תורת החבורות - הוכחות נבחרות

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

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.

הוכחה. נוכיח תחילה שלכל איבר, האיבר ההופכי השמאלי הוא גם הופכי ימני; יהי $a\in A$ ויהיו $b,c\in A$ כך ש-$b*a=e$ ו-$c*b=e$, מכאן שמתקיים:

$$\begin{aligned}a*b&=e*(a*b)=(c*b)*(a*b)=c*(b*(a*b))\\&=c*((b*a)*b)=c*(e*b)=c*b=e\end{aligned}$$

a הנ"ל היה שרירותי ולכן לכל $a\in A$ קיים $b\in A$ כך ש-$a*b=e=b*a$.
מכאן שלכל $a\in A$ קיים $b\in A$ כך שמתקיים:

$$a*e=a*(b*a)=(a*b)*a=e*a=a$$

ומכאן ש-e הוא גם איבר יחידה ימני. ■

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 $a^{|\mathbb{Z}_n^\times|}\equiv 1 \mod n$ (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.

הוכחה. יהי $a\in G$, נסמן $r:=|G|$ ויהיו $g_1,g_2,\ldots,g_r\in G$ כל האיברים ב-G.
מהעובדה שכפל ב-a משמאל הוא תמורה על G נובע כי $G=\{a\cdot g_1,a\cdot g_2,\ldots,a\cdot g_r\}$, ולכן מההנחה ש-$G$ אבלית נובע כי:

$$\prod_{i=1}^{r} g_i=\prod_{i=1}^{r}(a\cdot g_i)=a^r\cdot\prod_{i=1}^{r} g_i$$

וממילא $a^r=e$. ■

טענה 1.7. תהא $G\leqslant H$ 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:

$$\left\{\ g\ \middle|\ \forall H\in X: g\in H\ \right\}$$

חבורות נוצרות וקבוצות יוצרים

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:
$$\left\langle S\right\rangle =\left\{ \prod_{i=1}^{n}s_{i}\ \middle|\ n\in\mathbb{N}_{0},\ \forall n\geq i\in\mathbb{N}\ s_{i}\in S\cup S^{-1}\right\}$$

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

הוכחה. נניח ש-G ציקלית ויהיו $H\leqslant G$ תת-חבורה ו-$g\in G$ כך ש-$G=\left\langle g\right\rangle$.
נסמן $n:=\min\left\{ k\in\mathbb{N}:g^{k}\in H\right\}$, יהי $h\in H$ ויהי $m\in\mathbb{N}$ כך ש-$h=g^{m}$; יהיו $q,r\in\mathbb{Z}$ כך שמתקיים $m=q\cdot n+r$ ו-$0\leq r<n$ (חילוק עם שארית).
$$\Rightarrow h=g^{m}=g^{q\cdot n+r}=g^{q\cdot n}\cdot g^{r}=\left(g^{n}\right)^{q}\cdot g^{r}$$
$$\Rightarrow g^{r}=\left(\left(g^{n}\right)^{q}\right)^{-1}\cdot h=\left(\left(g^{n}\right)^{-1}\right)^{q}\cdot h\in H$$
מהגדרת n נובע ש-$r=0$ ולכן $h=\left(g^{n}\right)^{q}$, כלומר $h\in\left\langle g^{n}\right\rangle$; h הנ"ל היה שרירותי ומכאן ש-$H\subseteq\left\langle g^{n}\right\rangle$, ולכן גם $H=\left\langle g^{n}\right\rangle$. ■

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

הוכחה. נסמן $r:=\left|g\right|$, מהגדרת הסדר של g נובע שלכל $i,j\in\mathbb{N}$ $r>$ כך ש-$i\neq j$ מתקיים $g^{i}\neq g^{j}$ (אחרת נניח בהג"כ ש-$i>j$ ונקבל ש-$g^{i-j}=e$ בסתירה להגדרת r).
מכאן ש-$\left|\left\langle g\right\rangle \right|\geq r$, מצד שני הקבוצה $\left\{ e,g,g^{2},\ldots,g^{r-1}\right\}$ סגורה לכפל ולהופכי: לכל $i,j\in\mathbb{N}$ $r>$ כך ש-$i+j\geq r$ מתקיים $g^{i+j}=g^{i+j-r}$ ו-$i+j-r<r$, וכמו כן לכל $i\in\mathbb{N}$ מתקיים $g^{r-i}\cdot g^{i}=e$ ו-$r-i<r$. ■

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

הוכחה. יהי $m\in\mathbb{Z}$, ויהיו $q,r\in\mathbb{Z}$ כך ש-$m=q\cdot n+r$ ו-$0\leq q<r$.
$$\Rightarrow g^{m}=g^{q\cdot n+r}=g^{q\cdot n}\cdot g^{r}=\left(g^{n}\right)^{q}\cdot g^{r}=e^{q}\cdot g^{r}=e\cdot g^{r}=g^{r}$$
מהגדרת n נובע ש-$g^{m}=e$ אם"ם $r=0$, כלומר $g^{m}=e$ אם"ם $n\mid m$. ■

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

הוכחה. נסמן $n:=\left|g\right|$ ו-$m:=\left|h\right|$ ויהיו $q_{1},q_{2}\in\mathbb{N}$ כך שמתקיים $\text{lcm}\left(n,m\right)=q_{1}\cdot n$ ו-$\text{lcm}\left(n,m\right)=q_{2}\cdot m$.
$$\Rightarrow\left(gh\right)^{\text{lcm}\left(n,m\right)}=g^{\text{lcm}\left(n,m\right)}\cdot h^{\text{lcm}\left(n,m\right)}=\left(g^{n}\right)^{q_{1}}\cdot\left(g^{m}\right)^{q_{2}}=e^{q_{1}}\cdot e^{q_{2}}=e$$
מכאן ש-$\left|gh\right|$ סופי, ומהלמה האחרונה (1.13) נובע ש-$\left|gh\right|$ גם מחלק את $\text{lcm}\left(n,m\right)$. ■

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 $Hg = C$.

הוכחה. נניח ש-C היא מחלקה שמאלית של H, יהי $a \in G$ כך ש-$C = aH$.
לכל $g \in C$ קיים $h \in H$ כך ש-$g = ah$ ולכן גם $gH = ghH = aH = C$.
ההוכחה עבור מחלקה ימנית דומה למדי. ■

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. $b \in Ha$.

הוכחה. הפסוק הראשון והפסוק השני נובעים זה מזה ע"י העברת אגף, הפסוק השני והפסוק השלישי נובעים זה מזה אם זוכרים ששתי מחלקות מאותו סוג (ימניות/שמאליות) הן שוות או זרות (מסקנה 2.2), ומאותה סיבה גם הפסוק הראשון והפסוק הרביעי שקולים זה לזה. ∎

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).

הוכחה. מהיות H חבורה בפני עצמה נובע שלכל $g \in G$ מתקיים:

$$(gH)^{-1} = \left\{(gh)^{-1} \mid h \in H\right\} = \left\{h^{-1}g^{-1} \mid h \in H\right\} = \left\{h^{-1} \mid h \in H\right\} \cdot g^{-1} = Hg^{-1}$$
$$(Hg)^{-1} = \left\{(hg)^{-1} \mid h \in H\right\} = \left\{g^{-1}h^{-1} \mid h \in H\right\} = g^{-1} \cdot \left\{h^{-1} \mid h \in H\right\} = g^{-1}H$$

∎

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).

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

2.2 תתי-חבורות נורמליות

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

הוכחה. תהא $N \leqslant G$ תת-חבורה כך ש-$[G:N]=2$ (אם אין כאלה הטענה נכונה באופן ריק).
ל-N יש בדיוק שתי חבורות שמאליות שאחת מהן היא N עצמה, וכמו כן יש ל-N בדיוק שתי מחלקות ימניות שאחת מהן היא N עצמה; מהעובדה ש-G היא איחוד זר הן של המחלקות הימניות והן של השמאליות (מסקנה 2.3) נובע שהמחלקה השמאלית של N שאינה N עצמה היא גם המחלקה השמאלית של N שאינה N עצמה, מכאן שלכל $g \in G$ מתקיים $gN = Ng$, כלומר N 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!

הוכחה. הגרירה מימין לשמאל טריוויאלית; כדי להוכיח את הגרירה ההפוכה יש לזכור ש-G היא איחוד זר הן של המחלקות הימניות והן של השמאליות של N (מסקנה 2.3), ולכן מהשוויון $G/N = N\backslash G$ נובע ש-$gN = Ng$ לכל $g \in G$. ■

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

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

הוכחה. יהיו $h \in H$ ו-$k \in K$, לכל $a, b \in H \cap K$ כך ש-$a \neq b$ מתקיים:

$$(ha)\left(a^{-1}k\right) = hk = (hb)\left(b^{-1}k\right)$$

$$ha \neq hb \qquad\qquad a^{-1}k \neq b^{-1}k$$

מכאן שלכל איבר ב-HK יש לפחות $|H \cap K|$ הצגות שונות כמכפלה של איבר ב-H עם איבר ב-K.
מצד שני, לא קיימות הצגות נוספות מפני שלכל $\tilde{h} \in H$ ולכל $\tilde{k} \in K$ כך ש-$hk = \tilde{h}\tilde{k}$ מתקיים $g := h^{-1}\tilde{h} = k\tilde{k}^{-1} \in H \cap K$ ולכן גם:

$$hk = (hg)\left(g^{-1}k\right) = \left(h \cdot h^{-1}\tilde{h}\right)\left(\tilde{k}k^{-1} \cdot k\right) = \tilde{h}\tilde{k}$$

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

■

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

הוכחה.

- $\Leftarrow$
  נניח ש-$HK \leqslant G$, ויהיו $h \in H$ ו-$k \in K$.
  מהיות H ו-K תתי-חבורות נובע ש-$h^{-1} \in H$ ו-$k^{-1} \in K$, ולכן מההנחה ש-HK היא תת-חבורה ומהעובדה ש-$h^{-1}k^{-1} \in HK$ נובע כי:
  $$kh = \left((kh)^{-1}\right)^{-1} = \left(h^{-1}k^{-1}\right)^{-1} \in HK$$
  מצד שני, מההנחה ש-HK היא תת-חבורה נובע שקיימים $\tilde{h} \in H$ ו-$\tilde{k} \in K$ כך ש-$\tilde{h}\tilde{k} = (hk)^{-1}$, ומהיות H ו-K תתי-חבורות נובע ש-$\tilde{h}^{-1} \in H$ ו-$\tilde{k}^{-1} \in K$ ולכן גם:
  $$hk = \left((hk)^{-1}\right)^{-1} = \left(\tilde{h}\tilde{k}\right)^{-1} = \tilde{k}^{-1}\tilde{h}^{-1} \in KH$$
  h ו-k הנ"ל היו שרירותיים ולכן מתקיים $HK = KH$.
- $\Rightarrow$
  נניח ש-$HK = KH$.
  מהגדרה $e \in HK$ (כי $e \in H$ ו-$e \in K$), כמו כן לכל $h_1, h_2 \in H$ ולכל $k_1, k_2 \in K$ מתקיים:
  $$h_1k_1h_2k_2 = h_1\left((k_1h_2)^{-1}\right)^{-1}k_2 = h_1\left(h_2\right)^{-1} \cdot \left(k_1\right)^{-1}k_2 \in HK$$
  ובנוסף, לכל $h \in H$ ולכל $k \in K$ מתקיים $(hk)^{-1} = k^{-1}h^{-1} \in KH = HK$.

■

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

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. $x, y, z \in X$.

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

♣ 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.

הוכחה. יהי $x\in X$. מהגדרה $e\in G_x$, כמו כן מהאסוציאטיביות של הפעולה נובע שלכל $a,b\in G_x$ מתקיים:

$$ab.x=a.(b.x)=a.x=x$$
$$a^{-1}.x=a^{-1}.(a.x)=a^{-1}a.x=e.x=x$$

ולכן גם $ab,a^{-1}\in G_x$. ■

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-$O(x)$ (המסלול של x), ולכן ע"פ הגדרה מתקיים $[G:G_x]=|O(x)|$; בפרט אם G סופית אז ע"פ משפט לגראנז' מתקיים:

$$|O(x)|=\frac{|G|}{|G_x|}$$

הוכחה. יהי $x\in X$, ותהא $f:G/G_x\to O(x)$ פונקציה המוגדרת ע"י (לכל $a\in G$):

$$f(aG_x):=a.x$$

נשים לב לכך שלכל $a,b\in G$ כך ש-$aG_x=bG_x$ קיים $g\in G_x$ כך ש-$b=ag$ ולכן גם:

$$b.x=ag.x=a.(g.x)=a.x$$

ומכאן ש-f אכן מוגדרת היטב.
מהגדרה f על $O(x)$ ולכן נותר לנו להוכיח ש-f חח"ע.
לכל $a,b\in G$ מתקיים:

$$\begin{aligned}f(aG_x)=f(bG_x)&\longleftrightarrow a.x=b.x\longleftrightarrow b^{-1}.(a.x)=b^{-1}.(b.x)\\&\longleftrightarrow b^{-1}a.x=b^{-1}b.x=e.x=x\\&\longleftrightarrow b^{-1}a\in G_x\longleftrightarrow aG_x=bG_x\end{aligned}$$

ומכאן ש-f חח"ע. ■

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

♣ זהו סימון מקובל עבור קבוצת נקודות השבת של פונקציה.

משפט 3.6. הלמה של ברנסייד[2]

נניח ש-G ו-X סופיות, מתקיים:

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

הוכחה. נסמן $A:=\{(g,x)\in G\times X\mid g.x=x\}$, ממשפט מסלול-מייצב נובע כי:

$$\Rightarrow\frac{1}{|G|}\cdot\sum_{g\in G}|\mathrm{Fix}(g)|=\frac{|A|}{|G|}=\sum_{x\in X}\frac{|G_x|}{|G|}=\sum_{x\in X}\frac{1}{|O(x)|}$$

נזכור ש-X היא איחוד זר של המסלולים (מסקנה 3.2), ולכן בסכום שבאגף שמאל כל מסלול מופיע במספר נסכמים השווה לגודלו, כלומר כל מסלול "תורם" 1 לסכום הנ"ל ולכן הסכום שווה למספר המסלולים שהוא $|G\backslash X|$. ■

[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.

הוכחה. לכל $g\in G$ ולכל $h\in H$ מתקיים $gh=hg\iff ghg^{-1}=g$, מכאן ש-$Z(G)=\left\{g\in G\mid\forall h\in G\ g=hgh^{-1}\right\}$. ■

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):

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

הוכחה. ממשפט מסלול-מייצב נובע שלכל $g\in G$, הגודל של מחלקת הצמידות של g הוא:

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

G ניתנת להצגה כאיחוד זר של מחלקות הצמידות שלה (מסקנה 3.2), ולכן מתקיים:

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

בטענה הקודמת (3.7) ראינו שלכל $g\in Z(G)$, הגודל של מחלקת הצמידות של g הוא 1, ומכאן שמתקיים:

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

■

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

הוכחה. תהא $N\leqslant G$ תת-חבורה.

- $\Leftarrow$
  נניח ש-N נורמלית, בפרט N סגורה להצמדות ולכן לכל $n\in N$ מחלקת הצמידות של n מוכלת ב-N; מכאן ש-N היא איחוד של מחלקות הצמידות של כל האיברים שבה.

- $\Rightarrow$
  נניח ש-N ניתנת להצגה כאיחוד של מחלקות צמידות, ויהי $g\in G$.
  מההנחה ש-N היא איחוד של מחלקות צמידות נובע שלכל $n\in N$ מתקיים $gng^{-1}\in N$ (כלומר $gNg^{-1}\subseteq N$), ומצד שני נובע ממנה שלכל $n\in N$ קיים $n'\in N$ כך ש-$gn'g^{-1}=n$ (כלומר $gNg^{-1}\supseteq N$).
  מכאן ש-$gNg^{-1}=N$, ומכיוון ש-g היה שרירותי נדע שלכל $g\in G$ מתקיים $gNg^{-1}=N$, כלומר N נורמלית.

■

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:

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

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

הוכחה. נובע ממשפט מסלול מייצב עבור פעולת G על אוסף תתי-החבורות שלה ע"י הצמדה: המייצב הוא המנרמל, והמסלול הוא הקבוצה הנ"ל. ■

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 $\varphi\left(g^{-1}\right) = (\varphi(g))^{-1}$.

הוכחה. מתקיים $\varphi(e_G) = \varphi(e_G \cdot e_G) = \varphi(e_G) \cdot \varphi(e_G)$, ומכאן שגם:

$$e_H = (\varphi(e_G))^{-1} \cdot \varphi(e_G) = (\varphi(e_G))^{-1} \cdot \varphi(e_G) \cdot \varphi(e_G) = \varphi(e_G)$$

כמו כן לכל $g \in G$ מתקיים:

$$e_H = \varphi(e_G) = \varphi\left(g^{-1} \cdot g\right) = \varphi\left(g^{-1}\right) \cdot \varphi(g)$$

ולכן מיחידות ההופכי נובע ש-$\varphi\left(g^{-1}\right) = (\varphi(g))^{-1}$. ■

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

הוכחה. מהטענה הקודמת (4.2) נובע ש-$e_G \in \ker\varphi$ ו-$e_H \in \mathrm{Im}\varphi$, וכן שלכל $g \in \ker\varphi$ מתקיים $g^{-1} \in \ker\varphi$ ולכל $h \in \mathrm{Im}\varphi$ מתקיים $h^{-1} \in \mathrm{Im}\varphi$.
בנוסף, לכל $a, b \in \ker\varphi$ מתקיים:

$$\varphi(ab) = \varphi(a) \cdot \varphi(b) = e_H \cdot e_H = e_H$$

ולכן $ab \in \ker\varphi$. וכמו כן לכל $a, b \in \mathrm{Im}\varphi$ קיימים $x, y \in G$ כך ש-$\varphi(x) = a$ ו-$\varphi(y) = b$, ועבורם מתקיים:

$$ab = \varphi(x) \cdot \varphi(y) = \varphi(xy)$$

ומכאן ש-$ab \in \mathrm{Im}\varphi$.
עד כאן הוכחנו ש-$\ker\varphi \leqslant G$ ו-$\mathrm{Im}\varphi \leqslant H$, כעת נוכיח ש-$\ker\varphi$ היא תת-חבורה נורמלית של G.
לכל $a \in \ker\varphi$ ולכל $g \in G$ מתקיים:

$$\varphi\left(gag^{-1}\right) = \varphi(g) \cdot \varphi(a) \cdot \varphi\left(g^{-1}\right) = \varphi(g) \cdot e_H \cdot (\varphi(g))^{-1} = e_H$$

כלומר $gag^{-1} \in \ker\varphi$, ומכאן ש-$\ker\varphi$ סגורה להצמדות ולכן נורמלית. ■

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 $\ker\varphi=\{e_G\}$.

הוכחה. אם φ חח"ע אז e_G הוא האיבר היחיד ב-G ש-φ מעתיק ל-e_H ולכן מהגדרה $\ker\varphi=\{e_G\}$.
לכל $a,b\in G$ כך ש-$\varphi(a)=\varphi(b)$ מתקיים:

$$\varphi\left(ab^{-1}\right)=\varphi(a)\cdot\varphi(b)=\varphi(a)\cdot(\varphi(b))^{-1}=\varphi(a)\cdot(\varphi(a))^{-1}=e_H$$

ולכן אם $\ker\varphi=\{e_G\}$ אז לכל $a,b\in G$ כך ש-$\varphi(a)=\varphi(b)$ מתקיים $ab^{-1}=e_H$ ולכן גם $a=b$, כלומר φ חח"ע. ■

משפט 4.6. למת הגרעין
לכל $a,b\in G$ מתקיים $\varphi(a)=\varphi(b)$ אם"ם $a\cdot\ker\varphi=b\cdot\ker\varphi$.

הוכחה. יהיו $a,b\in G$.

- $\Leftarrow$
נניח ש-$\varphi(a)=\varphi(b)$, מכאן שמתקיים:

$$\begin{aligned}a\cdot\ker\varphi&=\{ag\mid g\in G,\ \varphi(g)=e_H\}=\left\{g\in G\mid\varphi\left(a^{-1}g\right)=e_H\right\}\\&=\left\{g\in G\mid\varphi\left(a^{-1}\right)\cdot\varphi(g)=e_H\right\}=\left\{g\in G\mid(\varphi(a))^{-1}\cdot\varphi(g)=e_H\right\}\\&=\left\{g\in G\mid(\varphi(b))^{-1}\cdot\varphi(g)=e_H\right\}=\left\{g\in G\mid\varphi\left(b^{-1}\right)\cdot\varphi(g)=e_H\right\}\\&=\left\{g\in G\mid\varphi\left(b^{-1}g\right)=e_H\right\}=\{bg\mid g\in G,\ \varphi(g)=e_H\}=b\cdot\ker\varphi\end{aligned}$$

- $\Rightarrow$
נניח ש-$a\cdot\ker\varphi=b\cdot\ker\varphi$, מכאן ש-$b\in a\cdot\ker\varphi$ ולכן קיים $g\in\ker\varphi$ כך ש-$b=a\cdot g$ וממילא:

$$\varphi(b)=\varphi(a\cdot g)=\varphi(a)\cdot\varphi(g)=\varphi(a)\cdot e_H=\varphi(a)$$

■

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 $\mathrm{Im}\varphi$.

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

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

♣ ראינו בהרצאה (ללא הוכחה) שלכל $n\in\mathbb{N}$ מתקיים $\mathrm{Inn}(S_n)=\mathrm{Aut}(S_n)$ 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-"$.$".

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

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.

הוכחה. נובע ישירות מטענה 4.5. ■

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:

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

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

הוכחה. יהי $a\in\mathrm{Core}_G(K)$, כלומר מתקיים $a\in gKg^{-1}$ לכל $g\in G$.
מכאן שלכל $g\in G$ קיים $k\in K$ כך ש-$a=gkg^{-1}$, וממילא גם: ■

$$a.gK=agK=gkg^{-1}gH=gkK=gK$$

מכאן ש-$a\in\ker\varphi$, ומכיוון ש-a היה שרירותי נדע ש-$\mathrm{Core}_G(K)\subseteq\ker\varphi$.
יהי $b\in\ker\varphi$, כלומר מתקיים $bgK=gK$ לכל $g\in G$. מכאן שלכל $g\in G$ מתקיים $bg\in gK$, ולכן קיים $k\in K$ כך ש-$bg=gk$ וממילא גם $b=gkg^{-1}$, כלומר $b\in gKg^{-1}$.
מכאן ש-$b\in\mathrm{Core}_G(K)$, ומכיוון ש-b היה שרירותי נדע ש-$\mathrm{Core}_G(K)\supseteq\ker\varphi$, וממילא $\mathrm{Core}_G(K)=\ker\varphi$.
העובדה ש$\mathrm{Core}_G(K)$ נורמלית נובעת מטענה 4.3.

משפט 4.16. תהא $K\leqslant G$ תת-חבורה, $\mathrm{Core}_G(K)$ 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 $L\subseteq\mathrm{Core}_G(K)$.

הוכחה. תהא $L\trianglelefteq G$ תת-חבורה נורמלית כך ש-$L\leqslant K$.
לכל $a\in L$ ולכל $g\in G$ קיים $b\in L$ כך שמתקיים $ag=gb$, ולכן גם $agK=gbK=gK$ (כי $b\in L\subseteq K$).
מכאן ש-$L\subseteq\ker\varphi$, כאשר φ הוא הומומורפיזם המבנה של פעולת G על G/K באמצעות כפל משמאל, מהטענה הקודמת נובע ש-$L\subseteq\mathrm{Core}_G(K)$. ■

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

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 $N\trianglelefteq G$.

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

הוכחה. נניח ש-$p=[G:N]$ ונסמן שוב ב-φ את ההומומורפיזם המבנה של פעולת G על G/N ע"י כפל משמאל.
מלמת הגרעין נובע שלכל $h\in\text{Im}\varphi$ קיימת מחלקה יחידה$C\in G/\ker\varphi$ כך ש-$\varphi^{-1}\left(\{h\}\right)=C$, מכאן ש-$|\text{Im}\varphi|=|G/\ker\varphi|$.
ע"פ טענה 4.15 מתקיים $\ker\varphi=\text{Core}_G\left(N\right)$, ולכן ממשפט לגראנז' נקבל:

$$|\text{Im}\varphi|=|G/\text{Core}_G\left(N\right)|=\frac{|G|}{|\text{Core}_G\left(N\right)|}$$

מכאן ש-$|\text{Im}\varphi|$ מחלק את $|G|$, ומצד שני $\text{Im}\varphi$ היא תת-חבורה של S_p ולכן ע"פ משפט לגראנז' $|\text{Im}\varphi|$ מחלק את $|S_p|=p!$.
מהעובדה ש-p הוא הראשוני הקטן ביותר שמחלק את $|G|$ נובע ש-$|\text{Im}\varphi|=p$ או ש-$|\text{Im}\varphi|=1$, לא ייתכן ש-$|\text{Im}\varphi|=1$ משום שאז נקבל:

$$|\text{Core}_G\left(N\right)|=\frac{|G|}{|\text{Im}\varphi|}=|G|=p\cdot|N|$$

בסתירה לכך ש-$N\subseteq\text{Core}_G\left(N\right)$, מכאן ש-$|\text{Im}\varphi|=p$ ולכן:

$$|\text{Core}_G\left(N\right)|=\frac{|G|}{|\text{Im}\varphi|}=\frac{|G|}{p}=|N|$$

וממילא $\text{Core}_G\left(N\right)=N$. מהמסקנה הקודמת (4.17) נובע ש-N נורמלית. ■

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.

הוכחה. תהא $G\neq K\leqslant G$ תת-חבורה ונניח בשלילה ש-$[G:K]$ סופי.
מהעובדה ש-G אין-סופית ו-G/K סופית נובע שהומומורפיזם המבנה של פעולת G על G/K באמצעות כפל משמאל אינו חח"ע, מכאן שהגרעין של הומומורפיזם זה אינו טריוויאלי (טענה 4.5), ומכיוון שזהו $\text{Core}_G\left(K\right)$ (טענה 4.15) נדע ש-$\text{Core}_G\left(K\right)\neq\{e\}$.
מצד שני $\text{Core}_G\left(K\right)\subseteq K$ ולכן מהעובדה ש-$G\neq K$ נובע שגם $\text{Core}_G\left(K\right)\neq G$, א"כ $\text{Core}_G\left(K\right)$ היא תת-חבורה נורמלית של G שאינה טריוויאלית בסתירה להנחה; מכאן שהנחת השלילה אינה נכונה ו-$[G:K]$ אינו סופי. ■

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

♣ כלומר כל חבורה G ניתנת לשיכון ב-S_G.

הוכחה. נסמן ב-φ את ההומומורפיזם המבנה של פעולת G על עצמה באמצעות כפל, לכל $a,b\in G$ כך ש-$a\neq b$ מתקיים:

$$\varphi\left(a\right)a^{-1}=a\cdot a^{-1}=e\neq b\cdot a^{-1}=\varphi\left(b\right)a^{-1}$$

ולכן גם $\varphi\left(a\right)\neq\varphi\left(b\right)$; מכאן ש-$\varphi$ חח"ע. ■

מסקנה 4.21. משפט קיילי[6]

כל חבורה איזומורפית לתת-חבורה של חבורות תמורות כלשהי.

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

הוכחה.

- $\Leftarrow$

  נניח ש-N נורמלית, לכל $a, b, c, d \in G$ כך ש-$aN = bN$ ו-$cN = dN$ מתקיים:

  $$(aN) \cdot (cN) = acN = adN = aNd = bNd = bdN = (bN) \cdot (dN)$$

  ולכן הפעולה "$\cdot$" מוגדרת היטב.

  – לכל $g \in G$ מתקיים $(eN) \cdot (gN) = egN = gN = geN = (gN) \cdot (eN)$, כלומר $eN = N$ הוא איבר היחידה.

  – לכל $a, b, c \in G$ מתקיים:

  $$((aN) \cdot (bN)) \cdot (cN) = (abN) \cdot (cN) = (abcN) = (aN) \cdot (bcN) = (aN) \cdot ((bN) \cdot (cN))$$

  כלומר הפעולה אסוציאטיבית.

  – לכל $g \in G$ מתקיים $\left(g^{-1}N\right) \cdot (gN) = g^{-1}gN = eN = N$, כלומר ההופכי של איבר gN הוא $g^{-1}N$.

  מכאן ש-$\left({}^{G}\!/_{N}, \cdot\right)$ היא אכן חבורה.
  מהגדרה מתקיים (לכל $g, h \in G$):

  $$\pi\left(gh\right) = ghN = (gN) \cdot (hN) = \pi\left(g\right) \cdot \pi\left(h\right)$$

  ולכן π הוא הומומורפיזם.

- $\Rightarrow$

  נניח שניתן להגדיר על ${}^{G}\!/_{N}$ מבנה של חבורה כך ש-π הוא הומומורפיזם, נסמן ב-"$\cdot$" את פעולת החבורה וא"כ מההנחה ש-π הוא הומומורפיזם נובע כי (לכל $g, h \in G$):

  $$(gN) \cdot (hN) = \pi\left(g\right) \cdot \pi\left(h\right) = \pi\left(gh\right) = ghN$$

  כלומר הכפל של החבורה מוכרח להיות זה שהגדרנו לעיל.
  כעת נשים לב לכך שלכל $g \in G$ מתקיים:

  $$\pi\left(g\right) = N \iff gN = N \iff g \in N$$

  ומכאן ש-$N = \ker\pi$ ובפרט N נורמלית.

■

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

מסקנה 5.2 תהא $N \leqslant G$ תת-חבורה, N היא תת-חבורה נורמלית אם"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 $G = Z(G)$.

הוכחה. נניח ש-$G/Z(G)$ ציקלית ויהי $g \in G$ כך ש-$G/Z(G) = \langle gZ(G) \rangle$.
יהיו $a, b \in G$ ויהיו $n, m \in \mathbb{N}$ כך שמתקיים:

$$(gZ(G))^m = bZ(G) \qquad\qquad (gZ(G))^n = aZ(G)$$

$$\begin{aligned}&\Rightarrow g^n Z(G) = aZ(G)\\ &\Rightarrow g^m Z(G) = bZ(G)\end{aligned}$$

מכאן ש-$a \in g^n Z(G)$ ו-$b \in g^m Z(G)$, ולכן קיימים $a', b' \in Z(G)$ כך שמתקיים:

$$\begin{aligned}a \cdot b &= g^n \cdot a' \cdot g^m \cdot b' = g^n \cdot g^m \cdot a' \cdot b' = g^{n+m} \cdot b' \cdot a'\\ &= g^{m+n} \cdot b' \cdot a' = g^m \cdot g^n \cdot b' \cdot a' = g^m \cdot b' \cdot g^n \cdot a' = b \cdot a\end{aligned}$$

כלומר G אבלית. ■

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

הוכחה. יהי $f \in \mathrm{Aut}(G)$, מכאן שלכל $g, x \in G$ מתקיים (φ_g הוא האוטומורפיזם המוגדר ע"י הצמדה ב-g):

$$\begin{aligned}\left(f \circ \varphi_g \circ f^{-1}\right)(x) &= f\left(\varphi_g\left(f^{-1}(x)\right)\right) = f\left(g\left(f^{-1}(x)\, g^{-1}\right)\right)\\ &= f(g) \cdot f\left(f^{-1}(x)\right) \cdot f\left(g^{-1}\right) = f(g) \cdot x \cdot (f(g))^{-1} = \varphi_{f(g)}\end{aligned}$$

ולכן $f \circ \varphi_g \circ f^{-1} \in \mathrm{Inn}(G)$. א"כ $\mathrm{Inn}(G)$ סגורה להצמדות ולכן היא נורמלית. ■

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:

$$\begin{aligned}{}^{H\times K}/_{H\times\{e_K\}} &\cong \{e_H\} \times K \cong K\\ {}^{H\times K}/_{\{e_H\}\times K} &\cong H \times \{e_K\} \cong H\end{aligned}$$

♣ 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.

[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:

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

הוכחה. תהא $f : {}^{G}/_{\ker\varphi} \to \mathrm{Im}\varphi$ פונקציה המוגדרת ע"י $f\left(g\ker\varphi\right) := \varphi\left(g\right)$ לכל $g \in G$; ע"פ למת הגרעין f אכן מוגדרת היטב, חח"ע ועל.
נוכיח ש-f היא הומומורפיזם, לכל $a, b \in G$ מתקיים:

$$f\left(\left(a\ker\varphi\right)\cdot\left(b\ker\varphi\right)\right) = f\left(ab\ker\varphi\right) = \varphi\left(ab\right) = \varphi\left(a\right)\cdot\varphi\left(b\right) = f\left(a\ker\varphi\right)\cdot f\left(b\ker\varphi\right)$$

$\blacksquare$

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

הוכחה. יהי $\varphi : G \to \mathrm{Inn}\left(G\right)$ ההומומורפיזם המעתיק כל איבר ב-G לאוטומורפיזם המוגדר ע"י הצמדה באותו איבר (בדיקה פשוטה מראה שפונקציה זו היא אכן הומומורפיזם).
לכל $g \in G$ מתקיים:

$$\varphi\left(g\right) = \mathrm{Id}_G \iff \forall h \in G\ ghg^{-1} = h \iff \forall h \in G\ gh = hg \iff g \in Z\left(G\right)$$

כלומר $Z\left(G\right) = \ker\varphi$ ולכן ע"פ משפט האיזומורפיזם הראשון מתקיים $^{G}/_{Z(G)} \cong \mathrm{Inn}\left(G\right)$. $\blacksquare$

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

$$^{HN}/_{N} \cong {}^{H}/_{H\cap N}$$

הוכחה. יהי $\varphi : H \to {}^{HN}/_{N}$ ההומומורפיזם המוגדר ע"י $\varphi\left(h\right) := hN$ לכל $h \in H$, מהגדרה φ על (כלומר $\mathrm{Im}\varphi = HN$) ו-$\ker\varphi = H \cap N$. מכאן שע"פ משפט האיזומורפיזם הראשון מתקיים:

$$^{HN}/_{N} \cong {}^{H}/_{H\cap N}$$

$\blacksquare$

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

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

הוכחה. יהי $\varphi : {}^{G}/_{N} \to {}^{G}/_{H}$ פונקציה המוגדרת ע"י $\varphi\left(gN\right) := gH$ לכל $g \in G$. φ אכן מוגדרת היטב מפני שלכל $a, b \in G$ מתקיים:

$$aN = bN \iff b^{-1}a \in N \Rightarrow b^{-1}a \in H \iff aH = bH$$

φ הוא הומומורפיזם שכן לכל $a, b \in G$ מתקיים:

$$\varphi\left(\left(aN\right)\cdot\left(bN\right)\right) = \varphi\left(abN\right) = abH = \left(aH\right)\cdot\left(bH\right) = \varphi\left(aN\right)\cdot\varphi\left(bN\right)$$

מהגדרה φ על (כלומר $\mathrm{Im}\varphi = {}^{G}/_{H}$), וכמו כן לכל $g \in G$ מתקיים:

$$\varphi(gN) = H \iff gH = H \iff g \in H$$

כלומר $\ker\varphi = {}^{H}/_{N}$. ממשפט האיזומורפיזם הראשון נובע ש-$({}^{G}/_{N}) / ({}^{H}/_{N}) \cong {}^{G}/_{H}$. ■

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 $[H : K] = [f(H) : f(K)] = [{}^{H}/_{N} : {}^{K}/_{N}]$.

הוכחה.

- תהא $L \leqslant {}^{G}/_{N}$ תת-חבורה, נוכיח תחילה ש-$N \leqslant \pi^{-1}(L) \leqslant G$.
מהיות L תת-חבורה נובע כי:
  - $N \in L$ ולכן $e \in \pi^{-1}(L)$.
  - לכל $a, b \in \pi^{-1}(L)$ מתקיים $\pi(a) \in L$ ו-$\pi(b) \in L$ ולכן גם $\pi(ab) = \pi(a) \cdot \pi(b) \in L$, כלומר $ab \in \pi^{-1}(L)$.
  - לכל $g \in \pi^{-1}(L)$ מתקיים $\pi(g) \in L$ ולכן גם $\pi(g^{-1}) = (\pi(g))^{-1} \in L$, כלומר $g^{-1} \in \pi^{-1}(L)$.

  מכאן ש-$\pi^{-1}(L) \leqslant G$. בנוסף, מהעובדה ש-$N \in L$ נובע שלכל $n \in N$ מתקיים $n \in \pi^{-1}(L)$, כלומר $N \subseteq \pi^{-1}(L)$.
  מהיות $\pi : G \to {}^{G}/_{N}$ על נובע ש-$L = \pi(\pi^{-1}(L)) = f(\pi^{-1}(L))$, ומכיוון ש-$L$ הייתה שרירותית נדע ש-f על.
  מהגדרה לכל $N \leqslant H \leqslant G$ מתקיים:

$$\begin{aligned}
\pi^{-1}(f(H)) &= \pi^{-1}(\pi(H)) = \pi^{-1}(\{\pi(h) \mid h \in H\}) \\
&= \{g \in G \mid \pi(g) \in \{\pi(h) \mid h \in H\}\} \\
&= \{g \in G \mid \exists h \in H \ \ \pi(g) = \pi(h)\} \\
&= \{g \in G \mid \exists h \in H \ \ gN = hN\} \\
&= \{g \in G \mid \exists h \in H \ \ g \in hN\} \\
&= \{g \in G \mid g \in HN\} = HN = H
\end{aligned}$$

  מכאן ש-f חח"ע וההופכית שלה מוגדרת ע"י $f^{-1}(L) := \pi^{-1}(L)$ לכל $L \leqslant {}^{G}/_{N}$.

---

[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 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 $\{g \in G \mid \pi(g) \in L\}$.

- תהיינה $N\leqslant H,K\leqslant G$ תתי-חבורות.
  - נניח ש-$H\leqslant K$.
    * מהגדרה מתקיים $\nicefrac{H}{N}\leqslant\nicefrac{K}{N}$. בנוסף, אם $H\trianglelefteq K$ אז לכל $h\in H$ מתקיים $hKh^{-1}=K$, ולכן גם:

$$hN\cdot\nicefrac{K}{N}\cdot\left(hN\right)^{-1}=hN\cdot\left\{ kN\mid k\in K\right\} \cdot\left(h^{-1}N\right)=\left\{ hkh^{-1}N\mid k\in K\right\} =\left\{ kN\mid k\in K\right\} =\nicefrac{K}{N}$$

כלומר $\nicefrac{H}{N}\trianglelefteq\nicefrac{K}{N}$.

    * תהא $\tilde{f}:H/K\to\left(\nicefrac{H}{N}\right)/\left(\nicefrac{K}{N}\right)$ פונקציה המוגדרת ע"י (לכל $h\in H$):

$$\tilde{f}\left(hK\right):=hN\cdot\nicefrac{K}{N}$$

$\tilde{f}$ אכן מוגדרת היטב מפני שלכל $a,b\in H$ מתקיים:

$$\begin{aligned}aK=bK\Rightarrow\tilde{f}\left(aK\right) & =aN\cdot\nicefrac{K}{N}=aN\cdot\left\{ kN\mid k\in K\right\} =\left\{ akN\mid k\in K\right\} \\
 & =\left\{ aNk\mid k\in K\right\} =\left\{ bNk\mid k\in K\right\} =\left\{ bkN\mid k\in K\right\} \\
 & =bN\cdot\left\{ kN\mid k\in K\right\} =bN\cdot\nicefrac{K}{N}=\tilde{f}\left(bK\right)
\end{aligned}$$

לכל $a,b\in H$ כך ש-$\tilde{f}\left(aK\right)=\tilde{f}\left(bK\right)$ מתקיים $\left\{ aNk\mid k\in K\right\} =\left\{ bNk\mid k\in K\right\}$, ולכן קיים $k\in K$ כך ש-$aNe=bNk$, וממילא:

$$aK=aNK=aNe\cdot K=bNk\cdot K=bNK=bK$$

מכאן ש-$\tilde{f}$ חח"ע, מהגדרה $\tilde{f}$ על ומכאן ש-$\left|H/K\right|=\left|\left(\nicefrac{H}{N}\right)/\left(\nicefrac{K}{N}\right)\right|$, כלומר:

$$\left[H:K\right]=\left[\nicefrac{H}{N}:\nicefrac{K}{N}\right]$$

  - נניח ש-$\nicefrac{H}{N}\leqslant\nicefrac{K}{N}$, כלומר לכל $k\in K$ קיים $h\in H$ כך ש-$hN=kN$ וממילא גם $k\in hN\subseteq H$, מכאן ש-$H\leqslant K$.
בנוסף אם $\nicefrac{H}{N}\trianglelefteq\nicefrac{K}{N}$ אז לכל $h\in H$ מתקיים:

$$\nicefrac{K}{N}=hN\cdot\nicefrac{K}{N}\cdot\left(hN\right)^{-1}=\left\{ hkh^{-1}N\mid k\in K\right\}$$

כלומר לכל $h\in H$ ולכל $k\in K$ קיים k' כך ש-$hkh^{-1}N=k'N$ וממילא גם $hkh^{-1}\in k'N\subseteq K$. א"כ K סגורה להצמדות באיברים מ-H ולכן $H\trianglelefteq K$.

■

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.

הוכחה. נסמן $X:=\left\{S\subseteq G:|S|=p^r\right\}$, מהגדרה מתקיים:

$$|X|=\binom{p^r\cdot m}{p^r}=\frac{\prod_{i=0}^{p^r-1}\left(p^r\cdot m-i\right)}{\prod_{i=0}^{p^r-1}\left(p^r-i\right)}=\prod_{i=0}^{r-1}\frac{p^r\cdot m-i}{p^r-i}$$

כל אחד מהגורמים במכפלה שבאגף שמאל אינו מתחלק ב-p[13], ולכן גם $|X|$ אינו מתחלק ב-p.

מכאן שקיים מסלול תחת פעולת G על X ע"י כפל משמאל שגודלו אינו מתחלק ב-p (כי X היא איחוד זר של המסלולים), א"כ תהא $S\in A$ במסלול כזה.

ע"פ משפט מסלול-מייצב מתקיים:

$$|G_S|=\frac{|G|}{|O_G\left(S\right)|}$$

$|O_G\left(S\right)|$ כפולה של p ולכן $|G_S|$ מתחלק ב-p^r.

מצד שני לכל $s\in S$ מתקיים $G_S\cdot s\subseteq S$, כלומר לכל $s\in S$ המחלקה הימנית של G_S שבה נמצא s מוכלת ב-S.

א"כ יהיו $s_1,s_2,\ldots,s_n\in S$ נציגים של כל המחלקות הימניות של G_S שבהן איבר מ-S, מכאן שמתקיים:

$$S=\dot{\bigcup_{i=1}^{n}}G_S\cdot s_i$$

ולכן גם:

$$p^r=|S|=\sum_{i=1}^{n}|G_S\cdot s_i|=\sum_{i=1}^{n}|G_S|=n\cdot|G_S|$$

בפרט $|G_S|$ מחלק את p^r וממילא $|G_S|=p^r$ ו-G_S היא חבורת p-סילו (למעשה נובע מזה גם ש-$S=G_S$ אך אין לנו צורך בזה). ■

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

הוכחה. נובע ישירות ממשפט לגראנז'. ■

מסקנה 6.3. משפט קושי

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

הוכחה. ע"פ משפט סילו הראשון קיימת תת-חבורה $P\leqslant G$ כך ש-$|P|=p^r$, א"כ תהא P חבורה כזו ויהי $e\neq x\in P$.

ע"פ הטענה הקודמת (6.2) קיים $k\in\mathbb{N}$ כך ש-$|x|=p^k$, יהי k כנ"ל ונסמן $g:=x^{p^{k-1}}$; מהעובדה ש-$|x|=p^k$ נובע ש-$|g|=p$. ■

להביא גם את ההוכחה שאינה מסתמכת על סילו.

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

[12] ערך בוויקיפדיה: לודוויג סילו

[13] החזקה הגדולה ביותר של p המחלקת את המונה היא גם החזקה הגדולה ביותר שמחלקת את המכנה.

הוכחה. אם G אבלית אז $Z\left(G\right)=G$, כלומר $\left|Z\left(G\right)\right|=\left|G\right|=p^{r}$ ובפרט $\left|Z\left(G\right)\right|$ מתחלק ב-p, לכן נניח ש-G אינה אבלית.
מכאן שלכל $g\in G$ מתקיים $C_{G}\left(g\right)\neq G$ ולכן $\left[G:C_{G}\left(g\right)\right]\neq1$, ומכיוון ש-$\left[G:C_{G}\left(g\right)\right]$ מחלק את $\left|G\right|=p^{r}$ נדע ש-$\left[G:C_{G}\left(g\right)\right]$ הוא חזקה של p ובפרט מתחלק ב-p.
כמובן ש-$\left|G\right|$ מתחלק ב-p ולכן ממשוואת המחלקה נובע שגם $\left|Z\left(G\right)\right|$ מתחלק ב-p. ∎

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-$\left|N\right|=p^{k}$.

אני לא בטוח שראינו את הטענה הזו בכיתה.

הוכחה. נוכיח את הטענה באינדוקציה שלמה, נניח שלכל חבורה G כך ש-$\left|G\right|=p^{s}$ עבור $r>s\in\mathbb{N}_{0}$ ולכל $s\geq k\in\mathbb{N}$ קיימת תת-חבורה נורמלית $G\trianglerighteq N$ כך ש-$\left|N\right|=p^{k}$.
מהטענה הקודמת (6.4) נובע ש-$\left|Z\left(G\right)\right|$ מתחלק ב-p, ולכן קיים $g\in Z\left(G\right)$ כך ש-$\left|g\right|=p$ (משפט קושי), יהי $g\in Z\left(G\right)$ כנ"ל.
נסמן $H:=\left\langle g\right\rangle$, מהגדרה $H\leqslant Z\left(G\right)$ ולכן איברי H מתחלפים עם כל איבר ב-G, וממילא $H\trianglelefteq G$.
כעת נשים לב לכך ש-$\left|{}^{G}/_{H}\right|=p^{r-1}$, ולכן מהנחת האינדוקציה נובע שלכל $r-1\geq k\in\mathbb{N}_{0}$ קיימת תת-חבורה נורמלית $K\trianglelefteq{}^{G}/_{H}$ כך ש-$\left|K\right|=p^{k}$.
מכאן שע"פ משפט ההתאמה לכל $r-1\geq k\in\mathbb{N}_{0}$ קיימת תת-חבורה $N\trianglelefteq G$ כך ש-$H\leqslant N$ ובנוסף:

$$\frac{\left|N\right|}{p}=\frac{\left|N\right|}{\left|H\right|}=\left[N:H\right]=\left[{}^{G}/_{H}:K\right]=\frac{\left|{}^{G}/_{H}\right|}{\left|K\right|}=p^{r-1-k}$$

וממילא $\left|N\right|=p^{r-k}$. כלומר לכל $r\geq k\in\mathbb{N}$ קיימת תת-חבורה $N\trianglelefteq G$ כך ש-$\left|N\right|=p^{k}$, וכמובן ש-$\left\{ e\right\}$ היא תת-חבורה נורמלית המקיימת $\left|\left\{ e\right\} \right|=p^{0}$ ולכן הטענה נכונה לכל $r\geq k\in\mathbb{N}_{0}$. ∎

מסקנה 6.6. לכל $\mathrm{Ord}_{p}\left(\left|G\right|\right)\geq k\in\mathbb{N}_{0}$ קיימת תת-חבורה $H\leqslant G$ כך ש-$\left|H\right|=p^{k}$.

משפט סילו ה-II

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

הוכחה. תהיינה $P\in\mathrm{Syl}_{p}\left(G\right)$ ו-$H\leqslant G$ ונסמן $k:=\mathrm{Ord}_{p}\left(\left|H\right|\right)$.
נשים לב לכך ש-H פועלת על ${}^{G}/_{P}$ ע"י כפל משמאל, ולכל $g\in G$ המייצב של המחלקה gP הוא:

$$\left\{ h\in H\mid hgP=gP\right\} =\left\{ h\in H\mid g^{-1}hg\in P\right\} =\left\{ h\in H\mid h\in gPg^{-1}\right\} =H\cap gPg^{-1}$$

מהגדרה מתקיים $\left|{}^{G}/_{P}\right|=m$, כלומר $\left|{}^{G}/_{P}\right|$ זר ל-p ולכן קיים מסלול תחת הפעולה הנ"ל שגודלו אינו מתחלק ב-p (כי ${}^{G}/_{P}$ היא איחוד זר של המסלולים).
א"כ יהי $g\in G$ כך ש-$\left|O\left(gP\right)\right|$ אינו מתחלק ב-p, ע"פ משפט מסלול מייצב מתקיים:

$$\left|H\cap gPg^{-1}\right|=\frac{\left|H\right|}{\left|O\left(gP\right)\right|}$$

ולכן מכיוון ש-$\left|O\left(gP\right)\right|$ אינו מתחלק ב-p נדע כי $\mathrm{Ord}_{p}\left(\left|H\cap gPg^{-1}\right|\right)=\mathrm{Ord}_{p}\left(\left|H\right|\right)=k$.
מצד שני $H\cap gPg^{-1}$ היא תת-חבורה של חבורת p (gPg^{-1}), ולכן ע"פ משפט לגראנז' קיים $j\in\mathbb{N}_{0}$ כך ש-$\left|H\cap gPg^{-1}\right|=p^{j}$, ומכאן נובע כי:

$$\left|H\cap gPg^{-1}\right|=p^{k}$$

כלומר $\left(gPg^{-1}\cap H\right)\in\mathrm{Syl}_{p}\left(H\right)$. ∎

מסקנה 6.8. משפט סילו השני
כל שתי חבורות p-סילו של G צמודות זו לזו, או בניסוח אחר $\mathrm{Syl}_p\left(G\right)$ 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 $P\in\mathrm{Syl}_p\left(G\right)$ מתקיים:
$$P\trianglelefteq G\iff\mathrm{Syl}_p\left(G\right)=\left\{P\right\}$$

♣ 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 $P_H\in\mathrm{Syl}_p\left(H\right)$ קיימת $P_G\in\mathrm{Syl}_p\left(G\right)$ כך ש-$P_H=P_G\cap H$.

הוכחה. תהא $H\leqslant G$ תת-חבורה ותהא $P_H\in\mathrm{Syl}_p\left(H\right)$.
תהא $P\in\mathrm{Syl}_p\left(G\right)$ ויהי $g\in G$ כך ש-$gPg^{-1}\cap H\in\mathrm{Syl}_p\left(H\right)$, ע"פ טענה 6.7 אכן קיים g כזה.
ממשפט סילו השני נובע שקיים $h\in H$ כך שמתקיים $h\left(gPg^{-1}\cap H\right)h^{-1}=P_H$, יהי h כנ"ל.
$$\begin{aligned}\Rightarrow P_H&=h\cdot\left\{gxg^{-1}\mid x\in P,\ gxg^{-1}\in H\right\}\cdot h^{-1}\\&=\left\{hgxg^{-1}h^{-1}\mid x\in P,\ gxg^{-1}\in H\right\}\\&=\left\{hgxg^{-1}h^{-1}\mid x\in P,\ hgxg^{-1}h^{-1}\in H\right\}\\&=\left\{hgxg^{-1}h^{-1}\mid x\in P\right\}\cap H\\&=\left(hg\cdot\left\{x\mid x\in P\right\}\cdot g^{-1}h^{-1}\right)\cap H\\&=\left(hg\cdot P\cdot\left(hg\right)^{-1}\right)\cap H\end{aligned}$$

מהגדרה הקבוצה $hg\cdot P\cdot\left(hg\right)^{-1}$ היא חבורת p-סילו של G, והיא מקיימת את המבוקש. ■

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

משפט סילו ה-III

משפט 6.12. משפט סילו השלישי

נסמן $\left|\mathrm{Syl}_p\left(G\right)\right| =: k_p$, 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.

הוכחה. תהא $P \in \mathrm{Syl}_p\left(G\right)$; P פועלת על $\mathrm{Syl}_p\left(G\right)$ ע"י הצמדה, וממשפט מסלול-מייצב נובע שגדלי המסלולים תחת פעולה זו הם חזקות של p (כי $|P| = p^r$).

כלומר הגודל של כל מסלול מתחלק ב-p או שהוא 1, ומכאן שאם נוכיח שקיים רק מסלול אחד בגודל 1 נקבל את המבוקש.

תהא $\tilde{P} \in \mathrm{Syl}_p\left(G\right)$ כך שגודל המסלול של $\tilde{P}$ תחת הפעולה הנ"ל הוא 1, כלומר לכל $g \in P$ מתקיים $g\tilde{P}g^{-1} = \tilde{P}$ ולכן גם $g\tilde{P} = \tilde{P}g$.

מכאן ש-$P\tilde{P} = \tilde{P}P$ ולכן מטענה 2.17 נובע ש-$P\tilde{P}$ היא חבורה, וע"פ טענה 2.16 הגודל של $P\tilde{P}$ הוא:

$$\left|P\tilde{P}\right| = \frac{|P| \cdot \left|\tilde{P}\right|}{\left|P \cap \tilde{P}\right|} = \frac{p^{2r}}{\left|P \cap \tilde{P}\right|}$$

$P \cap \tilde{P}$ היא תת-חבורה של חבורת p ולכן היא חבורת p בעצמה (טענה 6.2), א"כ יהי $k \in \mathbb{N}_0$ כך ש-$\left|P \cap \tilde{P}\right| = p^k$.

$$\Rightarrow \left|P\tilde{P}\right| = p^{2r-k}$$

מהעובדה ש-$r = \mathrm{Ord}_p\left(|G|\right)$ נובע ש-$\left|P\tilde{P}\right| \le p^r$, כלומר $k \ge r$; מצד שני מהעובדה ש-$|P| = p^r$ נובע ש-$\left|P \cap \tilde{P}\right| \le p^r$, כלומר $k \le r$.

א"כ $k = r$, כלומר $\left|P \cap \tilde{P}\right| = p^r = |P| = \left|\tilde{P}\right|$, ולכן בהכרח $P = P \cap \tilde{P} = \tilde{P}$.

מכאן ש-P היא החבורה היחידה ב-$\mathrm{Syl}_p\left(G\right)$ שגודל המסלול שלה הוא 1, ומכיוון שהגודל של שאר המסלולים מתחלק ב-p נדע ש-$k_p = \left|\mathrm{Syl}_p\left(G\right)\right| \equiv 1 \mod p$.

כדי להוכיח ש-$k_p \mid m$ נשים לב לכך שע"פ משפט סילו השני $\mathrm{Syl}_p\left(G\right)$ היא מסלול תחת הפעולה של G על תתי-חבורות שלה ע"י הצמדה, ולכן בהכרח $k_p \mid p^r \cdot m = |G|$.

מצד שני מהעובדה ש-$k_p \equiv 1 \mod p$ נובע ש-k_p אינו מתחלק ב-p ולכן גם זר ל-p^r, וממילא ע"פ העובדה ש-$k_p \mid p^r \cdot m$ נדע ש-$k_p \mid m$. ■

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:

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

הוכחה. הפונקציה $\varphi:H\times K\to {}^{H}/_{\tilde{H}}\times {}^{K}/_{\tilde{K}}$ המוגדרת ע"י $\varphi\left(h,k\right):=\left(h\tilde{H},k\tilde{K}\right)$ (לכל $(h,k)\in H\times K$) היא הומומורפיזם, ובנוסף $\text{Im}\varphi={}^{H}/_{\tilde{H}}\times {}^{K}/_{\tilde{K}}$ ו-$\ker\varphi=\tilde{H}\times\tilde{K}$; ממשפט האיזומורפיזם הראשון נקבל את המבוקש. ■

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

הוכחה. מהנתון ש-$G=H\rtimes K$ נובע שלכל $g\in G$ קיימים $h\in H$ ו-$k\in K$ יחידים כך ש-$g=hk$, הפונקציה המעתיקה כל $g\in G$ אל ה-$k\in K$ היחיד שמתאים לו היא הומומורפיזם, תמונתה היא K והגרעין שלה הוא H; ממשפט האיזומורפיזם הראשון נקבל את המבוקש. ■

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 $\left(H\times K,*\right)=\tilde{H}\rtimes\tilde{K}$[14] אם"ם קיים הומומורפיזם $\phi:K\to\text{Aut}\left(H\right)$ כך שלכל $\left(h,k\right),\left(h',k'\right)\in H\times K$ מתקיים[15]:

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

הוכחה. **צריך להוסיף הוכחה.** ■

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 $G\cong\mathbb{Z}_p\times\mathbb{Z}_p$.

הוכחה. נחלק למקרים:

- נניח שיש ב-G איבר מסדר p^2, מכאן ש-G ציקלית, וכפי שכבר ראינו כל חבורה ציקלית סופית איזומורפית ל-$\mathbb{Z}_n$ כאשר n הוא גודל החבורה, במקרה שלנו זה אומר ש-$G\cong\mathbb{Z}_{p^2}$.
- נניח שאין ב-G איבר מסדר p^2, מטענה 6.4 נובע ש-$|Z\left(G\right)|=p$ או ש-$|Z\left(G\right)|=p^2$, ולכן ע"פ משפט 5.5 בשני המקרים מתקיים $G=Z\left(G\right)$, כלומר G אבלית.
יהי $e\neq g\in G$, ממשפט לגראנז' נובע ש-$|\langle g\rangle|=|g|=p$ ולכן קיים $e\neq h\in G$ כך ש-$h\notin\langle g\rangle$, יהי h כנ"ל.
G אבלית ולכן $\langle g\rangle$ ו-$\langle h\rangle$ נורמליות, בנוסף מתקיים $\langle g\rangle\cap\langle h\rangle=\{e\}$ שכן $\langle g\rangle$ ו-$\langle h\rangle$ ציקליות ו-$h\notin\langle g\rangle$ (אם היה קיים $e\neq x\in\langle g\rangle\cap\langle h\rangle$ אז היא מתקיים $h\in\langle x\rangle=\langle g\rangle$); משיקולי גודל (טענה 2.16) נובע ש-$G=\langle h\rangle\cdot\langle g\rangle$ ולכן $G=\langle g\rangle\times\langle h\rangle\cong\mathbb{Z}_p\times\mathbb{Z}_p$.

■

[14] כלומר הזוג הסדור $\left(H\times K,*\right)$ הוא חבורה, ובנוסף זוהי החבורה $\tilde{H}\rtimes\tilde{K}$.
[15] ϕ_k הוא האוטומורפיזם ב-$\text{Aut}\left(H\right)$ שאליו מעתיק ϕ את k.

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 $\phi:\mathbb{Z}_p\to\mathrm{Aut}\left(\mathbb{Z}_q\right)$ 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 ($\mathbb{Z}_q\rtimes_\phi\mathbb{Z}_p$).

הוכחה. ממשפט קושי נובע שקיימות תתי-חבורות $Q,P\leqslant G$ כך ש-$|Q|=q$ ו-$|P|=p$, תהיינה Q ו-P כנ"ל.
ממשפט לגראנז' ומטענה 4.18 נובע ש-Q נורמלית, הסדרים של P ו-Q זרים ולכן החיתוך שלהן טריוויאלי, ובנוסף משיקולי גודל (2.16) מתקיים $QP=G$.
מכאן ש-$G=Q\rtimes P$, ומכיוון ש-$Q\cong\mathbb{Z}_q$ ו-$P\cong\mathbb{Z}_p$ נדע שקיים הומומורפיזם $\phi:\mathbb{Z}_p\to\mathrm{Aut}\left(\mathbb{Z}_q\right)$ כך ש-$G\cong\mathbb{Z}_q\rtimes_\phi\mathbb{Z}_p$.
כעת נחלק למקרים:

- אם $q\not\equiv 1 \mod p$ אז ממשפט סילו השלישי נובע ש-P היא חבורת p-סילו היחידה של G, ולכן גם היא נורמלית.
  מכאן ש-$G=Q\times P$, ומכיוון ש-$Q\cong\mathbb{Z}_q$ ו-$P\cong\mathbb{Z}_p$ נדע ש-$G\cong\mathbb{Z}_q\times\mathbb{Z}_p$ (כלומר ϕ הוא ההומומורפיזם הטריוויאלי).
- נניח ש-$q\equiv 1 \mod p$, כעת משפט סילו השלישי אינו קובע ש-P יחידה אך גם אינו שולל זאת, כלומר ייתכן ששוב P נורמלית ו-$G\cong\mathbb{Z}_q\times\mathbb{Z}_p$.
  נניח כעת ש-P אינה נורמלית, מכאן שקיים הומומורפיזם $\phi:\mathbb{Z}_p\to\mathrm{Aut}\left(\mathbb{Z}_q\right)$ לא טריוויאלי כך ש-$G\cong\mathbb{Z}_q\rtimes_\phi\mathbb{Z}_p$; נרצה להוכיח שלכל הומומורפיזם כזה מקבלים את אותה חבורה (עד כדי איזומורפיזם).
  צריך להמשיך.

■

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.

הוכחה. אם קיים גורם שאינו חבורה פשוטה אז ממשפט ההתאמה ניתן לעדן את הסדרה מבלי להוסיף חזרות ולכן הסדרה אינה סדרת הרכב, ולהפך: אם כל הגורמים הם חבורות פשוטות אז ממשפט ההתאמה נובע שאי אפשר לעדן את הסדרה מבלי לחזור על תת-חבורה פעמיים (העובדה שבסדרה אין חזרות נובעת מהגדרת החבורה הטריוויאלית - $\{e\}$ - כחבורה שאינה פשוטה). ■

משפט 7.8. משפט ז'ורדן-הלדר (Jordan–Hölder)[16]
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.

הוכחה. **לא למדנו את ההוכחה של המשפט בכיתה, אורי אמר שהיא סתם טכנית, ארוכה ואינה מוסיפה דבר.** ■

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

[16] ערכים בוויקיפדיה: קאמי ז'ורדן (עברית) ו-Otto Hölder (אנגלית).

מסקנה 7.10. נניח ש-G אבלית וסופית, ויהיו $p_1,p_2,\ldots,p_r\in\mathbb{N}$ מספרים ראשוניים כך שמתקיים[17]:
$$|G|=\prod_{i=1}^{r}p_i$$
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 $N_1,N_2,\ldots,N_r,H_1,H_2,\ldots,H_s$.

הוכחה. נובע ישירות ממשפט ההתאמה. ∎

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.

הוכחה. נובע ישירות מטענות 7.7 ו-7.9. ∎

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.

הוכחה. ניקח סדרה נורמלית של G בעלת גורמים אבליים ונחתוך את כל אחת מתתי-החבורות בסדרה עם H, התוצאה היא סדרה נורמלית של H בעלת מנות אבליות. ∎

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".

הוכחה.

1. נוכיח ש-G' סגורה להצמדות בכך שנוכיח שכל הצמדה של קומוטטור היא קומוטטור.
   לכל $a,b,g\in G$ מתקיים:
$$\begin{aligned}g\cdot[a,b]\cdot g^{-1}&=g\cdot aba^{-1}b^{-1}\cdot g^{-1}=\left(gag^{-1}\right)\cdot\left(gbg^{-1}\right)\cdot\left(ga^{-1}g^{-1}\right)\cdot\left(gb^{-1}g^{-1}\right)\\&=\left(gag^{-1}\right)\cdot\left(gbg^{-1}\right)\cdot\left(gag^{-1}\right)^{-1}\cdot\left(gbg^{-1}\right)^{-1}=\left[gag^{-1},gbg^{-1}\right]\end{aligned}$$
   מכאן ש-G' סגורה להצמדות ולכן $G'\trianglelefteq G$.

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

2. לכל $a,b\in G$ מתקיים (ב-${}^{G}/_{G'}$):

$$(aG')\cdot(bG')=abG'=ab\cdot\left[b^{-1},a^{-1}\right]\cdot G'=ab\cdot b^{-1}a^{-1}ba\cdot G'=baG'=(bG')\cdot(aG')$$

3. תהא $N\trianglelefteq G$ תת-חבורה נורמלית כך ש-${}^{G}/_{N}$ אבלית, נוכיח שכל הקומוטטורים ב-G שייכים ל-N ומכאן ש-$G'\leqslant N$.
לכל $a,b\in G$ מתקיים:

$$a^{-1}b^{-1}N=\left(a^{-1}N\right)\cdot\left(b^{-1}N\right)=\left(b^{-1}N\right)\cdot\left(a^{-1}N\right)=b^{-1}a^{-1}N$$

ולכן גם $aba^{-1}b^{-1}N=N$, כלומר $[a,b]=aba^{-1}b^{-1}\in N$.

■

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

הוכחה.

- $\Leftarrow$
נניח ש-G פתירה ותהא $(G_0,G_1,\ldots,G_r)$ סדרה נורמלית של G בעלת גורמים אבליים, נוכיח באינדוקציה שלכל $r\geq i\in\mathbb{N}$ מתקיים $G^{(i)}\leqslant G_i$.
  - בסיס האינדוקציה: ע"פ התכונה השלישית של החבורה הנגזרת מתקיים $G'\leqslant G_1$ (כי ${}^{G}/_{G_1}$ היא גורם של הסדרה ולכן אבלית).
  - צעד האינדוקציה: יהי $r>i\in\mathbb{N}$ ונניח ש-$G^{(i)}\leqslant G_i$, מהגדרה $G^{(i+1)}\leqslant(G_i)'$ (כי כל קומוטטור של $G^{(i)}$ הוא קומוטטור של G_i), ולכן ע"פ התכונה השלישית של החבורה הנגזרת מתקיים $G^{(i+1)}\leqslant(G_i)'\leqslant G_{i+1}$ (שוב מפני ש-${}^{G_i}/_{G_{i+1}}$ אבלית).

  בפרט נובע מכאן ש-$G^{(r)}\leqslant G_r=\{e\}$, כלומר $G^{(r)}=\{e\}$ כנדרש.
- $\Rightarrow$
נניח שקיים $n\in\mathbb{N}_0$ כך ש-$G^{(n)}=\{e\}$ ויהי n כנ"ל, א"כ ע"פ שתי התכונות הראשונות של החבורה הנגזרת הסדרה $\left(G^{(0)},G^{(1)},\ldots,G^{(n)}\right)$ היא סדרה נורמלית של G בעלת מנות אבליות ומהגדרה G פתירה.

■

7.5 חבורות נילפוטנטיות

טענה 7.18. כל חבורה נילפוטנטית היא חבורה פתירה.

הוכחה. נוכיח את הטענה באינדוקציה על מחלקת הנילפוטנטיות של החבורה, אם מדובר במחלקת נילפוטנטיות 0 הטענה טריוויאלית ולכן נעבור היישר לצעד האינדוקציה.
תהא G חבורה נילפוטנטית ממחלקת נילפוטנטיות $r\in\mathbb{N}$, ונניח שכל חבורה נילפוטנטית ממחלקת נילפוטנטיות $r-1$ היא חבורה פתירה.
מכאן ש-${}^{G}/_{Z(G)}$ היא חבורה פתירה וכמובן שגם $Z\left(G\right)\trianglelefteq G$ היא חבורה פתירה, ממסקנה 7.13 נובע ש-G 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.

הוכחה. יהי $p \in \mathbb{N}$ ראשוני ותהא G חבורת p, נסמן $r := \text{Ord}_p(|G|)$, ונוכיח את הטענה באינדוקציה שלמה על r.
נניח שלכל $r > k \in \mathbb{N}_0$, כל חבורת p בגודל p^k היא חבורה נילפוטנטית. ע"פ טענה 6.4 מתקיים $Z(G) \neq \{e\}$, מכאן שע"פ משפט לגראנז' קיים $r > k \in \mathbb{N}_0$ כך ש-$|{}^{G}/{}_{Z(G)}| = p^k$ ולכן ע"פ ההנחה ${}^{G}/{}_{Z(G)}$ נילפוטנטית ומהגדרה גם G נילפוטנטית. ■

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.

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

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

הוכחה. תהא $\varphi : N_G(H) \to {}^{G}/{}_{N}$ פונקציה המוגדרת ע"י $\varphi(g) := gN$ לכל $g \in N_G(H)$.
לכל $g \in G$ מתקיים:

$$g \in N_G(H) \Longleftrightarrow \left\{ghg^{-1} : h \in H\right\} = gHg^{-1} = H \Longleftrightarrow \left\{ghNg^{-1} : h \in H\right\} = \left\{ghg^{-1}N : h \in H\right\} = \{hN : h \in H\} = {}^{H}/{}_{N}$$

ולפיכך:

$$\begin{aligned} N_{G/N}\left({}^{H}/{}_{N}\right) &= \left\{gN \mid (gN) \cdot {}^{H}/{}_{N} \cdot (gN)^{-1} = {}^{H}/{}_{N},\ g \in G\right\} \\ &= \left\{gN \mid (gN) \cdot \{hN : h \in H\} \cdot \left(g^{-1}N\right) = {}^{H}/{}_{N},\ g \in G\right\} \\ &= \left\{gN \mid \left\{ghg^{-1}N : h \in H\right\} = {}^{H}/{}_{N},\ g \in G\right\} \\ &= \{\varphi(g) \mid g \in N_G(H)\} = \text{Im}\varphi \end{aligned}$$

בנוסף, מהגדרת φ מתקיים $\ker\varphi = N$, ולכן ממשפט האיזומורפיזם הראשון נובע כי $N_{G/N}\left({}^{H}/{}_{N}\right) \cong {}^{N_G(H)}/{}_{N}$. ■

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 $P \trianglelefteq G$.

הוכחה. נניח ש-$P \trianglelefteq H$, מכאן ש-P היא חבורת p-סילו היחידה של H.
מהיות H נורמלית נובע שלכל $g \in G$ מתקיים $gPg^{-1} \leqslant H$, ומכיוון ש-gPg^{-1} היא חבורת p-סילו של H הרי ש-$gPg^{-1} = P$ לכל $g \in G$, כלומר $P \trianglelefteq G$. ■

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[18].
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[19], 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:

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

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

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

הוכחה.

1. נוכיח שהפסוק הראשון גורר את השני.
נניח ש-G נילפוטנטית, תהא $H \leqslant G$ תת-חבורה ונחלק למקרים:

- אם $H \not\leqslant Z(G)$ אז קיים $g \in G$ כך ש-$gHg^{-1} = H$ ו-$g \notin H$, וממילא $H \neq N_G(H)$.
- אם $Z(G) \leqslant H$ ו-$H = N_G(H)$ אז מלמה 7.22 נובע ש-$N_{G/Z(G)}(H/Z(G)) \cong H/Z(G)$, ומכיוון שמדובר בקבוצות סופיות (כי G סופית) נדע ש-$N_{G/Z(G)}(H/Z(G)) = H/Z(G)$.

מהמקרה הקודם נובע ש-$Z(G/Z(G)) \leqslant H/Z(G)$ ולכן ניתן להמשיך בתהליך זה כמה פעמים שנרצה, אם נסמן ב-r את מחלקת הנילפוטנטיות של G אז לאחר $r-1$ פעמים נקבל שהמנרמל של תת-חבורה בחבורה אבלית הוא אותה תת-חבורה ולכן תת-חבורה זו היא כל החבורה אך זה ייתכן אם"ם מראש התחלנו את התהליך עם כל החבורה, כלומר $H = G$.

2. נוכיח שהפסוק השני גורר את השלישי.
נניח שכל תת-חבורה ממש של G היא גם תת-חבורה ממש של המנרמל שלה, ותהא $P \leqslant G$ חבורת p-סילו ($p \in \mathbb{N}$ ראשוני).
מהגדרה $P \trianglelefteq N_G(P) \trianglelefteq N_G(N_G(P))$, מלמה 7.23 נובע ש-$P \trianglelefteq N_G(N_G(P))$ ומכאן ש-$N_G(P) = N_G(N_G(P))$;
מכאן שע"פ ההנחה מתקיים $N_G(P) = G$, כלומר $P \trianglelefteq G$.

3. נוכיח שהפסוק השלישי גורר את הרביעי באינדוקציה על r, אם $r = 1$ הטענה טריוויאלית (כי אז $G = P_1$) ולכן נעבור היישר לצעד האינדוקציה.
נניח שהטענה מתקיימת עבור $r-1$, נניח שכל חבורת p-סילו של G ($p \in \mathbb{N}$ ראשוני) היא תת-חבורה נורמלית, ונסמן $H := P_1 \cdot P_2 \cdot \ldots \cdot P_{r-1}$.
מהיות H מכפלת תתי-חבורות נורמליות של G נובע שגם היא עצמה כזו, כמו כן $H \cap P_r = \{e\}$ משום ש-$|H|$ ו-$|P_r|$ הם מספרים זרים ולכן $G \cong H \times P_r$.
ע"פ הנחת האינדוקציה מתקיים $H \cong P_1 \times P_2 \times \ldots \times P_{r-1}$, ומכאן ש-$G \cong P_1 \times P_2 \times \ldots \times P_r$.

4. את העובדה שהפסוק הרביעי גורר את השלישי ראינו כבר במסקנה 7.21.

■

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-$|N| = d$.

הוכחה. יהיו $p_1, p_2, \ldots, p_r \in \mathbb{N}$ כל הראשוניים **השונים** בפירוק של $|G|$ לראשוניים, ותהיינה $P_1, P_2, \ldots, P_r \leqslant G$ חבורות כך ש-P_i היא חבורת p_i-סילו של G לכל $r \geq i \in \mathbb{N}$.
יהי $d \in \mathbb{N}$ מספר המחלק את $|G|$, ונסמן $e_i := \mathrm{Ord}_{p_i}(d)$ לכל $r \geq i \in \mathbb{N}$; מטענה 6.5 נובע שלכל $r \geq i \in \mathbb{N}$ קיימת תת-חבורה $N_i \trianglelefteq P_i$ כך ש-$|N_i| = (p_i)^{\mathrm{Ord}_{p_i}(d)}$.
תהיינה $N_1, N_2, \ldots, N_r$ תתי-חבורות כנ"ל, מכאן ש-$G \cong P_1 \times P_2 \times \ldots \times P_r \trianglerighteq N_1 \times N_2 \times \ldots \times N_r$ ו-$|N_1 \times N_2 \times \ldots \times N_r| = d$. ■

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

הוכחה. **צריך לכתוב הוכחה.** ■

8 חבורות חופשיות

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

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-$\tilde{f}|_S = f$.

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-$\varphi|_S = \mathrm{Id}_S$; 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-$\varphi|_S = \mathrm{Id}_S$.
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-$\tilde{f}|_S = f$.

♣ 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 $n \geq i \in \mathbb{N}$.