# מבנים אלגבריים 1

*סוכם והוקלד ע"י דינה זליגר*

*מבוסס על הרצאותיו של פרופ' אלכס לובוצקי והתרגולים של עמיחי אייזנמן*

## תוכן עניינים


חבורות והומומורפיזמים ..... 1

תת חבורות ..... 6

החבורה החופשית ..... 10

חבורות מעלגיות ..... 10

מחלקות של תת חבורה ..... 11

החבורה $\mathbb{Z}_n^*$ ..... 14


## חבורות והומומורפיזמים

**הגדרה**: <u>חבורה</u> היא מערכת $(G,\cdot,e)$ [1] כאשר:

- $G$ קבוצה
- $\cdot$ פעולה בינארית על $G$
- $e\in G$

ומתקיימות התכונות הבאות:

1. קשירות: לכל $a,b\in G$ קיים $c\in G$ יחיד כך ש- $a\cdot b=c$ [2]
2. אסוציאטיביות: לכל $a,b,c\in G$ $a\cdot(b\cdot c)=(a\cdot b)\cdot c$
3. איבר יחידה: לכל $a\in G$ $e\cdot a=a=a\cdot e$
4. קיום איבר הופכי: לכל $a\in G$ קיים $b\in G$ כך ש- $a\cdot b=e=b\cdot a$

**טענה**: תהי $G$ חבורה ויהי $a\in G$. אזי יש ל- $a$ הופכי יחיד ב- $G$.

**הוכחה**: נניח ש- $b_1,b_2$ הופכיים של $a$. אזי $ab_1=e=ab_2$. נכפול את שני אגפי המשוואה משמאל ב- $b_1$ ונקבל:

$$b_1=eb_1=(b_1a)b_1=b_1(ab_1)=b_1(ab_2)=(b_1a)b_2=eb_2=b_2$$

לכן ההופכי של $a$ הוא יחיד.

☺

[1] לפעמים נסמן $(G,\cdot)$ או אפילו רק $G$

[2] לפעמים נשמיט את הסימן $\cdot$ ונכתוב רק $ab=c$

**סימון**: תהי $G$ חבורה ויהי $a\in G$. לפי הטענה הקודמת קיים ל- $a$ הופכי יחיד ב- $G$. נסמן את ההופכי של $a$ ב- $a^{-1}$.

**טענה**: תהי $G$ קבוצה ועליה מוגדרת פעולה בינארית $\cdot$ כך שמתקיימות התכונות הבאות:

1. לכל $a,b\in G$ קיים $c\in G$ יחיד כך ש- $a\cdot b=c$
2. לכל $a,b,c\in G$ $a\cdot(b\cdot c)=(a\cdot b)\cdot c$
3. קיים $e\in G$ כך ש- $e\cdot a=a$ לכל $a\in G$
4. לכל $a\in G$ קיים $b\in G$ כך ש- $b\cdot a=e$

אז $(G,\cdot,e)$ חבורה.

**הוכחה**: צריך רק להראות ש- $e$ הוא איבר יחידה ושלכל איבר יש איבר הופכי. נתחיל מההופכי. יהי $a\in G$ ונניח ש- $b\cdot a=e$. אז $b\cdot a\cdot b=e\cdot b=b$ ולכן $(a\cdot b)\cdot(a\cdot b)=a\cdot b$. קיבלנו משוואה מהצורה $x\cdot x=x$. אבל קיים $y$ כך ש- $y\cdot x=e$. לכן $x=e\cdot x=(y\cdot x)\cdot x=y\cdot x=e$. לכן $a\cdot b=e$ אז $b$ הוא ההופכי של $a$ גם מימין וגם משמאל.

כעת, בהינתן $a\in G$ נראה ש- $a\cdot e=a$. ידוע ש- $e\cdot a=a$. נכפול משמאל ב- $a$ ונקבל $a\cdot e\cdot a=a\cdot a$. כעת נכפול ימין ב- $a^{-1}$ ונקבל $a\cdot e=a$.

☺

**טענה**: תהי $G$ חבורה ויהיו $a,b\in G$. אז למשוואה $ax=b$ קיים פיתרון יחיד ב- $G$.

**הוכחה**: ראשית, אם יש שני פתרונות $x_1,x_2$ אז $ax_1=b=ax_2$. ע"י כפל המשוואה משמאל ב- $a^{-1}$ נקבל ש- $x_1=x_2$. מכאן שאם קיים פיתרון אז הוא יחיד. מצד שני, ברור ש- $a^{-1}b$ הוא פיתרון, שהרי $a(a^{-1}b)=(aa^{-1})b=eb=b$. לכן קיים פיתרון וסיימנו.

☺

**טענה**: תהי $G$ חבורה ויהיו $a,b\in G$. אז למשוואה $xa=b$ קיים פיתרון יחיד ב- $G$.

משמעות הטענות היא שבלוח הכפל של חבורה סופית $G$ בכל שורה מופיע כל איבר פעם אחת בדיוק ובכל טור מופיע כל איבר פעם אחת בדיוק. שהרי, נניח שבשורה של $a$ מופיע $b$ פעמיים. פירוש הדבר שיש $x_1,x_2\in G$ כך ש- $ax_1=b=ax_2$. אבל זאת סתירה לטענה. באופן דומה גם בטור לא יכול להופיע אותו האיבר פעמיים.

**דוגמאות**:

1. $(\mathbb{Z},+,0)$ חבורה. ברור שיש קשירות ואסוציאטיביות. $0$ הוא כמובן איבר יחידה ואילו לכל $a\in\mathbb{Z}$ $-a$ הוא האיבר ההופכי שלו, שהרי $a+(-a)=0=(-a)+a$.
2. יהי $(F,+,\cdot)$ שדה. אז $(F,+,0)$ ו- $F^*=(F\setminus\{0\},\cdot,1)$ חבורות. זה נובע באופן מיידי מאקסיומות השדה. למעשה, אם יש קבוצה $G$ ומוגדרות עליה שתי פעולות בינארית קומוטטיביות $+,\cdot$ כך ש- $(G,+,0)$ ו- $(G\setminus\{0\},\cdot,1)$ חבורות ומתקיימת תכונת הדיסטריביוטיביות אז $G$ שדה (זה נובע מהגדרת השדה).

**הגדרה**: חבורה $G$ נקראת <u>חילופית</u> (או <u>קומוטטיבית</u>, או <u>אבלית</u>) אם לכל $a,b\in G$ מתקיים $ab=ba$.

**הגדרה**: תהי $G$ חבורה. אם קיים $n\in\mathbb{N}$ כך ש-$|G|=n$ נאמר ש-$n$ הוא <u>הסדר</u> של $G$ וש-$G$ מסדר $n$.

**הגדרה**: תהיינה $G,H$ חבורות. תהי פונקציה $\varphi:G\to H$.

1. $\varphi$ נקראת <u>הומומורפיזם</u> אם לכל $a,b\in G$ מתקיים $\varphi(a\cdot_G b)=\varphi(a)\cdot_H\varphi(b)$.
2. $\varphi$ נקראת <u>מונומורפיזם</u> אם $\varphi$ הומומורפיזם חח"ע.
3. $\varphi$ נקראת <u>אפימורפיזם</u> אם $\varphi$ הומומורפיזם על.
4. $\varphi$ נקראת <u>איזומורפיזם</u> אם $\varphi$ הומומורפיזם חח"ע ועל. במקרה זה נאמר ש-$G$ ו- $H$ <u>איזומורפיות</u> ונסמן $G\cong H$.

**טענה**: תהיינה $G,H$ חבורות ויהי $\varphi:G\to H$ הומומורפיזם. אזי $\varphi(e_G)=e_H$.

**הוכחה**: מתקיים $\varphi(e_G)=\varphi(e_Ge_G)=\varphi(e_G)\varphi(e_G)$. אבל $\varphi(e_G)=\varphi(e_Ge_G)=e_H\varphi(e_G)$ והפיתרון למשוואה $\varphi(e_G)=x\varphi(e_G)$ הוא יחיד. לכן $\varphi(e_G)=e_H$.

☺

**טענה**: תהיינה $G,H$ חבורות ויהי $\varphi:G\to H$ הומומורפיזם. אזי לכל $a\in G$ מתקיים $\varphi(a^{-1})=(\varphi(a))^{-1}$.

**הוכחה**: מתקיים $\varphi(a^{-1})\varphi(a)=\varphi(a^{-1}a)=\varphi(e_G)=e_H$ ובאותו אופן $\varphi(a)\varphi(a^{-1})=e_H$. לכן מיחידות ההופכי $\varphi(a^{-1})=(\varphi(a))^{-1}$.

☺

**הגדרה**: תהיינה $G,H$ חבורות ויהי $\varphi:G\to H$ הומומורפיזם. נגדיר:

1. <u>הגרעין</u> של $\varphi$ הוא $\operatorname{Ker}\varphi=\{a\in G:\varphi(a)=e_H\}$
2. <u>התמונה</u> של $\varphi$ היא $\operatorname{Im}\varphi=\{a\in H:\exists b\in G(\varphi(b)=a)\}$

**טענה**: תהיינה $G,H$ חבורות ויהי $\varphi:G\to H$ הומומורפיזם. אזי $\varphi$ חח"ע אמ"מ $\operatorname{Ker}\varphi=\{e_G\}$

**הוכחה**:

($\Leftarrow$) נניח ש-$\varphi$ חח"ע ונניח ש-$a\in\operatorname{Ker}\varphi$. אז $\varphi(a)=e_H=\varphi(e_G)$. מהחח"ע של $\varphi$ נובע ש-$a=e_G$. לכן $\operatorname{Ker}\varphi\subset\{e_G\}$. אבל ברור ש-$e_G\in\operatorname{Ker}\varphi$ ולכן $\operatorname{Ker}\varphi=\{e_G\}$.

($\Rightarrow$) נניח בשלילה ש-$\varphi(a)=\varphi(b)$ אבל $a\neq b$. אז $e_H=\varphi(a)(\varphi(b))^{-1}=\varphi(a)\varphi(b^{-1})=\varphi(ab^{-1})$. אבל $\operatorname{Ker}\varphi=\{e_G\}$ ולכן $ab^{-1}=e$. לכן $a=b$ בסתירה.

☺

**דוגמאות**:

1. חבורה מסדר $1$: יש חבורה יחידה מסדר $1$ והיא החבורה הטריוויאלית $G=(\{e\},\cdot,e)$ כאשר $e\cdot e=e$.
גם החבורה $G'=(\{1\},\cdot,1)$ כאשר $1\cdot 1=1$ היא חבורה טריוויאלית. אבל $G\cong G'$. כל החבורות מסדר $1$ הן איזומורפיות ולכך הכוונה שיש חבורה טריוויאלית יחידה.
2. חבורה מסדר $2$: נניח שקיימת חבורה מסדר $2$ $G$. אחד האיברים בחבורה חייב להיות $e$. נסמן את האיבר השני ב- $a$. לוח הכפל בהכרח נראה כך:

| $\cdot$ | $e$ | $a$ |
|---|---|---|
| $e$ | $e$ | $a$ |
| $a$ | $a$ | |

נותר רק לומר מהו $a\cdot a$. אבל מאחר שבכל שורה אמור להופיע כל איבר רק פעם אחת האופציה היחידה היא $a\cdot a=e$. לכן, אם אכן קיימת חבורה מסדר $2$ אז לוח הכפל שלה הוא:

| $\cdot$ | $e$ | $a$ |
|---|---|---|
| $e$ | $e$ | $a$ |
| $a$ | $a$ | $e$ |

אבל ידוע שקיימת חבורה מסדר $2$ והיא $(\mathbb{Z}_2,+)$. לוח הכפל שלה זהה ללוח הכפל של $G$ אך עם שינוי שמות:

| $+$ | $0$ | $1$ |
|---|---|---|
| $0$ | $0$ | $1$ |
| $1$ | $1$ | $0$ |

כל החבורות מסדר $2$ איזומורפיות ל- $\mathbb{Z}_2$!
3. חבורה מסדר $3$: באופן דומה לחישוב שנעשה עבור חבורות מסדר 2 ניתן להראות שלוח הכפל של חבורה מסדר $3$ חייב להיות:

| $\cdot$ | $e$ | $a$ | $b$ |
|---|---|---|---|
| $e$ | $e$ | $a$ | $b$ |
| $a$ | $a$ | $b$ | $e$ |
| $b$ | $b$ | $e$ | $a$ |

מאחר שידוע שקיימת חבורה מסדר $3$ והיא $(\mathbb{Z}_3,+)$ נובע שכל החבורות מסדר $3$ איזומורפיות ל- $\mathbb{Z}_3$.
4. חבורה מסדר $4$: נניח ש- $G=\{e,a,b,c\}$. נמצא את לוחות הכפל האפשריים. ראשית, ברור שמתקיים:

| $\cdot$ | $e$ | $a$ | $b$ | $c$ |
|---|---|---|---|---|
| $e$ | $e$ | $a$ | $b$ | $c$ |
| $a$ | $a$ | | | |
| $b$ | $b$ | | | |
| $c$ | $c$ | | | |

נבחן את האפשרויות להשלמת הלוח ע"י בחינת $a\cdot a$.
א. אם $aa=b$ אז בהכרח $ab=c$ ו- $ac=e$, כי אחרת נקבל ש- $c$ מופיע בעמודה הרביעית פעמיים.
באופן דומה גם $ba=c$ ו- $ca=e$:

| $\cdot$ | $e$ | $a$ | $b$ | $c$ |
|---|---|---|---|---|
| $e$ | $e$ | $a$ | $b$ | $c$ |
| $a$ | $a$ | $b$ | $c$ | $e$ |
| $b$ | $b$ | $c$ | | |
| $c$ | $c$ | $e$ | | |

באותו אופן לא יכול להיות ש- $bc=e$ או ש= $cb=e$ ולכן לוח הכפל הוא בהכרח:

| $\cdot$ | $e$ | $a$ | $b$ | $c$ |
|---|---|---|---|---|
| $e$ | $e$ | $a$ | $b$ | $c$ |
| $a$ | $a$ | $b$ | $c$ | $e$ |
| $b$ | $b$ | $c$ | $e$ | $a$ |
| $c$ | $c$ | $e$ | $a$ | $b$ |

ב. אם $aa=c$ נקבל לוח כפל איזומורפי ללוח הקודם, שהרי אין כל ייחוד ב- $b$ חוץ מאשר היותו שונה מ- $e$. אז ע"י החלפת שמות $b$ ו- $c$ ניתן לקבל שני לוחות איזומורפיים.

ג. אם $aa=e$ אז בהכרח $ac=b$ $ca=b$ ולוח הכפל הוא:

| $\cdot$ | $e$ | $a$ | $b$ | $c$ |
|---|---|---|---|---|
| $e$ | $e$ | $a$ | $b$ | $c$ |
| $a$ | $a$ | $e$ | $c$ | $b$ |
| $b$ | $b$ | $c$ | | |
| $c$ | $c$ | $b$ | | |

כעת יש שתי אפשרויות:

- $bb=e$ ואז לוח הכפל הוא:

| $\cdot$ | $e$ | $a$ | $b$ | $c$ |
|---|---|---|---|---|
| $e$ | $e$ | $a$ | $b$ | $c$ |
| $a$ | $a$ | $e$ | $c$ | $b$ |
| $b$ | $b$ | $c$ | $e$ | $a$ |
| $c$ | $c$ | $b$ | $a$ | $e$ |

זהו לוח כפל שאינו איזומורפי לקודמים שהרי, אם הלוח הזה מגדיר חבורה $G=\{e,a,b,c\}$ וחבורה אחרת $G'=\{e',a',b',c'\}$ איזומורפית לה ע"י $\varphi: i\mapsto i'$ עבור $i\in\{e,a,b,c\}$ אז לכל $i\in G$ מתקיים $\varphi(i\cdot i)=\varphi(e)=e'$ אבל זה הרי לא המצב ב-(א).

- $bb=a$ ואז לוח הכפל הוא:

| $\cdot$ | $e$ | $a$ | $b$ | $c$ |
|---|---|---|---|---|
| $e$ | $e$ | $a$ | $b$ | $c$ |
| $a$ | $a$ | $e$ | $c$ | $b$ |
| $b$ | $b$ | $c$ | $a$ | $e$ |
| $c$ | $c$ | $b$ | $e$ | $a$ |

במקרה זה קיבלנו לוח כפל איזומורפי ללוח הכפל מסעיף (א). אם נחליף כאן את $a$ ב- $b$ ולהפך נקבל את לוח הכפל:

| $\cdot$ | $e$ | $b$ | $a$ | $c$ |
|---|---|---|---|---|
| $e$ | $e$ | $b$ | $a$ | $c$ |
| $b$ | $b$ | $e$ | $c$ | $a$ |
| $a$ | $a$ | $c$ | $b$ | $e$ |
| $c$ | $c$ | $a$ | $e$ | $b$ |

ואם נשנה את סדר העמודות נקבל:

| $\cdot$ | $e$ | $a$ | $b$ | $c$ |
|---|---|---|---|---|
| $e$ | $e$ | $a$ | $b$ | $c$ |
| $b$ | $b$ | $c$ | $e$ | $a$ |
| $a$ | $a$ | $b$ | $c$ | $e$ |
| $c$ | $c$ | $e$ | $a$ | $b$ |

שהוא בדיוק לוח הכפל מ-(א). לכן האופציות איזומורפיות.

אז קיבלנו שאם יש חבורה מסדר $4$ אז לוח הכפל שלה הוא אחד מהבאים:

| $\cdot$ | $e$ | $a$ | $b$ | $c$ |
|---|---|---|---|---|
| $e$ | $e$ | $a$ | $b$ | $c$ |
| $a$ | $a$ | $e$ | $c$ | $b$ |
| $b$ | $b$ | $c$ | $e$ | $a$ |
| $c$ | $c$ | $b$ | $a$ | $e$ |

או

| $\cdot$ | $e$ | $a$ | $b$ | $c$ |
|---|---|---|---|---|
| $e$ | $e$ | $a$ | $b$ | $c$ |
| $a$ | $a$ | $b$ | $c$ | $e$ |
| $b$ | $b$ | $c$ | $e$ | $a$ |
| $c$ | $c$ | $e$ | $a$ | $b$ |

נשים לה שהאופציה הימנית איזומורפית לשדה מסדר $4$ עם מציין $2$ והאופציה השמאלית איזומורפית ל- $(\mathbb{Z}_4,+)$. לכן קיימות בדיוק שתי חבורות מסדר $4$ והם השדה מסדר $4$ ו- $\mathbb{Z}_4$.

עד עכשיו ראינו רק דוגמאות לחבורות קומוטטיביות. אבל לא כל החבורות הן כאלה.

**דוגמאות**:

1. תהי $X$ קבוצה. נסמן ב- $\mathrm{Perm}(X)$ את קבוצת התמורות מ- $X$ ל- $X$. זוהי חבורה ביחס להרכבת פונקציות. הסיבה לכך נעוצה בכך שפונקציה חח"ע ועל היא הפיכה ואילו הרכבת פונקציות הפיכות היא פונקציה הפיכה. זוהי כמובן לא חבורה קומוטטיבית.
מקרה מיוחד הוא חבורת התמורות $S_n = \mathrm{Perm}(\{1,...,n\})$ שבה נדון עוד הרבה.
2. יהי $F$ שדה. נסמן $GL_n(F)=\{A\in M_n(F):\det A\neq 0\}$. זוהי קבוצת המטריצות ההפיכות מעל $F$. זוהי חבורה ביחס לכפל מטריצות. הכפליות של הדטרמיננטה היא הסיבה לכך שהקבוצה סגורה תחת כפל ושיש איבר הופכי לכל מטריצה בקבוצה.
3. יהי $F$ שדה. נסמן $SL_n(F)=\{A\in GL_n(F):\det A=1\}$. זוהי חבורה ביחס לכפל מטריצות. הסגירות וקיום ההופכי נובעים מהכפליות של הדטרמיננטה. שהרי, אם $A,B\in SL_n(F)$ אז $\det(AB)=\det A\cdot\det B=1\cdot 1=1$ ולכן $AB\in SL_n(F)$, וכן $\det A^{-1}=(\det A)^{-1}=1^{-1}=1$ ולכן $A^{-1}\in SL_n(F)$.
4. נסמן ב- $O(n)$ את המטריצות האורתוגונליות[3] מעל $\mathbb{R}$ מסדר $n$. זוהי חבורה ביחס לכפל מטריצות. איבר היחידה הוא מטריצת היחידה.
5. נסמן ב- $U(n)$ את אוסף המטריצות האוניטריות[4] מעל $\mathbb{C}$ מסדר $n$. זוהי חבורה ביחס לכפל מטריצות. איבר היחידה הוא מטריצת היחידה.

## תת חבורות

**הגדרה**: תהי $G$ חבורה. תת קבוצה $H\subset G$ נקראת <u>תת חבורה</u> (או <u>חבורה חלקית</u>) של $G$ אם מתקיימים התנאים הבאים:

1. $H\neq\varnothing$
2. לכל $a,b\in H$ גם $ab\in H$
3. לכל $a\in H$ גם $a^{-1}\in H$

במקרה זה מסמנים $H\leq G$.

---

[3] מטריצה אורתוגונלית היא מטריצה $A\in M_n(\mathbb{R})$ שמקיימת $AA^T=I=A^TA$

[4] מטריצה אוניטרית היא מטריצה $A\in M_n(\mathbb{C})$ שמקיימת $AA^*=I=A^*A$ כאשר $A^*=\overline{A}^T$

**טענה**: תהי $G$ חבורה ו- $H \le G$. אזי $e \in H$.

**הוכחה**: $H \le G$ ולכן $H \ne \varnothing$. בפרט קיים $a \in H$. אבל גם $a^{-1} \in H$ ו- $H$ סגורה לכפל. לכן $e = aa^{-1} \in H$.

☺

**מסקנה**: אם $H \le G$ אז $H$ חבורה ביחס לאותה הפעולה של $G$.

**הוכחה**: מתקיימות כל התכונות של חבורה: $H$ סגורה לכפל ולהופכי כי $H \le G$. אסוציאטיביות של הפעולה מתקיימת ב- $H$ כי היא מתקיימת ב- $G$ ואיבר היחידה הוא $e \in H$.

☺

**דוגמה**: $(\mathbb{R},+,0)$ חבורה ומתקיים $R\setminus\{0\} \subset \mathbb{R}$ אבל $(\mathbb{R}\setminus\{0\},\cdot,1)$ אינה תת חבורה של $(\mathbb{R},+,0)$ משום שלא מדובר על אותה הפעולה!

**טענה**: תהי $G$ חבורה ונניח ש- $H \subset G$ תת קבוצה לא ריקה אזי $H$ תת חבורה של $G$ אמ"מ לכל $a,b \in H$ גם $a^{-1}b \in H$.

**הוכחה**:

($\Leftarrow$) יהיו $a,b \in H$. בגלל הסגירות של $H$ להופכי נובע ש- $a^{-1} \in H$ ובגלל הסגירות של $H$ לכפל נובע ש- $a^{-1}b \in H$.

($\Rightarrow$) יש להראות שמתקיימות התכונות שבהגדרת חבורה חלקית. ואכן, נתון ש- $H$ אינה ריקה. כעת, יהיו $a,b \in H$. לפי הנתון גם $e = a^{-1}a \in H$. ולכן גם $a^{-1} = a^{-1}e \in H$. מכאן ש- $\left(a^{-1}\right)^{-1} b \in H$. אבל $\left(a^{-1}\right)^{-1} = a$ ולכן $ab \in H$.

☺

**דוגמה**: יהי $F$ שדה. נסמן ב- $T_n(F)$ את קבוצת המטריצות המשולשיות העליונות ההפיכות מסדר $n$ מעל $F$ וב- $U_n(F)$ את המטריצות האוניפוטנטיות[5] מסדר $n$ מעל $F$.

נראה שאלה תת חבורות של $GL_n(F)$.

ראשית, ברור ש- $I \in T_n(F), U_n(F)$ ולכן אלה קבוצות לא ריקות. כעת, יהיו $A,B \in T_n(F)$ ונסמן $C = AB$. ברור ש- $C$ הפיכה כי היא מכפלה של הפיכות. נראה ש- $C_{i,j} = 0$ עבור $i > j$ ונקבל ש- $T_n$ משולשית עליונה.

מתקיים $C_{i,j} = \sum_{k=1}^{n} A_{i,k}B_{k,j}$. אם $i > k$ אז $A_{i,k} = 0$ ואם $k > j$ אז $B_{k,j} = 0$. לכן $A_{i,k}B_{k,j} \ne 0$ רק אם $i \le k$ וגם $j \le k$. אז אם $i > j$ מתקיים $C_{i,j} = 0$.

אם $A,B \in U_n(F) \subset T_n(F)$ אז $C = AB$ היא מטריצה משולשית עליונה הפיכה. נראה ש- $C_{i,i} = 1$ לכל $1 \le i \le n$ ואכן מתקיים:

[5] מטריצה $A \in M_n(F)$ היא אומניפוטנטית אם היא משולשית עליונה וכן $A_{i,i} = 1$ לכל $1 \le i \le n$

$$C_{i,i}=\sum_{k=1}^{n}A_{i,k}B_{k,i}=\sum_{k=1}^{i-1}A_{i,k}B_{k,i}+A_{i,i}B_{i,i}+\sum_{k=i+1}^{n}A_{i,k}B_{k,i}=$$
$$=\sum_{k=1}^{i-1}0\cdot B_{k,i}+A_{i,i}B_{i,i}+\sum_{k=i+1}^{n}A_{i,k}\cdot 0=A_{i,i}B_{i,i}=1\cdot 1=1$$

נותר להראות שהקבוצות סגורות להופכי.

נניח ש- $A\in U_n(F)$ . אז $A=I-N$ כאשר $N$ נילפוטנטית[6]. נניח ש- $N^{k+1}=0$ . אז מתקיים:

$$(I-N)\left(I+N+N^2+...+N^k\right)=$$
$$=\left(I+N+N^2+...+N^k\right)-\left(N+N^2+N^3+...+N^{k+1}\right)=$$
$$=I-N^{k+1}=I-0=I$$

אז $I+N+N^2+...+N^k$ היא ההופכית של $A=I-N$ . אבל $I+N+N^2+...+N^k$ כמובן אומניפוטנטית כי זה סכום של מטריצת היחידה עם מטריצות משולשיות עליונות שבהן על האלכסון הראשי יש אפסים.

כעת, אם $A\in T_n(F)$ אז $A=DB$ כאשר $D$ מטריצה אלכסונית הפיכה ו- $B\in U_n(F)$ . זו מכפלה של מטריצות הפיכות ולכן הפיכה. מאחר ש- $B^{-1}\in U_n(F)$ ו- $D^{-1}$ אלכסונית מתקבל $A^{-1}\in T_n(F)$ .

בזאת הוכחנו ש- $T_n(F)$ ו- $U_n(F)$ חבורות חלקיות של $GL_n(F)$ .

נניח ש- $F=\mathbb{Z}_q$ עבור $q$ ראשוני ונחשב את הגדלים של החבורות.

ראשית, נחשב את $\left|GL_n(F)\right|$ . ידוע שמטריצה היא הפיכה אמ"מ העמודות שלה הן בלתי תלויות לינארית. עבור העמודה הראשונה ניתן לבחור כל וקטור אפשרי פרט לווקטור האפס. לכן יש $q^n-1$ אפשרויות שונות לעמודה הראשונה. העמודה השנייה יכולה להיות כל ווקטור פרט לכפולה של העמודה הראשונה. יש $q$ איברים בשדה ולכן $q$ כפולות של העמודה הראשונה. מכאן שיש $q^n-q$ אפשרויות שונות לעמודה השנייה. העמודה השלישית לא יכולה להיות צירוף לינארי של העמודות הראשונה והשנייה. אם $\alpha$ העמודה הראשונה ו- $\beta$ העמודה השנייה אז הצירופים הלינאריים, כלומר האפשרויות הפסולות עבור העמודה השלישית הן מהצורה $a\alpha+b\beta$ כאשר $a,b\in F$ . יש $q^2$ צירופים לינאריים כאלה ולכן לעמודה השלישית יש $q^n-q^2$ אפשרויות. באופן כללי לעמודה ה- $i$ יש $q^n-q^{i-1}$ אפשרויות. לכן $\left|GL_n(G)\right|=\prod_{i=0}^{n-1}\left(q^n-q^i\right)$ . נפתח מעט:

$$\left|GL_n(G)\right|=\prod_{i=0}^{n-1}\left(q^n-q^i\right)=\left(q^n-q^0\right)\left(q^n-q^1\right)\left(q^n-q^2\right)...\left(q^n-q^{n-1}\right)=$$
$$=\left(q^n-1\right)q\left(q^{n-1}-1\right)q^2\left(q^{n-2}-1\right)...q^{n-1}\left(q-1\right)=q^0q^1q^2...q^{n-1}\prod_{i=1}^{n}\left(q^i-1\right)=$$
$$=q^{\sum_{i=1}^{n-1}i}\prod_{i=1}^{n}\left(q^i-1\right)=q^{\frac{n(n-1)}{2}}\prod_{i=1}^{n}\left(q^i-1\right)$$

כעת נחשב את $\left|U_n(F)\right|$ . ידוע שעל האלכסון הראשי מופיעות רק אחדות ולכן המטריצה הפיכה. לכן יש חופש מוחלט בבחירת האיברים שמעל האלכסון הראשי. יש $\sum_{i=1}^{n-1}i=\frac{n(n-1)}{2}$ איברים מעל האלכסון הראשוני ולכן $\left|U_n(F)\right|=q^{\frac{n(n-1)}{2}}$ . נשים לב ש- $q^{\frac{n(n-1)}{2}}$ היא החזקה המקסימלית של $q$ שמחלקת את $\left|GL_n(F)\right|$ . במקרה זה $U_n(F)$ נקראת חבורת $q$-סילוא של $GL_n(F)$ . אנחנו עוד נלמד על זה בעתיד.

---

[6] מטריצה $A\in M_n(F)$ נקראת נילפוטנטית אם קיים $k\in\mathbb{N}$ כך ש- $A^k=0$ . מטריצה משולשית עליונה שבה לכל $1\le i\le n$ מתקיים $A_{i,i}=0$ היא נילפוטנטית.

הגודל של $T_n(F)$ קל לחישוב. כדי שמטריצה משולשית עליונה תהיה הפיכה אסור שבאלכסון הראשוני יופיע אפס. לכן לאיברי האלכסון יש $(q-1)^n$ אופציות. כמו קודם, לאיברים שמעל האלכסון הראשי יש $q^{\frac{n(n-1)}{2}}$ אפשרויות ולכן $|T_n(F)| = q^{\frac{n(n-1)}{2}}(q-1)^n$.

**דוגמה**: נסתכל על $G=\mathbb{Z}$ עם פעולת החיבור. יהיו $H_1 = 5\mathbb{Z}$ ו- $H_2 = 7\mathbb{Z}$. קל לראות שאלה הן תת חבורות. כמו כן מתקיים $H_1 \cap H_2 = 35\mathbb{Z} = H \le G$. מצד שני, $H_1 \cup H_2$ אינה תת חבורה משום ש- $3,7 \in H_1 \cup H_2$ אבל $12 = 5+7 \notin H_1 \cup H_2$ שהרי $5 \nmid 12$ וגם $7 \nmid 12$.

**טענה**: תהי $G$ חבורה ויהי $\{H_i\}_{i\in I}$ אוסף של תת חבורות של $G$. אזי $H = \bigcap_{i\in I} H_i$ תת חבורה של $G$.

**הוכחה**: לכל $i \in I$ מתקיים $e \in H_i$ ולכן $e \in H$ ובפרט $H \neq \varnothing$. כעת, נניח ש- $a,b \in H$. אז $a,b \in H_i$ לכל $i \in I$. לכן $a^{-1}b \in H_i$ לכל $i \in I$ ולכן $a^{-1}b \in H$. לכן $H \le G$.

☺

**מסקנה**: תהיינה $G$ חבורה ו- $S \subset G$ תת קבוצה. אזי $\hat{S} = \bigcap_{\substack{H \le G \\ S \subset H}} H$ תת החבורה המינימלית של $G$ שמכילה את $S$.

**הוכחה**: לפי הטענה הקודמת, $\hat{S}$ תת חבורה שהרי היא חיתוך של תת חבורות. ברור גם שהיא מינימלית. שהרי אם הייתה $H \le \hat{S}$ כך ש- $S \subset H \neq \hat{S}$ אז $H$ הייתה חלק מהחיתוך שמגדיר את $\hat{S}$ ולכן $\hat{S} \le H$ וזו סתירה לכך ש- $H \neq \hat{S}$.

☺

**הגדרה**: תהיינה $G$ חבורה ו- $S \subset G$ תת קבוצה. אזי $\hat{S} = \bigcap_{\substack{H \le G \\ S \subset H}} H$ נקראת <u>החבורה החלקית הנוצרת</u> ע"י $S$.

**טענה**: תהי $G$ חבורה ותהי $S \subset G$ תת קבוצה. נסמן

$$\langle S \rangle = \left\{ x_1^{\varepsilon_1} \dots x_n^{\varepsilon_n} : n \in \mathbb{N} \cup \{0\} \wedge \forall 1 \le i \le n \left( \varepsilon_i \in \{+1,-1\} \wedge x_i \in S \right) \right\}$$ [7]

אזי $\langle S \rangle = \hat{S}$.

**הוכחה**: אם נראה ש- $\langle S \rangle$ תת חבורה שמכילה את $S$ אז מהמינימליות של $\hat{S}$ ינבע ש- $\langle S \rangle = \hat{S}$. ואכן, ראשית ברור ש- $S \subset \langle S \rangle$ שהרי לכל $a \in S$ מתקיים $a = a^1 \in \langle S \rangle$.

אז נותר להראות ש- $\langle S \rangle$ תת חבורה. ואכן, אם $a,b \in \langle S \rangle$ נניח ש- $a = x_1^{\varepsilon_1} \dots x_n^{\varepsilon_n}$ ו- $b = y_1^{\delta_1} \dots y_m^{\delta_m}$ אז $a^{-1}b = y_m^{-\delta_m} \dots y_1^{-\delta_1} x_1^{\varepsilon_1} \dots x_n^{\varepsilon_n}$ ומתקיים $\{x_i\} \subset S$ ו- $\{y_j\} \subset S$. כמו כן $\delta_j, \varepsilon_i \in \{+1,-1\}$ לכל $1 \le i \le n$ ולכל $1 \le j \le m$ ולכן גם $-\delta_j \in \{+1,-1\}$ לכל $1 \le j \le m$. לכן $a^{-1}b = y_m^{-\delta_m} \dots y_1^{-\delta_1} x_1^{\varepsilon_1} \dots x_n^{\varepsilon_n} \in \langle S \rangle$ וסיימנו.

---

[7] עבור $n=0$ מוגדר $x_1^{\varepsilon_1} \dots x_n^{\varepsilon_n} = e$

☺

**דוגמאות:**

1. נניח ש- $S=\{x\}\subset G$ עבור חבורה $G$. אז $\langle S\rangle=\{x^n : n\in\mathbb{Z}\}$.
2. נסתכל על החבורה $(\mathbb{Z},+,0)$ ועל $S=\{3\}$. אז $\langle S\rangle=3\mathbb{Z}$. אם $S=\{3,7\}$ נטען ש- $\langle S\rangle=\mathbb{Z}$. מספיק להראות ש- $1\in\langle S\rangle$ כי אז ע"י חיבור וחיסור ניתן לקבל כל מספר שלם. ואכן $1\in\langle S\rangle$ משום ש- $1=7+(-3)+(-3)$.
3. אם $G=\mathbb{Z}_n$ אז $G=\langle 1\rangle$.

## החבורה החופשית

**הגדרה**: תהי $X$ קבוצה. נגדיר קבוצה חדשה $X^{-1}$ שזרה ל- $X$ ויש התאמה חח"ע ועל $x\mapsto x^{-1}$ כאשר $x\in X$ ו- $x^{-1}\in X^{-1}$. <u>מילה</u> על $X$ היא סדרה $w=(a_1,a_2,...,a_n,...)$ כאשר $a_i\in X\cup X^{-1}\cup\{1\}$ ו- $a_n=1$ החל ממקום מסוים. המילה $(1,1,1,...)$ נקראת <u>המילה הריקה</u>. אם $w$ מילה כך ש- $a_k=1$ לכל $k>n$ נכתוב אותה כ- $w=x_1^{\varepsilon_1}...x_n^{\varepsilon_n}$ כאשר $x_i\in X$, $\varepsilon_i\in\{0,1,-1\}$ עבור $i<n$ ו- $\varepsilon_n\in\{1,-1\}$ ונגדיר $x^0=1$ המילה הריקה. בהינתן מילה $w=x_1^{\varepsilon_1}...x_n^{\varepsilon_n}$ נגדיר את <u>ההופכי</u> של $w$ להיות $x_n^{-\varepsilon_n}...x_1^{-\varepsilon_1}$. מילה $w=x_1^{\varepsilon_1}...x_n^{\varepsilon_n}$ תיקרא <u>מצומצמת</u>

## חבורות מעלגיות

**הגדרה**: תהי $G$ חבורה. נאמר ש- $G$ <u>מעגלית</u> (או <u>ציקלית</u>) אם קיים $a\in G$ כך ש- $G=\langle\{a\}\rangle$. במקרה זה נסמן $G=\langle a\rangle$.

**טענה**: תהי $G$ חבורה ציקלית. אזי $G$ אבלית.

**הוכחה**: נניח ש- $G=\langle a\rangle$. יהיו $x,y\in G$. אזי קיימים $n,m\in\mathbb{Z}$ כך ש- $x=a^n$ ו- $y=a^m$. לכן $xy=a^na^m=a^{n+m}=a^{m+n}=a^ma^n=yx$ ו- $G$ אבלית.

☺

**דוגמה**: נסתכל על $(\mathbb{R},+,0)$. זאת חבורה אבלית אבל היא לא ציקלית. זה נובע משיקולי עוצמה. אילו היה $a\in\mathbb{R}$ כך ש- $\mathbb{R}=\langle a\rangle=\{a^n : n\in\mathbb{Z}\}$ היינו מקבלים ש- $\mathbb{R}$ בת מניה וזה לא נכון.

**טענה**: תהי $G$ חבורה ציקלית.

א. אם $G$ אינסופית אז $G\cong\mathbb{Z}$
ב. אם $G$ סופית מסדר $n$ אז $G\cong\mathbb{Z}_n$

הוכחה: נתון ש- $G=\langle a\rangle=\{a^n : n\in\mathbb{Z}\}$. יש שתי אפשרויות:

א. לכל $k \neq l$ $a^k \neq a^l$. בפרט $G$ אינסופית. נגדיר העתקה $\varphi:\mathbb{Z}\to G$ ע"י $\varphi(n)=a^n$. צריך להראות שזה איזומורפיזם. ואכן, $\varphi$ הומומורפיזם כי לכל $x,y\in\mathbb{Z}$ מתקיים $\varphi(x+y)=a^{x+y}=a^xa^y=\varphi(x)\varphi(y)$. $\varphi$ היא על כי $G=\langle a\rangle=\{a^n:n\in\mathbb{Z}\}$ והיא חח"ע כי הנחנו שלכל $k\neq l$ $a^k\neq a^l$. אז מצאנו איזומורפיזם $\varphi:\mathbb{Z}\to G$. לכן $G\cong\mathbb{Z}$.

ב. קיימים $k<l$ כך ש- $a^k=a^l$. אז $a^{l-k}=e$. פירוש הדבר שיש $m\in\mathbb{N}$ כך ש- $a^m=e$. יהי $n=\min\{m\in\mathbb{N}:a^m=e\}$. המינימום קיים כי זו קבוצה לא ריקה של מספרים טבעיים. נטען ש- $G=\{e,a,...,a^{n-1}\}$. ברור ש- $\{e,a,...,a^{n-1}\}\subset G$. מצד שני נניח ש- $a^k\in G$ ונניח ש- $k=qn+r$ כאשר $0\le r<n$. אז $a^k=a^{qn+r}=a^{qn}a^r=a^{nq}a^r=(a^n)^q a^r=e^qa^r=ea^r=a^r$. אבל $0\le r<n$ ולכן $a^k\in\{e,a,...,a^{n-1}\}$. לכן $G=\{e,a,...,a^{n-1}\}$. כעת, נטען שכל האיברים בקבוצה שונים. ואכן אילו היו $0\le i<j\le n-1$ כך ש- $a^i=a^j$ היינו מקבלים ש- $a^{j-i}=e$ ו- $j-i<n$ וזו סתירה למינימליות של $n$. לכן $G=\{e,a,...,a^{n-1}\}$ ו- $|G|=n$. כעת נגדיר העתקה $\varphi:\mathbb{Z}_n\to G$ ע"י $\varphi(k)=a^k$. זה הומומורפיזם כי $\varphi(k+_n l)=a^{k+_n l}$ ואם $k+l<n$ אז פשוט $\varphi(k+_n l)=a^{k+_n l}=a^ka^l=\varphi(k)\varphi(l)$ ואם $k+l>n$ אז נניח $k+l=n+r$ כאשר $r<n-1$ אז $\varphi(k+_n l)=a^{k+_n l}=a^r=ea^r=a^na^r=a^{n+r}=a^{k+l}=\varphi(k)\varphi(l)$. $\varphi$ על כי $G=\{e,a,...,a^{n-1}\}$ והיא חח"ע כי אם $0\le i<j\le n-1$ אז $a^i\neq a^j$. אז $\varphi$ איזומורפיזם ו- $G\cong\mathbb{Z}_n$.

☺

**הגדרה**: תהי $G$ חבורה ויהי $a\in G$. נגדיר את <u>הסדר</u> של $a$ ע"י $o(a)=\min\{n:n>0\wedge a^n=e\}$. אם אין כזה נאמר שהסדר של $a$ הוא אינסוף.

**מסקנה**: תהי $G$ חבורה ויהי $a\in G$. תהי $H=\langle\{a\}\rangle$ תת החבורה הנוצרת ע"י $a$. אזי $|H|=o(a)$.

**הוכחה**: ראינו שמאחר ש- $H$ ציקלית אז $H\cong\mathbb{Z}$ או $H\cong\mathbb{Z}_n$ עבור $n$ כלשהו. אם $o(a)=\infty$ אז $H$ אינסופית ולכן $|H|=o(a)$. נניח כעת ש- $o(a)=n$. מההגדרה של $o(a)$ נובע שבקבוצה $\{e,a,...,a^{n-1}\}$ יש $n$ איברים שונים. ברור ש- $\{e,a,...,a^{n-1}\}\subset H$. מצד שני אם $a^k\in H$ ונניח ש- $k=qn+r$ כאשר $0\le r<n$. אז $a^k=a^{qn+r}=a^{qn}a^r=a^{nq}a^r=(a^n)^q a^r=e^qa^r=ea^r=a^r$. אבל $0\le r<n$ ולכן $a^k\in\{e,a,...,a^{n-1}\}$. לכן $H=\{e,a,...,a^{n-1}\}$. אז $|H|=n=o(a)$.

☺

## מחלקות של תת חבורה

**הגדרה**: תהי $X$ קבוצה. <u>יחס</u> על $X$ הוא תת קבוצה $R\subset X\times X$. אם $(a,b)\in R$ נסמן $a\sim_R b$. יחס $R$ נקרא <u>יחס שקילות</u> אם הוא מקיים את שלושת התכונות הבאות:

1. <u>רפלקסיביות</u>: לכל $x\in X$ $x\sim_R x$
2. <u>סימטריות</u>: לכל $x,y\in X$ אם $x\sim_R y$ אז $y\sim_R x$
3. <u>טרנזיטיביות</u>: לכל $x,y,z\in X$ אם $x\sim_R y$ וגם $y\sim_R z$ אז $x\sim_R z$

אם $R$ יחס שקילות ו- $x \sim_R y$ נאמר ש- $x$ ו- $y$ <u>שקולים</u>.

לכל $x \in X$ נגדיר את <u>מחלקת השקילות</u> של $x$ ע"י קבוצת האיברים ששקולים לו $[x] = \{y \in X : x \sim_R y\}$.

**דוגמה**: נסתכל על $X = \mathbb{Z}$. היחס $\leq$ הוא רפלקסיבי וטרנזיטיבי אבל הוא לא סימטרי. היחס $<$ הוא רק טרנזיטיבי. היחס $\equiv (\bmod n)$ לכל $n$ הוא יחס שקילות.

**טענה**: יחס שקילות על $X$ מחלק את $X$ למחלקות שקילות זרות שאיחודן הוא כל $X$.

**הוכחה**: ברור ש- $X = \bigcup_{x \in X} [x]$. נראה ש- $[x] \cap [y] = \varnothing$ או $[x] = [y]$. נניח ש- $z \in [x] \cap [y]$. אז $x \sim z$ וגם $y \sim z$. אבל בגלל הסימטריות $z \sim y$ ולכן בגלל הטרנזיטיביות $x \sim y$ ומכאן ש- $[x] = [y]$.

☺

**הגדרה**: תהי $G$ חבורה ונניח ש- $H \leq G$ חבורה חלקית. יהיו $a,b \in G$. נאמר ש- $a$ ו- $b$ <u>שקולים מודולו</u> $H$ ונסמן $a \equiv b (\bmod H)$ אם $a^{-1}b \in H$.

**טענה**: תהי $G$ חבורה ונניח ש- $H \leq G$ חבורה חלקית. אזי היחס $\equiv (\bmod H)$ יחס שקילות.

**הוכחה**: צריך להראות שמתקיימות שלושת התכונות:

1. רפלקסיביות: בגלל ש- $H$ חבורה $a^{-1}a = e \in H$ לכל $a \in G$ ולכן $a \equiv a (\bmod H)$.
2. סימטריות: נניח ש- $a \equiv b (\bmod H)$. אז $a^{-1}b \in H$. אז גם $b^{-1}a = (a^{-1}b)^{-1} \in H$, כלומר $b \equiv a (\bmod H)$.
3. טרנזיטיביות: נניח ש- $a \equiv b (\bmod H)$ וגם $b \equiv c (\bmod H)$. אז $a^{-1}b, b^{-1}c \in H$ ולכן גם המכפלה $(a^{-1}b)(b^{-1}c) = a^{-1}c \in H$, ז"א $a \equiv c (\bmod H)$.

☺

**דוגמה**: נסתכל על $G = \mathbb{Z}$ ועל $H = 2\mathbb{Z}$ קבוצת הזוגיים. אז $a$ ו- $b$ שקולים מודולו $H$ אמ"מ $b - a \in 2\mathbb{Z}$, כלומר אמ"מ ההפרש ביניהם זוגי. פירוש הדבר שכל המספרים הזוגיים שקולים אחד לשני וכל המספרים האי זוגיים שקולים אחד לשני. באופן כללי, אם $H = n\mathbb{Z}$ אז $a \equiv b (\bmod H)$ אמ"מ $a \equiv b (\bmod n)$.

**טענה**: תהי $G$ חבורה ותהי $H \leq G$ חבורה חלקית. אז $[a] = aH = \{ah : h \in H\}$.

**הוכחה**: נראה הכלה בשני הכיוונים. אם $b \in [a]$ אז $a \equiv b (\bmod H)$, כלומר $a^{-1}b \in H$. אז קיים $h \in H$ כך ש- $a^{-1}b = h$. לכן $b = ah$ ו- $b \in aH$. אז $[a] \subset aH$. מצד שני, אם $ah \in aH$ אז $a^{-1}(ah) = h \in H$ ולכן $a \equiv ah (\bmod H)$ ו- $ah \in [a]$. אז $aH \subset [a]$ וסיימנו.

☺

**דוגמה**: נשים לב שהמחלקות $aH$ הן לא בהכרח תת חבורות. למשל, אם $G$ מרחב וטורי ו- $H$ תת מרחב אז עבור $a \neq e$ $aH$ היא ישרייה ולא תת מרחב!

**הגדרה**: תהי $G$ חבורה ותהי $H \le G$ תת חבורה. אז $aH$ נקראת <u>המחלקה השמאלית</u> של $H$ שמכילה את $a$ ו- $Ha$ נקראת <u>המחלקה הימנית</u> של $H$ המכילה את $a$[8].

מספר המחלקות השמאליות של $H$ ב- $G$ נקרא <u>האינדקס</u> של $H$ ב- $G$ ומסומן ב- $[G:H]$.

חשוב לשים לב שלא בכרח $aH = Ha$, שהרי חבורה היא לא בהכרח קומוטטיבית.

**דוגמה**: יכול להיות מצב שבו $H \le G$ אינסופית אבל האינדקס שלה ב- $G$ הוא סופי. למשל, לכל $n \in \mathbb{N}$ $[\mathbb{Z}:n\mathbb{Z}] = n$.

**טענה**: תהי $G$ חבורה ותהי $H \le G$. תהיינה $aH, bH$ שתי מחלקות שמאליות של $H$ ב- $G$. אזי קיימת פונקציה חח"ע ועל $f: aH \to bH$ ובפרט $|aH| = |bH|$.

**הוכחה**: נגדיר $f: aH \to bH$ ע"י $f(ah) = bh$. $f$ מוגדרת היטב משום שכל איבר $c \in aH$ ניתן לכתיבה באופן יחיד כ- $ah$. שהרי אם $ah = ah'$ אז $h = h'$. נגדיר $g: bH \to aH$ ע"י $g(bh) = ah$. $g$ מוגדרת היטב מאותה סיבה כמו $f$ ומתקיים $f(g(bh)) = g(ah) = bh$ ו- $g(f(ah)) = g(bh) = ah$ ולכן $f^{-1} = g$. כלומר, $f$ הפיכה ולכן חח"ע ועל. מכאן גם ש- $|aH| = |bH|$.

☺

**מסקנה**: תהי $G$ חבורה סופית ותהי $H \le G$. אזי $|G| = [G:H]|H|$

**הוכחה**: יחס השקילות מודולו $H$ מחלק את $G$ ל- $[G:H]$ מחלקות שקילות זרות. אבל לפי הטענה הקודמת המחלקות הן שוות גודל. אחת המחלקות היא $eH = H$. לכן $|G| = [G:H]|H|$.

☺

**משפט לגרנז'**: תהי $G$ חבורה סופית ותהי $H \le G$. אזי $|H| \mid |G|$.

**הוכחה**: לפי המסקנה הקודמת $|G| = [G:H]|H|$. בפרט, $|H| \mid |G|$.

☺

**מסקנה**: תהי $G$ סופית. אז לכל $a \in G$ $o(a) \mid G$.

**הוכחה**: $o(a) = |\langle a \rangle|$. לפי משפט לגרנז' $|\langle a \rangle| \mid G$ שהרי $\langle a \rangle \le G$. לכן $o(a) \mid G$.

☺

**מסקנה**: תהי $G$ חבורה מסדר ראשוני $p$. אזי $G \cong \mathbb{Z}_p$.

**הוכחה**: יהי $e \ne a \in G$. אז $1 < o(a)$ ו- $o(a) \mid p$. אבל $p$ ראשוני ולכן $o(a) = p$. לכן $|\langle a \rangle| = p$. אבל $\langle a \rangle \le G$ ולכן $G = \langle a \rangle$. אז $G$ ציקלית מסדר $p$ ולכן $G \cong \mathbb{Z}_p$.

---

[8] המחלקות הימניות $Ha$ מתקבלות ע"י הגדרת יחס שקילות $a \equiv b \pmod{H}$ אמ"מ $ab^{-1} \in H$.

☺

**מסקנה**: תהי $G$ חבורה סופית מסדר $n$. אז לכל $g \in G$ מתקיים $g^n = e$.

**הוכחה**: מתקיים $o(g) \mid n$. אז $n = o(g)k$. לכן $g^n = g^{o(g)k} = \left(g^{o(g)}\right)^k = e^k = e$.

☺

## החבורה $\mathbb{Z}_n^*$

**הגדרה**: יהיו $a,b \in \mathbb{Z}$. נאמר ש-$d \in \mathbb{Z}$ הוא <u>מחלק משותף מקסימלי</u> של $a$ ו- $b$ ונסמן $(a,b) = d$ אם $d \mid a$ ו- $d \mid b$ ולכל $d' \in \mathbb{Z}$ כך ש-$d' \mid a$ וגם $d' \mid b$ מתקיים $d' \mid d$.

נאמר ש-$a$ ו- $b$ <u>זרים</u> אם $(a,b) = 1$.

**טענה**: יהיו $a,b \in \mathbb{Z}$. אזי קיימים $x,y \in \mathbb{Z}$ כך ש-$ax + by = (a,b)$.

**הוכחה**: נסמן $s = \min\{ax + by : x,y \in \mathbb{Z} \wedge ax + by > 0\}$ ונניח ש-$s = ax + by$. נניח ש-$a = qs + r$ כאשר $0 \le r < s$. אז $a \bmod s = r = a - qs = a - q(ax + by) = a(1 - qx) + b(-qy)$. אז הוא גם צירוף לינארי של $a$ ו- $b$. אבל $s$ הוא הצירוף הלינארי המינימלי ו- $0 \le a \bmod s < s$ ולכם $a \bmod s = 0$. אז $a = qs$ ו- $s \mid a$. באופן דומה $s \mid b$. לכן $s$ מחלק משותף של $a$ ו- $b$. אבל ברור שאם $d \mid a$ וגם $d \mid b$ אז $d \mid (ax + by)$. לכן $d \mid s$. לכן $(a,b) = s$.

☺

**טענה**: יהיו $a,b \in \mathbb{Z}$. אזי $(a,b) = 1$ אמ"מ קיימים $x,y \in \mathbb{Z}$ כך ש-$ax + by = 1$.

**הוכחה**:

($\Leftarrow$) נובע ישירות מהטענה הקודמת.

($\Rightarrow$) נניח ש-$ax + by = 1$ ונניח ש-$(a,b) = k > 1$. אז $k \mid (ax + by)$, כלומר $k \mid 1$ אבל זה לא יכול להיות.

☺

**הגדרה**: יהי $n \in \mathbb{N}$. נסמן $\mathbb{Z}_n^* = \{1 \le a < n : (a,n) = 1\}$ ונגדיר את <u>פונקצית אוילר</u> $\varphi : \mathbb{N} \to \mathbb{N}$ להיות $\varphi(n) = \left|\mathbb{Z}_n^*\right|$.

**טענה**: יהיו $m,n \in \mathbb{N}$ כך ש-$(m,n) = 1$. אזי $\varphi(mn) = \varphi(m)\varphi(n)$.

**טענה**: יהי $p$ ראשוני. אזי לכל $k \in \mathbb{N}$ $\varphi(p^k) = (p-1)p^{k-1}$.

**טענה**: לכל $n\in\mathbb{N}$ $\varphi(n)=n\prod_{p|n}\left(1-\frac{1}{p}\right)$.

**טענה**: לכל $n\in\mathbb{N}$ $\mathbb{Z}_n^*$ חבורה ביחס לכפל.

**הוכחה**: יש להראות שמתקיימות תכונות החבורה. ברור שיש אסוציאטיביות וברור ש- $1\in\mathbb{Z}_n^*$ הוא איבר יחידה. לכן נותר להראות סגירות לכפל ולהופכי.

יהיו $a,b\in\mathbb{Z}_n^*$ ונראה ש- $ab\in\mathbb{Z}_n^*$. יש להראות ש- $(ab,n)=1$. נניח בשלילה ב- $(ab,n)=k>1$. נתון ש- $(a,n)=1$ ולכן $k\nmid a$. אבל $k|ab$ ולכן $k|b$. אבל מכן ש- $(ab,n)=k>1$ נובע ש- $k|n$ וזו סתירה לכך ש- $(b,n)=1$. לכן $\mathbb{Z}_n^*$ סגורה לכפל. כעת, יהי $a\in\mathbb{Z}_n^*$. מאחר ש- $(a,n)=1$ נובע שקיימים $x,y\in\mathbb{Z}$ כך ש- $ax+ny=1$. לכן $ax\equiv1(\bmod n)$ ו- $b=x\bmod n$ הופכי ל- $a$. נראה ש- $b\in\mathbb{Z}_n^*$. מספיק להראות ש- $(x,n)=1$. אבל מהסתכלות ב- $xa+ny=ax+ny=1$ נובע ש- $(x,n)=1$.

☺

**טענה**: $a\in\mathbb{Z}_n^*$ אמ"מ קיים $b\in\mathbb{Z}_n^*$ כך ש- $ab\equiv1(\bmod n)$.

**הוכחה**:

($\Leftarrow$) ברור כי $\mathbb{Z}_n^*$ חבורה ובפרט יש ל- $a$ הופכי ב- $\mathbb{Z}_n^*$.

($\Rightarrow$) נניח ש- $ab\equiv1(\bmod n)$. אזי $ab=qn+1$, כלומר $ab-nq=1$. לכן $(a,n)=1$ ו- $a\in\mathbb{Z}_n^*$.

☺

**מסקנה**: יהיו $a,b\in\mathbb{Z}_n$ עבור $n$ כלשהו. אם $a,b$ הפיכים ביחד לכפל ב- $\mathbb{Z}_n$ אזי $ab$ הפיך ביחס לכפל ב- $\mathbb{Z}_n$.

**הוכחה**: אם $a,b$ הפיכים אז לפי הטענה הקודמת הם שייכים ל- $\mathbb{Z}_n^*$ ושם המכפלה שלהם כמובן הפיכה. בפרט המכפלה הפיכה ביחס לכפל ב- $\mathbb{Z}_n$.

☺

**טענה**: יהיו $a,n\in\mathbb{Z}$ כך ש- $(a,n)=1$. אזי $(a\bmod n,n)=1$.

**הוכחה**: נניח ש- $a\bmod n=a+kn$ עבור $k\in\mathbb{Z}$ כלשהו. נראה ש- $(a+kn,n)=1$. אחרת קיים $m>1$ כך ש- $m|n$ וגם $m|(a+kn)$. לכן $m|a$ אבל זו סתירה לכך ש- $(a,n)=1$.

☺

**למה**: יהיו $a,b\in\mathbb{Z}$ כך ש- $a\equiv b(\bmod n)$ עבור $n$ כלשהו. אזי לכל $m\in\mathbb{Z}$ מתקיים $a^m\equiv b^m(\bmod n)$.

**הוכחה**: מתקיים $n|(a-b)$ וצריך להראות ש- $n|(a^m-b^m)$ לכל $m\in\mathbb{Z}$. אם $m=0$ זה ברור. כעת, אם $m>0$ אז $a^m-b^m=(a-b)(a^{m-1}+a^{m-2}b+...+a^2b^{m-3}+ab^{m-2}+b^{m-1})$ שהרי

$$(a-b)\left(a^{m-1}+a^{m-2}b+...+a^2b^{m-3}+ab^{m-2}+b^{m-1}\right)=$$
$$=a\left(a^{m-1}+a^{m-2}b+...+a^2b^{m-3}+ab^{m-2}+b^{m-1}\right)-b\left(a^{m-1}+a^{m-2}b+...+a^2b^{m-3}+ab^{m-2}+b^{m-1}\right)=$$
$$=\left(a^m+\cancel{a^{m-1}b}+...+\cancel{a^2b^{m-2}}+\cancel{ab^{m-1}}\right)-\left(\cancel{ba^{m-1}}+\cancel{a^{m-2}b^2}+...+\cancel{a^2b^{m-2}}+\cancel{ab^{m-1}}+b^m\right)=a^m-b^m$$

לכן $(a-b)\mid\left(a^m-b^m\right)$ ולכן $n\mid\left(a^m-b^m\right)$ וסיימנו.

☺

**משפט פרמה הקטן**: יהי $p$ ראשוני ויהי $a\in\mathbb{Z}$. אזי $a^p\equiv a\pmod p$.

**הוכחה**: אם $p\mid a$ אז $a=np$ ולכן $a^p=(np)^p=n^pp^p$ ו- $p\mid a^p$. לכן $p\mid\left(a^p-a\right)$ כלומר $a^p\equiv a\pmod p$.

אם $(a,p)=1$ נטען שקיים $b\in\mathbb{Z}_p^*$ כך ש- $a\equiv b\pmod p$. אבל זה ברור כי אם $a=qp+r$ עבור $1\le r\le p-1$ אז $b=r\in\mathbb{Z}_p^*$. אז מתקיים $a^{p-1}\equiv b^{p-1}\pmod p$. אבל $\left|\mathbb{Z}_p^*\right|=p-1$ ולכן לכל $b\in\mathbb{Z}_p^*$ מתקיים $b^{p-1}=1$. לכן $a^{p-1}\equiv1\pmod p$. נכפול את שני האגפים ב- $a$ ונקבל את הדרוש.

☺

**משפט אוילר**: יהיו $a,n\in\mathbb{Z}$ כך ש- $(a,n)=1$. אזי $a^{\varphi(n)}\equiv1\pmod n$.

**הוכחה**: יהי $b=a\bmod n$. לפי הלמה מספיק להראות ש- $b^{\varphi(n)}\equiv1\pmod n$. ואכן, אם $(a,n)=1$ אז גם $(b,n)=1$. לכן $b\in\mathbb{Z}_n^*$. ולכן $b^{\varphi(n)}=b^{\left|\mathbb{Z}_n^*\right|}\equiv1\pmod n$.

☺

**טענה**: נסתכל על $\mathbb{Z}_n$. אז לכל $1\le a<n$ $(a,n)=1$ אמ"מ $\mathbb{Z}_n=\langle a\rangle$.

**הוכחה**:

($\Leftarrow$) נניח ש- $(a,n)=1$. ברור ש- $\langle a\rangle\subset\mathbb{Z}_n$. כמו כן, ברור שבקבוצה $\langle a\rangle=\{0,a,2a,...,(n-1)a\}$ יש לכל היותר $n$ איברים. נראה שיש $n$ איברים ונסיים. נניח ש- $ia=ja$ עבור $0\le i<j\le n-1$. אז $(j-i)a=0$. אז יש שלוש אפשרויות:

1. $j-i=0$ אבל זה לא יכול להיות כי $i<j$.
2. $a=0$ אבל זה לא יכול להיות כי $1\le a$.
3. $(j-i)a=nk$ עבור $k$ כלשהו. אז $k=1$ שהרי $1\le a<n$ ו- $1\le j-i<n-1$. אז $(j-i)a=n$ וזה לא יכול להיות כי אז $a\mid n$. אם $a=1$ נובע ש- $i=j$ וזו סתירה ולכן $a>1$ אבל זו סתירה כי אז $(a,n)=a>1$.

בכל מקרה מתקבלת סתירה. לכן $\left|\langle a\rangle\right|=n$ ו- $\mathbb{Z}_n=\langle a\rangle$.

($\Rightarrow$) נניח ש- $\mathbb{Z}_n=\langle a\rangle$. אם $(a,n)=k>1$ נסתכל על $\langle a\rangle=\{0,a,2a,...,(n-1)a\}$. נטען ש- $\frac{n}{k}a\equiv0\pmod n$.

אבל $k\mid a$ ולכן $\frac{a}{k}\in\mathbb{Z}$. ומכאן ש- $\frac{n}{k}a\equiv0\pmod n$. לכן $\left|\langle a\rangle\right|<n$ בסתירה לכך ש- $\mathbb{Z}_n=\langle a\rangle$ וסיימנו.

☺