תורת החבורות - הגדרות בלבד

מבנים אלגבריים (1) - 80445

מרצה: אורי פרזנצ'בסקי

מתרגל: ליאור נייהויזר

סוכם ע"י שריה אנסבכר

סמסטר א' תשפ"ד, האוניברסיטה העברית

תוכן העניינים

בהכנת סיכום זה נעזרתי רבות בסיכומו המצוין של אייל צווכר,

ובספר "מבנים אלגבריים" מאת: דורון פודר, אלכס לובוצקי ואהוד דה-שליט.

* * *

סביר להניח שהסיכומים שלי מכילים טעויות רבות - אני מוצא כאלה כל יום (רשימת טעויות נפוצות),
אני מפציר בכם לעדכן אותי בכל טעות שאתם מוצאים (ממש כל טעות ללא יוצא מן הכלל);
אתם מוזמנים להגיב על המסמכים ב-Google Drive, לשלוח לי דוא"ל או למלא פנייה באתר.

לסיכומים נוספים היכנסו לאתר:
אקסיומת השלמות - סיכומי הרצאות במתמטיקה
https://srayaa.wixsite.com/math

1 התחלה

1.1 הגדרות בסיסיות

הגדרה 1.1. חבורה

חבורה היא זוג סדור $(G,\cdot)$ כאשר "$\cdot$" היא פעולה דו-מקומית המוגדרת על הקבוצה G ומקיימת 3 תכונות:

1. קיבוץ (אסוציאטיביות) - לכל $a,b,c\in G$ מתקיים $(a\cdot b)\cdot c=a\cdot(b\cdot c)$.
2. קיום איבר יחידה (אדיש/ניטרלי) - קיים $e\in G$ כך שלכל $g\in G$ מתקיים $a\cdot e=a=e\cdot a$.
3. קיום איבר הופכי - לכל $a\in G$ קיים $b\in G$ כך ש-$a\cdot b=e=b\cdot a$ כאשר e הוא איבר יחידה.[1]

ניתן לדרוש מראש את הקיום של e כחלק מהאקסיומות, ואז נישאר עקביים עם ההגדרה של השדה והמרחב הווקטורי ולא נצטרך את הערה 1, יש הרבה שינויים עיצוביים שנדרשים בעקבות השינוי הזה.

- ♣ לפעמים נכתוב סתם ab במקום $a\cdot b$.
- ♣ פעמים רבות נכתוב משפטים מהסגנון "תהא G חבורה", והכוונה תהיה ש-$(G,\cdot)$ היא החבורה ע"פ ההגדרה, וכמו כן נסמן את איבר היחידה של כל חבורה שנעסוק בה ב-e אלא אם נעסוק בכמה חבורות במקביל ואז ניתן לכל אחד מהם סימן משלו (ולפעמים אפילו את זה לא נעשה).
- ♣ נשים לב לכך שהפעולה אינה נדרשת לקיים חילוף (קומוטטיביות).

סימון: בקובץ הטענות אנחנו נראה שלכל איבר בחבורה יש איבר יחיד, לכן נסמן את האיבר ההופכי ב-a^{-1} (לכל a בחבורה).

תהא G חבורה.

הגדרה 1.2. תת-חבורה

נאמר שתת-קבוצה $H\subseteq G$ היא תת-חבורה (להלן גם: ת"ח) ונסמן $H\leqslant G$ אם מתקיימים שלושת התנאים הבאים:

1. $e\in H$.
2. לכל $a,b\in H$ גם $a\cdot b\in H$.
3. לכל $a\in H$ גם $a^{-1}\in H$.

- ♣ לכל חבורה יש שתי תתי-חבורות טריוויאליות: החבורה עצמה והיחידון שכולל רק את איבר היחידה.
- ♣ גם כאן, כמו בהגדרת תת-מרחב וקטורי, ניתן היה להחליף את התנאי הראשון בכך ש-H אינה ריקה.

מסקנה 1.3. כל תת-חבורה של G היא חבורה בפני עצמה ביחס לאותה פעולת כפל ולאותו איבר יחידה.

הגדרה 1.4. חבורה אָבֶּלִית[2]

G תיקרא אבלית (או חילופית) אם הכפל שלה מקיים את חוק החילוף (קומוטטיבי), כלומר לכל $a,b\in G$ מתקיים $a\cdot b=b\cdot a$.

הגדרה 1.5. המֶרְכָּז

המרכז של G הוא הקבוצה $Z(G):=\{g\in G\mid\forall h\in G\ gh=hg\}$.

מסקנה 1.6. המרכז של חבורה הוא תת-חבורה אבלית.

[1] בקובץ ההוכחות נראה שיש ב-G איבר יחידה יחיד ולכן דרישה זו מוגדרת היטב.
[2] החבורות האבליות נקראות על שם המתמטיקאי נילס הנריק אָבֶּל.

1.2 דוגמאות

♣ לפני שניתן כאן רשימת דוגמאות נזכיר שחוג הוא קבוצה המקיימת את כל אקסיומות השדה מלבד קיום איבר הופכי והחילוף של הכפל, אם הכפל חילופי אז החוג נקרא גם חוג חילופי (קומוטטיבי).

הגדרה. חוג הוא קבוצה R בעלת שני איברים שונים (לכל הפחות) הנקראים "אפס" (יסומן ב-0) ו-"אחד" (יסומן ב-1), שעליה מוגדרות שתי פעולות דו-מקומיות הנקראות "חיבור" (תסומן ב-"$+$") ו-"כפל" (תסומן ב-"$\cdot$"), כך שמתקיימות 7 התכונות הבאות:

תכונה	חיבור (לכל $a,b,c\in R$)	כפל (לכל $a,b,c\in R$)
חילוף (קומוטטיביות)	$a+b=b+a$	-
קיבוץ (אסוציאטיביות)	$(a+b)+c=a+(b+c)$	$(a\cdot b)\cdot c=a\cdot(b\cdot c)$
קיום איבר אדיש (ניטרלי)	$a+0=a$	$a\cdot 1=a$
קיום איבר נגדי/הופכי	$\exists d\in R: a+d=0$	-
פילוג (דיסטריבוטיביות)	$a\cdot(b+c)=(a\cdot b)+(a\cdot c)$	

חוג R ייקרא חוג חילופי (קומוטטיבי) אם הכפל שלו מקיים את חוק החילוף.

♣ מהגדרה כל שדה הוא חוג חילופי.

♣ כל חוג מגדיר שתי חבורות: כל חוג R הוא חבורה ביחס לפעולת החיבור שלו (איבר היחידה הוא 0 וההופכי הוא הנגדי החיבורי) - חבורה זו נקראת החבורה החיבורית של החוג ומסומנת ב-R^+, וכמו כן קבוצת האיברים ההפיכים ב-R היא חבורה ביחס לפעולת הכפל של R (איבר היחידה הוא 1 וההופכי הוא ההופכי הכפלי) חבורה זו נקראת החבורה החיבורית של החוג ומסומנת ב-$R^\times$ או ב-R^*. החבורה החיבורי" של כל חוג היא אבלית, ואילו החבורה הכפלית של חוג היא אבלית אם"ם זהו חוג חילופי.

רשימת חוגים שאנחנו כבר מכירים

1. כל שדה $\mathbb{F}$.
2. חוג השלמים $\mathbb{Z}$.
3. חוג הפולינומים $\mathbb{F}[x]$ עבור שדה $\mathbb{F}$.
4. החוג המודולרי $\mathbb{Z}_n$ (בתורת המספרים סומן ע"י $\mathbb{Z}/n\mathbb{Z}$) - לכל שני מספרים שלמים בקבוצה $\{0,1,\ldots,n-1\}$ נגדיר את פעולות החיבור והכפל ע"י החיבור ב-$\mathbb{Z}$, וכדי שנקבל איבר בקבוצה נחלק ב-n עם שארית וניקח את השארית; ראינו בליניארית 1 שאם n ראשוני אז $\mathbb{Z}_n$ הוא שדה.
5. מרחב המטריצות $M_n(\mathbb{F})$ מעל שדה $\mathbb{F}$ עם פעולות החיבור וכפל מטריצות (דוגמה זו היא הדוגמה היחידה ברשימה לחוג שאינו חילופי), ובהתאמה עבור מ"ו נ"ס V גם $\mathrm{End}(V)$ (שהוא מרחב ההעתקות הליניאריות מ-V לעצמו) הוא חוג ביחס לחיבור העתקות ליניאריות והרכבתן.

א"כ כל החוגים הנ"ל הם חבורות ביחס לפעולת החיבור שלהם וכדי שנוכל לדבר על החבורה הכפלית שלהם עלינו לציין מהי קבוצת האיברים ההפיכים שלהם, להלן מופיעה הרשימה באותו הסדר.

1. $\mathbb{F}^\times=\mathbb{F}\setminus\{0_\mathbb{F}\}$
2. $\mathbb{Z}^\times=\{1,-1\}$
3. $(\mathbb{F}[x])^\times=\{P\in\mathbb{F}[x]:\deg P=0\}$
4. $\mathbb{Z}_n^\times=\{k\in\mathbb{Z}_n:\gcd(n,k)=1\}$
5. קבוצת המטריצות ההפיכות מסדר n מעל $\mathbb{F}$ - מסומנת ב-$\mathrm{GL}_n(\mathbb{F})$.

דוגמאות נוספות

- קבוצת התמורות של קבוצה X (קבוצת הפונקציות ההפיכות מקבוצה X לעצמה, נקראת גם חבורת הסימטריות ומסומנת ב-S_X או ב-$\mathrm{Sym}\left(X\right)$) היא חבורה ביחס לפעולת ההרכבה.
- חבורת הסימטריות של מצולע משוכלל (החבורה הדיהדרלית - מסומנת ב-D_n): סימטריה של מצולע משוכלל נוצרת ע"י שיקוף שנעשה ע"י "מראה" או ע"י סיבוב סביב מרכזו, כך שלאחר הפעולה הוא נראה זהה לחלוטין למצבו שלפניה; אנחנו נעסוק בחבורה זו בהרחבה בהמשך.
- כל מרחב וקטורי הוא חבורה ביחס לפעולת החיבור הווקטורי שלו, זוהי דוגמה חשובה מפני שהגדרות ומשפטים רבים שמופיעים במרחבים וקטוריים חלים בצורה דומה על חבורות וכך נוכל לקבל אינטואיציה מליניארית לכאן.
- תהיינה שתי חבורות $(G,\cdot_G)$ ו-$(H,\cdot_H)$, חבורת המכפלה הישרה של G ו-H היא החבורה $(G\times H,\cdot)$ שפעולת הכפל שלה מוגדרת ע"י (לכל $\left(g_1,h_1\right),\left(g_2,h_2\right)\in G\times H$):
$$\left(g_1,h_1\right)\cdot\left(g_2,h_2\right):=\left(g_1\cdot_G g_2,h_1\cdot_H h_2\right)$$
באותה צורה נגדיר גם את חבורת המכפלה הישרה של כל מספר סופי של חבורות.

תתי-חבורות של הדוגמאות הנ"ל

- לכל חבורה יש שתי תתי-חבורות שנכנה טריוויאליות - החבורה עצמה והיחידון שכולל את איבר היחידה שלה.
- קבוצת הרציונליים החיוביים ($\mathbb{Q}_{>0}$) היא תת-חבורה של $\mathbb{Q}^\times$, וזו יחד עם קבוצת הממשיים החיוביים ($\mathbb{R}_{>0}$) הן תתי-חבורות של $\mathbb{R}^\times$.
- קבוצת המטריצות שהדטרמיננטה שלהן היא 1 היא תת-חבורה של $\mathrm{GL}_n\left(\mathbb{F}\right)$ - מסומנת ע"י $\mathrm{SL}_n\left(\mathbb{F}\right)$, כמו כן קבוצת המטריצות שהדטרמיננטה שלהן היא ±1 היא תת-חבורה של $\mathrm{GL}_n\left(\mathbb{F}\right)$ ו-$\mathrm{SL}_n\left(\mathbb{F}\right)$ היא תת-חבורה שלה.
- ראינו בליניארית 2 שקבוצת המטריצות האוניטריות היא תת-חבורה של $\mathrm{SL}_n\left(\mathbb{C}\right)$ וקבוצת המטריצות האורתוגונליות היא תת-חבורה של $\mathrm{SL}_n\left(\mathbb{R}\right)$.
- מעגל היחידה המרוכב $S^1:=\{z\in\mathbb{C}:|z|=1\}$ הוא תת-חבורה של $\mathbb{C}^*$.
- קבוצת הסיבובים של מצולע משוכלל (בזוויות שהוזכרו לעיל) היא תת-קבוצה של החבורה הדיהדרלית.

1.3 חזקות

הגדרה 1.7. חזקה

לכל $g \in G$ ולכל $n \in \mathbb{N}$ נסמן:

$$g^n := \overbrace{g \cdot g \cdot \ldots \cdot g}^{n \text{ פעמים}}$$
$$g^0 := e$$
$$g^{-n} := \overbrace{g^{-1} \cdot g^{-1} \cdot \ldots \cdot g^{-1}}^{n \text{ פעמים}}$$

♣ מי שההגדרה הזו לא נראית לו מספיק פורמלית מוזמן להשתמש באחת ההגדרות הבאות[3]:

$$g^n = \prod_{i=1}^{n} g, \;\; g^{-n} = \prod_{i=1}^{n} g^{-1}$$

$$g^0 := e, \;\; g^{n+1} := g \cdot g^n, \;\; g^{-n} := \left(g^{-1}\right)^n$$

♣ שוב יש לשים לב לכך שאין לנו בעיות בסימון - ההופכי של g הוא בדיוק g בחזקת -1.

מסקנה 1.8. חוקי חזקות

לכל $g, h \in G$ ולכל $n, m \in \mathbb{Z}$ מתקיימים שלושת הפסוקים הבאים:

- $g^{n+m} = g^n \cdot g^m = g^m \cdot g^n$.
- $(g^n)^m = g^{n \cdot m}$.
- אם G אבלית אז $(g \cdot h)^n = g^n \cdot h^n$[4].

---

[3] הערך של המכפלה הריקה הוא איבר היחידה.

[4] למעשה גם הכיוון ההפוך נכון: אם מתקיים $(g \cdot h)^n = g^n \cdot h^n$ לכל $g, h \in G$ ולכל $n, m \in \mathbb{Z}$ אז G אבלית.

1.4 חבורות נוצרות וקבוצות יוצרים

טענה. תהא X קבוצת תתי-חבורות של G, החיתוך של כל תתי-החבורות ב-X הוא תת-חבורה של G.

הגדרה 1.9. תהא $S \subseteq G$ תת-קבוצה, תת-החבורה הנוצרת ע"י S (מסומנת ע"י $\langle S \rangle$) היא חיתוך כל תתי-החבורות המכילות את S.

מסקנה 1.10. תהא $S \subseteq G$ תת-קבוצה, מתקיימים שלושת הפסוקים הבאים:

1. $\langle S \rangle$ היא תת-חבורה של G.
2. $S \subseteq \langle S \rangle$.
3. לכל תת-חבורה $H \leqslant G$ המכילה את S מתקיים $\langle S \rangle \subseteq H$.

הגדרה 1.11. תהא $H \leqslant G$ תת-חבורה, נאמר שתת-קבוצה $S \subseteq G$ היא קבוצת יוצרים של H אם $H = \langle S \rangle$.

♣ קבוצת יוצרים היא המקבילה של קבוצה פורשת מליניארית. אולי היה מתבקש גם להגדיר קבוצה "בלתי תלויה"[5] כמו שבליניארית הגדרנו קבוצה בת"ל (ולאחר מכן להגדיר גם בסיסים); אלא שכאן אין לזה שום שימוש: הגודל שני "בסיסים" כאלה אינו מוכרח להיות שווה, ואמנם הגדרת הומומורפיזם (המקבילה של העתקה ליניארית) על קבוצת יוצרים היא יחידה (אם היא קיימת), אך אין שום ערובה לכך שהומומורפיזם כזה קיים בכלל אפילו אם הקבוצה "בלתי תלויה".

♣ בהמשך נראה שעבור חבורות מסוג מסוים (חבורות חופשיות) ניתן לדבר על בסיס של חבורה.

סימון: עבור קבוצה סופית $\{s_1, s_2, \ldots, s_n\} \subseteq G$ נכתוב גם $\langle s_1, s_2, \ldots, s_n \rangle := \langle \{s_1, s_2, \ldots, s_n\} \rangle$.

הגדרה 1.12. נאמר ש-G היא ציקלית אם קיים $g \in G$ כך ש-$G = \langle g \rangle$.

מסקנה 1.13. כל חבורה ציקלית היא חבורה אבלית.

הגדרה 1.14. תהיינה A ו-B שתי קבוצות; נאמר ש-A ו-B מאותה עוצמה, ונסמן $|A| = |B|$, אם קיימת פונקציה חח"ע ועל $f : A \to B$.

♣ זוהי הגדרה מתורת הקבוצות אך הבאתי אותה כאן מפני שהמונח עוצמה יחזור על עצמו עמה פעמים במהלך הקורס.

♣ בתורת הקבוצות מגדירים $0 := \emptyset$ ולכל n מוגדר ע"י קודמיו $n := (n-1) \cup \{n-1\} = \{0, 1, \ldots, n-1\}$, כלומר כל מספר טבעי[6] n הוא **קבוצה** שבה n איברים וכך הוא מגדיר את העוצמה של קבוצות סופיות בנות n איברים.

הגדרה 1.15. הסדר של G הוא $|G|$ - העוצמה של G, ואילו הסדר של איבר $g \in G$ בחבורה הוא $|g| := \min\{n \in \mathbb{N} : g^n = e\}$ (בהנחה שהקבוצה אינה ריקה), אם הקבוצה $\{n \in \mathbb{N} : g^n = e\}$ ריקה נאמר שהסדר של g הוא אין-סופי ונכתוב $|g| = \infty$.

♣ למשל, הסדר של חבורת התמורות על קבוצה סופית X הוא $n!$ כאשר $n := |X|$.

הגדרה 1.16. גרף קיילי[7]

גרף קיילי של תת-קבוצה $S \subseteq G$ הוא הגרף המכוון (G, E) כאשר $E := \{(g, sg) : s \in S\}$.

---

[5] ניתן היה להגדיר שקבוצה $S \subseteq G$ היא קבוצה בלתי תלויה אם לכל $s \in S$ מתקיים $s \notin \langle S \setminus \{s\} \rangle$.

[6] כאן הטבעיים כוללים את 0 ומכאן השאלה הנצחית "האם בקורס זה הטבעיים כוללים את 0 או לא?"

[7] ערך בוויקיפדיה: ארתור קיילי.

2 מחלקות ותתי-חבורות נורמליות

תהא G חבורה.

הגדרה 2.1. מחלקה שמאלית ומחלקה ימנית[8]

תהא $H \leqslant G$ תת-חבורה.

- מחלקה שמאלית של H היא כל קבוצה מהצורה $gH := \{gh : h \in H\}$ עבור $g \in G$.
- מחלקה ימנית של H היא כל קבוצה מהצורה $Hg := \{hg : h \in H\}$ עבור $g \in G$.

♣ שפי שנראה בקובץ הטענות להיות באותה מחלקה ימנית/שמאלית של H זה יחס שקילות, לכן יש המסמנים את המחלקה של איבר $g \in G$ ב-$\bar{g}$ כמו שעושים עם יחסי שקילות אחרים.

סימון: לכל תת-חבורה $H \leqslant G$ נסמן ב-G/H את קבוצת המחלקות השמאליות של H, וכמו כן נסמן ב-$H\backslash G$ את קבוצת המחלקות הימניות של H.

סימון: לכל תת-חבורה $H \leqslant G$ נסמן $[G:H] := |G/H|$ ונקרא ל-$[G:H]$ האינדקס של H.

הגדרה 2.2. תת-חבורה נורמלית

נאמר שתת-חבורה $N \leqslant G$ היא נורמלית אם לכל $g \in G$ מתקיים $gN = Ng$, ובמקרה כזה נסמן $N \trianglelefteq G$.

מסקנה 2.3. $Z(G) \trianglelefteq G$, ואם G אבלית אז כל תת-חבורה שלה היא נורמלית.

♣ בכל חוג כל תתי-החבורות של החבורה החיבורית שלו הן תתי-חבורות נורמליות, וכמו כן בכל חוג חילופי על תתי-החבורות של החבורה הכפלית הן תתי-חבורות נורמליות.

---

[8] אורי קרא למחלקה "קוסט" (coset).

3 פעולה של חבורה על קבוצה

תהא G חבורה.

3.1 פעולה כללית

הגדרה 3.1. תהא X קבוצה, פעולה של G על X היא פונקציה $. : G \times X \to X$ המקיימת שתי תכונות:

1. היחידה היא פונקציית הזהות - לכל $x \in X$ מתקיים $e.x = x$.
2. חוק הקיבוץ (אסוציאטיביות) - לכל $x \in X$ ולכל $a, b \in G$ מתקיים $(a \cdot b).x = a.(b.x)$.

במקרה כזה נאמר ש-G פועלת על X ע"י הפעולה ".".

סימון ל-"חבורה פועלת על קבוצה".

- ♣ זוהי פעולה שמאלית של חבורה על קבוצה, ניתן היה להגדיר גם פעולה ימנית אך הן מתנהגות באותה הצורה ולכן אין בזה צורך.
- ♣ גם כאן פעמים רבות נשמיט את סימן הפעולה ונכתוב gx במקום $g.x$.
- ♣ מספיק לדעת כיצד פועלת קבוצת יוצרים של G על X כדי לדעת הכל אודות פעולת G על X.
- ♣ כל חבורה G פועלת על עצמה ע"י הכפל של החבורה ($g.x := g \cdot x$ לכל $g, x \in G$), כמו כן כל חבורה G פועלת על קבוצת המחלקות השמאליות של תת-חבורה $H \leqslant G$ (G/H) ע"י הכפל של החבורה ($g.xH := gxH$ לכל $g, x \in G$).

תהא X קבוצה כך ש-G פועלת על X.

מסקנה 3.2. כל אחד מהאיברים ב-G מגדיר תמורה על איברי X ע"י פעולת החבורה על הקבוצה.

הגדרה 3.3. המסלול של איבר $x \in X$ הוא הקבוצה:

$$O_G(x) := O(x) := \{g.x \mid g \in G\}$$

סימון: נסמן ב-$G \backslash X$ את קבוצת המסלולים של האיברים ב-X ($G \backslash X := \{O(x) : x \in X\}$).

- ♣ אין לנו כאן בעיה של סימון מפני שאם X היא חבורה ו-$G \leqslant X$ תת-חבורה, אז קבוצת המסלולים בפעולת G על X ע"י הכפל של החבורה היא בדיוק קבוצת המחלקות הימניות של G ב-X.

הגדרה 3.4. נאמר שפעולת החבורה G על הקבוצה X היא:

- טרנזיטיבית אם לכל $x, y \in X$ מתקיים $O(x) = O(y)$ - כלומר קיים רק מסלול אחד תחת הפעולה.
- נאמנה אם e הוא האיבר היחיד ב-G שמקיים $e.x = x$ לכל $x \in X$.
- חופשית אם e הוא האיבר היחיד ב-G שעבורו קיים $x \in X$ המקיים $e.x = x$.

הגדרה 3.5. המייצב של איבר $x \in X$ הוא הקבוצה:

$$G_x := \mathrm{Stab}_G(x) := \{g \in G \mid g.x = x\}$$

3.2 הצמדה

הגדרה 3.6. לכל $g\in G$ נגדיר את ההצמדה ב-g ע"י $\varphi_g(x):=gxg^{-1}$[9] (לכל $x\in G$).

♣ האינטואיציה להצמדה היא שאנו הולכים לצורה שבה העולם נראה ע"פ g, מפעילים שם את x וחוזרים חזרה לעולם "הרגיל", למעשה כבר ראינו זאת בדמיון מטריצות - שם אמרנו ששתי מטריצות $A,B\in M_n(\mathbb{F})$ הן דומות אם קיימת מטריצה הפיכה $P\in M_n(\mathbb{F})$ כך ש-$A=PAP^{-1}$ - אנו עוברים לצורה שבה המרחב נראה ע"פ הבסיס המורכב מעמודות P, מפעילים שם את B וחוזרים חזרה. ניתן לראות את האינטואיציה הזו בצורה ברורה בחבורה הדיהדרלית, לדוגמה ב-D_3 מתקיים $\sigma\tau\sigma^{-1}=\tau\sigma$ - סובבנו את ציר השיקוף ע"פ σ!

הגדרה 3.7. תהיינה $H,K\leqslant G$ תתי-חבורות, נאמר ש-H ו-K צמודות זו לזו אם קיים $g\in G$ כך ש-$H=gKg^{-1}$ (וממילא גם $K=g^{-1}Hg$).

למה 3.8. G פועלת על עצמה ועל אוסף תתי-החבורות שלה ע"י הצמדה.

הגדרה 3.9. אנחנו נראה בקובץ הטענות שהמסלולים של איברים בקבוצה תחת פעולת חבורה הם מחלקות שקילות, המסלולים תחת פעולת ההצמדה נקראים מחלקות הצמידות של G ושני איברים בחבורה ייקראו צמודים אם הם שייכים לאותה מחלקת צמידות.

הגדרה 3.10. המְרַכֵּז והמְשַׁמֵּר
תהא $H\leqslant G$ תת-חבורה.

- המייצב של איבר $x\in G$ תחת פעולת ההצמדה באיברים מ-H נקרא גם המרכז (או הרכז) של x ומסומן ב-$C_H(x)$, כלומר (לכל $x\in G$):

$$C_H(x):=\left\{h\in H\mid hxh^{-1}=x\right\}$$

- המרכז (או הרכז) של תת-חבורה $K\leqslant G$ תחת הצמדה ב-H הוא:

$$C_H(K):=\left\{h\in H\mid \forall k\in K\ \ hkh^{-1}=k\right\}$$

- המייצב של תת-חבורה $K\leqslant G$ תחת פעולת ההצמדה באיברים מ-H נקרא גם המשמר (או המנרמל) ומסומן ב-$N_H(K)$, כלומר (לכל $K\leqslant G$):

$$N_H(K):=\left\{h\in H\mid hKh^{-1}=K\right\}$$

מסקנה 3.11. לכל שתי תתי-חבורות $H,K\leqslant G$ מתקיים $C_H(K)\leqslant N_H(K)$.

[9] אורי סימן גם ^{g}x - אני לא אשתמש בסימון הזה כאן.

4 הומומורפיזמים

תהיינה G ו-H שתי חבורות.

הגדרה 4.1. נאמר שפונקציה $\varphi:G\to H$ היא <u>הומומורפיזם</u> אם לכל $g_1,g_2\in G$ מתקיים $\varphi\left(g_1\cdot g_2\right)=\varphi\left(g_1\right)\cdot\varphi\left(g_2\right)$; קבוצת ההומומורפיזמים מ-G ל-H מסומנת ב-$\mathrm{Hom}\left(G,H\right)$.

הגדרה 4.2. הפונקציה המעתיקה את כל איברי G לאיבר היחידה של H היא הומומורפיזם[10], הומומורפיזם זה נקרא <u>ההומומורפיזם הטריוויאלי</u>.

הגדרה 4.3. יהי $\varphi:G\to H$ הומומורפיזם.

- נאמר ש-φ הוא <u>מונומורפיזם</u> (או <u>שיכון</u>) אם הוא חח"ע, ובמקרה כזה נסמן גם $\varphi:G\hookrightarrow H$.
- נאמר ש-φ הוא <u>אפימורפיזם</u> (ביחס ל-H[11]) אם הוא על ובמקרה כזה נסמן גם $\varphi:G\twoheadrightarrow H$.
- נאמר ש-φ הוא <u>איזומורפיזם</u> (ביחס ל-H) אם הוא חח"ע על ובמקרה כזה נסמן גם $\varphi:G\xrightarrow{\sim}H$.
- נאמר ש-φ הוא <u>אנדומורפיזם</u> אם $G=H$, קבוצת האנדומורפיזמים של G מסומנת ב-$\mathrm{End}\left(G\right)$.
- נאמר ש-φ הוא <u>אוטומורפיזם</u> אם הוא חח"ע ועל ובנוסף $G=H$[12], קבוצת האוטומורפיזם של G מסומנת ב-$\mathrm{Aut}\left(G\right)$.

הגדרה 4.4. יהי $\varphi:G\to H$ הומומורפיזם, <u>הגרעין</u> של φ הוא הקבוצה:

$$\ker\varphi:=\left\{g\in G:\varphi\left(g\right)=e_H\right\}$$

כלומר קבוצת כל האיברים ב-G ש-φ מעתיק לאיבר היחידה של H.

דוגמאות להומומורפיזמים

- פונקציית הדטרמיננטה $\det:\mathrm{GL}_n\left(\mathbb{F}\right)\to\mathbb{F}^{\times}$ היא אפימורפיזם.
- פונקציית העקבה $\mathrm{tr}:M_n\left(\mathbb{F}\right)\to\mathbb{F}^{+}$ היא אפימורפיזם.
- הפונקציה $f:\mathbb{R}\to\mathbb{C}^*$ המוגדרת ע"י $f\left(\theta\right):=\mathrm{cis}\left(\theta\right)$ היא הומומורפיזם (ואפימורפיזם ביחס ל-$\mathcal{S}^1$).

טענה 4.5. הפונקציה ההופכית של איזומורפיזם גם היא איזומורפיזם.

טענה. הרכבה של הומומורפיזמים היא הומומורפיזם, והרכבה של איזומורפיזמים היא איזומורפיזם.

הגדרה 4.6. נאמר ש-G ו-H <u>איזומורפיות</u> זו לזו אם קיים איזומורפיזם $\varphi:G\to H$, ובמקרה כזה נסמן $G\cong H$ (איזומורפיות הוא יחס שקילות).

הגדרה 4.7. תהא $K\leqslant G$ תת-חבורה, <u>הליבה</u> של K היא הקבוצה:

$$\mathrm{Core}_G\left(K\right):=\bigcap_{g\in G}gKg^{-1}$$

כלומר הליבה היא החיתוך של כל תתי-החבורות הצמודות ל-K.

---

[10] בפרט $\mathrm{Hom}\left(G,H\right)\neq\emptyset$, כלומר קיים הומומורפיזם מ-G ל-H.

[11] אנחנו נראה בקובץ הטענות שהתמונה של כל הומומורפיזם היא תת-חבורה של הטווח ולכן φ הוא אפימורפיזם ביחס ל-$\mathrm{Im}\varphi$.

[12] כלומר אם φ הוא איזומורפיזם ואנדומורפיזם.

דוגמאות לחבורות איזומורפיות

- לכל שתי קבוצות סופיות[13] X ו-Y כך ש-$|X|=|Y|$ מתקיים $S_X\cong S_Y$, כלומר חבורת התמורות על X איזומורפית לחבורת התמורות על Y.
- מתקיים $\mathrm{GL}_2\left(\mathbb{F}_2\right)\cong S_3\cong D_3$.[14]
- מתקיים $\left(\mathbb{R}_{>0},\cdot\right)\cong\left(\mathbb{R},+\right)$ - $\exp$ או כל פונקציה מעריכית אחרת מהוות איזומורפיזמים.
- מתקיים $\left(\mathbb{Z}\left[x\right],+\right)\cong\left(\mathbb{Q}_{>0},\cdot\right)$ - נעתיק כל מספר רציונלי $q\in\mathbb{Q}_{>0}$ לפולינום שהמקדם ה-n שלו הוא $\left|q\right|_{p_n}$[15] כאשר $\left(p_n\right)_{n=0}^{\infty}$ היא סדרת הראשוניים.
- כל הצמדה באיבר נתון בחבורה היא אוטומורפיזם על החבורה, אוטומורפיזמים המתקבלים ע"י הצמדה באיבר נתון נקראים <u>אוטומורפיזמים פנימיים</u>, וקבוצת האוטומורפיזמים הפנימיים של חבורה G מסומנת ב-$\mathrm{Inn}\left(G\right)$.
- נניח ש-G ציקלית, אם G אין-סופית אז $G\cong\mathbb{Z}$ ואם G סופית אז $G\cong\mathbb{Z}_{|G|}$.
- מתקיים $\mathrm{Aut}\left(\mathbb{Z}\right)\cong\mathbb{Z}^{\times}\cong\mathbb{Z}_2$.
- לכל $n\in\mathbb{N}$ מתקיים $\mathrm{Aut}\mathbb{Z}_n\cong\mathbb{Z}_n^{\times}$, האיזומורפיזם הוא העתקת איבר הפיך ב-$\mathbb{Z}_n$ לאוטומורפיזם שהוא מגדיר ע"י כפל, זה לא נכון בכל חוג - קיימים חוגים שבהם ישנם אוטומורפיזמים שאינם שקולים לכפל במספר הפיך בחוג (**דוגמה?**).

[13] למעשה הטענה נכונה גם עבור קבוצות שאינן סופיות שעוצמתן זהה.
[14] באופן דומה חבורות הסימטריות של הארבעון המשוכלל איזומורפית ל-S_4 וניתן להרחיב את התופעה לממדים גבוהים יותר.
[15] הנורמה ה-p-אדית של המספר הראשוני p_i.

5 חבורות מנה

הגדרה 5.1. פונקציית ההטלה של תת-חבורה

תהא G חבורה ותהא $H \leqslant G$ תת-חבורה, פונקציית ההטלה של H היא הפונקציה $\pi : G \to {}^{G}/_{H}$ המוגדרת ע"י (לכל $g \in G$):

$$\pi\left(g\right) := gH$$

♣ פונקציית ההטלה נקראת כך בגלל האינטואיציה ממרחבי מנה שבהם פעולתה היא להטיל כל וקטור במרחב על התמ"ו היוצר את מרחב המנה, גם בחבורות ניתן לראות פעולה דומה ובאלו שיש להן אינטואיציה גאומטרית הפעולה נראית דומה מאד להטלה ב-$\mathbb{R}^3$.

טענה. תהא G חבורה, תהא $N \leqslant G$ תת-חבורה ותהא $\pi : G \to {}^{G}/_{N}$ פונקציית ההטלה של N.
אם N נורמלית אז ניתן להגדיר על ${}^{G}/_{N}$ מבנה של חבורה[16] ע"י (לכל $g, h \in G$):

$$\left(gN\right) \cdot \left(hN\right) := ghN$$

בנוסף, ניתן להגדיר על ${}^{G}/_{N}$ מבנה של חבורה כך ש-π היא הומומורפיזם אם"ם N נורמלית, ובמקרה כזה קיימת דרך יחידה להגדיר על ${}^{G}/_{N}$ מבנה של חבורה כך ש-π הומומורפיזם והיא הדרך שהוזכרה לעיל.

הגדרה 5.2. חבורת המנה של תת-חבורה

תהא G חבורה ותהא $N \trianglelefteq G$ תת-חבורה נורמלית, חבורת המנה ${}^{G}/_{N}$ היא אותה חבורה יחידה שעבורה פונקציית ההטלה של N היא הומומורפיזם.

♣ פעמים רבות קוראים לחבורה ${}^{G}/_{N}$ "G מודולו N" ולא בכדי: האינטואיציה הראשונה במעלה לחבורות מנה נובעת מהחוגים המודולריים המקיימים ${}^{\mathbb{Z}}/_{n\mathbb{Z}} \cong \mathbb{Z}_n$.

♣ עבור תת-חבורה נורמלית פונקציית ההטלה נקראת גם הומומורפיזם ההטלה הקנוני.

♣ מהגדרה מתקיים $\left|{}^{G}/_{N}\right| = \left[G : N\right]$ ולכן ע"פ משפט לגראנז' אם G סופית אז גם:

$$\left|{}^{G}/_{N}\right| = \frac{\left|G\right|}{\left|N\right|}$$

כלומר הסדר של חבורת המנה הוא מנת הסדרים של החבורה ותת-החבורה הנורמלית.

טענה. לכל חבורה G מתקיים $\text{Inn}\left(G\right) \trianglelefteq \text{Aut}\left(G\right)$.

הגדרה 5.3. תהא G חבורה, חבורת המנה ${}^{\text{Aut}(G)}/_{\text{Inn}(G)}$ נקראת חבורת האוטומורפיזמים החיצוניים של G ומסומנת ב-$\text{Out}\left(G\right)$.

♣ לא להתבלבל, $\text{Inn}\left(G\right)$ היא תת-חבורה של $\text{Aut}\left(G\right)$ אבל $\text{Out}\left(G\right)$ אינה תת-חבורה של $\text{Aut}\left(G\right)$, היא אפילו לא מוכלת בה - האיברים של $\text{Out}\left(G\right)$ הם מחלקות של $\text{Inn}\left(G\right)$.

[16] כלומר קיימת פעולה $\cdot : {}^{G}/_{N} \times {}^{G}/_{N} \to {}^{G}/_{N}$ המקיימת את שלוש התכונות הנדרשות מכפל של חבורה.

6 חבורות p ומשפטי סילו

הגדרה 6.1. תהא G חבורה סופית ויהי $p\in\mathbb{N}$ ראשוני, נאמר ש-G היא חבורת p אם קיים $r\in\mathbb{N}$ כך ש-$|G|=p^r$.

סימון: לכל $0\neq n\in\mathbb{Z}$ ולכל $p\in\mathbb{Z}$ ראשוני נסמן $\mathrm{Ord}_p(n):=\max\{e\in\mathbb{N}_0:p^e\mid n\}$.

לא ראינו את הסימון בכיתה אך זהו סימון מקובל והוא יהיה נוח בהמשך.

הגדרה 6.2. חבורת p סילו[17]

תהא G חבורה סופית ויהי $p\in\mathbb{N}$ ראשוני, נאמר שתת-חבורה $H\leqslant G$ היא חבורת-p-סילו של G אם מתקיים:

$$|H|=p^{\mathrm{Ord}_p(|G|)}$$

סימון: עבור $p\in\mathbb{N}$ ראשוני וחבורה סופית G נסמן ב-$\mathrm{Syl}_p(G)$ את קבוצת חבורות p-סילו של G.

7 פירוק לחבורות פשוטות

תהא G חבורה.

הגדרה 7.1. חבורה פשוטה

חבורה G תיקרא פשוטה אם $G\neq\{e\}$ ואין לה תתי-חבורות נורמליות לא טריוויאליות.

- ♣ כפי שראינו בפרק 6 (חבורות מנה), אם לחבורה G יש תת-חבורה נורמלית ניתן להתבונן בחבורת המנה שלה וכך "לפרק" את G לשתי חבורות קטנות יותר; רעיון זה גורם לנו לרצות להבין את כל החבורות הפשוטות וכיצד הן מתחברות ליצירת חבורות מורכבות יותר. בעניין הראשון הצליחה האנושות להשביע את רעבונה: במאה ה-20 ישבו מתמטיקאים רבים והצליחו למיין את מרבית החבורות הפשוטות הסופיות[18], רק ב-2004 הסתיימה העבודה והוכח משפט המיון, לעומת זאת הבעיה השנייה עומדת על כנה: נכון לכתיבת שורות אלה אין בנמצא משפט הקובע כיצד ניתן להרכיב חבורות פשוטות לכדי יצירת חבורה גדולה יותר באופן כללי.
- ♣ החבורה הטריוויאלית ($\{e\}$) אינה נחשבת חבורה פשוטה מאותה סיבה ש-1 אינו נחשב מספר ראשוני: הצגה של 360 כ-$1\cdot 2^3\cdot 3^2\cdot 5$ במקום כ-$2^3\cdot 3^2\cdot 5$ אינה תורמת לנו מאומה בהבנתו, כמותו החבורה הטריוויאלית אינה נחשבת פשוטה משום שהיא אינה עוזרת לנו להבין חבורות מורכבות יותר. הדמיון של פירוק חבורות לפירוק מספרים מסתיים כאן: בעוד שיש רק דרך אחת להרכיב ממספרים ראשוניים מספר גדול יותר, ישנן דרכים רבות להרכיב חבורה גדולה מחבורות פשוטות, הדבר דומה יותר להרכבה של אטומים לכדי יצירת מולקולות - ישנן מולקולות הנוצרות מאותו מספר של אטומים מכל יסוד אך הן שונות לחלוטין[19].
- ♣ כבר בתחילת הקורס ראינו שבהינתן מספר סופי של חבורות ניתן להתבונן בחבורת המכפלה הישרה שלהן שבה הכפל מתבצע קואורדינטה קואורדינטה ללא שום קשר בין החבורות השונות; בקרוב נראה דרך נוספת להרכיב משתי חבורות חבורה גדולה יותר שהיא המכפלה הישרה למחצה, דרך זו מערבבת בין שתי הקואורדינטות בצורה מסוימת אך כמובן שישנן דרכים רבות אחרות לעשות זאת.

דוגמה 7.2. הדוגמאות הכי פשוטות לחבורות פשוטות[20] הן החבורות מהצורה $\mathbb{Z}_p$ עבור p ראשוני, אין להן תתי-חבורות לא טריוויאליות בכלל.

[17] ערך בוויקיפדיה: לודוויג סילו
[18] נראה שלעולם לא נצליח למיין את כל החבורות הפשוטות האין-סופיות, יש יותר מדי מהן...
[19] את המשל הזה הביא אורי ביעור והוא אף הביא דוגמה לכך אלא שאיני זוכר אותה, הדוגמה שמופיעה בוויקיפדיה (בערך "מולקולה") היא אתנול ודימתיל אתר.
[20] שימו לב לכפל המשמעות במילה "פשוטות".

7.1 מכפלה ישרה ומכפלה ישרה למחצה

למה 7.3. תהיינה $H,K\leqslant G$ תתי-חבורות ותהא $f:H\times K\to G$ הפונקציה המוגדרת ע"י $f\left(h,k\right):=hk$ לכל $(h,k)\in H\times K$.
f היא איזומורפיזם אם"ם מתקיימים שלושת התנאים הבאים:

1. $HK=G$.
2. $H\cap K=\{e\}$.
3. $H,K\trianglelefteq G$.

הגדרה 7.4. מכפלה ישרה פנימית
נאמר ש-G היא מכפלה ישרה פנימית של תתי-חבורות נורמליות $H,K\trianglelefteq G$ אם מתקיימים שלושת התנאים הבאים:

1. $HK=G$.
2. $H\cap K=\{e\}$.
3. $H,K\trianglelefteq G$.

ובמקרה כזה נכתוב $G=H\times K$.[21]

- ♣ אם $G\cong H\times K$ כאשר H ו-K אינן תתי-חבורות של G נאמר ש-G היא מכפלה ישרה חיצונית של H ו-K, גם במקרה זה נכתוב $G=H\times K$ למרות שמדובר באיזומורפיזם בלבד, וזאת משום שקיימות תתי-חבורות נורמליות $\tilde{H},\tilde{K}\trianglelefteq G$ כך ש-$\tilde{H}\cong H$ ו-$\tilde{K}\cong K$.[22]
- ♣ דוגמה למכפלה ישרה פנימית $\mathbb{C}^{*}=\mathbb{R}_{>0}\times S^{1}$ כאשר: $\mathbb{C}^{*}$ היא החבורה הכפלית של המרוכבים, $\mathbb{R}_{>0}$ היא קבוצת המספרים הממשיים החיוביים ו-S^{1} הוא מעגל היחידה המרוכב.
דוגמה זו היא פשוט המספרים המרוכבים בקואורדינטות קוטביות, וכך צריך לחשוב על כל המכפלות הישרות - כקואורדינטות.

[21] למעשה לא מדובר בשוויון אלא באיזומורפיזם, אבל בגלל שלכולנו ברור באיזה איזומורפיזם מדובר נוכל להשתמש בשוויון מבלי לוותר על הבהירות.
[22] הדרך למצוא את אותן תתי-חבורות נורמליות היא לקחת איזומורפיזם בין $H\times K$ ל-G ולבדוק לאן הוא מעתיק את $H\times\{e_K\}$ ו-$\{e_H\}\times K$ שהן תתי-חבורות נורמליות של $H\times K$.

הגדרה 7.5. מכפלה ישרה למחצה פנימית

נאמר ש-G היא מכפלה ישרה למחצה פנימית של תתי-חבורות $H,K\leqslant G$ אם מתקיימים שלושת התנאים הבאים:

1. $HK=G$.
2. $H\cap K=\{e\}$.
3. $H\trianglelefteq G$.

ובמקרה כזה נכתוב $G=H\rtimes K$.[23]

♣ לכל $g\in G$ קיימים $h\in H$ ו-$k\in K$ יחידים כך ש-$g=hk$,[24] וכך הכפל בחבורה $H\rtimes K$ מוגדר באופן הבא (לכל $h,h'\in H$ ולכל $k,k'\in K$):

$$hk\cdot h'k'=hkh'k^{-1}\cdot kk'$$

זוהי שוב הצגה כמכפלה של איבר ב-H עם איבר ב-K משום ש-$kh'k^{-1}\in H$ (כי $H\trianglelefteq G$).
בצורה זו נוכל להגדיר מבנה של חבורה על **הקבוצה** $H\times K$ ע"י (לכל $(h,k),(h',k')\in H\times K$):

$$(h,k)\cdot(h',k'):=\left(hkh'k^{-1},kk'\right)$$

נזהה את החבורה הזו עם החבורה $H\rtimes K$.

♣ איבר היחידה ב-$H\rtimes K$ הוא עדיין (e,e), אבל ההופכי של איבר $(h,k)\in H\rtimes K$ הוא $\left(k^{-1}h^{-1}k,k^{-1}\right)$ שכן:

$$(h,k)\cdot\left(k^{-1}h^{-1}k,k^{-1}\right)=\left(hk\cdot k^{-1}h^{-1}k\cdot k^{-1},kk^{-1}\right)=\left(e_H,e_K\right)$$

♣ כל מכפלה ישרה פנימית היא מכפלה ישרה למחצה פנימית.

♣ בהגדרה הנ"ל יש בעיה מעשית: הסיבה היחידה לכך שידענו כיצד לכפול איברים ב-G, כשהם נתונים כמכפלה של איבר ב-H עם איבר ב-K, היא שהכרנו את G מראש וידענו לומר מיהו $kh'k^{-1}$. מה נעשה בהינתן שלוש חבורות G, H ו-K, כך שקיימות תתי-חבורות $\tilde{H},\tilde{K}\leqslant G$ המקיימות $G=\tilde{H}\rtimes\tilde{K}$ ובנוסף $H\cong\tilde{H}$ ו-$K\cong\tilde{K}$? הידע שלנו אודות H ו-K לא יספיק כדי לקבוע כיצד עובד הכפל ב-G, לדוגמה:

$$\mathbb{Z}_3\cong\langle\sigma\rangle\qquad\mathbb{Z}_6=\mathbb{Z}_3\rtimes\mathbb{Z}_2$$
$$\mathbb{Z}_2\cong\langle\tau\rangle\qquad D_3=\langle\sigma\rangle\rtimes\langle\tau\rangle$$

וזאת למרות ש-$D_3\ncong\mathbb{Z}_6$. מהנוסחה שראינו לעיל לכפל במכפלה ישרה למחצה נובע שהשוני בין החבורות מראה שההצמדה שלהן שונה, ואכן בעוד שב-$\mathbb{Z}_6$ הצמדה פועלת כמו הזהות ב-D_3 הצמדה של סיבוב בשיקוף מעתיקה אותו אל ההופכי שלו.

משפט. תהיינה H ו-K שתי חבורות, ונסמן $\tilde{H}:=H\times\{e_K\}$ ו-$\tilde{K}=\{e_H\}\times K$.
לכל פעולה דו-מקומית "$*$" המוגדרת על $H\times K$ מתקיים $(H\times K,*)=\tilde{H}\rtimes\tilde{K}$[25] אם"ם קיים הומומורפיזם $\phi:K\to\operatorname{Aut}(H)$ כך שלכל $(h,k),(h',k')\in H\times K$ מתקיים:[26]

$$(h,k)*(h',k')=\left(h\cdot\phi_k\left(h'\right),k\cdot k'\right)$$

---

[23] הסימון אינו סימטרי משום שיש הבדל בין H ל-k: H נורמלית, לי עוזר לזכור שהמשולש הסגור מצביע על H כמו $H\trianglelefteq G$.
[24] הקיום נובע מהעובדה ש-$G=HK$ והיחידות מהנתון $H\cap K=\{e\}$.
[25] כלומר הזוג הסדור $(H\times K,*)$ הוא חבורה, ובנוסף זוהי החבורה $\tilde{H}\rtimes\tilde{K}$.
[26] ϕ_k הוא האוטומורפיזם ב-$\operatorname{Aut}(H)$ שאליו מעתיק ϕ את k.

הגדרה 7.6. מכפלה ישרה למחצה חיצונית

תהיינה H ו-K שתי חבורות, לכל הומומורפיזם $\phi : K \to \mathrm{Aut}\left(H\right)$ נסמן ב-$H \rtimes_{\phi} K$ את החבורה $\left(H \times K, *\right)$ המוגדרת ע"י (לכל $\left(h,k\right),\left(h',k'\right) \in H \times K$):

$$\left(h,k\right) * \left(h',k'\right) := \left(h \cdot \phi_k\left(h'\right), k \cdot k'\right)$$

כל חבורה כזו תיקרא מכפלה ישרה למחצה של H ו-K.

- ♣ מהגדרה קיימות תתי-חבורות $\tilde{H},\tilde{K} \leqslant H \rtimes_{\phi} K$ כך ש-$\tilde{H} \cong H$ ו-$\tilde{K} \cong K$ המקיימות $H \rtimes_{\phi} K = \tilde{H} \rtimes \tilde{K}$, אלו הן:

$$\tilde{H} := H \times \{e_K\} \qquad \tilde{K} := \{e_H\} \times K$$

בפרט H איזומורפית לתת-חבורה נורמלית של $H \rtimes_{\phi} K$.

- ♣ איבר היחידה הוא עדיין $\left(e_H, e_K\right)$, אבל האיבר ההופכי של איבר $\left(h,k\right) \in H \rtimes_{\phi} K$ הוא $\left(\phi_{k^{-1}}\left(h^{-1}\right), k^{-1}\right)$ שכן (נזכור ש-ϕ הוא הומומורפיזם ולכן $\phi_{k^{-1}} \circ \phi_k = \phi_e = \mathrm{Id}$):

$$\left(h,k\right) * \left(\phi_{k^{-1}}\left(h^{-1}\right), k^{-1}\right) = \left(h \cdot \phi_k\left(\phi_{k^{-1}}\left(h^{-1}\right)\right), k \cdot k^{-1}\right) = \left(hh^{-1}, kk^{-1}\right) = \left(e_H, e_K\right)$$

- ♣ מכפלה ישרה $H \rtimes_{\phi} K$ למחצה היא אבלית אם"ם $\phi_k = \mathrm{Id}_H$ לכל $k \in K$, כלומר אם"ם ϕ הוא ההומומורפיזם הטריוויאלי.

מסקנה 7.7. תהיינה $H,K \leqslant G$ תתי-חבורות כך ש-$G = H \rtimes K$, ויהי $\varphi : K \to \mathrm{Aut}\left(H\right)$ הומומורפיזם ההצמדה, כלומר לכל $h \in H$ ולכל $k \in K$ מתקיים $\varphi_k\left(h\right) = khk^{-1}$.
במקרה כזה מתקיים $G = H \rtimes_{\varphi} K$.

הגדרה 7.8. ההולומורף של חבורה G הוא המכפלה הישרה למחצה $\mathrm{Hol}\left(G\right) := G \rtimes_{\mathrm{Id}} \mathrm{Aut}\left(G\right)$.

7.2 סדרות נורמליות וסדרות הרכב

הגדרה 7.9. סדרה נורמלית

נאמר שסדרה סופית של תתי-חבורות $\left(G_0, G_1, \ldots, G_r\right)$ היא סדרה נורמלית של G אם מתקיימים שלושת התנאים הבאים[27]:

1. $G_0 = G$
2. $G_r = \{e\}$
3. לכל $r > i \in \mathbb{N}_0$ מתקיים $G_{i+1} \trianglelefteq G_i$

נאמר שסדרה נורמלית $\left(H_0, H_1, \ldots, H_s\right)$ של G היא עידון של סדרה נורמלית $\left(G_0, G_1, \ldots, G_r\right)$ אם קיימת סדרה עולה ממש $\left(k_0, k_1, \ldots, k_r\right)$ כך ש-$k_0 = 0$, $k_r = s$ ו-$H_{k_i} = G_i$ לכל $r \geq i \in \mathbb{N}_0$, כלומר הסדרה $\left(H_0, H_1, \ldots, H_s\right)$ כוללת את כל איברי $\left(G_0, G_1, \ldots, G_r\right)$ באותו סדר כשביניהם יכולים להיות איברים נוספים.

הגדרה 7.10. סדרת הרכב

נאמר שסדרה נורמלית $\left(G_0, G_1, \ldots, G_r\right)$ של G היא סדרת הרכב שלה אם לכל $r > i \in \mathbb{N}_0$ מתקיימים שני התנאים הבאים:

1. $G_{i+1} \neq G_i$
2. לא קיימת תת-חבורה $H \leqslant G$ המקיימת $G_{i+1} \trianglelefteq H \trianglelefteq G_i$ וגם $G_{i+1} \neq H \neq G_i$

כלומר סדרת הרכבה היא סדרה נורמלית ללא חזרות וללא יכולת לעדן אותה מבלי להוסיף חזרות.

הגדרה 7.11. הגורמים של סדרה נורמלית $\left(G_0, G_1, \ldots, G_r\right)$ שלה הם כל חבורות המנה מהצורה ${G_i}/{G_{i+1}}$ עבור $r > i \in \mathbb{N}_0$, כשמדובר בסדרת הרכב הם נקראים גם גורמי ההרכב של הסדרה.

[27] במקומות אחרים מסדרים את הסדרה בסדר הפוך, כלומר $G_0 = \{e\}$, $G_r = G$ ו-$G_i \trianglelefteq G_{i+1}$ לכל $r > i \in \mathbb{N}_0$.

7.3 חבורות פתירות

הגדרה 7.12. חבורה פתירה

נאמר ש-G היא חבורה פתירה אם יש לה סדרה נורמלית בעלת גורמים אבליים.

♣ כעת ניתן לפתוח צוהר אל הכיוון שאליו אנו שואפים להגיע שהוא פתרון משוואות פולינומיאליות: כולנו זוכרים את נוסחת השורשים מהתיכון ויודעים כיצד לפתור משוואה ממעלה שנייה, אך מה בדבר משוואות ממעלה גבוהה יותר? התשובה המפתיעה היא שיש נוסחה מפורשת לפתרון משוואות ממעלה 3 ו-4 אך אין וגם לא תהיה נוסחה לפתרון משוואות ממעלה גבוהה יותר, הסיבה לכך נעוצה במשפט שלא נוכיח כעת:

משפט. יהי $p\in\mathbb{Q}[x]$ פולינום ממעלה n ויהיו $a_1,a_2,\ldots,a_n\in\mathbb{C}$ כך ש-$f(a_k)=0_{\mathbb{C}}$ לכל $n\geq k\in\mathbb{N}$ (ע"פ המשפט היסודי של האלגברה אכן קיימים $a_1,a_2,\ldots,a_n$ כאלה).
נסמן ב-$\mathbb{Q}(a_1,a_2,\ldots,a_n)$ את תת-השדה המינימלי של $\mathbb{C}$ (ביחס להכלה) כך ש-$a_1,a_2,\ldots,a_n\in\mathbb{Q}(a_1,a_2,\ldots,a_n)$ (מהגדרה $\mathbb{Q}\subseteq\mathbb{Q}(a_1,a_2,\ldots,a_n)$).
ניתן לבטא את $a_1,a_2,\ldots,a_n$ באמצעות חיבור, חיסור, כפל וחילוק של מספרים רציונליים יחד עם הוצאת שורש מסדר טבעי אם"ם החבורה $\mathrm{Aut}(\mathbb{Q}(a_1,a_2,\ldots,a_n))$[28] פתירה.

כפי שראינו כשעסקנו בחבורת התמורות (בקובץ "חבורות חשובות"), לכל $4<n\in\mathbb{N}$ החבורה A_n היא פשוטה ולא אבלית, כלומר A_n ו-S_n אינן פתירות, העבודה הזו גוררת באמצעות המשפט הנ"ל שלמשוואות פולינומיאליות ממעלה חמישית ואילך אין "נוסחת שורשים".

♣ למעשה הניסוח שלעיל הוא צל חיוור של המשפט האמיתי של גלואה[29], המשפט האמיתי מדבר על פולינום מעל שדה כלשהו ועל שדה ההרחבה שלו (פירוט בהמשך), אך אותו לא אוכל להביא כאן מבלי להידרש לכמה הקדמות ארוכות שאותן נלמד במבנים 2. למרות זאת פטור בלא כלום אי אפשר ולכן אנסה לתת כאן טעימה: בהינתן פולינום חסר שורשים מעל שדה ניתן להרחיב את השדה לכדי שדה גדול יותר שבו הפולינום הופך לפריק, כך למשל $\mathbb{C}$ הוא שדה ההרחבה של הפולינום x^2+1 ו-$\mathbb{Q}(\sqrt{2}):=\left\{a+b\cdot\sqrt{2}\mid a,b\in\mathbb{Q}\right\}$ הוא שדה ההרחבה של הפולינום x^2-2. המשפט של גלואה אומר שעבור שדה $\mathbb{F}$ ופולינום $p\in\mathbb{F}[x]$ ניתן להציג את שורשי הפולינום p באמצעות חיבור, חיסור, כפל, חילוק והוצאות שורש[30] של איברים ב-$\mathbb{F}$ אם"ם חבורת האוטומורפיזמים של שדה ההרחבה המתאים היא חבורה פתירה.

---

[28] אוטומורפיזם מעל שדה הוא פונקציה חח"ע ועל השומרת הן על החיבור והן על הכפל.

[29] ערך בוויקיפדיה: אווריסט גלואה.

[30] הכוונה בהוצאת שורש n-י של איבר $a\in\mathbb{F}$ היא מציאת איבר $b\in\mathbb{F}$ כך ש-$b^n=a$, כמובן שגם $-b$ ואולי גם איברים אחרים יקיימו זאת ואין סיבה להעדיף אחד מהם על פני האחרים.

7.4 החבורה הנגזרת

הגדרה 7.13. קומוטטור (מחליפן)

יהיו $g,h\in G$, הקומוטטור (או המחליפן) של g ו-h הוא $[g,h]:=ghg^{-1}h^{-1}$[31].

♣ מהגדרה מתקיים $[g,h]\cdot hg=gh$ לכל $g,h\in G$, כלומר הקומוטטור מחליף את הסדר של האיברים וזו הסיבה לשמו.

מסקנה 7.14. לכל $g,h\in G$ מתקיימים שני הפסוקים הבאים:

1. $gh=hg\iff[g,h]=e$.
2. $[g,h]^{-1}=[h,g]$.

הגדרה 7.15. החבורה הנגזרת (חבורת הקומוטטורים)

החבורה הנגזרת (או חבורת הקומוטטורים) של G היא החבורה $G':=\langle\{[g,h]:g,h\in G\}\rangle$, כלומר זוהי החבורה הנוצרת ע"י קבוצת הקומוטטורים.

♣ החבורה הנגזרת "מודדת" עד כמה G אבלית: ככל ש-G "יותר" אבלית כך קבוצת הקומוטטורים תהיה קטנה יותר וממילא גם חבורת הנגזרת תקטן.

הגדרה 7.16. הסדרה הנגזרת

הסדרה הנגזרת של G היא הסדרה $\left(G^{(n)}\right)_{n=0}^{\infty}$ המוגדרת ע"י $G^{(0)}:=G$ ו-$G^{(n+1)}:=\left(G^{(n)}\right)'$ לכל $n\in\mathbb{N}_0$.

7.5 חבורות נילפוטנטיות

♣ ההגדרה הבאה היא הגדרה אינדוקטיבית.

הגדרה 7.17. חבורות נילפוטנטיות

- נאמר ש-G היא חבורה נילפוטנטית ממחלקת נילפוטנטיות 0 אם $G=\{e\}$.
- לכל $n\in\mathbb{N}$ נאמר ש-G היא חבורה נילפוטנטית ממחלקת נילפוטנטיות n אם ${}^{G}/_{Z(G)}$ היא חבורה נילפוטנטית ממחלקת נילפוטנטיות $n-1$.

אם קיים n כך ש-G נילפוטנטית ממחלקת נילפוטנטיות n, נאמר גם ש-G נילפוטנטית סתם.

בכיתה קראנו לחבורה נילפוטנטית ממחלקת נילפוטנטיות n בשם "n-נילפוטנטית" אך אינני אוהב אותו מסיבות לשוניות.

♣ חבורות נילפוטנטיות הן חבורות "כמעט" אבליות, כדי שחבורה תהיה ממחלקת נילפוטנטיות 1 היא צריכה להיות אבלית, וכדי שתהיה ממחלקת נילפוטנטיות 2 חבורת המנה ${}^{G}/_{Z(G)}$ צריכה להיות אבלית וכן הלאה.

♣ מהגדרה חבורה נילפוטנטית ממחלקת נילפוטנטיות n היא גם ממחלקת נילפוטנטיות m לכל $n<m\in\mathbb{N}$.

---

[31] יש המגדירים להפך: $[g,h]:=g^{-1}h^{-1}gh$.

8 חבורות חופשיות

תהא S קבוצה.

הגדרה 8.1. מילה באיברי S היא מחרוזת[32] מהצורה $s_1^{\varepsilon_1}s_2^{\varepsilon_2}\ldots s_n^{\varepsilon_n}$ כאשר $n\in\mathbb{N}_0$ ולכל $n\geq i\in\mathbb{N}$ מתקיים $s_i\in S$ ו-$\varepsilon_i\in\{1,-1\}$.

- S היא סתם קבוצה ללא שום מבנה אלגברי, אני חושב שהכי נוח לדמיין ש-S היא קבוצה של קשקושים חסרי פשר - אותיות באל"ף-בי"ת שהמצאנו בזה הרגע (לדוגמה $S=\{\diamondsuit,\heartsuit,\triangle,\pentagon,\smiley\}$), ואז מילה ב-$S$ היא מחרוזת כגון:

$$\pentagon^1\heartsuit^1\diamondsuit^{-1}\diamondsuit^{-1}\diamondsuit^1\smiley^1\triangle^1 \qquad \diamondsuit^{-1}\heartsuit^1\triangle^{-1}\triangle^1\triangle^1\pentagon^1$$
$$\smiley^1\smiley^{-1}\smiley^1\triangle^1\heartsuit^1\heartsuit^1 \qquad \diamondsuit^1\heartsuit^1\heartsuit^{-1}\smiley^1\triangle^1\diamondsuit^1$$

- ה-1 וה--1 הם אותם 1 ו--1 שב-$\mathbb{Z}$ ולכן מתקיים $1=-(-1)$.
- שוויון מתמטי הוא זהות מוחלטת בין שתי המשמעויות של הסימונים משני עבריו, כשמדובר במחרוזות כאלה הן צריכות להיות זהות בכל תו, בפרט $\triangle^1\neq\heartsuit^1\heartsuit^{-1}\triangle^1$.
- שימו לב לכך ש-n עלול להיות 0, במקרה כזה מדובר במילה הריקה וכדי שיהיה ברור היכן היא מופיעה והיכן היא אינה מופיעה אנחנו נסמן אותה ב-$\emptyset$, ב-$()$ או ב-"".

סימון: נסמן $S^{-1}:=\left\{s^{-1}\mid s\in S\right\}$[33].

סימון: לכל $s\in S$ נסמן $s:=s^1$, כלומר אם במחרוזת מופיע s^1 נזהה אותה עם מחרוזת דומה שבה מופיע s באותו מקום; כמו כן לכל $s\in S$ ולכל $k\in\mathbb{N}_0$ נסמן[34]:

$$s^{-k}:=\overbrace{s^{-1}s^{-1}\ldots s^{-1}}^{k\text{ פעמים}} \qquad s^k:=\overbrace{ss\ldots s}^{k\text{ פעמים}}$$

מהגדרה s^0 היא המילה הריקה לכל $s\in S$.

הגדרה 8.2. מילה באיברי S תיקרא מצומצמת אם לכל $s\in S$ אין בה מופעים של ss^{-1} ו/או $s^{-1}s$[35].

הגדרה 8.3. צמצום של מילה באיברי S הוא מחיקת כל המופעים מהצורה ss^{-1} ו/או $s^{-1}s$ עבור כל $s\in S$, וחזרה על פעולה זו עד שאין מופעים כאלה.

דוגמה 8.4. הצמצום של המילה $\diamondsuit^{-1}\heartsuit\triangle^{-1}\triangle\heartsuit^{-1}\pentagon$ הוא $\diamondsuit^{-1}\pentagon$ מפני שתחילה נמחק המופע $\triangle^{-1}\triangle$ ומתקבלת המילה $\diamondsuit^{-1}\heartsuit\heartsuit^{-1}\pentagon$, ולאחר מכן נמחק המופע $\heartsuit\heartsuit^{-1}$ ומתקבלת המילה $\diamondsuit^{-1}\pentagon$.

- המילה $\diamondsuit^{-1}\heartsuit\triangle^{-1}\triangle\heartsuit^{-1}\pentagon$ **אינה שווה** למילה $\diamondsuit^{-1}\pentagon$, מה שכן ניתן לומר הוא שהצמצום מגדיר יחס שקילות על המילים באיברי S: שתי מילים באיברי S הן שקולות אם"ם הצמצומים שלהן שווים.

סימון: נסמן ב-$F(S)$ את קבוצת המילים המצומצמות באיברי S.

הגדרה 8.5. הכפל של שתי מילים ב-$F(S)$ יוגדר ע"י שרשור המילים זו לזו ולאחר מכן צמצום של המילה המשורשרת.

מסקנה 8.6. $F(S)$, עם פעולת הכפל הנ"ל היא חבורה.

---

[32] מי שרוצה להיות ממש פורמלי ולא מוכן לקבל את האובייקט החדש מוזמן להשתמש בסדרות של איברים ב-S אם תוספת של ±1 מעליהם.
[33] נקודת המבט על S כקבוצה של קשקושים חסרי פשר פותרת את השאלה **הפילוסופית** "מי אמר ש-S^{-1} קיימת?", התשובה היא שקל מאוד לראות שהיא קיימת: נקשקש -1 מעל הקשקושים של S ונקבל את S^{-1}.
[34] נשים לב שאין כל בעיה בסימון: המשמעויות של s^1 ו-s^{-1} נותרו על כנן גם בסימון זה.
[35] ושוב מי שרוצה להיות פורמליסט חסר תקנה מוזמן לומר שבסדרה המהווה את המילה אין שני איברים סמוכים מצורה זו.

משפט. התכונה האוניברסלית
תהא G חבורה, לכל פונקציה $f:S\to G$ קיים הומומורפיזם יחיד $\tilde{f}:F\left(S\right)\to G$ כך ש-$\tilde{f}\mid_{S}=f$.

משפט. תהא G חבורה, תהא $T\subseteq G$ תת-קבוצה ויהי $\varphi:F\left(T\right)\to G$ אותו הומומורפיזם יחיד כך ש-$\varphi\mid_{T}=\text{Id}_{T}$. שלושת הפסוקים הבאים שקולים זה לזה:

1. φ חח"ע ועל, כלומר φ הוא איזומורפיזם ובפרט מתקיים $G\cong F\left(T\right)$.
2. לכל $g\in G$ קיים $x\in F\left(T\right)$ יחיד כך ש-$g=\varphi\left(x\right)$, כלומר כל איבר ב-G ניתן להצגה באופן יחיד כמילה מצומצמת באיברי T.
3. לכל חבורה H ולכל פונקציה $f:T\to H$ קיים הומומורפיזם יחיד $\tilde{f}:G\to H$ כך ש-$\tilde{f}\mid_{T}=f$.

♣ הפסוק השלישי הוא המקבילה של המשפט שראינו בלינארית 1:

משפט. יהיו V ו-W מרחבים וקטוריים מעל לשדה $\mathbb{F}$ ונניח ש-V נ"ס; לכל $v_{1},v_{2},\ldots,v_{n}\in V$ כך ש-$\left(v_{1},v_{2},\ldots,v_{n}\right)$ הוא בסיס סדור של V, ולכל $w_{1},w_{2},\ldots,w_{n}\in W$, קיימת העתקה ליניארית $T:V\to W$ יחידה כך ש-$T\left(v_{i}\right)=w_{i}$ לכל $n\geq i\in\mathbb{N}$.

הגדרה 8.7. תהיינה G חבורה ו-$T\subseteq G$ תת-קבוצה, ויהי $\varphi:F\left(T\right)\to G$ אותו הומומורפיזם יחיד כך ש-$\varphi\mid_{T}=\text{Id}_{T}$. נאמר ש-$G$ היא חבורה חופשית עם בסיס T אם φ הוא איזומורפיזם.