תורת החבורות - טענות 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:
אקסיומות השלמות - סיכומי הרצאות במתמטיקה
https://srayaa.wixsite.com/math

1 התחלה

טענה 1.1. תהא A קבוצה לא ריקה שעליה מוגדרת פעולה דו-מקומית "$*$" בעלת איבר יחידה $e\in A$, כלומר לכל $a\in A$ מתקיים $a*e=a=e*a$. e הוא איבר היחידה היחיד, כלומר לכל $\tilde{e}\in A$ המקיים גם הוא $a*\tilde{e}=a=\tilde{e}*a$ לכל $a\in A$, מתקיים $\tilde{e}=e$.

טענה 1.2. תהא A קבוצה לא ריקה שעליה מוגדרת פעולה דו-מקומית "$*$" המקיימת את חוק הקיבוץ (אסוציאטיביות), בעלת איבר יחידה שמאלי $e\in A$ (כלומר לכל $a\in A$ מתקיים $e*a=a$) וסגורה להופכי שמאלי (כלומר לכל $a\in A$ קיים $b\in A$ כך ש-$b*a=e$); $(A,*)$ היא חבורה.

♣ כמובן שהטענה תקפה גם אם היינו דורשים איבר יחידה ימני והופכי ימני, אבל אם היינו דורשים איבר יחידה ימני והופכי שמאלי או להפך לא היינו מקבלים בהכרח חבורה.

תהא G חבורה.

משפט 1.3. יהיו $a,b\in G$; קיים $x\in G$ יחיד המקיים $a\cdot x=b$, כמו כן קיים $y\in G$ יחיד כך ש-$y\cdot a=b$.

הפסוק השני לא הופיע במפורש בשיעור.

♣ מכאן נובע שהכפלה באיבר (מימין או משמאל) היא פונקציה חח"ע ועל, כלומר תמורה (פרמוטציה בלעז).

מסקנה 1.4. יחידות האיבר ההופכי

יהיו $a,b,c\in G$, אם $a\cdot b=e=b\cdot a$ וגם $a\cdot c=e=c\cdot a$ אז $b=c$.

♣ בגלל מסקנה זו יש משמעות לסימון a^{-1}.

מסקנה 1.5. תכונות של חבורות

לכל $a,b,c\in G$ מתקיימים כל הפסוקים הבאים:

- $\left(a^{-1}\right)^{-1}=a$.
- $(a\cdot b)^{-1}=b^{-1}\cdot a^{-1}$.
- אם $a\cdot b=e$ אז $b=a^{-1}$ ו-$a=b^{-1}$.
- $a\cdot b=a\cdot c\iff b=c$.
- $a\cdot b=c\cdot b\iff a=c$.
- $a\cdot b=c\iff b=a^{-1}\cdot c\iff a=c\cdot b^{-1}$.

משפט 1.6. משפט אוילר לחבורות אבליות

נניח ש-G סופית ואבלית, לכל $a\in G$ מתקיים $a^{|G|}=e$.

♣ למעשה המשפט נכון גם עבור פעולות שאינן מקיימות את חוק החילוף אלא שההוכחה שלמדנו מסתמכת עליו.

♣ בפרט לכל $1<n\in\mathbb{N}$ ולכל $a\in\mathbb{Z}$ מתקיים $a^{\left|\mathbb{Z}_n^\times\right|}\equiv 1 \mod n$ (זהו המשפט המקורי שהוכיח אוילר שכן בתקופתו עוד לא הכירו את תורת החבורות).
בפרט לכל p ראשוני ולכל $a\in\mathbb{Z}$ מתקיים $a^{p-1}\equiv 1 \mod p$, משפט זה נקרא "המשפט הקטן של פרמה".

♣ מבחני ראשוניות רבים מתבססים על המשפט הקטן של פרמה, ראו כאן.

טענה 1.7. תהא $H \leqslant G$ תת-חבורה ותהא $K \subseteq H$, K היא תת-חבורה של G אם"ם היא תת-חבורה של H.

טענה 1.8. תהא X קבוצת תתי-חבורות של G, החיתוך של כל תתי-החבורות ב-X הוא תת-חבורה של G.

♣ נשים לב לכך שיש כאן כמה אפשרויות:

- X יכולה להיות סופית ואז קיימות תתי-חבורות $H_1, H_2, \ldots, H_r \subseteq V$ כך ש-$X = \{H_1, H_2, \ldots, H_r\}$, ואז החיתוך של כל תתי-החבורות בה הוא הקבוצה:
$$\bigcap_{i=1}^{r} H_i$$
- X יכולה להיות אין-סופית בת-מנייה, כלומר ניתן לסדר את איבריה בסדרה אינסופית: $X = \{H_1, H_2, \ldots\}$ ואז החיתוך של כל תתי-החבורות בה הוא הקבוצה:
$$\bigcap_{i=1}^{\infty} H_i$$
- X יכולה להיות אין-סופית שאינה בת-מנייה, כלומר א"א לסדר את איבריה בסדרה אינסופית, ואז החיתוך של כל תתי-החבורות בה הוא הקבוצה:
$$\bigcap_{H \in X} H$$

בכל מקרה החיתוך של כל תתי-החבורות ב-X הוא הקבוצה:
$$\left\{ g \;\middle|\; \forall H \in X : g \in H \right\}$$

סימון: לכל תת-קבוצה $S \subseteq G$ נסמן $S^{-1} := \left\{s^{-1} \mid s \in S\right\}$.

טענה 1.9. תהא $S \subseteq G$ תת-קבוצה, הקבוצה:
$$\left\{ \prod_{i=1}^{n} s_i \;\middle|\; n \in \mathbb{N}_0,\ \forall n \geq i \in \mathbb{N}\ s_i \in S \cup S^{-1} \right\}$$
היא תת-חבורה.

מסקנה 1.10. תהא $S \subseteq G$ תת-קבוצה, מתקיים:
$$\langle S \rangle = \left\{ \prod_{i=1}^{n} s_i \;\middle|\; n \in \mathbb{N}_0,\ \forall n \geq i \in \mathbb{N}\ s_i \in S \cup S^{-1} \right\}$$

טענה 1.11. אם G ציקלית אז גם כל תת-חבורה שלה כזו.

טענה 1.12. יהי $g \in G$ איבר בעל סדר סופי, מתקיים $|g| = |\langle g \rangle|$.

למה 1.13. יהי $g \in G$ איבר מסדר סופי ונסמן $n := |g|$, לכל $m \in \mathbb{Z}$ מתקיים $g^m = e$ אם"ם $n \mid m$.

טענה 1.14. יהיו $g, h \in G$ איברים בעלי סדר סופי, אם G אבלית אז $|gh|$ סופי ומחלק את $\mathrm{lcm}(|g|, |h|)$.

טענה 1.15. תת-קבוצה S יוצרת את G אם"ם גרף קיילי שלה הוא קשיר כגרף לא מכוון.

2 מחלקות ותתי-חבורות נורמליות

תהא G חבורה.

2.1 מחלקות

טענה 2.1. תהא $H \leqslant G$ תת-חבורה ותהא $C \subseteq G$ תת-קבוצה.

- אם C היא מחלקה שמאלית של H אז לכל $g \in C$ מתקיים $gH = C$.
- אם C היא מחלקה ימנית של H אז לכל $g \in C$ מתקיים $Hg = C$.

מסקנה 2.2. תהא $H \leqslant G$ תת-חבורה.

- כל שתי מחלקות שמאליות של H הן שוות או זרות.
- כל שתי מחלקות ימניות של H הן שוות או זרות.

מסקנה 2.3. תהא $H \leqslant G$ תת-חבורה; G היא איחוד זר של כל המחלקות השמאליות של H, וכמו כן היא איחוד זר של כל המחלקות הימניות של H.

מסקנה 2.4. תהא $H \leqslant G$ תת-חבורה ויהיו $a, b, c \in G$.

- $a \in aH$ וגם $a \in Ha$.
- $b \in aH$ אם"ם $a \in bH$, וכמו כן $b \in Ha$ אם"ם $a \in Hb$.
- אם $a \in bH$ וגם $b \in cH$ אז $a \in cH$, וכמו כן אם $a \in Hb$ וגם $b \in Hc$ אז $a \in Hc$.

♣ בקיצור ניתן לומר שלהיות באותה מחלקה ימנית/שמאלית של H זה יחס שקילות.

טענה 2.5. תהא $H \leqslant G$ תת-חבורה ויהיו $a, b \in G$, ארבעת התנאים הבאים שקולים:

1. $aH = bH$.
2. $b^{-1}aH = H$
3. $b^{-1}a \in H$.
4. $b \in aH$.

כמו כן גם ארבעת התנאים הבאים שקולים:

1. $Ha = Hb$.
2. $H = Hba^{-1}$.
3. $ba^{-1} \in H$.
4. $b \in Ha$.

טענה 2.6. תהא $H \leqslant G$ תת-חבורה, לכל $g \in G$ מתקיים $(gH)^{-1} = Hg^{-1}$ וגם $(Hg)^{-1} = g^{-1}H$.
בפרט, קבוצת ההופכיים של מחלקה שמאלית היא מחלקה ימנית וקבוצת ההופכיים של מחלקה ימנית היא מחלקה שמאלית.

♣ ניתן להסיק מכאן שמתקיים גם $[G : H] = |G/H| = |H\backslash G|$, כלומר האינדקס של H הוא גם מספר המחלקות הימניות של H (או העוצמה של קבוצת המחלקות הימניות כשמדבור בקבוצה אין-סופית).

מסקנה 2.7. תהא $H \leqslant G$ תת-חבורה סופית, כל שתי מחלקות של H הן באותו הגודל (שהוא $|H|$), בין אם שתיהן ימניות/שמאליות ובין אם אחת מהן ימנית ואחת שמאלית.

מסקנה 2.8. משפט לגראנז'[1]

אם G סופית אז לכל תת-חבורה $H \leqslant G$ מתקיים:

$$[G:H]=\frac{|G|}{|H|}$$

ובפרט הגודל של כל תת-חבורה מחלק את הגודל של החבורה.

מסקנה 2.9. אם G סופית אז לכל $g \in G$ הסדר של g מחלק את הסדר של G.

מסקנה 2.10. משפט אוילר לחבורות שאינן בהכרח אבליות

נניח ש-G סופית, לכל $a \in G$ מתקיים $a^{|G|}=e$.

מסקנה 2.11. תהיינה $H,K \leqslant G$ תתי-חבורות סופיות, אם $|H|$ ו-$|K|$ הם מספרים זרים אז $H \cap K = \{e\}$.

מסקנה 2.12. תהא G חבורה סופית, אם $|G|$ הוא מספר ראשוני אז אין ל-G תתי-חבורות שאינן טריוויאליות ו-G נוצרת ע"י כל איבר שאינו איבר היחידה (בפרט G ציקלית).

2.2 תתי-חבורות נורמליות

טענה 2.13. כל תת-חבורה $N \leqslant G$ מאינדקס 2 ($[G:N]=2$) היא תת-חבורה נורמלית.

טענה 2.14. תת-חבורה $N \leqslant G$ היא נורמלית אם"ם $N=gNg^{-1}$ לכל $g \in G$.

טענה 2.15. תת-חבורה $N \leqslant G$ היא נורמלית אם"ם $G/N=N\backslash G$.

♣ שימו לב לכך שהשוויון $G/N=N\backslash G$ הוא שוויון בין קבוצות, הוא אינו אומר שלכל איבר $g \in G$ המחלקה השמאלית gN שווה למחלקה הימנית Ng!

טענה 2.16. לכל שתי תתי-חבורות סופיות $H,K \leqslant G$ מתקיים:

$$|HK|=\frac{|H|\cdot|K|}{|H\cap K|}$$

טענה 2.17. תהיינה $H,K \leqslant G$ תתי-חבורות, מתקיים $HK \leqslant G$ אם"ם $HK=KH$.

מסקנה 2.18. תהא $N \trianglelefteq G$ תת-חבורה נורמלית, לכל $H \leqslant G$ מתקיים $NH, HN \leqslant G$.

[1] ערך בוויקיפדיה: ז'וזף-לואי לגראנז'.

3 פעולה של חבורה על קבוצה

תהא G חבורה.

3.1 פעולה כללית

תהא X קבוצה כך ש-G פועלת על X ע"י פעולה שנסמן ב-"$.$".

טענה 3.1. $x,y,z\in X$.

- $x\in O\left(x\right)$.
- $y\in O\left(x\right)$ אם"ם $x\in O\left(y\right)$.
- אם $x\in O\left(x\right)$ וגם $y\in O\left(z\right)$ אז $x\in O\left(z\right)$.

♣ בקיצור ניתן לומר שלהיות באותו מסלול זה יחס שקילות.

מסקנה 3.2. ניתן להציג את X כאיחוד זר של המסלולים תחת הפעולה של G.

טענה 3.3. אם $X\neq\emptyset$ ופעולת G על X חופשית אז היא גם נאמנה.

טענה 3.4. לכל $x\in X$ מתקיים $G_{x}\leqslant G$, כלומר המייצב הוא תמיד תת-חבורה.

משפט 3.5. משפט מסלול-מייצב

לכל $x\in X$ קיימת פונקציה חח"ע ועל מ-G/G_{x} (קבוצת המחלקות השמאליות של G_{x} ב-G) ל-$O\left(x\right)$ (המסלול של x), ולכן ע"פ הגדרה מתקיים $\left[G:G_{x}\right]=\left|O\left(x\right)\right|$; בפרט אם G סופית אז ע"פ משפט לגראנז' מתקיים:

$$\left|O\left(x\right)\right|=\frac{\left|G\right|}{\left|G_{x}\right|}$$

סימון: לכל $g\in G$ נסמן $\text{Fix}\left(g\right):=\left\{ x\in X\mid gx=x\right\}$.

♣ זהו סימון מקובל עבור קבוצת נקודות השבת של פונקציה.

משפט 3.6. הלמה של ברנסייד[2]

נניח ש-G ו-X סופיות, מתקיים:

$$\left|G\backslash X\right|=\frac{1}{\left|G\right|}\cdot\sum_{g\in G}\left|\text{Fix}\left(g\right)\right|$$

[2] ערך בוויקיפדיה האנגלית: William Burnside. למעשה הלמה הייתה מוכרת לפני ברנסייד ונקראה על שמו בטעות - ראו כאן.

3.2 הצמדה

טענה 3.7. מתקיים $Z(G)=\left\{g\in G\mid \forall h\in G\ g=hgh^{-1}\right\}$, כלומר האיברים היחידים שמחלקות הצמידות שלהם כוללות רק אותם הם האיברים שבמרכז.

משפט 3.8. משוואת המחלקה

נניח ש-G סופית ותהא I קבוצת נציגים של מחלקות הצמידות, מתקיים:

$$|G|=\sum_{g\in I}\left[G:C_G(g)\right]=\sum_{g\in I}\frac{|G|}{|C_G(g)|}$$

או בניסוח אחר ($\tilde{I}$ היא קבוצת נציגים של כל מחלקות הצמידות של איברים שאינם במרכז):

$$|G|=|Z(G)|+\sum_{g\in\tilde{I}}\left[G:C_G(g)\right]=|Z(G)|+\sum_{g\in\tilde{I}}\frac{|G|}{|C_G(g)|}$$

משפט 3.9. תת-חבורה $N\leqslant G$ היא נורמלית אם"ם ניתן להציג אותה כאיחוד של מחלקות צמידות.

משפט 3.10. תהא $H\leqslant G$ תת-חבורה, $N_G(H)$ היא תת-החבורה המקסימלית ביחס להכלה שבה H נורמלית; כלומר מתקיים $H\trianglelefteq N_G(H)$ ולכל $K\leqslant G$ כך ש-$H\trianglelefteq K$ מתקיים $K\subseteq N_G(H)$.

טענה 3.11. תהא $H\leqslant G$ תת-חבורה, מתקיים:

$$\left[G:N_G(H)\right]=\left|\left\{K\leqslant G\mid \exists g\in G\ gHg^{-1}=K\right\}\right|$$

כלומר האינדקס של $N_G(H)$ הוא מספר תתי-החבורות הצמודות ל-H (אם יש אין-סוף כאלה מדובר בעוצמה של הקבוצה המתאימה).

4 הומומורפיזמים

תהיינה G ו-H שתי חבורות ויהי $\varphi:G\to H$ הומומורפיזם.

טענה 4.1. הרכבה של הומומורפיזמים היא הומומורפיזם, והרכבה של איזומורפיזמים היא איזומורפיזם.

טענה 4.2. מתקיים $\varphi(e_G)=\varphi(e_H)$, וכמו כן לכל $g\in G$ מתקיים $\varphi\left(g^{-1}\right)=\left(\varphi(g)\right)^{-1}$.

טענה 4.3. מתקיים $\ker\varphi\trianglelefteq G$ ו-$\text{Im}\varphi\leqslant H$.

מסקנה 4.4. כל הומומורפיזם הוא אפימורפיזם ביחס לתמונתו, וכמו כן כל מונומורפיזם הוא איזומורפיזם בין תחום ההגדרה שלו לתמונתו.

♣ זו הסיבה לכך שמונומורפיזם נקרא גם **שיכון** - אנחנו **משכנים** את החבורה המהווה את תחום ההגדרה בתוך החבורה המהווה את הטווח.

טענה 4.5. φ הוא חח"ע (מונומורפיזם) אם"ם $\ker\varphi=\{e_G\}$.

משפט 4.6. למת הגרעין

לכל $a,b\in G$ מתקיים $\varphi(a)=\varphi(b)$ אם"ם $a\cdot\ker\varphi=b\cdot\ker\varphi$.

מסקנה 4.7. לכל $h\in H$ מתקיים $\varphi^{-1}(\{h\})\in G/\ker\varphi$, כלומר קבוצת המקורות של איבר נתון היא מחלקה של הגרעין[3].

טענה 4.8. תהא $S\subseteq G$ קבוצת יוצרים של G, $\varphi(S)$ היא קבוצת יוצרים של $\text{Im}\varphi$.

[3] כזכור הגרעין הוא תת-חבורה נורמלית (טענה 4.3) ולכן כל מחלקה ימנית היא מחלקה שמאלית עם אותם איברים.

משפט 4.9. הומומורפיזם נקבע ביחידות ע"פ קבוצת יוצרים

יהיו $\varphi_1,\varphi_2:G\to H$ הומומורפיזמים ותהא $S\subseteq G$ קבוצת יוצרים של G.

אם לכל $s\in S$ מתקיים $\varphi_1(s)=\varphi_2(s)$ אז $\varphi_1=\varphi_2$.

טענה 4.10. $\text{Aut}(G)$ היא חבורה ביחס לפעולת ההרכבה (איבר היחידה הוא פונקציית הזהות וההופכי הפונקציה ההופכית).

טענה 4.11. מתקיים $\text{Inn}(G)\leqslant\text{Aut}(G)$.

♣ ראינו בהרצאה (ללא הוכחה) שלכל $n\in\mathbb{N}$ מתקיים $\text{Inn}(S_n)=\text{Aut}(S_n)$ בתנאי אחד: $n\neq 6$, בשלב הזה כל הכיתה התפוצצה מצחוק...

תהא X קבוצה כך ש-G פועלת על X ע"י פעולה שנסמן ב-"."

טענה 4.12. כשעסקנו בפעולת חבורה על קבוצה ראינו שכל איבר ב-G משרה תמורה ב-S_X ע"י פעולתו על כל אחד מן האיברים ב-X, א"כ תהא $\rho:G\to S_X$ פונקציה המעתיקה כל איבר ב-G אל התמורה שהוא משרה על X, כלומר לכל $g\in G$ ו-$x\in X$ מתקיים:

$$(\rho(g))\,x:=g.x$$

ρ הוא הומומורפיזם, הומומורפיזם זה נקרא <u>הומומורפיזם המבנה</u> של פעולת G על X.

טענה 4.13. כל הומומורפיזם $\rho:G\to S_X$ מגדיר פעולה של G על X ע"י (לכל $g\in G$ ולכל $x\in X$):

$$g.x:=(\rho(g))\,x$$

♣ זוהי ממש שקילות בין הומומורפיזמים מ-G ל-S_X לבין פעולות של G על X.

טענה 4.14. הומומורפיזם המבנה של פעולת G על X הוא חח"ע (מונומורפיזם) אם"ם הפעולה של G על X היא פעולה נאמנה.

טענה 4.15. תהא $K\leqslant G$ תת-חבורה, G פועלת על G/K באמצעות כפל משמאל[4], א"כ נסמן ב-φ את הומומורפיזם המבנה של פעולת G על ${}^{G}/_{K}$; מתקיים:

$$\text{Core}_G(K)=\ker\varphi$$

ובפרט $\text{Core}_G(K)\trianglelefteq G$.

משפט 4.16. תהא $K\leqslant G$ תת-חבורה, $\text{Core}_G(K)$ היא תת-החבורה המקסימלית (ביחס להכלה) מבין תתי-החבורות הנורמליות של G שמוכלות ב-K; כלומר לכל $L\trianglelefteq G$ כך ש-$L\leqslant K$ מתקיים $L\subseteq\text{Core}_G(K)$.

מסקנה 4.17. תהא $N\leqslant G$ תת-חבורה, N נורמלית אם"ם $N=\text{Core}_G(N)$.

טענה 4.18. נניח ש-G סופית, יהי $p\in\mathbb{N}$ הראשוני הקטן ביותר שמחלק את $|G|$ ותהא $N\leqslant G$ תת-חבורה; אם $[G:N]=p$ אז $N\trianglelefteq G$.

מסקנה 4.19. נניח ש-G אין-סופית ושאין ל-G תתי-חבורות נורמליות שאינן טריוויאליות[5], לכל תת-חבורה $G\neq K\leqslant G$ האינדקס $[G:K]$ אינו סופי.

טענה 4.20. כשעסקנו בפעולת חבורה על קבוצה ראינו ש-G פועלת על עצמה ע"י כפל משמאל, הומומורפיזם המבנה של פעולה זו הוא חח"ע (מונומורפיזם).

♣ כלומר כל חבורה G ניתנת לשיכון ב-S_G.

מסקנה 4.21. משפט קיילי[6]

כל חבורה איזומורפית לתת-חבורה של חבורות תמורות כלשהי.

---

[4] הפעולה מוגדרת ע"י $g.C:=g\cdot C$ לכל $C\in{}^{G}/_{K}$ ולכל $g\in G$.

[5] כלומר לכל $N\trianglelefteq G$ מתקיים $N=\{e\}$ או ש-$N=G$. בהמשך נראה שחבורות כאלה נקראות חבורות פשוטות.

[6] ערך בוויקיפדיה: ארתור קיילי.

5 חבורות מנה

תהא G חבורה.

5.1 התחלה

טענה 5.1. 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[7] ע"י (לכל $g, h \in G$):

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

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

מסקנה 5.2. תהא $N \leqslant G$ תת-חבורה, N היא תת-חבורה נורמלית אס"ם היא גרעין של הומומורפיזם.

טענה 5.3. תהא $N \trianglelefteq G$ תת-חבורה נורמלית ותהא $S \subseteq G$ קבוצת יוצרים של G, הקבוצה $\{sN : s \in S\}$ היא קבוצת יוצרים של G/N.

מסקנה 5.4. אם G ציקלית אז לכל תת-חבורה $N \trianglelefteq G$ חבורת המנה G/N גם היא ציקלית.

משפט 5.5. אם $G/Z(G)$ ציקלית אז G אבלית, כלומר $G = Z(G)$.

טענה 5.6. מתקיים $\mathrm{Inn}(G) \trianglelefteq \mathrm{Aut}(G)$.

טענה 5.7. תהיינה H ו-K שתי חבורות, מתקיים $\{e_H\} \times K \trianglelefteq H \times K$ ו-$H \times \{e_K\} \trianglelefteq H \times K$, ובנוסף:

$$H \times K / H \times \{e_K\} \cong \{e_H\} \times K \cong K$$
$$H \times K / \{e_H\} \times K \cong H \times \{e_K\} \cong H$$

♣ הכיוון ההפוך אינו עובד: העובדה ש-$G/N \cong H$ אינה אומרת ש-$G \cong N \times H$, לדוגמה $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n$ אבל $\mathbb{Z} \ncong n\mathbb{Z} \times \mathbb{Z}_n$ (ב-$n\mathbb{Z} \times \mathbb{Z}_n$ יש איברים מסדר סופי).

טענה 5.8. אם G אבלית אז לכל $H \leqslant G$ חבורת המנה G/H[8] גם היא אבלית.

---

[7] כלומר קיימת פעולה $\cdot : G/N \times G/N \to G/N$ המקיימת את שלוש התכונות הנדרשות מכפל של חבורה.
[8] ראינו שבחבורה אבלית כל תת-חבורה היא נורמלית.

5.2 משפטי האיזומורפיזם

משפט 5.9. משפט האיזומורפיזם הראשון
תהא H חבורה ויהי $\varphi : G \to H$ הומומורפיזם, מתקיים:

$$G/\ker\varphi \cong \mathrm{Im}\varphi$$

מסקנה 5.10. מתקיים $G/Z(G) \cong \mathrm{Inn}(G)$.

מסקנה 5.11. משפט האיזומורפיזם השני
תהיינה $N, H \leqslant G$ תתי-חבורות כך ש-N נורמלית, מתקיים $H \cap N \trianglelefteq H$ ובנוסף:

$$HN/N \cong H/H\cap N$$

משפט 5.12. משפט האיזומורפיזם השלישי
תהיינה $N, H \trianglelefteq G$ תתי-חבורות נורמליות כך ש-$N \leqslant H$, מתקיים:

$$(G/N) / (H/N) \cong G/H$$

משפט 5.13. משפט ההתאמה[9]
תהא $N \trianglelefteq G$ תת-חבורה נורמלית ונסמן ב-π את הומומורפיזם ההטלה הקנוני של N.
קיימת התאמה חח"ע ועל בין תתי-חבורות של G המכילות את N לבין תתי-חבורות של G/N המשמרת הכלה, נורמליות ואינדקסים.
התאמה זו היא הפונקציה $f : \{H \leqslant G \mid N \subseteq H\} \to \{L \mid L \leqslant G/N\}$ המוגדרת ע"י (לכל $H \leqslant G$ כך ש-$N \leqslant H$)[10]:

$$f(H) := H/N = HN/N = \pi(H)$$

כלומר משפט ההתאמה טוען כי:

- f הנ"ל היא פונקציה חח"ע ועל (כלומר הפיכה, ההופכית שלה מוגדרת ע"י $f^{-1}(L) := \pi^{-1}(L)$[11] לכל $L \leqslant G/N$).
- לכל $N \leqslant H, K \leqslant G$ מתקיים:

$$K \leqslant H \iff K/N = f(K) \leqslant f(H) = H/N$$
$$K \trianglelefteq H \iff K/N = f(K) \trianglelefteq f(H) = H/N$$

ובנוסף, אם $K \leqslant H$ אז $[H : K] = [f(H) : f(K)] = [H/N : K/N]$.

---

[9] יש המכנים משפט זה בשם "משפט האיזומורפיזם הרביעי", למרות שבעצם אין בו איזומורפיזם בין חבורות.
[10] נזכיר ש-π היא פונקציה מ-G ל-G/N (תחום ההגדרה של f אינו זה של f), ופירושו של הסימון "$\pi(H)$" הוא $\{\pi(h) \mid h \in H\}$.
[11] גם כאן נזכיר ש-π כלל אינו מוכרח להיות הפיך, פירושו של הסימון "$\pi^{-1}(L)$" הוא $\{g \in G \mid \pi(g) \in L\}$.

6 חבורות p ומשפטי סילו

תהא G חבורה סופית ויהי $p\in\mathbb{N}$ ראשוני; נסמן $r:=\text{Ord}_p\left(|G|\right)$, ויהי $m\in\mathbb{N}$ כך ש-$|G|=p^r\cdot m$.

משפט סילו ה-I

משפט 6.1. משפט סילו הראשון[12]

יש ל-G חבורות p-סילו, או במילים אחרות $\text{Syl}_p\left(G\right)$ אינה ריקה.

טענה 6.2. תת-חבורה של חבורת p היא חבורת p, בפרט הסדר של כל איבר בחבורת p הוא חזקה של p.

מסקנה 6.3. משפט קושי

אם p מחלק את $|G|$ (כלומר $r\geq 1$) אז קיים $g\in G$ כך ש-$|g|=p$.

טענה 6.4. אם G היא חבורת p לא טריוויאלית (כלומר $m=1$ ו-$r>1$), אז p מחלק את $\left|Z\left(G\right)\right|$ ובפרט $Z\left(G\right)\neq\{e\}$.

טענה 6.5. אם G היא חבורת p (כלומר $m=1$ ו-$r>1$), אז לכל $r\geq k\in\mathbb{N}_0$ קיימת תת-חבורה נורמלית $N\trianglelefteq G$ כך ש-$|N|=p^k$.

אני לא בטוח שראינו את הטענה הזו בכיתה.

מסקנה 6.6. לכל $\text{Ord}_p\left(|G|\right)\geq k\in\mathbb{N}_0$ קיימת תת-חבורה $H\leqslant G$ כך ש-$|H|=p^k$.

משפט סילו ה-II

טענה 6.7. לכל $P\in\text{Syl}_p\left(G\right)$ ולכל $H\leqslant G$ קיים $g\in G$ כך ש-$\left(gPg^{-1}\cap H\right)\in\text{Syl}_p\left(H\right)$.

מסקנה 6.8. משפט סילו השני

כל שתי חבורות p-סילו של G צמודות זו לזו, או בניסוח אחר $\text{Syl}_p\left(G\right)$ מהווה מסלול תחת פעולת G על אוסף תתי-החבורות שלה ע"י הצמדה.

- ♣ מהגדרה כל חבורה שצמודה לחבורת p-סילו גם היא חבורת p-סילו (הן באותו גודל), החידוש של המשפט הוא שגם הכיוון ההפוך נכון.

מסקנה 6.9. חבורת p-סילו היא נורמלית אם"ם היא יחידה, כלומר לכל $P\in\text{Syl}_p\left(G\right)$ מתקיים:

$$P\trianglelefteq G\Longleftrightarrow\text{Syl}_p\left(G\right)=\{P\}$$

- ♣ הגרירה מימין לשמאל היא טריוויאלית (כל החבורות הצמודות ל-P הן באותו הגודל של P), רק בשביל הגרירה בכיוון ההפוך יש צורך במשפט סילו השני.

מסקנה 6.10. לכל תת-חבורה $H\leqslant G$ ולכל $P_H\in\text{Syl}_p\left(H\right)$ קיימת $P_G\in\text{Syl}_p\left(G\right)$ כך ש-$P_H=P_G\cap H$.

מסקנה 6.11. לכל תת-חבורה $H\leqslant G$ כך ש-H היא חבורת p קיימת $P\in\text{Syl}_p\left(G\right)$ כך ש-$H\leqslant P$.

משפט סילו ה-III

משפט 6.12. משפט סילו השלישי

נסמן $k_p:=\left|\text{Syl}_p\left(G\right)\right|$, מתקיים $k_p\equiv 1\mod p$ ו-$k_p\mid m$.

- ♣ בפרק הבא אנחנו נראה שמשפטי סילו, ובפרט המשפט השלישי, הם כלים רבי עוצמה בניתוח של חבורות סופיות.

[12] ערך בוויקיפדיה: לודוויג סילו

7 פירוק לחבורות פשוטות

תהא G חבורה.

7.1 מכפלה ישרה ומכפלה ישרה למחצה

טענה 7.1. תהיינה H ו-K חבורות ותהיינה $\tilde{H} \trianglelefteq H$ ו-$\tilde{K} \trianglelefteq K$ תתי-חבורות נורמליות, מתקיים:

$$^{H\times K}/_{\tilde{H}\times\tilde{K}} \cong {}^{H}/_{H_0} \times {}^{K}/_{\tilde{K}}$$

טענה 7.2. תהיינה $H, K \leqslant G$ תתי-חבורות כך ש-$G = H \rtimes K$, מתקיים $K \cong {}^{G}/_{H}$.

משפט 7.3. 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 $(H \times K, *) = \tilde{H} \rtimes \tilde{K}$[13] אם"ם קיים הומומורפיזם $\phi : K \to \mathrm{Aut}\,(H)$ כך שלכל $(h,k)\,,(h',k') \in H \times K$ מתקיים[14]:

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

משפט 7.4. יהי $p \in \mathbb{N}$ ראשוני ונניח ש-$|G| = p^2$;
אם יש ב-G איבר מסדר p^2 אז $G \cong \mathbb{Z}_{p^2}$, אחרת $G \cong \mathbb{Z}_p \times \mathbb{Z}_p$.

משפט 7.5. יהיו $p, q \in \mathbb{N}$ מספרים ראשוניים כך ש-$p < q$, ונניח ש-$|G| = p \cdot q$.

- אם $q \not\equiv 1 \mod p$ אז $G \cong \mathbb{Z}_q \times \mathbb{Z}_p$.
- אם $q \equiv 1 \mod p$ אז $G \cong \mathbb{Z}_q \times \mathbb{Z}_p$ או שלכל הומומורפיזם לא טריוויאלי $\phi : \mathbb{Z}_p \to \mathrm{Aut}\,(\mathbb{Z}_q)$ מתקיים $G \cong \mathbb{Z}_q \rtimes_\phi \mathbb{Z}_p$.

♣ מכאן שאם $q \equiv 1 \mod p$ אז אז יש בדיוק שתי חבורות מסדר $p \cdot q$ (עד כדי איזומורפיזם): אחת אבלית ($\mathbb{Z}_q \times \mathbb{Z}_p$) ואחרת שאינה אבלית ($\mathbb{Z}_q \rtimes_\phi \mathbb{Z}_p$).

7.2 סדרות נורמליות וסדרות הרכב

טענה 7.6. לכל חבורה סופית יש סדרת הרכב.

טענה 7.7. סדרה נורמלית של חבורה היא סדרת הרכב שלה אם"ם כל הגורמים שלה הם חבורות פשוטות.

משפט 7.8. משפט ז'ורדן-הלדר (Jordan–Hölder)[15]
נניח של-G יש סדרות הרכב, גורמי ההרכב של כל שתי סדרות הרכב של G זהים עד כדי סדר ואיזומורפיזם; כלומר מדובר באותן חבורות מנה (עד כדי איזומורפיזם) וכל אחת מהן מופיעה אותו מספר של פעמים עבור כל אחת משתי סדרות ההרכב.

♣ בגלל משפט זה ניתן לדבר על גורמי ההרכב של חבורה (ולא רק של סדרת הרכב), אך יש לשים לב לכך שגורמי ההרכב של חבורה אינם קובעים אותה ביחידות, כלומר קיימות חבורות שאינן איזומורפיות זו לזו אך יש להן את אותם גורמי הרכב.

♣ בכל מקום שנדבר על גורמי ההרכב של חבורה ייתכן שכמה מן החבורות מופיעות כמה פעמים.

[13] כלומר הזוג הסדור $(H \times K, *)$ הוא חבורה, ובנוסף זוהי החבורה $\tilde{H} \rtimes \tilde{K}$.
[14] ϕ_k הוא האוטומורפיזם ב-$\mathrm{Aut}\,(H)$ שאליו מעתיק ϕ את k.
[15] ערכים בוויקיפדיה: קאמי ז'ורדן (עברית) ו-Otto Hölder (אנגלית).

טענה 7.9. כל חבורה סופית, פשוטה ואבלית איזומורפית ל-$\mathbb{Z}_p$ עבור $p \in \mathbb{N}$ ראשוני כלשהו.

מסקנה 7.10. נניח ש-G אבלית וסופית, ויהיו $p_1, p_2, \ldots, p_r \in \mathbb{N}$ מספרים ראשוניים כך שמתקיים[16]:

$$|G| = \prod_{i=1}^{r} p_i$$

גורמי ההרכב של G הם $\mathbb{Z}_{p_1}, \mathbb{Z}_{p_2}, \ldots, \mathbb{Z}_{p_r}$.

משפט 7.11. נניח של-G יש סדרות הרכב ותהא $N \trianglelefteq G$ תת-חבורה נורמלית, יהיו $N_1, N_2, \ldots, N_r$ גורמי ההרכב של N ויהיו $H_1, H_2, \ldots, H_s$ גורמי ההרכב של G/N. גורמי ההרכב של G הם כולם יחד, כלומר $N_1, N_2, \ldots, N_r, H_1, H_2, \ldots, H_s$.

7.3 חבורות פתירות

משפט 7.12. נניח ש-G סופית, G פתירה אם"ם כל אחד מגורמי ההרכב שלה איזומורפי ל-$\mathbb{Z}_p$ עבור ראשוני $p \in \mathbb{N}$ כלשהו.

מסקנה 7.13. נניח ש-G סופית, G פתירה אם"ם קיימת תת-חבורה נורמלית $N \trianglelefteq G$ כך ש-N ו-G/N פתירות.

טענה 7.14. אם G פתירה אז כל תת-חבורה שלה גם היא פתירה.

מסקנה 7.15. נניח ש-G סופית, G פתירה אם"ם לכל תת-חבורה נורמלית $N \trianglelefteq G$ החבורות N ו-G/N פתירות.

7.4 החבורה הנגזרת

משפט 7.16. תכונות החבורה הנגזרת

1. $G' \trianglelefteq G$
2. G/G' אבלית
3. G' היא תת-החבורה הנורמלית הקטנה ביותר של G (ביחס להכלה) כך ש-G/G' אבלית,
כלומר לכל $N \trianglelefteq G$ כך ש-G/N אבלית מתקיים $G' \leqslant N$.

♣ לפעמים מתארים את התכונה השלישית במילים "G/G' היא חבורת המנה האבלית הגדולה ביותר של G".

טענה 7.17. G פתירה אם"ם קיים $n \in \mathbb{N}_0$ כך שמתקיים $G^{(n)} = \{e\}$.

7.5 חבורות נילפוטנטיות

טענה 7.18. כל חבורה נילפוטנטית היא חבורה פתירה.

טענה 7.19. תהיינה H ו-K חבורות נילפוטנטיות; גם $H \times K$ נילפוטנטית, ומחלקת הנילפוטנטיות שלה היא המקסימלית מבין אלו של H ו-K.

טענה 7.20. כל חבורת p (עבור $p \in \mathbb{N}$ ראשוני) היא חבורה נילפוטנטית ובפרט פתירה.

מסקנה 7.21. יהיו $p_1, p_2, \ldots, p_r \in \mathbb{N}$ מספרים ראשוניים, ותהיינה $P_1, P_2, \ldots, P_r$ חבורות כך ש-P_i היא חבורת p_i לכל $r \geq i \in \mathbb{N}$; החבורה $P_1 \times P_2 \times \ldots \times P_r$ היא חבורה נילפוטנטית.

[16] ייתכן שקיימים $r \geq i, j \in \mathbb{N}$ כך ש-$p_i = p_j$ למרות ש-$i \neq j$.

למה 7.22. תהיינה $N, H \leqslant G$ כך ש-$N \leqslant H$ ו-$N \trianglelefteq G$, מתקיים:

$$N_{G/N}\left({}^{H}/_{N}\right) \cong {}^{N_G(H)}/_{N}$$

למה 7.23. נניח ש-G סופית, יהי $p \in \mathbb{N}$ ראשוני, ותהיינה $H \trianglelefteq G$ תת-חבורה נורמלית, ו-$P \leqslant H$ חבורת p-סילו של H; אם $P \trianglelefteq H$ אז $P \trianglelefteq G$.

משפט 7.24. נניח ש-G סופית, ארבעת הפסוקים הבאים שקולים:

1. G נילפוטנטית.
2. כל תת-חבורה ממש של G היא גם תת-חבורה ממש של המנרמל שלה[17].
3. כל חבורת p-סילו של G (עבור $p \in \mathbb{N}$ ראשוני) היא תת-חבורה נורמלית.
4. יהיו $p_1, p_2, \ldots, p_r \in \mathbb{N}$ כל הראשוניים **השונים** בפירוק של $|G|$ לראשוניים[18], ותהיינה $P_1, P_2, \ldots, P_r \leqslant G$ חבורות כך ש-P_i היא חבורת p_i-סילו של G לכל $r \geq i \in \mathbb{N}$; מתקיים:

$$G \cong P_1 \times P_2 \times \ldots \times P_r$$

מסקנה 7.25. נניח ש-G סופית ונילפוטנטית ויהיו $g, h \in G$, אם $|g|$ ו-$|h|$ הם מספרים זרים אז $gh = hg$.

מסקנה 7.26. נניח ש-G סופית ונילפוטנטית, לכל $d \in \mathbb{N}$ המחלק את $|G|$ קיימת תת-חבורה נורמלית $N \trianglelefteq G$ כך ש-$|N| = d$.

טענה 7.27. אם G נילפוטנטית אז לכל תת-חבורה $\{e\} \neq N \trianglelefteq G$ מתקיים $Z(G) \cap N \neq \{e\}$.

---

[17] כלומר לכל תת-חבורה $H \leqslant G$ כך ש-$H \neq G$ מתקיים $H \neq N_G(H)$.

[18] כלומר מתקיים:

$$|G| = \prod_{i=1}^{r} (p_i)^{\mathrm{Ord}_{p_i}(|G|)}$$

8 חבורות חופשיות

טענה 8.1. תהיינה S ו-T שתי קבוצות (לאו דווקא סופיות), אם $|T|=|S|$ אז $F(S)\cong F(T)$.

סימון: לכל $n\in\mathbb{N}_0$ נסמן ב-F_n את החבורה החופשית על הקבוצה $\{1,2,\ldots,n\}$.

מסקנה 8.2. $F_1\cong\mathbb{Z}$.

משפט 8.3. התכונה האוניברסלית
תהא S קבוצה ותהא G חבורה, לכל פונקציה $f:S\to G$ קיים הומומורפיזם יחיד $\tilde{f}:F(S)\to G$ כך ש-$\tilde{f}\mid_S=f$.

מסקנה 8.4. תהא G חבורה ותהא $S\subseteq G$ קבוצת יוצרים של G, ויהי $\varphi:F(S)\to G$ אותו הומומורפיזם יחיד כך ש-$\varphi\mid_S=\mathrm{Id}_S$; מתקיים:

$$G\cong {}^{F(S)}/_{\ker\varphi}$$

משפט 8.5. תהא G חבורה, תהא $S\subseteq G$ תת-קבוצה ויהי $\varphi:F(S)\to G$ אותו הומומורפיזם יחיד כך ש-$\varphi\mid_S=\mathrm{Id}_S$. שלושת הפסוקים הבאים שקולים זה לזה:

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

♣ 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-$(v_1,v_2,\ldots,v_n)$ 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-$T(v_i)=w_i$ לכל $n\geq i\in\mathbb{N}$.