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

תשס"ז

נערך על ידי

דן הרן

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 אלגברים 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 בינריות (אחת או שתים לכל היותר):

הגדרה 1.3: **פעולה בינרית** על קבוצה S היא העתקה $\pi\colon S \times S \to S$. למשל פעולת החיבור על $\mathbb{R}$ היא ההעתקה $\mathbb{R} \times \mathbb{R} \to \mathbb{R}$ המוגדרת על ידי $(a,b) \mapsto a+b$. **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 בינרית (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 בינרית $\circ$ 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:

$$((f \circ g) \circ h)(x) = (f \circ g)(h(x)) = f(g(h(x)));$$
$$(f \circ (g \circ h))(x) = f((g \circ h)(x)) = f(g(h(x)))$$

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 $1 \le k < n$ 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 $1 \le k, l < n$

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

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: **אבר יחידה**) ביחס לפעולה על S אם $ea = ae = a$ לכל $a \in S$. אם הוא קיים, הוא יחיד: 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־$\{f\colon X \to X\}$.

הגדרה 1.8: תהי S קבוצה עם פעולה בינרית אסוציאטיבית ועם אבר ניטרלי $e \in S$. אבר $a \in S$ נקרא **הפיך** אם קיים $b \in S$ כך ש־$ab = ba = e$. אבר 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 אבר שונה מ־0 ב־$\mathbb{R}$ הפיך ביחס לכפל ב־$\mathbb{R}$. כל אבר ב־$\mathbb{R}$ הפיך ביחס לחיבור ב־$\mathbb{R}$ וההופכי של a הוא $-a$. פונקציה f ב־$\{f\colon X \to X\}$ הפיכה אמ"ם היא חח"ע ועל.

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

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

כלומר, **חבורה** היא קבוצה לא ריקה עם פעולה בינרית אסוציאטיבית, בה יש אבר ניטרלי וכל אבר הוא הפיך.

חבורה נקראת **חילופית** (גם: **אַבֶּלית**) אם הפעולה חילופית.

דוגמאות של חבורות 1.11:

(א) $\{\pm 1\}$, $\{1\}$ עם פעולת הכפל.

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

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

(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 $\{f\colon X\to X \mid f$ חח"ע ועל$\}$ $S(X)=$ עם פעולת ההרכבה, כלומר: $(\alpha\circ\beta)(x)=\alpha(\beta(x))$.

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

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

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

הגדרה של **חישוק** $(a_1a_2\dots a_r)$.

(ח) אם G,H שתי חבורות, אז $G\times H$ עם הפעולה לפי הקואורדינטות $(g_1,h_1)(g_2,h_2)=(g_1g_2,h_1h_2)$ 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 $\varphi\colon G\to H$ נקראת **הומומורפיזם** אם היא שומרת את הפעולות המתאימות, כלומר

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

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

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

דוגמה 1.13: $\psi\colon S_2\to\{\pm1\}$ הנתונה על ידי $1\mapsto +1$, $(12)\mapsto -1$ היא איזומורפיזם חבורות.
$\psi\colon S_3\to\{\pm1\}$ הנתונה על ידי $(123),(132),1\mapsto +1$, 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 השויון הנתון ב- a^{-1} משמאל (מימין).

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

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

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

הוכחה:

(א) $\varphi(e_G)\varphi(e_G)=\varphi(e_Ge_G)=\varphi(e_G)=e_H\varphi(e_G)$, 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* $\varphi\colon G\to H$ *איזומורפיזם של מבנים אלגבריים. אזי ההעתקה ההפוכה* $\varphi^{-1}\colon H\to G$ *אף היא איזומורפיזם.*

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

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

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

2. משחק המחשבת (שעשעון עם חבורת קליין)

משחק המחשבת (solitaire, solitary) 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).

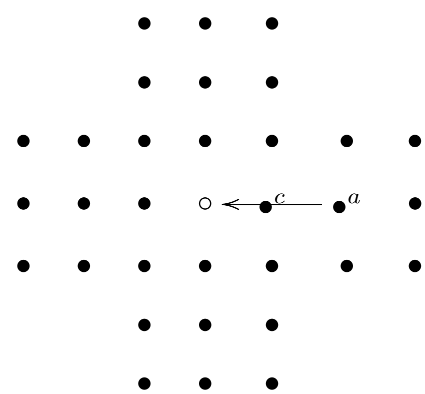
מהלך המשחק: בכל מצב במשחק יכול השחקן להעביר כלי אחד שני חורים ימינה, שמאלה, קדימה או אחורה, בתנאי שהחור החדש פנוי והחור מעליו הכלי עבר — תפוס. מיד לאחר מכן חייב השחקן לסלק מהלוח את הכלי שמעליו הוא עבר. (כך למשל, בהתחלה יכול השחקן להעביר את הכלי המסומן a לחור באמצע ולסלק את הכלי c מהלוח.) בכך קטן מספר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

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

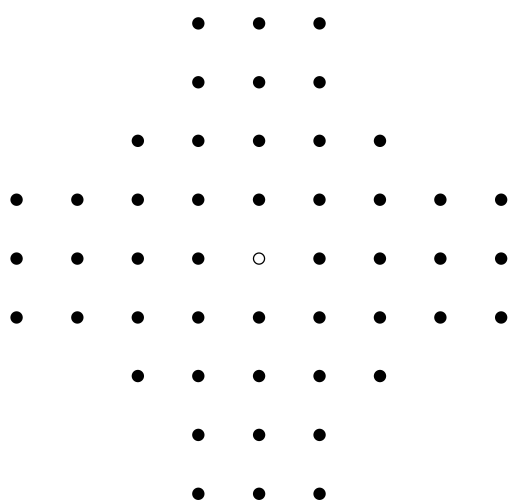
גאון — אם נשאר כלי אחד על גבי הלוח והוא בחור המרכזי,

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(?) 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 לא ניתן 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 באברי K כדלקמן:

			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			

(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 לא ניתן 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.)

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 בינריות אסוציאטיביות: חיבור $(+)$ וכפל (בלי סימן), כך ש-R הוא חבורה חלופית ביחס לחיבור ומתקיימים חוקי הפילוג:

$a(b+c)=ab+ac$ לכל $a,b\in R$

$(b+c)a=ba+ca$ לכל $a,b\in R$.

חוג נקרא **חילופי** אם הכפל חילופי.

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

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

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

הערה 3.2: בכל חוג R מתקיים: $a0=0=0a$ 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:

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

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

המעלה של $f(X)\neq 0$ היא $\max\{n|\ a_n\neq 0\}$. 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 אבר $\sum_{n=0}^{\infty} a_n X^n$ 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 $1 = 1+0X+0X^2+\dots$ היא היחידה של $R[X]$.

ניח כי R תחום שלמות: אם $f(X), g(X) \neq 0$ אז $\deg(f+g) = \deg(f) + \deg(g)$, בפרט $f + g \neq 0$. 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 $a \sim b \Leftrightarrow n\big|(r_a - r_b) \Leftrightarrow r_a = r_b$. נסמן מחלקת השקילות של a ב־$[a]$, ואת קבוצת המנה ב־$\mathbb{Z}/n\mathbb{Z}$. ב־$\mathbb{Z}/n\mathbb{Z}$ יש n אברים: $[0], [1], \dots, [n-1]$.

היחס $\sim$ שומר על הפעולות על $\mathbb{Z}$: אם $a \sim a', b \sim b'$ אז $a + b \sim a' + b', ab \sim a'b'$. 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 חבור וכפל על $\mathbb{Z}/n\mathbb{Z}$ על ידי

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

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־k, n 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:

$$[k] \text{ הפיך } \Leftrightarrow k \text{ זר ל־} n \Rightarrow n \not| k \Leftrightarrow [k] \neq [0].$$

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 $R^\times = \{r \in R | \ \text{הפיך}\ r\}$ 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) $(\mathbb{Z}/n\mathbb{Z})^\times = \{[k] | \ n\text{־זר ל}\ k\}$.

(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 אברי 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 (אבר $g \in G$, קבוצה $A \subseteq G$) יהיה גם נכון עבור $\varphi(G) = H$ (אבר $\varphi(g) \in H$, 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 המרבי המשותף** 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 המזערית** 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 $d = \gcd(a_1, a_2, \ldots, a_k)$ ו־$q \in \mathbb{Z}$ אז $d = \gcd(a_1 - q a_2, a_2, \ldots, a_k)$. כי לכל $d' \in \mathbb{Z}$:

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

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

הלמה ודאי נכונה אם

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

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

המשך ההוכחה באינדוקציה על $\sum_i a_i$. המקרה $\sum_i a_i = 0$ בסדר (לא יתכן). נניח $\sum_i a_i > 0$. בה"כ $a_1, a_2 \neq 0$, אחרת (*). יש $q, r \in \mathbb{Z}$ כך ש־$a_1 = q a_2 + r$ ו־$0 \leq r < a_2$. כיון 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

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

∎

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־$p \nmid b$. כיון 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 א.י., 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 $u \in \{\pm 1\}$ 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 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 $a=u=v$. אם $r \geq 1$ אז $p_r\big|a$ ולכן יש i כך ש־$p_r\big|p'_i$. כיון ש־p'_i אי פריק, נובע ש־$p_r=p'_i$, ולכן (צמצום!) $p_1p_2\cdots p_{r-1}=p'_1p'_{i-1}\cdots p'_{i+1}p'_s$. 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* $a, b \in \mathbb{Z}$,

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

באשר u, v *הפיכים, אז*

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

$\Leftrightarrow$ קיימים w הפיך 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 הפיך ו־$k_p \geq 0$ (כמעט כולם 0) כך ש־$v = uw, n_p = m_p + k_p$. ∎

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

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 $\pi\colon G\times G\to G$ פעולה בינרית על קבוצה G ו־$H\subseteq G$, נאמר שהצמצום של π ל־H היא פעולה בינרית 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 בינריות 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*:* $a,b\in H \Leftarrow ab\in H$

(ג) $a\in H \Leftarrow a^{-1}\in H$.

הוכחה: הכרחיות: (א), (ב) ־ ברור. (א'): מתקיים $1_H1_H=1_H=1_G1_H$, 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 בינרית 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 אבר 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 מתקיים: $\{1_G\}\leq G$.

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

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

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) $|Ag|=|A|=|gA|$.

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

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

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

למה 5.8: *תהי $G\le H$ 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: (1) (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־$g_1h_1=g_2h_2$. יהי $h\in H$. אז $g_1h=g_1h_1h_1^{-1}h=g_2h_2h_1^{-1}h\in g_2H$. ∎

הערה 5.9: על G יש יחס שקילות: $g_1\sim g_2$ אמ"ם 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 $H\le G$. 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 אבר אחד מכל מחלקה שמאלית של G ב־H (R נקראת מערכת מיצגים של G מודולו H).*

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

(א) **הסדר של** G הוא העוצמה $|G|$,

(ב) **האינדקס** $(G:H)$ של H ב־G הוא העוצמה $|G/H|$. ברור ש־$|R| = (G:H)$, 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 $\varphi\colon R \times H \to G$ על ידי $\varphi(r,h) = rh$. אזי φ 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 $h_1 = h_2$; φ על, כי $G = \bigcup_{g \in R} gH$. לכן $|G| = |R \times H| = |R| \times |H|$. ∎

מסקנה 5.12: *אם G חבורה סופית, $H \leq G$, אז $|H|, (G:H)$ מחלקים את $|G|$.*

הגדרה 5.13: תהי G חבורה ותהי $M \subseteq G$. נסמן ב־$\langle M \rangle$ את חתוך כל החבורות החלקיות של G שמכילות את M.

למה 5.12:

(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) *$\langle M \rangle = \{x_1x_2\cdots x_n |\ x_1, x_2, \ldots, x_n \in M \cup M^{-1}, n \geq 0\}$. (המכפלה הריקה היא אבר היחידה.)*

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

סימון 5.13: $\langle M, N \rangle = \langle M \cup N \rangle$, $\langle a, b, .. \rangle = \langle \{a, b, \ldots\} \rangle$;

דוגמה 5.14: $\mathbb{Z} = \langle 1 \rangle$.

6. סדר של אבר בחבורה. חבורות מעגליות.

חזקות.

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

$a^0 = e$ [בכתיב חבורי: $0a = 0$];

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

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

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 $i < 0, j > 0$.

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

אם G חבורה ו־$g \in G$ אז $\langle g \rangle = \{g^i | \; i \in \mathbb{Z}\}$ (=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: $\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}$ - ביחס לחבור - 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 $\mathrm{ord} g$. אם $g^n \neq e$ לכל n טבעי, נסמן $\mathrm{ord} g = \infty$. (**נשים לב:** $\mathrm{ord} g = 1 \Leftrightarrow g = e$.)

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

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

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

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

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

(ד1) $k \big| n \Leftrightarrow \mathrm{ord} g^k = n/k$;

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

הוכחה: יהי m שלם. נכתוב

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

אז

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

ולכן:

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

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

(ג) יהיו $0 \le m_1 \le m_2 < n$. אזי

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

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) $(g^k)^m = e \Leftrightarrow n\big|km \Leftrightarrow (n/d)\big|(k/d)m \Leftrightarrow (n/d)\big|m$ (כי $(n/d), (k/d)$ זרים ־ ראה תרגיל 4.9). אבל לפי (א) גם $(g^k)^m = e \Leftrightarrow \mathrm{ord} g^k\big|m$. מכאן $\mathrm{ord} g^k = n/d$. (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) $\mathrm{ord} g^d = n_1$ ולפי (ד2) $\mathrm{ord}(g^d)^{k_1} = n_1$). ∎

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* $\mathrm{ord} g^k = \infty$.

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

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

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

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

הוכחה:

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

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

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

הוכחה: תהי G מסדר ראשוני. יהי $e \neq g \in G$. אז $1 < \mathrm{ord} g \big| |G|$, לכן $\mathrm{ord} g = |G|$, 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 קימת 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 $\frac{n}{n/d} = d$. 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 שויון 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 $\mathrm{ord} h \big| |H|$, 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 $h = g^m \in \{(g^{\frac{n}{d}})^k |\ k \in \mathbb{Z}\} = \langle g^{\frac{n}{d}} \rangle$. מכאן $H \subseteq \langle g^{\frac{n}{d}} \rangle$. ∎

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־$\mathrm{ord} g = n$.) 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 $\langle g \rangle = \{g^0, g, g^2, \dots, g^{n-1}\}$. היא הומומורפיזם:

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

∎

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 $\mathbb{Z}\to\langle g\rangle$: 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 $d\in\mathbb{N}$ קימת 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־$\{0,1,\dots,d-1\}$ היא מערכת מיצגים של $\mathbb{Z}$ מודולו $d\mathbb{Z}$. צ"ל: לכל $k\in\mathbb{Z}$ יש $0\le r<d$ 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 $\{0\}\neq H\le\mathbb{Z}$. 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, $d\mathbb{Z}=\langle d\rangle\le H$. להיפך, אם $k\in H$, יהיו q,r כך ש־$k=dq+r$, $0\le r<d$. 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), $\mathrm{ord}(d)=\infty$, 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 $\theta\colon G \to H$ נקרא

(א) **איזומורפיזם** אם הוא חח"ע ועל;

(ב) **אפימורפיזם** אם הוא על;

(ג) **מונומורפיזם** אם הוא חח"ע;

(ד) **אנדומורפיזם** 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 $M^a = \{g^a \mid g \in M\} = a^{-1}Ma$.

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 $H \le G$ אז $H^a \le G$ לכל $a \in G$.

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

(א) $gN = Ng$ *לכל* $g \in G$.

(ב) $N^g = N$ *לכל* $g \in G$.

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

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

הוכחה:

(א) $\Leftrightarrow$ (ב) ע"י הכפלה מימין.

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

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

(ד) $\Rightarrow$ (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: $N \lhd G$.

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

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

למה 7.9: *תהיינה $N \lhd G$, $A \leq G$. 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 $N \lhd G$. אזי $G/N = \{gN \mid g \in G\}$ היא חבורה ביחס לכפל של קבוצות חלקיות של G. מתקיים $(g_1N)(g_2N) = g_1g_2N$, אבר היחידה של G/N הוא $1N = N$, וההפכי של gN הוא $(gN)^{-1} = g^{-1}N$.*

[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: $n\mathbb{Z} = \{nz \mid z \in \mathbb{Z}\} \lhd \mathbb{Z}$ 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 $\theta\colon G \to H$ הומומורפיזם חבורות. אזי*

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

משפט 7.16 (משפט האיזומורפיזם השלישי):

(א) *תהי* $N\triangleleft G$ *ונסמן* $\bar G=G/N$. *אם* $N\le A\le G$ *אז* $N\triangleleft A$. *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:* $\bar A_1\le\bar A_2\Leftrightarrow A_1\le A_2$

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

(3) *נורמליות:* $\bar A_1\triangleleft\bar A_2\Leftrightarrow A_1\triangleleft A_2$

(4) *מנות: אם* $A_1\triangleleft A_2$ *אז* $\bar A_2/\bar A_1\cong A_2/A_1$

הוכחה:

(א) ברור ש-$N\triangleleft A$. יהי $\pi\colon G\to\bar G$ 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 $B=\pi(A)$, אז $N\le A\le G$. 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-$\pi(g)=\pi(a)$. 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)

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

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

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

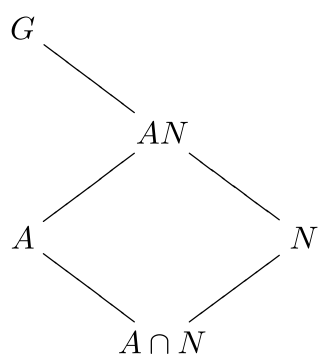
$$\Leftrightarrow A_1 \triangleleft A_2$$

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

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

דוגמה 7.17: $kn\mathbb{Z} \triangleleft n\mathbb{Z} \triangleleft \mathbb{Z}$; לפי (ג)3, $n\mathbb{Z}/kn\mathbb{Z} \triangleleft \mathbb{Z}/kn\mathbb{Z}$; 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 $N \triangleleft G$ ותהי $A \le G$. אזי $A \cap N \triangleleft A$ ו־$A/A \cap N \cong AN/N$ על ידי $a(A \cap N) \mapsto aN$.*



הוכחה: יהי $\pi\colon G \to G/N$ האפימורפיזם הטבעי. גרעינו N. צמצומו $\theta\colon A \to G/N$ ל־A הוא הומומורפיזם. תמונתו [שאמורה לפי משפט האיזומורפיזם השלישי להיות מהצורה H/N באשר $N \le H \le A$] 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 $\theta_{A\cap N}\colon A/A \cap N \to AN/N$ הנתון על ידי $(a(A \cap N)) \mapsto \theta(a) = aN$. $\blacksquare$

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

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

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

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

(ב) $A_1(A \cap B_1) \triangleleft A_1(A \cap B)$ *ובאפן סימטרי* $B_1(A_1 \cap B) \triangleleft B_1(A \cap B)$

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

הוכחה:

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

$$\begin{tikzcd}
 & A \arrow[d, dash] & & & & B \arrow[d, dash] & \\
 & A_1(A\cap B) \arrow[d, dash, "\triangledown"] \arrow[drr, dash] & & & & B_1(A\cap B) \arrow[d, dash, "\triangledown"] \arrow[dll, dash] & \\
 & A_1(A\cap B_1) \arrow[dl, dash] \arrow[drr, dash] & & A\cap B \arrow[d, dash, "\triangledown"] & & B_1(A_1\cap B) \arrow[dll, dash] \arrow[dr, dash] & \\
A_1 \arrow[dr, dash] & & & (A\cap B_1)(A_1\cap B) \arrow[dll, dash] \arrow[drr, dash] & & & B_1 \arrow[dl, dash] \\
 & A_1\cap B & & & & A\cap B_1 &
\end{tikzcd}$$

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

(ג) קל לראות ש־$[B_1(A_1 \cap B)](A \cap B) = B_1(A \cap B)$, כי $A_1 \cap B \subseteq A \cap B$, ו־$[B_1(A_1 \cap B)] \cap (A \cap B) = (A_1 \cap B)(A \cap B_1)$: אכן, אם $b_1 \in B_1, c \in A_1 \cap B$ כך ש־$b_1c \in A \cap B$ אז $b_1c, c \in A$ ולכן גם $b_1 \in A$. מכאן $b_1 \in A \cap B_1$.
לפי משפט האיזומורפיזם השני $B_1(A \cap B)/B_1(A_1 \cap B) \cong (A \cap B)/(A_1 \cap B)(A \cap B_1)$ 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, $G = \dot\bigcup_{g\in R} gH = \dot\bigcup_{g\in R} Hg$.*

8. אוטומורפיזמים. פעולה של חבורה על קבוצה.

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

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

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 האוטומורפיזמים הפנימיים של G.*

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

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

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** $g_1, g_2 \in G$, $x \in X$,

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

דוגמה 8.5:

(1) חבורת המטריצות ההפיכות $Gl_n(\mathbb{C})$ 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 $\{H|\ H \le G\}$ 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 קונפיגורציות של מרכיבי הקוביה.

(7) הפעולה הטריביאלית 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: $X = \dot\bigcup_{i\in I}\{{}^g x_i |\ g \in G\}$, באשר $\{x_i\}_{i\in I}$ היא מערכת מיצגים של מסלולי־G (כלומר מכילה בדיוק אבר 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 המְשַמֵר** *של x.*

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

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

תרגיל 8.8: *חבורה מעגלית $G = \langle\sigma\rangle$ מסדר n פועלת על קבוצה X. יהי $x \in X$ ונניח כי $|G_x| = m$. יהי X' המסלול של x. מה ארכו? מהם אבריו?*

פתרון: ארכו $(G : G_x) = n/m$, לפי הלמה. נסמן $d = n/m$. אז $G_x \le G = \langle\sigma\rangle$ מסדר m, לכן $G_x = \langle\sigma^d\rangle$. כמו כן $X' = \{x = {}^{\sigma^0}x, {}^{\sigma^1}x, {}^{\sigma^2}x, \ldots, {}^{\sigma^{n-1}}x\}$, אך

$$d \big| j - i \Leftrightarrow \sigma^{j-i} = (\sigma^i)^{-1}\sigma^j \in \langle\sigma^d\rangle \Leftrightarrow \sigma^i\langle\sigma^d\rangle = \sigma^j\langle\sigma^d\rangle \Leftrightarrow {}^{\sigma^i}x = {}^{\sigma^j}x$$

לכן $X' = \{x, {}^\sigma x, \ldots, {}^{\sigma^{d-1}}x\}$ ו־${}^{\sigma^d}x = x$. ∎

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

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

הגדרות 8.10: אם $a \in G$ אז $\{g \in G|\ {}^g a = a\}$ הוא **המְרַכֵּז** $C_G(a)$ של a. בפרט $C_G(a) \le G$.
אם $H \le G$ אז $\{g \in G|\ {}^g H = H\}$ הוא **המְשַמֵר (נורמליזטור)** $N_G(H)$ של H. בפרט $N_G(H) \le G$.

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 מאבר אחד אז*

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

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

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

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

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

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

כלומר

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

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 $\varphi\colon G\to S(X)$ 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.) ∎

9. חבורות תמורות.

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

$$ {}^{\pi}a_1 = a_2,\ {}^{\pi}a_2 = {}^{\pi}a_3,\dots,{}^{\pi}a_k = a_1, \qquad {}^{\pi}a = a \text{ לכל } X \ni a \neq a_1,a_2,\dots,a_k. $$

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

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

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

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

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

$$
\begin{aligned}
{}^{\sigma}a_{i1} &= {}^{\rho_i}a_{i1} = a_{i_2},\\
{}^{\sigma^2}a_{i1} &= {}^{\sigma}a_{i2} = {}^{\rho_i}a_{i2} = a_{i3},\\
&\dots\\
{}^{\sigma^{k_i-1}}a_{i1} &= a_{ik_i},\\
{}^{\sigma^{k_i}}a_{i1} &= a_{i1}
\end{aligned}
$$

לכן $\{{}^{\sigma^j}a_{i1} \mid j \geq 0\} = \{a_{i1},a_{i2},\dots,a_{ik_i}\} = X_i'$ הוא מסלול של $\langle\sigma\rangle = \{1,\sigma,\sigma^2,\dots\}$ מאורך k_i. המסלולים $X_1',\dots,X_m'$ זרים (כי $\rho_1,\dots\rho_m$ זרים), והם כל מסלולי־$\langle\sigma\rangle$ מאורך> 1: אם $x \in X \setminus \bigcup_{i=1}^m X_i'$ 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. כעת $x_i = a_{ij_i}$ עבור איזה j_i, ובה"כ $x_i = a_{i1}$ (לפי ההערה לפני הלמה). לכן

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

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

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

הוכחה: בה"כ σ היא חישוק. אך $(a_1a_2\dots a_k) = (a_1a_2)(a_1a_3)\cdots(a_1a_k)$ ∎

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

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

הוכחה: 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 אבר 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 אמ"ם 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 ${}^{(12)}i > {}^{(12)}j$ 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* $\mathrm{Sg}\colon S_n \to \{\pm 1\}$ *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 מארך k אז $\operatorname{Sg}(\pi) = (-1)^{k-1}$. בפרט,*

(ב) *כל חישוקון הוא אי זוגי.*

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

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

(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 מארך 3 ב־S_n.*

הוכחה: מצד אחד כל חישוק מארך 3 הינו זוגי ולכן נמצא ב־A_n. מצד שני כל אבר 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 נקראת **פשוטה** אם אין $N \lhd G$, $\{1\} \neq N \neq G$.

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

משפט 9.17: *A_n פשוטה לכל $n \geq 5$.*

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

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

ניח $(abc) \in N$. לפי הלמה הקודמת די להראות ש־N מכילה כל חישוק $(a'b'c')$ מאורך 3. נבחר $\sigma \in S_n$ כך ש־$c^\sigma = c'$, $a^\sigma = a'$, $b^\sigma = b'$., אזי $(abc)^\sigma = (a'b'c')$, 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 $\sigma' := (df)\sigma \in A_n$ ו־$(abc)^{\sigma'} = (a'b'c')$. לכן שוב $(a'b'c') \in N$.

טענה ב: *אם $N \neq 1$, יש חישוק מארך 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 $1, 2, \dots, n$.

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

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

נשים לב שאם σ שומרת כל אות שמופיעה ב־π_i אז לפי תרגיל 9.6, ${}^{\sigma}\pi_i = \pi_i$ ולכן $\pi_i^{-1}\ {}^{\sigma}\pi_i = 1$.

נבדיל בין כמה מקרים:

(1) אם $k_1 \geq 4$, נקח $\sigma = (a_2a_3a_4)$. אם $k_1 \geq 5$ אז

$$\pi^{-1}\ {}^{\sigma}\pi = \pi_1^{-1}\ {}^{\sigma}\pi_1 = (\ldots a_5a_4a_3a_2a_1)(a_1a_3a_4a_2a_5\ldots) = (a_1a_2a_4)$$

ואם $k_1 = 4$ אז

$$\pi^{-1}\ {}^{\sigma}\pi = \pi_1^{-1}\ {}^{\sigma}\pi_1 = (a_4a_3a_2a_1)(a_1a_3a_4a_2) = (a_1a_2a_4)$$

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

$$.N \ni \pi^2 = \pi_1^2 = (a_1a_2a_3)^2 = (a_1a_3a_2)$$

(3) אם $k_1 = k_2 = 3$, נקח $\sigma = (a_1a_2a_4)$. אז

$$\pi^{-1}\ {}^{\sigma}\pi = \pi_2^{-1}\pi_1^{-1}\ {}^{\sigma}\pi_1{}^{\sigma}\pi_2 = (a_6a_5a_4)(a_3a_2a_1)(a_2a_4a_3)(a_1a_5a_6) = (a_1a_4a_2a_6a_3)$$

זהו חישוק מאורך 5, ולכן לפי מקרה (2) יש חישוק מאורך 3 ב־A_n.

(4) אם $k_1 = k_2 \cdots = k_r = 2$, נקח $\sigma = (a_3a_4a_5)$. אז

4.1 אם $r = 2$,

$$\pi^{-1}\ {}^{\sigma}\pi = (a_4a_3)(a_2a_1)(a_1a_2)(a_4a_5) = (a_4a_3)(a_4a_5) = (a_3a_4a_5)$$

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

$$\pi^{-1}\ {}^{\sigma}\pi = (a_6a_5)(a_4a_3)(a_2a_1)(a_1a_2)(a_4a_5)(a_3a_6) = (a_3a_5)(a_4a_6)$$

ולכן לפי מקרה (4.1) יש חישוק מאורך 3 ב־A_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).

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

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 $f\mapsto g^{-1}fg$. אז ψ מוגדרת היטב (כלומר, $g^{-1}fg\colon Y\to Y$ אכן חח"ע ועל) ושומרת הרכבה. ההעתקה ההפוכה נתונה על ידי $h\mapsto ghg^{-1}$. ∎