סיכום מבנים אלגבריים - תשפ"ו 2026

9 במאי 2026

גיא יער־און

הסיכום נכתב במהלך סמסטר ב' תשפ"ו (2026), ומבוסס על הרצאותיו של ד"ר ארז שיינר, לכן יתכן שנפלו טעויות בסיכום, כך שהשימוש בו על אחריותכם בלבד.

תוכן עניינים

1 הקדמה . . . 1
1.1 חבורה $(Group)$ . . . 2
1.2 חוג $(Ring)$ . . . 2
1.3 שדה $(Field)$ . . . 2
2 חבורות . . . 2
2.1 דוגמאות מרכזיות לחבורות . . . 3
2.2 תת חבורה . . . 4
2.3 סדרים . . . 5
2.4 מכפלה ישרה של חבורות . . . 7
2.5 תמורות . . . 7
2.6 הומומורפיזם ואיזומורפיזם . . . 11
2.7 משפט קיילי . . . 13
2.8 משפט לגראנז' . . . 14

1 הקדמה

מהם מבנים אלגבריים? למעשה, כבר למדנו מבנה אלגברי מסויים בקורס אלגברה לינארית: **שדה**. למשל, $\mathbb{Z}_7$ הוא מופע של שדה. בקורס, נעסוק בעיקר במבנה אלגברי שנקרא **חבורה**, ומעט במבנה אלגברי שנקרא **חוג**. כמו כן, נרחיב על מושג השדה.

אנחנו סטודנטים למדעי המחשב, למה שנלמד קורס מתקדם על מבנים אלגבריים? נלמד בקורס זה על שני שימושים חשובים של מבנים אלגבריים אלו שקשורים לעולם מדעי המחשב:

- הצפנה
- קידוד

מה זה **הצפנה**? אפשר לחשוב על כך **כהסתרה** של מידע, זו המטרה העיקרית של הצפנה. נרצה לדאוג גם ל**אמינות** ו**שלמות** של המידע. למשל: כאשר מייקרוסופט מורידים עדכון גרסה, הוא לא צריך להיות מוסתר - אבל אנחנו צריכים להיות בטוחים שמייקרוסופט הם אלו שכתבו את העדכון, על מנת שלא נוריד בטעות וירוס - זה נקרא אמינות, ושלמות הכוונה היא שלא "יתנקשו" לי במידע ואקבל את כולו.

מה זה **קידוד**? מוסכמה לתבנית להעברת מידע. למשל: "יום ההולדת שלי הוא 2", הכוונה היא שכנראה אפשר להסתכל על כך כיום השני בשנה. שני הצדדים כמובן, צריכים להסכים על הקידוד: אחרת - יהיו לנו כמה וכמה פרשנויות שונות למידע. למשל, אפשר להתייחס למשפט אודות יום ההולדת כ"יום ההולדת שלי הוא בשני לחודש הבא" או "אני בן שנתיים" וכדומה. **פרוטוקול** (פרוטוקול תקשורת הוא סט של חוקים ומוסכמות המגדירים כיצד מכשירים דיגיטליים מעבירים נתונים ביניהם, כדי שיבינו את המידע הנשלח ויגיבו אליו בצורה תקינה.) למשל, הוא סוג של קידוד. בקורס נתמקד בעיקר בזיהוי ותיקון של שגיאות בקידוד ונלמד על RSA (אלגוריתם הצפנה).

האנלוגיה הכי קרובה למבנים אלגבריים מעולם מדעי המחשב, היא תכנות מונחה עצמים ובפרט ממשק (interface).
כפי שאמרנו, נתקלנו בעבר בשדות (מבנה אלגברי) ואף הוכחנו את הטענה הבאה:

משפט 1. יהי שדה $\mathbb{F}$, איבר האפס $0_{\mathbb{F}} \in \mathbb{F}$, ויהי $a \in \mathbb{F}$, אזי מתקיים: $a \cdot 0_{\mathbb{F}} = 0_{\mathbb{F}}$.

1.1 חבורה $(Group)$

הגדרה 2. **חבורה** היא קבוצה G יחד עם פעולה (בהיעדר מידע נוסף, נשתמש בסימון הכפל) שתסומן $(G,\cdot)$ כך שמתקיימות התכונות הבאות:

1. סגירות: $\forall a,b\in G: a\cdot b\in G$
2. אסוציאטיביות: $\forall a,b,c\in G: (ab)c=a(bc)$
3. ניטרלי (איבר יחידה): $\exists e_G\in G$ המקיים: $\forall a\in G: a\cdot e_G=e_G\cdot a=a$
4. קיום איבר הופכי: $\forall a\in G, \exists a^{-1}\in G: a\cdot a^{-1}=a^{-1}\cdot a=e_G$

הערה 3. מניטרליות, נקבל כי בהכרח חבורה G לא יכולה להיות ריקה: תמיד קיים איבר ניטרלי. את האיבר הניטרלי נסמן בe_G לרוב.

הערה 4. אנחנו לא דורשים קומוטטיביות (חילופיות) בחבורה.

הגדרה 5. תהי G חבורה עם פעולה $\cdot$. נאמר כי G היא חבורה אבלית / קומוטטיבית / חילופית אם הפעולה $\cdot$ מקיימת את חוק החילוף: כלומר $\forall a,b\in G: ab=ba$.

דוגמה 6. נתבונן ב$G=(\mathbb{N},+)$. האם מדובר בחבורה? אפילו אם $0\in G$, אין בחבורה איברים הופכיים. הרי 0 הוא איבר ניטרלי לחיבור, ולכן עבור $2\in\mathbb{N}$ למשל צריך להתקיים: $2+2^{-1}=0$, כלומר $2^{-1}=-2$, אך $-2\notin\mathbb{N}$ ולכן לא מדובר בחבורה.

דוגמה 7. לעומת זאת, $G=(\mathbb{Z},+)$ היא כן חבורה. האיברים ההופכיים הם הנגדיים. מיהו האיבר ההופכי של 0? נבחין כי 0 הוא האיבר ההופכי (ה"נגדי") של עצמו.

דוגמה 8. האם $(\mathbb{Q},\cdot)$ חבורה? לא! ל0 אין הופכי. אך, $(\mathbb{Q}\backslash\{0\},\cdot)$ וכן $(\mathbb{Q},+)$ הן חבורות.

1.2 חוג $(Ring)$

הגדרה 9. חוג הוא קבוצה R עם שתי פעולות (שנקרא להן חיבור וכפל, וכמובן רק נקרא להם כך), כך שמתקיימות התכונות הבאות:

1. $(R,+)$ הוא חבורה אבלית.
2. הכפל סגור, אסוציאטיבי ויש איבר יחידה.
3. פילוג: $\forall a,b,c\in G: (a+b)c=ac+bc=\wedge[a(b+c)=ab+ac]$

הערה 10. נבחין שוויתרנו על חילופיות (קומוטטיביות) ואיבר הופכי עבור הכפל. כיוון שאין חילוף, היינו חייבים לכתוב פעמיים את הפילוג.

דוגמה 11. ישנם שני מופעים מוכרים ביותר לחוג שאינם שדות:

1. $\mathbb{Z}_n$ - חוג השאריות עם פעולות מודלו n.
2. **המטריצות הריבועיות מסדר** n - החיבור טוב כחבורה, אך הכפל לא חילופי ולא כל המטריצות הפיכות! נראה כי חוג בדיוק מתאים עבור עולם המטריצות.

1.3 שדה $(Field)$

הגדרה 12. **שדה** הוא קבוצה $\mathbb{F}$ עם שתי פעולות (להן נקרא חיבור וכפל) כך שמתקיימות התכונות הבאות:

1. $(\mathbb{F},+)$ היא חבורה אבלית.
2. $(\mathbb{F}\backslash\{0\},\cdot)$ היא חבורה אבלית.
3. פילוג: $\forall a,b,c\in\mathbb{F}: a(b+c)=ab+ac$

הערה 13. נשים לב להבדל בין שדה לחבורה - בחבורה אנחנו דורשים שלכולם יש הופכי, בשדה לכולם פרט לאפס יש הופכי. לכן השדה ללא אפס הוא אכן חבורה.

הערה 14. האם צריך לומר במפורש כי $1\neq 0$? לא, שהרי $1\in\mathbb{F}\backslash\{0\}$ ולכן $1\neq 0$.

הערה 15. כל שדה הוא בפרט חוג (גם זה מזכיר OOP - הורשה).

2 חבורות

הערה 16. כאשר ייאמר לנו החבורה $\mathbb{R}$ או החבורה $\mathbb{Z}$ - אנחנו ישר נניח כי מדובר בחבורה ביחס לפעולת החיבור. מדוע? כי $(\mathbb{R},\cdot)$ איננו חבורה! שכן עם פעולת הכפל אין הפיכות וכו'.

הערה 17. החבורה הטריוואלית תסומן $(\{e\},^*\}$ כאשר $*$ היא פעולה. מדובר בחבורה אבלית!

משפט 18. (משפט חלוקה עם שארית) יהי $n\in\mathbb{N}_+$ ויהי $b\in\mathbb{Z}$. אזי קיימים $q,r\in\mathbb{Z}$ יחידים כך ש: $b=n\cdot q+r$ וכן $0\leq r\leq n-1$. q יקרא המנה של החלוקה של b בn וr היא השארית.

הוכחה: נחלק למקרים:

אם $b\geq 0$ (עבור $b<0$ הוכחה דומה). אזי $(b+1)n>b$ בהכרח שהרי $n\geq 1$. כמו כן, $-1\cdot n<b$. כלומר, קיים מס' שלם k כך ש$kn<b$ וקיים מס' שלם k כך ש$kn>b$. לכן נבחר את המס' השלם הגדול ביותר $q\in\mathbb{Z}$ כך ש$qn\leq b$. נסמן: $r=b-qn$ (השארית). נראה כי: $qn\leq b$ ולכן $r\geq 0$. כעת, נב"ש כי $r\geq n$ אזי $b-qn\geq n$ ולכן $b\geq(q+1)n$ בסתירה לכך שq הוא הגדול ביותר. ולכן סה"כ $0\leq r\leq n-1$. כעת, לאחר שהראינו קיום, נוכיח יחידות:

נניח כי ישנם שני פירוקים: $b = q_1 n + r_1 = q_2 n + r_2$. נעביר אגפים ונקבל: $(q_1 - q_2)n = r_2 - r_1$. נב"ש כי $q_1 \neq q_2$ ולכן $|q_1 - q_2| \geq 1$ ולכן $|(q_1 - q_2)n| \geq n$. עם זאת, $|r_2 - r_1| \leq n - 1$ (שהרי $r_1, r_2 \in [0, n-1]$ ובפרט המרחק שלהם לא יכול לעבור את הטווח). לכן קיבלנו סתירה - שהרי צד אחד של המשוואה מקיים שערכו גדול שווה מn, וצד אחד קטן מn. סתירה! לכן $q_1 = q_2$ ומכאן גם בהכרח לפי המשוואה $r_1 = r_2$, ולכן הפירוק הוא יחיד.

■

הגדרה 19. יהיו $a, b \in \mathbb{Z}$. נאמר כי a **מחלק את** b אם קיים $k \in \mathbb{Z}$ כך ש$b = ka$ ונסמן $a|b$.

הגדרה 20. יהיו $a, b \in \mathbb{Z}$ ויהי $n \in \mathbb{N}$. נאמר כי a, b שקולים מודלו n אם $n|(a-b)$. (כלומר, יש להם אותה חלוקה בשארית r).

משפט 21. שקילות מודלו n היא יחס שקילות.

הגדרה 22. יהי $n \in \mathbb{N}$. נגדיר את אוסף מחלקות השקילות מודלו n כך: $\mathbb{Z}_n = \{[a] | a \in \mathbb{Z}\}$. לרוב, נסמן $\mathbb{Z}_n = \{0, ..., n-1\}$ אם כי האיברים הם מחלקות שקילות וצריך לסמן פורמלית כך: $\mathbb{Z}_n = \{[0], ..., [n-1]\}$. נגדיר חיבור מודלו n לפי: $[a] + [b] = [a+b]$.

משפט 23. יהי $n \in \mathbb{N}$. אזי, $(\mathbb{Z}_n, +)$ היא חבורה אבלית.

2.1 דוגמאות מרכזיות לחבורות

משפט 24. נגדיר את S_A להיות אוסף הפונקציות ההפיכות $f : A \to A$ עם פעולת ההרכבה. אזי, $(S_A, \circ)$ היא חבורה ונקראת **חבורת התמורות.**

הוכחה: נוכיח שאכן מדובר בחבורה. לכן, נעבור תכונה תכונה:

1. **סגירות:** תהיינה $f, g \in S_A$ שתי פונקציות הפיכות. נרצה להראות כי $fg = f \circ g \in S_A$. לפי בדידה, הרכבת הפיכות היא פונקציה הפיכה כנדרש.
2. **אסוציאטיביות:** תהיינה $f, g, h \in S_A$. הרי, שוב לפי בדידה הרכבת פונקציות היא פעולה אסוציאטיביות ולכן $(fg)h = f(gh)$
3. **ניטרלי:** פונקציית הזהות $Id \in S_A$ כי הפיכה ומקיימת לכל $f \in S_A$ כי: $f \circ Id = Id \circ f = f$
4. **קיום איבר הופכי:** תהי $f \in S_A$, אזי קיימת לf פונקציה הופכית ונסמנה f^{-1} (והרי בבירור ההופכית היא הפיכה בעצמה) והרי בבירור לפי בדידה מתקיים $f \circ f^{-1} = f^{-1} \circ f = Id$.

■

משפט 25. נגדיר את הקבוצה הבאה:

$$GL_n(\mathbb{F}) = \{A \in \mathbb{F}^{n \times n} : |A| \neq 0\}$$

כלומר, קבוצת כל המטריצות ההפיכות. אזי, $(GL_n(\mathbb{F}), \cdot)$ היא חבורה.

הוכחה: נוכיח שאכן מדובר בחבורה. לכן, נעבור תכונה תכונה:

1. **סגירות:** תהיינה $A, B \in GL_n(\mathbb{F})$. אזי, כפל מטריצות הפיכות היא מטריצה הפיכה לפי לינארית 1 ולכן אכן $AB \in GL_n(\mathbb{F})$.
2. **אסוציאטיביות:** כפל מטריצות כמובן אסוציאטיבי.
3. **ניטרלי:** מטריצת הזהות I מקיימת לכל $A \in GL_n(\mathbb{F})$ כי: $AI = IA = A$.
4. **קיום איבר הופכי:** תהי $A \in GL_n(\mathbb{F})$. אזי, כיוון שA הפיכה קיימת לה הופכית A^{-1} שגם היא הפיכה. מכאן, מתקיים: $AA^{-1} = A^{-1}A = I$.

■

משפט 26. תהיינה חבורות $(G, \cdot_G)$ ו$(H, \cdot_H)$. נביט במכפלה הקרטזית: כלומר אוסף הזוגות

$$G \times H = \{(g, h) | g \in G, h \in H\}$$

ונגדיר את הפעולה: $(g_1, h_1) \cdot_{G \times H} (g_2, h_2) = (g_1 \cdot_G g_2, h_1 \cdot_H h_2)$. אזי מדובר בחבורה.

הערה 27. $(GL_n(\mathbb{F}), +)$ איננה חבורה! $I, -I$ הן הפיכות אך $I + (-I)$ אינה הפיכה. אין סגירות (וחסר עוד הרבה תכונות).

משפט 28. יהי $\mathbb{F}$ שדה. נסמן ב$M_n(\mathbb{F})$ את המטריצות מגודל $n \times n$ מעל $\mathbb{F}$. אזי, $(M_n(\mathbb{F}), \cdot)$ היא חבורה אבלית.

הגדרה 29. תהי G חבורה. המרכז של G הוא:

$$Z(G) = \{x \in G | \forall y \in G : xy = yx\}$$

כלומר, מרכז החבורה הוא קבוצת האיברים בחבורה שמתחלפים עם כולם.

משפט 30. G היא חבורה אבלית $\iff Z(G) = G$

הערה 31. תמיד מתקיים $e_G \in Z(G)$.

2.2 תת חבורה

הגדרה 32. תהי חבורה G ותהי $H \subseteq G$ תת קבוצה. נאמר כי H היא תת חבורה של G ונסמן $H \leq G$ אם H היא חבורה ביחס לפעולה של G.

משפט 33. תהי חבורה G ויהיו $a, b, c \in G$ כך ש$ab = ac$ אזי $b = c$.
הוכחה:

$$ab = ac \Longrightarrow (a^{-1})(ab) = (a^{-1})(ac) \Longrightarrow (a^{-1}a)b = (a^{-1}a)c \Longrightarrow e_G b = e_G h \Longrightarrow b = h$$

■

משפט 34. (קריטריון מקוצר לתת חבורה). תהי חבורה G ותהי $H \subseteq G$. אזי, $H \leq G$ אם ורק אם שני התנאים הבאים מתקיימים:
1. $e_G \in H$
2. לכל $a, b \in H$ מתקיים כי $a \cdot_G b^{-1} \in H$.

הוכחה:
$\Longleftarrow$ בכיוון ראשון, נניח כי $H \leq G$ ונראה כי מתקיימים התנאים $1 + 2$. נרצה להוכיח $e_G \in H$. כיוון שH תת חבורה, בH חייב להיות איבר יחידה כי זו חבורה ונסמנו e_H. אך $e_H \in G$. G חבורה ולכן יש לו איבר יחידה e_G. (כיוון שגוי להוכחה: לומר כי ישנו איבר יחידה יחיד, זה שגוי כי יתכן וe_H איבר יחידה רק בתת החבורה הנ"ל ולא עבור שאר האיברים).
נרצה להוכיח $e_G = e_H$. נכיט ב$e_G \cdot e_H$. מצד אחד, $e_H \in H \subseteq G$ ובפרט $e_H \in G$. כמו כן גם $e_G \in G$ ובגלל שG חבורה, יש סגירות לפעולה, וכן e_G ניטרלית לפעולה ולכן $e_H \cdot e_G = e_H$. כמו כן, $e_H \cdot e_H = e_H$ (כאן e_H כן ניטרלי). כעת מטרנזטיביות: $e_H \cdot e_H = e_H \cdot e_G$ ומתכונת הצמצום (משפט 29) הרי שקיבלנו $e_H = e_G$.
כעת נרצה להראות את התכונה השנייה. יהיו $a, b \in H$. נרצה להוכיח $ab^{-1} \in H$. אם כן, כיוון שH היא חבורה וכן $b \in H$ קיים לו הופכי, נסמנו c. אזי $bc = cb = e$. מצד שני, עבור b^{-1} (ההופכי של b בG) מתקיים: $bb^{-1} = b^{-1}b = e$. ושוב מטרנזטיביות קיבלנו $bc = bb^{-1}$ ומתכונת הצמצום $c = b^{-1}$. כלומר, הוכחנו כי $b^{-1} \in H$ (ההופכי הוא יחיד, ובפרט הוא קיים גם בתת חבורה). כעת, כיוון ש$a, b^{-1} \in H$ מסגירות של H נקבל $ab^{-1} \in H$.
$\Longrightarrow$ בכיוון השני, נניח כי התנאים מתקיימים ונוכיח כי H חבורה.
סגירות: יהיו $a, b \in H$. נרצה להוכיח $ab \in H$. אם כן, $b^{-1} \in H$ ממה שראינו כבר, וכן $a \in H$. לפי תנאי 2 אם נסמן $c = b^{-1}$ נקבל $ac^{-1} \in H$. אך:

$$ac^{-1} = a(b^{-1})^{-1} = ab \in H$$

אסוציאטיביות: כיוון שהפעולה אסוציאטיבית על כל איברי G, היא בפרט אסוציאטיבית על איברי H ולכן ישנה אסוציאטיביות גם כאן.
קיום איבר יחידה: ראשית, $e_G \in H$ ובבירור הוא ניטרלי בH, כי ניטרלי לכל איברי H.
הפיכות: יהי $b \in H$. נרצה להוכיח $b^{-1} \in H$ (יודעים כי הוא קיים, אך בG. אם נראה כי הוא בH אזי יש הופכי לb). אם כן, $e_G \in H$ וכן $b \in H$ ולפי תנאי 2 שמניחים שמתקיים $e_G b^{-1} \in H$, אך $e_G b^{-1} = b^{-1} \in H$ כנדרש.
ולכן סה"כ H היא תת חבורה.

■

דוגמה 35. נתבונן ב$SL_n(\mathbb{F}) = \{A \in \mathbb{F}^{n \times n} | det(A) = 1\} \subseteq GL_n(\mathbb{F})$. אזי, $SL_n(\mathbb{F}) \leq GL_n(\mathbb{F})$.
הוכחה: נוכיח לפי הקריטריון המקוצר.
אם כן, $det(I) = 1$ ולכן $I \in SL_n$ והרי $I = e_{GL_n}$.
שנית, יהיו $A, B \in SL_n$. אזי, נרצה להראות $AB^{-1} \in SL_n$. והרי ש:

$$det(AB^{-1}) = det(A) \cdot det(B)^{-1} = 1 \cdot 1^{-1} = 1$$

ולכן $AB^{-1} \in SL_n$, כנדרש.

■

הגדרה 36. תהי חבורה G ויהי $a \in G$. נגדיר את תת החבורה הציקלית הנוצרת מa להיות:

$$< a >= \{a^k | k \in \mathbb{Z}\}$$

באשר נגדיר את פעולת החזקה: עבור $n \in \mathbb{N}_+$ נגדיר $a^n = a \cdot a \cdot ..... \cdot a$ וכן $a^0 = e_G$ וכן $a^{-n} = (a^{-1})^n = (a^n)^{-1}$.

הערה 37. סימון החזקה עשוי להיות מבלבל מאוד כאשר הפעולה אינה כפל. למשל, $G = (\mathbb{Z}, +)$. אזי, $< 1 >= \mathbb{Z}$. מדוע? כי $1^4 = 1 + 1 + 1 + 1 = 4$, אז לשים לב. לכן לעיתים אם נדע מראש שהפעולה חיבורית, במקום a^n נכתוב na.

דוגמה 38. נביט בחבורה $(\mathbb{C}\backslash\{0\},\cdot)$ ונביט בתת החבורה הציקלית $<2>$. נראה כי:

$$<2>=\{2^k|k\in\mathbb{Z}\}=\{1,2,4,8,.....\frac{1}{2},\frac{1}{4},.....\}$$

בדומה,

$$<i>=\{i^k|k\in\mathbb{Z}\}=\{1,i,-1,\frac{1}{i}=-i\}$$

כיצד אכן אנחנו יודעים כי לא חסרים עוד איברים ב$<i>$? מדוע גודל תת החבורה הציקלית הוא 4? מיד נגלה. (רמז: $i^4=1=e_G$).

הגדרה 39. יהי $n>1$ כך ש$n\in\mathbb{N}$. נגדיר את חוג השאריות $\mathbb{Z}_n=\{0,...,n-1\}$ עם פעולות כפל וחיבור מודולו n כלומר: $a+_{\mathbb{Z}_n}b$ מוגדר להיות שארית החלוקה של $a+n$ בn.

משפט 40. $\mathbb{Z}_n$ הוא שדה $\iff$ n הוא מס' ראשוני.

הגדרה 41. חבורה G ששווה לתת חבורה ציקלית כלשהי $a\in G$ $<a>$, כלומר $G=<a>$ נקראת חבורה ציקלית. האיבר a שממנו נוצרה תת החבורה הציקלית נקרא **יוצר** של החבורה.

דוגמה 42. נתבונן ב$(\mathbb{Z}_5,+)$. ונתבונן ב$<2>$.
$2^0=0$. מדוע? שהרי החזקה מתייחסת לפעולה, והכוונה לחבר את 2 אפס פעמים - זה שווה אפס.
$2^1=2$ שהרי מחברים את 2 פעם אחת.
$2^2=2+2=4$ שמחברים את 2 שני פעמים.
$2^3=2+2+2=6\equiv 1$
$2^4=2+2+2+2=8\equiv 3$
וקיבלנו $<2>=\{0,1,2,3,4\}=\mathbb{Z}_5$ ולכן מדובר בחבורה ציקלית, עם יוצר 2. בדומה, $<4>=\mathbb{Z}_5$ ולכן גם 4 הוא יוצר.

משפט 43. תת החבורה הציקלית היא תת חבורה.

הוכחה: תהי חבורה G ויהי $a\in G$. נביט בתת החבורה הציקלית של a. כלומר, $<a>$. נוכיח שהיא תת חבורה של G באמצעות הקריטריון המקוצר:
א. נראה כי עבור $a^0=e_G$ (שהרי עבור $k=0$ נקבל $a^0=e_G$ שהרי מדובר בהפעלת הפעולה 0 פעמים על a, ולכן מקבלים את איבר היחידה).
ב. נרצה להראות כי לכל $a^k,a^m\in G$ מתקיים $a^k\cdot(a^m)^{-1}\in G$. והרי:

$$a^k\cdot(a^m)^{-1}=a^k\cdot a^{-m}=a^{k-m}\in G$$

שהרי $k-m$ הוא מס' שלם כחיסור של מס' שלמים.
לכן סה"כ $<a>$ היא תת חבורה של G לכל $a\in G$.

■

2.3 סדרים

הגדרה 44. תהי G חבורה. נגדיר את הסדר של G להיות עוצמתה כקבוצה. כלומר, כמה איברים יש בG. נסמן זאת ב$|G|$.

דוגמה 45. $|\mathbb{Z}_4|=4$ וכן $|\mathbb{Z}|=\aleph_0$.

הגדרה 46. תהי G חבורה ויהי $g\in G$. הסדר של האיבר g הוא המס' הטבעי n הקטן ביותר כך שמתקיים $g^n=e_G$. נסמן זאת ע"י $o(g)=n$.
אם אין מס' טבעי שכזה, נאמר כי הסדר של g הוא אנסוף. וכן מתקיים $o(a)=1\iff a=e_G$.

משפט 47. תהי G חבורה ויהי $a\in G$. אזי, $o(a)=o(a^{-1})$
הוכחה: כטענת עזר - נראה כי תמיד $aa^{-1}=a^{-1}a=e$ ובפרט $aa^{-1}=a^{-1}a$ כלומר כל איבר מתחלף עם עצמו.
נחלק למקרים:
1. הסדר של a הוא סופי כלומר $o(a)=n<\infty$. אזי, לפי הגדרה: $a^n=e$. וכן:

$$e=e^n=(a^{-1}a)^n=_*(a^{-1})^na^n=_{**}(a^{-1})^ne=(a^{-1})^n$$

שכן $*$ נכון בגלל שכל איבר a מתחלף עם עצמו (זה לא נכון תמיד בחבורה) ו$**$ נכון כי $a^n=e$. כלומר קיבלנו $e=(a^{-1})^n$. מכאן, $o(a^{-1})\leq n$.
אם נחזור בדומה על התהליך עם a^{-1}, נקבל כי $n=o(a)\leq o(a^{-1})$. לכן סה"כ $o(a)=o(a^{-1})$
2. הסדר של a אינו סופי. דהיינו $o(a)=\infty$. נניח כי $o(a^{-1})=n$ עבור n טבעי כלשהו בשלילה, כלומר שהסדר של ההופכי סופי. אזי, לפי הפסקה הקודם נקבל כי $o(a^{-1})=o(a)=n$ אך $o(a)=\infty$ בסתירה.

■

משפט 48. תהי חבורה G ויהי $a \in G$. אזי, $o(a) = |< a >|$. כלומר, הסדר של איבר הוא גודלה של תת החבורה הציקלית. כמו כן, אם $o(a) = n$ אזי $< a >= \{e, a, a^2, ..., a^{n-1}\}$ וכן הם שונים זה מזה.

הוכחה: תהי חבורה G ויהי $a \in G$. נחלק למקרים:

ראשית נניח כי הסדר סופי: כלומר $o(a) = n$. נרצה להוכיח כי $< a >= \{e, a, a^2, ..., a^{n-1}\}$. נבחין כי אם נוכיח זאת ושהם שונים אכן נקבל כי $|< a >| = n$ (שכן לא יתכנו עוד איברים שאלו כל החזקות כי זה שווה ל$o(a)$) ונסיים. נבצע הכלה דו כיוונית על מנת להוכיח שוויון זה.

$\supseteq$ לפי הגדרה, כל החזקות השלמות של a אכן נמצאות ב$< a >$ לפי הגדרת הסדר כלומר אכן $\{e, a, a^2, ..., a^{n-1}\} \subseteq < a >$.

$\subseteq$ יהי $a^k \in < a >$. נרצה להוכיח כי בהכרח $a^k \in \{e, ..., a^{n-1}\}$. נבצע חלוקה עם שארית של k בn: $k = qn + r$. מכאן:

$$a^k = a^{qn+r} = a^{qn} \cdot a^r = (a^n)^q \cdot a^r = (e)^q \cdot a^r = a^r$$

ולכן בהכרח $k = r \in [n-1]$ כפי שרצינו.

כעת נוכיח כי איברי הקבוצה שונים זה מזה. נג"ש כי קיימים $0 \leq n_1 < n_2 \leq n-1$ כך ש: $a^{n_1} = a^{n_2}$. נכפול את שני הצדדים בa^{-n_1} ונקבל:

$$e = a^{n_2-n_1}$$

כעת, אנחנו יודעים כי $n_2 - n_1 > 0$ וכיוון ש$n_2 \leq n-1$ נקבל $n_2 - n_1 \leq n-1$ ומצאנו ערך $(n_2 - n_1)$ קטן מn שעבורו מתקיים $a^{n_2-n_1} = e$, ולכן $o(a) = n_2 - n_1 < n$ בסתירה. לכן איברי החבורה שונים זה מזה.

מקרה שני: נניח כי $o(a) = \infty$ במקרה האינסופי. נג"ש כי $o(a)$ סופי. לכן, בהכרח ישנן לפחות 2 חזקות שנותנות את אותה התוצאה. כלומר, $a^{n_1} = a^{n_2}$ (כי אנחנו במקרה הסופי). שוב, נקבל כי $a^{n_2-n_1} = e$ ונקבל $o(a) = n_2 - n_1$ בסתירה לכך שהסדר אינסופי (שהרי לפי ההגדרה, אף חזקה חיובית לא מגיעה לe).

■

דוגמה 49. אם G סופית, אזי כל תת חבורה שלה מוכלת בה ולכן גם היא בהכרח סופית, לכן בפרט כל תתי החבורות הציקליות הן סופיות, ולכן לכל איבר בחבורה יש סדר סופי.

הערה 50. נבחין כי בחבורה ציקלית, הסדר של יוצר הוא הסדר של החבורה. מדוע? כי לפי הגדרה מתקיים $G =< a >$. וכן, $|< a >| = o(a)$ וכן $|G|$ זהו סדר החבורה ומטרנזטיביות השוויון נקבל: $|G| = o(a)$.

משפט 51. תהי G חבורה ציקלית, אזי G אבלית.

הוכחה: תהי G חבורה ציקלית, אזי קיים איבר $a \in G$ כך ש$G =< a >$. נרצה להוכיח כי לכל $g_1, g_2 \in G$ מתחלפים. אם כן, G ציקלית לכן קיימים $g_1 = a^i, g_2 = a^j$. מכאן:

$$g_1 g_2 = a^i a^j = a^{i+j} = a^{j+i} = a^j a^i = g_2 g_1$$

כנדרש.

■

משפט 52. אם G ציקלית, אזי כל תת חבורה של G ציקלית.

הוכחה: תהי $H \leq G$ תת חבורה של G וכן G ציקלית. נרצה להראות כי H ציקלית בהכרח. נסמן $G =< a >$. אם כן, כל האיברים בG מהצורה a^i. לכן, גם כל האיברים בH מצורה זו. נחלק למקרים:

אם $H = \{e\}$ אזי $H =< e >$ וסיימנו.

אחרת, לא טריוואלי. יהי $s \in \mathbb{Z} \backslash \{0\}$ המספר המינימלי בערך מוחלט כך ש$a^s \in H$. נניח כי $s \in \mathbb{N}$. נרצה להראות כי $H =< a^s >$. נראה זאת ע"י הכלה.

תחילה, בבירור $< a^s > \subseteq H$, שכן לפי הגדרה $< a^s >$ זו תת החבורה הקטנה ביותר שמכילה את a^s והרי $a^s \in H$ ולכן H מכילה את $< a^s >$.

בכיוון השני, יהי $h \in H$. אזי, קיים k עבורו $h = a^k$ כי $h \in G$. לפי משפט חלוקה עם שארית, קיימים q וr עבורם: $k = qs + r$ כך ש$0 \leq r < s$. מכאן:

$$a^k = a^{qs+r} = a^{qs} \cdot a^r = (a^s)^q \cdot a^r$$

ולכן, $a^r = a^k \cdot ((a^s)^q)^{-1}$. אז, $a^s, a^k \in H$ ומכאן גם $a^r \in H$ (מסגירות לכפל ולהופכי). אם $r \neq 0$, נבחין כי זו סתירה למינימליות של s כי $a^r \in H$ וגם $0 < r < s$ ומצאנו חזקה קטנה מs בסתירה. ולכן $r = 0$. כלומר, $k = qs$. ולכן, $s|k$. כלומר, $a^k \in < a^s >$.

■

משפט 53. תהי G חבורה ויהי $a \in G$. אזי, $a^n = e$ אמ"מ $o(a)|n$.
הוכחה: בכיוון ראשון, נניח $o(a)|n$. לכן קיים k עבורו $n = k \cdot o(a)$. מכאן,

$$a^n = a^{k \cdot o(a)} = (a^{o(a)})^k = (e)^k = e$$

בכיוון שני, נניח $a^n = e$. נרצה להראות כי $o(a)|n$. מכאן בהכרח נקבל $o(a) \leq |n|$. לפי משפט חלוקה עם שארית, קיימים q וr עבורם $n = q \cdot o(a) + r$ עם $0 \leq r < o(a)$. מכאן:

$$e = a^n = a^{q \cdot o(a) + r} = (a^{o(a)})^q \cdot a^r = (e)^q \cdot a^r = a^r$$

כלומר קיבלנו $a^r = e$, אך אנחנו יודעים כי $o(a)$ הוא המס' הטבעי הקטן ביותר כך ש$a^{o(a)} = e$. מכאן, $r = 0$ בהכרח שכן לא יתכן אצלנו כי $0 < r < o(a)$. לכן, $n = q \cdot o(a)$ ונקבל כי אכן $o(a)|n$.

■

2.4 מכפלה ישרה של חבורות

תהיינה $(G, *), (H, \bullet)$ חבורות. נתבונן במכפלה הקרטזית בניהן $G \times H$ עם פעולת רכיב רכיב שנסמנה $\odot$ כך:

$$(g_1, h_1) \odot (g_2, g_2) = (g_1 * g_2, h_1 \bullet h_2)$$

אזי מתקיים כי $G \times H$ ביחס ל$\odot$ היא חבורה. איבר היחידה בחבורה זו הינו (e_G, e_H).

משפט 54. $\mathbb{Z}^n \times \mathbb{Z}^n$ איננה ציקלית לכל $n \geq 2$.
הוכחה: כמובן, ביחס לחיבור. יהי איבר (a, b) בחבורה. נראה כי:

$$(a, b)^n = (a, b) \cdot (a, b) \cdot .... \cdot (a, b) = (a + ... + a, b + ...b) = (na, nb) = (0, 0)$$

מכאן, בהכרח $o(a, b) \leq n$. כלומר, לכל זוג איברים הסדר לכל היותר n. עם זאת, $|\mathbb{Z}_n \times \mathbb{Z}_n| = n^2$ וכן אם החבורה הייתה ציקלית, היה בה איבר מסדר n^2, כיוון ש$n^2 > n$ לכל $n \geq 2$ נקבל כי בהכרח החבורה לא ציקלית.

■

2.5 תמורות

דוגמה 55. נביט בלוח הכפל של $\mathbb{Z}_5 \backslash \{0\}$ עם פעולת הכפל:

$\cdot$	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

נבחין: כל שורה בטבלה מהווה תמורה של המספרים $\{1, 2, 3, 4\}$ (איברי החבורה). נבחין ־ לא כל תמורה (שהרי יש $n!$ ובטבלה n שורות) נכנסת לטבלה. אלא ־ נכנסות כמה תמורות נבחרות שמייצגות את החבורה.

תזכורת: לכל קבוצה A, קבוצת הפונקציות ההפיכות $A \to A$ עם פעולת ההרכבה מסומנת S_A, ונקראת חבורת התמורות.

הגדרה 56. נגדיר S_n להיות אוסף כל הפונקציות $f : \{1, ..., n\} \to \{1, ..., n\}$ ההפיכות. פורמלית,

$$S_n = \{f : \{1, ..n\} \to \{1, .., n\} | \text{f is onto and 1-1}\}$$

כיצד נסמן תמורות? באופן בזבזני, נוכל לכתוב בשורה ראשונה את המספרים $(1, 2, ..., n)$ ושורה מתחתיו לאן כל איבר נשלח, כלומר $f(i)$: $\forall i \in [n]$.

דוגמה 57. אם נקח את S_4, ונקח את Id_4: נקבל את התמורה (פונקציה) הבאה:

$$Id_4 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}$$

בדומה,

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{pmatrix} \in S_4 \mid f(1) = 2, f(2) = 1, f(3) = 3, f(4) = 4$$

$$g = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix} \in S_4 \mid f(1) = 3, f(2) = 1, f(3) = 2, f(4) = 4$$

נרצה לחשב את ההרכבה של התמורות.

$$f \circ g(1) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ f(g(1)) = 3 & f(g(2)) = 2 & f(g(3)) = 1 & f(g(4)) = 4 \end{pmatrix}$$

דוגמה 58. נרצה לחשב תת חבורה ציקלית של תמורה.

$$< \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} >= \{I, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}^2, ...\} = \{I, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}\}$$

ונראה כי כבר $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}^3 = I$ ולכן נקבל $o(\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}) = 3$.
בדומה,

$$< \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} >= \{I, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}\}$$

נבחין כי $o(\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}) = 2$.
נשים לב כי $|S_3| = 3! = 6$. האם זה מקרי שתתי החבורות הציקליות מגודל (סדר) שמחלק את גודל החבורה S_3? כמובן שלא - נלמד בהמשך (משפט לגראנז').

■

הגדרה 59. לכל תמורה סופית $f \in S_n$ נגדיר את הסימן של התמורה כך:

$$sign(f) = \prod_{1 \le j < i \le n} \frac{f(i) - f(j)}{i - j}$$

הגדרה 60. מחזור (או עגיל) בS_n הוא תמורה המציינת מעגל אחד של החלפות של מספרים שונים $a_1 \to a_2 \to .... \to a_k \to a_1$ ושאר המספרים נשלחים לעצמם. כותבים את התמורה הנ"ל בקיצור $(a_1, ..., a_k)$ ואורך המחזור הוא k.

לדוגמה:

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

התמורה הנ"ל היא המחזור $(1, 2, 3)$. מדוע? $1 \to \sigma(1) = 2 \to \sigma(2) = 3 \to \sigma(3) = 1$.

משפט 61. כל תמורה ניתנת לכתיבה כהרכבת מחזורים זרים, כאשר הכוונה ב"זרים" היא שאין להם מס' משותף שהם משנים את מיקומו.

דוגמה 62. נתבונן בתמורה הבאה:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 4 & 7 & 3 & 1 & 5 & 2 & 6 \end{pmatrix} \in S_7$$

נקח מספר ונתחיל לעבור על המחזור שמתחיל בו. למשל: $1 \to 4 \to 1$. כלומר $(1,4)$.
ושוב, $2 \to 7 \to 6 \to 2$ וקיבלנו $(2,7,6)$.
ושוב, $3 \to 3$ וקיבלנו (3).
ושוב, $5 \to 5$ וקיבלנו (5).
כיוון שהמספרים הולכים לעצמם הם מחזורים בודדים ולרוב לא נכתוב אותם. לכן נוכל לכתוב את התמורה כ:

$$\sigma = (1\ 4)(2\ 7\ 6)$$

נראה שימוש לדרך זו - ניתן לחשב את σ^2 בקלות. כיוון שמחזורים זרים מתחלפים זה עם זה, כלומר,

$$\sigma^2 = ((1\ 4)(2\ 7\ 6))^2 = (1\ 4)^2(2\ 7\ 6)^2$$

כעת, $(1,4)^2$ כאשר נפעיל פעולה פעמיים נחזור לאותה נקודה. לכן, $1 \to 4 \to 1$ וכן $4 \to 1 \to 4$ וקיבלנו $(1)(4)$ ולא נכתוב זאת בתמורה (נשלחים לעצמם).
בדומה, $6 \to 7 \to 2$ וכן $2 \to 6 \to 7$ וכן $7 \to 2 \to 6$. קיבלנו: $(2,6,7)$ כמחזור. לכן:

$$\sigma^2 = (2,6,7)$$

■

משפט 63. מתקיים $sign(f) = \prod_{1\le j<i\le n} \frac{f(i)-f(j)}{i-j} = \pm 1$.
הוכחה: בעקרון, אם נרצה להוכיח פחות פורמלית בשורה: כיוון שf היא פונקציה חח"ע ועל, אנחנו מקבלים זוגות במונה מהצורה $(f(i), f(j))$ ובמכנה (i,j). כיוון שf היא תמורה ובפרט חח"ע ועל כל הזוגות שיופיעו במונה ובמכנה יהיו זהים. לכן $|sign(f)| = 1$. מכאן, בהתאם לסימן נקבל ± 1. כעת, להוכחה פורמלית:
נסמן את קבוצת האיברים הלא סדורים של זוגות איברים שווים ב$\{1,..,n\}$ כ- $A = \{(i,j) | 1 \le i,j \le n \wedge i \ne j\}$. נגדיר פונקציה $\Phi : A \to A$ ע"י $\Phi(\{i,j\}) = \{f(i), f(j)\}$. קל לראות כי Φ היא פונקציה חח"ע ועל לפי החח"ע ועל של f. אם כן נקבל:

$$sign(f) = \prod_{1\le j<i\le n} \frac{f(i)-f(j)}{i-j} = \frac{\prod_{1\le j<i\le n} f(i)-f(j)}{\prod_{1\le j<i\le n} i-j}$$

כיוון שf היא תמורה,

$$\{|f(i)-f(j)| 1 \le j < i \le n\} = \{|i-j| 1 \le i < j \le n\}$$

ולכן המונה והמכנה שווים בערכם המוחלט לכן נקבל $|sign(f)| = 1$ כלומר $sign(f) = \pm 1$.
יתרה מכן, כל זוג (i,j) המקיים $i > j$ אך $f(i) < f(j)$ תורם -1 למכפלה. לכן, סימן התמורה הוא מס' החילופים N ומתקיים: $sign(f) = (-1)^N$.

■

משפט 64. יהיו שתי תמורות f, g. אזי: $sing(f \circ g) = sign(f) \cdot sign(g)$.
הוכחה:

$$sing(f \circ g) = \prod_{i>j} \frac{x_{f(g(i))} - x_{f(g(j))}}{x_i - x_j} = \prod_{i>j} \frac{x_{f(g(i))} - x_{f(g(j))}}{x_{g(i)} - x_{g(j)}} \cdot \frac{x_{g(i)} - x_{g(j)}}{x_i - x_j} =$$

$$\prod_{i>j} \frac{x_{f(g(i))} - x_{f(g(j))}}{x_{g(i)} - x_{g(j)}} \times \prod_{i>j} \frac{x_{g(i)} - x_{g(j)}}{x_i - x_j}$$

כיוון שf היא תמורה, אוסף הזוגות $i > j$ שווה לאוסף הזוגות $g(i), g(j)$ לכן: $\prod_{i>j} \frac{x_{f(g(i))} - x_{f(g(j))}}{x_{g(i)} - x_{g(j)}} = sing(f)$. סה"כ נקבל:

$$sing(f \circ g) = sing(f) \times sign(g)$$

■

הגדרה 65. יהיו $1 \leq p_1 \neq p_2 \leq n$ זוג איברים. נגדיר את תמורת החילוף $f = (p_1 p_2) \in S_n$ להיות:

$$f(x) = \left\{ \begin{array}{cc} p_2 & x = p_1 \\ p_1 & x = p_2 \\ x & o.w \end{array} \right\}$$

אזי, f היא תמורה.

משפט 66. תהי f תמורת חילוף. אזי, $sign(f) = -1$.

הוכחה: בה"כ שהאיברים שמבצעים את החילוף הם p_1, p_2 ויהיו $(p_3, ..., p_n)$ שאר האיברים. אם כן:

$$sign((p_1 p_2)) = \frac{p_1 - p_2}{p_2 - p_1} \times \frac{p_3 - p_2}{p_3 - p_1} \times ... \times \frac{p_n - p_2}{p_n - p_1} \times \frac{p_3 - p_1}{p_3 - p_2} \times ... \times \frac{p_n - p_1}{p_n - p_2} \times \frac{p_4 - p_3}{p_4 - p_3} ... \times \frac{p_n - p_{n-1}}{p_n - p_{n-1}} = -1 \cdot 1 \cdot ... \cdot 1 = -1$$

כנדרש.

■

הגדרה 67. יהיו $1 \leq p_1, ..., p_k \leq n$ שונים. נגדיר את המחזור:

$$(p_1 p_2 .... p_k) = (p_1 p_2)(p_2 p_3)(p_3 p_4) \cdot ... \cdot (p_{k-1} p_k)$$

כלומר, כהרכבה של חילופים. נבחין כי מכפליות הסימן ומכך שסימן חילוף הוא שלילי נקבל כי: $sing(p_1 .... p_k) = (-1)^{k-1}$.

דוגמה 68. נתבונן במחזור הבא: $(4, 2, 6, 3) \in S_6$. (וכן $1, 5$ נשלחים לעצמם). נראה כי לפי הגדרה:

$$(4, 2, 6, 3) = (4, 2)(2, 6)(6, 3) = \left(\begin{array}{cccccc} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 6 & 4 & 2 & 5 & 3 \end{array} \right)$$

כעת נרצה לחשב זאת.
נתחיל מ1. מהו החילוף ש3 עושה ל1? כלום. ומ$(6, 3)$ מקבלים 1. וכן הלאה - כיוון ש1 לא מופיע במחזורים: מקבלים 1.
נעבור ל2. הוא עובר במחזור ראשון $(6, 3)$ ולא קורה לו כלום. משם: מגיע ל$(2, 6)$ ומוחלף ל6. לא מושפע מ$(4, 2)$ וסה"כ מקבלים 6.
וכן הלאה.
נבחין, כי קיבלנו תמורה שפשוט שולחת את 4 ל2, את 2 ל6 וכן הלאה. נרצה להוכיח שזה מה שקורה באופן כללי:

משפט 69. יהי $f = (p_1 .... p_k)$ מחזור. אזי,

$$f(x) = \left\{ \begin{array}{cc} p_1 & x = p_k \\ p_i & x = p_{i-1} \forall i \geq 2 \\ x & o.w \end{array} \right\}$$

דוגמה 70. נתבונן בדוגמה הבאה:

$$f = \left(\begin{array}{ccccccc} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 7 & 4 & 1 & 6 & 2 & 5 \end{array} \right)$$

נרצה לחשב את $sing(f)$ בקלות. ראשית, נפרק את התמורה להרכבה של מחזורים זרים. נבחין כי:

$$f = (1, 3, 4)(2, 7, 5, 6)$$

מכאן, נבחין כי $sing(1, 3, 4) = sing((1, 3)(3, 4)) = (-1)^2 = 1$. וכן: $sing(2, 7, 5, 6) = sing((2, 7)(7, 5)(5, 6)) = (-1)^3 = -1$.
סה"כ מכפליות הסימן נקבל $sing(f) = 1 \cdot -1 = -1$.

2.6 הומומורפיזם ואיזומורפיזם

הגדרה 71. תהיינה שתי חבורות G, H ותהי פונקציה $f : G \to H$. נאמר כי f היא הומומרפיזם אם לכל $a, b \in G$ מתקיים:

$$f(a \cdot_G b) = f(a) \cdot_H f(b)$$

הגדרה 72. נאמר כי $f : G \to H$ פונקציה בין חבורות היא איזומורפיזם אם:
1. f היא הומומורפיזם.
2. f היא חח"ע ועל.

הערה 73. הומומורפיזם שומר במובן מסוים על מבנה החבורה ואיזומורפיזם מראה שהחבורות הן "אותה גברת בשינוי אדרת" - ועל כך נרחיב בהמשך במשפט קיילי.

משפט 74. אם $f : G \to H$ היא הומומורפיזם אזי $f(e_G) = e_H$
הוכחה: מתקיים $f(e_G) = f(e_G \cdot e_G) = f(e_G) \cdot_H f(e_G)$. כעת, קיבלנו בפרט $f(e_G) = f(e_G) \cdot_H f(e_G)$ ומתכונת הצמצום נקבל $e_H = f(e_G)$.

■

משפט 75. יהי $f : G \to H$ הומומורפיזם. אזי, מתקיים $o(f(g)) \leq o(g)$ ואם f איזומורפיזם אזי יש שוויון. כמו כן מתקיים $o(f(g))|o(g)$.
הוכחה: נחלק למקרים.
מקרה ראשון: $o(g) = n$ סופי. אזי, $g^n = e_G$. מכאן: $f(g^n) = f(g \cdot g \cdot ... \cdot g) = (f(g))^n$. אבל גם $f(g^n) = f(e_G) = e_H$ וקיבלנו $(f(g))^n = e_H$ ולכן $o(f(g)) \leq n = o(g)$.
מקרה שני: $o(g)$ לא סופי. אזי בהכרח מתקיים $o(f(g)) \leq \infty$ באופן טריוואלי.
כעת, נניח כי f איזומורפיזם. כעת נטען כי $o(g) \leq o(f(g))$.
אם כן, נניח כי $o(f(g))$ סופי אחרת הטענה נכונה באופן טריוואלי. נסמן $o(f(g)) = k$. אזי, $(f(g))^k = e_H$. אם כן,

$$f(g)^k = f(g) \cdot .... \cdot f(g) = f(g^k) = e_H$$

כיוון שf היא איזומורפיזם, ואנו יודעים כי $f(e_G) = e_H$ וגם $f(g^k) = e_H$ אזי נקבל $e_G = g^k$ כלומר $o(g) \leq k = o(f(g)$.
סה"כ אכן אם f איזומורפיזם נקבל $o(g) = o(f(g))$ לכל $g \in G$.

■

משפט 76. יהי f הומומורפיזם, ויהי $a \in G$. אזי $f(a^{-1}) = (f(a))^{-1}$
הוכחה: נראה כי $f(a) \cdot_H f(a^{-1}) = f(aa^{-1}) = f(e_G) = e_H$. ולכן, אם נכפיל ב$(f(a))^{-1}$ (שקיים, כי מדובר באיבר בחבורה שקיים לו הופכי) משמאל נקבל את הדרוש.

■

הערה 77. לא צריך במשפט הקודם לדרוש הפיכות (איזומורפיזם). בפרט, האיברים בתוך חבורה ולהם קיים הפיך. נבחין כי לא מתקיים $f^{-1}(a) = f(a^{-1})$ שכן $f(a^{-1}) \in H$ וכן $f^{-1} \in G$ וכלל זה לא מוגדר.

הגדרה 78. יהי $f : G \to H$ הומומורפיזם. נגדיר:
א. התמונה של f:

$$Im(f) = \{f(g)|g \in G\}$$

ב. הגרעין של f:

$$Ker(f) = \{g \in G|f(g) = e_H\}$$

הגדרה 79. יהי $f : G \to H$ הומומורפיזם. אזי f חח"ע אמ"מ $Ker(f) = \{e_G\}$.

משפט 80. יהי $f: G \to H$ הומומורפיזם. אזי, $Ker(f) \leq G$ ו $Im(f) \leq H$.
הוכחה:
יהי הי $f: G \to H$ הומומורפיזם.
ו. נוכיח כי $Ker(f) \leq G$:
ראשית, אכן לפי הגדרה מתקיימת ההכלה שהרי $Ker(f) = \{g \in G | f(g) = e_H\} \subseteq G$. כעת, נוכיח לפי הקריטריון המקוצר.
א. מתקיים $f(e_G) = e_H$ ולכן אכן $e_G \in Ker(f)$.
ב. יהיו $a, b \in Ker(f)$. נרצה להראות כי $ab^{-1} \in Ker(f)$. אם כן, מתקיים:

$$f(ab^{-1}) = f(a) \cdot_H f(b^{-1}) = f(a) \cdot_H (f(b))^{-1} =_{a \in Ker(f)} e_H \cdot_H (f(b)^{-1}$$

$$= (f(b))^{-1} =_{b \in Ker(f)} (e_H)^{-1} = e_H$$

לכן אכן $ab^{-1} \in Ker(f)$.
סה"כ לפי הקריטריון המקוצר $Ker(f)$ תת חבורה של G.
ז. נראה כי $Im(f) \leq H$.
ראשית, נבחין כי אכן ההכלה מתקיימת שהרי $Im(f) = \{f(g) \in H | g \in G\} \subseteq H$. כעת נוכיח לפי הקריטריון המקוצר.
א. מקיים $f(e_G) = e_H$ לכן $e_H \in Im(f)$.
ב. יהיו $a, b \in Im(f)$. $a \in Im(f)$ ולכן קיים $g_1 \in G$ כך ש$f(g_1) = a$. בדומה, קיים $g_2 \in G$ כך ש$f(g_2) = b$. מכאן: נרצה להראות כי $ab^{-1} \in Im(f)$. אנו יודעים כי מתקיים $f(x^{-1}) = (f(x))^{-1}$. בפרט עבור g_2 נקבל:

$$f(g_2^{-1}) = (f(g_2)^{-1} = (b)^{-1}$$

כלומר, המקור של b^{-1} תחת f הוא g_2^{-1} (שמוגדר כי G חבורה). מכאן, נראה כי:

$$f(g_1 g_2^{-1}) = f(g_1) f(g_2^{-1}) = ab^{-1}$$

מסגירות להופכי $g_2^{-1} \in G$ ומסגירות כחבורה מקבלים $g_1 g_2^{-1} \in G$. לכן נסמן $x = g_1 g_2^{-1}$ וקיבלנו כי x מקור של ab^{-1} כלומר אכן $ab^{-1} \in Im(f)$.
לכן סה"כ $Im(f)$ היא תת חבורה של H. כנדרש.

■

הערה 81. נסמן $A \cong B$ עבור איזומורפיזם בין קבוצות.

משפט 82. יהי $f: G \to H$ הומומורפיזם חח"ע. אזי $G \cong Im(f)$ (G איזומורפית לתמונה שהיא תת חבורה של H).
הוכחה: ההוכחה פשוטה, צריך לצמצם את H לתמונה שלה ונקבל פונקציה $f: G \to Im(f)$ שהיא גם חח"ע וגם על: ולכן איזומורפיזם.

הערה 83. תהי חבורה G ונביט בחבורת התמורות S_G. כלומר, כל הפונקציות ההפיכות מG לעצמה עם פעולת ההרכבה.

הגדרה 84. יהי $f: G \to H$ הומומורפיזם. אזי,
א. אם f חח"ע נאמר כי f מונומורמיזם או שיכון. במקרה זה נאמר כי G משוכנת בH אם קיים שיכון $f: G \to H$.
ב. אם f על נאמר כי f אפמיורפיזם. במקרה זה H היא תמונה אפימורפית של G.
ג. איזומורפיזם $f: G \to G$ נקרא גם אוטומורפיזם.

משפט 85. איזומורפיזם היא תכונה סימטרית, רפלקסיבית וטרנזיטיבית.

משפט 86. כל חבורה ציקלית $(G =< a >)$ איזומורפית או ל$\mathbb{Z}_n$ או ל$\mathbb{Z}$.

משפט 87. ההעתקה $i: G \to G$ המוגדרת לפי: $i(g) = g^{-1}$ היא אוטומורפיזם (איזומורפיזם) רק אם G אבלית.
פתרון: בבירור כי i היא פונקציה הפיכה. נותר לבדוק מתי $i(gh) = i(g)i(h)$. אם כן:

$$i(gh) = (gh)^{-1} = h^{-1}g^{-1} = i(h)i(g) = i(hg)$$

כיוון שi חח"ע זה יקרה אמ"מ $gh = hg$ לכל $g, h \in G$. כלומר: אמ"מ G אבלית.

■

הגדרה 88. חבורת החילופין A_n מוגדרת באופן הבא:

$$A_n = \{\sigma \in S_n | sign(\sigma) = 1\}$$

ומתקיים $A_n \leq S_n$.
הוכחה: בבירור שיש הכלה. מכאן לפי הקריטריון המקוצר בקלות:
1. Id, תמורת הזהות אכן מקיימת כי $sign(Id) = 1$ לכן $Id \in A_n$.
2. יהיו ϕ, τ זוג תמורות בA_n. מכאן לפי כפליות הסימן: $sign(\phi\tau^{-1}) = sign(\phi)sign(\tau)^{-1} = 1 \cdot 1^{-1} = 1$.

הערה 89. **מטרתנו להמשך הדרך:** תהי G חבורה ותהי S_G חבורת התמורות. נבנה פונקציה $\phi : G \to S_G$ ששולחת כל איבר מG לתמורה כלשהי. ההומומורפיזם חח"ע יקרא שיכון כי הוא משכן את G בתוך הטווח כך שכל איבר מקבל מיקום פרטי. משם - נסיק את משפט קיילי שאומר שכל חבורה איזומורפית לתת חבורה של חבורת התמורות. כלומר: $G \cong Im(\phi)$. כלומר - כל חבורה בעולם היא תת חבורה של חבורת התמורות (בשינוי אדרת) וכל פעולה בעצם לבסוף היא הרכבה.

2.7 משפט קיילי

נרצה לבנות פונקצייה ϕ מחבורה G לS_G (חבורת כל הפונקציות ההפיכות מG לעצמה - חבורת התמורות). נרצה כי בהינתן איבר מG הפונקציה תחזיר תמורה, ושהפונקציה תהיה:
1. מוגדרת היטב.
2. הומומורפיזם.
3. חח"ע

אם נבנה כזו - נקבל את משפט קיילי: $G \cong Im(\phi)$ (כל חבורה איזומורפית לתמונה של הפונקציה - חבורת התמורות).

משפט 90. משפט קיילי: כל חבורה איזומורפית לתת חבורה של חבורת התמורות.

כעת נרצה להוכיח את משפט קיילי:

לכן, לכל איבר $a \in G$ נגדיר פונקציה f_a שמוגדרת ע"י:

$$f_a(g) = ag$$

כיוון ש$a, g \in G$ גם $ag \in G$ ולכן $f_a : G \to G$. כלומר הפונקציה מקבלת איבר g ומפעילה עליו את הפעולה של G עם a.

הפונקציה f_a אכן מוגדרת היטב. אך עלינו להראות כי $f_a \in S_G$. כלומר - שמדובר בפונקציה חח" ועל.
חח"ע: נניח $f_a(x_1) = f_a(x_2)$ אזי $ax_1 = ax_2$. ל$a \in G$ קיים הופכי a^{-1}. נכפיל משמאל ונקבל $x_1 = x_2$, חח"ע.
על: יהי $y \in G$. נבחין כי:

$$y = (aa^{-1})y = a(a^{-1}y) = f_a(a^{-1}y)$$

לכן מקור של $y \in G$ תחת f_a הוא $a^{-1}y \in G$ וסה"כ לכל y קיים מקור.

נגדיר את **שיכון קיילי** ע"י:

$$\phi(a) = f_a$$

כלומר - שולחים כל איבר לפונקציה ש"כופלת" באותו איבר.
כיוון ש$f_a \in S_G$ (פונקציה הפיכה מ$G \to G$ מוגדרת היטב) נקבל כי $\phi : G \to S_G$.

כעת נרצה להראות כי שיכון קיילי הוא הומומורפיזם. לשם כך: יהיו $a_1, a_2 \in G$:

$$\phi(a_1 \cdot_G a_2) = \phi(a_1) \circ \phi(a_2)$$

נרצה למעשה להוכיח כי: $f_{a_1a_2} = f_{a_1} \circ f_{a_2}$. כלומר - שוויון בין פונקציות. ראשית, נראה כי התחום והטווח אכן שווים וכעת נרצה להראות כי לכל איבר x הוא נשלח לאותו מקום. אם כן:

$$f_{a_1a_2}(x) = (a_1a_2)x$$

$$f_{a_1} \circ f_{a_2}(x) = f_{a_1}(a_2x) = (a_1)(a_2x) =_* (a_1a_2)x$$

שכן * נכון שכן מדובר בחבורה ויש אסוציאטיביות.

כעת - נותר להראות כי ϕ היא פונקציה חח"ע.
יהיו $a_1, a_2 \in G$ כך ש$\phi(a_1) = \phi(a_2)$. אזי, $f_{a_1} = f_{a_2}$. נרצה להוכיח כי $a_1 = a_2$. אנו יודעים כי לכל איבר $x \in G$, ובפרט עבור e_G נקבל כי:

$$f_{a_1}(e_G) = f_{a_2}(e_G) \Longrightarrow a_1e_G = a_2e_G \Longrightarrow a_1 = a_2$$

חח"ע.

סה"כ הראינו שמדובר בהומומורפיזם מוגדר היטב, חח"ע, ואם נצמצם את התחום ל$Im(\phi)$ נקבל כי אכן מדובר באיזומורפיזם: $G \cong Im(\phi)$. כנדרש.

■

כעת, אם נחפש תת חבורה של תמורות שהיא איזומורפית לחבורה G - נקח את התמונה של שיכון קיילי.

משפט 91. כל חבורה סופית מגודל n איזומורפית לתת חבורה של S_n.

2.8 משפט לגראנז'

הגדרה 92. תהי חבורה G, ותהי תת חבורה $H \subseteq G$.
לכל איבר $a \in G$ נגדיר את המחלקה

$$aH = \{ah | h \in H\}$$

לדוגמה:
עבור חבורת התמורות S_3 ניתן להגדיר את תת החבורה :

$$H = \{I, (1,3)\}$$

למשל, עבור התמורה $(1,2) \in S_3$ נקבל:

$$(1,2)H = \{(1,2), (1,2)(1,3)\} = \{(1,2), (2,1)(1,3)\} = \{(1,2), (2,1,3)\}$$

משפט 93. גודל כל המחלקות מהצורה aH יהיה $|H|$. כלומר לכל $a \in G$ מתקיים $|aH| = |H|$.

מסקנה 94. ממשפט לגראנז': כיוון שהגודל של כל תת חבורה צריך לחלק את גודל החבורה, כלומר $|H| | |G|$, אזי אם $|G| = p$ עבור p ראשוני, אזי בהכרח לG ישנן תתי חבורות מגודל 1 ו$|G|$ בלבד. כלומר זוג חבורות: החבורה הטריוואלית $\{e_G\}$ וG.

משפט 95. תהי חבורה G ותת חבורה שלה H. נגדיר יחס שקילות R על G ע"י:
לכל $g_1, g_2 \in G$ נגדיר: $g_1Rg_2 \Longleftrightarrow g_1^{-1}g_2 \in H$ (כלומר, זוג נמצא ביחס אמ"מ ה"הפרש" $(g_1g_2^{-1})$ בניהם נמצא באותה תת חבורה).
אזי:
1. R יחס שקילות
2. לכל איבר $a \in G$ מתקיים $[a]_R = aH$
3. לכל $a \in G$ מתקיים $|aH| = |H|$.

הוכחה:
1. נוכיח שאכן מדובר ביחס שקילות.
רפלקסיביות - יהי $g_1 \in G$. אזי, נראה כי $g_1^{-1}g_1 = e_G \in H$ מהגדרת תת חבורה תמיד $e_G \in H$ ולכן g_1Rg_1.

סימטריות - נניח g_1Rg_2. אזי, $g_1^{-1}g_2 \in H$. נרצה להראות כי $g_2^{-1}g_1 \in H$. אם כן, כיוון ש$(g_1^{-1}g_2) \in H$, גם $(g_1^{-1}g_2)^{-1} \in H$ והרי $(g_1^{-1}g_2)^{-1} = g_2^{-1}g_1$ ולכן סה"כ הראינו $g_2^{-1}g_1 \in H$ ולכן g_2Rg_1

טרנזטיביות - נניח g_1Rg_2 וגם g_2Rg_3. אזי, $g_1^{-1}g_2 \in H$ וגם $g_2^{-1}g_3 \in H$. כיוון שH תת חבורה ישנה סגירות ולכן $(g_1^{-1}g_2)(g_2^{-1}g_3) = g_1^{-1}(g_2^{-1}g_2)g_3 = g_1^{-1}e_Gg_3 = g_1^{-1}g_3 \in H$ שכן יש אסוציאטיביות בחבורה ובתת חבורה בפרט. סה"כ קיבלנו g_1Rg_3.

2. כעת יהי $a \in G$. נרצה להראות כי $[a]_R = aH$. יש לנו כאן שוויון בין קבוצות לכן נבצע הכלה זו כיוונית:

$\subseteq$ יהי $x \in [a]_R$. אזי, aRx, כלומר $a^{-1}x \in H$. כלומר, קיים $h \in H$ כך ש: $a^{-1}x = h$. כעת, נכפיל בa משמאל ונקבל $aa^{-1}x = ah$ כלומר $x = ah$ ולכן $x \in aH$.

$\supseteq$ בכיוון השני, יהי $x \in aH$. אזי קיים $h \in H$ כך ש$x = ah$. נכפול בa^{-1} מימין ונקבל $a^{-1}x = h$, כלומר $a^{-1}x \in H$ כלומר aRx, כלומר $x \in [a]_R$.

3. נרצה להראות עבור $a \in G$ כי $|aH| = |H|$. לכן נבנה פונקציה חח"ע ועל בין שתי הקבוצות. נגדיר $f : H \to aH$ ע"י:

$$f(h) = ah$$

בבירור מוגדרת היטב. כעת נוכיח שחח"ע ועל:

חח"ע: יהיו $h_1, h_2 \in H$, כך ש$f(h_1) = f(h_2)$. אזי $ah_1 = ah_2$. נכפול בa^{-1} משמאל (בחבורה) ונקבל $h_1 = h_2$

על: יהי $x \in aH$. אזי קיים $h \in H$ עבורו $x = ah$. נראה כי $f(h) = ah$ ולכן h מקור לx.

סה"כ נקבל כי $|aH| = |H|$.

■

הגדרה 96. נסמן $[G : H]$ כאינדקס של תת החבורה. ערך זה מוגדר להיות כמות המחלקות השונות שH מגדירה.

משפט 97. משפט לגראנז': עבור חבורה סופית G, ותת חבורה שלה (בהכרח סופית גם היא) H מתקיים:

$$|G| = |H| \cdot [G : H]$$

כלומר: גודל כל חבורה הוא גודל תת חבורה שלה, כפול מס' המחלקות שאותה תת חבורה מגדירה.

מכאן נסיק: הגודל של כל תת חבורה, בהכרח מחלק את גודל החבורה.

הוכחה: כפי שראינו בבדיקה, יחס שקילות על קבוצה G מחלק אותה לחלוקה. קבוצות זרות שאיחודן הוא כל G. וכן ראינו כי $[a]_R = aH$ (ולכן כל איבר בG נמצא באחת מהקבוצות aH) כיוון שהראינו כי $|aH| = |H|$, וכן $[G : H]$ הוא מס' המחלקות שH מגדירה, נקבל כי: G היא קבוצה שמחולקת ל$[G : H]$ חתיכות - גודל כל חתיכה הוא $|H|$ ולכן סה"כ $|G| = |H| \cdot [G : H]$.

■

98. aÿoà¨ כיוון שתת החבורות הציקליות הן תת חבורה, וכן מתקיים $|< a >| = o(a)$, כמסקנה ממשפט לגראנז' הסדר של כל איבר מקיים $o(a)||G|$. (בחבורה סופית!).

99. èôùî תהי G סופית, אזי G מסדר זוגי אמ"מ קיים בה איבר מסדר 2.

משפט 100. איבר מסדר 2 הוא הופכי לעצמו.

משפט 101. לחבורה מסדר זוגי יש מס' אי זוגי של איברים מסדר 2. (שכן איבר היחידה מסדר אחד).