrow Ag = Bg$

(ד) $A = B \Leftrightarrow gA = gB$.

(ה) $(AB)^{-1} = B^{-1}A^{-1}$.

(ו) $|Ag| = |A| = |gA|$ (כלומר, הקבוצות שוות עוצמה).

(ז) אם $H \leq G$ אז $H^{-1} = H, HH = H$ ו־$hH = Hh = H$ לכל $h \in H$.

(ח) אם $H \leq G$ אז $g^{-1}Hg = \{g^{-1}hg | \ \in H\} \leq G$.

הגדרה 5.7: תהי H חבורה חלקית של חבורה G. קבוצה מהצורה gH (Hg), באשר $g \in G$ תיקרא **מחלקה שמאלית** (**ימנית**) של H ב־G. אסף המחלקות השמאליות $\{gH | \ g \in G\}$ יסומן G/H. נשים לב ש־$g \in gH$, כי $g = ge$.

למה 5.8: *תהי $H \leq G$ ויהיו $g_1, g_2 \in G$. התנאים הבאים שקולים:*

(א) $g_1H = g_2H$.

(ב) $g_1H \subseteq g_2H$.

(ג) $g_1H \cap g_2H \neq \emptyset$.

(ד) $g_1 \in g_2H$.

(ה) $g_2^{-1}g_1 \in H$.

הוכחה: (ו) (א) $\Leftarrow$ (ב) $\Leftarrow$ (ד) $\Leftarrow$ (ג) ברור (כי $g_1 \in g_1H$). (ה) $\Leftrightarrow$ (ד) ברור.

(ג) $\Leftarrow$ (א): בגלל הסימטריה די להראות (ג) $\Leftarrow$ (ב). אז יש $h_1, h_2 \in H$ כך ש־$g_1h_1 = g_2h_2$. לכל $h \in H$ מתקיים $g_1h = g_1h_1h_1^{-1}h = g_2h_2h_1^{-1}h \in g_2H$. לכן $g_1H \subseteq g_2H$. ∎

הערה 5.9: על G יש יחס שקילות: $g_1 \sim g_2$ אם ורק אם יש $h \in H$ כך ש־$g_1 = g_2h$, כלומר, מתקיימים התנאים השקולים של למה 5.8. המחלקות השמאליות הן בדיוק מחלקות השקילות של יחס זה.

מסקנה 5.10: *תהי $H \leq G$. אזי G היא אחוד זר של המחלקות השמאליות שלה. כלומר, $G = \dot{\bigcup}_{g \in R} gH$ (איחוד זר), באשר $R \subseteq G$ כך ש־R מכילה בדיוק איבר אחד מכל מחלקה שמאלית של G ב־H (R נקראת **מערכת מיצגים של** G **מודולו** H).*

הגדרה 5.11: תהי G חבורה ותהי $H \leq G$.

(א) **הסדר של** G הוא העוצמה $|G|$,

(ב) **האינדקס** $(G : H)$ של H ב־G הוא העוצמה $|G/H|$. ברור ש־$(G : H) = |R|$, באשר R מערכת מיצגים של G מודולו H.

משפט 5.12 (לגרנז'): *תהי G חבורה ותהי $H \leq G$. אז $|G| = (G : H) \cdot |H|$.*

הוכחה: תהי R מערכת מיצגים של G מודולו H. נגדיר $\varphi : R \times H \to G$ על ידי $\varphi(r, h) = rh$. אזי חח"ע: אם $\varphi(r_1, h_1) = \varphi(r_2, h_2)$, כלומר $r_1h_1 = r_2h_2$, אז $r_1H = r_2H$ ולכן $r_1 = r_2$ ומכאן $h_1 = h_2$. כמו כן φ על, כי $G = \bigcup_{g \in R} gH$. לכן $|G| = |R \times H| = |R| \times |H|$. ∎

מסקנה 5.13: *אם G חבורה סופית, $H \leq G$, אז $|H|, (G : H)$ מחלקים את $|G|$.*

הגדרה 5.14: תהי G חבורה ותהי $M \subseteq G$. נסמן ב־$\langle M \rangle$ את חיתוך כל החבורות החלקיות של G שמכילות את M.

אם $G = \langle M \rangle$ נאמר כי M היא מערכת יוצרים של G וגם ש־M **יוצרת** את G.

סימון 5.15: $\langle a, b, \ldots \rangle = \langle \{a, b, \ldots\} \rangle, \langle M, N \rangle = \langle M \cup N \rangle$.

למה 5.16: *תהי G חבורה ותהי $M \subseteq G$.*

(א) $\langle M \rangle$ *היא החבורה החלקית הקטנה ביותר של G המכילה את M, כלומר: $M \subseteq \langle M \rangle \leq G$ ואם $M \subseteq H \leq G$ אז $\langle M \rangle \leq H$. (חבורה חלקית כזו היא יחידה; לפי כך (א) הגדרה שקולה של $\langle M \rangle$.)*

(ב) $\langle M \rangle = \{x_1 x_2 \cdots x_n | \ x_1, x_2, \ldots, x_n \in M \cup M^{-1}, n \geq 0\}$. *(המכפלה הריקה היא איבר היחידה.)*

דוגמה 5.17: $\mathbb{Z} = \langle 1 \rangle$.

6. סדר של איבר בחבורה. חבורות מעגליות.

חזקות.

יהי G מבנה עם פעולת כפל אסוציאטיבית ואיבר ניטרלי $e \in G$. לכל $a \in G$ נגדיר

$a^0 = e$ [בכתיב חיבורי: $0a = 0$];

$a^{n+1} = a^n a$ עבור $n \in \mathbb{N}$ [$(n+1)a = na + a$];

$a^{-n} = (a^{-1})^n$ עבור $n \in \mathbb{N}$ [$(-n)a = n(-a)$] אם a גם הפיך:

טענה 6.1: *לכל $i, j \in \mathbb{N} \cup \{0\}$ (לכל $i, j \in \mathbb{Z}$ - אם a הפיך)*

(א) $a^i a^j = a^{i+j}$ *[$ia + ja = (i+j)a$]*

(ב) $(a^i)^j = a^{ij}$ *[$j(ia) = (ji)a$]*

(ג) *הכלל $a^i b^i = (ab)^i$ אינו בהכרח נכון, אך הוא נכון אם $ab = ba$.*

הוכחה: אם $i, j \geq 0$ אז (א), (ב) נובעות מכלל הצירוף המוכלל, ו־(ג) באינדוקציה. המקרה הכללי (עבור a הפיך) נובע מהמקרה הפרטי לפי הכלל $a^{-n} = (a^{-1})^n$. למשל, נראה (ב) עבור $i < 0, j > 0$:

$a^{ij} = (a^{-1})^{-ij}$ ואילו $(a^i)^j = ((a^{-1})^{-i})^j = (a^{-1})^{(-i)j} = (a^{-1})^{-ij}$. ∎

אם G חבורה ו־$g \in G$ אז $\langle g \rangle = \{g^i \mid i \in \mathbb{Z}\}$ (=החבורה החלקית הקטנה ביותר של G המכילה את g).

הגדרה 6.2: חבורה G נקראת **מעגלית** (**ציקלית**) אם יש $g \in G$ כך ש־$G = \langle g \rangle$.

דוגמה 6.3: $\mathbb{Z}, \mathbb{Z}/n\mathbb{Z}$ - ביחס לחיבור - מעגליות (נוצרות על ידי 1, $[1]$).

אם G חבורה ו־$g \in G$ אז $\langle g \rangle$ תת חבורה מעגלית של G.

הגדרה 6.4: תהי G חבורה ויהי $g \in G$. המספר הטבעי הקטן ביותר n עבורו $g^n = e$ נקרא **הסדר** של g ויסומן $\operatorname{ord} g$. אם $g^n \neq e$ לכל n טבעי, נסמן $\operatorname{ord} g = \infty$. (נשים לב: $g = e \Leftrightarrow \operatorname{ord} g = 1$.)

למה 6.5: *תהי G חבורה ויהי $g \in G$ בעל סדר סופי n. אזי*

(א) *לכל m שלם: $n \mid m \Leftrightarrow g^m = e$.*

(ב) $\langle g \rangle = \{e = g^0, g, g^2, \ldots, g^{n-1}\}$.

(ג) $|\langle g \rangle| = n$, *כלומר,* $|\langle g \rangle| = \operatorname{ord} g$

(ד) *אם k הוא מספר שלם אז* $\operatorname{ord} g^k = n/\gcd(n,k)$. *בפרט*

(ד1) $\operatorname{ord} g^k = n/k \Leftrightarrow k \mid n$;

(ד2) $\operatorname{ord} g^k = n \Leftrightarrow k$ *זר ל־*n.

הוכחה: יהי m שלם. חילוקו ב־n עם שארית נותן

$$m = nq + r \qquad , q, r \in \mathbb{Z}, 0 \leq r < n.$$

אז

$$g^m = (g^n)^q g^r = e^q g^r = g^r, \tag{3}$$

ולכן:

(א) $g^m = e \Leftrightarrow$ (בגלל המינימליות של n) $r = 0 \Leftrightarrow n \mid m$.

(ב) צ"ל: $\{g^m \mid m \in \mathbb{Z}\} = \{g^r \mid 0 \le r < n\}$. ההכלה $\subseteq$ נובעת מ־(3). ההכלה ההפוכה טריוויאלית.

(ג) יהיו $0 \le m_1 \le m_2 < n$. אזי

$$g_1^{m_1} = g^{m_2} \Leftrightarrow g^{m_2 - m_1} = e \Leftrightarrow n \mid (m_2 - m_1) \text{ (לפי (א))} \Leftrightarrow m_2 - m_1 = 0 \Leftrightarrow m_2 = m_1.$$

לכן $e = g^0, g, g^2, \ldots, g^{n-1}$ שונים זה מזה.

(ד) יהי $d = \gcd(n,k)$ ויהי m שלם. אז לפי (א) $(n/d) \mid m \Leftrightarrow (n/d) \mid (k/d)m \Leftrightarrow n \mid km \Leftrightarrow (g^k)^m = e$ (כי $(n/d), (k/d)$ זרים - ראה תרגיל 4.9). לכן m הטבעי הקטן ביותר שמקיים $(g^k)^m = e$ הוא m הטבעי הקטן ביותר שמקיים $(n/d) \mid m$, הוא n/d. (למעשה (ד) נובע מ־(ד1), (ד2). יהי $d = \gcd(n,k)$ וכתוב $k = dk_1, n = dn_1$, באשר k_1, n_1 זרים. לפי (ד1) $\operatorname{ord} g^d = n_1$ ולפי (ד2) $\operatorname{ord} (g^d)^{k_1} = n_1$). ∎

למה 6.6: *תהי G חבורה ויהי $g \in G$ בעל סדר אינסופי. אזי*

(א) *לכל m שלם:* $g^m = e \Leftrightarrow m = 0$.

(ב) $\langle g \rangle = \{g^n \mid \ \in \mathbb{Z}\}$.

(ג) $|\langle g \rangle| = \aleph_0$. *ביתר דיוק:* $g^m = g^k \Leftrightarrow m = k$.

(ד) *אם $k \neq 0$ הוא מספר שלם אז* $\operatorname{ord} g^k = \infty$.

הוכחה:

(א) אם $m > 0$, אז לפי ההגדרה של הסדר, $g^m \neq e$. אם $m < 0$, אז לפי המקרה הקודם $g^{-m} \neq e$, ולכן $g^m = (g^{-m})^{-1} \neq e$. לבסוף, $g^0 = e$.

(ב) $\langle g \rangle = \{\overbrace{g^{\pm 1} g^{\pm 1} \cdots g^{\pm 1}}^{k} \mid k \ge 0\} = \{g^n \mid \ \in \mathbb{Z}\}$.

(ג) $m = k \Leftrightarrow m - k = 0 \Leftrightarrow g^{m-k} = e \Leftrightarrow g^m = g^k$.

(ד) יהי $m > 0$. אז $km \neq 0$, לכן, לפי (א), $(g^k)^m = g^{km} \neq e$. ∎

מסקנה 6.7: *(א) תהי G חבורה ויהי $g \in G$ בעל סדר סופי n. אז g^k יוצר את $\langle g \rangle$ אמ"מ k, n זרים. מספר היוצרים של $\langle g \rangle$ הוא איפוא $|(\mathbb{Z}/n\mathbb{Z})^\times|$="מספר הזרים ל־$n$ מבין $\{1, 2, \ldots, n\}$" $= \varphi(n)$ (**פונקצית אוילר**).*

(ב) *סדר של איבר בחבורה סופית מחלק את סדר החבורה.*

הוכחה:

(א) $g^k \in \langle g \rangle$, לכן $\langle g^k \rangle \le \langle g \rangle$. לכן $\langle g^k \rangle = \langle g \rangle \Leftrightarrow |\langle g^k \rangle| = |\langle g \rangle| = n \Leftrightarrow \operatorname{ord} g^k = n \Leftrightarrow k, n$ זרים.

(ב) אם G סופית, $g \in G$, אז $|\langle g \rangle| < \infty$, לכן g מסדר סופי. כעת $\operatorname{ord} g = |\langle g \rangle| \,\big|\, |G|$ לפי לגרנז'. ∎

משפט 6.8: *כל חבורה מסדר ראשוני היא מעגלית.*

הוכחה: תהי G מסדר ראשוני. יהי $e \neq g \in G$. אז $1 < \operatorname{ord} g \big| |G|$, לכן $\operatorname{ord} g = |G|$, ומכאן $|\langle g \rangle| = |G|$ ולכן $\langle g \rangle = G$.

משפט 6.9: *תהי $\langle g \rangle$ חבורה מעגלית מסדר סופי n. לכל מחלק d של n קיימת ל־$\langle g \rangle$ בדיוק חבורה חלקית אחת מסדר d, היא $\langle g^{\frac{n}{d}} \rangle$. אלה כל החבורות החלקיות של $\langle g \rangle$, בפרט כולן מעגליות.*

הוכחה: $\langle g^{\frac{n}{d}} \rangle$ אכן מסדר $d = \frac{n}{n/d}$. לפי לגרנז' כל חבורה חלקית של $\langle g \rangle$ היא מסדר שמחלק את n. נותר להראות כי אם $d \big| n$ ו־$H \leq \langle g \rangle$ מסדר d, אז $H = \langle g^{\frac{n}{d}} \rangle$. בגלל שוויון הסדרים די להראות $H \subseteq \langle g^{\frac{n}{d}} \rangle$.

יהי $h \in H$; אז $h = g^m$, באשר $0 \leq m < n$. לפי הלמה הקודמת $\operatorname{ord} h \big| |H|$, כלומר $n/\gcd(n,m) \big| d$, מכאן $n \big| \gcd(n,m) d$, ולכן $\frac{n}{d} \big| \gcd(n,m)$, ובפרט $\frac{n}{d} \big| m$. לכן $\langle g^{\frac{n}{d}} \rangle = \{(g^{\frac{n}{d}})^k | \ k \in \mathbb{Z}\}$. מכאן $h = g^m \in \langle g^{\frac{n}{d}} \rangle$. $H \subseteq \langle g^{\frac{n}{d}} \rangle$. ∎

למה 6.10: *תהי $\langle g \rangle$ חבורה מעגלית מסדר n סופי. אז ההעתקה $\lambda \colon \mathbb{Z}/n\mathbb{Z} \to \langle g \rangle$ הנתונה על ידי $[k] \mapsto g^k$ היא איזומורפיזם.*

הוכחה: (נשים לב ש־$\operatorname{ord} g = n$.) ההעתקה λ מוגדרת היטב והיא חח"ע:

$$g^{k_1} = g^{k_2} \Leftrightarrow g^{k_1 - k_2} = e \Leftrightarrow n \big| k_1 - k_2 \Leftrightarrow [k_1] = [k_2].$$

היא על, כי $\langle g \rangle = \{g^0, g, g^2, \ldots, g^{n-1}\}$. היא הומומרפיזם:

$$\lambda([k_1] + [k_2]) = \lambda([k_1 + k_2]) = g^{k_1 + k_2} = g^{k_1} g^{k_2} = \lambda([k_1])\lambda([k_2]). \quad ∎$$

מסקנה 6.11: *חבורה מסדר ראשוני p הינה איזומורפית ל־$\mathbb{Z}/p\mathbb{Z}$.*

למה 6.12: *תהי $\langle g \rangle$ חבורה מעגלית מסדר אינסופי. אז ההעתקה $\lambda \colon \mathbb{Z} \to \langle g \rangle$ הנתונה על ידי $k \mapsto g^k$ היא איזומורפיזם.*

הוכחה: ההעתקה חח"ע: $g^{k_1} = g^{k_2} \Leftrightarrow k_1 = k_2$. היא על, כי $\langle g \rangle = \{g^k | \ k \in \mathbb{Z}\}$. היא הומומרפיזם: $g^{k_1 + k_2} = g^{k_1} g^{k_2}$. ∎

למה 6.13: *לכל $d \in \mathbb{N}$ קיימת ל־$\mathbb{Z}$ בדיוק חבורה חלקית אחת מאינדקס d, היא $d\mathbb{Z} = \langle d \rangle = \{dk | \ k \in \mathbb{Z}\}$. חבורות אלה הן כל החבורות החלקיות של $\mathbb{Z}$ (פרט ל־$\{0\}$). בפרט כולן מעגליות ואיזומורפיות ל־$\mathbb{Z}$.*

הוכחה: תחלה נראה כי $(\mathbb{Z} : d\mathbb{Z}) = d$, וביתר דיוק, ש־$\{0, 1, \ldots, d-1\}$ היא מערכת מיצגים של $\mathbb{Z}$ מודולו $d\mathbb{Z}$. צ"ל: לכל $k \in \mathbb{Z}$ יש $0 \leq r < d$ שלם יחיד כך ש־k, r באותה מחלקה שמאלית של $d\mathbb{Z}$ כלומר, כך ש־$k - r$ מתחלק ב־d. זה ידוע (חילוק עם שארית ב־d) . תהי $\mathbb{Z} \geq H \neq \{0\}$. יהי $d \in H$ הטבעי הקטן ביותר (יש מספרים טבעיים ב־H: אם $k \in H$ אז גם $-k \in H$). נראה ש־$H = d\mathbb{Z}$. אכן, $d\mathbb{Z} = \langle d \rangle \leq H$. להיפך, אם $k \in H$,

יהיו q, r כך ש־$0 \leq r < d, k = dq + r$. אז $r = k + (-q)d \in H$, לכן לפי המינימליות של d יוצא $r = 0$. מכאן $k = dq \in d\mathbb{Z}$.

לפי למה 6.6(ד), $\operatorname{ord}(d) = \infty$, לכן לפי למה 6.6(ג), $d\mathbb{Z} = \langle d \rangle$ אינסופית. לפי למה 6.12, $d\mathbb{Z}$ איזומורפית ל־$\mathbb{Z}$. ∎

תרגיל 6.14: *כל חבורה מסדר 4 הנה איזומורפית ל־$\mathbb{Z}/4\mathbb{Z}$ או לחבורת קליין $(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$.*

7. תת חבורות נורמליות. משפטי איזומורפיזם.

הגדרה 7.1: הומומורפיזם $\theta: G \to H$ נקרא

(א) **אִיזוֹמורפיזם** אם הוא חח"ע ועל;

(ב) **אֶפִימורפיזם** אם הוא על;

(ג) **מונומורפיזם** אם הוא חח"ע;

(ד) **אֶנדוֹמורפיזם** אם $H = G$;

(ה) **אוטומורפיזם** אם הוא חח"ע ועל ו־$H = G$.

תהי G חבורה. עבור $a, g \in G$ נסמן $g^a = a^{-1}ga$. אם $M \subseteq G$, נסמן $M^a = \{g^a | \ g \in M\} = a^{-1}Ma$.

טענה 7.2: *לכל* $a, b, g, h \in G$

(א) $(gh)^a = g^a h^a$

(ב) $g^{ab} = (g^a)^b$

(ג) $(g^a)^{-1} = (g^{-1})^a$.

(ד) $e^a = e, g^e = g$

מסקנה 7.3: *ההעתקה* $g \mapsto g^a$ *היא אוטומורפיזם של* G *(ההפכי שלו הוא* $g \mapsto g^{a^{-1}}$*). נקראת* **ההצמדה ב־**a.

הגדרה 7.4: תהי G חבורה. $g, h \in G$ נקראים **צמודים** אם יש $a \in G$ כך ש־$h = g^a$.

יחס הצמידות הוא יחס שקילות. לפי תרגיל 5.6(ח), אם $H \leq G$ אז $H^a \leq G$ לכל $a \in G$.

למה 7.5: *תהיינה* $N \leq G$ *חבורות ותהי* $S \subseteq N$ *כך ש־* $N = \langle S \rangle$*. התנאים הבאים שקולים:*

(א) $Ng = gN$ *לכל* $g \in G$.

(ב) $N^g = N$ *לכל* $g \in G$.

(ג) $N^g \subseteq N$ *לכל* $g \in G$ *(כלומר,* $g^{-1}ng \in N$ *לכל* $g \in G$, $n \in N$*).*

(ד) $S^g \subseteq N$ *לכל* $g \in G$.

הוכחה:

(א) $\Leftarrow$ (ב) ע"י הכפלה משמאל ב־g^{-1}; (ב) $\Leftarrow$ (א) ע"י הכפלה משמאל ב־g.

(ב) $\Leftarrow$ (ג) $\Leftarrow$ (ד) טריוויאלי.

(ג) $\Leftarrow$ (ב): נתון גם $N^{g^{-1}} \subseteq N$, ומכאן $N = (N^{g^{-1}})^g \subseteq N^g$.

(ד) $\Leftarrow$ (ג): $S = (S^g)^{g^{-1}} \subseteq N^{g^{-1}}$, לכן $N \subseteq N^{g^{-1}}$, ומכאן $N^g \subseteq N$.

הגדרה 7.6: $N \leq G$ נקראת **נורמלית** ב־G אם היא מקיימת את תנאי הלמה. סימון: $N \triangleleft G$.

דוגמה 7.7: אם G חילופית אז כל $H \leq G$ נורמלית. $\mathrm{SL}_n(\mathbb{C}) \triangleleft \mathrm{GL}_n(\mathbb{C})$, $\langle (123) \rangle = A_3 \triangleleft S_3$.

למה 7.8: *אם $\{N_i\}_{i\in I}$ נורמליות ב־G אז $\bigcap_{i\in I} N_i \triangleleft G$.*

למה 7.9: *תהיינה $N \triangleleft G$, $A \leq G$. אזי $AN = NA = \langle A, N\rangle \leq G$.*

הוכחה: $AN = \bigcup_{a\in A} aN = \bigcup_{a\in A} Na = NA \subseteq \langle A, N\rangle$. ודאי $N, A \subseteq NA \subseteq \langle A, N\rangle$ לכן נותר עוד להראות ש־AN תת חבורה של G.

ואכן, $1 \in AN$, $(AN)(AN) = (AA)(NN) = AN$, $(AN)^{-1} = N^{-1}A^{-1} = NA = AN$.

∎

למה 7.11: *תהי $N \triangleleft G$. אזי $G/N = \{gN|\ g \in G\}$ היא חבורה ביחס לכפל של קבוצות חלקיות של G. מתקיים $(g_1N)(g_2N) = g_1g_2N$, איבר היחידה של G/N הוא $1N = N$, וההפכי של gN הוא $g^{-1}N = (gN)^{-1}$.*
[הערנו ש־$g \in gN$. אז הכפל ב־G/N הוא לפי כפל המייצגים ב־G.]

הוכחה: הוכחנו בתרגיל שהכפל אסוציאטיבי. נוודא את הנוסחה לעיל. היתר - פשוט. ∎

דוגמה 7.12: $n\mathbb{Z} = \{nz|\ z \in \mathbb{Z}\} \triangleleft \mathbb{Z}$ נותנת את $\mathbb{Z}/n\mathbb{Z}$.

$|S_3/A_3| = 2$, לכן $S_3/A_3 \cong \mathbb{Z}/2\mathbb{Z}$, לפי מסקנה 6.11.

למה 7.13: *יהי $\theta: G \to H$ הומומורפיזם חבורות. אזי*

(א) *$\theta(e_G) = e_H$, באשר $e_G \in G, e_H \in H$ הם איברי היחידה.*

(ב) *$\theta(g^{-1}) = (\theta(g))^{-1}$ לכל $g \in G$.*

(ג) *$\operatorname{Ker}\theta = \{g \in G|\ \theta(g) = e_H\}$ היא חבורה חלקית נורמלית ב־G.*

(ג') *אם $H' \leq H$ אז $\theta^{-1}(H') = \{g \in G|\ \theta(g) \in H'\} \leq G$ היא חבורה חלקית של G.*

(ד) *$\operatorname{Im}\theta = \{\theta(g)|\ g \in G\}$ היא חבורה חלקית של H.*

(ד') *אם $G' \leq G$ אז $\operatorname{Im}(G') = \{\theta(g)|\ g \in G'\} \leq H$.*

(ה) *θ חח"ע אמ"ם $\operatorname{Ker}\theta = \{e_G\}$ (אמ"ם $\operatorname{Ker}\theta \leq \{e_G\}$).*

הוכחה: את (א), (ב) הוכחנו בעבר. (להוכיח תחלה את (ג'), (ד') ואח"כ (ג), (ד).)

משפט 7.14 (משפט האיזומורפיזם הראשון): *תהי N חבורה חלקית נורמלית של חבורה G.*

(א) *ההעתקה $\pi: G \to G/N$ הנתונה על ידי $\pi(g) = gN$ היא אפימורפיזם שגרעינו N. הוא נקרא האפימורפיזם הטבעי.*

(ב) *יהי $\theta: G \to H$ הומומורפיזם חבורות כך ש־$N \leq \operatorname{Ker}\theta$. אזי קיים הומומורפיזם יחיד $\theta_N: G/N \to H$ כך ש־$\theta = \theta_N \circ \pi$; הוא מוגדר על ידי $\theta_N(gN) = \theta(g)$ ומקיים: θ_N חח"ע $\Leftrightarrow \operatorname{Ker}\theta = N, \operatorname{Im}(\theta) = \operatorname{Im}(\theta_N)$.*

(ג) *אם $N = \operatorname{Ker}\theta$ אז $\theta_N: G/\operatorname{Ker}\theta \to \operatorname{Im}\theta$ הוא איזומורפיזם.*

הוכחה: (ב) אם θ_N קיים, הוא מקיים $\theta_N(gN) = \theta(g)$ ומכאן היחידות; קל לבדוק שהוא הומומורפיזם.
קיום: נראה שההגדרה $\theta_N(gN) = \theta(g)$ טובה. (...)

$$\text{לכן, } \operatorname{Ker}\theta_N = \{gN|\ \theta(g)=e\} = \{gN|\ g\in\operatorname{Ker}\theta\}$$

$$g\in\operatorname{Ker}\theta \text{ לכל } g\in N \Leftrightarrow g\in\operatorname{Ker}\theta \text{ לכל } gN=N \Leftrightarrow \theta_N \text{ חח"ע}$$

$$.\operatorname{Ker}\theta = N \Leftrightarrow \operatorname{Ker}\theta \le N \Leftrightarrow$$

(ג) לפי (ב) $\theta_N: G/\operatorname{Ker}\theta \to H$ חח"ע ועל $\operatorname{Im}(\theta)$. ∎

דוגמה 7.15: העתקת הדטרמיננטה $d: \mathrm{GL}(n,\mathbb{C}) \to \mathbb{C}^\times$ היא הומומורפיזם. היא על: $d(\mathrm{diag}(a,1,\ldots,1)) = a$, וגרעינה $\mathrm{SL}_n(\mathbb{C}) = \{A\in\mathrm{GL}_n(\mathbb{C})|\ |A|=1\}$. לכן

$$.\mathrm{GL}(n,\mathbb{C})/\mathrm{SL}(n,\mathbb{C}) \cong \mathbb{C}^\times \text{ו-} \qquad \mathrm{SL}(n,\mathbb{C}) \lhd \mathrm{GL}(n,\mathbb{C})$$

משפט 7.16 (משפט האיזומורפיזם השלישי):

(א) *תהי $N\lhd G$ ונסמן $\bar{G}=G/N$. אם $N\le A\le G$ אז $N\lhd A$. כמו כן $\bar{A}=\{aN|\ a\in A\}$ היא חבורה חלקית של $\bar{G}$.*

(ב) *ההעתקה $A\mapsto \bar{A}$ היא העתקה חח"ע ממשפחה $\{A|\ N\le A\le G\}$ על משפחת כל החבורות החלקיות של $\bar{G}=G/N$.*

(ג) *יתר על כן: העתקה זו שומרת:*

(1) הכלה: $A_1\le A_2 \Leftrightarrow \bar{A}_1\le\bar{A}_2$

(2) חיתוכים: $\overline{\bigcap_{i\in I}A_i} = \bigcap_{i\in I}\bar{A}_i$

(3) נורמליות: $A_1\lhd A_2 \Leftrightarrow \bar{A}_1\lhd\bar{A}_2$

(4) מנות: אם $A_1\lhd A_2$ אז $A_2/A_1 \cong \bar{A}_2/\bar{A}_1$

הוכחה:

(א) ברור ש-$A\le G$. $N\lhd A$. יהי $\pi: G\to\bar{G}$ האפימורפיזם הטבעי אז $\bar{A}=\pi(A)$. לכן $\bar{A}\le\bar{G}$. (כמו כן, $\bar{A}=A/N$.)

(ב)

על: תהי $B\le\bar{G}$. אז $N=\operatorname{Ker}\pi\le\pi^{-1}(B)\le G$ ו-$\pi(\pi^{-1}(B))=B$ (כי π על.)

חח"ע: נניח $\pi(A)=B$ באשר $N\le A\le G$. נראה ש $A=\pi^{-1}(B)$. ההכלה "$A\subseteq\pi^{-1}(B)$" ברורה. להיפך, אם $g\in\pi^{-1}(B)$, כלומר $\pi(g)\in B$, אז יש $a\in A$ כך ש-$\pi(a)=\pi(g)$. מכאן $\pi(ga^{-1})=1$, ולכן $ga^{-1}\in\operatorname{Ker}\pi\le N\le A$. לכן $g=(ga^{-1})a\in A$.

אם כן, ההעתקה ההפוכה נתונה על ידי $B\mapsto\pi^{-1}(B)$. בפרט $A=\pi^{-1}(\bar{A})$ לכל $N\le A\le G$.

(ג) (1) $A_1\le A_2 \Rightarrow \pi(A_1)\le\pi(A_2)$; $\bar{A}_1\le\bar{A}_2 \Rightarrow \pi^{-1}(\bar{A}_1)\le\pi^{-1}(\bar{A}_2)$.

(2) $\pi^{-1}(\bigcap_{i\in I}\bar{A}_i) = \bigcap_{i\in I}\pi^{-1}(\bar{A}_i) = \bigcap_{i\in I}A_i$; הפעל π על שני האגפים.

(3)

$$a_1 \in A_1, a_2 \in A_2 \text{ לכל } \quad (a_2N)^{-1}(a_1N)(a_2N) \in \bar{A}_1 \Leftrightarrow \bar{A}_1 \lhd \bar{A}_2$$

$$a_1 \in A_1, a_2 \in A_2 \text{ לכל } \quad \pi(a_2^{-1}a_1a_2) = \pi(a_2)^{-1}\pi(a_1)\pi(a_2) \in \bar{A}_1 \Leftrightarrow$$

$$a_1 \in A_1, a_2 \in A_2 \text{ לכל } \quad a_2^{-1}a_1a_2 \in \pi^{-1}(\bar{A}_1) = A_1 \Leftrightarrow$$

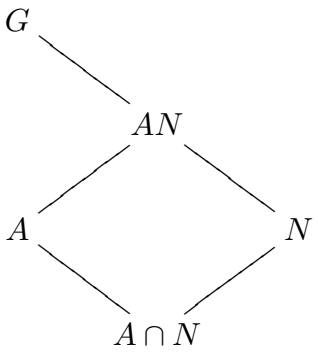
$$A_1 \lhd A_2 \Leftrightarrow.$$

(4) יהי $\lambda: A_2 \to \bar{A}_2/\bar{A}_1$ ההרכבה של האפימורפיזמים הטבעיים $\rho: \bar{A}_2 \to \bar{A}_2/\bar{A}_1$ ו־$\pi: A_2 \to \bar{A}_2$. אזי λ אפימורפיזם, לכן לפי משפט האיזומורפיזם הראשון יש איזומרופיזם $A_2/\operatorname{Ker}\lambda \to \bar{A}_2/\bar{A}_1$. אבל

$$\operatorname{Ker}\lambda = \lambda^{-1}(e) = \pi^{-1}(\rho^{-1}(e)) = \pi^{-1}(\bar{A}_1) = A_1. \qquad \blacksquare$$

דוגמה 7.17: $kn\mathbb{Z} \lhd n\mathbb{Z} \lhd \mathbb{Z}$ לפי (ג)3; $n\mathbb{Z}/kn\mathbb{Z} \lhd \mathbb{Z}/kn\mathbb{Z}$ לפי (ג)4; $(\mathbb{Z}/kn\mathbb{Z})/(n\mathbb{Z}/kn\mathbb{Z}) \cong \mathbb{Z}/n\mathbb{Z}$.

משפט 7.18 (משפט האיזומורפיזם השני): *תהי $N \lhd G$ ותהי $A \leq G$. אזי $A \cap N \lhd A$ ו־$A/A \cap N \cong AN/N$ על ידי $a(A \cap N) \mapsto aN$.*



הוכחה: יהי $\pi: G \to G/N$ האפימורפיזם הטבעי. גרעינו N. צמצומו $\theta: A \to G/N$ ל־A הוא הומומרפיזם. תמונתו [שאמורה לפי משפט האיזומרפיזם השלישי להיות מהצורה H/N באשר $N \leq H \leq A$] היא

$$\operatorname{Im}\theta = \{\pi(a) |\ a \in A\} = \{\pi(a)\pi(n) |\ a \in A, n \in N\} = AN/N.$$

כמו כן $\operatorname{Ker}\theta = \{a \in A |\ \pi(a) = e\} = A \cap \operatorname{Ker}\pi = A \cap N$. לפי משפט האיזומורפיזם הראשון יש איזומורפיזם $\theta_{A\cap N}: A/A \cap N \to AN/N$ הנתון על ידי $a(A \cap N) \mapsto \theta(a) = aN$. $\blacksquare$

תרגיל 7.19: *תהיינה $N \lhd G$ ו־$H_1 \lhd H \leq G$. אז $H_1N \lhd HN$.*

הוכחה: מתקים $N \leq H_1N \leq HN \leq G$. לפי משפט האיזומורפיזם השלישי די להוכיח $H_1N/N \lhd HN/N$. איבר ב־HN/N הוא מהצורה $hnN = hN$, באשר $h \in H, n \in N$, ובאותו אפן איבר ב־H_1N/N הוא מהצורה h_1N, באשר $h_1 \in H_1$. כעת $(hN)^{-1}(h_1N)(hN) = h^{-1}h_1hN \in H_1N/N$. $\blacksquare$

למת הפרפר 7.20 (Zassenhaus): *יהיו* $A_1 \lhd A \leq G$ *ו־* $B_1 \lhd B \leq G$. *אזי*

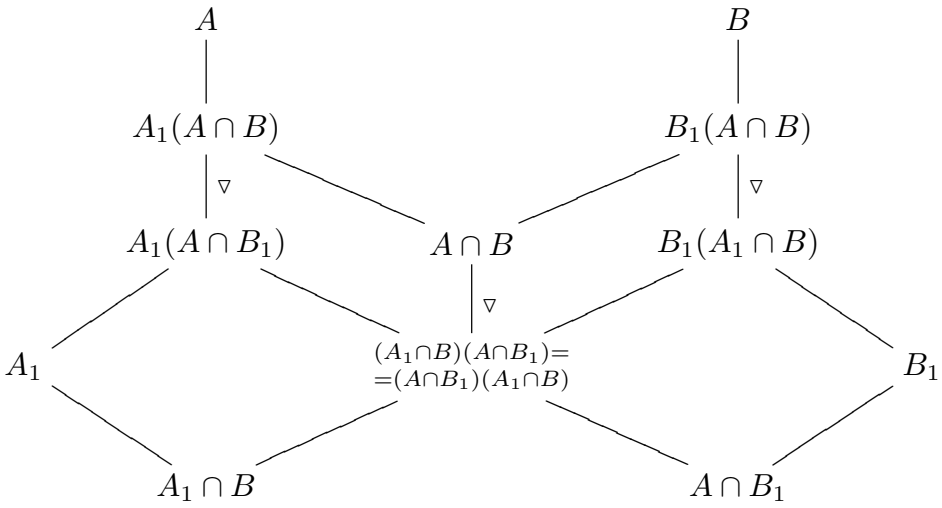
(א) $A_1(A \cap B_1), A_1(A \cap B) \leq G$

(ב) $A_1(A \cap B_1) \lhd A_1(A \cap B)$ *ובאופן סימטרי* $B_1(A_1 \cap B) \lhd B_1(A \cap B)$

(ג) $B_1(A \cap B)/B_1(A_1 \cap B) \cong A_1(A \cap B)/A_1(A \cap B_1)$.

הוכחה:

(א) $A \cap B_1 \leq A \cap B \leq A$, $A_1 \lhd A$, לכן $A_1(A \cap B_1), A_1(A \cap B) \leq A \leq G$, לפי למה 7.9.



(ב) $B_1 \lhd B$, לכן לפי משפט האיזומורפיזם השני $B_1 \cap (A \cap B) \lhd A \cap B$, כלומר $A \cap B_1 \lhd A \cap B$. שתי החבורות האלה חלקיות ל־A, ו־$A_1 \lhd A$, לכן לפי התרגיל נובע (ב).

כמו כן, כיוון ש־$A \cap B_1 \lhd A \cap B$ ובאופן סימטרי גם $A_1 \cap B \lhd A \cap B$, לפי למה 7.9 החבורה הנוצרת על ידי $A_1 \cap B, A \cap B_1$ היא $(A_1 \cap B)(A \cap B_1) = (A \cap B_1)(A_1 \cap B)$ ולפי התרגיל היא נורמלית ב־$A \cap B$.

(ג) קל לראות ש־$[B_1(A_1 \cap B)](A \cap B) = B_1(A \cap B)$, כי $A_1 \cap B \subseteq A \cap B$. כמו כן,
$[B_1(A_1 \cap B)] \cap (A \cap B) = (A \cap B_1)(A_1 \cap B)$: אכן, $\supseteq$ ברור ואם $b_1 \in B_1, c \in A_1 \cap B$ כך ש־$b_1 c \in A \cap B$ אז $b_1 c, c \in A$ ולכן גם $b_1 \in A$. מכאן $b_1 \in A \cap B_1$.
לפי משפט האיזומורפיזם השני $(A \cap B)/(A_1 \cap B)(A \cap B_1) \cong B_1(A \cap B)/B_1(A_1 \cap B)$ ואז (ג) נובע מטעמי סימטריה. ∎

התרגיל הבא יהיה בתרגול:

תרגיל 7.21: *מצא כל החבורות מסדר* 6 *(עד כדי איזומורפיזם)*

השאלה הבאה איננה קשורה לחומר הלימוד, ואין לה, לפי מיטב ידיעתי, שימושים בתורת החבורות. אך היא מעניינת לשם ידע כללי.

שאלת אתגר 7.22: *תהי G חבורה סופית ותהי $H \leq G$ תת חחבורה שלה. הוכח שקיימת $R \subseteq G$ שהינה מערכת מייצגים הן למחלקות השמאליות של H ב־G והן למחלקות הימניות של H ב־G. כלומר, $G = \bigcup_{g\in R} gH = \bigcup_{g\in R} Hg$.*

הטענה היא תוצאה של משפט Hall בקומבינטוריקה שנקרא גם משפט נישואין (marriage theorem). נביא את הניסוח הפופולרי שלו:

נתונה קבוצה W של נשים וקבוצה M של גברים. נניח $|W| = |M|$. רוצים לחתן את הנשים עם הגברים כך שכל אישה תהיה מרוצה (גבר ממילא מרוצה אם אשתו מרוצה...). לשם כך מכינה כל אישה $w \in W$ רשימה M_w של גברים אתם היא מוכנה להתחתן. (כלומר, M_w היא תת קבוצה של M, לכל $w \in W$.) כעת רוצים להתאים לכל אישה חתן מתוך רשימתה, ועל ידי כך לחתן כל אישה עם גבר אחד וכל גבר עם אישה אחת, כמובן.

מובן שזה אינו תמיד אפשרי. תנאי הכרחי ברור (בדוק!) להצלחת המבצע הוא שלכל תת קבוצה W' של W יתקיים $|\bigcup_{w\in W'} M_w| \geq |W'|$.

משפט הנישואין אומר שתנאי זה הוא גם מספיק!

פתרון שאלה 7.22: יהי $n = \frac{|G|}{|H|}$. תהיינה

$$W = \{\tau H|\ \tau \in G\} \quad M = \{H\sigma|\ \sigma \in G\},$$

קבוצות המחלקות הימניות והשמאליות של H ב־G, בהתאמה. אז $|W| = |M| = n$, לפי משפט לגרנז'.

נניח שאפשר לרשום $W = \{\tau_i H\}_{i=1}^n$, $M = \{H\sigma_i\}_{i=1}^n$, (כלומר, לסדר את W, M) כך ש־$\tau_i H \cap H\sigma_i \neq \emptyset$ לכל $i = 1, \ldots, n$. אז, לכל $1 \leq i \leq n$, נבחר $g_i \in \tau_i H \cap H\sigma_i$. הוא יקיים, לפי למה 5.8, $\tau_i H = g_i H$ וגם $H\sigma_i = Hg_i$. לכן $R = \{g_i\}_{i=1}^n$ המערכת המבוקשת.

כדי להוכיח שיש התאמה כזאת בין איברי W ואיברי M, נגדיר לכל $w \in W$

$$M_w = \{m \in M|\ m \cap w \neq \emptyset\}.$$

לפי משפט הנישואין די לבדוק שלכל $W' \subseteq W$ מתקיים $|\bigcup_{w\in W'} M_w| \geq |W'|$. נסמן $X = \bigcup_{w\in W'} w$. קל לראות שמתקיים

$$\bigcup_{w\in W'} M_w = \{H\sigma \in M|\ H\sigma \cap X \neq \emptyset\},$$

לכן די להראות כי X חותכת באופן לא טריוויאלי לפחות $|W'|$ מחלקות ימניות.

כעת, X היא איחוד זר של מחלקות שמאליות τH, כל אחת בת $|H|$ איברים, לכן $|X| = |W'| \cdot |H|$. כל איבר של G נמצא באיזו מחלקה ימנית $H\sigma$, וכל מחלקה ימנית מכילה בדיוק $|H|$ איברים, לכן X חותכת באופן לא טריוויאלי לפחות $|W'| = \frac{|X|}{|H|}$ מחלקות ימניות. ∎

8. אוטומורפיזמים. פעולה של חבורה על קבוצה.

הגדרה 8.1: **אוטומורפיזם** של חבורה G הוא איזומורפיזם מ־G על G. אוסף כל האוטומרפיזמים של G יסומן $\mathrm{Aut}(G)$. זוהי חבורה ביחס לפעולת ההרכבה

$$(\alpha\beta)(g) = \alpha(\beta(g)), \qquad \alpha, \beta \in \mathrm{Aut}(G),\ a, \in G.$$

לפעמים רושמים ${}^{\alpha}g$ במקום $\alpha(g)$. אז ${}^{\alpha\beta}g = {}^{\alpha}({}^{\beta}g)$.

דוגמה 8.2: יהי $a \in G$. ההעתקה $g \mapsto {}^{a}g = aga^{-1}$ היא אוטומורפיזם של G (מסקנה 7.3). הוא נקרא **האוטומורפיזם הפנימי** המתאים ל־a וגם **ההצמדה ב־a** (**משמאל**).

תרגיל 8.3: *(א) ההעתקה $G \to \mathrm{Aut}(G)$ המעתיקה a לאוטומורפיזם הפנימי המתאים לו, היא הומומורפיזם. תמונתה $\mathrm{Inn}(G)$, היא אוסף כל האוטומרפיזמים הפנימיים של G.*

(ב) *(הגרעין של הומומרפיזם זה:) האוטומורפיזם הפנימי המתאים ל־a הוא זהות אם ורק אם a שייך ל**מֶרְכָּז** של G,*

$$Z(G) = \{a \in G |\ g \in G \text{ לכל } ag = ga\}.$$

הגדרה 8.4: תהי G חבורה ותהי X קבוצה. **פעולה** (**משמאל**) של G על X היא העתקה $\pi\colon G \times X \to X$ [בד"כ נרשום ${}^{g}x$ במקום $\pi(g,x)$] המקיימת

(א) $\pi(g_1g_2, x) = \pi(g_1, \pi(g_2, x))$ [${}^{g_1g_2}x = {}^{g_1}({}^{g_2}x)$] לכל $x \in X,\ g_1, g_2 \in G$,

(ב) $\pi(e, x) = x$ [${}^{e}x = x$] לכל $x \in X$.

דוגמה 8.5:

(1) חבורת המטריצות ההפיכות $\mathrm{Gl}_n(\mathbb{C})$ מסדר $n \times n$ מעל $\mathbb{C}$ פועלת על $\mathbb{C}^n$ על ידי הכפל: ${}^{A}v = Av$.

(2) $S(X)$ פועלת על X; בפרט, S_n פועלת על $\{1, 2, \ldots, n\}$.

(3) חבורה G פועלת על עצמה על ידי ההצמדה משמאל .

(4) חבורה G פועלת על האוסף $\{H |\ H \leq G\}$ על ידי ההצמדה משמאל.

(5) חבורה G פועלת על עצמה על ידי כפל משמאל: $\pi(g,x) = gx$.

(6) אוסף כל הפעולות שאפשר לעשות על הקוביה ההונגרית הוא חבורה; היא פועלת על אוסף כל הקונפיגורציות של מרכיבי הקוביה.

(7) הפעולה הטריוויאלית של חבורה G על קבוצה X: ${}^{g}x = x$ לכל $g \in G,\ x \in X$.

(8) יש גם **פעולה מימין** $(x,g) \mapsto x^g$ של חבורה G על קבוצה X ($x^{g_1g_2} = (x^{g_1})^{g_2}$, $x^e = x$). אך היא מגדירה פעולה משמאל על ידי ${}^{g}x = x^{g^{-1}}$.

הגדרה 8.6: אם G פועלת על X אז היחס על X: "$x_1 \sim x_2$ אם יש $g \in G$ כך ש־$x_2 = {}^g x_1$" הוא יחס שקילות. מחלקת השקילות נקראת **מסלול־G**. עוצמת מסלול נקראת **אורך** המסלול. בפרט: X היא אחוד זר של מסלולי־G השונים: $X = \bigcup_{i\in I}\{{}^g x_i |\ g \in G\}$, באשר $\{x_i\}_{i\in I}$ היא מערכת מיצגים של מסלולי־G (כלומר מכילה בדיוק איבר אחד מכל מסלול־G).

למה 8.7: *נניח כי G פועלת על X ויהי $x \in X$. אזי*

(א) $G_x = \{g \in G |\ {}^g x = x\}$ *היא חבורה חלקית של G הנקראת* **חבורת המייצב** *של x.*

(ב) ${}^{g_1}x = {}^{g_2}x \Leftrightarrow g_1 G_x = g_2 G_x \Leftrightarrow G_x g_1^{-1} = G_x g_2^{-1}$.

(ג) *אורך המסלול X' של x הוא $(G : G_x)$. יש התאמה חח"ע ועל $\rho : R \to X'$ על ידי $g \mapsto {}^g x$, באשר R מערכת מייצגים של המחלקות השמאליות של G_x ב־G. (כלומר, $G = \bigcup_{g\in R} gG_x$.)*

הוכחה: (א) בודקים שהקבוצה מכילה את 1, סגורה תחת הכפל ולקיחת ההופכי.

(ב) $G_x g_1^{-1} = G_x g_2^{-1} \Leftrightarrow g_1 G_x = g_2 G_x \Leftrightarrow g_2^{-1} g_1 \in G_x \Leftrightarrow {}^{g_2^{-1}g_1}x = x \Leftrightarrow {}^{g_1}x = {}^{g_2}x$.

(ג) ρ חח"ע לפי (ב). היא על: אם $g \in G$, יש $\sigma \in R, \tau \in G_x$ כך ש־$g = \sigma\tau$. אז ${}^g x = {}^{\sigma\tau}x = {}^{\sigma}x$, לכן $\rho(\sigma) = {}^g x$. לכן אורך המסלול הוא $|R| = (G : G_x)$. ∎

תרגיל 8.8: *חבורה מעגלית $G = \langle\sigma\rangle$ מסדר n פועלת על קבוצה X. יהי $x \in X$ ונניח כי $(G : G_x) = d$. הראה כי $x, {}^{\sigma}x, \ldots, {}^{\sigma^{d-1}}x$ הם כל איבריו השונים של מסלול־G של x ו־$G_x = \langle\sigma^d\rangle$.*

פתרון: יהי X' מסלול־G של x. לפי הלמה יש לו בדיוק d איברים. ברור ש־$x, {}^{\sigma}x, \ldots, {}^{\sigma^{d-1}}x \in X'$. לפי הלמה, ${}^{\sigma^i}x = {}^{\sigma^j}x$ אם ורק אם $\sigma^i G_x = \sigma^j G_x$, כלומר, $\sigma^{j-i} \in G_x$. לפי משפט לגרנז' $|G_x| = \frac{n}{d}$, לכן לפי למה 6.9, $G_x = \langle\sigma^d\rangle$. לכן ${}^{\sigma^i}x = {}^{\sigma^j}x$ אם ורק אם $\sigma^{j-i} \in \langle\sigma^d\rangle$. כלומר, $d|j-i$. מכאן ש־$x, {}^{\sigma}x, \ldots, {}^{\sigma^{d-1}}x$ שונים זה מזה. ∎

מסקנה 8.9: *אם חבורה G פועלת על קבוצה סופית X, ו־$\{x_i\}_{i\in I}$ היא מערכת מיצגים של מסלולי־G אז $|X| = \sum_{i\in I}(G : G_{x_i})$. אם $\{x_i\}_{i\in I'}$ היא מערכת מיצגים של מסלולי־G בעלי אורך > 1 אז*

$$|X| = \sum_{i\in I'}(G : G_{x_i}) + |\{x \in X |\ g \in G \text{ לכל } {}^g x = x\}|.$$

הוכחה: מתקיים $X = \bigcup_{i\in I}\{{}^g x_i |\ g \in G\}$. לפי למה 8.7, $|\{{}^g x_i |\ g \in G\}| = (G : G_{x_i})$ לכל $i \in I$. מכאן הנוסחה הראשונה. כמו כן, אורך המסלול של $x \in X$ הוא 1 אם ורק אם ${}^g x = x$ לכל $g \in G$. מכאן הנוסחה השניה. ∎

הגדרות 8.10: נתבונן בפעולת ההצמדה משמאל.

אם $a \in G$ אז $\{g \in G |\ {}^g a = a\} = \{g \in G |\ aga^{-1} = g\}$ הוא **המְרַכֵּז** $C_G(a)$ של a. בפרט $C_G(a) \leq G$.

אם $H \leq G$ אז $\{g \in G|\ {}^gH = H\} = \{g \in G|\ aHa^{-1} = H\}$ הוא **המְשַמֵּר (נורמליזטור)** $N_G(H)$ של H. בפרט $H \leq N_G(H) \leq G$.

מסקנה 8.11: *אם חבורה G סופית, ו־$\{x_i\}_{i\in I}$ מערכת מיצגים של מחלקות הצמידות ב־G אז $|G| = \sum_{i\in I}(G : G_{x_i})$. אם $\{x_i\}_{i\in I'}$ היא מערכת מיצגים של מחלקות הצמידות ב־G בעלות יותר מאיבר אחד אז*

$$|G| = \sum_{i\in I'}(G : C_G(x_i)) + |Z(G)|.$$

משפט 8.12: *פעולה π של G על X מגדירה הומומורפיזם $\varphi: G \to S(X)$ על ידי*

$$\varphi(g)(x) = \pi(g, x) \quad [= {}^gx] \qquad (*)$$

ההעתקה $\{\text{פעולות של } G \text{ על } X\} \to \{\text{הומומורפיזמים מ־} G \text{ ל־} S(X)\}$ על ידי $\pi \mapsto \varphi$ הנתונה על ידי (*) היא חח"ע ועל. ההעתקה ההפוכה נתונה גם על ידי (*).

הוכחה: ההעתקה $\varphi: G \to \{f: X \to X\}$ המוגדרת על ידי (*) מקיימת

$$\varphi(g_1g_2)(x) = {}^{(g_1g_2)}x = {}^{g_1}({}^{g_2}x) = \varphi(g_1)(\varphi(g_2)(x)), \qquad \text{לכל } g_1, g_2 \in G, x \in X,$$

וכן $\varphi(e)(x) = x$ לכל $x \in X$, כלומר

$$\varphi(g_1g_2) = \varphi(g_1)\varphi(g_2), \quad \varphi(e) = \mathrm{id}, \qquad \text{לכל } g_1, g_2 \in G.$$

בפרט לכל $g \in G$ מתקים $\varphi(g)\varphi(g^{-1}) = \varphi(gg^{-1}) = \varphi(e) = \mathrm{id}$, ובאופן דומה $\varphi(g^{-1})\varphi(g) = \mathrm{id}$, כלומר $\varphi(g)$ תמורה על X. ברור ש־φ הומומורפיזמים. זה מוכיח את הטענה הראשונה.

לגבי הטענה השניה: אם $\varphi: G \to S(X)$ הומומורפיזם, אז π המוגדרת על ידי (*) אכן פעולה. ההעתקות $\varphi \mapsto \pi$ ו־$\pi \mapsto \varphi$ הפוכות זו לזו (כי הן נתונות על ידי אותה נוסחה.) ∎

מסקנה 8.13: *תהיינה $H \leq G$ חבורות. נניח כי $n = (G : H) < \infty$. תהי $K = \bigcap_{g\in G} H^g$. אז $K \lhd G$, $K \leq H$ ו־G/K איזומורפית לתת חבורה של S_n. בפרט, אם G סופית ו־$|G| \nmid n!$ אז $K \neq 1$.*

הוכחה: תהי $X = \{gH|\ g \in G\}$. אז $|X| = n$. החבורה G פועלת על X על ידי כפל משמאל: ${}^\sigma gH = \sigma gH$. לפי (*), פעולה זו מגדירה הומומורפיזם $\varphi: G \to S(X) \cong S_n$. הגרעין של φ הוא

$$= \{\sigma \in G|\ g \in G \text{ לכל } \sigma gH = gH\} = \{\sigma \in G|\ g \in G \text{ לכל } \sigma gHg^{-1} \in gHg^{-1}\} =$$
$$= \bigcap_g gHg^{-1} = K.$$

לכן $K \lhd G$. לפי משפט האיזומורפיזם הראשון $G/K \cong \varphi(G) \leq S(X) \cong S_n$. אם $\sigma \in K$ אז $\sigma 1H = 1H$, לכן $\sigma \in H$. לכן $K \leq H$. ∎

9. חבורות תמורות.

חבורת התמורות על $X=\{1,2,\ldots,n\}$ נקראת **החבורה הסימטרית** S_n. **חישוק** (cyclus) $\pi=(a_1a_2\ldots a_k)$ **מאורך** k, באשר $a_1,a_2,\ldots,a_k\in X$ שונים זה מזה, מוגדר על ידי

$$\pi(a_1)=a_2,\ \pi(a_2)=a_3,\ldots,\pi(a_k)=a_1 \qquad \text{לכל } a\neq a_1,a_2,\ldots,a_k\in X \text{ כל } \pi(a)=a.$$

קל לראות ש־$\operatorname{ord}\pi=k$. חישוק מאורך 2 נקרא **חישוקון** (transposition).

שני חישוקים $(a_1a_2\ldots a_k),(b_1b_2\ldots b_m)$ **זרים** אם $a_i\neq b_j$ לכל i,j. חישוקים זרים מתחלפים ביניהם בכפל!

הערה 9.1: $(a_1a_2\ldots a_k)=(a_2\ldots a_ka_1)=(a_3\ldots a_ka_1a_2)=\ldots$.

למה 9.2: *כל $\sigma\in S_n$ ניתן להציג כמכפלה $\sigma=\pi_1\pi_2\cdots\pi_r$ של חישוקים זרים מאורך >1. הצגה זו הנה יחידה עד כדי סדר החישוקים.*

הוכחה: **קיום**: $\langle\sigma\rangle$ פועלת על $X=\{1,\ldots,n\}$. יהיו $X_1,\ldots,X_r$ המסלולים מאורך >1 של $\langle\sigma\rangle$, נאמר, X_i מאורך k_i, ונבחר $x_i\in X_i$. לפי תרגיל 8.8, $X_i=\{x_i,\sigma(x_i),\ldots\sigma^{k_i-1}(x_i)\}$ ו־$\sigma^{k_i}(x_i)=x_i$. יהי $\pi_i=\big(x_i\ \sigma(x_i)\ \ldots\ \sigma^{k_i-1}(x_i)\big)$. אז $\sigma=\pi_1\pi_2\cdots\pi_r$, כי (בדוק!) שני האגפים פועלים באותו אופן על איבר מהצורה $\sigma^j(x_i)\in X_i$ ועל איבר במסלול מאורך 1.

יחידות: נניח כי $\sigma=\rho_1\rho_2\cdots\rho_m$, באשר $\rho_i=(a_{i1}a_{i2}\ldots a_{il_i})$ חישוק מאורך $l_i>1$ ו־$\rho_1,\ldots,\rho_m$ זרים. אז

$$\begin{aligned}
\sigma(a_{i1})&=(\rho_1\rho_2\cdots\rho_m)(a_{i1})=\rho_i(a_{i1})=a_{i_2},\\
\sigma^2(a_{i1})&=\sigma(a_{i2})=(\rho_1\rho_2\cdots\rho_m)(a_{i2})=\rho_i(a_{i2})=a_{i3},\\
&\ldots\\
\sigma^{l_i-1}(a_{i1})&=a_{il_i},\\
\sigma^{l_i}(a_{i1})&=a_{i1}
\end{aligned}$$

לכן $X_i'=\{a_{i1},a_{i2},\ldots,a_{il_i}\}=\{\sigma^j(a_{i1})|\ j\geq 0\}=\{1,\sigma,\sigma^2,\ldots\}$ הוא מסלול של $\langle\sigma\rangle$ מאורך l_i. המסלולים $X_1',\ldots,X_m'$ זרים (כי $\rho_1,\ldots\rho_m$ זרים), והם כל מסלולי־$\langle\sigma\rangle$ מאורך >1: אם $x\in X\smallsetminus\bigcup_{i=1}^m X_i'$ אז $\rho_i(x)=x$ לכל i, לכן $\sigma(x)=x$, ולכן $\{x\}$ מסלול מאורך 1 של $\langle\sigma\rangle$. לכן $m=r$ ובה"כ $X_i'=X_i$ לכל i. בפרט $l_i=k_i$ לכל i. כעת $x_i=a_{ij_i}$ עבור איזה j_i, ובה"כ $x_i=a_{i1}$ (לפי ההערה 9.1). לכן

$$\rho_i=(a_{i1}a_{i2}\ldots a_{ik_i})=(x_i\ \sigma(x_i)\ \ldots\ \sigma^{k_i-1}(x_i))=\pi_i. \qquad \blacksquare$$

דוגמה 9.3: $\begin{pmatrix}1&2&3&4&5&6&7&8&9\\3&5&8&9&2&6&7&1&4\end{pmatrix}=(138)(25)(49)$.

מסקנה 9.4: *כל תמורה $\sigma\in S_n$ אפשר לכתוב כמכפלה של חישוקונים (לא בהכרח באופן יחיד).*

הוכחה: בה"כ σ היא חישוק. אז $(a_1a_2\ldots a_k)=(a_ka_1)(a_{k-1}a_1)\cdots(a_3a_1)(a_2a_1)$. $\blacksquare$

דוגמה 9.5: אין יחידות בהצגה כמכפלה של חישוקונים: $(12)(13)(23) = (13)$.

תרגיל 9.6: *יהיו* $\sigma \in S_n, \pi = (a_1 \dots a_k) \in S_n$ *אז* $\sigma\pi\sigma^{-1} = (\sigma(a_1) \dots \sigma(a_k))$.

פתרון: כל $1 \le i \le n$ הוא מהצורה $\sigma(j)$, באשר $1 \le j \le n$. בדוק את פעולת שתי התמורות $(\sigma(a_1) \dots \sigma(a_k)) \, , \sigma(a_1 \dots a_k)\sigma^{-1}$ עליו. ∎

הערה 9.7: זוגיות של תמורות. תהי $X = \{(i,j) | \ 1 \le i,j \le n, i \ne j\}$. נקרא ל־$Y \subseteq X$ **תקנית** אם היא מכילה בדיוק איבר אחד מכל זוג $(i,j),(j,i) \in X$. למשל $T = \{(i,j) | \ 1 \le i < j \le n\}$ תקנית.

S_n פועלת על X על ידי $^{\sigma}(i,j) = (\sigma(i), \sigma(j))$. אם $Y \subseteq X$ תקנית אז גם $^{\sigma}Y$ תקנית (כי קל לראות שאם $^{\sigma}Y$ אינה תקנית, אז Y אינה תקנית).

(1) לכל $x = (i,j) \in X$ נסמן $\mathrm{Sg}(x) = \begin{cases} 1 & \text{אם } i < j \\ -1 & \text{אם } i > j \end{cases}$.

(2) לכל $Y \subseteq X$ (תקנית) נגדיר $\mathrm{Sg}(Y) = \prod_{x \in Y} \mathrm{Sg}(x) \in \{\pm 1\}$.

(3) לכל $\sigma \in S_n$ נגדיר $\mathrm{Sg}(\sigma) = \prod_{x \in Y} \mathrm{Sg}(^{\sigma}x)/\mathrm{Sg}(x) = \mathrm{Sg}(^{\sigma}Y)/\mathrm{Sg}(Y) \in \{\pm 1\}$, באשר $Y \subseteq X$ תקנית. הגדרה זו אינה תלויה ב־Y כי $\mathrm{Sg}(i,j) = -\mathrm{Sg}(j,i), \mathrm{Sg}\,^{\sigma}(i,j) = -\mathrm{Sg}\,^{\sigma}(j,i)$, ולכן אם נחליף את (i,j) ב־(j,i), לא תשתנה ההגדרה.

תמורה $\sigma \in S_n$ תקרא **זוגית** אם $\mathrm{Sg}(\sigma) = 1$ **ואי זוגית** אם $\mathrm{Sg}(\sigma) = -1$. בפרט (קח $Y = T$) σ זוגית אם ורק אם המספר $|\{(i,j) | \ i < j, \ \sigma(i) > \sigma(j)\}|$ הוא זוגי.

דוגמה 9.8: חישוקון $\sigma = (12)$ הוא אי זוגי.

אכן, יהיו $i < j$. אז $\sigma(i) > \sigma(j)$ אם ורק אם $i = 1, j = 2$. ∎

משפט 9.9: $\mathrm{Sg}(\sigma\tau) = \mathrm{Sg}(\sigma)\mathrm{Sg}(\tau)$.

הוכחה: אם Y תקנית ו־$\sigma \in S_n$ אז לפי ההגדרות $\mathrm{Sg}(^{\sigma}Y) = \mathrm{Sg}(\sigma)\mathrm{Sg}(Y)$. לכן

$$\mathrm{Sg}(\sigma\tau)\mathrm{Sg}(Y) = \mathrm{Sg}(^{\sigma\tau}Y) = \mathrm{Sg}(^{\sigma}(^{\tau}Y)) = \mathrm{Sg}(\sigma)\mathrm{Sg}(^{\tau}Y) = \mathrm{Sg}(\sigma)\mathrm{Sg}(\tau)\mathrm{Sg}(Y),$$

ומכאן המסקנה. ∎

מסקנה 9.10: *ההעתקה* $\mathrm{Sg}: S_n \to \{\pm 1\}$ *היא אפימורפיזם (עבור* $n > 1$*).*

מסקנה 9.11: $A_n = \{\sigma \in S_n | \ \mathrm{Sg}(\sigma) = 1\}$ *היא חבורה חלקית נורמלית ב־* S_n *מאינדקס 2. נקראת* **חבורת החילופין**.

מסקנה 9.12: *(א) אם* π *חישוק מאורך* k *אז* $\mathrm{Sg}(\pi) = (-1)^{k-1}$. *בפרט,*

(ב) *כל חישוקון הוא אי זוגי.*

הוכחה: (ב) יהי (kl) חישוקון. יש $\sigma \in S_n$ כך ש־$\sigma(1) = k, \sigma(2) = l$. לפי תרגיל 9.6, $(kl) = \sigma(12)\sigma^{-1}$, לכן

$$\mathrm{Sg}(kl) = \mathrm{Sg}(\sigma)\mathrm{Sg}(12)\mathrm{Sg}(\sigma)^{-1} = \mathrm{Sg}(12) = -1.$$

(א) $(a_1a_2\dots a_k)=(a_ka_1)\cdots(a_3a_1)(a_2a_1)$ הוא מכפלה של $k-1$ חישוקונים. ∎

מסקנה 9.13: *σ זוגית אמ"ם אפשר לכתוב אותה כמכפלה של מספר זוגי של חישוקונים.*

למה 9.14: *A_n נוצרת על ידי החישוקים מאורך 3 ב־S_n.*

הוכחה: מצד אחד כל חישוק מאורך 3 הינו זוגי ולכן נמצא ב־A_n. מצד שני כל איבר ב־A_n הוא מכפלה של מספר זוגי של חישוקונים, לכן די להראות שמכפלה של שני חישוקונים אפשר לכתוב כמכפלה של חישוקים מאורך 3. ואכן, יהיו i,j,k,l שונים זה מזה, אז

$$(ij)(ij)=1,\qquad (ik)(ij)=(ijk),\qquad (kl)(ij)=(kl)(jk)(jk)(ij)=(jlk)(ikj),$$

ו־1 הוא מכפלה ריקה של חישוקים. ∎

הגדרה 9.15: חבורה $G\neq\{1\}$ נקראת **פשוטה** אם אין $N\triangleleft G$ כך ש־$\{1\}\neq N\neq G$.

דוגמה 9.16: $\mathbb{Z}/p\mathbb{Z}$ פשוטה לכל p ראשוני. S_n אינה פשוטה לכל $n\geq 3$, כי $A_n\triangleleft S_n$ ו־$1<A_n<S_n$.

משפט 9.17: *A_n פשוטה לכל $n\geq 5$.*

הוכחה: יהי $n\geq 5$ ותהי $N\triangleleft A_n$.

טענה א: *אם N מכילה חישוק מאורך 3 אז $N=A_n$.*

נניח $(abc)\in N$. לפי הלמה הקודמת די להראות ש־N מכילה כל חישוק $(a'b'c')$ מאורך 3. נבחר $\sigma\in S_n$ כך ש־$\sigma(c)=c'$, $\sigma(b)=b'$, $\sigma(a)=a'$. אזי $\sigma(abc)\sigma^{-1}=(a'b'c')$, לכן אם $\sigma\in A_n$ אז $(a'b'c')\in N$. אם σ אי זוגית, נבחר d,f שונים מ־a,b,c (אפשר, כי $n\geq 5$) ואז $\tau:=\sigma(df)\in A_n$ ו־$\tau(abc)\tau^{-1}=(a'b'c')$. לכן שוב $(a'b'c')\in N$.

טענה ב: *אם $N\neq 1$, יש חישוק מאורך 3 ב־N.*

יש $1\neq\pi\in N$. נכתוב אותו כמכפלה של $r\geq 1$ חישוקים זרים $\pi=\pi_1\pi_2\cdots\pi_r$, מאורכים $k_1\geq k_2\geq\cdots\geq k_r\geq 2$. יהיו $\pi_1=(a_1\dots a_{k_1})$, $\pi_2=(a_{k_1+1}\dots,a_{k_1+k_2}),\dots$ באשר $a_1,a_2,\dots,a_n$ סידור של המספרים $1,2,\dots,n$.

שיטת ההוכחה: לכל $\sigma\in A_n$ מתקיים $\pi^{-1},\sigma\pi\sigma^{-1}\in N$ לכן

$$\pi^{-1}\,\sigma\pi\sigma^{-1}=\pi_r^{-1}\cdots\pi_2^{-1}\pi_1^{-1}(\sigma\pi_1\sigma^{-1})(\sigma\pi_2\sigma^{-1})\cdots(\sigma\pi_r\sigma^{-1})=$$
$$=\pi_1^{-1}\pi_2^{-1}\cdots\pi_r^{-1}(\sigma\pi_r\sigma^{-1})\cdots(\sigma\pi_2\sigma^{-1})(\sigma\pi_1\sigma^{-1})\ni N.$$

נרצה לבחור σ כך שאיבר זה יהיה חישוק מאורך 3. נשים לב שאם σ שומרת כל אות שמופיעה ב־π_i אז לפי תרגיל 9.6, $\sigma\pi_i\sigma^{-1}=\pi_i$. זה מפשט את החישוב לעיל.

נבדיל בין כמה מקרים:

(1) אם $k_1 \geq 4$ או $k_1 = k_2 = 3$, נקח $\sigma = (a_2 a_3 a_4)$.

1.1 אם $k_1 \geq 5$ אז

$$\pi^{-1}\,\sigma\pi\sigma^{-1} = \pi_1^{-1}\,\sigma\pi_1\sigma^{-1} = (\ldots a_5 a_4 a_3 a_2 a_1)(a_1 a_3 a_4 a_2 a_5 \ldots) = (a_1 a_2 a_4)$$

1.2 ואם $k_1 = 4$ אז

$$\pi^{-1}\,\sigma\pi\sigma^{-1} = \pi_1^{-1}\,\sigma\pi_1\sigma^{-1} = (a_4 a_3 a_2 a_1)(a_1 a_3 a_4 a_2) = (a_1 a_2 a_4)$$

1.3 ואם $k_1 = k_2 = 3$ אז

$$\pi^{-1}\,\sigma\pi\sigma^{-1} = \pi_2^{-1}\pi_1^{-1}\,\sigma\pi_1\sigma^{-1}\sigma\pi_2\sigma^{-1} =$$

$$= (a_6 a_5 a_4)(a_3 a_2 a_1)(a_1 a_3 a_4)(a_2 a_5 a_6) = (a_1 a_2 a_4 a_3 a_6)$$

זהו חישוק מאורך 5, ולכן לפי מקרה (1.1) יש חישוק מאורך 3 ב־N.

(2) אם $k_1 = 3, k_2 = \cdots = k_r = 2$ אז $\pi_2^2 = \cdots = \pi_r^2 = 1$, ולכן

$$N \ni \pi^2 = \pi_1^2 = (a_1 a_2 a_3)^2 = (a_1 a_3 a_2).$$

(3) אם $k_1 = k_2 \cdots = k_r = 2$, נקח $\sigma = (a_3 a_4 a_5)$. אז

3.1 אם $r = 2$,

$$\pi^{-1}\,\sigma\pi\sigma^{-1} = (a_4 a_3)(a_2 a_1)(a_1 a_2)(a_4 a_5) = (a_4 a_3)(a_4 a_5) = (a_3 a_4 a_5)$$

3.2 אם $r \neq 2$, ולכן $r \geq 4$ (כי π זוגית),

$$\pi^{-1}\,\sigma\pi\sigma^{-1} = (a_6 a_5)(a_4 a_3)(a_2 a_1)(a_1 a_2)(a_4 a_5)(a_3 a_6) = (a_3 a_5)(a_4 a_6)$$

ולכן לפי מקרה (3.1) יש חישוק מאורך 3 ב־N. ∎

משפט 9.18 (Cayley): *תהי G חבורה סופית מסדר n. אזי G איזומורפית לחבורה חלקית של S_n.*

הוכחה: נזהה את הקבוצה G עם הקבוצה $\{1, 2, \ldots, n\}$. אז $S(G) = S_n$ (ראה גם תרגיל בהמשך). נגדיר פעולה של G על עצמה על ידי הכפל משמאל: $(\sigma, g) \mapsto \sigma g$. פעולה זו מגדירה הומומורפיזם $\psi\colon G \to S(G)$ על ידי $\psi(\sigma)(g) = \sigma g$ (משפט 8.12).

$$\text{Ker}\,\psi = \{\sigma \in G |\ \psi(\sigma) = id\} = \{\sigma \in G |\ g \in G \text{ לכל } \sigma g = g\} = \{1\},$$

לכן ψ חח"ע. ∎

תרגיל 9.19: *אם X, Y קבוצות מאותה העצמה אז $S(X) \cong S(Y)$.*

פתרון: יש $g\colon X \to Y$ חח"ע ועל. נגדיר $\psi\colon S(X) \to S(Y)$ על ידי $f \mapsto gfg^{-1}$. אז ψ מוגדרת היטב (כלומר, $gfg^{-1}\colon Y \to Y$ אכן חח"ע ועל) ושומרת הרכבה. ההעתקה ההפוכה נתונה על ידי $h \mapsto g^{-1}hg$. ∎

.

10. מכפלות ישרות.

תהיינה $G_1, \ldots, G_n$ חבורות. אזי

$$G^* = G_1 \times \cdots \times G_n = \{(g_1, \ldots, g_n) |\ g_1 \in G_1, \ldots, g_n \in G_n\}$$

היא חבורה ביחס לכפל המוגדר לפי מרכיבים (היחידה: $(e_1, \ldots, e_n)$, באשר e_i היחידה של G_i). נקראת **המכפלה הישרה (החיצונית)** של $G_1, \ldots, G_n$.

קיים הומומורפיזם $G_i \to G_1 \times \cdots \times G_n$ הנתון על ידי

$$g_i \mapsto (e_1, \ldots, e_{i-1}, g_i, e_{i+1}, \ldots, e_n).$$

הוא חח"ע. לכן תמונתו G_i^* איזומורפית ל־G_i.

קל לראות (נזניח את הכוכבית *):

(1) $G = \langle G_1, \ldots, G_n \rangle$; [ואפילו (1′) $G = G_1 \cdots G_n$]

(2) $G_i \lhd G$ לכל i;

(3) $G_i \cap \langle G_1, \ldots, \widehat{G_i}, \ldots, G_n \rangle = \{1\}$;

(4) $xy = yx$ לכל $x \in G_i, y \in G_j$, $i \neq j$;

(5) אם $x_1 \cdots x_n = y_1 \cdots y_n$, באשר $x_i, y_i \in G_i$ אז $x_i = y_i$ לכל i.

משפט 10.1: *תהי G חבורה ו־$G_1, \ldots, G_n \leq G$. התנאים הבאים שקולים:*

(א) *קיים איזומורפיזם $G^* = G_1 \times \cdots \times G_n \to G$ אשר מעתיק את G_i^* על G_i.*

(ב)

(1) $G = \langle G_1, \ldots, G_n \rangle$.

(2) $G_i \lhd G$ לכל i;

(3) $G_i \cap \langle G_1, \ldots, \widehat{G_i}, \ldots, G_n \rangle = \{1\}$.

(ג)

(1) $G = \langle G_1, \ldots, G_n \rangle$.

(4) $xy = yx$ לכל $x \in G_i, y \in G_j$, $i \neq j$;

(5) אם $x_1 \cdots x_n = y_1 \cdots y_n$, באשר $x_i, y_i \in G_i$ אז $x_i = y_i$ לכל i.

הוכחה: (א) $\Leftarrow$ (ב) – ברור.

(ב) $\Leftarrow$ (ג): נראה (4). לפי (2) $x^{-1}y^{-1}xy = (y^{-1})^x y \in G_j$, וגם $x^{-1}y^{-1}xy = x^{-1}x^y \in G_i$, ולפי (3) $G_i \cap G_j = \{1\}$, לכן $x^{-1}y^{-1}xy = 1$. מכאן (4).

נראה (5). אם $x_1 \cdots x_n = y_1 \cdots y_n$, באשר $x_i, y_i \in G_i$, אז לפי (4) $x_1 y_1^{-1} \cdots x_n y_n^{-1} = 1$, לכן $x_i y_i^{-1} \in G_i \cap \langle G_1, \ldots, \widehat{G_i}, \ldots, G_n \rangle$. מכאן $x_i y_i^{-1} = 1$ לפי (3), כלומר, (5) מתקיים.

(ג) $\Leftarrow$ (א): נגדיר העתקה $\theta: G^* = G_1 \times \cdots \times G_n \to G$ על ידי $\theta(g_1, \ldots, g_n) = g_1 \cdots g_n$. אז θ הומומורפיזם: אם $(x_1, \ldots, x_n), (y_1, \ldots, y_n) \in G^*$ אז לפי (4)

$$\theta((x_1, \ldots, x_n)(y_1, \ldots, y_n)) = \theta(x_1 y_1, \ldots, x_n y_n) = x_1 y_1 x_2 y_2 \cdots x_n y_n =$$
$$x_1 \cdots x_n y_1 \cdots y_n = \theta(x_1, \ldots, x_n)\theta(y_1, \ldots, y_n).$$

θ חח"ע לפי (5).

כמו כן $\theta(G_i^*) = G_i$. בפרט $\langle G_1, \ldots, G_n \rangle \leq \theta(G^*)$, לכן לפי (1) θ על. ∎

הגדרה 10.2: אם התנאים של המשפט מתקיימים, G נקראת **מכפלה ישרה (פנימית)** של $G_1, \ldots, G_n$ ונכתוב $G = G_1 \times \cdots \times G_n$. אם הפעולות של $G_1, \ldots, G_n$ הן חיבור, נכתוב בד"כ $G_1 \oplus \cdots \oplus G_n$ (סכום ישר) במקום $G_1 \times \cdots \times G_n$. קל לראות ש־$G_1 \times \cdots \times G_n$ חילופית אם $G_1, \ldots, G_n$ חילופיות.

דוגמה 10.3: $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ היא חבורת קליין. אם $m, n \in \mathbb{N}$ זרים אז $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/mn\mathbb{Z}$ (המכפלה היא חילופית, מסדר mn, והאיבר $([1], [1])$ מסדר mn.)

למה 10.4: *תהי G חבורה סופית ו־$G_1, \ldots, G_n \lhd G$. נניח שהמספרים $|G_1|, \ldots, |G_n|$ זרים בזוגות ומתקיים $|G| = |G_1| \cdots |G_n|$. אז*

(א) $G = G_1 \times \cdots \times G_n$;

(ב) $\mathrm{Aut}(G) \cong \mathrm{Aut}(G_1) \times \cdots \times \mathrm{Aut}(G_n)$.

הוכחה:

(א) תחלה נעיר שאם $A, B \leq H$ מסדרים זרים אז $A \cap B = \{1\}$, כי $|A \cap B|$ מחלק הן את $|A|$ והן את $|B|$. אם גם $A \lhd H$, אז $AB \leq H$ מסדר $|A| \cdot |B|$, כי לפי משפט האיזומורפיזם השני $AB/A \cong B/(A \cap B)$. לכן (באינדוקציה על n):

(1) $G_1 \cdots G_n \leq G$ מסדר $|G_1| \cdots |G_n| = |G|$, לכן $G_1 \cdots G_n = G$.

(3) $G_i \cdots \widehat{G_i} \cdots G_n$ מסדר $|G_1| \cdots \widehat{|G_i|} \cdots |G_n|$, שהנו זר ל־$|G_i|$. מכאן $G_i \cap (G \cdots \widehat{G_i} \cdots G_n) = 1$.

(ב) קודם נוכיח

טענה: $\alpha(G_i) = G_i$ *לכל* $\alpha \in \mathrm{Aut}(G)$ *ולכל* i.

אכן, $\alpha(G_i)/G_i \cap \alpha(G_i) \cong \alpha(G_i)G_i/G_i \leq G/G_i$, לכן $|\alpha(G_i)/G_i \cap \alpha(G_i)|$ מחלק את

$$(G : G_i) = |G_1| \cdots \widehat{|G_i|} \cdots |G_n|$$

ולכן הנו זר ל־$|G_i|$. אך הוא גם מחלק את $|\alpha(G_i)| = |G_i|$. לכן $\alpha(G_i)/G_i \cap \alpha(G_i) = 1$, ומכאן $\alpha(G_i) = G_i \cap \alpha(G_i)$. בפרט $\alpha(G_i) \leq G_i$ ומשוויון הסדרים $\alpha(G_i) = G_i$.

מהטענה נובע שהצמצום α_i של α ל־G_i שייך ל־$\mathrm{Aut}(G_i)$. נגדיר העתקה
$\varphi(\alpha) = (\alpha_1, \ldots, \alpha_n)$ על ידי $\varphi\colon \mathrm{Aut}(G) \to \mathrm{Aut}(G_1) \times \cdots \times \mathrm{Aut}(G_n)$. אזי:

(1) φ הומומורפיזם [אם $\alpha, \beta \in \mathrm{Aut}(G)$ אז הצמצום של $\alpha\beta$ ל־G_i הוא מכפלת הצמצומים של α, β ל־G_i].

(2) φ חח"ע: אם $\varphi(\alpha) = (1, \ldots, 1)$ אז הצמצום של α ל־G_i הוא זהות ולכן α הינו זהות על $G_1 \cdots G_n = G$.

(3) φ על: אם $\alpha_i \in \mathrm{Aut}(G_i), i = 1, \ldots, n$, נגדיר העתקה $\alpha\colon G \to G$ באופן הבא:
$\alpha(g_1 \cdots g_n) = \alpha_1(g_1) \cdots \alpha_n(g_n)$ באשר $g_i \in G_i$. זוהי הגדרה טובה (כי לכל $g \in G$ יש הצגה יחידה $g = g_1 \cdots g_n, g_i \in G_i$), α הומומורפיזם (בדוק), והוא חח"ע (בדוק). לכן $\alpha \in \mathrm{Aut}(G)$ וברור ש־$\varphi(\alpha) = (\alpha_1, \ldots, \alpha_n)$. ∎

מסקנה 10.5: *יהי m טבעי ויהי $m = p_1^{n_1} \cdots p_k^{n_k}$ פירוקו לחזקות של מספרים ראשוניים שונים. אז*

$$\mathbb{Z}/m\mathbb{Z} \cong \mathbb{Z}/p_1^{n_1}\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/p_k^{n_k}\mathbb{Z}$$

ו־$\mathrm{Aut}(\mathbb{Z}/m\mathbb{Z}) \cong \mathrm{Aut}(\mathbb{Z}/p_1^{n_1}\mathbb{Z}) \times \cdots \times \mathrm{Aut}(\mathbb{Z}/p_k^{n_k}\mathbb{Z})$.

משפט 10.6:

(א) $\mathrm{Aut}(\mathbb{Z}/m\mathbb{Z}) \cong (\mathbb{Z}/m\mathbb{Z})^\times$.

(ב) $(\mathbb{Z}/p\mathbb{Z})^\times \cong \mathbb{Z}/(p-1)\mathbb{Z}$ *עבור p ראשוני.*

(ג) $(\mathbb{Z}/p^r\mathbb{Z})^\times \cong \mathbb{Z}/(p-1)\mathbb{Z} \oplus \mathbb{Z}/p^{r-1}\mathbb{Z} \cong \mathbb{Z}/p^{r-1}(p-1)\mathbb{Z}$ *מעגלית עבור p ראשוני $\neq 2$.*

(ד) $(\mathbb{Z}/2^r\mathbb{Z})^\times \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2^{r-2}\mathbb{Z}$ *עבור $r \geq 2$.*

הוכחה:

(א) נגדיר פעולה של $(\mathbb{Z}/m\mathbb{Z})^\times$ על $\mathbb{Z}/m\mathbb{Z}$ על ידי $^x y = xy$. פעולה זו מגדירה הומומורפיזם $\varphi\colon (\mathbb{Z}/m\mathbb{Z})^\times \to S(\mathbb{Z}/m\mathbb{Z})$ על ידי $\varphi(x)(y) = xy$. ההעתקה $\varphi(x)$ היא הומומורפיזם (שומרת חיבור), כי $x(y_1 + y_2) = xy_1 + xy_2$; היא תמורה, כלומר חח"ע ועל, לכן $\varphi(x) \in \mathrm{Aut}(\mathbb{Z}/m\mathbb{Z})$.
φ חח"ע: אם $x \in \mathrm{Ker}\,\varphi$ אז $xy = y$ לכל $y \in \mathbb{Z}/m\mathbb{Z}$, לכן (קח $y = [1]$) $x = [1]$.
φ על: יהי $\alpha \in \mathrm{Aut}(\mathbb{Z}/m\mathbb{Z})$. נסמן $x = \alpha([1])$ ונראה ש־$x \in (\mathbb{Z}/m\mathbb{Z})^\times$ ו־$\alpha = \varphi(x)$. לכל $y = [k] \in \mathbb{Z}/m\mathbb{Z}$ מתקים $\alpha(y) = \alpha(k[1]) = k\alpha([1]) = kx = k[1]x = yx = xy$ כלומר, $\alpha = \varphi(x)$,
בתנאי שנראה כי $x \in (\mathbb{Z}/m\mathbb{Z})^\times$. יהי $y = \alpha^{-1}([1])$, אז $xy = \alpha(y) = \alpha(\alpha^{-1}([1])) = [1]$, ולכן $x \in (\mathbb{Z}/m\mathbb{Z})^\times$.

(ב) $|(\mathbb{Z}/p\mathbb{Z})^\times| = p - 1$, ו־$(\mathbb{Z}/p\mathbb{Z})^\times$ מעגלית. (משפט שלא הוכח: כל תת חבורה סופית של החבורה הכפלית של שדה היא מעגלית.)

(ג,ד) לא נוכיח. רק נציין ש־$|(\mathbb{Z}/p^r\mathbb{Z})^\times| = p^r - p^{r-1} = (p-1)(p^r - 1)$.

דוגמה 10.7:

$$\mathrm{Aut}(\mathbb{Z}/2^2\cdot 3^3\cdot 7\mathbb{Z}) =(\mathbb{Z}/2^2\cdot 3^3\cdot 7\mathbb{Z})^\times = (\mathbb{Z}/2^2\mathbb{Z})^\times \times (\mathbb{Z}/3^3\mathbb{Z})^\times \times (\mathbb{Z}/7\mathbb{Z})^\times \cong$$

$$(\mathbb{Z}/2\mathbb{Z}) \oplus (\mathbb{Z}/2\mathbb{Z}) \oplus (\mathbb{Z}/3^2\mathbb{Z}) \oplus (\mathbb{Z}/6\mathbb{Z})$$

.

11. סדרות נורמליות.

סדרה נורמלית מאורך m של חבורה G היא סדרה סופית

$$\{1\} = G_0 \lhd G_1 \lhd \cdots \lhd G_m = G \tag{1}$$

(לא בהכרח $G_i \lhd G$ לכל i; לא בהכרח $G_{i-1} \neq G_i$). אם $G_{i-1} \neq G_i$ לכל i, אומרים שהסדרה היא **ללא חזרות**.

החבורות G_i/G_{i-1} נקראות **מנות הסדרה**.

סדרה נורמלית נוספת

$$\{1\} = H_0 \lhd H_1 \lhd \cdots \lhd H_n = G \tag{2}$$

תקרא **שקולה** ל־(1) אם לשתיהן אותו האורך ואותן המנות, עד כדי הסדר, כלומר, אם $m = n$ ואם קיימת תמורה $i \mapsto j$ של S_n כך שלכל $1 \leq i \leq n$ $G_i/G_{i-1} \cong H_j/H_{j-1}$.

(2) תקרא **עידון** של (1) אם כל ה־G_i־ים מופיעים בין ה־H_j־ים.

דוגמה 11.1: $K = \{1, (12)(34), (13)(24), (14)(23)\}$ כאן $\{1\} \lhd \langle (12)(34)\rangle \lhd K \lhd S_4$;

מנות הסדרה $\mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/2\mathbb{Z}, S_4/K \cong S_3$.

סדרה נוספת: $\{1\} \lhd A_4 \lhd S_4$; מנות הסדרה $A_4, \mathbb{Z}/2\mathbb{Z}$.

עידון לשתיהן: $\{1\} \lhd \langle (12)(34)\rangle \lhd K \lhd A_4 \lhd S_4$; מנות הסדרה $\mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/3\mathbb{Z}, \mathbb{Z}/2\mathbb{Z}$.

אם $\langle\sigma\rangle$ חבורה מעגלית מסדר 6 אז $\{1\} \lhd \langle\sigma^2\rangle \lhd \langle\sigma\rangle$, $\{1\} \lhd \langle\sigma^3\rangle \lhd \langle\sigma\rangle$ שקולות (לשתיהן מנות הסדרה $\mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/3\mathbb{Z}$), אבל אין להן עידון משותף.

משפט 11.2 (Schreier): *לכל שתי סדרות נורמליות של אותה החבורה קיימים עידונים שקולים זה לזה.*

הוכחה: תהיינה (1), (2) — לעיל — שתי סדרות נורמליות של G. נסמן $G_{i,j} = G_{i-1}(G_i \cap H_j)$, $j = 0, 1, \ldots, n$. אז

$$G_{i-1} = G_{i,0} \subseteq G_{i,1} \subseteq \cdots \subseteq G_{i,n} = G_i.$$

באופן דומה נגדיר $H_{i,j} = H_{j-1}(G_i \cap H_j)$, $i = 0, 1, \ldots, m$ אז

$$H_{j-1} = H_{0,j} \subseteq H_{1,j} \subseteq \cdots \subseteq H_{m,j} = H_j.$$

לפי למת הפרפר 7.20, $G_{i,j-1} \lhd G_{i,j}$, $H_{i-1,j} \lhd H_{i,j}$ ומתקיים

$$G_{i,j}/G_{i,j-1} \cong H_{i,j}/H_{i-1,j}. \tag{3}$$

לכן

$$\begin{array}{rcccccccc}
\{1\}=G_0= & G_{1,0} & \lhd & G_{1,1} & \lhd & \cdots & \lhd & G_{1,n} & =G_1= \\
= & G_{2,0} & \lhd & G_{2,1} & \lhd & \cdots & \lhd & G_{2,n} & =G_2= \\
\cdots= & G_{m,0} & \lhd & G_{m,1} & \lhd & \cdots & \lhd & G_{m,n} & =G_m=G \\
\{1\}=H_0= & H_{0,1} & \lhd & H_{1,1} & \lhd & \cdots & \lhd & H_{m,1} & =H_1= \\
= & H_{0,2} & \lhd & H_{1,2} & \lhd & \cdots & \lhd & H_{m,2} & =H_2= \\
\cdots= & H_{0,n} & \lhd & H_{1,n} & \lhd & \cdots & \lhd & H_{m,n} & =H_n=H
\end{array}$$

סדרות נורמליות. הן בודאי עידונים של (1), (2) בהתאמה, ויש להן mn איברים (לא כולל $\{1\}$): $\{H_{i,j},G_{i,j}\}_{i=1}^{m}{}_{j=1}^{n}$. הן שקולות לפי (3). ∎

מסקנה 11.3: *אם (1), (2) ללא חזרות, יש להן עידונים שקולים ללא חזרות.*

הוכחה: לפי המשפט לסדרות (1), (2) עידונים שקולים. נשמיט מהם איברים שמופיעים יותר מפעם אחת ("חזרות"); מנות הסדרה המתאימות להם טריוויאליות ובשני העידונים בהכרח אותו מספר של איברים כאלה, כי העידונים שקולים. לכן אחרי ההשמטה עידונים יישארו שקולים. ∎

הגדרה 11.4: **סדרת הֶרכֵּב** היא סדרה נורמלית ללא חזרות שאין לה עידון ללא חזרות (פרט לעצמה).

הערה 11.5: לחבורה סופית יש, כמובן, סדרת הרכב. ל־$\mathbb{Z}$ אין סדרת הרכב.

מהמסקנה נובע מיידית:

משפט 11.6 (Jordan-Hölder): *אם לחבורה G יש סדרת הרכב אז כל שתי סדרות הרכב שלה שקולות.*

לפי משפט זה ־ אם ל־G יש סדרת הרכב ־ מנות סדרת הרכב של G אינן תלויות בסדרת הרכב. הם נקראות **מנות ההרכב** של G.

למה 11.7: *תהי (1) סדרה נורמלית. התנאים הבאים שקולים:*

(א) *(1) סדרת הרכב.*

(ב) G_{i-1} *נורמלית מקסימלית ב־* G_i *(כלומר:* $G_{i-1}<G_i$ *ואין* $G_{i-1}<H<G_i$ *כך ש־*$H\lhd G_i$*),* $i=1,\ldots m$.

(ג) $G_i/G_{i-1}\neq\{1\}$ *חבורה פשוטה,* $i=1,\ldots m$.

הוכחה:

(א) $\Leftrightarrow$ (ב): ברור.

(ב) $\Leftrightarrow$ (ג): לפי משפט האיזומורפיזם השלישי

$$\text{(ב)}\Leftrightarrow G_{i-1}/G_{i-1}<G_i/G_{i-1}\text{ ואין }G_{i-1}/G_{i-1}<B<G_i/G_{i-1}\text{ כך ש־}B\lhd G_i/G_{i-1}$$

$$\Leftrightarrow\{1\}<G_i/G_{i-1}\text{ ואין }\{1\}<B<G_i/G_{i-1}\text{ כך ש־}B\lhd G_i/G_{i-1}\Leftrightarrow\text{(ג)}$$

תרגיל 11.8: *חבורה חילופית G היא פשוטה אם ורק אם היא מעגלית מסדר ראשוני.*

(אם היא פשוטה, יהי $1\neq g\in G$. אז $1<\langle g\rangle\lhd G$, לכן $G=\langle g\rangle$. אם $\operatorname{ord}(g)$ אינו ראשוני (או אם הוא אינסופי), יש ל־G חבורה חלקית ממש.

הגדרה 11.9: חבורה (סופית) נקראת **פתירה** אם כל מנות ההרכב שלה חילופיות.

למה 11.10: *תהי G חבורה סופית ותהי $K \triangleleft G$. אז G פתירה אם ורק אם $K, G/K$ פתירות.*

הוכחה: בלי הגבלת הכלליות $K \neq \{1\}, G$, אחרת הטענה טריוויאלית. די להראות שסדרת מנות ההרכב של G היא הצירוף של סדרת מנות ההרכב של K סדרת מנות ההרכב של G/K.

לסדרה $\{1\} \triangleleft K \triangleleft G$ יש עידון לסדרת הרכב, כלומר, סדרת הרכב (1), בה $G_k = K$ עבור איזה $0 < k < m$. אז $K = G_k \triangleleft G_{k+1} \triangleleft \cdots \triangleleft G_m = G$ סדרת הרכב של K שמנותיה $G_1/G_0, \ldots, G_k/G_{k-1}$, ואילו

$$\{1\} = K/K = G_k/K \triangleleft G_{k+1}/K \triangleleft \cdots \triangleleft G_m/K = G/K \tag{4}$$

היא סדרה נורמלית שמנותיה, לפי משפט האיזומורפיזם השלישי, הן $G_{k+1}/G_k, \ldots, G_m/G_{m-1}$. הן מנות של (1), לכן לפי למה 11.10 הן פשוטות, ולכן, שוב לפי למה 11.10, (4) היא סדרת הרכב של G/K. ∎

משפט 11.11 (Feit-Thompson, 1963): *כל חבורה מסדר אי זוגי הנה פתירה.*

לא ניתן הוכחה למשפט זה (וגם לא נסתמך עליו בעתיד.) ההוכחה המקורית שלו משתרעת על פני 255 עמודים. עד כמה שידוע לי, לא הצליחו לקצר אותה מאז באופן משמעותי.

מהמשפט נובע בפרט, שכל חבורה סופית פשוטה לא חילופית הינה מסדר זוגי.

הערה 11.11: מיון חבורות סופיות פשוטות. שאלה חשובה במתמטיקה היתה, מהן כל החבורות הסופיות הפשוטות ("מיון החבורות הפשוטות"). מלבד החבורות המעגליות מסדר ראשוני ומלבד $\{A_n\}_{n=5}^{\infty}$ ידועות עוד כמה משפחות אינסופיות של חבורות פשוטות. (למשל החבורות $\mathrm{PSL}(n,q) = \mathrm{SL}_n(\mathbb{F}_q)/Z$ עבור $n > 2$ או $q > 3$, באשר $\mathbb{F}_q$ שדה בן q איברים ו־Z היא חבורת המטריצות הסקלריות בתוך $\mathrm{SL}_n(\mathbb{F}_q)$.) בנוסף אליהן היו ידועות עוד חבורות פשוטות בודדות ("ספוראדיות").

תוך כדי המאמץ להוכיח שאלה כל החבורת הסופיות הפשוטות, מצאו חוקרים במחצית השניה של המאה ה־20 חבורות ספוראדיות נוספות, 26 בסך הכל.

משפט Feit-Thompson היה אבן דרך במיון החבורות הפשוטות.

בתחילת שנות ה־80 הודיע צוות של מתמטיקאים שהם הצליחו במשימה זו: החבורות הפשוטות המוכרות הן כל החבורות הפשוטות.

יש לציין שעדיין אין הוכחה כתובה **מלאה** (אולי בגלל שרוב המומחים עזבו את השטח מאז שהוא איבד מיוקרתו) ולכן יש כאלה שאינם מקבלים את המיון כסגור (בעקר חתן פרס וולף ז'אן־פייר סֶר).

.

12. חבורות־p.

יהי p מספר ראשוני. חבורה G נקראת **חבורת־p** אם $|G|$ הוא חזקה של p. בפרט G כזו סופית.

למה 12.1: *חבורה חלקית וחבורת מנה של חבורת־p היא חבורת־p. מכפלה ישרה של חבורות־p היא חבורת־p.*

משפט 12.2: *תהי $G \neq \{1\}$ חבורת־p. אז $Z(G) \neq \{1\}$ (=המֶרכז של G).*

הוכחה: לפי נוסחת המחלקות (מסקנה 8.11) $|G| = \sum_{i\in I'}(G : C_G(x_i)) + |Z(G)|$, באשר $\{x_i\}_{i\in I'}$ היא מערכת מיצגים של מחלקות הצמידות ב־G בעלות יותר מאבר אחד. גם $|G|$ וגם $(G : C_G(x_i))$ הם חזקות של p, לא טריוויאליות (כי $x_i \notin Z(G)$, לכן $C_G(x_i) \neq G$), לכן הם מתחלקים ב־p. מכאן ש־$|Z(G)|$ מתחלק ב־p, ובפרט $Z(G) \neq \{1\}$. ∎

מסקנה 12.3: *כל חבורה G מסדר p^2 היא חילופית.*

הוכחה: יהי $1 \neq a \in Z(G)$. אם $G = \langle a\rangle$ אז G מעגלית ולכן חילופית. אחרת יש $b \in G \setminus \langle a\rangle$. אז $\{1\} < \langle a\rangle < \langle a, b\rangle \leq G$. היות ו־$|G| = p^2$, גם $|\langle a, b\rangle| = p^2$, ולכן $\langle a, b\rangle = G$. הואיל ו־$ab = ba$, G חילופית. ∎

למה 12.4: *תהי G חבורת־p ותהי $U < G$. אזי $U < N_G(U) = \{g \in G |\ g^{-1}Ug = U\}$.*

הוכחה: ברור ש־$U \leq N_G(U)$. לכן די למצוא $g \in G \setminus U$ כך ש־$g^{-1}Ug = U$.

נגדיר פעולה של U על הקבוצה $X = \{gU |\ g \in G\}$ על ידי הכפל משמאל: $\pi(u, gU) = ugU$. לפי מסקנה 8.9

$$|X| = \sum_{i\in I'}(U : U_{x_i}) + |X_0|,$$

באשר $X_0 = \{gU \in X |\ u \in U \text{ לכל } ugU = gU\}$ ו־$\{x_i\}_{i\in I'}$ מיצגים מסלולי־U מאורך $(U : U_{x_i}) > 1$. גם $|X| = (G : U) > 1$, כי $U < G$. כמו כן $(U : U_{x_i})$ מחלק את $|U|$ ולכן את $|G|$, וגם $|X| = (G : U)$ מחלק את $|G|$, לכן שניהם חזקות של p. לכן שניהם חזקות לא טריוויאליות של p, ובפרט מתחלקים ב־p. מכאן שגם $|X_0|$ מתחלק ב־p, ובפרט $|X_0| \geq 2$.

כיוון שבבירור $U = eU \in X_0$, זה אומר שיש $g \in G$ כך ש־$gU \neq U$ ו־$ugU = gU$ לכל $u \in U$.

התנאי הראשון אומר ש־$g \in G \setminus U$. התנאי השני שקול ל־$g^{-1}Ug = U$:

$$ugU = gU \text{ לכל } u \in U \Leftrightarrow g^{-1}ug \in U \text{ לכל } u \in U \Leftrightarrow g^{-1}Ug \subseteq U \Leftrightarrow g^{-1}Ug = U$$

כאשר השקילות הראשונה (מימין) נובעת מלמה 5.8, והאחרונה מכך ש־$|U| = |g^{-1}Ug|$. ∎

משפט 12.5: *תהי G חבורת־p ותהי U חבורה חלקית מרבית שלה (כלומר $U < G$ ואין $U < H < G$). אזי*

(א) $U \triangleleft G$.

(ב) $(G : U) = p$.

(ג) *ל־G סדרת הרכב שכל גורמיה מעגליים מסדר p. בפרט G פתירה.*

הוכחה:

(א) לפי הלמה $U < N_G(U) \leq G$, לכן $N_G(U) = G$, כלומר $U \triangleleft G$.

(ב) G/U חבורת־p שונה מ־$\{1\}$, וחבורות חלקיות שלה מתאימות לפי משפט האיזומורפיזם השלישי לחבורות חלקיות של G המכילות את U. לכן אין לה חבורה חלקית לא טריוויאלית. מכאן ש־G/U מעגלית (כי כל חבורה חלקית $\{1\} \neq$ מעגלית שלה שווה לה) מסדר ראשוני (כי לחבורה מעגלית יש תת חבורה מסדר d לכל מחלק d של סדרה), כלומר מסדר p (כי היא חבורת־p).

(ג) באינדוקציה נבנה סדרה $G = U_0 > U_1 > \cdots > U_n = \{1\}$, באשר U_i מרבית ב־U_{i-1}. לפי (א) ו־(ב) זוהי סדרת הרכב. ∎

13. חבורות סילוב (Sylow)

יהי p מספר ראשוני ותהי G חבורה סופית. חבורה חלקית $P \leq G$ נקראת **חבורת סילוב־p** של G אם $|P|$ הוא החזקה המרבית של p אשר מחלקת את $|G|$, ז.א., אם $|G| = p^n m$ ו־m זר ל־p אז $|P| = p^n$. כלומר, P חבורת־p ו־$(G : P)$ זר ל־p. בפרט אם $|G|$ זר ל־p אז P חבורת סילוב־p אם ורק אם $P = \{1\}$.

למה 13.1: *תהי G חבורה **חילופית** סופית. אם p מחלק את $|G|$ אז יש איבר ב־G מסדר p.*

הוכחה: די להוכיח שיש $g \in G$ כך ש־$p \big| \operatorname{ord} g$, כי אז, לפי למה 6.5(ד), $g^{(\operatorname{ord} g)/p}$ הוא מסדר p.

תהי $H \leq G$ תת חבורה מסדר מרבי שסדרה זר ל־p. אז $H \neq G$, לכן יש $g \in G \setminus H$. אז $H < H\langle g \rangle$, לכן $p \big| |H\langle g \rangle|$. מכאן

$$p \Big| \frac{|H\langle g \rangle|}{|H|} = |H\langle g \rangle / H| = |\langle g \rangle / H \cap \langle g \rangle| = \frac{|\langle g \rangle|}{|H \cap \langle g \rangle|} \Big| |\langle g \rangle| = \operatorname{ord} g \qquad \blacksquare$$

משפט 13.2 (המשפט הראשון של סילוב)**:** *לכל חבורה סופית G יש חבורת סילוב־p.*

הוכחה: באינדוקציה על $|G|$. המקרה $|G| = \{1\}$ טריוויאלי.

(א) אם קיימת $N \lhd G$ כך ש־$N \neq \{1\}$ חבורת־p אז לפי הנחת האינדוקציה יש ל־G/N חבורת סילוב־p; לפי משפט האיזומ' השלישי חבורה זו מהצורה P/N באשר $N \leq P \leq G$. כעת P חבורת־p (כי $P/N, N$ חבורות־p) ו־$(G : P) = (G/N : P/N)$ זר ל־p, לכן P חבורת סילוב־p של G.

(ב) אם קיימת $H < G$ כך ש־$(G : H)$ זר ל־p אז לפי הנחת האינדוקציה יש ל־H חבורת סילוב־p P; היא חבורת־p ו־$(G : P) = (G : H) \cdot (H : P)$ זר ל־p, לכן P גם חבורת סילוב־p של G.

(ג) נניח איפוא ש־$|G| > 1$ ושלכל $H < G$ מתקיים $p \big| (G : H)$. בפרט $p \big| |G| = (G : 1)$ ואם $x \in G \setminus Z(G)$ אז $C_G(x) < G$ ולכן $p \big| (G : C_G(x))$. מנוסחת המחלקות: $|G| = \sum_{i \in I'} (G : C_G(x_i)) + |Z(G)|$ נובע ש־$p \big| |Z(G)|$. המרכז הוא חבורה חילופית, לכן לפי הלמה יש $N \leq Z(G)$ מסדר p. אך $N \lhd G$, כי לכל $n \in N$ ולכל $g \in G$ מתקיים $g^{-1}ng = n \in N$. לפי (א) סיימנו. $\blacksquare$

דוגמה 13.3: ל־S_6 יש חבורה חלקית מסדר 9 וחבורה חלקית מסדר 16. ($|S_6| = 6! = 720 = 2^4 \cdot 3^2 \cdot 5$.)

משפט 13.4: *תהי G חבורה סופית.*

(א) *אם H חבורת־p חלקית של G אז H מוכלת בחבורת סילוב־p של G.*

(ב) (המשפט השני של סילוב) *כל חבורות סילוב־p של G צמודות זו לזו.*

(ג) (המשפט השלישי של סילוב) *יהי $n_p(G)$ מספר חבורות סילוב־p של G. אז $n_p(G) \equiv 1 (\bmod p)$.*

הוכחה:

(א) נראה (כביכול) קצת יותר:

(א') תהי P חבורת סילוב־p של G. אז יש $g \in G$ כך ש־$H \leq P^g$ (וכמובן, גם P^g חבורת סילוב־p).

טענה 1: יהי $X = \{ {}^gP := gPg^{-1} = P^{g^{-1}} \mid g \in G\}$. אז $|X|$ זר ל־p. אכן, G פועלת על X על ידי ההצמדה. ברור ש־X היא מסלול־G (של P), ולכן $|X| = (G : G_P)$, באשר $G_P = \{g \in G|\ {}^gP = P\} = N_G(P)$. אבל $P \leq G_P \leq G$, לכן $(G : G_P)$ זר ל־p, לכן $|X| = (G : G_P)$ זר ל־p.

חלק 2: חבורת־p H פועלת על X על ידי ההצמדה. לכן $X = \bigcup_{i \in I} X_i$ באשר X_i מסלול־H, ואם $P_i \in X_i$ אז $|X_i| = (H : H_{P_i})$. לכן $|X_i|$ חזקה של p. אבל $|X| = \sum_i |X_i|$, לכן לפי (1) יש $i \in I$ כך ש־$|X_i| = 1$.

טענה 3: $H \leq P_i \Leftrightarrow |X_i| = 1$. אכן, אם $H \leq P_i$ אז ${}^hP_i = P_i$ לכל $h \in H$, לכן $X_i = \{P_i\}$.
להיפך, נניח $|X_i| = 1$, אז

$$H = H_{P_i} = \{h \in H|\ {}^hP_i = P_i\} \leq \{g \in G|\ {}^gP_i = P_i\} = N_G(P_i).$$

אבל $P_i \lhd N_G(P_i)$, לכן $HP_i = \langle H, P_i\rangle \leq G$. כעת $|HP_i| = |H||P_i|/|H \cap P_i|$ הוא חזקה של p. אך P_i חבורת סילוב־p של G ו־$P_i \leq HP_i$, לכן בהכרח $P_i = HP_i$. מכאן $H \leq P_i$.

חלק 4: לפי (2), (3) יש i כך ש־$H \leq P_i$ (ו־$P_i \in X$). זה מוכיח את (א').

כדי להוכיח את (ב) ו־(ג) נניח עתה כי H חבורת סילוב־p של G (ואז $|H| = |P| = |P_i|$).

(ב) לפי (א') יש $g \in G$ כך ש־$H \leq {}^gP$. משוויון הסדרים נובע $H = {}^gP$.

(ג) בגלל שוויון הסדרים נובע מ־(3) $H = P_i \Leftrightarrow |X_i| = 1$, לכל $i \in I$. לכן יש i_0 יחיד כך ש־$|X_{i_0}| = 1$ ו־$|X_i| \neq 1$ לכל $i \neq i_0$. אך $|X_i|$ חזקה של p, לכן $p \big| |X_i|$ לכל $i \neq i_0$. מכאן $|X| = \sum_i |X_i| \equiv 1 (\bmod p)$. ∎

הערה 13.5: תהי P חבורת סילוב־p של G. אז $n_p(G) = (G : N_G(P))$ ובפרט $n_p(G) \big| (G : P)$.
(את החלק הראשון ראינו בהוכחת טענה 1, כאשר לפי (ב) $|X| = n_p(G)$. החלק השני נובע מכך ש־$P \leq N_G(P) \leq G$ ולכן $(G : N_G(P))$ מחלק את $(G : P)$.) זה נותן מידע נוסף אודות $n_p(G)$ על (ג) לעיל. שים לב ש־1 הוא מועמד ל־$n_p(G)$ לפי שני התנאים גם יחד.

הערה 13.6: $n_p(G) = 1$ אם ורק אם יש חבורת סילוב־p נורמלית ב־G.

דוגמה 13.7: כמה חבורות מסדר 5 יש ב־S_5? ־ ($|S_5| = 120 = 5 \cdot 24$.) לפי הערה 13.5 מספרן מחלק את 24 ולפי המשפט הוא אחד מהמספרים $1, 6, 11, 16, 21, 26, \ldots$. לכן הוא 6 או 1. אם הוא היה 1, כל איבר מסדר 5 היה מוכל בתת החבורה היחידה מסדר 5 (בה יש בדיוק 4 איברים מסדר 5) ולכן היו רק 4 איברים מסדר 5 ב־S_5. אך יש $4! = 24$ חישוקים מאורך 5 ב־S_5. לכן $n_5(S_5) = 6$.

דוגמה 13.8: כמה חבורות מסדר 8 יש ב־S_4? ־ לפי הערה 13.5 מספרן מחלק את 3, לכן הנו 1 או 3. (לפי משפט סילוב השלישי הוא אי זוגי; אך זה ידענו גם בלי המשפט.) חישוב קל מראה שיש 16 איברים מסדר $2, 4, 8$ או 1. (ביתר פירוט: 6 חישוקים מאורך 4; 3 מכפלות של שני חישוקים זרים; 6 חישוקונים; 1 זהות.) לפי המשפט, כל אחד מהם מוכל באיזו חבורת סילוב־2 (מסדר 8), ולכן יש יותר מחבורת סילוב־2 אחת. מספרן איפוא 3. (שים לב שלא יתכן שחיתוך כל שתים מבין שלושתן הוא $\{1\}$, כי אז היו $3 \cdot 7 = 21$ איברים לא טריוויאליים בשלושתן; אך יש רק 15 כאלה.)

למה 13.9: *תהי G חבורה סופית ו־$N \triangleleft G$. תהי P חבורת סילוב־p של G. אזי*

(א) *$P \cap N$ היא חבורת סילוב־p של N.*

(ב) *PN/N היא חבורת סילוב־p של G/N.*

הוכחה: מתקיים $P \leq PN \leq G$. לפי לגרנז' $(G : P) = (G : PN)(PN : P)$ זר ל־p, לכן

(1) $(G : PN), (PN : P)$ זרים ל־p.

לפי משפט האיזומורפיזם השני

(2) $PN/N \cong P/(P \cap N)$ ובפרט $|PN|/|N| = |P|/|P \cap N|$.

(א) $P \cap N \leq P$, לכן $P \cap N$ חבורת־p. לפי (2)

$$(N : (P \cap N)) = |N|/|P \cap N| = |PN|/|P| = (PN : P),$$

לכן לפי (1) $(N : (P \cap N))$ זר ל־p.

(ב) $P/(P \cap N)$ היא מנה של חבורת־p ולכן חבורת־p. לפי (2) גם PN/N חבורת־p. כעת

$$(G/N : PN/N) = (G : PN),$$

לכן לפי (1) $(G/N : PN/N)$ זר ל־p. ∎

תרגיל 13.10: *תהי G חבורה מסדר pq, באשר p, q שני ראשוניים שונים. אזי*

(א) *G פתירה.*

(ב) *אם $q < p$ ו־$q \nmid p - 1$ אזי $G \cong \mathbb{Z}/pq\mathbb{Z}$.*

פתרון: בה"כ $q < p$. ל־G חבורה P מסדר p וחבורה Q מסדר q.

(א) $n_p(G) \mid (G : P) = pq/p = q$ ו־$n_p(G) \equiv 1 \pmod{p}$. מכאן $n_p(G) = 1$. לכן $P \triangleleft G$. כעת $P, G/P$ מסדרים ראשוניים, לכן מעגליות, ולכן G פתירה.

(ב) היות ו־p ראשוני, $n_q(G) \mid (G : Q) = pq/q = p$ ו־$n_q(G) = 1$ או $n_q(G) = p$. אם $n_q(G) = p$, אז $p \equiv 1 \pmod{q}$, בסתירה לנתון. לכן $n_q(G) = 1$, כלומר, $Q \triangleleft G$. לפי למה 10.4(א), $G = Q \times P$. מכאן לפי מסקנה 10.5, $G = Q \times P \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z} \cong \mathbb{Z}/pq\mathbb{Z}$. ∎

תרגיל 13.11: *כל חבורה G מסדר 12 הנה פתירה.*

הוכחה: אם חבורת סילוב־3 של G נורמלית –סיימנו. אחרת יש בדיוק 4 כאלה. זה נותן $4 \cdot 2 = 8$ איברים מסדר 3. נותרו עוד 4 איברים. היות ובכל חבורת סילוב־2 של G יש 4 איברים שלא מסדר 3, יש רק חבורת סילוב־2 אחת; ושוב ־ סיימנו.

תרגיל 13.12: *כל חבורה G מסדר $2^m \cdot 3$ הנה פתירה.*

פתרון: באינדוקציה על m. עבור $m = 0, 1$ זה ברור. נניח $m \geq 2$. תהי $P \leq G$ חבורת סילוב־2. אז $(G : P) = 3$ ו־ $|G| = 2^m \cdot 3 \nmid 6 = 3!$, לכן לפי מסקנה 8.13 יש $K \lhd G$ לא טריוויאלית, $K \leq P$. אז $|K|, |G/K| < |G|$, לכן $K, G/K$ פתירות (G/K לפי הנחת האינדוקציה ו־K חבורת־2), ולפי למה 11.10 גם G פתירה.

תרגיל 13.13: *יהי $0 \leq m \leq 3$. כל חבורה G מסדר $2^m \cdot 3^n$ הנה פתירה.*

פתרון: באינדוקציה על n (לכל m). עבור $n = 0, 1$ זה ברור (או ש־G חבורת־2 או לפי התרגיל הקודם). נניח $n \geq 2$. תהי $P \leq G$ חבורת סילוב־3. אם $P \lhd G$ אז $P, G/P$ פתירות כחבורות־p, ולכן G פתירה. אחרת יש בדיוק 4 חבורות סילוב־3 (ו־ $m = 2$ או $m = 3$). G פועלת עליהן על ידי ההצמדה, וזה נותן הומומורפיזם $\psi\colon G \to S_4$ [$\psi(g)(P_i) = gP_ig^{-1}$]. יהי $K = \operatorname{Ker}\psi$. אז $\psi(G) \neq \{id\}$, כי ארבע חבורות סילוב־2 צמודות זו לזו. כמו כן $K \neq \{1\}$, כי $|G| \geq 2^2 \cdot 3^2 = 36 > |S_4|$. לכן $K, G/K$ פתירות (לפי הנחת האינדוקציה), ולכן (למה 11.10) גם G פתירה.

תרגיל 13.14: *כל חבורה G מסדר 90 אינה פשוטה. (ואז, בהנחה שכל חבורה מסדר שמחלק ממש 90 הנה פתירה, גם G פתירה).*

הוכחה: בה"כ לכל $p \big| 90$ ראשוני מספר חבורות סילוב־p אינו 1. לכן יש 6 חבורות סילוב־5 (=24 איברים מסדר 5); יש 10 חבורות סילוב־3 (והן מסדר 9, לכן חילופיות), וחיתוך כל שתיים מהן לא יכול להיות $\{1\}$, כי אז היו 80 איברים מסדר 3 או 9, סתירה. תהיינה איפוא $P_1, P_2 \leq G$ שתי חבורות סילוב־3 כך ש־$|P_1 \cap P_2| = 3$. אז $P_1 \cap P_2 \lhd P_1, P_2$, לכן $P_1 \cap P_2 \lhd H := \langle P_1, P_2 \rangle$.

(א) אם $H = G$ אז $P_1 \cap P_2 \lhd G$ –וסיימנו.

(ב) אם $(G : H) = 2$ אז $H \lhd G$ –וסיימנו.

(ג) אם $(G : H) = 5$ אז, כיוון ש־ $|G| = 90 \nmid 120 = 5!$, לפי מסקנה 8.13 יש $K \lhd G$ כך ש־$1 \neq K \leq H$; בפרט $K \neq G$. ∎

משפט 13.15 (משפט קושי): *תהי G חבורה סופית. אם p מחלק את $|G|$ אז יש איבר $g \in G$ מסדר p.*

הוכחה: תהי P חבורת סילוב־p של G. לפי ההנחה, $P \neq \{1\}$. נבחר $1 \neq g \in P$. אז $\operatorname{ord}(g) \big| |P|$ חזקה של p ו־$\operatorname{ord}(g) \neq 1$. לכן $p | \operatorname{ord}(g)$. לפי למה 6.5(ד), $g^{\frac{\operatorname{ord} g}{p}}$ מסדר p. ∎

משפט 13.16: *יהי F שדה ותהי G תת חבורה סופית של החבורה הכפלית $F^\times$ של F. אז G מעגלית.*

הוכחה: כיוון ש־$F^\times$ חילופית, גם G חילופית. בפרט כל תת חבורה שלה נורמלית ב־G.

יהי $|G| = p_1^{n_1} \cdots p_r^{n_r}$ הפירוק של $|G|$ לחזקות של מספרים ראשוניים שונים. לכל i תהי G_i חבורת סילוב־p_i של G. אז G_i מסדר $p_i^{n_i}$. לפי למה 10.4(א), $G = G_1 \times \cdots \times G_r$. אם נראה שכל G_i היא מעגלית, אז $G_i \cong \mathbb{Z}/p_i^{n_i}\mathbb{Z}$, ולפי מסקנה 10.5, $G \cong \mathbb{Z}/p_1^{n_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_r^{n_r}\mathbb{Z} \cong \mathbb{Z}/p_1^{n_1} \cdots p_r^{n_r}\mathbb{Z}$ מעגלית. לכן די להניח כי G חבורת־p.

יהי $g \in G$ בעל הסדר הגדול ביותר. הסדר הזה מחלק את $|G|$, לכן הוא חזקה של p, נאמר, $\operatorname{ord}(g) = p^r$. יהי $x \in G$, אז $\operatorname{ord}(x)$ גם חזקה של p, אבל $\operatorname{ord}(x) \le p^r$, ולכן $\operatorname{ord}(x) | p^r$. מכאן ש־$x^{p^r} = 1$, ולכן x הוא שרש של הפולינום $X^{p^r} - 1 \in F[X]$. אך לפולינום זה לכל היותר p^r שרשים שונים ב־F (משפט שלומדים בדרך כלל באלגברה לינארית 2), לכן $|G| \le p^r$. כיוון ש־$p^r = \operatorname{ord}(g) || G|$, יוצא ש־$|G| = p^r = \operatorname{ord}(g) = |\langle g \rangle|$. מכאן שההכלה $\langle g \rangle \le G$ היא שוויון. לכן G מעגלית. ∎

תרגיל 13.17 (הטיעון של Frattini): *תהי G חבורה סופית, $N \lhd G$, ו־P חבורת סילוב־p של N. אז $G = N_G(P)N$.*

הוכחה: יהי $g \in G$. אז $P^g \le N^g = N$ גם חבורת סילוב־p של N, לכן לפי משפט סילוב השני יש $n \in N$ כך ש־$P^g = P^n$. מכאן $P^{gn^{-1}} = P$. לכן $gn^{-1} \in N_G(P)$. בפרט $g \in N_G(P)N$. ∎

14. החבורות חילופית (חפשיות) נוצרות סופית

תהי A חבורה חילופית (בכתיב חיבורי).

הגדרה 14.1: (א) $A^t = \{a \in A | \operatorname{ord} a < \infty\}$ נקראת **חבורת הפיתול של** A.

(ב) A נקראת **חבורת פיתול** אם $A = A^t$.

(ו) A נקראת **חסרת פיתול** אם $A^t = \{0\}$.

למה 14.2: *(א)* $A^t \leq A$ *תת חבורה.*

(ב) A/A^t *חסרת פיתול.*

(ג) *אם* A *חבורת פיתול חילופית נוצרת סופית אז* A *סופית.*

הוכחה: (בכתיב חיבורי!)

(א) ברור ש־$0 \in A^t$. יהיו $a, b \in A^t$. אז יש $m, n \in \mathbb{N}$ כך ש־$ma = nb = 0$. מכאן

$$mn(a+b) = mna + mnb = n(ma) + m(nb) = 0,$$

לכן $a + b \in A^t$. כמו כן $m(-a) = -(ma) = -0 = 0$, לכן $-a \in A^t$.

(ב) צריך להוכיח לכל $a \in A$: אם $a + A^t$ מסדר $n < \infty$ ב־A/A^t אז $a + A^t = A^t$, כלומר $a \in A^t$. ואכן, $n(a + A^t) = A^t$, לכן $na \in A^t$, כלומר, יש $m \in \mathbb{N}$ כך ש־$m(na) = 0$. מכאן $a \in A^t$.

(ג) באינדוקציה על מספר היוצרים n של A. אם $A = \langle a \rangle$ אז A מעגלית ו־$|A| = \operatorname{ord}(a) < \infty$.

נניח $A = \langle a_1, \ldots, a_n \rangle$. לפי הנחת האינדוקציה $B = \langle a_1, \ldots, a_{n-1} \rangle$ סופית. כעת $A = B + \langle a_n \rangle$, לכן לפי משפט האיזומורפיזם השני $|A/B| = |\langle a_n \rangle / B \cap \langle a_n \rangle| \leq |\langle a_n \rangle| < \infty$. מכאן לפי נוסחת לגרנז' $|A| = (A : B) \cdot |B| < \infty$. ∎

דוגמאות 14.3: (א) כל חבורה חילופית סופית היא חבורת פיתול.

(ב) $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{Z} \oplus \mathbb{Z}$ חסרות פיתול.

(ג) $\mathbb{Q}/\mathbb{Z}$ חבורת פיתול אינסופית (לכל $\frac{m}{n} \in \mathbb{Q}$ מתקיים $n\frac{m}{n} = m \in \mathbb{Z}$).

(ד) $\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ אינה חבורת פיתול ואינה חסרת פיתול.

הגדרה 14.4: תהי F חבורה חילופית. סדרה $v_1, \ldots, v_n$ של איברי F היא

(א) **סדרת יוצרים** של F אם לכל $v \in F$ יש הצגה מהצורה

$$v = m_1 v_1 + \cdots + m_n v_n \quad , m_1, \ldots, m_n \in \mathbb{Z} \tag{1}$$

(זוהי הגדרה 5.14, עבור חבורות חילופיות; ראה גם למה 5.16.)

(ב) **בלתי תלויה** אם לכל $v \in F$ יש לכל היותר הצגה אחת (1).

(ג) **בסיס** של F אם לכל $v \in F$ יש הצגה יחידה (1).

חבורה חילופית נוצרת סופית F נקראת **חפשית** אם יש לה בסיס.

משפט 14.5: *תהי F חפשית עם בסיס $v_1, \dots, v_n$. תהי A חילופית ויהיו $a_1, \dots a_n \in A$. אזי קיים הומומורפיזם יחיד $\varphi\colon F \to A$ כך ש־$\varphi(v_i) = a_i$ לכל i. בפרט, אם $A = \langle a_1, \dots a_n \rangle$ אז $A \cong F/\operatorname{Ker}\varphi$.*

הוכחה: נגדיר φ על ידי $\varphi(m_1v_1 + \cdots + m_nv_n) = m_1a_1 + \cdots + m_na_n$, לכל $m_1, \dots, m_n \in \mathbb{Z}$. זוהי הגדרה טובה, לפי הגדרת בסיס. ברור ש־φ הומומורפיזם, ויחיד כך ש־$\varphi(v_i) = a_i$ לכל i. ∎

למה 14.6: *תהי F חבורה חילופית. סדרה $v_1, \dots, v_n$ בסיס של F אם ורק אם*

(2) $F = \langle v_1 \rangle \oplus \cdots \oplus \langle v_n \rangle$ ו־

(3) $\langle v_i \rangle \cong \mathbb{Z}$ *לכל i.*

הוכחה: לפי משפט 10.1(ג), (2) שקול ל־

(א) $F = \langle \langle v_1 \rangle, \dots, \langle v_n \rangle \rangle$. [כלומר: לכל $v \in F$ הצגה (1), אולי לא יחידה.]

(ב) $g_ig_j = g_jg_i$ לכל $g_i \in \langle v_i \rangle$, $g_j \in \langle v_j \rangle$, עבור $i \neq j$; [מתקיים כי F חילופית.]

(ג) אם $x_1 + \cdots + x_n = y_1 + \cdots + y_n$ באשר $x_i, y_i \in \langle v_i \rangle$ אז $x_i = y_i$ לכל i; כלומר

(ג′) אם $m_1'v_1 + \cdots + m_n'v_n = m_1v_1 + \cdots + m_nv_n$ אז $m_i'v_i = m_iv_i$ לכל i.

ואילו (3) שקול ל־$\operatorname{ord} v_i = \infty$, כלומר $k_iv_i = 0 \Leftarrow k_i = 0$, כלומר

(3′) אם $m_i'v_i = m_iv_i$ אז $m_i' = m_i$.

כעת, (א) שקול לקיום ההצגה (1) [אך לא ליחידותה] ואילו (ג′) + (3′) $\Leftrightarrow$ היחידות של (1). (עבור $\Rightarrow$ קח $m_j = 0$ לכל $j \neq i$.) (עבור (1) $\Leftarrow$ (3′) קח $m_j = 0$ לכל $j \neq i$.) ∎

מסקנה 14.7: *חבורה חילופית F חפשית אם ורק אם $F \cong F_n := \overbrace{\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}}^{n}$.*

תרגיל 14.8: *תהי F חילופית ותהי $v_1, v_2, \dots, v_n$ סדרת יוצרים [בסיס] של F. יהיו $k_2, \dots, k_n \in \mathbb{Z}$. אז גם*

$$v_1 + k_2v_2 + \cdots + k_nv_n, v_2, \dots, v_n$$

סדרת יוצרים [בסיס] של F.

פתרון: יהי $v \in A$. עלינו להוכיח שיש $m_1', \dots, m_n' \in \mathbb{Z}$ [יחידים] כך ש־

$$\begin{aligned} v &= m_1'(v_1 + k_2v_2 + \cdots + k_nv_n) + m_2'v_2 + \cdots + m_n'v_n \\ &= m_1'v_1 + (k_2m_1' + m_2')v_2 + \cdots + (k_nm_1' + m_n')v_n \end{aligned} \tag{4}$$

ואכן, יש $m_1, \dots, m_n \in \mathbb{Z}$ [יחידים] כך שמתקיים (1). נגדיר

$$\begin{aligned} m_1' &= m_1 \\ m_2' &= m_2 - k_2m_1 \\ \cdots &\quad \cdots \\ m_n' &= m_n - k_nm_1 \end{aligned}$$

ואז מתקיים (4). [וכאשר (1) הצגה יחידה, זאת ההגדרה היחידה האפשרית.] ∎

משפט 14.9: *אם A חבורה חילופית נוצרת סופית וחסרת פיתול אז A חפשית.*

הוכחה: יהי n מזערי עבורו יש סדרת יוצרים בת n איברים ל־A. נראה שיש בסיס בן n איברים.

אחרת לכל סדרת יוצרים $v_1, \ldots, v_n$ יש $m_1, \ldots, m_n \in \mathbb{Z}$, לא כולם 0, כך ש־

$$m_1 v_1 + \cdots + m_n v_n = 0.$$

נבחר סדרת יוצרים $v_1, \ldots, v_n$ עם $\delta(v_1, \ldots, v_n) := |m_1| + \cdots + |m_n|$ מזערי.

אם יש i יחיד כך ש־$m_i \neq 0$, אז $m_i v_i = 0$ ולכן $v_i = 0$ (A חסרת פתול). אז גם $v_1, \ldots, \widehat{v_i} \ldots, v_n$ סדרת יוצרים, סתירה למזעריות של n.

אם i כזה אינו יחיד, אז בה"כ $m_1, m_2 \neq 0$. בה"כ $|m_1| \leq |m_2|$ ובה"כ $m_1 > 0$ (אחרת נכפיל כל m_i ב־(-1)). חילוק עם שארית נותן

$$m_2 = m_1 q + r, \qquad 0 \leq r < m_1 = |m_1| \leq |m_2|.$$

לכן

$$m_1(v_1 + q v_2) + r v_2 + m_3 v_3 + \cdots + m_n v_n = 0$$

ולפי תרגיל 14.8 גם $v_1 + q v_2, v_2, v_3, \ldots, v_n$ סדרת יוצרים של A. עבורה

$$\delta(v_1 + q v_2, v_2, \ldots, v_n) \leq |m_1| + r + |m_3| + \cdots + |m_n| < \delta(v_1, \ldots, v_n)$$

סתירה למזעריות. ∎

משפט 14.10: *אם $v_1, \ldots, v_n$ בסיס (די להניח שהיא בלתי תלויה), ו־$u_1, \ldots, u_k$ סדרת יוצרים, אז $n \leq k$.*

הוכחה: יש הצגות

$$\begin{array}{ccccc} v_1 & = m_{11}u_1 + & \cdots & + m_{1k}u_k \\ \vdots & \vdots & & \vdots \\ v_n & = m_{n1}u_1 + & \cdots & + m_{nk}u_k \end{array}$$

נניח בשלילה $n > k$. אז שורותיה של המטריצה $(m_{ij}) \in \mathrm{M}_{n\times k}(\mathbb{Q})$ תלויות לינארית מעל $\mathbb{Q}$. לכן יש $\epsilon_1, \ldots, \epsilon_n \in \mathbb{Q}$, לא כולם 0, כך ש־

$$\epsilon_1(m_{11}, \ldots, m_{1k}) + \cdots + \epsilon_n(m_{n1}, \ldots, m_{nk}) = 0.$$

בה"כ $\epsilon_1, \ldots, \epsilon_n \in \mathbb{Z}$ (אחרת נכפיל אותם במכנה משותף). מתקיים $\epsilon_1 v_1 + \cdots + \epsilon_n v_n = 0$, בסתירה לאי תלות (יחידות ב־(1)). ∎

הגדרה 14.11: עבור חבורה נוצרת סופית G תהי $\operatorname{rk} G = \min\{|S|| \ G = \langle S\rangle\}$ **הדרגה** של G.

מסקנה 14.12: *לכל הבסיסים של חבורה חילופית חפשית F אותו מספר איברים:* $\operatorname{rk} F$.

משפט 14.13 (משפט החבורות החלקיות של החבורה החילופית החפשית F_n): *תהי $H \leq F_n$. אזי H חילופית חפשית: קיים בסיס $v_1, \ldots, v_n$ של F_n וקיימים $0 \leq k \leq n$ ו־$\epsilon_1, \ldots, \epsilon_k \in \mathbb{N}$ כך ש־$\epsilon_1 \big| \epsilon_2 \big| \cdots \big| \epsilon_k$ ו־$\epsilon_1 v_1, \ldots, \epsilon_k v_k$ בסיס של H.*

הוכחה: אם $H = \{0\}$, המשפט ברור ($k = 0$); בפרט המשפט נכון עבור $n = 0$. נניח $n \geq 1$ ונניח נכונות עבור $n - 1$. בה"כ $H \neq \{0\}$.

א. טענה: יש $u_1, \ldots, u_n, v \in F_n$ כך ש־

$$(5) \quad u_1, \ldots, u_n \text{ בסיס של } F_n, \quad v \in H, \quad v = m_1 u_1 + m_2 u_2 + \cdots + m_n u_n, \quad m_1 > 0.$$

אכן, נבחר בסיס $u_1, \ldots, u_n$ כלשהו ו־$0 \neq v \in H$. אז $v = m_1 u_1 + m_2 u_2 + \cdots + m_n u_n$. יש i כך ש־$m_i \neq 0$; בה"כ $i = 1$. אם $m_1 < 0$ נחליף את v ב־$(-v)$.

ב: יהי $\epsilon_1 = \min\{m_1 | \ (5) \text{ ומתקיים } u_1, \ldots, u_n, v \in F_n\}$.

טענה: *יש בסיס $u_1, \ldots, u_n$ של F_n כך ש־$\epsilon_1 u_1 \in H$.*

אכן, יש $u_1, \ldots, u_n, v$ כך שמתקיים (5) ו־$m_1 = \epsilon_1$. נחלק עם שארית:

$$m_i = \epsilon_1 q_i + r_i, \qquad 0 \leq r_i < \epsilon_1, \qquad i = 2, \ldots, n$$

ונגדיר $u_1' = u_1 + q_2 u_2 + \cdots + q_n u_n$. אז $u_1', u_2, \ldots, u_n$ בסיס של F_n (תרגיל 14.8) ומתקיים

$$v = \epsilon_1 u_1' + r_2 u_2 + \cdots + r_n u_n.$$

בגלל המזעריות של ϵ_1 מתקיים $r_2 = \cdots = r_n = 0$, ולכן $v = \epsilon_1 u_1'$.

ג: נבחר בסיס $u_1, \ldots, u_n$ של F_n כך ש־$\epsilon_1 u_1 \in H$. נסמן $F' = \langle u_2, \ldots, u_n\rangle$. אז $H' = H \cap F'$. $F_n = \langle u_1\rangle \oplus F'$, לפי משפט 10.1, ו־$F'$ חפשית עם בסיס $u_2, \ldots, u_n$.

טענה: $H = \langle \epsilon_1 u_1\rangle \oplus H'$.

אכן, ברור ש־$\langle \epsilon_1 u_1\rangle \cap H' \subseteq \langle u_1\rangle \cap \langle u_2, \ldots, u_n\rangle = \{0\}$. נראה ש־$H = \langle \epsilon_1 u_1\rangle + H'$. זה יוכיח את הטענה לפי משפט 10.1(ב). יהי $u = m_1 u_1 + m_2 u_2 + \cdots + m_n u_n$ איבר של H. אם $m_1 = \epsilon_1 q + r, 0 \leq r < \epsilon_1$ אז

$$H \ni u - q(\epsilon_1 u_1) = r u_1 + m_2 u_2 + \cdots + m_n u_n$$

ו־$r = 0$ בגלל המזעריות של ϵ_1. לכן $u - q(\epsilon_1 u_1) \in H \cap F' = H'$, ומכאן $u \in \langle \epsilon_1 u_1\rangle + H'$.

ד: F' היא חפשית ו־$u_2, \ldots, u_n$ בסיס שלה. לפי הנחת האינדוקציה H' היא חפשית ויש בסיס $v_2, \ldots, v_n$ של F' ו־$\epsilon_2, \ldots, \epsilon_k \in \mathbb{N}$ כך ש־$\epsilon_2 \Big| \cdots \Big| \epsilon_k$ ו־$\epsilon_2 v_2, \ldots, \epsilon_k v_k$ בסיס של H'. יהי $v_1 = u_1$. אז $F_n = \langle v_1 \rangle \oplus F'$, לכן, לפי למה 14.6, $v_1, v_2, \ldots, v_n$ בסיס של F_n, ו־$H = \langle \epsilon_1 v_1 \rangle \oplus H'$, לכן, שוב לפי למה 14.6, $\epsilon_1 v_1, \epsilon_2 v_2, \ldots, \epsilon_k v_k$ בסיס של H.

ה טענה: $\epsilon_1 \Big| \epsilon_2$. אכן, נכתוב $\epsilon_2 = \epsilon_1 q + r, 0 \leq r < \epsilon_1$. יהי $v_1' = v_1 - q v_2$, אזי $v_1', v_2, \ldots, v_n$ בסיס של F_n ו־

$$H \ni \epsilon_2 v_2 - \epsilon_1 v_1 = \epsilon_1 q v_2 + r v_2 - \epsilon_1 v_1 = -\epsilon_1 v_1' + r v_2 = -\epsilon_1 v_1' + r v_2 + 0 v_3 + \cdots + 0 v_n.$$

ולפי המזעריות של ϵ_1 יוצא $r = 0$. לכן $\epsilon_1 \Big| \epsilon_2$. ∎

מסקנה 14.14: *אם F חפשית,* $H \leq F$ *אז* $\operatorname{rk} H \leq \operatorname{rk} F$.

15. מבנה של חבורות חילופית נוצרות סופית

תרגיל 15.1: *תהי* $G = G_1 \times \cdots \times G_n$ *ולכל* i *תהי* $N_i \triangleleft G_i$. *נגדיר* $N = N_1 \cdots N_n$. *אז* $N \triangleleft G$ *ו־* $G/N \cong G_1/N_1 \times \cdots \times G_n/N_n$.

פתרון: נגדיר $\lambda: G \to G_1/N_1 \times \cdots \times G_n/N_n$ על ידי $(g_1, \cdots, g_n) \mapsto (g_1N_1, \cdots, g_nN_n)$. העתקה זו מוגדרת היטב והיא על. קל לראות שהיא הומומורפיזם. גרעינה N. לכן $N \triangleleft G$. לפי משפט האיזומורפיזם הראשון $G/N \cong G_1/N_1 \times \cdots \times G_n/N_n$. ∎

משפט 15.2 (המשפט היסודי של החבורות החילופיות הנוצרות סופית): *כל חבורה חילופית נוצרת סופית* A *היא סכום ישר של מספר סופי של חבורות מעגליות. ביתר דיוק:* $A \cong \mathbb{Z}/\epsilon_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/\epsilon_k\mathbb{Z} \oplus \overbrace{\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}}^{r}$ *באשר* $\epsilon_1 \Big| \cdots \Big| \epsilon_k$ *מספרים טבעיים ו־* $k, r \geq 0$.

הוכחה: לפי משפט 14.5 קיים n ו־$H \leq F_n$ כך ש־$A \cong F_n/H$. לפי משפט החבורות החלקיות של F_n (משפט 14.13) יש בסיס $v_1, \ldots, v_n$ של F_n כך ש־

$$\begin{aligned} F_n &= \langle v_1 \rangle \oplus \cdots \oplus \langle v_k \rangle \oplus \langle v_{k+1} \rangle \oplus \cdots \oplus \langle v_n \rangle \\ H &= \langle \epsilon_1 v_1 \rangle \oplus \cdots \oplus \langle \epsilon_k v_k \rangle = \langle \epsilon_1 v_1 \rangle \oplus \cdots \oplus \langle \epsilon_k v_k \rangle \oplus \overbrace{\langle 0 \rangle \oplus \cdots \oplus \langle 0 \rangle}^{n-k} \end{aligned}$$

ומכאן לפי תרגיל 15.1

$$\begin{aligned} F_n/H &\cong \langle v_1 \rangle/\langle \epsilon_1 v_1 \rangle \oplus \cdots \oplus \langle v_k \rangle/\langle \epsilon_k v_k \rangle \oplus \langle v_{k+1} \rangle/\langle 0 \rangle \oplus \cdots \oplus \langle v_n \rangle/\langle 0 \rangle \\ &\cong \mathbb{Z}/\epsilon_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/\epsilon_k\mathbb{Z} \oplus \overbrace{\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}}^{n-k} \end{aligned}$$

∎

לפי מסקנה 10.5 חבורה מעגלית $\mathbb{Z}/m\mathbb{Z}$ הינה איזומורפית לסכום ישר של חבורות מעגליות מהצורה $\mathbb{Z}/q\mathbb{Z}$, באשר q חזקה של ראשוני. לכן:

משפט 15.3: *תהי* A *חבורה חילופית נוצרת סופית. אזי*

$$A \cong \mathbb{Z}/p_1^{\alpha_1}\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/p_k^{\alpha_k}\mathbb{Z} \oplus F_r \tag{1}$$

באשר $p_1, \ldots, p_k$ *מספרים ראשוניים (לא בהכרח שונים),* $r \geq 0$, $\alpha_1, \ldots, \alpha_k \in \mathbb{N}$ *ו־* $F_r = \overbrace{\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}}^{r}$.

נרצה להוכיח יחידות של ההצגה (1). לשם כך נזדקק להכנות:

תרגיל 15.4: *תהי* A *חבורה חילופית. יהי* $m \in \mathbb{N}$ *ויהי* $p \in \mathbb{N}$ *ראשוני.*

(א) *ההעתקה* $A \to A$ *הנתונה על ידי* $a \mapsto ma$ *היא הומומורפיזם.*

בפרט, גרעינו $A_m = \{a \in A |\ ma = 0\}$ *ותמונתו* $mA = \{ma |\ a \in A\}$ *הם תת חבורות של* A.

(ב) $A^t = \bigcup_m A_m$.

(ג) $A^{(p)} = \{a \in A |\ p \text{ הוא חזקה של } \operatorname{ord} a\} = \bigcup_{\alpha=1}^{\infty} A_{p^\alpha}$ *היא תת חבורה של* A.

(ד) *אם* A *סופית אז* $A^{(p)}$ *היא חבורת סילוב־*p *היחידה של* A.

(ה) $p^\beta(\mathbb{Z}/p^\alpha\mathbb{Z}) \cong \begin{cases} \mathbb{Z}/p^{\alpha-\beta}\mathbb{Z} & \beta \le \alpha \\ \{0\} & \beta \ge \alpha \end{cases}$.

(ו) אם $p \big| m$ אז $(\mathbb{Z}/m\mathbb{Z})_p \cong \mathbb{Z}/p\mathbb{Z}$.

(ז) *יהי* $\theta: A \to B$ *איזומורפיזם של חבורות חילופיות. אז* $\theta(A^t) = B^t$, $\theta(A_m) = B_m$, $\theta(mA) = mB$, $\theta(A^{(p)}) = B^{(p)}$, *ו־*$A/A^t \cong B/B^t$.

פתרון: (ג) אם $p^\alpha a = 0$ ו־$p^\beta b = 0$ אז $p^{\alpha+\beta}(a+b) = p^{\alpha+\beta}a + p^{\alpha+\beta}b = 0$.

(ד) תהי P חבורת סילוב־p של A. היא יחידה כי האחרות צמודות לה, ו־A חילופית. ברור ש־$P \subseteq A^{(p)}$. להיפך, יהי $a \in A^{(p)}$. אז $\langle a \rangle$ היא חבורת־p ולכן (המשפט השני של סילוב) מוכלת ב־P. בפרט $a \in P$.

(ה) תהי $A = \mathbb{Z}/p^\alpha\mathbb{Z}$ ויהי a יוצר שלה. אז $\operatorname{ord}(a) = p^\alpha$ ו־$A = \{ka |\ k \in \mathbb{Z}\}$. לכן

$$p^\beta A = \{p^\beta ka |\ k \in \mathbb{Z}\} = \langle p^\beta a \rangle \le A$$

מעגלית (זה גם נובע מכך שהיא חבורה חלקית של מעגלית) וסדרה הוא

$$|p^\beta A| = \operatorname{ord}(p^\beta a) = \begin{cases} \operatorname{ord}(a)/p^\beta & p^\beta \big| \operatorname{ord}(a) \\ 1 & \operatorname{ord}(a) \big| p^\beta \end{cases}.$$

(ו) בחבורה $(\mathbb{Z}/m\mathbb{Z})_p = \{k[1] |\ pk[1] = [0]\} = \{k[1] |\ m \big| pk\} = \{k[1] |\ \frac{m}{p} \big| k\}$ יש בדיוק p איברים: $[0] = \frac{m}{p}[1], 2\frac{m}{p}[1], \ldots, p\frac{m}{p}[1]$.

(ז) נראה רק ש־$A/A^t \cong B/B^t$. הגרעין של ההרכבה $A \xrightarrow{\theta} B \to B/B^t$ הוא A^t. לכן האיזומורפיזם נובע ממשפט האיזומורפיזם הראשון. ∎

למה 15.5: *תהיינה* $A_1, \ldots, A_k$ *חבורות חילופיות ותהי* $A = A_1 \oplus \cdots \oplus A_k$. *יהי* $m \in \mathbb{N}$ *ויהי* p *ראשוני. אזי*

(א) $A^t = A_1^t \oplus \cdots \oplus A_k^t$.

(ב) $A_m = (A_1)_m \oplus \cdots \oplus (A_k)_m$.

(ג) $A^{(p)} = A_1^{(p)} \oplus \cdots \oplus A_k^{(p)}$.

(ד) $mA = mA_1 \oplus \cdots \oplus mA_k$.

הוכחה: כל $a \in A$ הוא מהצורה $(a_1, \ldots, a_k)$ באשר $a_i \in A_i$. אז די להוכיח:

$$a \in A^t\ [a \in A_m,\ a \in mA] \quad \Leftrightarrow \quad \text{לכל } i\ a_i \in A^t\ [a_i \in A_m,\ a_i \in mA].$$

זה נובע בקלות מהעובדה $m(a_1, \ldots, a_k) = (ma_1, \ldots, ma_k)$. ∎

משפט 15.6 (משפט יחידות הפירוק של חבורה חילופית נוצרת סופית): *תהי A חילופית נוצרת סופית. אזי הפירוק (1)*

$$A \cong \mathbb{Z}/p_1^{\alpha_1}\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/p_k^{\alpha_k}\mathbb{Z} \oplus F_r \tag{1}$$

יחיד, עד כדי סדר המחוברים. ביתר דיוק:

(א) $r = \mathrm{rk}(A/A^t)$.

(ב) *יהי p ראשוני ויהי $0 \le \beta \in \mathbb{Z}$. נסמן $s_\beta = s_\beta(p) = \#\{i|\ p_i = p,\ \alpha_i > \beta\}$. אז $s_\alpha = \log_p |p^{\alpha-1}A^{(p)}/p^\alpha A^{(p)}|$, ולכן $\#\{i|\ p_i = p,\ \alpha_i = \beta\} = s_{\beta-1} - s_\beta$ תלוי רק ב־A, לכל $\beta \in \mathbb{N}$.*

הוכחה: נסמן את אגף ימין של (1) ב־B. לפי למה 15.5, $B^t = \mathbb{Z}/p_1^{\alpha_1}\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/p_k^{\alpha_k}\mathbb{Z} \oplus \{0\}$ ולפי תרגיל 15.1 $B/B^t \cong F_r$. לכן $A/A^t \cong B/B^t = F_r$. מכאן $\mathrm{rk}(A/A^t) = \mathrm{rk}(F_r) = r$.

(ב) לפי למה 15.5,

$$\begin{aligned}
B^{(p)} &= (\mathbb{Z}/p_1^{\alpha_1}\mathbb{Z})^{(p)} \oplus \cdots \oplus (\mathbb{Z}/p_k^{\alpha_k}\mathbb{Z})^{(p)} \oplus (F_r)^{(p)} \\
&= \oplus_{\{i|\ p_i=p\}} \mathbb{Z}/p^{\alpha_i}\mathbb{Z} \\
p^\beta B^{(p)} &= \oplus_{\{i|\ p_i=p\}} p^\beta(\mathbb{Z}/p^{\alpha_i}\mathbb{Z}) \\
&\cong \oplus_{\{i|\ p_i=p,\ \beta<\alpha_i\}} \mathbb{Z}/p^{\alpha_i-\beta}\mathbb{Z} \qquad \text{לפי תרגיל 15.4(ה)} \\
(p^\beta B^{(p)})_p &\cong \oplus_{\{i|\ p_i=p,\ \beta<\alpha_i\}} (\mathbb{Z}/p^{\alpha_i-\beta}\mathbb{Z})_p \\
&\cong \oplus_{\{i|\ p_i=p,\ \beta<\alpha_i\}} \mathbb{Z}/p\mathbb{Z} \qquad \text{לפי תרגיל 15.4(ו)}
\end{aligned}$$

מכאן

$$|(p^\beta A^{(p)})_p| = |(p^\beta B^{(p)})_p| = \prod_{\{i|\ p_i=p,\ \beta<\alpha_i\}} p \quad = \quad p^{s_\beta}. \qquad \blacksquare$$

תרגיל 15.7: *כמה חבורות חילופיות מסדר 24 יש, עד כדי איזומורפיזם?*

פתרון: אם A חילופית מסדר 24 אז $A = (\mathbb{Z}/3\mathbb{Z}) \oplus B$ באשר $B = \mathbb{Z}/8\mathbb{Z}$ או $B = (\mathbb{Z}/4\mathbb{Z}) \oplus (\mathbb{Z}/2\mathbb{Z})$ או $B = (\mathbb{Z}/2\mathbb{Z}) \oplus (\mathbb{Z}/2\mathbb{Z}) \oplus (\mathbb{Z}/2\mathbb{Z})$. לכן יש 3 חבורות כאלה, לא איזומורפיות זו לזו.

משפט 15.8 (משפט החבורות החלקיות של חבורות חילופיות נוצרות סופית): *תהי A חילופית נוצרת סופית ותהי $B \le A$. אז B נוצרת סופית. יהי p מספר ראשוני. נניח כי בפירוק (1) של A [של B] מופיעים F_r [F_s], ו־$k = k(p)$ חמחוברים מעגליים מסדרים $p^{\alpha_1}, p^{\alpha_2}, \ldots, p^{\alpha_k}$ [$l = l(p)$] $p^{\beta_1}, p^{\beta_2}, \ldots, p^{\beta_l}$ באשר $\alpha_1 \ge \alpha_2 \ge \cdots \ge \alpha_k \ge 1$ [$\beta_1 \ge \beta_2 \ge \cdots \ge \beta_l \ge 1$]. אזי $s \le r$, $l \le k$, ו־$\beta_i \le \alpha_i$ לכל $1 \le i \le l$.*

הוכחה:

(א) לפי משפט 14.5 יש אפימורפיזם $\varphi: F_n \to A$. אז $H = \varphi^{-1}(B) \leq F_n$. לפי משפט 14.13, H (חפשית) נוצרת סופית. הצמצום של φ ל־H נותן אפימורפיזם $H \to B$. לכן B נוצרת סופית (על ידי התמונות של יוצרים של H).

(ב) $B^t = B \cap A^t$, לכן לפי משפט האיזומורפיזם השני $B/B^t \cong (B+A^t)/A^t \leq A/A^t$. לפי למה 14.14(ב), $B/B^t, A/A^t$ חסרות פיתול, לכן לפי משפט 14.9 הן חפשיות. מכאן לפי מסקנה 14.14

$$s = \mathrm{rk}(B/B^t) \leq \mathrm{rk}(A/A^t) = r.$$

(ג) $B \leq A$, לכן $B^{(p)} \leq A^{(p)}$, לכן $p^\beta B^{(p)} \leq p^\beta A^{(p)}$, ולכן $(p^\beta B^{(p)})_p \leq (p^\beta A^{(p)})_p$, לכל $\beta \geq 0$. מכאן

$$p^{\#\{i|\ \beta<\beta_i\}} = |(p^\beta B^{(p)})_p| \leq |(p^\beta A^{(p)})_p| = p^{\#\{i|\ \beta<\alpha_i\}}.$$

ולכן

$$\#\{i|\ \beta < \beta_i\} \leq \#\{i|\ \beta < \alpha_i\}.$$

נציב $\beta = 0$: נקבל $l \leq k$.

נציב $\beta = \beta_j - 1$: נקבל $\#\{i|\ \beta_j \leq \beta_i\} \leq \#\{i|\ \beta_j \leq \alpha_i\}$. הקבוצה השמאלית מכילה לפחות את האינדקסים $1, 2, \ldots, j$ ולכן יש בה לפחות j איברים. מכאן שגם בקבוצה הימנית לפחות j אינדקסים. לכן $\alpha_1 \geq \cdots \geq \alpha_j \geq \beta_j$. ∎

16. חבורות (חילופיות) חופשיות.

הגדרה 16.1: תהי S קבוצה חלקית של חבורה [חילופית] F. נאמר כי F היא **חבורה [חילופית] חפשית על** S אם כל העתקה $\varphi_0: S \to A$ לתוך איזושהי חבורה [חילופית] A ניתנת להרחבה להומומורפיזם יחיד $\varphi: F \to A$.

דוגמה 16.2:

(1) $\mathbb{Z}$ היא חפשית על $\{1\}$ ולכן גם חילופית חפשית על $S = \{1\}$.

(2) תהי S קבוצה. תהי

$$F(S) = \oplus_{s\in S}\mathbb{Z} = \{f: S \to \mathbb{Z} |\ s \in S \text{ כמעט לכל } f(s) = 0\}.$$

ההעתקה $s \mapsto \hat{s}$ מ־S לתוך $F(S)$ הנתונה על ידי

$$\hat{s}(s) = 1$$

$$s' \neq s \text{ לכל } \hat{s}(s') = 0$$

היא חח"ע. נסמן את תמונתה ב־$\hat{S}$.

טענה: *$F(S)$ חילופית חפשית על $\hat{S}$.*

אכן, לכל $f \in F(S)$ הצגה יחידה מהצורה

$$f = \sum_{s\in S} n_s \hat{s} \quad , n_s \in \mathbb{Z}\ ,\ n_s = 0 \text{ כמעט לכל } s \in S. \tag{1}$$

אם $\varphi: F(S) \to A$ הומומורפיזם המרחיב $\varphi_0: \hat{S} \to A$ אז בהכרח

$$\varphi(f) = \sum_{s\in S} n_s \varphi_0(\hat{s}) \tag{2}$$

ומכאן היחידות של φ.

קיום: נגדיר את φ על פי (2); זוהי הגדרה טובה בגלל יחידות ההצגה (1), וקל לראות ש־φ הומומורפיזם המרחיב את φ_0.

אם נזהה כל $s \in S$ עם $\hat{s}$ אז $F(S)$ חילופית חפשית על S. אבל גם אם לא נזהה, הלמה הבאה מראה איך לקבל חבורה חילופית חפשית על S מתוך $F(S)$:

למה 16.3: *אם $\theta: F_1 \to F_2$ איזומורפיזם של חבורות ו־F_1 [חילופית] חפשית על S_1 אז F_2 [חילופית] חפשית על $S_2 = \theta(S_1)$.*

הוכחה: אם $\varphi_0: S_2 \to A$ העתקה לתוך חבורה [חילופית] A, יהי $\psi: F_1 \to A$ ההומומורפיזם שמרחיב את $\psi_0 = \varphi_0 \circ \theta: S_1 \to A$ ואז $\varphi = \psi \circ \theta^{-1}: F_2 \to A$ הומומורפיזם שמרחיב את φ_0. אם גם $\varphi': F_2 \to A$ הומומורפיזם שמרחיב את φ_0 אז $\psi' = \varphi' \circ \theta: F_1 \to A$ הומומורפיזם שמרחיב את ψ_0. בגלל היחידות $\psi = \psi'$ ומכאן $\varphi = \psi \circ \theta^{-1} = \varphi'$. ∎

למה 16.4: *תהי $\theta_0\colon S_1 \to S_2$ העתקה חח"ע ועל של קבוצות. אם F_i [חילופית] חפשית על S_i, $i = 1, 2$, אז קיים איזומרפיזם $\theta\colon F_1 \to F_2$ יחיד אשר מרחיב את θ_0.*

הוכחה: (abstract nonsense) לפי החפשיות של F קיים הומומורפיזם יחיד $\theta\colon F_1 \to F_2$ שמרחיב את $\theta_0\colon S_1 \to S_2$. לפי החפשיות של F_2 קיים הומומורפיזם יחיד $\rho\colon F_2 \to F_1$ שמרחיב את $\theta_0^{-1}\colon S_2 \to S_1$. כעת $\rho \circ \theta\colon F_1 \to F_1$ וגם $\mathrm{id}_{F_1}\colon F_1 \to F_1$ הומומורפיזמים שמרחיבים את $\mathrm{id}\colon S_1 \to S_1$, לכן לפי היחידות $\rho \circ \theta = \mathrm{id}_{F_1}$. באפן דומה $\theta \circ \rho = \mathrm{id}_{F_2}$.

מסקנה 16.5: *לכל S קיימת חבורה חילופית חפשית על S, והיא יחידה, עד כדי איזומורפיזם (יחיד).*

סימון: F_n = חבורה [חילופית] חפשית על קבוצה בת n איברים. (יחידה עד כדי איזומורפיזם)

תרגיל 16.6: *אם F חבורה [חילופית] חפשית על S אז $F = \langle S \rangle$.*

אכן, קיים הומומורפיזם $\varphi\colon F \to \langle S \rangle$ אשר מרחיב את $\mathrm{id}_S\colon S \to S$. גם $\mathrm{id}_F\colon F \to F$ מרחיב את id_S. בגלל היחידות $\varphi = \mathrm{id}_F$, ומכאן $F = \varphi(F) \subseteq \langle S \rangle$. ∎

מסקנה 16.7: *תהי F חילופיות, $S \subseteq F$. התנאים הבאים שקולים:*

(א) *F חילופיות חפשית על S.*

(ב) *קיים איזומורפיזם $F \to F(S) = \oplus_{s \in S} \mathbb{Z}$ כך ש־$s \mapsto \hat{s}$.*

(ג) *$F = \oplus_{s \in S} \langle s \rangle$ ו־$\langle s \rangle \cong \mathbb{Z}$ לכל $s \in S$.*

(ד) *S בסיס של F: לכל $f \in F$ הצגה יחידה מהצורה*

$$f = \sum_{s \in S} n_s s \quad , n_s \in \mathbb{Z} \ , n_s = 0 \text{ כמעט לכל } s \in S. \tag{1}$$

הוכחה:

(א) $\Leftarrow$ (ב): לפי הלמה הקודמת.

(ב) $\Leftarrow$ (ג): בגלל ש־$F(S) = \oplus_{s \in S} \langle \hat{s} \rangle = \mathbb{Z}$ ו־$\langle \hat{s} \rangle = \mathbb{Z}$ לכל $s \in S$.

(ג) $\Leftarrow$ (ד): תכונה של סכום ישר: לכל $x \in F$ הצגה יחידה מהצורה $x = \sum_{s \in S} x_s$, באשר $x_s \in \langle s \rangle$ ו־$x_s = 0$ כמעט לכל $s \in S$. אבל $\langle s \rangle \cong \mathbb{Z}$, לכן לכל x_s יש $n_s \in \mathbb{Z}$ יחיד כך ש־$x_s = n_s s$.

(ד) $\Leftarrow$ (א): כמו בהוכחה ש־$F(S)$ חילופית חפשית על S. ∎

למה 16.8: *כל חבורה [חילופית] A איזומורפית למנה של חבורה [חילופית] חפשית. ביתר דיוק, אם $A = \langle S \rangle$ אז A איזומורפית למנה של חבורה [חילופית] חפשית F על S.*

הוכחה: את $\mathrm{id}\colon S \to S$ אפשר להרחיב להומומורפיזם $\varphi\colon F \to A$. הוא על, כי $S \subseteq \varphi(F)$ ולכן $A = \langle S \rangle \subseteq \varphi(F)$. לכן $A \cong F/\operatorname{Ker}\varphi$. ∎

הגדרה 16.9: תהי G חבורה. $\mathrm{rk}(G) = min\{|S|| \ \langle S\rangle = G\}$ נקרא **הדרגה** של G.

דוגמה 16.10: $\mathrm{rk}(G) = 0$ אמ"ם $G = \{1\}$.

$\mathrm{rk}(G) = 1$ אמ"ם $G \neq \{1\}$ מעגלית.

$\mathrm{rk}(S_n) = 2$ עבור $n \geq 3$, כי $S_n = \langle (12), (12\dots n)\rangle$.

תהי $A = \overbrace{\mathbb{Z}/p\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/p\mathbb{Z}}^{n\times}$. אזי $\mathrm{rk}(A) = n$. (אכן, A הוא מרחב וקטורי מעל $\mathbb{Z}/p\mathbb{Z}$. לכל $a \in A$ מתקיים $pa = 0$, ולכן לכל $m \in \mathbb{Z}$ מתקיים $ma = ra$, באשר $0 \leq r < p$ השארית של m לאחר החילוק ב־p. יהיו $a_1, \dots, a_k \in A$. אז

$$\begin{aligned}\langle a_1, \dots, a_k\rangle &= \{m_1a_1 + \cdots + m_ka_k|\ m_1, \dots, m_n \in \mathbb{Z}\} \\ &= \{r_1a_1 + \cdots + r_ka_k|\ 0 \leq r_1, \dots, r_n < p\} = \mathrm{Span}(a_1, \dots, a_k)\end{aligned}$$

ולכן $\mathrm{rk}(A) = \dim(A)$.)

יתכן ש־$H \leq G$ ו־$\mathrm{rk}(G) < \mathrm{rk}(H)$ (למשל את A לעיל אפשר לראות כחבורה חלקית של S_{p^n}).

נשים לב ש־$\mathrm{rk}(G) \geq \mathrm{rk}(G/N)$.

למה 16.11: *תהי F [חילופית] חפשית על S סופית. אז $\mathrm{rk}(F) = |S|$.*

הוכחה: (רק עבור S סופית).

(א) $F = \langle S\rangle$. לכן $\mathrm{rk}(F) \leq |S|$.

(ב) תהי A הסכום הישר של $|S|$ העתקים של $\mathbb{Z}/2\mathbb{Z}$. אז $\mathrm{rk}(A) = |S|$. לכן קיימת העתקה חח"ע $\varphi_0\colon S \to A$ כך ש־$\varphi_0(S)$ קבוצת יוצרים של A. היא ניתנת להרחבה להומומורפיזם $\varphi\colon F \to A$. הוא על, כי $A = \langle\varphi(S)\rangle \subseteq \langle\varphi(F)\rangle = \varphi(F)$ אך $\mathrm{rk}(A) = |S|$, כלומר A איזומורפית למנה של F. מכאן $\mathrm{rk}(F) \geq \mathrm{rk}(A) = |S|$.

תרגיל 16.12: *תהי F חילופית חפשית עם בסיס $S = \{s_1, s_2, \dots, s_n\}$, ויהיו $k_2, \dots k_n \in \mathbb{Z}$. אז גם*

$$\{s_1 + k_1s_2 + \cdots + k_ns_n, s_2, \dots, s_n\}, \{-s_1 + k_1s_2 + \cdots + k_ns_n, s_2, \dots, s_n\}$$

בסיסים של F.

תרגיל 16.13: *. נניח כי $G = G_1 \times \cdots \times G_n$ ותהיינה $H_i \triangleleft G_i$ לכל $i = 1, \dots, n$. נסמן $H = H_1H_2 \cdots H_n$. אזי*

(א) $H \triangleleft G$.

(ב) $G/H = (G_1/H_1) \cdots \times (G_n/H_n)$

17. חבורות חופשיות.

תהי X קבוצה. תהי X^{-1} קבוצה זרה לה עם העתקה חח"ע ועל $X \to X^{-1}$ אשר תסומן כך: $x \mapsto x^{-1}$. גם ההעתקה ההופכית $X^{-1} \to X$ תסומן באותו הסימון, כלומר $(x^{-1})^{-1} = x$. לפעמים נכתוב x^1 במקום x, עבור $x \in X$. כך ש־$X \cup X^{-1} = \{x^\varepsilon \mid x \in X,\ \varepsilon \in \{\pm 1\}\}$.

יהי $F(X)$ אוסף כל **הסדרות המצומצמות**, כלומר, סדרות סופיות $z_1 z_2 \dots z_n$ של איברי $Z = X \cup X^{-1}$ המקיימות $z_{i+1} \neq z_i^{-1}$ לכל $1 \leq i < n$. (גם $n = 0$ יתכן.) נסמן $\ell(z_1 z_2 \dots z_n) = n$. נגדיר פעולה בינארית ("צירוף עם צמצום") על $F(X)$:

אם $u = z_m \dots z_2 z_1, v = z_1' z_2' \dots z_n' \in F(X)$ אז

$$u \cdot v = z_m \dots z_{k+1} z_{k+1}' \dots z_n' \tag{1}$$

באשר $0 \leq k \leq \min(m,n)$ הגדול ביותר כך ש־$z_1^{-1} = z_1', z_2^{-1} = z_2', \dots, z_k^{-1} = z_k'$.
בפרט $u \cdot v \in F(X)$.

למה 17.1: *אם $u, v, \in F(X)$ אז $(u \cdot v) \cdot w = u \cdot (v \cdot w)$.*

הוכחה: אם אחד מבין u, v, w סדרה ריקה אז הטענה ברורה. לכן נניח שהן אינן סדרות ריקות.

ההוכחה באינדוקציה על האורך $\ell(v)$ של v:

(א) $\ell(v) = 1$: אז $u = u'x, \quad v = y, \quad w = zw'$,

באשר u', v' סדרות מצומצמות (אולי ריקות) ו־$x, y, z \in X \cup X^{-1}$. שים לב שאיבר האחרון של u' אינו x^{-1} והאיבר הראשון של w' אינו z^{-1}. הבדיקה קלה, לפי ארבעה מקרים:

$x = y^{-1} = z$, $x = y^{-1} \neq z$, $x \neq y^{-1} = z$, $x = y^{-1} \neq z$.

למשל, נניח $x = y^{-1} \neq z$. אז $u \cdot v = u'$, לכן $(u \cdot v) \cdot w = u' \cdot (zw)$. (שים לב שיתכן צמצום בין u' לבין zw.) מצד שני, $v \cdot w = yzw'$, והסדרה yzw' מצומצמת ו־$x \neq y^{-1}$, לכן $u \cdot (v \cdot w) = (u'x) \cdot (yzw) = u' \cdot (zw)$.

(ב) נניח $\ell(v) > 1$, אז $v = v_1 v_2 = v_1 \cdot v_2$, לפי הנחת האינדוקציה $\ell(v_1), \ell(v_2) < \ell(v)$.

$$\big(u \cdot (v_1 \cdot v_2)\big) \cdot w = \big((u \cdot v_1) \cdot v_2\big) \cdot w = (u \cdot v_1) \cdot (v_2 \cdot w) = u \cdot \big(v_1 \cdot (v_2 \cdot w)\big) = u \cdot \big((v_1 \cdot v_2) \cdot w\big). \qquad \blacksquare$$

מסקנה 17.2: *$F(X)$ היא חבורה, X קבוצת יוצרים שלה.*

הוכחה: הכפל אסוציאטיבי, יש איבר יחידה (הסדרה הריקה) ולכל איבר יש הופכי: ההופכי של סדרה מצומצמת $z_1 \dots z_n$ הוא הסדרה $z_n^{-1} \dots z_1^{-1}$. ברור ש־$z_1 \dots z_n = z_1 \cdot \dots \cdot z_n$. $\blacksquare$

מעתה נוותר על כתיבת $\cdot$.

טענה 17.3: *כל $1 \neq w \in F(X)$ הוא מסדר אינסופי.*

הוכחה: צריך להוכיח ש־$w^k \neq 1$ לכל $k \geq 1$. נראה זאת באינדוקציה על $\ell(w)$.

אם $\ell(w) = 1$, זה ברור. נניח $w = z_1 \dots z_n$. אם $z_n \neq z_1^{-1}$, הטענה ברורה. אם $z_n = z_1^{-1}$, אז $w = z_1 w' z_n = z_1 w' z_1^{-1}$, באשר $w' \in F(X)$ ו־$\ell(w') < \ell(w)$. היות ו־w' צמוד ל־w הוא אינו 1 והוא מאותו הסדר ובפרט $w' \neq 1$. לפי הנחת האידוקציה, $\operatorname{ord} w' = \infty$, לכן $\operatorname{ord} w = \infty$. ∎

הגדרה 17.4: תהי F חבורה ו־$X \subseteq F$ קבוצה. אזי F **חבורה חפשית על** X אם יש לה התכונה האוניברסאלית: כל העתקה $X \to G$ לתוך חבורה G אפשר להרחיב להומומורפיזם יחיד $F \to G$.

דוגמה 17.5: $\mathbb{Z}$ היא חבורה חפשית על $\{1\}$; $\{1\}$ היא חבורה חפשית על $\emptyset$.

תרגיל 17.6: *אם F_i חבורה חופשית על X_i, $i = 1, 2$, ו־$\theta\colon X_1 \to X_2$ היא העתקה חח"ע ועל אז קיים איזומורפיזם יחיד $\theta\colon F_1 \to F_2$ אשר מרחיב את $\theta\colon X_1 \to X_2$.*

הוכחה: לפי החפשיות קיימים הומומורפיזמים יחידים $\theta\colon F_1 \to F_2$ ו־$\theta'\colon F_2 \to F_1$ המרחיבים את ההעתקות $\theta\colon X_1 \to X_2 \subseteq F_2$ ואת $\theta^{-1}\colon X_2 \to X_1 \subseteq F_1$, בהתאמה. אז $\theta' \circ \theta\colon F_1 \to F_1$ מרחיב את העתקת הזהות $X_1 \to X_1 \subseteq F_1$ אבל גם הזהות של F_1 מרחיבה העתקה זו. לפי היחידות, $\theta' \circ \theta$ היא הזהות של F_1. באופן דומה, $\theta \circ \theta'$ היא הזהות של F_2. לכן θ איזומורפיזם (ו־$\theta' = \theta^{-1}$). ∎

מסקנה 17.7: *קימת חבורה חפשית אחת לכל היותר על קבוצה X, עד כדי איזומורפיזם (יחיד).*

הוכחה: קח $X_1 = X_2 = X$ בתרגיל הקודם. ∎

משפט 17.8: *$F(X)$ היא חבורה חופשית על X.*

הוכחה: תהי $f\colon X \to G$ העתקה לתוך חבורה G. האפשרות היחידה להרחיבה להומומורפיזם $F(X) \to G$ היא על ידי ההגדרה $f(x^{-1}) = f(x)^{-1}$ עבור $x \in X$ ואח"כ $f(z_1 \dots z_n) = f(z_1) \cdots f(z_n)$, באשר $z_1, \dots, z_n \in X \cup X^{-1}$, ומכאן היחידות של ההרחבה. הרחבה זו היא הומומורפיזם: בסימון של (1)

$$
\begin{aligned}
&f(z_m \dots z_2 z_1 \cdot z_1' z_2' \dots z_n') = f(z_m \dots z_{k+1} z_{k+1}' \dots z_n') = \\
&f(z_m) \cdots f(z_{k+1}) f(z_{k+1}') \cdots f(z_n') = \\
&f(z_m) \cdots f(z_{k+1}) f(z_k) \cdots f(z_1) f(z_1') \cdots f(z_k') f(z_{k+1}') \cdots f(z_m') = \\
&f(z_n \cdots z_1) f(z_1') \cdots z_n')
\end{aligned}
$$

מסקנה 17.9: *תהי F חבורה ותהי $X \subseteq F$. אזי F היא חבורה חופשית על X אם ורק אם:*

(א) $F = \langle X \rangle$

(ב) *אם $z_1, \dots, z_n \in X \cup X^{-1}$ כך ש־$z_{i+1} \neq z_i^{-1}$ לכל $1 \leq i < n$ ו־$z_1 \cdots z_n = 1$ אז $n = 0$.*

הוכחה: נניח כי F חפשית על X. בה"כ $F = F(X)$ ואז (א), (ב) נובעים בקלות.

להיפך, נניח (א), (ב). תהי $F(X)$ החבורה החופשית על X. לפי התכונה האוניברסאלית קיים הומומורפיזם $\varphi\colon F(X)\to F$ אשר הינו הזהות של X. לפי (א) הוא על. יהי $u=z_1\cdots z_n\in\operatorname{Ker}\varphi$. אזי $1=z_1\cdots z_n=\varphi(z_1\cdots z_n)$ ב־F, לכן לפי (ב) $n=0$ ומכאן $u=1$. לכן φ איזומורפיזם. ∎

תהי $F=F(X)$.

טענה 17.10: לכל $x\in X$ נגדיר העתקה $\sigma_x\colon F\to\mathbb{Z}$ באופן הבא:

$$\sigma_x(z_1z_2\ldots z_n)=|\{i|\ z_i=x\}|-|\{i|\ z_i=x^{-1}\}|$$

באשר $z_1,\ldots,z_m\in X\dot\cup X^{-1}$ ו־$z_1z_2\ldots z_n$ מלה מצומצמת. אז

(א) σ_x הומומורפיזם לכל x.

(ב) $F'=\{w\in F|\ \sigma_x(w)=0\ \text{לכל}\ x\in X\}$ (=הקומוטטור).

הוכחה: (א) יהיו $u=z_m\ldots z_2z_1, v=z_1'z_2'\ldots z_n'\in F$, ויהי $0\le k\le\min(m,n)$ הגדול ביותר עבורו $z_1^{-1}=z_1', z_2^{-1}=z_2',\ldots,z_k^{-1}=z_k'$. אז $\sigma_x(z_k\ldots z_1)=-\sigma_x(z_1'\ldots z_k')$. לכן

$$\sigma_x(u\cdot v)=\sigma_x(z_m\ldots z_{k+1}z_{k+1}'\ldots z_n')=\sigma_x(z_m\ldots z_{k+1})+\sigma_x(z_{k+1}'\ldots z_n')=$$
$$=\sigma_x(z_m\ldots z_{k+1})+\sigma_x(z_k\ldots z_1)+\sigma_x(z_1'\ldots z_k')+\sigma_x(z_{k+1}'\ldots z_n')=\sigma_x(u)+\sigma_x(v)$$

(ב) "$\subseteq$": יהי $x\in X$. צריך להוכיח שכל איבר של F' נמצא ב־$\operatorname{Ker}\sigma_x$. זוהי תת חבורה של F, לכן די להראות שיוצרים של F' –הקומוטטורים– נמצאים בה. ואכן, יהיו $u,v\in F$, אז

$$\sigma_x\big([u,v]\big)=\sigma_x(u^{-1}v^{-1}uv)=-\sigma_x(u)-\sigma_x(v)+\sigma_x(u)+\sigma_x(v)=0$$

"$\supseteq$": יהי $w=z_1\ldots z_n\in F$ כך ש־$\sigma_x(w)=0$ לכל $x\in X$. צריך להוכיח ש־$w\in F'$. תהי $v\mapsto\bar v$ העתקת המנה $\pi\colon F\to F/F'$. אז צריך להוכיח ש־$\bar w=1$. ואכן, $\bar w=\bar z_1\cdots\bar z_n$, החבורה F/F' חילופית, ובסדרה $\bar z_1\cdots\bar z_n$ מופיע כל איבר $\bar x$ בדיוק אותו מספר פעמים כמו $\bar x^{-1}$. לכן $\bar w=1$. ∎

מסקנה 17.11: *אם $X=\{x_1,\ldots,x_n\}$ בת n איברים, אז F/F' היא חבורה חילופית חפשית עם בסיס $\bar x_1,\ldots,\bar x_n$.*

הוכחה: תהי $v\mapsto\bar v$ העתקת המנה $\pi\colon F\to F/F'$. כיוון ש־$x_1,\ldots,x_n$ יוצרים את F, גם $\bar x_1,\ldots,\bar x_n$ יוצרים את F/F'. צריך להוכיח (בכתיב כפלי): אם $\bar x_1^{m_1}\cdots\bar x_n^{m_n}=1$, אז $m_i=0$ לכל i. ואכן, $\pi(x_1^{m_1}\cdots x_n^{m_n})=1$, לכן $x_1^{m_1}\cdots x_n^{m_n}\in F'$. ברור ש־$\sigma_{x_i}(x_1^{m_1}\cdots x_n^{m_n})=m_i$, לכן לפי טענה 17.10, $m_i=0$. ∎

מסקנה 17.12: *אם X_1,X_2 קבוצות סופיות אז $F(X_1)\cong F(X_2)$ אם ורק אם $|X_1|=|X_2|$.*

הוכחה: נניח $|X_1|=|X_2|$. לפי תרגיל 17.5, $F(X_1)\cong F(X_2)$.

להיפך, נסמן $m = |X_1|, n = |X_2|$, ויהי $\theta\colon F(X_1) \to F(X_2)$ איזומורפיזם. אז θ מעתיק קומוטטורים על קומוטטורים ולכן $\theta\big(F(X_1)'\big) = \big(F(X_2)'\big)$. לפי משפט האיזומורפיזם הראשון θ משרה איזומורפיזם $\bar{\theta}\colon F(X_1)/F(X_1)' \to F(X_2)/F(X_2)'$. לפי מסקנה 17.11, $F(X_1)/F(X_1)' \cong F_m$, $F(X_2)/F(X_2)' \cong F_n$. לכן $F_m \cong F_n$. לכן $m = \operatorname{rk} F_m = \operatorname{rk} F_n = n$. ∎

18. חבורות נילפוטנטיות.

הגדרה 18.1: עבור $H, K \leq G$ מסמנים $[H,K] = \langle [h,k] = h^{-1}k^{-1}hk |\ h \in H, k \in K \rangle \leq G$. אנו נשתמש רק במקרה פרטי $[H,G]$. נעיר ש־$G' = [G,G]$.

תרגיל 18.2:

(א) אם $H_1 \leq H_2 \leq G$ אז $[H_1, G] \leq [H_2, G]$.

(ב) $H \triangleleft G \Leftrightarrow [H,G] \leq H$.

(ג) תהי $K \leq H \leq G, K \triangleleft G$. אז $H/K \leq Z(G/K) \Leftrightarrow [H,G] \leq K$.

פתרון: (א) ברור.

(ב) $[H,G] \leq H \Leftrightarrow$

$$H \triangleleft G \Leftrightarrow h \in H, g \in G \text{ לכל } g^{-1}hg \in H \Leftrightarrow h \in H, g \in G \text{ לכל } h^{-1}g^{-1}hg = [h,g] \in H.$$

(ג) $[H,G] \leq K \Leftrightarrow h \in H, g \in G$ לכל $h^{-1}g^{-1}hg \in K \Leftrightarrow h \in H, g \in G$ לכל $ghK = hgK \Leftrightarrow$
$\Leftrightarrow h \in H, g \in G$ לכל $(gK)(hK) = (hK)(gK) \Leftrightarrow H/K \leq Z(G/K)$. ∎

הגדרה 18.3: נגדיר באינדוקציה $\Phi_i = \Phi_i(G) \leq G$ באפן הבא:

$$\Phi_1 = G, \Phi_2 = [G,G] = G', \Phi_{i+1} = [\Phi_i, G].$$

למה 18.4:

(א) $\Phi_{i+1} \leq \Phi_i$.

(ב) $\Phi_i \triangleleft G$.

(ג) $\Phi_i / \Phi_{i+1} \leq Z(G/\Phi_{i+1})$.

הוכחה:

(א) באינדוקציה: עבור $i = 1$ זה ברור, ואם $\Phi_{i+1} \leq \Phi_i$ אז לפי תרגיל 18.2(א)
$\Phi_{i+2} = [\Phi_{i+1}, G] \leq [\Phi_i, G] = \Phi_{i+1}$.

(ב) נובע מ־(א) לפי תרגיל 18.2(ב).

(ג) לפי תרגיל 18.2(ג), עם $K = \Phi_{i+1}$, $H = \Phi_i$; לפי ההגדרה, $[H,G] = K$. ∎

הגדרה 18.5:

$$\cdots \triangleleft \Phi_i \triangleleft \cdots \triangleleft \Phi_2 \triangleleft \Phi_1 = G \tag{1}$$

נקראת **הסדרה המרכזית היורדת של** G.

הגדרה 18.6: **הסדרה המרכזית העולה** היא סדרה של חבורות נורמליות ב־G

$$\{1\} = Z_0(G) \lhd Z_1(G) \lhd \cdots \lhd Z_i(G) \lhd \cdots$$

המוגדרות כך: $Z_0(G) = \{1\}$, $Z_1(G) = Z(G)$, ו־$Z_{i+1}(G)/Z_i(G) = Z(G/Z_i(G))$. נסמן גם $Z_i = Z_i(G)$. מתקיים $Z_{i+1}/Z_i \lhd G/Z_i$, לכן לפי משפט האיזומורפיזם השלישי $Z_i \lhd G$, לכל i.
כמו כן, $[Z_{i+1}/Z_i, G/Z_i] = \{1\}$, לכן $[Z_{i+1}, G] \leq Z_i$, לכל i.

משפט 18.7: $Z_m = G \Leftrightarrow \Phi_{m+1} = 1$. *יתר על כן:*

(א) *אם* $Z_m = G$ *אז* $\Phi_{i+1} \leq Z_{m-i}$ *לכל* $0 \leq i \leq m$.

(ב) *אם* $\Phi_{m+1} = 1$ *אז* $\Phi_{i+1} \leq Z_{m-i}$ *לכל* $0 \leq i \leq m$.

הוכחה: (א) באינדוקציה על i. עבור $i = 0$ שני האגפים הם G. נניח $\Phi_{i+1} \leq Z_{m-i}$, אז לפי תרגיל 18.2,

$$\Phi_{i+2} = [\Phi_{i+1}, G] \leq [Z_{m-i}, G] \leq Z_{m-i-1}.$$

(ב) צריך להוכיח: $\Phi_{m-j+1} \leq Z_j$ לכל $0 \leq j \leq m$. ההוכחה באינדוקציה על j. עבור $j = 0$ שני האגפים הם 1. נניח $\Phi_{m-j+1} \leq Z_j$. אז האפימורפיזם הקנוני $\pi: G \to G/Z_j$ משרה את האפימורפיזם $\pi': G/\Phi_{m-j+1} \to G/Z_j$. לפי למה 18.4(ג), $\Phi_{m-j}/\Phi_{m-j+1} \leq Z(G/\Phi_{m-j+1})$, ומכאן (הסברו!) $\pi(\Phi_{m-j}) = \pi'(\Phi_{m-j}/\Phi_{m-j+1}) \leq Z(G/Z_j)$, כלומר, $\Phi_{m-j}Z_j/Z_j \leq Z_{j+1}/Z_j$ ומכאן $\Phi_{m-j}Z_j \leq Z_{j+1}$.

נניח $Z_m = G$. לפי (א) (עם $i = m$) מתקיים $\Phi_{m+1} \leq Z_0 = 1$, לכן $\Phi_{m+1} = 1$,

נניח $\Phi_{m+1} = 1$. לפי (ב)(עם $i = 0$) מתקיים $G = \Phi_1 \leq Z_m$, לכן $Z_m = G$. ∎

הגדרה 18.8: G נקראת **נילפוטנטית** אם יש m כך ש־$\Phi_{m+1}(G) = 1$, ואז m מזערי כזה נקרא **המחלקת הנילפוטניות** של G.

דוגמה 18.9: כל חבורה חילופית היא נילפוטנטית ($Z = G$). כל חבורת־p (ז.א. סופית) היא נילפוטנטית (המרכז לא טריוויאלי). כל חבורה נילפוטנטית היא פתירה (גורמי הסדרה המרכזית חילופיים). S_3 אינה נילפוטנטית, כי $Z = 1$.

למה 18.10: *אם* $G_1, \ldots, G_r$ *נילפוטנטיות אז* $G_1 \times \cdots \times G_r$ *נילפוטנטית.*

הוכחה: די להראות כי $\Phi_i(G_1 \times \cdots \times G_r) = \Phi_i(G_1) \times \cdots \times \Phi_i(G_r)$. באינדוקציה: עבור $i = 1$ זה ברור.

$$\Phi_{i+1}(G_1 \times \cdots \times G_r) = [\Phi_i(G_1 \times \cdots \times G_r), G_1 \times \cdots \times G_r] =$$
$$= [\Phi_i(G_1) \times \cdots \times \Phi_i(G_r), G_1 \times \cdots \times G_r] = [\Phi_i(G_1), G_1] \times \cdots \times [\Phi_i(G_r), G_r] =$$
$$= \Phi_{i+1}(G_1) \times \cdots \times \Phi_{i+1}(G_r)$$ ∎

למה 18.11: *אם G נילפוטנטית ו־$H < G$ אז $H < N_G(H)$. (משפט זה הוכח עבור חבורות־p –למה 12.4.)*

הוכחה: יהי i השלם הראשון כך ש־$\Phi_{i+1} \leq H$. אז יש $a \in \Phi_i \setminus H$. נראה ש־$a \in N_G(H)$. לכל $h \in H$

$$a^{-1}hah^{-1} = [a, h^{-1}] \in [\Phi_i, G] = \Phi_{i+1} \leq H$$

ולכן $a^{-1}ha \in H$. מכאן $a \in N_G(H)$. ∎

תרגיל 18.12: *תהי P חבורת סילוב־p של חבורה סופית G. אם $N_G(P) \leq H \leq G$ אז $N_G(H) = H$.*

פתרון: אכן, נסמן $G_0 = N_G(H)$. מתקיים $P \lhd N_G(P) \leq H \lhd G_0 \leq G$. נשים לב, ש־$P$ היא גם חבורת סילוב־p של G_0. לפי הארגומנט של פרטיני (תרגיל בית) $G_0 = HN_{G_0}(P)$. אבל $N_{G_0}(P) \leq N_G(P) \leq H$, לכן $HN_{G_0}(P) = H$. מכאן $H = G_0$. ∎

משפט 18.13: *תהי G חבורה סופית. התנאים הבאים שקולים:*

(א) *G נילפוטנטית.*

(ב) *כל חבורות סילוב־p של G הן נורמליות ב־G.*

(ג) *G היא המכפלה הישרה של חבורות סילוב־p שלה.*

הוכחה:

(א) $\Leftarrow$ (ב): תהי P חבורת סילוב־p של G, ויהי $H = N_G(P)$. צ"ל: $H = G$. לפי תרגיל 18.12, $N_G(H) = H$. לכן לפי למה 18.11, $H = G$.

(ב) $\Leftarrow$ (ג): יהי $|G| = p_1^{m_1} \cdots p_r^{m_r}$ הפירוק של $|G|$ לחזקות של מספרים ראשוניים שונים. לכל $1 \leq i \leq r$ תהי P_i חבורת סילוב־p_i של G. אז $|P_i| = p_i^{m_i}$. לכן $|P_1|, \ldots, |P_r|$ זרים בזוגות ו־$|G| = |P_1| \cdots |P_r|$. לפי ההנחה $P_1, \ldots, P_r \lhd G$. לכן לפי למה 10.4, $G = P_1 \times \cdots \times P_r$.

(ג) $\Leftarrow$ (א): לפי דוגמה 18.9 חבורות סילוב־p של G הינן נילפוטנטיות. לפי למה 18.10 המכפלה הישרה שלהן G נילפוטנטית. ∎

19. מכפלות ישרות למחצה.

תהיינה A, N חבורות, ויהי $\psi\colon A \to \mathrm{Aut}(N) \leq S(N)$ הומומורפיזם. הוא מגדיר פעולה של A על N, אבל כך שכל $a \in A$ פועל לא רק כתמורה של N, אלא כאוטומורפיזם של N. כלומר, בנוסף לתנאים הרגילים של פעולה מתקיים גם $^a(n_1 n_2) = {}^a n_1 \, {}^a n_2$ לכל $a \in A,\ n_1, n_2 \in N$.

נסמן ב־$A \ltimes N$ את הקבוצה $N \times A$ ונגדיר עליה כפל באופן הבא:

$$\big(n_1, a_1\big)\big(n_2, a_2\big) = \big(n_1 \cdot {}^{a_1} n_2, a_1 a_2\big) = \big(n_1 \cdot \psi(a_1)(n_2), a_1 a_2\big). \tag{1}$$

תהיינה $\alpha\colon A \to N \ltimes A$, $\beta\colon N \to N \ltimes A$ נתונות על ידי $\alpha(a) = \big(1, a\big), \beta(n) = \big(n, 1\big)$.

למה 19.1: *נסמן $G = N \ltimes A$.*

(א) *G עם הפעולה הנ"ל היא חבורה. היא נקראת המכפלה הישרה למחצה של A ו־N (ביחס ל־ψ).*

(ב) *ההעתקות α ו־β הן הומומורפיזמים חח"ע.*

נזהה את A עם תמונתה A^* על ידי α ואת N עם תמונתה N^* על ידי β.

(ג) $N \lhd G$, $AN = G$, $A \leq G$, $A \cap N = \{1\}$.

(ד) $ana^{-1} = {}^a n$ *(כלומר:* $\alpha(a)\beta(n)\alpha(a)^{-1} = \beta({}^a n)$ *לכל* $a \in A,\ n \in N$.

הוכחה: (א) הכפל הנו אסוציאטיבי:

$$\begin{aligned}
&\Big(\big(n_1, a_1\big)\big(n_2, a_2\big)\Big)\big(n_3, a_3\big) = \\
&\quad = \big(n_1 \, {}^{a_1} n_2, a_1 a_2\big)\big(n_3, a_3\big) = \big(n_1 \, {}^{a_1} n_2 \, {}^{a_1 a_2} n_3, (a_1 a_2) a_3\big) \\
&\big(n_1, a_1\big)\Big(\big(n_2, a_2\big)\big(n_3, a_3\big)\Big) = \\
&\quad = \big(n_1, a_1\big)\big(n_2 \, {}^{a_2} n_3, a_2 a_3\big) = \big(n_1 \, {}^{a_1}(n_2 \, {}^{a_2} n_3), a_1 (a_2 a_3)\big)
\end{aligned}$$

וברור ששני הביטויים שווים.

איבר היחידה הוא $(1,1)$. ההופכי של (n, a) הוא $({}^{a^{-1}} n^{-1}, a^{-1})$.

(ב) ברור

(ג) מתוך (ב) נובע ש־$A, N \leq G$. נראה ש־$N \lhd G$:

$$(n_1, a_1)(n_2, 1)(n_1, a_1)^{-1} = \big(n_1({}^{a_1} n_2), a_1\big)({}^{a_1^{-1}} n_1^{-1}, a_1^{-1}) = (\text{משהו}, 1) \in N.$$

(ד) $\big(1, a\big)\big(n, 1\big)\big(1, a^{-1}\big) = \big({}^a n, a\big)\big(1, a^{-1}\big) = \big({}^a n, 1\big)$. ∎

משפט 19.2: *תהי G חבורה ו־$N \lhd G, A \leq G$ כך ש־$N \cap A = \{1\}, NA = G$. אזי $\psi(a)(n) := ana^{-1}$ מגדירה הומומורפיזם $\psi\colon A \to \mathrm{Aut}(N)$ (ובפרט $^a n := ana^{-1}$ מגדירה פעולה של A על N) וההעתקה $N \ltimes A \to G$ הנתונה על ידי $na \mapsto (n, a)$ היא איזומורפיזם אשר הינו זהות על A ועל N.*

הוכחה: ברור ש־ψ הומומורפיזם. ההעתקה $N \ltimes A \to G$ היא הומומורפיזם:

$$\big(n_1, a_1\big)\big(n_2, a_2\big) = \big(n_1 \, {}^{a_1} n_2, a_1 a_2\big) \mapsto n_1 \, {}^{a_1} n_2 a_1 a_2 = n_1 (a_1 n_2 a_1^{-1}) a_1 a_2 = (n_1 a_1)(n_2 a_2).$$

היא על, כי $G = NA$, וגרעינה $\{1\}$, כי $N \cap A = \{1\}$. ∎

הערה 19.3: תהי $G = N \rtimes A$. אז $G = N \times A$ אם ורק אם ψ טריוויאלי, ז.א. $\psi(A) = \{1\}$. אכן, זה נובע מהבוחן של משפט 10.1(ג): מתקיים $G = NA$, ההצגה $g = na$ של כל $g \in G$ היא יחידה, כי ההעתקה $(n, a) \mapsto na$ חח"ע. מתקיים $na = an$ אם ורק אם ${}^a n = \psi(a)(n) = n$ לכל $n \in N, a \in A$, כלומר, אם ורק אם $\psi(N) = \{1\}$.

דוגמה 19.4: $N = \mathbb{Z}/n\mathbb{Z}$, באשר $n > 2$. אזי $k \mapsto -k$ הוא אוטומורפיזם ω של N מסדר 2. נגדיר הומומורפיזם $\psi\colon \mathbb{Z}/2\mathbb{Z} = \{\pm 1\} \to N$ על ידי $\psi(1) = 1, \psi(-1) = \omega$. אז $D_n = \mathbb{Z}/n\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$ חבורה מסדר $2n$, הנקראת **חבורה דיהדרית**. היא מכילה את N כתת חבורה נורמלית. כל איבר ב־$D_n \smallsetminus N$ הוא מסדר 2. אכן, $((k,-1)(k,-1) = (k + \psi(-1)(k), 1) = (k-k, 1) = 1$). היא אינה חילופית לפי למה 19.1 (ד). נעיר ש־$D_3 = S_3$, ו־D_4 היא חבורה לא חילופית מסדר 8.

דוגמה 19.5: כל חבורה G מסדר 2001 היא מעגלית.

אכן, $2001 = 3 \cdot 23 \cdot 29$. (נסמן ב־$n_p$ את מספר חבורות סילוב־p של G.) אז $n_{23} | 3 \cdot 29$ וגם $n_{23} \equiv 1 \pmod{23}$, ולכן $n_{23} = 1$. באותו אופן $n_{29} = 1$. לכן יש $P \lhd G$ מסדר 23 ו־$Q \lhd G$ מסדר 29. מכאן $PQ \lhd G$ היות ו־$P, Q \lhd PQ$ מסדרים זרים, $PQ = P \times Q$. ובפרט $|PQ| = 23 \cdot 29$. תהי S חבורת סילוב־3 של G. אז $S \cap (PQ) = \{1\}$, $|S(PQ)| = 3 \cdot 23 \cdot 29$ (כי הסדר מתחלק בכל אחד מהראשוניים באגף ימין), ולכן $S(PQ) = G$. לכן $G = (PQ) \rtimes S$ ביחס לאיזה הומומורפיזם $\psi\colon S \to \mathrm{Aut}(PQ)$ אבל $S \cong \mathbb{Z}/3\mathbb{Z}$, ואילו

$$\mathrm{Aut}(PQ) = \mathrm{Aut}(P) \times \mathrm{Aut}(Q) \cong \mathrm{Aut}(\mathbb{Z}/23\mathbb{Z}) \times \mathrm{Aut}(\mathbb{Z}/29\mathbb{Z}) \cong \mathbb{Z}/22\mathbb{Z} \oplus \mathbb{Z}/28\mathbb{Z}$$

מסדר זר ל־3, לכן ψ טריוויאלי. לפי הערה 19.3,

$$G = S \times (P \times Q) \cong \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/23\mathbb{Z} \oplus \mathbb{Z}/29\mathbb{Z} \cong \mathbb{Z}/(3 \cdot 23 \cdot 29\mathbb{Z}) \cong \mathbb{Z}/2001\mathbb{Z}.$$

תרגיל 19.6: *א. יהי $\beta\colon N \to N'$ איזומורפיזם של חבורות. אז β מגדיר איזומורפיזם $\hat{\beta}\colon \mathrm{Aut}(N) \to \mathrm{Aut}(N')$ על ידי $\hat{\beta}(\omega) = \beta\omega\beta^{-1}$ (במלים אחרות, $\hat{\beta}$ מוגדר כך שהתרשים הבא חילופי.)*

$$\begin{array}{ccc} N & \xrightarrow{\omega} & N \\ \downarrow{\scriptstyle \beta} & & \downarrow{\scriptstyle \beta} \\ N' & \xrightarrow{\hat{\beta}(\omega)} & N' \end{array}$$

ב. יהיו $\alpha\colon A \to A'$ ו־$\beta\colon N \to N'$ שני איזומורפיזמים של חבורות. תהיינה $N \rtimes^{\psi} A$, $N' \rtimes^{\psi'} A'$ שתי מכפלות ישרות למחצה, מוגדרות בעזרת הומומורפיזמים $\psi\colon A \to \mathrm{Aut}(N)$ ו־$\psi'\colon A' \to \mathrm{Aut}(N')$ כך שהתרשים הבא חילופי

$$\begin{array}{ccc} A & \xrightarrow{\psi} & \mathrm{Aut}(N) \\ \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle \hat{\beta}} \\ A' & \xrightarrow{\psi'} & \mathrm{Aut}(N') \end{array}$$

הראה שההעתקה $N \rtimes^{\psi} A \to N' \rtimes^{\psi'} A'$*, הנתונה על ידי* $(n,a) \mapsto \big(\beta(n), \alpha(a)\big)$ *היא איזומורפיזם.*

הגדרה 19.7: חבורת הסימטריות. יהי $P_n \subseteq \mathbb{R}^2$ מצולע משוכלל בעל n קדקדים, $n \geq 3$. (למשל, P_3 הוא משולש שוה־צלעות.) סימטריה של P_n היא העתקה $\mathbb{R} \to \mathbb{R}$ ששומרת מרחקים ומעתיקה את P_n על עצמו. אוסף הסימטריות של P_n הוא חבורה $\mathrm{Sym}(P)$ תחת ההרכבה. סימטריה נקבעת על ידי פעולתה על קודקודי P_n, ולכן אפשר לראותה כתמורה ב־S_n. מכאן $\mathrm{Sym}(P_n) \leq S_n$.

טענה 19.8: $\mathrm{Sym}(P_n) \cong D_n$.

הוכחה: נתבונן בשני איברים של $\mathrm{Sym}(P_n)$: הסיבוב σ בזוית $\frac{2\pi}{n}$ והשיקוף ε ביחס לציר העובר דרך המרכז ודרך קדקד n. כלומר

$$\varepsilon = (1\ n-1)(2\ n-2)(3\ n-3)\cdots \in \mathrm{Sym}(P_n), \quad \sigma = (12\cdots n).$$

אז $\varepsilon^2 = 1$. תהי $H = \langle \sigma, \varepsilon \rangle \leq \mathrm{Sym}(P_n)$. נראה:

(א) $H \cong D_n$;

(ב) $H = \mathrm{Sym}(P_n)$.

(א) $\mathrm{ord}\,(\sigma) = n$, ולכן $\langle \sigma \rangle \cong \mathbb{Z}/n\mathbb{Z}$. $\mathrm{ord}\,(\varepsilon) = 2$, לכן $\langle \varepsilon \rangle \cong \mathbb{Z}/2\mathbb{Z}$. בוודאי $\langle \sigma \rangle \cap \langle \varepsilon \rangle = 1$. לפי תרגיל 9.6,

$$\varepsilon\sigma\varepsilon^{-1} = \big(\varepsilon(1)\ \varepsilon(2)\ \cdots \varepsilon(n)\big) = (n-1\ n-2 \cdots 2\ 1\ n) = \sigma^{-1}.$$

בפרט $\sigma^{\varepsilon} \in \langle \sigma \rangle$; לכן $\langle \sigma \rangle^{\varepsilon} = \langle \sigma \rangle$; ובוודאי $\sigma^{\sigma}, \sigma^{\sigma^{-1}} \in \langle \sigma \rangle$, לכן $\sigma^h \in \langle \sigma \rangle$ לכל $h \in H$. מכאן $\langle \sigma \rangle \lhd H$. לפי משפט 19.2, $H \cong \langle \sigma \rangle \rtimes \langle \varepsilon \rangle$, כאשר הפעולה נתונה על ידי $\tau^{\varepsilon} = \tau^{-1}$. לפי תרגיל 19.6, $H \cong D_n$.

(ב) תהי $\tau \in \mathrm{Sym}(P_n)$. משיקולים גיאומטריים נובע (בלי הוכחה):

"אם $\tau(n) = n$ אז $\tau(1) = 1$ או $\tau(1) = n-1$ ובמקרה הראשון $\tau = 1$".

נניח $\tau(n) = i$. יש $\sigma' \in \langle \sigma \rangle \leq H$ כך ש־$\sigma'(i) = n$ ולכן $\sigma'\tau(n) = n$. כעת $\sigma'\tau \in \mathrm{Sym}(P_n)$ ודי להראות $\sigma'\tau \in H$. לכן בה"כ $\tau(n) = n$. אם $\tau(1) = 1$ אז $\tau = 1 \in H$. אם $\tau(1) = n-1$ אז $\varepsilon\tau(1) = n$ ו־$\varepsilon\tau(n) = 1$ ולכן $\varepsilon\tau = \varepsilon^{-1} \in H$, כלומר $\tau \in H$. ∎

הערה 19.9: באופן דומה אפשר לדון בחבורת הסימטריות של גוף משוכלל, למשל פירמידה (= ארבעון).

הגדרה 19.10: חבורת הקווטרניונים של Hamilton. $Q = \{\pm 1, \pm i, \pm j \pm k\}$ עם כלל הכפל:

לכל $a \in Q$: $1a = a = a1$; $(-1)a = -a = a(-1)$, באשר $-(-a) = a$.

$ij = k, jk = i, ki = j$;

$ji = -k, kj = -i, ik = -j$;

$(\pm i)^2 = (\pm j)^2 = (\pm k)^2 = -1$;

תרגיל 19.11: *Q היא חבורה מסדר 8. היא איננה חילופית. יש לה 6 איברים מסדר 4 ואחד מסדר 2. בפרט $Q \neq D_4$.*

תרגיל 19.12: *תהי G חבורה לא חילופית מסדר 8. אזי $G \cong D_4$ או $G \cong Q$.*

הוכחה: כל איברי $G \smallsetminus \{1\}$ הם מסדר $2, 4, 8$. לא כולם מסדר 2, כי G אינה חילופית; אין איבר מסדר 8, כי G אינה מעגלית. לכן יש $\sigma \in G$ מסדר 4; אז $2 = (G : \langle\sigma\rangle)$, לכן $\langle\sigma\rangle \lhd G$. יהי $\tau \in G \smallsetminus \langle\sigma\rangle$. אז $\langle\sigma, \tau\rangle = G$, כי $\langle\sigma\rangle < \langle\sigma, \tau\rangle \leq G$. מתקיים

$$ {}^{\tau}\sigma \in \langle\sigma\rangle = \{1, \sigma, \sigma^2, \sigma\} $$

ו־$\operatorname{ord}({}^{\tau}\sigma) = \operatorname{ord}(\sigma) = 4$; לכן ${}^{\tau}\sigma = \sigma$ או ${}^{\tau}\sigma = \sigma^{-1}$. המקרה הראשון לא יתכן, כי אז $\tau\sigma = \sigma\tau$ ולכן G חילופית. אם כן, ${}^{\tau}\sigma = \sigma^{-1}$, ומכאן, ${}^{\tau}(\sigma^i) = (\sigma^{-1})^i = (\sigma^i)^{-1}$ לכל i, כלומר,

$$ {}^{\tau}\alpha = \alpha^{-1} \quad , \quad \text{לכל } \alpha \in \langle\sigma\rangle. \tag{2} $$

נבדיל בין שני מקרים:

(א) $\operatorname{ord}(\tau) = 2$.

אז $\langle\sigma\rangle \cap \langle\tau\rangle = \{1\}$ ו־$G = \langle\sigma\rangle\langle\tau\rangle$, לכן $G = \langle\sigma\rangle \rtimes \langle\tau\rangle$, באשר הפעולה של $\langle\tau\rangle$ על $\langle\sigma\rangle$ נתונה על ידי (2). לכן $G \cong D_4$.

(ב) $\operatorname{ord}(\tau) = 4$.

אז לא יתכן ש־$\langle\sigma\rangle \cap \langle\tau\rangle = \{1\}$, אחרת $G = \langle\sigma\rangle \rtimes \langle\tau\rangle$ מסדר $4 \cdot 4 = 16$. לכן $\langle\sigma\rangle \cap \langle\tau\rangle$ מסדר 2, כלומר, $\tau^2 \in \langle\sigma\rangle$, ומכאן $\tau^2 = \sigma^2$, כי τ^2 מסדר 2, ו־σ^2 הוא האיבר היחיד של $\langle\sigma\rangle$ מסדר 2. נסמן

$$ \begin{array}{llll} -1 = \sigma^2 = \tau^2, & i = \tau, & j = \sigma, & k = \tau\sigma, \\ & -i = (-1)i, & -j = (-1)j, & -k = (-1)k \end{array} $$

אז

$$ G = \langle\sigma\rangle \cup \tau\langle\sigma\rangle = \{1, \sigma, \sigma^2, \sigma^3\} \cup \{\tau, \tau\sigma, \tau\sigma^2, \tau\sigma^3\} = \{1, j, -1, -j\} \cup \{i, k, -i, -k\} $$

וקל לוודא שמתקיים לוח הכפל של Q בהגדרה 19.10. למשל,

$$ ki = (\tau\sigma)\tau = (\tau\sigma\tau^{-1})\tau^2 = \sigma^{-1}\sigma^2 = \sigma = j, $$

$$ jk = \sigma(\tau\sigma) = \sigma(\tau\sigma\tau^{-1})\tau = \sigma\sigma^{-1}\tau = \tau = i. $$

∎

20. תרגילים.

תרגיל 20.1: *תהי G חבורה מסדר 1225. הראה שהיא חילופית. כמה חבורות מסדר זה ישנן?*

הוכחה: פתרון: $|G| = 1225 = 5^2 \cdot 7^2$. יש חבורת סילוב־$5$ יחידה A וגם חבורת סילוב־7 יחידה B. לכן הן נורמליות ב־G. הן מסדרים זרים ו־$|G| = |A| \cdot |B|$, לכן $G = A \times B$. A ו־B חילופיות, לכן G חילופית. יש 4 חבורות כאלה.

תרגיל 20.2: *תהי G חבורה מסדר 150. הראה שיש $N \triangleleft G$ מסדר 25 או מסדר 5.*

הוכחה: פתרון: $150 = 2 \cdot 3 \cdot 5^2$. אם יש רק חבורת סילוב־$5$ אחת, סיימנו. אחרת יש בדיוק 6 חבורות סילוב־5 ב־G. תהי P אחת מהן.

(א) נניח שחיתוך של כל שתים מביניהן הוא טריוויאלי. אז יש $6 \cdot 24$ איברים מסדר 25 או מסדר 5 ב־G. נותרו עוד 6 איברים. יש 25 או 10 או 1 חבורות סילוב־3, לכן יש רק אחת. נסמן אותה K. אז $K \triangleleft G$. $|G/K| = 2 \cdot 5^2$, ומכאן שיש ל־G/K חבורת סילוב־5 יחידה, היא PK/K. לכן $PK/K \triangleleft G/K$, ומכאן ש־$PK \triangleleft G$. אבל $|PK| = 3 \cdot 5^2$, ומכאן שיש ל־PK חבורת סילוב־5 יחידה, היא P. מכאן $P \triangleleft G$. סתירה.

(ב) נניח שיש עוד חבורת סילוב־5 P' כך ש־$P \cap P' \neq \{1\}$. אז $|P \cap P'| = 5$, ומכאן $|\langle P, P' \rangle| \geq |PP'| = |P| \cdot |P'|/|P \cap P'| = 125$. היות ו־$|G|$ | $|\langle P, P' \rangle|$, יוצא $\langle P, P' \rangle = G$. אך $P \cap P' \triangleleft P, P'$, כי P, P' חילופיות. לכן $P \cap P' \triangleleft G$.

הוכחה נוספת: כמו קודם, אך במקום (א),(ב)

הפעולה של G על $\{gP \mid g \in G\}$ על ידי כפל משמאל מגדירה הומומורפיזם $\psi: G \to S_6$. יהי $K = \mathrm{Ker}(\psi)$. אז $K \leq P$ ו־$|G/K|$ מחלק את $|S_6| = 6!$. כיוון ש־$6! \nmid |G| = 150$, יוצא $K \neq 1$.

תרגיל 20.3: *מצא את כל החבורות מסדר 105, עד כדי איזומורפיזם ($105 = 3 \cdot 5 \cdot 7$).*

הוכחה: פתרון: אם G חילופית אז היא מעגלית. נניח כי G אינה חילופית. מספר חבורות סילוב־3 הוא 1 או 7, ולכן יש ב־G 2 או 1 איברים מסדר 3. מספר חבורות סילוב־5 הוא 1 או 21, ולכן יש ב־G 4 או 84 איברים מסדר 5. מספר חבורות סילוב־7 הוא 1 או 15, ולכן יש ב־G 6 או 90 איברים מסדר 7. חשבון קל מראה שלפחות עבור שני ראשונים שונים חבורות סילוב־p המתאימות הן יחידות ב־G, ולכן נורמליות. (לכאורה יתכן $P_7 \triangleleft G$, $P_3, P_5 \not\triangleleft G$, כי אז יש $104 = 6 + 84 + 14$ איברים מסדרים $7, 5, 3$ ועוד איבר היחידה - ותו לא. אך $P_5 P_7 \leq G$ מסדר 35 הינה מעגלית ולכן יש בה איבר מסדר 35, סתירה.) אז גם מכפלתן נורמלית ב־G; חבורה זו היא מכפלה ישרה של שתי חבורות מסדרים ראשונים זרים ולכן מעגלית. לכן G אחת המכפלות הישרות להמחצה הבאות:

(א) $\mathbb{Z}/3\mathbb{Z}$ פועלת על $\mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z}$.

(ב) $\mathbb{Z}/5\mathbb{Z}$ פועלת על $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z}$.

(ג) $\mathbb{Z}/7\mathbb{Z}$ פועלת על $\mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$.

אם הפעולה טריויאלית אז המכפלה הישרה למחצה היא המכפלה הישרה, ולכן G חילופית. זה המצב במקרים (ב), (ג). במקרה (א) תיתכן פעולה לא טריויאלית:

$$\psi\colon \mathbb{Z}/3\mathbb{Z} \to \mathrm{Aut}(\mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z}) = \mathrm{Aut}(\mathbb{Z}/5\mathbb{Z}) \times \mathrm{Aut}(\mathbb{Z}/7\mathbb{Z}) = \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}$$

המעתיקה את $\mathbb{Z}/3\mathbb{Z}$ על החבורה החלקית היחידה מסדר 3 של אגף ימין. העתקה כזאת הינה יחידה, עד כדי הומומורפיזם (לפרט).

תרגיל 20.4 (השערת Schreier): *תהי G חבורה סופית ויהי α אוטומורפיזם של G ללא נקודות שבת, דהינו:*

$$\{g \in G |\ g^\alpha = g\} = \{1\}.$$

אזי G פתירה.

אנו לא נפתור כאן השערה מפורסמת זו. ידוע הוא (ואנו נקבל זאת ללא הוכחה), שהשערת שרייר נכונה לכל חבורות פשוטות לא חילופיות. (כאן משתמשים כמובן במשפט המיון של חבורות סופיות פשוטות.) נוכיח את ההשערה תחת הנחה זו, באינדוקציה על $|G|$.

תחילה:

טענה 1: *ההעתקה $g \mapsto g^{-1}g^\alpha$ היא תמורה של G.*

אכן, נראה שהיא חח"ע: נניח $g^{-1}g^\alpha = h^{-1}h^\alpha$, אז $hg^{-1} = (hg^{-1})^\alpha$, לכן $hg^{-1} = 1$, כלומר $h = g$.

אם G פשוטה (חילופית או לא), סיימנו. נניח כי G אינה פשוטה. אז יש $K \lhd G$ מזערית (כלומר $K \neq 1$, ואין $K_0 \lhd G$ כך ש־$1 < K_0 < K$).

טענה: $K^\alpha = K$.

יהי n המספר הטבעי הקטן ביותר כך ש־$K^{\alpha^n} = K$ ונניח בשלילה כי $n > 1$. לכל $1 \leq i < n$ מתקיים $K^{\alpha^i} \neq K$; אבל $K^{\alpha^i} \lhd G^{\alpha^i} = G$, לכן $K^{\alpha^i} \cap K \lhd G$ ומהמזעריות $K^{\alpha^i} \cap K = 1$. מכאן, לכל $1 \leq i < j < n$ מתקיים $K^{\alpha^i} \cap K^{\alpha^j} = (K \cap K^{\alpha^{j-i}})^{\alpha^i} = 1$. קיבלנו ש־ $K^{\alpha^i}K^{\alpha^j} = K^{\alpha^i} \times K^{\alpha^j}$. ולכן $ab = ba$ לכל $a \in K^{\alpha^i}, b \in K^{\alpha^j}$.

נבחר $1 \neq x \in K$. אז $1 \neq g = xx^\alpha \cdots x^{\alpha^{n-1}} \in G$. היות ו־ $x, x^\alpha, \ldots, x^{\alpha^{n-1}}$ מתחלפים ביניהם, $g^\alpha = x^\alpha \cdots x^{\alpha^{n-1}}x = g$, סתירה.

מסקנה: *הצמצום של α ל־ K הוא אוטומורפיזם של K ללא נקודות שבת.*

טענה: 2: *$gK \mapsto (gK)^\alpha = g^\alpha K$ הוא אוטומורפיזם ללא נקודות שבת של G/K.*

אכן, נניח כי $g^\alpha K = gK$. אז $g^{-1}g^\alpha \in K$. לפי טענה 1 (עבור K) יש $k \in K$ כך ש-$k^{-1}k^\alpha = g^{-1}g^\alpha$.
בגלל חח"ע $g = k(\in K)$ ומכאן $gK = K$.

לפי הנחת האינדוקציה $K, G/K$ פתירות ולכן G פתירה. ∎

תרגיל 20.5: *תהי H תת חבורה של חבורה סופית G בעלת אינדקס 5 ויהי $a \in Z(G)$ מסדר 3. הוכח כי $a \in H$.*

פתרון: כל תת חבורה של המרכז של G הינה נורמלית ב-G, לכן $\langle a\rangle \lhd G$. מכאן $\langle a\rangle H \leq G$. מתקיים (לא לפי משפט האיזומורפיזם השני) $(\langle a\rangle H : H) = \big(\langle a\rangle : (\langle a\rangle \cap H)\big)$. אך אגף שמאל מחלק את $(G : H) = 5$ ואילו אגף ימין מחלק את $|\langle a\rangle| = 3$. לכן מספר זה הוא 1. מכאן $\langle a\rangle \leq H$. ∎

תרגיל 20.6: *תהי G חבורה סופית ויהי p הראשוני הקטן ביותר שמחלק את הסדר של G. תהי $H \leq G$ כך ש-$(G : H) = p$. הוכח כי $H \lhd G$.*

פתרון: החבורה G פועלת (משמאל) על $X = \{gH \mid g \in G\}$ על ידי כפל משמאל. פעולה זו מגדירה הומומורפיזם $\psi\colon G \to S(X) \cong S_p$ על ידי $\psi(g')(gH) = g'gH$. יהי $\bar{G} = \psi(G) \leq S(X)$. אז הסדר של $\bar{G}$ מחלק את $|S_p| = p!$ וגם את $|G|$, לכן, לפי הנתון, הוא מחלק את p.
יהי $K = \mathrm{Ker}(\psi)$. אז לכל $g' \in K$ מתקיים $1H = g'(1H) = g'H$, לכן $g' \in H$. מכאן $K \leq H$.
לכן $(G : H) = p$ מחלק את $(G : K) = |G/K|$
אבל $G/K \cong \bar{G}$. לכן $(G : K) = p = (G : H)$ ומכאן $H = K$. בפרט $H \lhd G$. ∎

תרגיל 20.7: *תהיינה A, B, C חבורות חילופיות נוצרות סופית. נניח כי $A \oplus B \cong A \oplus C$. הוכח כי $B \cong C$.*

פתרון: פתרון שגוי: $(A \oplus B)/A \cong B$, $(A \oplus C)/A \cong C$, לכן מהאיזומורפיזם הנתון נובע $B \cong C$.
נציג את A, B, C כסכום ישר של חבורות מעגליות מסדר אינסופי ומסדר שהוא חזקה של ראשוני. האיזומורפיזם המבוקש יתקבל מיחידות ההצגה הזאת.
ביתר פירוט, נניח כי $\mathbb{Z}/p^m\mathbb{Z}$ (באשר p ראשוני) או $\mathbb{Z}$ מופיעה

- $a \geq 0$ פעמים בפירוק של A;
- $b \geq 0$ פעמים בפירוק של B;
- $c \geq 0$ פעמים בפירוק של C.

אז היא מפיעה

- $a + c \geq 0$ פעמים בפירוק של $A \oplus B$;
- $b + c \geq 0$ פעמים בפירוק של $A \oplus C$.

בגלל האיזומורפיזם הנתון ויחידות הפירוק, $a + b = a + c$ ולכן $b = c$. מכאן של-B, C אותו פירוק ולכן $B \cong C$. ∎

תרגיל 20.8: *תהיינה G_1, G_2 פשוטות. תהי $G = G_1 \times G_2$ ותהי $N \triangleleft G$ לא טריוויאלית. הוכח:*

(א) $N \cong G_1$ או $N \cong G_2$.

(ב) *תהי $\pi : G \to G_1$ ההטלה על הקואורדינטה הראשונה. אז $N = G_2$ או π מעתיק באופן חח"ע את N על G_1.*

(ההוכחות של שני החלקים אינן תלויות; חלק שני חזק יותר מהחלק הראשון.)

פתרון: (א) $1 \triangleleft G_1 \triangleleft G$ היא סדרת הרכב, שמנותיה הן G_1, G_2. גם $1 \triangleleft N \triangleleft G$ סדרה נורמלית ללא חזרות. יש לה עידון לסדרת הרכב; אך כיוון שבסדרת הרכב יש 2 גורמים בדיוק, היא כבר בעצמה סדרת הרכב. לכן $N \cong G_1$ (ו־$G/N \cong G_2$) או $N \cong G_2$ (ו־$G/N \cong G_1$).

(ב) $N \triangleleft G$, לכן $\pi(N) \triangleleft \pi(G) = G_1$. אך G_1 פשוטה, לכן $\pi(N) = 1$ או $\pi(N) = G_1$. במקרה הראשון $N \leq \operatorname{Ker}\pi = G_2$ ולכן, כיוון ש־G_2 פשוטה, $N = G_2$. במקרה השני הגרעין של $\pi|_N$ הוא $G_2 \cap N$. הוא אינו N (כי $\pi(N) \neq 1$), ולכן, כיוון שהוא נורמלי ב־G_2 הפשוטה, הוא 1. ∎

תרגיל 20.9: *תהיינה G_1, G_2 פשוטות לא אבליות. תהי $G = G_1 \times G_2$ ותהי $N \triangleleft G$ לא טריוויאלית. אז $N = G_1$ או $N = G_2$.*

פתרון: עבור $i = 1, 2$ תהי $\varphi_i : N \to G_i$ הצמצום של ההטלה על הקואורדינטה ה־i ל־N. לפי תרגיל 20.08(ב) אפשר להניח כי φ_1, φ_2 איזומורפיזמים. אז $\varphi = \varphi_2 \circ \varphi_1^{-1} : G_1 \to G_2$ הוא איזומורפיזם ומתקיים $N = \{(g, \varphi(g)) | \ g \in G_1\}$

כיוון ש־G_1 אינה חילופית, יש $a, g \in G_1$ כך ש־$g^a \neq g$. אז $\varphi(g^a) \neq \varphi(g)$, לכן $(g, \varphi(g))^{(a,1)} = (g^a, \varphi(g)) \notin N$, בסתירה ל־$N \triangleleft G$. ∎

תרגיל 20.10: *תהיינה $K \triangleleft G$ כך ש־$G/K \cong \mathbb{Z}$. אז יש $H \leq G$ מעגלית אינסופית כך ש־$H \cap K = 1$ ו־$G = HK$. (לכן G מכפלה ישרה למחצה של K, H.)*

פתרון: יש $h \in G$ כך ש־hK יוצר של חבורת המנה G/K. נגדיר $H = \langle h \rangle$. כל איבר של H הוא מהצורה h^i, באשר $i \in \mathbb{Z}$. אם גם $h^i \in K$, אז $(hK)^i = h^i K = K$, וכיוון ש־$\operatorname{ord} hK = \infty$, זה יתכן רק אם $i = 0$; אז $h^i = 1$. לכן $H \cap K = 1$.

החבורה HK מכילה את K ותמונתה ב־G/K היא G/K כולה, כי היא מכילה את היוצר hK. לפי משפט האיזומורפיזם השלישי $HK = G$. ∎

תרגיל 20.11: *(א) הוכח ש־S_n נוצרת על ידי $(12), (13), \ldots, (1n)$.*

(ב) *הוכח ש־S_n נוצרת על ידי $(12), (123\ldots n)$.*

פתרון: (א) $(1i)(1j)(1i) = (ij)$ לכל $i, j \geq 1$. לכן $\langle (12), (13), \ldots, (1n) \rangle$ מכילה את כל החישוקונים.

(ב) נסמן $\pi = (123\ldots n)$ ותהי $G = \langle \pi \rangle$. לפי (א) די להוכיח כי $(12), (13), \ldots, (1n) \in G$.

נניח באינדוקציה כי $(12), (13), \ldots, (1k) \in G$. אז $(k \ k+1) = \pi^{k-1}(12)\pi^{-k} \in G$, לכן $(1 \ k+1) = (1k)(k \ k+1)(1k) \in G$. ∎

תרגיל 20.12: *תהי G יהיו n מספר טבעי כך ש־$(xy)^n = x^n y^n$ לכל $x, y \in G$.*

(א) *הוכח כי $H = \{z \in G | \ z^n = 1\}$ ו־$K = \{x^n | \ x \in G\}$ הן תת חבורות נורמליות של G.*

(ב) *אם G סופית, הוכח כי $|G| = |H| \cdot |K|$.*

(ג) *האם בהכרח $H \cap K = \{1\}$?*

פתרון: (א) נגדיר $\varphi : G \to G$ על ידי $\varphi(x) = x^n$. אז φ הומומורפיזם, $K = \operatorname{Ker}\varphi$, $H = \operatorname{Im}(\varphi)$. לכן $K \lhd G$, $H \leq G$. מתקיים $H \lhd G$, כי לכל $g, x \in G$ מתקיים $(x^n)^g = (x^g)^n \in H$.

(ב) לפי משפט האיזומורפיזם הראשון $G/K \cong H$. לכן $|H| = \frac{|G|}{|K|}$.

(ג) לא. התנאי $(xy)^n = x^n y^n$ מתקיים לכל G חילופית. תהי G מעגלית מסדר n^2 ויהי x יוצר שלה. אז $1 \neq x^n \in K \cap H$. ∎

תרגיל 20.13: *תהי G חבורה מסדר 2002.*

(א) *הוכח כי G מכילה תת חבורה נורמלית לא טריוויאלית K.*

(ב) *הוכח כי –עבור K מתאימה מסעיף (א)– G/K מכילה תת חבורה נורמלית לא טריוויאלית.*

פתרון: (א) מתקיים $2002 = 2 \cdot 7 \cdot 11 \cdot 13$. יהי n_p מספר חבורות סילוב־p של G. אז $n_{11} | \frac{|G|}{11} = 2 \cdot 7 \cdot 13$ ו־$n_{11} \equiv 1 \pmod{11}$, לכן

$$n_{11} \in \{1, 2, 7, 13, 2 \cdot 7, 2 \cdot 13, 7 \cdot 13, 2 \cdot 7 \cdot 13\} \qquad n_{11} \equiv 1 \pmod{11}$$

ומכאן $n_{11} = 1$. לכן חבורת סילוב־11 של G נורמלית ב־G.

(ב) תהי K כמו ב־(א). אז G/K מסדר $13 \cdot 7 \cdot 2$. בדיקה כמו בסעיף (א) מראה כי $n_{13} = 1$ או $n_{13} = 2 \cdot 7$, ו־$n_7 = 1$ או $n_7 = 2 \cdot 13$, אם $n_{13} = 2 \cdot 7$ וגם $n_7 = 2 \cdot 13$, אז יש ב־G/K $2 \cdot 7 \cdot 12$ איברים מסדר 13, $6 \cdot 13 \cdot 2$ איברים מסדר 7, בסה"כ יותר איברים מהסדר של G/K, סתירה. לכן חבורת סילוב־13 או חבורת סילוב־7 של G/K נורמלית. ∎

תרגיל 20.14: *תת חבורה K של G נקראת* **אופיינית** *($K \operatorname{char} G$) אם $\alpha(K) = K$ לכל $\alpha \in \operatorname{Aut}(G)$. הוכח:*

(א) $G' := [G, G] \operatorname{char} G$.

(ב) $Z(G) \operatorname{char} G$.

(ג) *אם $K \operatorname{char} N \lhd G$ אז $K \lhd G$.*

(ד) *אם $N \lhd G$ אז $N' \lhd G$.*

(ה) *אם $H \leq Z(G)$ אז $H \lhd G$.*

פתרון: (א) $\alpha([x_1, x_2]) = [\alpha(x_1), \alpha(x_2)]$.

תרגיל 20.15: *תהי G חבורה. נגדיר סדרה*

$$\cdots \lhd G_{(2)} \lhd G_{(1)} \lhd G_{(0)} = G \tag{1}$$

על ידי $G_{(i)} = (G_{(i-1)})'$. הוכח: חבורה סופית G הינה פתירה אם ורק אם יש m כך ש־$G_{(m)} = 1$.

פתרון: נניח כי G פתירה. אז יש סדרה נורמלית

$$\{1\} = G_m \lhd \cdots \lhd G_1 \lhd G_0 = G \tag{2}$$

כך ש־G_{i-1}/G_i חילופית לכל i. כדי להוכיח שסדרה (1) מסתיימת ב־1, די להוכיח כי $G_{(i)} \leq G_i$ לכל i. נניח באידוקציה כי $G_{(i-1)} \leq G_{i-1}$ לכל i. אז G_{i-1}/G_i חילופית, לכן $(G_{i-1})' \leq G_i \leq G_{i-1}$. אבל $G_{(i)} = (G_{(i-1)})' \leq (G_{i-1})'$, ומכאן המסקנה.

להיפך, נניח כי בסדרה (1) מתקיים $G_{(m)} = 1$. נמצא לה עידון שהוא סדרת הרכב. אז מנות ההרכב הן מנות של תת חבורות של $G_{(i-1)}/G_{(i)}$, שהינן אבלית, לכן כל גורמי ההרכב הן חבורות אבליות. לכן G פתירה. ∎

תרגיל 20.16: *תהי $G = N \rtimes A$ מכפלה חצי ישרה של חבורות. נניח $ana^{-1} \neq n$ לכל $1 \neq a \in A,\ 1 \neq n \in N$.*

הוכח:

(א) $A \cap A^g = \{1\}$ *לכל* $g \in G \smallsetminus A$.

(ב) *אם G סופית אז* $G = N \cup \bigcup_{g \in G} A^g$.

פתרון: (א) מתקיים $G = AN = NA$. לכן יש $a \in A, 1 \neq n \in N$ כך ש־$g = an$. כיוון ש־$A^g = A^{an} = A^n$, אפשר להחליף את g ב־n.

כעת, $A = \{(1,a)|\ a \in A\}$ ואת n מזהים עם $(n,1) \in G$. לכן

$$\begin{aligned} A^n &= \{(n,1)(1,a)(n,1)^{-1}|\ a \in A\} \\ &= \{(n,a)(n^{-1},1)|\ a \in A\} \\ &= \{(n(an^{-1}a^{-1}),a)|\ a \in A\} \end{aligned}$$

לכן $a \in A \cap A^n$ אם ורק אם $n(an^{-1}a^{-1}) = 1$, כלומר, $na = an$. לפי ההנחה, כיוון ש־$n \neq 1$ זה קורה רק אם $a = 1$.

(ב) די להוכיח כי $G = N \cup \bigcup_{n \in N} A^n$. (כמו בסעיף הקודם, זה אפילו שקול למה שצריך להוכיח.) לכל $n \in N$ מתקיים $A^n \cap N = A^n \cap N^n = (A \cap N)^n = \{1\}$. לפי סעיף (א), לכל שתיים מבין $1 + |N|$ הקבוצות

$$N, A^n, \quad (n \in N)$$

יש רק איבר משותף, הוא 1. לכן באיחוד שלהם יש

$$|N \cup \bigcup_{n \in N} A^n| = |N| + |N| \cdot |A| - |N| = |A| \cdot |N| = |G|$$

איברים. לכן אלה **כל** איברי G. ∎

תרגיל 20.17: *הראה כי* $S_n \cong A_n \rtimes \mathbb{Z}/2\mathbb{Z}$.

פתרון: תהי $A = \langle (12) \rangle$. אז A מסדר 2, לכן $A \cong \mathbb{Z}/2\mathbb{Z}$, $A_n \lhd S_n$, $A \cap A_n = \{1\}$, $AA_n = S_n$. ∎

תרגיל 20.18: *יה* V *מרחב וקטורי ממימד סופי מעל שדה* $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ *ויהי* G *אוסף (חלקי) של העתקות לינאריות מ־* V *לעצמו. נניח כי* G *חבורה (ביחס להרכבה) ושזו חבורת־*p*. הוכח שיש* $0 \neq v \in V$ *כך ש־* $T(v) = v$ *לכל* $v \in V$.

פתרון: G פועלת על V, לכן V הוא איחוד זר של מסלולי־G. מספר האיברים ב־V הוא חזקה של p, אורך של כל מסלול הוא גם חזקה של p, והמסלול של 0 הוא מאורך 1. לכן יש $0 \neq v \in V$ כך שמסלולו הוא $\{v\}$. ∎

תרגיל 20.19: *הוכח: אם* G *חבורה לא חילופית מסדר* p^3 *(באשר* p *ראשוני) אז* $Z(G) = G'$.

תרגיל 20.20: *תהי* G *חבורה מסדר* n *אי זוגי ויהיו* $g_1, \ldots, g_n$ *כל איבריה השונים. הוכח:* $g_1 \cdots g_n \in G'$.

TEL AVIV UNIVERSITY אוניברסיטת תל-אביב
RAYMOND AND BEVERLY SACKLER FACULTY OF EXACT SCIENCES הפקולטה למדעים מדויקים ע"ש ריימונד ובברלי סאקלר
SCHOOL OF MATHEMATICAL SCIENCES בית הספר למדעי המתמטיקה

מבחן באלגברה ב' 1

0366.2132.01

לתלמידי דן הרן

י"ב בשבט, תשס"א
5 בפברואר 2001

משך המבחן: 3 שעות.
אין להשתמש בחומר עזר כלשהו.
ענה על ארבע (בלבד) מתוך שש השאלות הבאות.

שאלה 1: הוכח את משפט שראייר: *לכל שתי סדרות נורמליות של חבורה סופית G יש עידונים שקולים זה לזה.*

שאלה 2: תהי G חבורה סופית, תהי $K \triangleleft G$, ותהי P חבורת סילוב־p של K. הוכח שלכל $g \in G$ יש $k \in K$ כך ש־$P^g = P^k$. הסק ש־$G = K\ N_G(P)$.

שאלה 3: תהי G חבורה מסדר 40.

א. הראה שחבורת סילוב־5 של G הנה נורמלית ב־G.

ב. הראה שיש תת חבורות $H_1 < H_2 < H_3$ ב־G מסדרים $5, 10, 20$, בהתאמה.

שאלה 4: תהיינה A, B, C חבורות חילופיות נוצרות סופית. נניח כי $A \oplus B \cong A \oplus C$. הוכח כי $B \cong C$.

שאלה 5: א. הוכח כי ל־A_5 אין תת חבורה מסדר 20.

ב. תהי $\sigma = (1\ 2\ 3 \cdots n) \in S_n$ תמורה. הראה שלמחלקת הצמידות של σ ב־S_n יש $(n-1)!$ אברים וש־$C_G(\sigma) = \langle\sigma\rangle$.

שאלה 6: תהי G חבורה ותהי H תת חבורה שלה מאינדקס 5. יהי $a \in Z(G)$ אבר מסדר 3 במֶרכָּז של G. הוכח: $a \in H$.

בהצלחה!

TEL AVIV UNIVERSITY אוניברסיטת תל-אביב
RAYMOND AND BEVERLY SACKLER FACULTY OF EXACT SCIENCES
SCHOOL OF MATHEMATICAL SCIENCES
הפקולטה למדעים מדויקים ע"ש ריימונד ובברלי סאקלר
בית הספר למדעי המתמטיקה

0366.2132.01

מבחן באלגברה ב' 1

לתלמידי דן הרן

כ"ד באדר ב', תשס"ח
31 במרץ 2008

משך המבחן: 3 שעות.
אין להשתמש בחומר עזר כלשהו.
ענה על ארבע (בלבד) מתוך שש השאלות הבאות.

שאלה 1: הגדר חבורת סילוב־p של חבורה סופית והוכח שלכל חבורה סופית יש חבורת סילוב־p.

פתרון: ראה בחוברת (ההגדרה בתחילת סעיף 13 והמשפט הוא משפט 13.2.).

שאלה 2: הגדר זוגיות $\mathrm{Sg}(\sigma)$ של תמורה σ והוכח שההעתקה $\mathrm{Sg}: S_n \to \{\pm 1\}$ היא הומומורפיזם.

פתרון: ראה בחוברת. (זוהי הערה 9.7 ומשפט 9.9).

שאלה 3: תהי G חבורת־p ותהי $\{1\} \neq N \triangleleft G$. הוכח שבפעולת ההצמדה של G על N יש לפחות p מסלולים בעלי אורך 1 והסק או הוכח אחרת כי $N \cap Z(G) \neq \{1\}$.

פתרון: לפי נוסחת המחלקות

$$|N| = \sum_{i \in I'} (G : G_{x_i}) + |M|. \qquad (1)$$

באשר $\{x_i\}_{i \in I'}$ היא מערכת מיצגים של מסלולי־G בעלי אורך > 1. ו־

$$M = \{x \in N |\ g \in G \text{ לכל } g \quad gxg^{-1} = x\} = \{x \in N |\ x \in Z(G)\} = N \cap Z(G)$$

אורך של המסלול של x_i הוא $(G : G_{x_i})$, שהינו חזקה של p (כי הוא מחלק את $|G|$ שהינו חזקה של p), ואם הוא > 1, אז זו חזקה לא טריביאלית של p ובפרט מספר שמתחלק ב־p. לכן הסכום הראשון באגף ימין של (1) מתחלק ב־p. גם אגף שמאל מתחלק ב־p כי $|N|$ מחלק את $|G|$ ואינו 1. לכן $|M| = |N \cap Z(G)|$ מתחלק ב־p ובפרט יש בו לפחות שני איברים. אחד מהם הוא 1, לכן $N \cap Z(G) \neq \{1\}$.

שאלה 4: תהי G חבורה מסדר p^2q, באשר p,q ראשוניים שונים. הוכח שאחת מחבורות סילוב של G הינה נורמלית ב־G. (שים לב שאם $2 \neq p < q$ אז q אינו מחלק את $(p-1)(p+1)$.)

פתרון: תהי P חבורת סילוב־p ו־Q חבורת סילוב־q של G. נסמן ב־n_p את מספר חבורות סילוב־p וב־n_q את מספר חבורות סילוב־q של G. די להוכיח כי $n_p = 1$ או $n_q = 1$, כי אם חבורת סילוב מסוימת הינה יחידה, אז היא נורמלית.

מתקיים $n_p | (G:P) = p^2q/p^2 = q$, לכן $n_p = 1$ או $n_p = q$. אך לפי המשפט השלישי של סילוב, $n_p \equiv 1 \pmod{p}$. לכן אם $q < p$, אז לא יתכן $n_p = q$, כי $1 < q < p$. לכן תחת ההנחה $q < p$ מתקיים $n_p = 1$, כמבוקש.

נניח, איפוא, $p < q$. מתקיים $n_q | (G:Q) = p^2q/q = p^2$, לכן $n_q = 1$ או $n_p = q$ או $n_q = p^2$. אך לפי המשפט השלישי של סילוב, $n_q \equiv 1 \pmod{q}$. לכן לא יתכן $n_q = p$, כי $1 < p < q$. אם $n_q = 1$, סיימנו. נניח אם כן כי $n_q = p^2$. אז $p^2 \equiv 1 \pmod{q}$ פירושו $q | p^2 - 1 = (p-1)(p+1)$, וכיון ש־q ראשוני, זה אומר $q | p-1$ או $q | p+1$. בפרט $q \leq p-1$ או $q \leq p+1$, כלומר, $q \leq p+1$. כיון ש־$p < q$ זה אומר $q = p+1$. כיון ש־p, q ראשוניים, זה אומר $p = 2, q = 3$.

במקרה זה G מסדר 12, יש לה $n_q = p^2 = 4$ חבורות סילוב־3. בכ"א מהן יש 2 איברים מסדר 3, וחיתוך כל שתי חבורות סילוב־3 הוא $\{1\}$, לכן יש בחבורות סילוב־3 בדיוק $4 \times 2 = 8$ איברים מסדר 3. מלבד האיברים האלה יש עוד קבוצה A בת 4 איברים ב־G. איברים בחבורות סילוב־2 אינם מסדר 3, לכן הם בתוך A. היות ובכל חבורות סילוב־2 יש ארבעה איברים, היא שווה ל־A. לכן יש חבורת סילוב־2 יחידה ב־G.

שאלה 5: כתוב הגדרה של חבורה פשוטה. הוכח שאם G_1, G_2 חבורות סופיות פשוטות אז כל תת חבורה נורמלית של $G = G_1 \times G_2$ השונה מ־G ומ־$\{1\}$ הינה איזומורפית ל־G_1 או ל־G_2.

פתרון: חבורה G הינה פשוטה אם אין לה תת חבורות נורמליות, מלבד $\{1\}$ ו־G.

נניח כי $G = G_1 \times G_2$, באשר G_1, G_2 סופיות פשוטות. אז $\{1\} \triangleleft G_1 \triangleleft G$ סדרת הרכב של G, כי $G_1/\{1\} \cong G_1, G/G_1 \cong G_2$ פשוטות. תהי $N \triangleleft G$ שונה מ־G ומ־$\{1\}$. אז $\{1\} \triangleleft N \triangleleft G$ סדרה נורמלית ללא חזרות מאורך 2. אפשר לעדן אותה לסדרת הרכב. לפי משפט Jordan-Hölder כל שתי סדרות הרכב שקולות, ובפרט יש להן אותו מספר של איברים. במקרה שלנו סדרת ההרכב הראשונה מאורך 2, לכן $\{1\} \triangleleft N \triangleleft G$ כבר סדרת הרכב וגורמיה הם כמו בסדרת הרכב הראשונה, עד כדי הסדר. לכן

(א) $N \cong G_1$, $G/N \cong G_2$; או

(ב) $N \cong G_2$, $G/N \cong G_1$.

בכל מקרה, $N \cong G_1$ או $N \cong G_2$.

שאלה 6: תהי A חבורה חילופית סופית. יהי m המספר הטבעי הקטן ביותר כך ש־$ma = 0$ לכל $a \in A$. הוכח שקיים $a \in A$ בעל סדר m.

פתרון: לפי המשפט היסודי של חבורות חילופיות נוצרות סופית אפשר להניח כי

$$A = \mathbb{Z}/\epsilon_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/\epsilon_k\mathbb{Z} \oplus \overbrace{\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}}^{r}$$

באשר $\epsilon_1 | \cdots | \epsilon_k$ מספרים טבעיים ו־$k, r \geq 0$. בגלל ש־A סופית, $r = 0$. לכן $A = \mathbb{Z}/\epsilon_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/\epsilon_k\mathbb{Z}$. יהי $1 \leq i \leq k$. כל $a_i \in \mathbb{Z}/\epsilon_i\mathbb{Z}$ הוא מסדר שמחלק את ϵ_i ו־$\epsilon_i | \epsilon_k$, לכן $\epsilon_k a_i = 0$. מכאן לכל $a = a_1 + \cdots + a_k \in \mathbb{Z}/\epsilon_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/\epsilon_k\mathbb{Z} = A$ מתקיים $\epsilon_k a = \epsilon_k a_1 + \cdots + \epsilon_k a_k = 0$. מצד שני, יש $b_k \in \mathbb{Z}/\epsilon_k\mathbb{Z} \leq A$ מסדר ϵ_k. מכאן ש־$m = \epsilon_k$. כאמור, b_k מסדר m.

משחק המחשבת – פתרון

(א) מתקים $abc = 1$ ומכאן קל לראות שמכפלתם ב־K של כל החורים התפוסים בתחילת המשחק היא 1.

(ב) בכל מהלך בוחרים שלישיה של חורים סמוכים $x \quad y \quad z$ (בשורה או בעמודה) בהם x, y תפוסים ו־z פנוי, ומרוקנים את x, y וממלאים את z. לכן המכפלה אחרי המהלך מתקבלת מהמכפלה לפני המהלך על ידי ההכפלה ב־$zx^{-1}y^{-1}$. אבל x, y, z הם בהכרח a, b, c עד כדי הסדר, לכן $xy = z$. לכן המכפלה אינה משתנה!

(ג) לפי (א) ו־(ב), המכפלה ב־K של כל החורים התפוסים בסוף המשחק נשארת 1.

(ד) אם נשאר על הלוח רק כלי אחד, מכפלת החורים התפוסים היא ערך החור בו נמצא הכלי. בכל אופן, ערך זה אינו 1, בסתירה לסעיף הקודם.

(ה) נסמן את החורים במשחק המקורי על ידי אברי K כדלקמן (התעלם מהאינדקסים):

$$
\begin{array}{ccccccc}
 & & b & c_1 & a & & \\
 & & c & a_1 & b & & \\
b & c_0 & a & b_1 & c & a & b \\
c_2 & a & b & c & a & b & c_3 \\
a & b_0 & c & a & b & c & a \\
 & & a & b & c & & \\
 & & b & c_4 & a & &
\end{array}
$$

במקרה זה, מכפלת הערכים של החורים התפוסים בתחילת המשחק היא c. היא אינה משתנה במהלך המשחק. לכן אם ישאר בסוף המשחק כלי אחד, הוא יהיה בחור מסומן ב־c. יש 11 חורים כאלה.

הלוח הינו סימטרי ביחס לציר האופקי דרך המרכז. אילו ניתן היה לסיים את המשחק עם כלי בחור c_0, על ידי משחק סימטרי ניתן היה לסיימו בחור הסימטרי b_0. זאת סתירה לאמור לעיל. לכן אם ניתן לסיים עם כלי אחד בלבד, הוא יהיה בחור המרכזי או באחד החורים c_1, c_2, c_4, c_4.

אך אם המשחק הסתיים עם כלי אחד בחור c_1, למשל, לפני המהלך האחרון היו 2 כלים בחורים a_1, b_1 ויתר החורים היו פנויים. במצב כזה, במקום להעביר כלי מ־b_1 ל־c_1 ולסלק a_1 אפשר גם להעביר כלי מ־a_1 לחור המרכזי ולסלק b_1 ובכך להגיע לדרגת "גאון". דרוש "כשרון" מיוחד כדי לא לראות אפשרות זו. (באופן דומה לגבי c_2, c_3, c_4.)