חבורות חשובות - הגדרות וטענות

מבנים אלגבריים (1) - 80445

מרצה: אורי פרזנצ'בסקי

מתרגל: ליאור נייהויזר

סוכם ע"י שריה אנסבכר

סמסטר א' תשפ"ד, האוניברסיטה העברית

1 החבורה החיבורית של חוג השלמים

יהי $n \in \mathbb{N}$.

משפט 1.1. מתקיים $\text{Aut}(\mathbb{Z}) \cong \mathbb{Z}^{\times} = \{1, -1\}$.

סימון: לכל $m \in \mathbb{Z}$ נסמן $m\mathbb{Z} := m \cdot \mathbb{Z} := \{mk \in \mathbb{Z} : k \in \mathbb{Z}\}$.

טענה 1.2. לכל $m \in \mathbb{Z}$ מתקיים $\langle m \rangle = m \cdot \mathbb{Z}$.

משפט 1.3. לכל תת-חבורה $H \leqslant \mathbb{Z}$ קיים $d \in \mathbb{Z}$ יחיד כך ש-$H = \langle d \rangle$, ואותו d הוא:

$$d := \min\{m \in \mathbb{N}_0 \mid m \in H\}$$

♣ כלומר אין ל-$\mathbb{Z}$ תתי-חבורות שאינן מהצורה $m\mathbb{Z}$.

משפט 1.4. יהיו $a_1, a_2, \ldots, a_n \in \mathbb{Z}$ כך שלפחות אחד מהם שונה מ-0 מתקיים:

$$\langle a_1, a_2, \ldots, a_n \rangle = \langle \gcd(a_1, a_2, \ldots, a_n) \rangle$$

2 החוג המודולרי $\mathbb{Z}_n$

יהי $n \in \mathbb{N}$.

תזכורת: אומרים ש-$m, k \in \mathbb{Z}$ <u>שקולים מודולו</u> n אם מתקיים $n \mid m - k$ (זהו אכן יחס שקילות), את <u>החוג המודולרי</u> מגדירים ע"י $\mathbb{Z}_n := \{k \in \mathbb{N}_0 : k < n\}$ או ע"י קבוצת מחלקות השקילות שמגדיר יחס השקילות המודולרי.
החיבור והכפל ב-$\mathbb{Z}_n$ מוגדרים ע"י לקיחת השארית של חלוקת הסכום/המכפלה ב-n (בהגדרה הראשונה) או ע"י לקיחת מחלקת השקילות של המכפלה/הסכום (בהגדרה השנייה).

♣ כמובן ששתי ההגדרות איזומורפיות ואנחנו נשתמש בשתיהן כאוות נפשנו לפי הנוחות.

♣ $n\mathbb{Z}$ היא תת-חבורה נורמלית של $\mathbb{Z}$, וכפי שראינו כל תת-חבורה מגדירה יחס שקילות ע"י המחלקות השמאליות שלה וקבוצת המנה של יחס זה היא קבוצת המחלקות השמאליות. במקרה שלנו $\mathbb{Z}/n\mathbb{Z}$ שהיא קבוצת המחלקות השמאליות של $n\mathbb{Z}$ היא בדיוק קבוצת המנה של יחס השקילות המודולרי.

♣ בשתי ההגדרות אנחנו מקבלים חוג חילופי, וכמו בכל חוג נסמן את קבוצת האיברים ההפיכים שבו ב-$\mathbb{Z}_n^{\times}$ שהיא חבורה ביחס לכפל של $\mathbb{Z}_n$.

משפט 2.1. מתקיים $\text{Aut}(\mathbb{Z}_n) \cong \mathbb{Z}_n^{\times} = \{m \in \mathbb{Z}_n \mid \gcd(m, n) = 1\}$.

משפט 2.2. לכל $m \in \mathbb{Z}_n$ מתקיים $\langle m \rangle = \langle \gcd(m, n) \rangle$.

מסקנה 2.3. לכל $m \in \mathbb{Z}_n$ מתקיים $\langle m \rangle = \mathbb{Z}_n$ אם"ם m זר ל-n (כלומר $\gcd(m, n) = 1$).

משפט 2.4. יהיו $n_1, n_2, \ldots, n_r \in \mathbb{N}$ זרים זה לזה בזוגות[1] ונסמן $m := n_1 \cdot n_2 \cdot \ldots \cdot n_r$, מתקיים $\mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \ldots \times \mathbb{Z}_{n_r} \cong \mathbb{Z}_m$.

♣ אחד האיזומורפיזמים הוא זה שמעתיק כל איבר $a \in \mathbb{Z}_m$ לסדרה $(a_1, a_2, \ldots, a_r)$ כאשר $a_i \equiv a \mod n_i$, וזה שקול למשפט השאריות הסיני.

[1] $\gcd(n_i, n_j) = 1$ לכל $r \geq i, j \in \mathbb{N}$ כך ש-$i \neq j$.

3 חבורת התמורות

יהי $n \in \mathbb{N}$.

תזכורת: תמורה על קבוצה היא העתקה חח"ע ועל (הפיכה) מהקבוצה לעצמה.

ראינו שיש רק חבורת תמורות[2] אחת על קבוצה סופית מגודל n (עד כדי איזומורפיזם), ולכן נעסוק רק בקבוצת התמורות על $\{1,2,\ldots,n\}$ (שהיא חבורה שפעולתה היא הרכבת פונקציות) ונסמן אותה ב-S_n.

סימון: ניתן לייצג כל תמורה $\sigma \in S_n$ ע"י מטריצה מהצורה הבאה:

$$\begin{pmatrix} 1 & 2 & \ldots & n \\ \sigma(1) & \sigma(2) & \ldots & \sigma(n) \end{pmatrix}$$

3.1 מחזורים

הגדרה 3.1. תמורה $\sigma \in S_n$ תיקרא מחזור אם קיימים $n \geq a_1, a_2, \ldots, a_r \in \mathbb{N}$ שונים זה מזה כך ש-$\sigma(a_i) = a_{i+1}$ לכל $r > i \in \mathbb{N}$ ו-$\sigma(a_r) = a_1$ ובנוסף $\sigma(x) = x$ לכל $x \in \{1,2,\ldots,n\} \setminus \{a_1, a_2, \ldots, a_r\}$.
מחזור כזה נסמן ע"י הסדרה $(a_1, a_2, \ldots, a_r)$, ונאמר ש-$(a_1, a_2, \ldots, a_r)$ פועל על כל $x \in \{1,2,\ldots,n\} \setminus \{a_1, a_2, \ldots, a_r\}$ באופן טריוויאלי.

♣ כמובן, הרעיון הוא שמחזור פועל על קבוצת איברים באופן מעגלי ומסיבה זו לכל $r \geq i \in \mathbb{N}$ שונה מ-1 מתקיים:

$$(a_1, a_2, \ldots, a_r) = (a_i, a_{i+1}, \ldots, a_r, a_1, a_2, \ldots, a_{i-1})$$

הגדרה 3.2. מחזור באורך 0 או באורך 1 ייקרא טריוויאלי, שכן הוא פועל על כל האיברים באופן טריוויאלי.

טענה 3.3. הסדר של מחזור לא טריוויאלי הוא האורך שלו.

הגדרה 3.4. נאמר שמחזור $(a_1, a_2, \ldots, a_r) \in S_n$ הוא תת-מחזור של תמורה $\sigma \in S_n$ אם לכל $r > i \in \mathbb{N}$ מתקיים $\sigma(a_i) = a_{i+1}$ וגם $\sigma(a_r) = a_1$.

למה 3.5. תהא $\sigma \in S_n$ תמורה, לכל $n \geq i \in \mathbb{N}$ קיים תת-מחזור של S_n כך ש-i מופיע בתת-המחזור, ובנוסף אותו תת-מחזור הוא טריוויאלי אם"ם $\sigma(i) = i$.

הגדרה 3.6. נאמר שמחזורים $(a_1, a_2, \ldots, a_m), (b_1, b_2, \ldots, b_k) \in S_n$ הם זרים זה לזה אם הקבוצות $\{a_1, a_2, \ldots, a_m\}$ ו-$\{b_1, b_2, \ldots, b_k\}$ זרות זו לזו.

למה 3.7. שני תתי-מחזורים של תמורה הם שווים או זרים.

טענה 3.8. לכל תמורה ב-S_n קיימת קבוצה יחידה של מחזורים זרים בזוגות שאינם טריוויאליים כך ש-σ שווה להרכבה של כל המחזורים הללו (לא משנה באיזה סדר) כשכל מחזור בדיוק מופיע פעם אחת בהרכבה.
כלומר כל תמורה ניתנת להצגה כהרכבה של מחזורים זרים בזוגות שאינם טריוויאליים (ללא חזרות), והצגה זו היא יחידה עד כדי סדר; נקרא להצגה זו הפירוק של התמורה למחזורים זרים.

[2] הכוונה היא לחבורת **כל** התמורות על הקבוצה.

טענה 3.9. כל תמורה ב-S_n ניתנת להצגה כהרכבה של מחזורים באורך 2 (לאו דווקא זרים), כלומר:

$$S_n = \langle\{(k,l) \mid n \geq k,l \in \mathbb{N},\ \ k \neq l\}\rangle$$

מסקנה 3.10. כל תמורה ב-S_n ניתנת להצגה כהרכבה של מחזורים מהצורה $(i,i+1)$ עבור $n > i \in \mathbb{N}$ כלשהו, כלומר:

$$S_n = \langle\{(i,i+1)\} \mid n > i \in \mathbb{N}\rangle$$

מסקנה 3.11. כל תמורה ב-S_n ניתנת להצגה כהרכבה של המחזורים $(1,2)$ ו-$(1,2,\ldots,n)$, כלומר:

$$S_n = \langle (1,2)\,, (1,2,\ldots,n)\rangle$$

טענה 3.12. יהי $(a_1,a_2,\ldots,a_r) \in S_n$ מחזור ותהא $\tau \in S_n$ תמורה, מתקיים:

$$\varphi_\tau\left(a_1,a_2,\ldots,a_r\right) = \tau \circ \left(a_1,a_2,\ldots,a_r\right) \circ \tau^{-1} = \left(\tau\left(a_1\right), \tau\left(a_2\right), \ldots, \tau\left(a_r\right)\right)$$

מסקנה 3.13. תהא $\sigma \in S_n$ ויהיו $\sigma_1,\sigma_2,\ldots,\sigma_r \in S_n$ מחזורים כך ש-$\sigma = \sigma_1 \circ \sigma_2 \circ \ldots \circ \sigma_r$ היא ההצגה של כהרכבה של מחזורים זרים, לכל תמורה $\tau \in S_n$ מתקיים:

$$\begin{aligned}\varphi_\tau\left(\sigma\right) &= \tau \circ \sigma \circ \tau^{-1} = \tau \circ \sigma_1 \circ \sigma_2 \circ \ldots \circ \sigma_r \circ \tau^{-1} \\ &= \tau \circ \sigma_1 \circ \tau^{-1} \circ \tau \circ \sigma_2 \circ \tau^{-1} \circ \tau \circ \ldots \circ \tau^{-1} \circ \tau \circ \sigma_r \circ \tau^{-1} \\ &= \varphi_\tau\left(\sigma_1\right) \circ \varphi_\tau\left(\sigma_2\right) \circ \ldots \circ \varphi_\tau\left(\sigma_r\right)\end{aligned}$$

♣ מכאן שמחלקת הצמידות של תמורה היא קבוצת כל התמורות שבפירוק שלהן למחזורים זרים יש את אותה כמות של מחזורים מכל גודל.

3.2 הסימן והתמורות הזוגיות

הגדרה 3.14. סימן של תמורה

תהא $\sigma \in S_n$ תמורה, מספר החילופים של תמורה הוא מספר הזוגות $(i,j) \in \mathbb{N}^2$ כך ש-$i < j \leq n$ ו-$\sigma\left(i\right) > \sigma\left(j\right)$, ואילו הסימן של σ הוא:

$$\text{sgn}\left(\sigma\right) := \begin{cases} 1 & \left|\left\{(i,j) \in \mathbb{N}^2 : i < j \leq n,\ \ \sigma\left(i\right) > \sigma\left(j\right)\right\}\right| \in \text{Even} \\ -1 & \left|\left\{(i,j) \in \mathbb{N}^2 : i < j \leq n,\ \ \sigma\left(i\right) > \sigma\left(j\right)\right\}\right| \in \text{Odd} \end{cases}$$

כלומר הסימן של תמורה הוא 1 אם מספר החילופים זוגי ו--1 אם מספר החילופים אי-זוגי, לכן נקרא לתמורה שסימנה הוא 1 תמורה זוגית ולתמורה שסימנה -1 נקרא אי-זוגית.

♣ בהגדרה של מספר חילופים יש משהו שרירותי: אין יחס סדר טבעי על סתם קבוצה, והעובדה שאנו עוסקים רק בקבוצה $\{1,2,\ldots,n\}$ אינה פותרת אותנו מעניין זה מפני שבאותה מידה היינו יכולים לתת לאיברים שמות אחרים. ובאמת מספר החילופים של תמורה אינו נשמר תחת הצמדה - כלומר לו היינו נותנים לאיברים שמות אחרים ייתכן שעבור אותה תמורה היינו מקבלים מספר חילופים שונה. לעומת זאת **הזוגיות** של מספר החילופים נשמרת תחת הצמדה ולכן אינה שרירותית.

טענה 3.15. תהא $\sigma \in S_n$ תמורה ויהיו $\tau_1, \tau_2, \ldots, \tau_r \in S_n$ מחזורים באורך 2 כך שמתקיים $\sigma = \tau_1 \circ \tau_2 \circ \ldots \circ \tau_r$, מתקיים:

$$\operatorname{sgn}(\sigma) = (-1)^r$$

מסקנה 3.16. הסימן של מחזור באורך $r \in \mathbb{N}$ הוא $(-1)^{r-1}$.

מסקנה 3.17. לכל שתי תמורות צמודות יש את אותו סימן.

טענה 3.18. נסמן $X := \left\{(i,j) \in \mathbb{N}^2 : i < j \leq n\right\}$, לכל $\sigma \in S_n$ מתקיים:

$$\operatorname{sgn}(\sigma) = \prod_{(i,j)\in X} \frac{j-i}{\sigma(j) - \sigma(i)}$$

סימון: נסמן $A_n := \{\sigma \in S_n \mid \operatorname{sgn}(\sigma) = 1\}$ - זוהי קבוצת התמורות הזוגיות.

טענה 3.19. לכל שתי תמורות $\sigma_1, \sigma_2 \in S_n$ מתקיים $\operatorname{sgn}(\sigma_1 \circ \sigma_2) = \operatorname{sgn}(\sigma_1) \cdot \operatorname{sgn}(\sigma_2)$, כלומר פונקציית הסימן היא הומומורפיזם מ-S_n ל-$\{1,-1\}$.

טענה 3.20. sgn הוא ההומומורפיזם היחיד ב-$\operatorname{Hom}(S_n, \{-1,1\})$ שאינו טריוויאלי.

מסקנה 3.21. מתקיים $\ker(\operatorname{sgn}) = A_n$, בפרט $A_n \trianglelefteq S_n$.

טענה 3.22. מתקיים $|A_n| = \frac{|S_n|}{2} = \frac{n!}{2}$ (בהנחה ש-$n > 1$).

טענה 3.23. תהא $\sigma \in A_n$ ותהא $O(\sigma)$ מחלקת הצמידות של σ ב-S_n, מתקיימת אחת משתי האפשרויות הבאות:

1. אם $C_{S_n}(\sigma) \nsubseteq A_n$ אז $O(\sigma)$ היא מחלקת הצמידות של σ גם ב-A_n.
2. אם $C_{S_n}(\sigma) \subseteq A_n$ אז קיימים $O_1, O_2 \subseteq A_n$ כך ש-$|O_1| = |O_2|$ ו-$O(\sigma) = O_1 \uplus O_2$ ו-O_1 היא מחלקת הצמידות של σ ב-A_n.[3]

מסקנה 3.24. A_5 היא חבורה פשוטה.

טענה 3.25. A_n נוצרת ע"י קבוצת המחזורים באורך 3 לכל $3 \leq n \in \mathbb{N}$.

טענה 3.26. קבוצת המחזורים באורך 3 היא מחלקת צמידות ב-A_n לכל $5 \leq n \in \mathbb{N}$.

למה 3.27. לכל $5 \leq n \in \mathbb{N}$ ולכל תת-חבורה נורמלית $N \trianglelefteq A_n$ קיים $e \neq \tau \in N$ כך שמתקיים:

$$|\{n \geq i \in \mathbb{N} : \tau(i) \neq i\}| \leq 5$$

כלומר τ משנה לכל היותר 5 איברים ולכל הפחות איבר אחד.

מסקנה 3.28. A_n היא חבורה פשוטה לכל $5 \leq n \in \mathbb{N}$.

- ♣ A_4 אינה פשוטה, מתקיים $\{\operatorname{Id}, (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\} \trianglelefteq A_4$.
- ♣ מתקיים $\{\operatorname{Id}, (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\} \cong \mathbb{Z}_2 \times \mathbb{Z}_2$, חבורה זו נקראת גם חבורת קליין על שמו של פליקס קליין ומסומנת גם ב-V.

[3] כלומר מחלקת הצמידות של σ ב-S_n "מתפרקת" לשתי קבוצות באותו גודל שאחת מהן היא מחלקת הצמידות של σ ב-A_n.

4 החבורה הדיהדרלית

יהי $n \in \mathbb{N}$.

החבורה הדיהדרלית D_n היא חבורת הסימטריות של מצולע משוכלל בעל n צלעות, כל סימטריה כזו נוצרת ע"י שיקוף שנעשה ע"י "מראה" או ע"י סיבוב סביב מרכזו, כך שלאחר הפעולה הוא נראה זהה לחלוטין למצבו שלפניה. ליתר דיוק מדובר בשיקופים דרך חוצי הזוויות של הקודקודים, בשיקופים דרך האנכים האמצעיים של הצלעות ובסיבובים בזווית $\frac{2\pi k}{n}$ רדיאנים כאשר n הוא מספר הצלעות ו-$n > k \in \mathbb{N}_0$.

♣ אם n אי-זוגי אז כל שיקוף דרך חוצה זווית של קודקוד הוא שיקוף דרך האנך האמצעי של הצלע הנגדית, ומצד שני אם n זוגי אז כל שיקוף סביב חוצה זווית של קודקוד הוא שיקוף סביב חוצה הזווית של הקודקוד הנגדי, ואותו הדבר קורה עבור שיקוף סביב האנכים האמצעיים של הצלעות (עם הצלעות הנגדיות כמובן); א"כ מתקיים $|D_n| = 2n$.

ננסה למצוא את הנוסחה להכפלת שני איברים בחבורה הדיהדרלית D_n, למעשה נעשה הרבה יותר מזה - אין שום צורך להתמקד דווקא בסיבובים ובשיקופים בזוויות הנ"ל ניתן להתבונן בכל שיקוף וסיבוב של המישור[4].

ראשית נשים לב לכך שכל סיבוב סביב ראשית הצירים (לא משנה באיזו זווית) אינו משנה את היחס שבין הצירים[5]: מבחינת ציר ה-x, ציר-y תמיד יישאר $\frac{\pi}{2}$ רדיאנים משמאלו, ומבחינת ציר ה-y ציר ה-x תמיד יישאר $\frac{\pi}{2}$ רדיאנים מימינו. לעומת זאת כל שיקוף (לא משנה דרך איזה ישר אנחנו משקפים) הופך את היחס שבין הצירים: לאחר כל פעולת השיקוף ציר ה-x יהיה $\frac{\pi}{2}$ רדיאנים משמאל לציר ה-y. בנוסף, ניתן לתאר כל פעולה ששומרת על היחס שבין הצירים כסיבוב בזווית כלשהי, וכמו כן כל פעולה שהופכת את היחס בין הצירים ניתנת להצגה כשיקוף דרך ישר כלשהו[6]. מכאן שההרכבה של שני סיבובים או שני שיקופים היא סיבוב, וההרכבה של סיבוב ושיקוף (לא משנה באיזה סדר) היא שיקוף; ובנוסף, כדי לדעת כיצד פועל סיבוב או שיקוף נתונים מספיק שנדע כיצד הוא פועל על ציר ה-x.

לכל $\alpha \in \mathbb{R}$ נסמן ב-$s(\alpha)$ את הסיבוב ב-α רדיאנים נגד כיוון השעון וב-$r(\alpha)$ את השיקוף דרך הישר שיוצר זווית α עם החלק החיובי של ציר ה-x נגד כיוון השעון[7]. א"כ המטריצות המייצגות של העתקות אלה[8] הן:

$$[s(\alpha)]_E = \begin{bmatrix} \cos\alpha & \cos\left(\alpha+\frac{\pi}{2}\right) \\ \sin\alpha & \sin\left(\alpha+\frac{\pi}{2}\right) \end{bmatrix} = \begin{bmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{bmatrix}$$

$$[r(\alpha)]_E = \begin{bmatrix} \cos 2\alpha & \cos\left(2\alpha-\frac{\pi}{2}\right) \\ \sin 2\alpha & \sin\left(2\alpha-\frac{\pi}{2}\right) \end{bmatrix} = \begin{bmatrix} \cos 2\alpha & \sin 2\alpha \\ \sin 2\alpha & -\cos 2\alpha \end{bmatrix}$$

כבר כעת ניתן להסיק את הנוסחה להרכבה של שיקופים וסיבובים (ע"י כפל מטריצות), אבל אני הבאתי אותן כאן רק כדי שיהיה ברור למה אני מתכוון, אני רוצה למצוא את הנוסחה בצורה אינטואיטיבית יותר.

סיבוב בזווית α מעביר את הישר שבזווית θ לישר שבזווית $\alpha+\theta$, ואילו שיקוף בזווית β מעביר את הישר שבזווית θ לישר שבזווית $2\beta-\theta$.

הזכרנו שכדי להבין כיצד פועל שיקוף או סיבוב מספיק לדעת כיצד הוא פועל על ציר ה-x (זווית 0), לפיכך (ע"פ הנוסחות הנ"ל):

- $s(\beta)\circ s(\alpha)$ הוא סיבוב ששולח את הציר ה-x לזווית $\alpha_1+\alpha_2$, כלומר $s(\beta)\circ s(\alpha) = s(\alpha+\beta)$.
- $r(\beta)\circ r(\alpha)$ הוא סיבוב ששולח את ציר ה-x לזווית $2\beta-2\alpha$, כלומר $r(\beta)\circ r(\alpha) = s(2\beta-2\alpha)$.
- $r(\beta)\circ s(\alpha)$ הוא שיקוף ששולח את ציר ה-x לזווית $2\beta-\alpha$, כלומר $r(\beta)\circ s(\alpha) = r\left(\beta-\frac{\alpha}{2}\right)$.
- $s(\beta)\circ r(\alpha)$ הוא שיקוף ששולח את ציר ה-x לזווית $2\alpha+\beta$, כלומר $s(\beta)\circ r(\alpha) = r\left(\alpha+\frac{\beta}{2}\right)$.

[4] ניתן להסתכל על זה בתור חבורת הסימטריות של המעגל, או החבורה. הדיהדרלית האין-סופית.
[5] מה שחברי, איתמר סלהוב, כינה בשיעור כיראליות.
[6] נבדוק לאיזו זווית הולך ציר ה-x ונחלק ב-2.
[7] נשים לב לכך שבסימון זה מתקיים $s(\alpha) = s(\alpha+2\pi k)$ ו-$r(\alpha) = r(\alpha+\pi k)$ (לכל $\alpha \in \mathbb{R}$ ולכל $k \in \mathbb{Z}$).
[8] ראינו בליניארית 2 שאכן מדובר בהעתקות ליניאריות.

♣ מי שיכפיל את המטריצות המתאימות להרכבה $s\left(\beta\right)\circ s\left(\alpha\right)$ יקבל הוכחה אלגנטית לזהויות הטריגונומטריות:

$$\sin\left(\alpha+\beta\right)=\sin\alpha\cdot\cos\beta+\cos\alpha\cdot\sin\beta$$
$$\cos\left(\alpha+\beta\right)=\cos\alpha\cdot\cos\beta-\sin\alpha\cdot\sin\beta$$

שכן $s\left(\beta\right)\circ s\left(\alpha\right)=s\left(\alpha+\beta\right)$.

סימון: נהוג לסמן ב-s או ב-σ את הסיבוב ב$\frac{2\pi}{n}$ רדיאנים, וב-r או ב-τ את השיקוף "הראשי" - זה לא לגמרי מוגדר, לא אמרנו באיזה כיוון הסיבוב ומהו הציר שדרכו אנו משקפים אך למעשה זה כלל לא משנה. משום מה בקורס שלנו בחרו שכיוון הסיבוב החיובי יהיה עם כיוון השעון ושציר השיקוף הראשי יהיה הציר האנכי ("ציר ה-y"); למרות זאת, כדי לשמור על עקביות עם הסיכומים האחרים שלי ועם המקובל בעולם המתמטי בכלל[9], אבחר בסיכום זה שכיוון הסיבוב החיובי יהיה נגד כיוון השעון וציר השיקוף הראשי יהיה הציר האופקי.

♣ לבחירה זו יש רווח נוסף והוא שכך סיבוב ב-$\frac{2\pi k}{n}$ רדיאנים מתאים למספר המרוכב $\text{cis}\left(\frac{2\pi k}{n}\right)$ והשיקוף הראשי מתאים לפעולת ההצמדה במרוכבים.

טענה 4.1. לכל $n>k\in\mathbb{N}$ כך ש-$k\mid n$ מתקיים $\left\langle \sigma^{k}\right\rangle \cong\mathbb{Z}_{\frac{n}{k}}$, בפרט $\left\langle \sigma\right\rangle \cong\mathbb{Z}_{n}$.

טענה 4.2. מתקיים $D_{n}=\left\langle \sigma,\tau\right\rangle$.

טענה 4.3. מתקיים $D_{n}=\left\{ e,\sigma,\sigma^{2},\ldots,\sigma^{n-1},\tau,\sigma\tau,\sigma^{2}\tau,\ldots,\sigma^{n-1}\tau\right\}$.

♣ ההוכחה פשוטה: ראינו כבר ש-$\left|D_{n}\right|=2n$ ואנחנו יודעים שלכל $i,j\in\mathbb{N}_{0}$ מתקיים:

$$\sigma^{i}=\sigma^{j}\iff i\equiv j\mod n$$
$$\sigma^{i}\tau=\sigma^{j}\tau\iff i\equiv j\mod n$$

מכאן שלכל $n>i,j\in\mathbb{N}_{0}$ כך ש-$i\neq j$ מתקיים $\sigma^{i}\neq\sigma^{j}$ ו-$\sigma^{i}\tau\neq\sigma^{j}\tau$.

♣ ע"פ הסימונים שלנו לעיל מתקיים $\sigma=s\left(\frac{2\pi}{n}\right)$ ו-$\tau=r\left(0\right)$, לכן ע"פ כללי הכפל שראינו לעיל מתקיים (לכל $n>k\in\mathbb{N}_{0}$):

$$\sigma^{k}=s\left(\frac{2\pi k}{n}\right),\ \sigma^{k}\tau=r\left(\frac{\pi k}{n}\right)$$

ולכן לכל $n>i,j\in\mathbb{N}_{0}$ מתקיים:

$$\sigma^{i}\cdot\sigma^{j}=s\left(\frac{2\pi i}{n}\right)\circ s\left(\frac{2\pi j}{n}\right)=s\left(\frac{2\pi\left(i+j\right)}{n}\right)=\sigma^{i+j}$$
$$\sigma^{i}\tau\cdot\sigma^{j}\tau=r\left(\frac{\pi i}{n}\right)\circ r\left(\frac{\pi j}{n}\right)=s\left(\frac{2\pi\left(i-j\right)}{n}\right)=\sigma^{i-j}$$
$$\sigma^{i}\tau\cdot\sigma^{j}=r\left(\frac{\pi i}{n}\right)\circ s\left(\frac{2\pi j}{n}\right)=r\left(\frac{\pi\left(i-j\right)}{n}\right)=\sigma^{i-j}\tau$$
$$\sigma^{i}\cdot\sigma^{j}\tau=s\left(\frac{2\pi i}{n}\right)\circ r\left(\frac{\pi j}{n}\right)=r\left(\frac{\pi\left(i+j\right)}{n}\right)=\sigma^{i+j}\tau$$

טענה 4.4. לכל $n>i,j\in\mathbb{N}_{0}$ מתקיים:

$$\sigma^{i}\cdot\sigma^{j}\cdot\left(\sigma^{i}\right)^{-1}=\sigma^{j}$$
$$\left(\sigma^{i}\tau\right)\cdot\sigma^{j}\cdot\left(\sigma^{i}\tau\right)^{-1}=\sigma^{-j}$$
$$\sigma^{i}\cdot\sigma^{j}\tau\cdot\left(\sigma^{i}\right)^{-1}=\sigma^{j+2i}\tau$$
$$\left(\sigma^{i}\tau\right)\cdot\sigma^{j}\tau\cdot\left(\sigma^{i}\tau\right)^{-1}=\sigma^{-j+2i}\tau$$

[9] הסיבה הראשונה חלה על שתי הבחירות, אך סיבה זו חלה רק על כיוון הסיבוב שבאופן מקובל מוגדר כך שנגד כיוון השעון הוא הכיוון החיובי.

מסקנה 4.5. יהי $n > k \in \mathbb{N}_0$, מחלקת הצמידות של σ^k היא $\left\{\sigma^k, \sigma^{-k}\right\}$, ומחלקת הצמידות של $\sigma^k\tau$ היא $\left\{\sigma^i\tau \mid i \in \mathbb{Z},\ i-k \equiv 0 \mod 2\right\}$.

♣ כאשר n אי-זוגי זה אומר שמחלקת הצמידות של שיקוף היא קבוצת כל השיקופים, אך אם n זוגי אז קבוצת השיקופים מתחלקת לשתי מחלקות צמידות: אלו שצמודים ל-τ ואלו שצמודים ל-$\sigma\tau$.
המצב הזה אינו מפתיע אם זוכרים שהאינטואיציה מאחורי פעולת ההצמדה היא שאנו עוברים לעולם מ"נקודת המבט" של האיבר המצמיד, מפעילים שם את האיבר המוצמד וחוזרים חזרה לעולם "הרגיל". זה אומר שהצמדה חייבת לשמור על התכונות הגאומטריות של האיבר המוצמד: כשמדובר בסיבוב זה אומר שניתן להגיע רק לסיבוב באותו גודל ורק הכיוון יכול להשתנות, וכשמדובר בשיקוף זה אומר שהצמדה חייבת לשמור על "סוג" השיקוף - האם הוא שיקוף דרך חוצה זווית של קודקוד או שהוא שיקוף דרך אנך אמצעי של צלע. עבור n אי-זוגי כל השיקופים שייכים לשני הסוגים ולכן יש רק מחלקת צמידות אחת, אבל כש-n זוגי השיקופים מתחלקים לשני הסוגים הנ"ל והם מחלקות הצמידות.

מסקנה 4.6. לכל $n > k \in \mathbb{N}$ כך ש-$n \mid k$ מתקיים $\left\langle\sigma^k\right\rangle \trianglelefteq D_n$.

מסקנה 4.7. אם n אי-זוגי אז $Z\left(D_n\right) = \{e\}$, ואם n זוגי אז $Z\left(D_n\right) = \left\{e, \sigma^{\frac{n}{2}}\right\}$.

מסקנה 4.8. D_n היא חבורה נילפוטנטית אם"ם קיים $k \in \mathbb{N}$ כך ש-$n = 2^k$.

5 חבורת הקווטרניונים

♣ כולנו מכירים המספרים המרוכבים המייצגים את המישור, כך שהכפל והחיבור שלהם מתארים פעולות פשוטות עליו (הזזה, מתיחה/כיווץ וסיבוב). המתמטיקאי ויליאם רואן המילטון חיפש מבנה אלגברי בעל פעולות חיבור וכפל שיוכל לתאר את המרחב התלת-ממדי, אך מבנה כזה לא נמצא עד היום[10]. בשנת 1843, בעת שטייל עם אשתו בדבלין, מצא המילטון את אלגברת הקווטרניונים של המילטון - מבנה אלגברי בעל פעולות חיבור וכפל המתאר את המרחב הארבע-ממדי - ובהתלהבותו הרבה חרט את הנוסחה הבסיסית לכפל על גשר שנמצא בסמוך:

$$i^2 = j^2 = k^2 = ijk = -1$$

האיברים i, j, k הם הווקטורים e_2, e_3, e_4 ב-$\mathbb{R}^4$, ומהנוסחה הנ"ל ניתן להסיק את הכפל של כל שני וקטורים ב-$\mathbb{R}^4 = \{a + bi + cj + dk \mid a, b, c, d \in \mathbb{R}\}$ (החיבור הוא החיבור הווקטורי שאנחנו כבר מכירים).

הגדרה 5.1. חבורת הקווטרניונים היא הקבוצה $Q := \{\pm1, \pm i, \pm j, \pm k\}$ והיא אכן סגורה לכפל המתקבל מן הנוסחה הנ"ל, ליתר בהירות נביא כאן את טבלת הכפל שלה:

$\cdot$	1	i	j	k
1	1	i	j	k
i	i	-1	k	$-j$
j	j	$-k$	-1	i
k	k	j	-1	-1

כאשר שינוי הסימן של אחד מן האיברים המוכפלים הופך את הסימן של תוצאת המכפלה, ושינוי הסימן של שניהם משאיר את הסימן על כנו.

♣ א"כ לכל $x \in \{\pm i, \pm j, \pm k\}$ מתקיים $x^{-1} = -x$.

[10] המרחב הווקטורי $\mathbb{R}^3$ "מוותר" על האפשרות לכפול כל שני וקטורים זה בזה ו"מסתפק" ביכולת לכפול רק בווקטורים מסוימים - המספרים הממשיים.

♣ כדי לזכור את כללי הכפל ניתן לסדר את i,j,k במעגל:

$$\begin{array}{ccccc} & & i & & \\ & \nearrow & & \searrow & \\ k & & \longleftarrow & & j \end{array}$$

כך שכפל שני איברים עם כיוון השעון יחזיר את האיבר השלישי, וכפל שני איברים נגד כיוון השעון יחזיר את הנגדי של האיבר השלישי.

טענה 5.2. מתקיים $Z(Q)=\{1,-1\}$.

טענה 5.3. מחלקות הצמידות של Q הן $\{1\}$, $\{-1\}$, $\{\pm i\}$, $\{\pm j\}$ ו-$\{\pm k\}$.

טענה 5.4. מתקיים $\mathrm{Inn}(Q)\cong\mathbb{Z}_2\times\mathbb{Z}_2$.

6 נספחים

6.1 מיון כל החבורות מסדר קטן מ-12

תזכורת: ראינו שלכל ראשוני $p\in\mathbb{N}$ קיימת רק חבורה אחת מסדר p ($\mathbb{Z}_p$), וכמו כן קיימות שתי חבורות מסדר p^2: $\mathbb{Z}_{p^2}$ ו-$\mathbb{Z}_p\times\mathbb{Z}_p$.
בנוסף, ראינו שלכל שני מספרים ראשוניים $p,q\in\mathbb{N}$ כך ש-$p\equiv 1 \mod p$, קיימות שתי חבורות מסדר $p\cdot q$ (עד כדי איזומורפיזם):
$\mathbb{Z}_q\times\mathbb{Z}_p$ שהיא חבורה ציקלית, וחבורה שאינה אבלית $\mathbb{Z}_q\rtimes_\varphi\mathbb{Z}_p$ עבור הומומורפיזם $\varphi:\mathbb{Z}_p\to\mathrm{Aut}(\mathbb{Z}_q)$ שאינו טריוויאלי.

מסקנה 6.1.

- החבורה היחידה מסדר 1 היא $\{e\}$.
- החבורות היחידות מסדר 2, 3, 5, 7 או 11 הן $\mathbb{Z}_2$, $\mathbb{Z}_3$, $\mathbb{Z}_5$, $\mathbb{Z}_7$ או $\mathbb{Z}_{11}$ (בהתאמה).
- יש שתי חבורות מסדר 4: $\mathbb{Z}_4$ ו-$\mathbb{Z}_2\times\mathbb{Z}_2$, וכמו כן יש שתי חבורות מסדר 9: $\mathbb{Z}_9$ ו-$\mathbb{Z}_3\times\mathbb{Z}_3$.

משפט 6.2. כל חבורה מסדר 8 איזומורפית לאחת מחמש החבורות הבאות:

$$\begin{array}{ll} D_4 & \mathbb{Z}_8 \\ Q & \mathbb{Z}_2\times\mathbb{Z}_4 \\ & \mathbb{Z}_2\times\mathbb{Z}_2\times\mathbb{Z}_2 \end{array}$$

6.2 כל חבורה מסדר קטן מ-60 היא חבורה פתירה

♣ כפי שראינו לעיל A_5 אינה פתירה ומתקיים $|A_5| = 60$.

תזכורת: ראינו שחבורה סופית G היא פתירה אם"ם כל אחד מגורמי ההרכב שלה איזומורפי ל-$\mathbb{Z}_p$ עבור ראשוני $p \in \mathbb{N}$ כלשהו.

♣ מכאן שאם לכל חבורה פשוטה G כך ש-$|G| < 60$ קיים ראשוני $p \in \mathbb{N}$ כך ש-$G \cong \mathbb{Z}_p$, אז כל חבורה מסדר קטן מ-60 היא חבורה פתירה.

תזכורת: ראינו שכל חבורת p היא פתירה.

למה 6.3. יהיו $p, q, n \in \mathbb{N}$ כך ש-p ו-q הם מספרים ראשוניים, אם $p^n < q$ אז כל חבורה מסדר $p^n \cdot q$ היא חבורה פתירה.

למה 6.4. יהיו $p, q, n, m \in \mathbb{N}$ כך ש-p ו-q הם מספרים ראשוניים, אם $p^n \cdot q^m$ אינו מחלק את $(p^n)!$ אז כל חבורה מסדר $p^n \cdot q^m$ היא חבורה פתירה.

♣ כדי שיהיה ברור אלו חבורות פסלנו עד כה נכתוב כעת את כל המספרים מ-1 עד 59 ונצבע אותם כך:

- **בכחול** יופיעו כל המספרים המהווים חזקה של מספר ראשוני.
- **בירוק** יופיעו כל המספרים מהצורה $p^n \cdot q$ כך ש-$p^n < q$.
- **בסגול** יופיעו כל המספרים מהצורה $p^n \cdot q^m$ כך ש-$p^n \cdot q^m$ אינו מחלק את $(p^n)!$.
- **באדום** יופיעו המספרים הנותרים.

1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	

למה 6.5. ממשפט סילו השלישי נובע שגם חבורות מסדר 30, 40, 42 או 56 הן חבורות פתירות.

מסקנה 6.6. כל חבורה סופית מסדר קטן מ-60 היא חבורה פתירה.