משפטי סילו

ציון לנדס

6 במאי 2018

1 מבוא

תורת החבורות היא ענף באלגברה מופשטת. לעיתים, כאשר חוקרים מבנה מתמטי, מבחינים כי חלק מתכונותיו זהה לאלו של מבנה אחר, ששייך אולי לתחום מתמטי אחר. מתבקש במקרה זה להכלילם כמקרים פרטיים של מבנה גדול יותר, בעל תכונות אלו.
התעלמות מפרטים שייחודיים לכל מבנה מאפשרת לאחד מבנים רבים תחת אותה כותרת - **מבנה אלגברי**. הפשטה זו מאפשרת להסיק מסקנות משותפות לכל המבנים מאותו סוג, ללא צורך להוכיחן בכל מקרה בנפרד, ואף להבחין בתכונות שהובלעו תחת הפרטים.
ניתן כמובן למצוא הכללות כאלו לאין ספור. אך במבחן הזמן, רק הכללות 'מענינות' - כאלה שבזכותן הושגו מסקנות חשובות - זוכות להתענינות. ואחד המבנים האלגבריים השימושיים ביותר היא החבורה.
האלגברה המופשטת מתמודדת עם בעיה כללית יותר: ככל שדיון רחב יותר, הוא מתייחס לנושאים רבים יותר, במחיר מסקנות כלליות מדי. כשהדיון ממוקד יותר, המסקנות רבות ומדויקות יותר.
מבנה אלגברי מוגדר על־פי הגבלות מסוימות, שקובעות מה נדרש על מנת להיכלל בו. ככל שההגבלות רבות יותר, כך ניתן להסיק יותר על איבריו, במחיר הכנסת פחות מבנים מתמטיים תחת אותו מבנה אלגברי.
חבורה היא מקרה בו מושג 'רווח' מרובה במחיר מועט:
כדי שמבנה מתמטי יחשב לחבורה, עליו לעמוד בדרישות מועטות למדי (בהשוואה למבנים נפוצים אחרים) - קיומה של פעולה בעלת תכונות נפוצות בודדות, ובהתאם לכך הדוגמאות לחבורות בענפי המתמטיקה השונים רבות מאוד. אך כבר הגבלות אלו מגלות עושר רב של תכונות שמשותפות למבנים אלו.

תוכן עניינים

1 מבוא 2
2 הגדרות ומשפטים 4
2.1 חבורות 4
2.2 תת־חבורות 4
2.3 חבורה צקלית 4
2.4 משפט לגרנז' 5
2.5 קוסטים 6
2.6 הומומורפיזם 7
3 פעולות חבורה 8
3.1 אינטואיציות 8
3.2 מסלולים 8
4 משפטי סילו 10
4.1 משפט סילו, חלק ראשון 10
4.2 משפט סילו, חלק שני 11
4.3 משפט סילו, חלק שלישי 12
5 נספח: יישום של משפטי סילו 14
6 מקורות 15

2 הגדרות ומשפטים

2.1 חבורות

הגדרה 2.1 חבורה היא הזוג הסדור $(G,\bullet)$, בו G קבוצה ו־$\bullet$ פעולה מ־$G\times G$ ל־G, שמקיימת:

1. סגירות – אם $a,b\in G$ אז גם $a\bullet b\in G$.
2. אסוציאטיביות – אם $a,b,c\in G$ אז $(a\bullet b)\bullet c=a\bullet(b\bullet c)$.
3. קיים איבר אדיש e בקבוצה כך שלכל $a\in G$ מתקיים $a\bullet e=e\bullet a=a$.
4. לכל איבר a בקבוצה קיים איבר הופכי שמסומן ב־a^{-1} ומתקיים $a^{-1}\bullet a=a\bullet a^{-1}=e$.

מקובל לקרוא לפעולה הבינארית 'כפל' (גם אם אינה פעולת הכפל המוכרת בין מספרים ממשיים) ולכתוב ab במקום $a\bullet b$.

הגדרה 2.2 חבורה בה הפעולה חילופית (קומוטטיבית), כלומר $ab=ba$, נקראת **חבורה אבלית**.

בתוך חבורה מתקיימים כללי הצמצום החד־צדדיים: $a\not{b}=b\not{b}\implies a=b$ וכן $\not{a}a=\not{b}b\implies a=b$, אך רק בחבורה אבלית אפשר לצמצם משני הצדדים: $a\not{b}=\not{b}b\implies a=b$.

הגדרה 2.3 נסמן ב־$|G|$ את מספר האיברים בקבוצה G. מספר זה מכונה ה**סדר של** ה**חבורה** (או גודל החבורה).

קיימות חבורות מסדר אינסופי, אך נעסוק כאן בעיקר בחבורות סופיות, שהן בעלות עושר רב יותר של תכונות.

2.2 תת־חבורות

הגדרה 2.4 תהי G חבורה, H תת־קבוצה לא ריקה שלה. H נקראת **תת־חבורה** של G אם היא בעצמה חבורה ביחס לפעולה של G, ומסומנת $H\leq G$.

תת־החבורה זהה לחבורה המקורית, אם מצטמצמים לקבוצה H בלבד: האיבר האדיש שלה הוא גם האדיש של החבורה, ולכל איבר בתת־החבורה יש אותו הופכי בחבורה ובתת־החבורה.

טענה 2.5 תת־חבורה של תת־חבורה היא תת־חבורה של החבורה המקורית: $K\leq H,H\leq G\implies K\leq G$.

טענה 2.6 אם H קבוצה סופית, מספיק לבדוק רק את סגירותה כדי להוכיח שהיא תת־חבורה.
אם היא קבוצה אינסופית, יש לבדוק לשם כך גם קיום איברים הופכיים.

2.3 חבורה צקלית

הגדרה 2.7 יהי a איבר בחבורה, i מספר שלם.
a^i מוגדר כהכפלת a בעצמו i פעמים, $a^{-i}=(a^{-1})^i$, ו־$a^0=e$.

הגדרה 2.8 תהי G חבורה, $a\in G$. הקבוצה $\{a^i|i\in\mathbb{Z}\}$ מכונה **החבורה הצקלית שנוצרת ע"י** a. נהוג לסמנה ב־$\langle a\rangle$, ולומר ש־a **יוצר** של החבורה.

מתוך שימוש בכללי החזקות, אפשר בקלות לראות שכל חבורה צקלית היא גם אבלית.

הגדרה 2.9 הקבוצה $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$ עם פעולת החיבור מודולו n מכונה **החבורה הצקלית מסדר** n.

לחבורה יכולים להיות כמה יוצרים, אך כל החבורות הצקליות מאותו סדר איזומורפיות זו לזו (איזומורפיזם בין חבורות יידון בהמשך).

הקבוצה $\mathbb{Z}$ עם פעולת החיבור הרגילה היא החבורה הצקלית (היחידה עד כדי איזומורפיזם) מסדר אינסופי.

נתעכב מעט על תכונת המעגליות שמאפיינת חבורות צקליות.

אם G חבורה צקלית סופית, גם $\langle a \rangle$ סופית. לכן ניתן לכתוב $\langle a \rangle = \{e, a, a^2, \ldots, a^{n-1}\}$.
אפשר להכפיל את איברי הקבוצה ב־a ־ $a \cdot \langle a \rangle = \{a, a^2, \ldots, a^{n-1}, a^n\}$. אלו גם חזקות של a, שכבר נכללו כולן ב־$\langle a \rangle$, ז"א $a \cdot \langle a \rangle = \langle a \rangle$.
אחד מאיברי $a \cdot \langle a \rangle$ חייב להיות האיבר האדיש. האיבר היחיד שנוסף הוא a^n, ולכן $a^n = a^{|\langle a \rangle|} = e$.

הגדרה 2.10 ה**סדר של איבר** בחבורה $g \in G$ הוא המספר הטבעי הקטן ביותר m שעבורו $g^m = e$.
במילים אחרות, בכמה 'קפיצות' האיבר 'מתאפס'.
אם לא קיים מספר כזה, אז הסדר אינסופי.

כמוסבר לעיל, סדר האיבר הוא גם הסדר של $\langle g \rangle$ ־ החבורה הצקלית שהוא יוצרה. לכן כשהחבורה סופית, סדר איבריה גם הוא מספר סופי.
העובדה שהפעולה בחבורה היא מחזורית, שקיימת בהכרח בחבורות סופיות, היא זו שעושה אותן מעניינות יותר. מתכונה זו נגזרות תכונות רבות נוספות.

2.4 משפט לגרנז'

המשפט הבא הינו כלי שימושי ביותר בתורת החבורות.

משפט 2.11 (משפט לגרנז') מספר איברי תת־חבורה של חבורה סופית מחלק את מספר איברי החבורה:
$H \leq G \implies |H| \mid |G|$.

הוכחת המשפט משתמשת בקוסטים, שיוסברו להלן, אך מתאים יותר להביאו כאן מבחינת רצף הענין.
בעזרת משפט לגרנז' אפשר לשלול את קיומן של תת־חבורות מגדלים שאינן מתחלקים בסדר החבורה.
הכיוון השני ־ הוכחת קיום תת־חבורות מסדר מסוים ־ אינו מתאפשר באמצעות משפט זה, והוא מתחום עיסוקם של משפטי סילו, שהם ליבו של המאמר.

מסקנות ממשפט לגרנז'

מסקנה 2.12 כל חבורה מסדר ראשוני היא צקלית.

הוכחה: תהי G מסדר ראשוני, $g \in G$.
לפי משפט לגרנז', סדר תת־החבורה שנוצרת ע"י g מחלק את $|G|$. אבל G מסדר ראשוני, לכן $|\langle g \rangle| = G$ לכל $g \neq e$. מכאן נובע גם שכל איבר בחבורה זו, למעט האדיש, הוא יוצר שלה. □

המשפטים הבאים באים מתחום תורת המספרים, והובאו כאן כדי להדגים את הוכחתם כמסקנות ממשפט בתורת החבורות.

מסקנה 2.13 (משפט אוילר) יהיו a ו־n מספרים טבעיים זרים.
אזי $a^{\Phi(n)} \equiv 1 (\mathrm{mod} n)$, כאשר $\Phi(n)$ היא פונקציית אוילר.

הוכחה: נבנה את $\mathbb{Z}_n^*$ - **החבורה הכפלית מודולו** n - חבורה של מספרים טבעיים שקטנים מ-n, והפעולה בה היא כפל מודולו n.
האיבר האדיש בחבורה הוא 1. 0 אינו נכלל בה, מאחר שאין לו הופכי.
אם b הוא מספר שאינו זר ל-n, אז קיים $c < n$ כך ש-$bc \equiv 0(\mathrm{mod}n)$, ואין זה מתיישב עם דרישת הסגירות. על כן, החבורה מכילה רק את המספרים שאין להם גורם משותף עם n.
אפשר בקלות לוודא ששאר אקסיומות החבורה מתקיימות בקבוצה זו.
קבלנו ש-$\mathbb{Z}_n^*$ היא חבורת המספרים הטבעיים שקטנים מ-n וזרים לו, וגודלה $|\mathbb{Z}_n^*| = \Phi(n)$.

יהי $a \in \mathbb{Z}_n^*$. כבר ראינו כי $a^{|\langle a\rangle|} = e = 1$. לפי משפט לגרנז', קיים מספר טבעי c כך ש- $|\langle a\rangle| \cdot c = |\mathbb{Z}_n^*| = \Phi(n)$, ולכן $a^{\Phi(n)} = a^{|\langle a\rangle|\cdot c} \equiv e^c(\mathrm{mod}n) = 1$. □

מסקנה 2.14 (משפט פרמה) יהי a מספר טבעי ו-p מספר ראשוני. אזי $a^p \equiv a(\mathrm{mod}p)$.

הוכחה: אם p מחלק של a, אז $p \equiv 0 \equiv a(\mathrm{mod}p)$ ועל כן $a^p \equiv 0 \equiv a(\mathrm{mod}p)$.
אחרת, כל המספרים הטבעיים שקטנים ממספר ראשוני זרים לו, ולכן $\Phi(p) = p-1$.
בשימוש במשפט אוילר, $a^p = a^{\Phi(p)+1} \equiv e \cdot a(\mathrm{mod}p) = a$. □

2.5 קוסטים

הגדרה 2.15 תהי H תת-חבורה של G, $g \in G$. הקבוצה $Hg = \{hg|h \in H\}$ - הקבוצה שנוצרת מהכפלת כל איברי H ב-g - נקראת **קוסט ימני** (או **מחלקה** ימנית) של G.
איבר g זה מכונה **נציג** של הקוסט.
באותו אופן תוגדר $gH = \{gh|h \in H\}$ כקוסט שמאלי.

טענה 2.16 לכל תת-חבורה H יש בדיוק $|G|/|H|$ קוסטים (מאותו צד) שונים.
הקוסטים הללו זרים זה לזה, ז"א כל אחד מהם מכיל איברים שייחודיים רק לו.
במילים אחרות, שני קוסטים (של אותה תת-חבורה) יכולים להיות אחד מהשניים: זהים, או זרים.

הקוסטים השונים של תת-חבורה מכסים את G ומחלקים אותה למחלקות שקילות – איברים מאותו קוסט שקולים זה לזה. יחס השקילות הוא $a \sim b \iff ab^{-1} \in H$ כשהקוסטים ימניים, או $a \sim b \iff b^{-1}a \in H$ לשמאליים.

אפשר להתיחס לפעולה שנעשית בהכפלת H ב-g כ'הזזה' של כל אחד מהאיברים של H ב-g.
אם $g \in H$ ו-$g \neq e$, אז $gH = H$ וכל איבר $h \in H$ מוזז ל-gh, כך שנעשה רק שינוי סדר איברי הקבוצה H.

טענה 2.17 תהי N תת-חבורה של G. התנאים הבאים שקולים:

- $\forall g \in G : gNg^{-1} = N$.
- הקוסטים הימניים והשמאליים, שנוצרים מהכפלה באותו איבר, שווים: $\forall g \in G : gN = Ng$.

הגדרה 2.18 תת-חבורה N שמקיימת את התנאים הללו מכונה **תת-חבורה נורמלית**, ומסומנת $N \triangleleft G$.

הגדרה 2.19 אוסף הקוסטים השונים של תת־חבורה נורמלית N מסומן G/N.

אוסף זה מהווה חבורה ש־Ne איברה האדיש, Ng^{-1} הופכי ל־Ng, והפעולה מקבילה לפעולה בחבורה: $(Na)(Nb) = N(ab)$. חבורה זו נקראת **חבורת המנה** של G ביחס ל־N.

אוסף הקוסטים הימניים או השמאליים של תת־חבורה מחלקים אותה למחלקות שקילות, אך רק אם זו תת־חבורה נורמלית אוסף כזה מהווה בעצמו חבורה (ביחס לפעולה בחבורה המקורית).

הגדרה 2.20 מספר הקוסטים השונים של תת־חבורה מכונה ה**אינדקס** שלה, ומסומן $[G : H]$.

מסקנה ממשפט לגרנז' שבקבוצה סופית $[G : H] = |G|/|H|$.

2.6 הומומורפיזם

הגדרה 2.21 העתקה ϕ מחבורה G לחבורה $\bar{G}$ נקראת **הומומורפיזם** אם לכל $a, b \in G$ מתקיים $\phi(ab) = \phi(a)\phi(b)$.

נהוג לתאר הומומורפיזם כהעתקה שמשמרת פעולה: היחס בין a ל־b בקבוצת המקור G נשמר בין התמונות שלהם $\phi(a)$ ו־$\phi(b)$ בחבורת היעד.
יש לשים לב שהיחס נשמר ביחס לפעולה שמוגדרת בחבורה המתאימה. כדי להדגיש זאת, נסמן ב־$\bullet$ את הפעולה ב־G, וב־$*$ את הפעולה ב־$\bar{G}$. בסימון זה $\phi(a \bullet b) = \phi(a) * \phi(b)$.

הגדרה 2.22 תהי ϕ הומומורפיזם מ־G ל־$\bar{G}$. נסמן ב־$\bar{e}$ את האיבר האדיש ב־$\bar{G}$.
גרעין ההעתקה $Ker(\phi)$ מוגדר כקבוצת האיברים ב־G ש־ϕ מעתיקה ל־$\bar{e}$: $Ker(\phi) = \{k \in G | \phi(k) = \bar{e}\}$.

טענה 2.23 גרעין של הומומורפיזם מהווה תת־חבורה נורמלית של חבורת המקור.

הגדרה 2.24 תהי ϕ הומומורפיזם מ־G על $\bar{G}$.
x יקרא **תמונה הפוכה** של $\bar{g} \in \bar{G}$ תחת ϕ אם $\phi(x) = \bar{g}$.

טענה 2.25 יהי x תמונה הפוכה של $\bar{g}$. קבוצת כל התמונות ההופכיות של $\bar{g}$ מתקבלת כהכפלת גרעין ההעתקה ב־x: $x \cdot Ker(\phi) = \{xk | \phi(k) = \bar{e}\}$.

הגדרה 2.26 הומומורפיזם חח"ע ועל נקרא **איזומורפיזם**.
שתי חבורות איזומורפיות זו לזו אם קיים בינהן איזומורפיזם, ומסמנים $G \cong \bar{G}$.

בשימוש בהגדרות הקודמות אפשר לומר שאם ϕ על $\bar{G}$ ו־$Ker(\phi) = e$ אז ϕ איזומורפיזם.

מקובל לתאר חבורות שבינהן איזומורפיזם כ'אותה חבורה, עד כדי שמות האיברים'.

משפט 2.27 (משפט האיזומורפיזם הראשון)
תהי ϕ הומומורפיזם מ־G על $\bar{G}$. אזי $G/Ker(\phi) \cong \bar{G}$.
במילים, חבורת המנה ביחס לגרעין ההעתקה איזומורפית לתמונת ההעתקה.

משפט זה מסכם במידה רבה את הטענות האחרונות.
כאמור לעיל, כשיש העתקה איזומורפית מ־G ל־$\bar{G}$, אפשר לומר שהחבורות זהות עד כדי שמות איבריהן. מצב זה מאפשר להסיק מסקנות דומות על שתי החבורות. כאשר העתקה זו אינה חח"ע אלא רק הומומורפיזם 'על', חד־חד־ערכיות נשמרת בין $\bar{G}$ לקוסטים של הגרעין.

עוד ניתן לראות שהתמונות ההופכיות של כל איבר מ־$\bar{G}$ הן בדיוק באותו גודל - גודל הגרעין. גודל זה יכול להוות מדד לכמה ההומומורפיזם קרוב להיות איזומורפיזם, כשכמובן אם הגרעין טריוויאלי זהו איזומורפיזם.

3 פעולות חבורה

הגדרה 3.1 תהי G חבורה ו־X קבוצה. **פעולה של G על X** היא פונקציה $G \times X \to X$. כלומר לכל זוג (g, x_1), כאשר $g \in G, x_1 \in X$, מותאם $x_2 \in X$, ומסמנים $gx_1 = x_2$.
הפעולה צריכה לקיים את התנאים הבאים, לכל $x \in X$:

- $(g_1g_2)x = g_1(g_2x)$ לכל $g_1, g_2 \in G$.
- $ex = x$, כאשר e האיבר האדיש ב־G.

3.1 אינטואיציות

כאשר X היא החבורה G בעצמה, הפעולה של G על G מוכרת כבר כפעולה מהצורה $g_1g_2 = g_3$ ־ הכפלת איברים בתוך החבורה.
בפעולה על קבוצה, הטווח והתחום מורחבים לקבוצה כלשהי, והאקסיומות שמגדירות חבורה מורחבות בהתאמה:

1. סגירות ־ לפי ההגדרה, תמונת הפעולה של G על איבר מ־X היא איבר מ־X.
2. אסוציאטיביות ־ כפי ש־$(g_1g_2)g_3 = g_1(g_2g_3)$, כך בפעולה על קבוצה $(g_1g_2)x = g_1(g_2x)$.
3. קיום איבר אדיש ־ $ex = x$ כפי ש־$eg = g$.
4. קיום איבר הופכי ־ כאן ההרחבה פחות דומה, שהרי לא מוגדרים איברים הופכיים ב־X. ואולם עדיין פעולת g^{-1} 'מבטלת' את פעולת g: $g^{-1}(gx) = x$.

אקסיומות החבורה מבטיחות מבנה עם תכונות מסוימות, שנוחות ושימושיות במקרים רבים. משום כך טבעי שנרצה למצוא מקרים שיהיו בהם תכונות דומות.

כעת נראה הקבלות נוספות מתכונות של חבורה לתכונות של פעולות חבורה על קבוצה.

3.2 מסלולים

הגדרה 3.2 לכל $x \in X$ יוגדר **המסלול של x תחת** G כקבוצה $orb_G(x) = \{gx | g \in G\}$.

טענה 3.3 המסלולים מחלקים את X למחלקות שקילות.

הוכחה: יהיו $x_1, x_2 \in X$. נגדיר $x_1 \sim x_2$ אם הם באותו מסלול, כלומר קיים $g \in G$ כך ש־$x_1 = gx_2$. נראה שזה יחס שקילות:
רפלקסיבי ־ $ex = x$.
סימטרי ־ $x_1 = gx_2 \implies x_2 = g^{-1}x_1$.
טרנזיטיבי ־ $x_2 = g_1x_1,\ x_3 = g_2x_2 \implies x_3 = g_2g_1x_1$. □

הקבוצה X מחולקת למסלולים, שמכסים את כל הקבוצה ואין בינהם חפיפה, באופן שמזכיר את החלוקה של G לקוסטים (אם כי המסלולים לא בהכרח שווים בגודלם, בשונה מהקוסטים).
יש גם לשים לב שכל מסלול הוא קבוצה שסגורה לפעולות של החבורה: הפעלת החבורה על איבר מהמסלול תחזיר איבר מהמסלול.

הגדרה 3.4 תהי G חבורה שפועלת על קבוצה X. לכל $x \in X$, הקבוצה $stab_G(x) = \{g \in G | gx = x\}$ נקראת **המייצב של** x.

אפשר לראות הגדרה זו כמקבילה להגדרת הגרעין של הומומורפיזם. בסימונים של הגדרות 2.21 ו־2.22, הגרעין מכיל את האיבר האדיש של G, וכל איבריו מועתקים כמוהו. גם המייצב מכיל את האדיש של G, וכל איברי המייצב פועלים כמוהו.

טענה 3.5 המייצב הוא תת־חבורה של G.

הוכחה: יהיו $g_1, g_2 \in stab_G(x)$, ז"א $g_1x = x, g_2x = x$.
סגירות ־ $g_1g_2 \in stab_G(x) \implies (g_1g_2)x = g_1(g_2x) = g_1x = x$.
איבר הופכי ־ $g^{-1} \in stab_G(x) \implies g^{-1}x = g^{-1}gx = gg^{-1}x = ex$. □

לגרעין יש תכונה דומה ־ הוא מהווה תת־חבורה נורמלית.

ההקבלה הבאה תהיה לחבורת המנה של הגרעין, ולשימוש שלה במשפט האיזומורפיזם הראשון.

משפט 3.6 תהי G חבורה סופית שפועלת על קבוצה X, $x \in X$.
לכל אחד מאברי הקבוצה, גודל החבורה שווה למכפלת גודל המייצב בגודל המסלול:
$|G| = |orb_G(x)| \cdot |stab_G(x)|$.

הוכחה: נסמן $S = stab_G(x)$.
נתבונן בקבוצה $\{gS|g \in G\}$ ־ אוסף הקוסטים של המייצב. נראה שקיימת התאמה חח"ע ועל בין הקוסטים השונים של המייצב לאיברי המסלול $orb_G(x)$.
לכל $s \in S$ מתקיים, לפי הגדרת המייצב, $sx = x$.
יהי gS קוסט של המייצב.
הכפלת x בכל איבר שהוא מקוסט זה תחזיר אותה תוצאה:
$\forall gs \in gS : gsx = g(sx) = gx$.
מאידך, הכפלה באיבר מקוסט אחר ־ $hs \in hS \neq gS$ ־ בהכרח תחזיר איבר אחר במסלול:
$hsx = gsx \iff (hs)^{-1}(gs)x = x \iff (hs)^{-1}(gs) \in S$,
ולפי טענה 2.16 זה יקרה אם"ם gs ו־hs שייכים לאותו קוסט.
קיבלנו שלכל קוסט של המייצב מותאם איבר אחד מהמסלול, שייחודי לו.
לפי המסקנה ממשפט לגרנז', $|G| = |S| \cdot |G : S|$. הוכחנו כעת ש־$|G : S| = |orb_G(x)|$, ולכן $|G| = |S| \cdot |orb_G(x)|$. □

מסקנה 3.7 המייצבים של איברים מאותו מסלול הם בגודל זהה.

4 משפטי סילו

כפי שראינו, משפט לגרנז' הציב תנאי הכרחי לקיום תת־חבורה. משפטי סילו משלימים אותו, כשהם מציגים תנאים מספיקים לכך.

4.1 משפט סילו, חלק ראשון

משפט 4.1 (חלק ראשון של משפט סילו) אם p מספר ראשוני ו־p^α מחלק את סדר החבורה, אז יש לה תת־חבורה מסדר p^α.

הוכחה: לפי הנתון $p^\alpha \mid |G|$, ואפשר לכתוב $|G| = p^{\alpha+r}c$, כאשר $r \geq 0$ ו־$p \nmid c$.
תהי $\mathcal{M}$ קבוצת כל תת־הקבוצות בנות p^α איברים של G. בקבוצה זו יש

$$|\mathcal{M}| = \binom{|G|}{p^\alpha} = \binom{p^{\alpha+r}c}{p^\alpha}$$

איברים.

נעבור כעת לחישוב עזר של המחלקים של $|\mathcal{M}|$.
נסמן $m = p^r c$. בסימון זה
$\binom{p^\alpha m}{p^\alpha} = \frac{(p^\alpha m)!}{(p^\alpha)!(p^\alpha m - p^\alpha)!}$
$= \frac{p^\alpha m(p^\alpha m-1)\dots(p^\alpha m-p^\alpha+1)(p^\alpha m-p^\alpha)\dots(p^\alpha m-p^\alpha m+1)}{(p^\alpha)!(p^\alpha m-p^\alpha)\dots(p^\alpha m-p^\alpha m+1)} =$
$= \frac{p^\alpha m(p^\alpha m-1)\dots(p^\alpha m-p^\alpha+1)}{(p^\alpha)!}$
$= m\frac{p^\alpha m-1}{p^\alpha-1} \cdot \frac{p^\alpha m-2}{p^\alpha-2} \dots \frac{p^\alpha-p^\alpha+1}{1}$
נתבונן בביטוי $\frac{p^\alpha m-k}{p^\alpha-k}$, כאשר $0 < k < p^\alpha$, ונראה שאין הוא מתחלק ב־p.
נניח שהמכנה מתחלק ב־p^i, כאשר $i \leq \alpha$ שלם.
$p^\alpha m - k = p^\alpha(m-1) + p^\alpha - k$
המחובר הימני מתחלק ב־p^i לפי ההנחה. ברור שגם המחובר השמאלי מתחלק ב־p^i. לכן גם הביטוי באגף השמאלי מתחלק ב־p^i.
נניח כעת כי $p^i|(p^\alpha m - k)$:
$\frac{p^\alpha m-k}{p^i} = \frac{p^\alpha-k}{p^i} + (m-1)p^{\alpha-i}$ אגף שמאל שלם לפי ההנחה. ברור שגם המחובר הימני שלם, ולכן גם המחובר השמאלי הוא מספר שלם, ז"א $p^i|(p^\alpha - k)$.
קבלנו שהמונה והמכנה בביטוי $\frac{p^\alpha m-k}{p^\alpha-k}$ מתחלקים באותן חזקות של p, ולכן השבר $\frac{p^\alpha m(p^\alpha m-1)\dots(p^\alpha m-p^\alpha+1)(p^\alpha m-p^\alpha)\dots(p^\alpha m-p^\alpha m+1)}{(p^\alpha)!(p^\alpha m-p^\alpha)\dots(p^\alpha m-p^\alpha m+1)}$, אינו מתחלק ב־$p$. משום כך שמורכב מכפולות שברים כאלה, יתחלק רק בכפולות של p שמחלקות את m, ובפרט ב־p^r, אך לא ב־p^{r+1}.
לסיכום, $p^r \mid \binom{p^{\alpha+r}c}{p^\alpha}$ אך $p^{r+1} \nmid \binom{p^{\alpha+r}c}{p^\alpha}$.

נחזור לגוף ההוכחה.
לפי חישוב העזר, $p^r \mid |\mathcal{M}|$ אך $p^{r+1} \nmid |\mathcal{M}|$.
נגדיר פעולה של G על $\mathcal{M}$ באופן הבא: $\forall g \in G, M \in \mathcal{M}, gM = \{gm | m \in M\}$.
נבדוק שזו אכן פעולת חבורה על קבוצה:
אסוציאטיביות - $\forall g_1, g_2 \in G : (g_1g_2)M = \{(g_1g_2)m | m \in M\} = \{(g_1(g_2m)|m \in M\} = g_1(g_2M)$.
הכפלה באדיש - $eM = M$.
מספר האיברים ב־gM לא שונה ממספרם ב־M, שהרי אם $gm_1 = gm_2$ אז $m_1 = m_2$, ז"א לכל $m \in M$ מותאם איבר אחד $gm \in gM$ שייחודי לו, ולכן $|gM| = |M| = p^\alpha$.
פעולת G על $\mathcal{M}$ מחלקת את $\mathcal{M}$ למסלולים. מאחר ש־$p^{r+1} \nmid |\mathcal{M}|$, קיים לפחות מסלול אחד שמספר איבריו לא מתחלק ב־p^{r+1}.

נתבונן במסלול כזה $\{M_1 \dots M_k\}$, $p^{r+1} \nmid k$, ונחשב את גודל המייצב $stab_G(M_1)$.
לפי משפט 3.6 $|G| = k|stab_G(M_1)| \implies |stab_G(M_1)| = \frac{|G|}{k} = \frac{p^{\alpha+r}c}{k} \geq p^\alpha$.
יהיו $s \in stab_G(M_1)$, $m_1 \in M_1$. לפי הגדרת המייצב, $sM_1 = M_1$, ומכאן $sm_1 \in M_1$.
$s_1 \cancel{m_1} = s_2 \cancel{m_1} \implies s_1 = s_2$ ז"א לכל $s_i \in stab_G(M_1)$ מותאם איבר אחד $s_i m_1 \in M_1$ שייחודי לו. לכן $|stab_G(M_1)| \leq |M_1| = p^\alpha$.
צירוף שני אי־השיוויונים נותן $p^\alpha = |stab_G(M_1)|$.
קיבלנו שיש ב־G תת־חבורה בגודל p^α, ואף מצאנו דרך לבנותה. □

4.2 משפט סילו, חלק שני

הגדרה 4.2 יהיו x, y איברים בחבורה G. נאמר ש־x **צמוד** ל־y אם קיים $g \in G$ כך ש־$y = gxg^{-1}$.
באותו אופן, תת־קבוצה H_1 של G **צמודה** לתת־קבוצה H_2 אם קיים $g \in G$ כך ש־$H_2 = gH_1g^{-1}$.

טענה 4.3 ההצמדה משרה יחס שקילות בקבוצת תת־הקבוצות של G.

טענה 4.4 קבוצה שצמודה לתת־חבורה היא תת־חבורה מאותו גודל.

הוכחה: תהי $H \leq G$.
הקבוצה gHg^{-1} סגורה לפעולה בחבורה, שהרי $(gh_1g^{-1})(gh_2g^{-1}) = g(h_1h_2)g^{-1}$ וזו הצמדה של $h_1h_2 \in H$. האיבר ההופכי של ghg^{-1} הוא $gh^{-1}g^{-1}$. משום כך זוהי תת־חבורה.
לפי חוקי הצמצום $gh_1g^{-1} = gh_2g^{-1}$ אם"ם $h_1 = h_2$, ועל כן הן שוות בגודלן. □

הגדרה 4.5 תת־חבורה בגודל p^α של G, כאשר p ראשוני, $p^\alpha \mid |G|$ אבל $p^{\alpha+1} \nmid |G|$, נקראת **חבורת p־סילו** של G (או תת־חבורה p־סילו).

נסמן ב־S_p את קבוצת כל חבורות p־סילו בחבורה.

משפט 4.6 (חלק שני של משפט סילו) כל תת־חבורה מסדר p^β הינה תת־חבורה של חבורת p־סילו: $\forall K \leq G, |K| = p^\beta, \exists H \in S_p : K \leq H$.

הוכחה: נקח חבורת p־סילו P. P מסדר p^α, ויש לה $n = \frac{|G|}{|P|} = \frac{p^\alpha n}{p^\alpha}$ קוסטים שונים.
אוסף הקוסטים השמאליים של P יסומן ב־$\Omega = \{xP | x \in G\}$.
נגדיר פעולה של K על הקוסטים כך - $\forall k \in K : k \cdot xP = kxP$ ונוודא שמתקיימות הדרישות מפעולה:
אסוציאטיביות - $\forall k_1, k_2 \in K : k_1(k_2x)P = k_1k_2xP = (k_1k_2)xP$.
הכפלה באדיש - $exP = (ex)P = xP$.
K מחלקת את Ω למסלולים. מאחר ש־$|\Omega| = n$ ו־$p \nmid n$, קיים לפחות מסלול אחד, Ω_1, שאורכו אינו מתחלק ב־p: $p \nmid |\Omega_1|$.
אבל ממשפט 3.6 נובע שאורך המסלול מחלק את גודל החבורה, ז"א $|\Omega_1||K| = p^\beta$.
צירוף שתי השורות האחרונות גורר ש־$|\Omega_1| = 1$. זהו מסלול בעל איבר יחיד, שיסומן aP. פעולת החבורה עליו לא משנה אותו - לכל $k \in K$, תמיד $kaP = aP$, או בצורה שקולה $a^{-1}kaP = P$. מהשוויון האחרון נובע ש־$a^{-1}ka \in P$ (כי $a \in H \iff aH = H$), ז"א לכל $k \in K$ יש איבר $p \in P$ שעבורו $a^{-1}ka = p$. מכך נובע כי $k = apa^{-1} \in aPa^{-1}$.
קבלנו שאיברי k מוכלים בתת־החבורה aPa^{-1}, ועל כן K תת־חבורה של aPa^{-1} - חבורת p־סילו בעצמה, לפי טענה 4.4. □

אפשר לבחור K שגודלה $|K| = p^\alpha$ - חבורת p־סילו בעצמה, ומכאן מתקבלת המסקנה הבאה:

מסקנה 4.7 (סילו 2ב) כל תת־החבורות p־סילו של אותה חבורה צמודות זו לזו.

4.3 משפט סילו, חלק שלישי

הגדרה 4.8 הקבוצה $N_G(H) = \{g \in G | gHg^{-1} = H\}$ - כל איברי G שמצמידים את H לעצמה - נקראת ה**מנרמל** של H ב־G.

טענה 4.9 המנרמל $N_G(H)$ של תת־חבורה $H \leq G$ הוא תת־חבורה של G.

הוכחה: רעיון ההוכחה: להגדיר מייצב של H כך שיהיה שווה למנרמל.
תהי Ω קבוצת תת־החבורות הצמודות ל־H: $\Omega = \{gHg^{-1} | g \in G\}$ (טענה 4.4).
G פועלת על Ω באמצעות הצמדה: $g \cdot H = gHg^{-1}$.
המייצב של H הוא $stab_G(H) = \{g \in H : gHg^{-1} = H\} = N_G(H)$.
לפי טענה 3.5, המייצב תת־חבורה של G, ולכן גם המנרמל. □

טענה 4.10 הצמדת תת־חבורה ע"י אחד מאיבריה מחזירה אותה תת־חבורה:
$\forall h \in H : hHh^{-1} = H$.

הוכחה: $hH = H$ בשל סגירות תת־החבורה, וכך גם $Hh^{-1} = H$. □

טענה 4.11 כל תת־חבורה הינה תת־חבורה נורמלית של המנרמל שלה:
$H \leq G \implies H \triangleleft N_G(H)$.

הוכחה: כל איבר $h \in H$ מצמיד את H לעצמה - $hHh^{-1} = H$ (טענה 4.10), ולכן $H \subseteq N_G(H)$.
לפי הגדרת המנרמל, לכל $g \in N_G(H)$ מתקיים $gHg^{-1} = H$, ז"א H נורמלית ב־$N_G(H)$. □

טענה 4.12 בחבורה יש חבורת p־סילו יחידה אם"ם בחבורה יש חבורת p־סילו נורמלית:
$|S_p| = 1 \iff \exists N \in S_p, N \triangleleft G$.

הוכחה: נניח שקיימת חבורת p־סילו נורמלית. לפי מסקנה 4.7, כל חבורות p־סילו צמודות זו־לזו. אבל הצמדת תת־חבורה נורמלית מחזירה אותה תת־חבורה, ולכן היא חבורת p־סילו היחידה.

נניח שיש רק חבורת p־סילו אחת, N. הצמדתה ע"י $g \in G$ תתן תת־חבורה מאותו גודל (טענה 4.10) - חבורת p־סילו בעצמה. אבל יש רק חבורת p־סילו אחת, ועל כן $\forall g \in G : gNg^{-1} = N$, ז"א N נורמלית. □

טענה 4.13 לכל חבורת p־סילו ב־G, אינדקס המנרמל שווה למספר החבורות p־סילו ב־G:
$\forall P \in S_p : |S_p| = |G : N_G(P)|$.

הוכחה: נגדיר פעולה של G על איברי S_p באמצעות הצמדה:
$\forall g \in G, \forall P \in S_p : g \cdot P = gPg^{-1}$.
הצמדת P באמצעות $n \in N_G(P)$ נותנת שוב את P.
הצמדה באמצעות $g = nx_1$ - איבר מהקוסט הימני של המנרמל $N_G(P)x_1$ - נותנת חבורת p־סילו $P_1 = nx_1P(nx_1)^{-1}$ (טענה 4.4). באותו האופן P_2 מתקבלת מהצמדה באמצעות nx_2.
$P_1 = P_2$ אם"ם x_1, x_2 נציגים של אותו קוסט - $N_G(P)x_1 = N_G(P)x_2$:
$P_1 = P_2 \iff (nx_1)P(nx_1)^{-1} = (nx_2)P(nx_2)^{-1}$

$\iff P = (nx_2)^{-1}(nx_1)P(nx_1)^{-1}(nx_2) \iff (nx_2)^{-1}(nx_1) \in N_G(P)$
ולפי טענה 2.16 זה יקרה אם"ם nx_2 ו־nx_1 שייכים לאותו קוסט.
קבלנו שכל חבורות p־סילו השונות מתקבלות מהצמדות באיברים מקוסטים ימניים שונים של המנרמל. זוהי התאמה חח"ע ועל בין חבורות p־סילו לקוסטים של המנרמל, ועל כן מספרם שווה. □

משפט 4.14 (חלק שלישי של משפט סילו) יהי $|S_p|$ מספר החבורות p־סילו ב־G, $|G| = p^\alpha n$, $p \nmid n$. אזי:
א. $|S_p| \equiv 1 \pmod{p}$
ב. $|S_p| \mid n$.

הוכחה: [הוכחת סילו 3א] רעיון ההוכחה: מוציאים חבורת p־סילו אחת Q מ־S_p, ומראים שמספר הנותרות מתחלק ב־p. הכלי השימושי לכך הוא משפט 3.6. לצורך כך מגדירים פעולה של Q על $S_p \setminus \{Q\}$. לפי משפט זה המסלולים מתחלקים ב־$|Q| = p^\alpha$.
אם אין מסלול בגודל יחידה, סיימנו.
את האפשרות השניה שוללים באמצעות טענה 4.12, כשמצטמצמים למנרמל של הקבוצה במסלול.

תהי $Q \in S_p$. Q פועלת על $S_p^* = S_p \setminus \{Q\}$ באמצעות הצמדה:
$\forall q \in Q, \forall P \in S_p^* : q \cdot P = qPq^{-1}$.
האם זו פעולה? נוודא ש־Q לא מתקבל בטעות:
נניח בשלילה $qPq^{-1} = Q \implies P = q^{-1}Qq$. אבל מטענה 4.10 $q^{-1}Qq = Q$ וזה יקרה רק אם $P = Q$.
הפעולה מחלקת את S_p^* למסלולים. לפי משפט 3.6 אורך כל מסלול חייב להיות מחלק של $|Q| = p^\alpha$. אם אין מסלול באורך יחידה, אז S_p^* מורכבת מאיחוד מסלולים זרים שאורכם מתחלק ב־p, ועל כן $p \mid |S_p^*|$, וסיימנו.
נניח בשלילה שיש מסלול ב־S_p^* שמכיל רק איבר אחד P,
ז"א $\forall q \in Q : q \cdot P = P \iff qPq^{-1} = P$,
כלומר כל איברי q מצמידים את P לעצמה, ולכן $Q \leq N_G(P)$. מאידך $P \triangleleft N_G(P)$ (טענה 4.11).
כדי להשתמש בטענה 4.12, 'נצטמצם' ל־$N_G(P)$. נמצא את גודל $N_G(P)$:
$P \leq N_G(P) \implies p^\alpha = |P| \mid |N_G(P)|$
$N_G(P) \leq G \implies |N_G(P)| \mid |G| = p^\alpha n$
צירוף שתי השורות האחרונות גורר ש־$N_G(P) = p^\alpha k, k|n, p \nmid k$.
קבלנו את תנאי טענה 4.12, שלפיה לא תתכנה יותר מחבורת p־סילו אחת ב־$N_G(P)$. מכאן שלא יתכן ש־P וגם Q תת־חבורות נפרדות של $N_G(P)$, ז"א $P = Q$, כלומר אין מסלול בגודל יחידה. □

הוכחה: [הוכחת סילו 3ב] לפי טענה 4.13, $|S_p| = \frac{|G|}{|N_G(P)|}$. נציב $|G| = |P| \cdot n$, ונקבל $\frac{n}{|S_p|} = \frac{|N_G(P)|}{|P|}$.
P תת־חבורה של $N_G(P)$ (טענה 4.11) ועל כן הביטוי האחרון חייב להיות מספר שלם. □

5 נספח: יישום של משפטי סילו

נציג כאן תנאי, שמתקבל בשימוש במשפטי סילו, לכך שעבור סדר מסוים קיימת רק חבורה אחת.

טענה 5.1 לשתי תת־חבורות, שסדריהן מספרים ראשוניים שונים, משותף האיבר האדיש בלבד.

הוכחה: תהיינה $H = \langle h\rangle, K = \langle k\rangle$ תת־חבורות של G, $|H| = p, |K| = q$, p ו־q מספרים ראשוניים שונים.
$h^a = k^b \implies (h^a)^p = (k^b)^p \implies k^{bp} = e = k^q \implies q|bp \implies q|b \implies h^a = k^b = e$.
□

טענה 5.2 מכפלות איברים שונים של תת־חבורות כאלו שבטענה 5.1, שונות זו מזו:
$h^a k^b = h^c k^d \iff h^a = h^c, k^b = k^c$.

הוכחה: $h^a k^b = h^c k^d \iff h^{a-c} = k^{d-b}$ ולפי הטענה הקודמת זה יקרה אם"ם $h^{a-c} = e = k^{d-b}$, זו"א $h^a = h^c, k^b = k^c$.
□

טענה 5.3 יש רק חבורה אחת (עד כדי איזומורפיזם) מסדר pq, כאשר $p > q$, p ו־q מספרים ראשוניים שונים, ולא קיים $v > 1$ שלם שעבורו $1 + vq$ מחלק של p.

הוכחה: תהי $|G| = pq$, p ו־q מספרים ראשוניים שונים, $p > q$.
לפי משפט 4.1 יש לה חבורת p־סילו וחבורת q־סילו.
לפי משפט 4.14, $|S_p| = 1 + up$ וכן $q \mid |S_p|$. אך מכיוון ש־$p > q$, יש רק חבורת p־סילו אחת, והיא נורמלית לפי טענה 4.12.
שוב בשימוש באותו משפט, $|S_q| = 1 + vq$, $p \mid |S_q|$.
נתייחס למקרה בו לא קיים $v > 1$ שלם שעבורו $1 + vq$ מחלק של p, ואז יש ב־G חבורת q־סילו יחידה, גם היא נורמלית.
מאחר ש־p ו־q ראשוניים, חבורות סילו המתאימות להם תהיינה צקליות (טענה 2.12), ואפשר לסמנן ב־ $H = \{e, h, h^2, \ldots, h^{p-1}\},\ K = \{e, k, k^2, \ldots, k^{q-1}\}$.
נבחן את הקוסטים של תת־החבורות.
לקוסטים $Hk = \{k, hk, h^2k, \ldots, h^{p-1}k\}$ ו־$hK = \{h, hk, hk^2, \ldots, hk^{q-1}\}$ יש, לפי טענה 5.2 איבר משותף יחיד hk.
באותו האופן, ל־$kH = \{k, kh, kh^2, \ldots, kh^{p-1}\}$ ו־$Kh = \{h, kh, k^2h, \ldots, k^{q-1}h\}$ איבר משותף יחיד kh. ואולם, K ו־H נורמליות, זו"א $Kh = hK, kH = Hk$. דבר זה מוביל למסקנה כי $hk = kh$.
מאחר שכל איבר בחבורה מסדר ראשוני (למעט האיבר האדיש) הוא יוצר שלה, מסקנה זו נכונה לכל איברי חבורות סילו של G.
נתבונן כעת בקבוצה $\{h^a k^b | a = 0, 1, \ldots, p-1,\ b = 0, 1, \ldots, q-1\} \subseteq G$. לפי טענה 5.2 כל איבריה שונים זה־מזה, ועל כן יש בה pq איברים שונים, כמספר האיברים ב־G. לכן קבוצה זו שווה ל־G, וכל איבר ב־G יכול להכתב בצורה $h^a k^b$.
קל לראות כעת שכל שני איברים $h^a k^b, h^c k^d \in G$ מתחלפים בינהם בכפל, ומכאן ש־G חבורה אבלית. מכך נובע בפרט כי $\forall n \in \mathbb{Z} : (hk)^n = h^n k^n$.
כדי לבדוק האם יש יוצר ל־G, נבדוק את המשוואה $(hk)^n = e$:
$(hk)^n = h^n k^n = e = h^0 k^0$.
לפי טענה 5.2 זה יקרה אם"ם $p|n$ וגם $q|n$. מאחר ש־p ו־q זרים, זה יקרה אם"ם $pq|n$. זו"א $(hk)^n = e \iff pq|n$.
קבלנו ש־hk יוצר של G. לכן G צקלית, ועד כדי איזומורפיזם יש רק חבורה אחת כזו מכל סדר.
□

6 מקורות

1. I N Herstein, Topics in Algebra, Second Edition, שמכיל הסברים ומבואות מאירי עיניים.
2. פרופ׳ ג׳ון ווילסון, סיכומי הרצאות שנכתבו ע״י ד״ר מרק ברמן.
3. הבלוג של גדי אלכסנדרוביץ׳, ״לא מדויק״, gadial.net, שמספק תובנות מועילות.
4. ויקיפדיה העברית, he.wikipedia.org.