

# מבנים אלגבריים 1

14 בדצמבר 2010

המרצה:

המתרגל:

איני לוקחת אחריות על מה שכתוב מטה.  
אין המרצה או המתרגלים קשורים לסיכום זה בשום דרך.

הערות יתקבלו בברכה - [noga.rotman@gmail.com](mailto:noga.rotman@gmail.com)

## תוכן עניינים

|    |                                                    |     |
|----|----------------------------------------------------|-----|
| 3  | חבורות                                             | 1   |
| 3  | הגדרות בסיסיות                                     | 1.1 |
| 4  | תכונות של חבורות                                   | 1.2 |
| 6  | חבורות סופיות                                      | 1.3 |
| 8  | 1.3.1 החבורה הנוצרת\נפרשת                          |     |
| 10 | 1.4 מחלקות שמאליות של $H$ בחבורה $G$               |     |
| 13 | 1.5 חבורת תמורות                                   |     |
| 14 | 1.5.1 חבורת התמורות על $n$ עצמים $S_n$             |     |
| 17 | 1.5.2 גרף קיילי                                    |     |
| 18 | 1.6 אוטומורפיזם של חבורות                          |     |
| 20 | 1.7 חבורות נורמליות, חבורות מנה ומשפטי הומומורפיזם |     |
| 20 | 1.7.1 חבורות חלקיות נורמליות                       |     |
| 22 | 1.7.2 חבורות מנה                                   |     |
| 23 | 1.7.3 משפט ההומומורפיזם הראשון                     |     |
| 25 | 1.7.4 משפט ההומומורפיזם השני                       |     |
| 26 | 1.7.5 משפט ההתאמה                                  |     |
| 27 | 1.7.6 משפט ההומומורפיזם השלישי                     |     |
| 28 | 1.8 סדרות נורמליות, סדרות הרכב                     |     |
| 28 | 1.8.1 למת צצנהאוס                                  |     |
| 28 | 1.8.2 סדרות נורמליות                               |     |
| 30 | 1.8.3 סדרות הרכב                                   |     |
| 30 | 1.8.4 משפט ג'ורדן הולדר                            |     |
| 30 | 1.9 חבורות פתירות                                  |     |
| 31 | 1.10 פעולה של חבורה $G$ על קבוצה $X$               |     |
| 34 | 1.11 משפט סילוא - $Sylow$                          |     |

## 1 חבורות

### 1.1 הגדרות בסיסיות

11/10/2010

**הגדרה 1.1** חבורה זו שלישיה  $(G, \cdot, e)$  כאשר  $G$  היא קבוצה,  $\cdot$  היא פעולה דו משתנית על  $G$ ,  $^1: G \times G \rightarrow G$ ,  
וכמו כן קיים  $e \in G$ , כך שהתנאים הבאים מתקיימים:

1. אסוציאטיביות - קיבוציות:

$$\forall a, b, c \in G \quad a \cdot (b \cdot c) = (a \cdot b) \cdot c$$

2.  $e$  איבר היחידה:

$$\forall a \in G \quad a \cdot e = e \cdot a = a$$

3. קיום איבר הפכי:

$$\forall a \in G \quad \exists b \in G \quad a \cdot b = b \cdot a = e$$

**הערה 1.2** למעשה יש גם תנאי 0 - קשירות, אך למעשה אין בו צורך, כי מההגדרה שלנו  $a \cdot b$  מוגדר באופן יחיד.

**הגדרה 1.3** חבורה נקראת אבליה<sup>2</sup> אם מתקיים:

$$\forall a, b \in G \quad a \cdot b = b \cdot a$$

**הערה 1.4** נשים  $\heartsuit$  שבאמת לא כל החבורות שנפגוש הינן חבורות אבליות, כלומר אנחנו בפירוש לא מצפים לקמוטטיביות מחבורות.

### דוגמאות

1.  $(\mathbb{Z}, +, 0)$  היא חבורה.

2. יהי  $\mathbb{F}$  שדה כלשהוא, אזי  $(\mathbb{F}, +, 0)$  היא תמיד חבורה.

3. נסמן  $\mathbb{F}^x = \mathbb{F} \setminus \{0\}$ . אזי  $(\mathbb{F}^x, \cdot, 1)$  היא גם חבורה.

4. יהי  $\mathbb{F}$  שדה,  $V$  מ"ו מעל  $\mathbb{F}$ , אזי  $(V, +, \vec{0})$  חבורה.

---

<sup>1</sup>כלומר לכל  $a, b \in G$  מוגדר  $a \cdot b$   
<sup>2</sup>שמות נוספים - אבליה, חילופית.

5. תהי  $X$  קבוצה (סופית או אינסופית). נביט ב-

$$G = \text{Perm}(X) = \{f : X \rightarrow X \mid f \text{ injective and surjective}\}$$

עם פעולת ההרכבה  $(f \circ g)(x) = f(g(x))$  לכל  $x \in X$ .  
 איבר היחידה יהיה פונקציית הזהות  $Id$ .  
 קל לראות כי  $(G, \circ, Id)$  היא חבורה (האיבר ההפכי קיים מהיות כל  $f \in X$  פונקציה חח"ע ועל).  
 זוהי חבורה שאינה קמוטטיבית. לדוגמא:

$$\begin{aligned} X = \mathbb{R}, f : \mathbb{R} \rightarrow \mathbb{R}, f(x) = 3x, g : \mathbb{R} \rightarrow \mathbb{R}, g(x) = x + 5 \\ (f \circ g)(x) = f(g(x)) = f(x + 5) = 3 \cdot (x + 5) = 3x + 15x \\ (g \circ f)(x) = g(f(x)) = g(3x) = 3x + 5 \end{aligned}$$

כלומר אין שיוויון, ועל כן החבורה אינה קמוטטיבית.  
 נראה חבורה לא קמוטטיבית נוספת:

6. יהי  $\mathbb{F}$  שדה, ונגדיר  $GL_n(\mathbb{F}) = \{M_n \mid \det(a) \neq 0\}$ . אזי  $(GL_n(\mathbb{F}), \cdot, I_n)$  היא חבורה (כאשר  $I_n$  היא מטריצת היחידה בגודל  $n \times n$ ).  
 לקורא השקדן מושאר למצוא דוגמא המראה מדוע חבורה זו אינה קמוטטיבית הכל מ- $n \geq 2$ .

## 1.2 תכונות של חבורות

**טענה 1.5** נרצה להראות:

1. איבר היחידה הוא יחיד,  
 כלומר אם  $e, e' \in G$  כך שלכל  $a \in G$  מתקיים  $a \cdot e = e \cdot a = a$  וגם  $a \cdot e' = e' \cdot a = a$ , אזי  $e = e'$ .

2. האיבר ההופכי הוא יחיד,  
 כלומר אם  $a \in G$  ו- $b, b' \in G$  כך ש- $a \cdot b = e = a \cdot b'$ , אזי  $b = b'$ .

במקום הוכחה ישירה, נוכיח טענה כללית יותר שימושית:

**טענה 1.6** לכל  $d, a \in G$  קיים  $x \in G$  יחיד כך ש:

$$a \cdot x = d$$

**הוכחה: קיום:**

מדובר בחבורה, ולכן ל- $a$  יש הפכי  $a'$  כך ש- $a' \cdot a = e$ . ניקח:

$$a' \cdot a = a \cdot a' = e, x = a' \cdot d$$

אזי:

$$a \cdot x = a \cdot (a' \cdot d) = (a \cdot a') \cdot d = e \cdot d = d$$

### יחידות:

נניח  $ay = d = ax$ , ונרצה להראות כי  $x = y$ . נכפול בהפכי משני הצדדים ונקבל:

$$ax = yx \Rightarrow a' \cdot (a \cdot x) = a' \cdot (a \cdot x) = (a' \cdot a) \cdot x = (a' \cdot a) \cdot y \Rightarrow ex = ey \Rightarrow x = y$$

■

כנדרש.

**הערה 1.7** הוכחה דומה מראה שלכל  $a, d \in G$  קיים  $y \in G$  יחיד כך ש:

$$ya = d$$

נוכיח עתה את הטענה 1.5: **הוכחה:** 1. לפי הטענה הקודמת, בפרט למשוואה  $ax = x$  יש פתרון יחיד, ולכן  $e' = e$ .

2. לפי הטענה הקודמת, בפרט למשוואה  $ax = e$  יש פתרון יחיד, ולכן  $b' = b$ . ■

**הערה 1.8** את ההפכי היחיד של  $a \in G$  נסמן ב- $a^{-1}$ .

**הגדרה 1.9** יהיו  $G, H$  חבורות.

$\varphi : G \rightarrow H$  תקרא הומומורפיזם אם לכל  $x, y \in G$ :

$$\varphi \left( \underbrace{a \cdot y}_{\in G} \right) = \varphi(x) \underbrace{\cdot}_{\in H} \varphi(y)$$

**הגדרה 1.10** הומומורפיזם  $\varphi$  יקרא מונומורפיזם אם הוא חח"ע.

**הגדרה 1.11** הומומורפיזם  $\varphi$  יקרא אפימורפיזם אם הוא על.

**הגדרה 1.12** איזומורפיזם הוא הומומורפיזם שהוא גם מונ' וגם אפ'. נסמנו ב- $\simeq$ .

**דוגמא:**

$$\varphi : x \rightarrow 2^x, (\mathbb{R}, +, -) \simeq (\mathbb{R}_{>0}, \cdot, 1)$$

### 1.3 חבורות סופיות

3

**מסדר 1** יש חבורה יחידה מסדר 1 עד כדי איזומורפיזם!

**מסדר 2** גם כאן יש חבורה יחידה עד כדי איזומורפיזם!

**מסדר 3** גם כאן אותו הדבר.

**מסדר 4** כאן יש שתי חבורות עד כדי איזומורפיזם!

13/10/2010

**תרגיל:** הוכח:

1.

$$\varphi(e_G) = e_H$$

2.

$$\forall x \in G \quad \varphi(x^{-1}) = \varphi(x)^{-1}$$

**הוכחה:** נביא הוכחה לטענה הראשונה, השניה מושארת כתרגיל.

$$\varphi(e_G) = \varphi(e_G - e_G) = \varphi(e_G) \cdot \varphi(e_G)$$

אם נסמן  $z = \varphi(e_G)$ , אזי נקבל:

$$z = z \cdot z$$

ולכן אם נכפיל את  $z^{-1}$  - ההפכי של  $z$  ב- $H$ , נקבל:

$$z = e_H$$

■

**הגדרה 1.13**  $G$  תהי חבורה.

$H \subset G$  תקרא **חבורה חלקית** ( $H$ ) או תת חבורה אם מתקיים:

$$1. e_G \in H$$

$$2. a, b \in H \Rightarrow a \cdot b \in H$$

$$3. a \in H \Rightarrow a^{-1} \in H$$

<sup>3</sup>הקטע הזה יסודר במועד מאוחר יותר - הצירים מצריכים עבודה נוספת..

במקרה  $H \leq G$  נסמן  $H \leq G$ .

נשים ♡ -

במקרה זה,  $H$  גם מהווה חבורה!

**טענה 1.14** תהי  $H \subseteq G$  תת קבוצה לא ריקה. אזי  $H$  חבורה חלקית אמ"מ לכל  $a, b \in H$  מתקיים  $a \cdot b^{-1} \in H$ .

**הוכחה:**  $\Leftarrow$  אם  $H$  חבורה חלקית אזי  $H$  לא ריקה כי  $e \in H$ , וברור שאם  $a, b \in H$  אזי גם  $b^{-1} \in H$  (מהתנאי השלישי), ולפי התנאי השני המכפלה שלהם  $a \cdot b^{-1} \in H$ .  
 $\Rightarrow$  אם  $H$  לא ריקה וכל  $a, b \in H$  מתקיים  $a \cdot b^{-1} \in H$ , אזי:  
 1.  $e \in H$ , כי אם  $a \in H$  (קיים כי  $H$  אינה ריקה), אז  $a \in H$ , ולכן  $e = a \cdot a^{-1} \in H$ .  
 2. נניח  $a, b \in H$ . ראינו שאם  $a, b^{-1} \in H$ , ולכן  $a \cdot (b^{-1})^{-1} \in H$  (לפי התנאי).  
 3. ראינו מעלה כי  $e \in H$ , אזי  $e, a \in H$ , ולפי התנאי  $e \cdot a^{-1} \in H$ ,  $a^{-1} = e \cdot a^{-1} \in H$ .  
 ■

**תרגיל:** הוכח  $(b^{-1})^{-1} = b$ .

**דוגמאות:**

- בהנתן  $G$  חבורה כלשהיא,  $\{e\}$  תת חבורה.
- $G = (\mathbb{Z}, +, 0)$ ,  $H = m\mathbb{Z} = \{n \in \mathbb{Z} | m|n\}$ , כאשר  $m \in \mathbb{Z}$  קבוע, חבורה חלקית. מדוע? כל מספר מחלק את 0 ולכן  $0 \in H$ . חיבור של כל שני מספרים שמתחלקים ב- $m$  מתחלק ב- $m$ , וכו'.

**טענה 1.15** אם  $H \leq \mathbb{Z}$ , אזי קיים  $m \in \mathbb{Z}$  כך ש- $H = m\mathbb{Z}$ .

**הוכחה:** נסתכל ב- $H \cap \mathbb{N}^+$ : אם ריק אזי  $H = \{0\}$ , כי במקרה כזה גם  $H \cap \mathbb{N}^+ = \{0\}$  כי אם  $H \ni a < 0$  אזי גם  $H \ni -a > 0$  (כי  $H$  ח"ח), ולכן גם  $H = 0 \cdot \mathbb{Z}$ , וסיימנו.  
 לכן, נניח כי  $H \cap \mathbb{N}^+ \neq \{0\}$ , ויהא  $m$  האיבר הקטן ביותר בקבוצה הזו. נטען ש:  $H = m\mathbb{Z}$ .

נוכיח הכלה דו כיוונית:  
 $H \supseteq m\mathbb{Z}$ : יהי  $z \in \mathbb{Z}$ , אזי  $m \cdot z \in H$ , כי אם  $z = 0$  אז  $m \cdot 0 = 0 \in H$ .  
 אחרת, אם  $z > 0$ ,  $m \cdot z = m + m + \dots + m$ , ומכיון ר"ח  $H$  אזי  $m \cdot z \in H$ .  
 אם  $z < 0$ , אזי  $m \cdot z = -m \cdot (-z) \in H$ , בגלל השורה הקודמת.  
 $H \subseteq m\mathbb{Z}$ : נניח כי  $n \in H$  חיובי, ונרצה להראות כי הוא מתחלק ב- $m$ .

<sup>4</sup>זוהי לא טעות הקלדה!! אנו משתמשים כאן בתנאי שלכל  $a, b \in H$  מתקיים  $a \cdot b^{-1} \in H$  ולכן בפרט עבור  $a, b = a$ .

נחלק אותו ב- $m$  ונקבל:

$$n = q \cdot m + r$$

כאשר  $0 \leq r < m$ . נרצה להראות כי הוא אפס.  
נשים  $\heartsuit$  כי  $n, q \cdot m \in H$  ולכן גם  $r = n - q \cdot m \in H$ .  
אבל  $m$  הוא המינימלי ב- $H$ , ולכן בהכרח  $r = 0$ .  
נניח כי  $n \in H$  שליש. אזי  $-n \in H$  יהיה חיובית,  
ולכן לפי השורה הקודמת  $m$  מחלק את  $-n$  ולכן גם את  $n$ .

■

**ואפילו עוד דוגמאות!**

18/10/2010

- $G = GL_n(\mathbb{F})$ , שדה  $\mathbb{F}$ . אזי  $H = SL_n(\mathbb{F}) = \{A \in M_n(\mathbb{F}) \mid \det(A) = 1\}$  ח"ח.
- $G = S_n = \text{sign}(n)$ , אזי  $A_n$  - אוסף התמורות הזוגיות ח"ח.
- $G = V$  מ"ו מעל שדה  $\mathbb{F}$ , אזי כל תת מרחב  $W$  הוא ח"ח.  
נשים  $\heartsuit$  שלא להיפך! לדוגמא,  $V = \mathbb{R}^n$  אזי  $\mathbb{Q}^n$  ח"ח ולא תת מרחב, וכך גם  $\mathbb{Z}^n$ .

### 1.3.1 החבורה הנוצרת \ נפרשת

**למה 1.16** אם  $\{H_i\}_{i \in I}$  אוסף לא ריק של ח"ח של חבורה  $G$ , אזי  $K = \bigcap_{i \in I} H_i$  ח"ח.

**הוכחה:**  $e \in H_i$  לכל  $i$ , ולכן  $e \in K$ .  
כמו כן, לכל  $a, b \in H_i$  לכל  $i$  -  $a \cdot b \in K$ ,  $a^{-1} \in K$ .

■

**הגדרה 1.17** תהא  $X \subseteq G$  תת קבוצה. נסמן  $\langle X \rangle = H$  את חיתוך כל החבורות החלקיות של  $G$  המכילות את  $X$ .  
זהו אוסף לא ריק כי  $X$  שם, ולפי הלמה זו ח"ח, שתקרא החבורה החלקית הנוצרת ע"י  $X$ .

**הערה 1.18**  $\langle X \rangle$  זו הח"ח הקטנה ביותר המכילה את  $X$ , כלומר אם  $L$  ח"ח של  $G$  המכילה את  $X$ , אזי  $L$  מכילה את  $\langle X \rangle$ , כי  $L$  היא חלק מאוסף הח"ח המכילות את  $\langle X \rangle$ , ולכן מופיעה בחיתוך שבהגדרה.

**הערה 1.19** אם  $X = \{\phi\}$ , אז  $\langle X \rangle = e$ .

**טענה 1.20** תהא  $G$  חבורה,  $X \subseteq G$  תת קבוצה, אזי:

$$\langle X \rangle = \{x_1^{\varepsilon_1} \cdot x_2^{\varepsilon_2} \cdot \dots \cdot x_n^{\varepsilon_n} \mid i \in \mathbb{N} \cup \{0\}, \varepsilon_i \in \{\pm 1\}, x_i \in X\}$$

כאשר  $e$  מתקבל עבור  $n = 0$ .

**הוכחה:** נוכיח הכלה דו כיוונית:

$\supseteq$ : כל "מילה" מהצורה  $x_1^{\varepsilon_1} \cdot x_2^{\varepsilon_2} \cdot \dots \cdot x_n^{\varepsilon_n}$  נמצאת בכל ח"ח המכילה את  $X$ , ולכן נמצאת בחיתוך, ולכן נמצאת ב- $\langle X \rangle$ .

$\subseteq$ : נוכיח שאוסף כל המילים הנ"ל מהווה ח"ח, ואכן האוסף מכיל את  $\{e\}$  עבור  $n = 0$ .  
אם  $x_1^{\varepsilon_1} \cdot x_2^{\varepsilon_2} \cdot \dots \cdot x_n^{\varepsilon_n}$  באוסף, אז גם  $x_1^{-\varepsilon_1} \cdot x_2^{-\varepsilon_2} \cdot \dots \cdot x_n^{-\varepsilon_n} = (x_1^{\varepsilon_1} \cdot x_2^{\varepsilon_2} \cdot \dots \cdot x_n^{\varepsilon_n})^{-1}$  גם באוסף.

כמו כן, בהנתן  $y_1^{\delta_1} \cdot y_2^{\delta_2} \cdot \dots \cdot y_n^{\delta_n}$  באוסף, אזי גם  $x_1^{\varepsilon_1} \cdot x_2^{\varepsilon_2} \cdot \dots \cdot x_n^{\varepsilon_n} \cdot y_1^{\delta_1} \cdot y_2^{\delta_2} \cdot \dots \cdot y_n^{\delta_n}$  באוסף, וסיימנו. ■

**הגדרה 1.21** חבורה  $G$  נקראת ציקלית\מחזורית אם קיים  $g \in G$  כך ש- $G = \langle g \rangle$ .

**הערה 1.22** אם  $G = \langle g \rangle$ , אזי  $G = \{g^n | n \in \mathbb{Z}\}$ .

**דוגמאות לחבורות ציקליות:**

1.  $G = \mathbb{Z}, +$ , אזי  $G = \langle -1 \rangle$ ,  $G = \langle 1 \rangle$ .

2.  $G = m\mathbb{Z}$ ,  $G = \langle m \rangle$ .

3.  $\mathbb{Z} = \{0, 1, \dots, n-1\}$  בחיבורה מודולו  $n$ , אזי  $\mathbb{Z}_n = \langle 1 \rangle$ .

**הערה 1.23** תרגיל למתקדמים -  $\mathbb{Z}_n = \langle a \rangle$  כאשר  $a \in \mathbb{Z}_n$  אם  $(a, n) = 1$ .

4.  $G = \{1, -1, i, -i\}$ , אזי  $G = \langle -i \rangle$ ,  $G = \langle i \rangle$ . נשים  $\heartsuit$  שאין הבדל בין חבורה זו לבין חבורה עם 4 איברים.

**משפט 1.24** אם  $G$  חבורה ציקלית, אזי או ש- $G$  איזומורפית ל- $\mathbb{Z}$ , או ש- $G$  איזומורפית ל- $\mathbb{Z}_n$  לאיזשהו  $n \in \mathbb{N}$ .

נשים  $\heartsuit$  שכמסקנה מכך, אם נתונה חבורה אינסופית ציקלית, היא בהכרח איזומורפית ל- $\mathbb{Z}$ . אם היא מסדר סופי  $n$ , אזי היא איזומורפית ל- $\mathbb{Z}_n$ .

**הגדרה 1.25** תהי  $g \in G$ . נסמן את  $O(g) = \min \{n \in \mathbb{N} | g^n = e\}$  להיות הסדר של  $g$ , ונאמר ש- $O(g) = \infty$  מסדר אינסופי אם אין  $n$  כזה.

כעת, נוכיח את המשפט מעלה: **הוכחה:** תהא  $G$  חבורה ציקלית הנוצרת ע"י  $g$ , כלומר  $G = \langle g \rangle$ .

נוכיח שאם  $O(g) = \infty$ , אזי  $G \simeq \mathbb{Z}$ ,

ואם  $O(g) = n \in \mathbb{N}$ , אזי  $G \simeq \mathbb{Z}_n$ .

נראה כי קיים הומומורפיזם חח"ע ועל  $\varphi$  מה"ע לע"מ להוכיח את הטענה.

**מקרה 1:**  $O(g) = \infty$ .

נגדיר  $\varphi : \mathbb{Z} \rightarrow G$ ,  $\varphi(n) = g^n$ ,  $n \in \mathbb{Z}$ . צ"ל ש- $\varphi$  איזומורפיזם, כלומר הומומורפיזם, חח"ע ועל.

זהו הומומורפיזם, כי:

$$\varphi(n+m) = g^{n+m} = g^n \cdot g^m = \varphi(n) \cdot \varphi(m)$$

כמו כן, נניח ש- $\varphi(n) = \varphi(m)$  עבור  $n, m \in \mathbb{Z}$  שונים. בה"כ  $m > n$  ואז  $m - n > 0$  כעת:

$$\varphi(m-n) = g^{m-n} = g^m \cdot g^{-n} = g^m \cdot (g^n)^{-1} = \varphi(m) \cdot \varphi(n)^{-1} = e$$

כלומר  $e = g^{m-n}$  ולכן הסדר של  $g$  הוא סופי - סתירה. לכן הפונקציה חח"ע. לסיום, איבר כללי ב- $G$  הוא חזקה (חיובית או שלילית) של  $g$ , כי  $G$  ציקלית. כלומר כל  $h \in G$  הוא מהצורה  $h = g^n$  לאיזשהו  $n \in \mathbb{N}$ , כלומר  $h = \varphi(n)$ , כלומר הפונקציה היא על, כנדרש.

נעבור לרגע לדיון כללי, לפני שנוכיח את המקרה השני:  
 תהי  $G$  חבורה,  $g \in G$ , ונניח ש- $O(g) = n < \infty$ .  
 נטען - במקרה זה  $H = \langle g \rangle$  - האיברים חוזרים על עצמם!  
 כלומר, ב- $H = \langle g \rangle$  יש לכל היותר  $n$  איברים:

$$e, g, g^2, \dots, g^{n-1}$$

עכשיו נוכיח שיש בדיוק  $n$  איברים, דהיינו שכל האיברים הרשימה האחרונה שונים זה מזה.

אם  $g^i = g^j$ , וכמו כן  $i \neq j$ , בה"כ  $0 \leq i < j \leq n-1$ , אזי:

$$g^{j-i} = g^j \cdot (g^i)^{-1} = e, \quad n > j - i > 0$$

בסתירה למינימליות של  $n$ . לכן, יש בדיוק  $n$  איברים, כפי שרצינו להוכיח.

**מקרה 2:**  $O(g) < \infty$ .

תהי  $G$  ציקלית כך ש- $G = \langle g \rangle$ , וכמו כן  $O(g) = n < \infty$ .  
 על פי הדיון הקודם,  $|G| = n$ .

נראה כי  $G$  איזומורפית ל- $\mathbb{Z}_n$ : נגדיר העתקה  $\varphi: \mathbb{Z}_n \rightarrow G$  כך ש  $\varphi(i) = g^i$  לכל  $0 \leq i \leq n$ . נראה כי העתקה זו היא הומומורפיזם חח"ע ועל, ונסיים:

1. ההעתקה היא על לפי הדיון - ראינו שאם  $G = \langle g \rangle$  ו- $O(g) = n$  אזי  $G = \{e, g, g^2, \dots, g^{n-1}\}$  כלומר בדיוק  $n$  איברים.

2. שתי הקבוצות הן כאמור בגודל  $n$ , וכמו כן ההעתקה היא על, לכן היא גם חח"ע.

3. ההעתקה היא הומומורפיזם כי:

$$\varphi(i \oplus j) = g^{i \oplus j} = g^{i+j} = g^i \cdot g^j = \varphi(i) \cdot \varphi(j)$$

■

#### 1.4 מחלקות שמאליות של ח"ח $H$ בחבורה $G$

**הגדרה 1.26** תהי  $G$  חבורה ו- $H$  ח"ח.

נגדיר יחס שקילות על  $G$  באופן הבא:

לכל  $a, b \in G$ ,  $a \equiv_H b$  אם  $a^{-1}b \in H$ .

**טענה 1.27** זהו יחס שקילות.

**הוכחה:** נוכיח את קיום שלושת התנאים:

1. רפלקסיביות: לכל  $a \in G$ ,  $a \equiv_H a$  שהרי  $a^{-1} \cdot a = e \in H$ .

2. סימטריה: נניח  $a \equiv_H b$ , כלומר  $a^{-1} \cdot b \in H$ . ח"ח ולכן גם:

$$b^{-1} \cdot a = b^{-1} \cdot (a^{-1})^{-1} = (a^{-1} \cdot b)^{-1} \in H$$

כלומר  $b \equiv_H a$  כנדרש.

3. טרנזיטיביות: נניח כי  $a \equiv_H b$ ,  $b \equiv_H c$ . כלומר  $a^{-1} \cdot b \in H$ ,  $b^{-1} \cdot c \in H$ . לכן גם מכפלתם ב- $H$ . נקבל:

$$a^{-1} \cdot c = a^{-1} \cdot b \cdot b^{-1} \cdot c \in H$$

ולכן  $a \equiv_H c$  כנדרש.

■

**הגדרה 1.28** <sup>5</sup> יחס שקילות מחלק את הקבוצה, שמעליה הוא מוגדר, למחלקות שקילות: בהינתן קבוצה  $A$  ויחס שקילות  $R$  שהוגדר עליה, מגדירים את מחלקת השקילות של איבר כלשהו כקבוצת כל האיברים השקולים לו. נסמן את מחלקת השקילות של  $a \in H$  ב- $[a]$ .

**תרגיל** הוכיחו כי  $\{ah | h \in H\} = aH = [a]$ .

**דוגמא**

20\10\2010

$$1. G = \mathbb{Z}, H = 2\mathbb{Z}$$

באופן כללי  $e \in G$ , וכמו כן  $e = b$  אמ"מ  $b = e^{-1}b \in H$ .

במקרה שלנו:  $[0] = 2\mathbb{Z}$ . מהו  $[1]$ ?

$b \equiv_{H=2\mathbb{Z}} 1 \Leftrightarrow b - 1 = -1 + b \in 2\mathbb{Z}$ , כלומר אמ"מ  $b - 1$  זוגי, כלומר אמ"מ  $b$  אי זוגי.

לכן  $[0] = 2\mathbb{Z}$  = הזוגיים,  $[1] =$  האי זוגיים.

$$2. G = \mathbb{Z}, H = 5\mathbb{Z}$$

$$[0] = 5\mathbb{Z}, [1] = 1 + 5\mathbb{Z} = \{a \in \mathbb{Z} | a \equiv 1 \pmod{5}\}, [2] = 2 + 5\mathbb{Z} = 7 + 5\mathbb{Z}$$

$$[3] = 3 + 5\mathbb{Z}, [4] = 4 + 5\mathbb{Z}$$

$$3. G = \mathbb{R}^3, H = \{0\}$$

הוא מרחב חד מימדי כלשהו, כלומר יש דרך ראשית הצירים.

אזי מחלקות השקילות של  $H$  ב- $G$  הם הישרים המקבילים ל- $H$ .

**טענה 1.29** <sup>5</sup> תהי  $G$  חבורה, ח"ח  $H$ . יהי  $a \in G$ , ותהא  $[a]$  מחלקת השקילות של  $a$  ביחס ל- $H$ . אזי מתקיים:

$$[a] = a \cdot H = \{ah | h \in H\}$$

<sup>5</sup>מתוך ויקיפדיה

**הוכחה:** בכיוון הראשון, נניח כי  $a \equiv_H b$ , אזי  $a^{-1} \cdot b \in H$ , נסמנו ב- $h$ . כעת:

$$a \cdot h = a \cdot (a^{-1} \cdot b) = (a \cdot a^{-1}) \cdot b = eb = b$$

בכיוון השני, נניח כי  $b \in a \cdot h$ . נרצה להראות כי  $a \equiv_H b$ . אזי:

$$b = a \cdot h, h \in H \Rightarrow a^{-1} \cdot b = a^{-1} \cdot (a \cdot h) = (a^{-1} \cdot a) \cdot h = eh = h \in H$$

ולכן  $a \equiv_H b$ . ■

**הגדרה 1.30** קבוצה מהצורה  $aH$  כאשר  $a \in G, H \leq G$  נקראת מחלקה שמאלית של  $H$  ב- $G$ .

נשים  $\heartsuit$  ששתי מחלקות שקילות שמאליות ב- $H$  הן או שוות או זרות.<sup>6</sup>

**טענה 1.31** תהי  $G$  חבורה,  $a, b \in G, H \leq G$ , אזי יש התאמה חח"ע ועל בין המחלקה  $aH$  למחלקה  $bH$ , ובפרט יש להן אותו מספר איברים.

**הוכחה:** נגדיר  $f: aH \rightarrow bH$  כך ש:  $f(ah) = bh$ . נעיר קודם שאיבר  $ah \in aH$  כתיבתו כך היא יחידה, כלומר אם  $ah_1 = ah_2$  אזי  $h_1 = h_2$  ולכן  $f$  מוגדרת היטב.  $f$  חח"ע כי אם נניח ש- $f(ah_1) = f(ah_2)$ , כלומר  $bh_1 = bh_2$ , אז  $h_1 = h_2$  ולכן  $ah_1 = ah_2$ .  $f$  על כי אם  $bh \in bH$ , אזי  $bh = f(ah)$  ולכן  $f$  על. ■

#### משפט לגראנג'

**משפט 1.32** אם  $G$  חבורה סופית ו- $H \leq G$  ח"ח, אזי  $|H| \mid |G|$ .

**הוכחה:**  $G$  מחלקת למחלקות שקילות זרות מהצורה  $ah$  עבור  $a \in G$ , וכולן בעלות אותו סדר מהטענה מעלה. לכן  $|H| = |G|$  כפול מספר המחלקות השמאליות של  $H$  ב- $G$ . ■

**הגדרה 1.33** תהי  $G$  חבורה כלשהי,  $H \leq G$ . אזי מספר (סופי או אינסופי) של המחלקות השמאליות של  $H$  ב- $G$  יקרא האינדקס של  $H$  ב- $G$ , ויסומן  $[G : H]$ .

**מסקנה 1.34** אם  $G$  חבורה סופית מסדר ראשוני  $p$ , אזי  $G \simeq \mathbb{Z}_p$ .

**הוכחה:** אם  $|G| = p > 1$ , ניקח  $a \in G, a \neq e$ , ונתבונן ב- $\langle a \rangle = H$ . ממשפט לגראנג',  $|H| \mid |G| = p$ , ולכן  $|H| = 1$  או  $p$  (שהרי  $p$  ראשוני). אבל לא ייתכן שהוא 1, כי קבוצה זו מכילה לפחות את  $a$  ואת  $e$ , ולכן  $|H| = |G|$ , כלומר  $H = G$ , כלומר  $G$  נוצרת ע"י  $a$  ועל כן היא ציקלית מסדר  $p$ . ראינו כי כל חבורה ציקלית מסדר  $p$  היא איזומורפית ל- $\mathbb{Z}_p$ , ולכן  $G \simeq \mathbb{Z}_p$ , כנדרש. ■

בצורה דומה למחלקה שמאלית, ניתן להגדיר מחלקה ימנית:

<sup>6</sup>כי הן מחלקות שקילות של יחס שקילות שהוגדר קודם. לקורא השקדן - הוכח ישירות!

### 1.35 הגדרה

$$Hg = \{hg | h \in H\}$$

נשים לב כי באופן כללי  $Hg \neq gH$ .

**1.36 הערה**  $[G : H]$  הוא גם מספר המחלקות הימניות של  $G$  ב- $H$ . עובדה זו תשאר ללא הוכחה.

**1.37 מסקנה** ממשפט לגראנג':

$$1. \text{ לכל } a \in G, |O(a)| \mid |G|.$$

$$2. \text{ בהנתן } G \text{ סופית, לכל } a \in G \text{ מתקיים } a^{|G|} = e.$$

**הוכחה:** נוכיח את 2 מ-1,  $|O(a)| \mid |G|$ , כלומר  $|G| = |O(a)| \cdot k$  עבור  $k \in \mathbb{N}$ . אז:

$$a^{|G|} = a^{O(a) \cdot k} = \left(a^{O(a)}\right)^k = e^k = e$$

■

### משפט פרמה הקטן

**1.38 משפט** אם  $p$  ראשוני,  $a \in \mathbb{Z}$ , אזי  $a^p \equiv a \pmod{p}$ .

**הוכחה:** אם  $a \equiv 0 \pmod{p}$ , אזי  $a^p = 0 \pmod{p}$ , וסיימנו.

נניח, אם כן, כי  $a \not\equiv 0 \pmod{p}$ , כלומר  $p$  לא מחלק את  $a$ , דהיינו  $(a, p) = 1$ . אזי  $a \pmod{p} \in \{1, 2, \dots, p-1\}$ . כלומר, אפשר לחשוב על חזקות  $a$  כמבוצעות בשדה  $\mathbb{Z}_p$ . נמצא בחבורה הכפלית של השדה  $\mathbb{Z}_p$  זוהי חבורה מסדר  $p-1$ , ולכן לפי המסקנה האחרונה,  $a^{p-1} \equiv 1 \pmod{p}$ . נכפיל את שני הצדדים ב- $a$  ונקבל  $a^p \equiv a \pmod{p}$ . ■

### 1.5 חבורת תמורות

**1.39 הגדרה** תהא  $X$  קבוצה כלשהי, לא ריקה. פונקציה  $f : X \rightarrow X$  נקראת תמורה אם  $f$  חח"ע ועל.

**1.40 הגדרה** אוסף כל התמורות על  $X$  מהווה חבורה שתסומן ב- $Perm(X)$  או  $Sym(X)$ , ונקראת חבורת התמורות של  $X$ , כאשר איבר היחידה היא תמורת הזהות, הפעולה היא הרכבה, וההפכי של תמורה כלשהי היא הפונקציה ההפכית.

## משפט Cayley

**משפט 1.41** כל חבורה  $G$  איזומורפית לח"ח של איזושהיא חבורת תמורות.

**הוכחה:** ניקח  $X = G$ , ולכל  $g \in G$  נתאים תמורה  $\varphi_g$  על  $X$  (כלומר על  $G$ ) באופן הבא:

$$x \in X = G, \varphi_g(x) = g \cdot x$$

**למה 1.42**  $\varphi_g$  הינה תמורה של  $X = G$ .

**הוכחה:** יש להוכיח כי  $\varphi_g$  חח"ע ועל.

היא חח"ע, כי אם  $\varphi_g(x_1) = \varphi_g(x_2)$ , אזי  $g \cdot x_1 = g \cdot x_2$ , כלומר  $x_1 = x_2$ .  
היא על, כי אם  $y \in X = G$ , אזי  $y = g \cdot (g^{-1} \cdot y) = \varphi_g(g^{-1} \cdot y)$ .

**למה 1.43** ההתאמה  $g \rightarrow \varphi_g$  היא איזומורפיזם מ- $G$  ל- $Perm(G)$ .

**הוכחה:** נסמן  $\psi(g) = \varphi_g$ , ונרצה להוכיח כי  $\psi$  הומומורפיזם, חח"ע ועל.  
תחילה נראה כי היא הומומורפיזם, כלומר, נרצה להראות שלכל  $x \in G$  מתקיים  
 $\psi(g_1 \cdot g_2)(x) = (\psi(g_1) \cdot \psi(g_2))(x)$  נחשב:

$$\forall x \in G \quad \varphi_{g_1 \cdot g_2}(x) \stackrel{?}{=} \varphi_{g_1}(\varphi_{g_2}(x)) \Leftrightarrow (g_1 \cdot g_2) \cdot x \stackrel{?}{=} g_1 \cdot (g_2 \cdot x)$$

אבל הצד הימני נכון בגלל אסוציאטיביות, ולכן  $\psi$  הומומורפיזם!  
כעת,  $\varphi(G)$  ח"ח של  $Perm(G)$ , שהרי תמורה של ח"ח היא ח"ח (כפי שהראינו בתרגיל 1).

נוכיח כעת כי  $\psi$  חח"ע - ואכן אם נניח כי  $\psi(g_1) = \psi(g_2)$  עבור  $g_1, g_2 \in G$ , נקבל:

$$(\psi(g_1))(e) = (\psi(g_2))(e) \Rightarrow \varphi_{g_1}(e) = \varphi_{g_2}(e) \Rightarrow g_1 \cdot e = g_2 \cdot e \Rightarrow g_1 = g_2$$

■ ברור כי  $\psi$  היא גם על, מהגדרתה.

■

■ על כן,  $\psi$  איזומורפיזם בין  $G$  ל- $\varphi(G)$ , שהיא ח"ח של  $Perm(G)$ , כנדרש!

**מסקנה 1.44** (מההוכחה) - אם  $G$  חבורה מסדר  $n$ , אז אפשר לשכן את  $G$  בחבורה:

$$Sym(n) = Perm\{1, 2, \dots, n\}$$

**1.5.1 חבורת התמורות על  $n$  עצמים -  $S_n$**

איבר של  $S_n = Sym(n) = Perm\{1, 2, \dots, n\}$  היא תמורה  $\pi : \{1, 2, \dots, n\} \rightarrow \{1, 2, \dots, n\}$ .  
סימון מקובל:

$$\pi = \begin{pmatrix} 1 & 2 & \dots & n \\ \pi(1) & \pi(2) & \dots & \pi(n) \end{pmatrix}$$

## דוגמא

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 3 & 1 & 4 \end{pmatrix}, \varphi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 1 & 4 & 3 & 2 \end{pmatrix}$$

$$\pi \cdot \varphi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 2 & 1 & 3 & 5 \end{pmatrix}, \varphi \cdot \pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 4 & 5 & 3 \end{pmatrix},$$

**הגדרה 1.45** תמורה  $G \in S_n$  נקראת ציקלוס (מחזור) באורך  $r$  אם קיימת תת קבוצה  $Y \subseteq \{1, 2, \dots, n\}$  באורך  $r$   $Y = \{i_1, i_2, \dots, i_r\}$  כך ש:

$$\sigma_{ij} = \begin{cases} i_{j+1} & j = 1, \dots, r-1 \\ i_1 & j = r \end{cases}, \forall x \notin Y \quad \sigma(x) = x$$

לקבוצה  $Y$  נקרא התומך של  $\sigma$ .

**דוגמאות**  $\varphi \cdot \pi$  מהדוגמא הקודמת הוא מחזור באורך 3 (כאשר 5 חוזר ל-3):

$$3 \rightarrow 4 \rightarrow 5$$

כמו כן  $\pi \cdot \varphi$  מהדוגמא הקודמת גם הוא מחזור באורך 3.  $\varphi$  אינה מחזור, כי היא מורכבת משני חלקים:

$$1 \rightarrow 5 \rightarrow 2, 3 \rightarrow 4$$

**טענה 1.46** אם  $\sigma$  היא מחזור מאורך  $r$ , אז  $O(\sigma) = r$ , כלומר היא מסדר  $r$ .

**טענה 1.47** כל תמורה היא מכפלה של מחזורים בעלי תומכים זרים המתחלפים זה עם זה.

## דוגמא

$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 1 & 3 & 4 & 2 \end{pmatrix}, \eta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 4 & 3 & 5 \end{pmatrix}$$

$$\varphi = \eta \cdot \tau = \tau \cdot \eta$$

**הערה 1.48** נשים  $\heartsuit$  כי יכולנו להכפיל משני הצדדים ולקבל את אותה התוצאה כי המחזורים זרים. כלומר, באופן כללי מחזורים עם תומכים זרים מתחלפים זה עם זה.

את הפירוק נסמן ב:

$$\varphi \cdot \pi = (3, 4, 5), (1, 2) (3, 4, 5)$$

**הערה 1.49** הפירוק שהראנו למחזורים זרים הוא יחיד עד כדי סדר.

**הגדרה 1.50** מחזור (ציקלוס) באורך 2 נקרא חילוף.

**טענה 1.51** כל תמורה היא מכפלה של חילופים.

**הוכחה:** לפי הדיון הקודם, מספיק להוכיח שכל מחזור מהצורה  $(a_1, a_2, \dots, a_r)$  הוא מכפלה של חילופים.

אבל הראנו שמחזור באורך  $r$  הוא מכפלה של  $r - 1$  חילופים, ולכן סיימנו. ■

**תרגיל:** אי אפשר לכתוב כמכפלה של פחות מ- $(r - 1)$  חילופים.

**מסקנה 1.52** כל תמורה ב- $S_n$  ניתנת לכתיבה כמכפלה של  $n > n$  חילופים.

**הוכחה:** אם  $\sigma \in S_n$ , אזי היא ניתנת לכתיבה כמכפלה של מחזורי זרים באורכים  $k_1, k_2, \dots, k_l$ , כאשר  $k_1 + k_2 + \dots + k_l \leq n$ .

כל מחזור כזה ניתן לכתיבה כמכפלה של  $k_i - 1$  חילופים, ולכן בסה"כ  $\sigma$  היא מכפלה של  $(k_1 - 1) \cdot (k_2 - 1) \cdot \dots \cdot (k_l - 1) < n$  חילופים. ■

**מסקנה 1.53**

$$S_n = \langle \{(i, j) \mid 1 \leq i < j \leq n\} \rangle$$

**טענה 1.54**

$$S_n = \langle \{(i, i + 1) \mid 1 \leq i \leq n - 1\} \rangle$$

**הוכחה:** מספיק להוכיח שכל אחד מהחילופים  $(i, j)$  ניתן לכתיבה כמכפלה של "חילופים סמוכים". נניח  $i < j$ . אז:

$$(i, j) = (j - 1, j) (j - 2, j - 1) \dots (i + 3, i + 2) (i + 1, i + 2) \dots (j - 3, j - 2) (j - 2, j - 1) (j - 1, j)$$

$$i < k < j \Rightarrow j \rightarrow i, k \rightarrow k + 1 \rightarrow k, i \rightarrow j$$

$$k > j \text{ or } k < i \Rightarrow k \rightarrow k$$

■

**מסקנה 1.55** כל תמורה ניתנת לכתיבה כמכפלה של  $2n^2 \geq 2n^2$  חילופים מהצורה  $(i, i + 1)$ .

**הוכחה:** ראינו שכל תמורה ניתנת לכתיבה כמכפלה של  $n \geq n$  חילופים, וכל חילוף הוא מכפלה של  $2n \geq 2n$  חילופים סמוכים. ■

**טענה 1.56**

$$S_n = \langle \tau = (1, 2), \sigma = (1, 2, \dots, n) \rangle$$

**הוכחה:** מספיק להוכיח שכל חילוף מהצורה  $(i, i+1)$  ניתן לכתיבה כ- $\tau$  ו- $\sigma$ .

$$(i, i+1) = \sigma^{i-1} \tau \sigma^{-(i-1)} :$$

$$k \neq i, i+1 \quad k \rightarrow k - (i-1) \pmod{n} \rightarrow k - (i-1) + (i-1) \pmod{n} = k$$

$$k - (i-1) = 1 \Rightarrow k = i$$

$$k - (i-1) = 2 \Rightarrow k = i+1$$

$$k = i+1 \quad k \rightarrow 2 \rightarrow 1 \rightarrow 1+i-i = 1$$

$$k = i \quad k \rightarrow 1 \rightarrow 2 \rightarrow 2+i-1 = 1+i$$

■

**מסקנה 1.57** כל תמורה היא "מילה" ב- $\tau$  וב- $\sigma$  באורך  $4n^3 \geq$ .

**הוכחה:** כל תמורה היא מכפלה של  $2n^2 \geq$  חילופים מהצורה  $(i, i+1)$ , וכל  $(i, i+1)$  הוא "מילה" באורך  $2n \geq$  ב- $\tau$  וב- $\sigma$  (על פי הוכחת הטענה הקודמת). ■

## 1.5.2 גרף קיילי

1/11/2010

**הגדרה 1.58** יהא  $f(x_1, \dots, x_n) = \prod_{n \geq i > j \geq 1} (x_i - x_j)$  בהנתן תמורה  $\sigma \in S_n$ , הסימן שלה יהיה:

$$(\sigma.f) = \prod_{n \geq i > j \geq 1} (x_{\sigma(i)} - x_{\sigma(j)})$$

## עובדה

• לכל  $f, \sigma \in S_n$ ,  $\sigma.f = \pm f$ .

**הגדרה 1.59** נאמר ש- $\sigma \in S_n$  היא תמורה זוגית אם  $\sigma.f = f \Rightarrow \text{sign}(\sigma) = 1$ .  
נאמר ש- $\sigma \in S_n$  היא תמורה אי-זוגית אם  $\sigma.f = -f \Rightarrow \text{sign}(\sigma) = -1$ .

## עובדות נוספות

• הסימן הוא פונקציה כפלית, כלומר לכל  $\sigma_1, \sigma_2 \in S_n$ :

$$\text{sign}(\sigma_1 \cdot \sigma_2) = \text{sign}(\sigma_1) \cdot \text{sign}(\sigma_2)$$

•  $\sigma$  זוגית  $\Leftrightarrow \sigma$  היא מכפלה של מספר זוגי של חילופים  $\Leftrightarrow$  בכל כתיבה של  $\sigma$  כמכפלה של חילופים יש מספר זוגי של חילופים.

• מהתרגיל - סימן כל חילוף הוא -1.

• אם  $\sigma = (a_1, a_2, \dots, a_l)$  מחזור באורך  $l$ , אזי  $\text{sign}(\sigma) = (-1)^{l+1}$ .

## 1.6 אוטומורפיזם של חבורות

3/11/2010

**הגדרה 1.60** תהי  $G$  חבורה. אזי  $\alpha : G \rightarrow G$  הומומורפיזם חח"ע ועל (כלומר איזומורפיזם) יקרא אוטומורפיזם. נסמן ב- $Aut(G)$  את אוסף כל האוטומורפיזמים של  $G$ .

**טענה 1.61**  $Aut(G)$  היא חבורה בעצמה ביחס לפעולת ההרכבה.

1. יהיו  $\alpha, \beta \in Aut(G)$ , ונסמן  $(\alpha \circ \beta)(g) = \alpha(\beta(g))$ . נוכיח את הנדרש - קל לראות כי  $(\alpha \circ \beta)(g)$  חח"ע ועל, וזאת ישירות מהגדרתו. לכן נותר להוכיח כי זהו הומומורפיזם:

$$(\alpha \circ \beta)(g_1 \cdot g_2) = \alpha(\beta(g_1 \cdot g_2)) \stackrel{\beta \text{ homomorphism}}{=} \alpha(\beta(g_1) \cdot \beta(g_2)) \stackrel{\alpha \text{ homomorphism}}{=} \alpha(\beta(g_1)) \cdot \alpha(\beta(g_2))$$

כנדרש.

2. איבר היחידה יהיה העתקת הזהות.

3. נגדיר את האיבר ההופכי לכל  $\alpha \in Aut(G)$  להיות  $\alpha^{-1}$  -  $\alpha$  היא אוטומורפיזם ולכן קיימת לה פונקציה הפכית. נשאר לקורא השקדן להוכיח כי פונקציה היא גם הומומורפיזם.

4. אסוציאטיביות - נשאר גם לקורא השקדן.

### דוגמאות

1.  $\{-1, 1\} \simeq Aut(\mathbb{Z})$  - אם נוצרת ע"י 1, אזי נקבעת על ידי מה ההעתקה עושה ל-1. לדוגמא, תהי  $\alpha$  כך ש- $\alpha(1) = 3$ . אזי נוכל מכאן לדעת מה  $\alpha$  עושה לכל איבר, לדוגמא:

$$\alpha(2) = \alpha(1 + 1) = \alpha(1) + \alpha(1) = 3 + 3 = 6$$

2. תהי  $G = \mathbb{Z}_p^2$ . בכל מ"ו, כל ה"ל היא הומומורפיזם. נטען כי אלו בדיוק ההומומורפיזמים, כלומר שאין עוד. דהיינו  $Aut(G) = GL_2(\mathbb{Z}_p)$ . הוכח: כל אוטומורפיזם של  $G$  הוא ט"ל הפיכה.

**הגדרה 1.62** נגדיר את המרכז של חבורה  $G$  להיות:

$$Z(G) = \{x \in G \mid xg = gx \ \forall g \in G\}$$

לדוגמא:

$$Z(GL_2(\mathbb{Z}_p)) = \left\{ \begin{pmatrix} c & 0 \\ 0 & c \end{pmatrix} \mid c \in \mathbb{Z}_p^* \right\}$$

**טענה 1.63** תהי  $G$  חבורה. כל איבר  $x \in G$  מגדיר העתקה  $i_x$  באופן הבא:

$$i_x(g) = xgx^{-1}$$

אזי:

1.  $i_x$  הוא אוטומורפיזם של  $G$ .

2. ההעתקה  $i : G \rightarrow \text{Aut}(G)$  כאשר  $x \rightarrow i_x$  היא הומומורפיזם, ותמונתה היא ח"ח של  $\text{Aut}(G)$  שתקרא חבורת האוטומורפיזמים הפנימיים של  $G$ .

3. הגרעין על  $i$  הוא המרכז של  $G$ .

**הוכחה:** נוכיח:

1.  $i_x$  חח"ע:

$$i_x(g_1) = i_x(g_2) \Rightarrow xg_1x^{-1} = xg_2x^{-1} \Rightarrow g_1 = g_2$$

$i_x$  על:

$$g = i_x(x^{-1}gx)$$

$i_x$  הומומורפיזם:

$$i_x(g_1 \cdot g_2) = x(g_1 \cdot g_2)x^{-1} = xg_1x^{-1}xg_2x^{-1} = i_x(g_1) \cdot i_x(g_2)$$

2.  $i$  הומומורפיזם:

$$i_{xy}(g) = (xy)g(xy)^{-1} = xygy^{-1}x^{-1} = i_x(ygy^{-1}) = i_x(i_y(g)) = (i_x \circ i_y)(g)$$

3. מהו הגרעין של  $i$ ?

$$\begin{aligned} \ker(i) &= \{x \in G \mid i_x = id\} = \{x \in G \mid i_x(g) = g \ \forall g \in G\} = \{x \in G \mid xgx^{-1} = g \ \forall g \in G\} \\ &= \{x \in G \mid xg = gx \ \forall g \in G\} = Z(G) \end{aligned}$$

■

**בתרגיל** ראינו שהומומורפיזם  $\varphi$  הוא חח"ע אמ"מ הגרעין שלו הוא טריוויאלי, כלומר  $\ker \varphi = \{e\}$  - ולכן  $i : G \rightarrow \text{Aut}(G)$  היא חח"ע אמ"מ  $Z(G) = \{e\}$ .  
**תרגיל:** הוכח שאם  $Z(G) = \{e\}$  אזי  $Z(\text{Aut}(G)) = \{e\}$ .

**משפט 1.64** אם  $G$  חבורה סופית, וכמו כן  $Z(G) = \{e\}$ , אזי קיים  $n$  כך ש:

$$\text{Aut}^{(n)}(G) = \text{Aut}^{(n+1)}(G)$$

## 1.7 חבורות נורמליות, חבורות מנה ומשפטי הומומורפיזם

### 1.7.1 חבורות חלקיות נורמליות

**הגדרה 1.65** ח"ח  $N \leq G$  תקרא נורמלית אם לכל  $g \in G$  מתקיים  $gN = Ng$ . במקרה זה, נסמן  $N \triangleleft G$ .

**תזכורת:**

$$gN = \{gn | n \in N\}, \quad Ng = \{ng | n \in N\}$$

**טענה 1.66** תהי  $G$  חבורה,  $N \leq G$ . אזי הטענות הבאות שקולות:

1. לכל  $g \in G$ ,  $gN = Ng$ .

2. לכל  $g \in G$ ,  $g^{-1}Ng = N$ .

3. לכל  $g \in G$ ,  $g^{-1}Ng \subseteq N$ .

4. כל מחלקה ימנית של  $N$  ב- $G$  היא גם מחלקה שמאלית.

5. כל מחלקה שמאלית של  $N$  ב- $G$  היא גם מחלקה ימנית.

6. לכל  $g \in G, n \in N$ ,  $g^{-1}ng \in N$ .

**הוכחה:**  $1 \Leftarrow 2$ : אם לכל  $g \in G$ ,  $gN = Ng$ , אזי:

$$g^{-1}ng = g^{-1}(Ng) = g^{-1}(gN) = (g^{-1}g)N = N$$

$2 \Leftarrow 3$ : מיידי.

$2 \Leftarrow 3$ : בהנתן  $g \in G$ , צ"ל כי  $g^{-1}Ng = N$ . נתון רק כי  $g^{-1}Ng \subseteq N$ . אבל, זהנתון לכל  $g \in G$ , ובפרט גם ל- $g^{-1}$ . לכן:

$$\begin{aligned} (g^{-1})^{-1}Ng^{-1} \subseteq N &\Rightarrow gNg^{-1} \subseteq N \Rightarrow g(g^{-1}Ng)g^{-1} \subseteq gNg^{-1} \\ &\Rightarrow N \subseteq gNg^{-1} \end{aligned}$$

$1 \Leftarrow 2$ : לכל  $g \in G$  נתון כי  $g^{-1}Ng = N$ . נכפול בקבוע  $g$  משמאל ונקבל את השיויון המבוקש  $Ng = gN$ .

עד עכשיו הוכחנו שקילות בין שלוש התכונות הראשונות. ברור כי  $1 \Leftarrow 4$ ,  $5 \Leftarrow 1$ , לכן נותר להראות את הכיוון ההפוך:

$4 \Leftarrow 1$ : לכל  $g \in G$  קיים  $h \in G$  כלשהוא כך ש- $Ng = hN$ . מצד שני, נזכור כי אם  $H \leq G$ , ח"ח,  $a, b \in G$  אזי  $aH = bH$  אם ומ"מ  $a \in bH$ .

אזי  $Ng = hN$ , ולכן  $g = e \cdot g \in hN$ , כנדרש. ההוכחה של  $1 \Leftarrow 5$  היא תמונת ראי של ההוכחה הזו, וסיימנו. ■

<sup>7</sup>מהנתון - שהרי כל מחלקה ימנית היא גם מחלקה שמאלית.

### דוגמאות לחבורות חלקיות נורמליות

1. אם  $G$  אבלית אזי כל ח"ח היא נורמלית.
2. בכל חבורה  $G$ ,  $G$  ו- $\{e\}$  הן ח"ח נורמליות.
3. יהי  $F$  שדה, ונסמן  $G = GL_n(F)$ , וכמו כן:  

$$N = SL_n(F) = \{A \in GL_n(F) \mid \det(A) = 1\}$$

נוכיח כי  $N$  נורמלית:  
יהיו  $g \in G$ ,  $n \in N$  נוכיח כי  $g^{-1}ng \in N$ . אזי:  

$$\det(g^{-1}ng) = \det(g^{-1}) \cdot \det(n) \cdot \det(g) = \det(g)^{-1} \cdot \det(n) \cdot \det(g) = \det(g)^{-1} \cdot \det(n) \cdot \det(g) = \det(n) = 1$$
ומכיון והדטרמיננטה של  $g^{-1}ng$  היא אחד, אזי הוא ב- $N$ , כנדרש.
4. תהי  $G = Sym(n)$ , ותהי  $A_n = N$  חבורת התמורות הזוגיות. יהיו  $g \in G$ ,  $n \in N$  נוכיח כי  $g^{-1}ng \in N$ . כלומר, נרצה להראות כי הסימן שלו הוא 1. נחשב:  

$$\text{sign}(g^{-1}ng) = \text{sign}(g^{-1}) \cdot \text{sign}(n) \cdot \text{sign}(g) = \text{sign}(g^{-1} \cdot g) = \text{sign}(e) = 1$$
5. יהיו  $H \leq G$  מאינדקס 2 כלשהיא. אזי  $H$  נורמלית ב- $G$ .  
זאת מכיון ויש רק שתי מחלקות שמאליות. הן זרות, ויחד מכסות את  $G$ , מההגדרה. אחת מהן היא  $eH = H$ , ולכן בהכרח המחלקה השניה היא  $G \setminus H$ . אותו טיעון תופס גם למחלקות הימניות (כי אינדקס ימני = אינדקס שמאלי), ולכן המחלקות הימניות הן  $H$  ו- $G \setminus H$ , כלומר המחלקות הימניות הן גם מחלקות שמאליות, ולכן  $H$  נורמלית, כנדרש.

**למה 1.67**  $[S_n : A_n] = 2$  לכל  $n \geq 2$ . כלומר, ל- $A_n$  יש שתי מחלקות שמאליות:

$A_n$ , מחלקת התמורות הזוגיות, ו- $A_n(12)$ , מחלקת התמורות האי-זוגיות.

**הוכחה:** צ"ל שכל תמורה  $\sigma \in S_n/A_n$  נמצאת ב- $A_n(12)$ . אם  $\sigma \in S_n/A_n$ , אזי היא אי זוגית, ולכן:

$$\begin{aligned}\sigma' &= (12)\sigma \in A_n \\ \Rightarrow \sigma &= (12) \cdot (12) \cdot \sigma = (12) \cdot \sigma' \in (12)A_n\end{aligned}$$

■

6. יהיו  $G, L$  חבורות, ויהי  $\varphi : G \rightarrow L$  הומומורפיזם של חבורות.  
אזי  $\ker(\varphi) = \{g \in G \mid \varphi(g) = e_L\}$ . אזי,  $\ker(\varphi)$  היא תת חבורה נורמלית של  $G$ .  
קל לראות כי 3 דוגמא פרטית של 5 ו-6.

**הוכחה:** יהיו  $g \in G$ ,  $n \in \ker(\varphi)$ , וכרגיל, נרצה להראות כי  $g^{-1}ng \in N = \ker(\varphi)$ . נחשב:

$$\varphi(g^{-1}ng) = \varphi(g^{-1}) \cdot \varphi(n) \cdot \varphi(g) = \varphi(g^{-1}) \cdot e_L \cdot \varphi(g) = \varphi(g^{-1} \cdot g) = \varphi(e_G) = e_L$$

■

## 1.7.2 חבורות מנה

**הגדרה 1.68** תהי  $G$  חבורה, ותהי  $N \triangleleft G$ .  
נסמן ב- $G/N$  ("מוד  $N$ ") את חבורת המחלקות השמאליות של  $N$  ב- $G$ .

**טענה 1.69** אם נגדיר את הכפל בצורה הבאה:

$$\forall g_1, g_2 \in G \quad (g_1 N) \cdot (g_2 N) = g_1 g_2 N$$

אזי  $G/N$  חבורה.  
כלומר, נצטרך להוכיח:

1. הכפל מוגדר היטב.

2.  $G/N$  היא חבורה בקשר לפעולת הכפל הזו - כלומר, עלינו להוכיח:

(א) אסוציאטיביות.

(ב) קיום איבר היחידה.

(ג) קיום איבר הופכי.

**הוכחה:** נוכיח תחילה כי הכפל מוגדר היטב:

**למה 1.70** כמכפלת קבוצות, מתקיים:

$$\forall g_1, g_2 \in G \quad (g_1 N) \cdot (g_2 N) = g_1 g_2 N$$

**הוכחה:**

$$(g_1 N) \cdot (g_2 N) = g_1 N g_2 N \stackrel{N \text{ is Normal}}{=} g_1 (g_2 N) N = g_1 g_2 N$$

■

יהיו  $x_1, x_2 \in G$ , וכמו כן  $g_1 N = x_1 N$ ,  $g_2 N = x_2 N$ . נרצה להוכיח כי  $g_1 g_2 N = x_1 x_2 N$ .  
נחשב:

$$g_1 = x_1 n_1, g_2 = x_2 n_2 \Rightarrow g_1 g_2 N = x_1 n_1 x_2 n_2 N = x_1 n_1 x_2 N$$

$$\stackrel{N \text{ is normal}}{=} x_1 x_2 n_1 N = x_1 x_2 N$$

ולכן הכפל מוגדר. נוכיח כי  $G/N$  היא אכן חבורה ביחס לפעולת הכפל הנ"ל.  
אסוציאטיביות:

$$(g_1 N) ((g_2 N) (g_3 N)) \stackrel{?}{=} ((g_1 N) (g_2 N)) (g_3 N)$$

$$\Rightarrow (g_1 N) (((g_2 N) (g_3 N))) = (g_1 N) (g_2 g_3 N) = g_1 (g_2 g_3) N = (g_1 g_2) g_3 N$$

$$= (g_1 g_2 N) g_3 N = ((g_2 N) (g_3 N)) (g_1 N)$$

איבר היחידה הוא  $eN$ :

$$(gN)(eN) = (ge)N = gN, (eN)(gN) = egN = gN$$

האיבר ההפכי של  $gN$  הוא  $g^{-1}N$ :

$$(gN)(g^{-1}N) = gg^{-1}N = eN$$

■

**טענה 1.71** ההעתקה  $\pi : G \rightarrow G/N$  כאשר  $\pi(g) = gN$  היא הומומורפיזם, וכמו כן,  $\ker(\pi) = N$ .

**הגדרה 1.72** הומומורפיזם הנ"ל נקרא ההשלכה הטבעית.

**הוכחה:**

$$\pi(g_1g_2) = (g_1g_2)N = g_1N \cdot g_2N = \pi(g_1) \cdot \pi(g_2)$$

ולכן זהו אכן הומומורפיזם.  
נוכיח כי הקרנל הוא אכן  $N$ :

$$\begin{aligned} \ker(\pi) &= \{g \in G \mid \pi(g) = e_{G/N}\} = \{g \in G \mid \pi(g) = eN\} \\ &= \{g \in G \mid gN = eN = N\} = \{g \in N \mid g \in N\} = N \end{aligned}$$

■

**הערה 1.73** זהו גם אפימורפיזם!

### 1.7.3 משפט הומומורפיזם הראשון

10/11/2010

**משפט 1.74** יהא  $\varphi : G \rightarrow H$  אפימורפיזם, ונסמן  $N = \ker(\varphi)$  חבורות. אזי  $G/N \simeq H$ , והאיזומורפיזם ניתן ע"י  $\bar{\varphi}(gN) = \varphi(g)$ .

**הוכחה:** נוכיח תחילה כי  $\bar{\varphi}$  מוגדרת היטב - כלומר, אם  $g_1N = g_2N$ , אזי צריך לוודא כי  $\varphi(g_1) = \varphi(g_2)$ . ואכן, אם  $g_1 = ng_2$  עבור  $n \in N$  כלשהוא, אזי

$$\varphi(g_1) = \varphi(g_2n) = \varphi(g_2) \cdot \varphi(n) \stackrel{n \in \ker(\varphi)}{=} \varphi(g_2) \cdot e_H = \varphi(g_2)$$

כעת, נוכיח כי  $\bar{\varphi}$  היא הומומורפיזם:

$$\bar{\varphi}((g_1g_2)N) = \varphi(g_1g_2) = \varphi(g_1) \cdot \varphi(g_2) = \bar{\varphi}(g_1) \cdot \bar{\varphi}(g_2)$$

ולבסוף, נוכיח כי  $\bar{\varphi}$  היא חח"ע ועל, ונסיים:

יהי  $h \in H$ , וע"מ להוכיח כי ההעתקה היא על, יש להוכיח כי קיימת  $gN \in G/N$  כך ש:  $\bar{\varphi}(gN) = h$ .  
 $\varphi$  איזומורפיזם, ולכן קיים  $g \in G$  כך ש-  $\varphi(g) = h$ . אם כך, עבור המחלקה  $gN$  מתקיים  $\bar{\varphi}(gN) = \varphi(g) = h$ .  
 נזכור כי  $\bar{\varphi}$  חח"ע אמ"מ גרעינו טריוויאלי. נבדוק אם כך מהו:  
 $\ker(\bar{\varphi}) = \{gN | \bar{\varphi}(gN) = e_H\} = \{gN | \varphi(g) = e_H\} = \{gN | g \in N\} = \{eN\} = \{e_{G/N}\}$   
 כלומר הגרעין טריוויאלי, כנדרש. ■

## דוגמאות

- תהי  $\varphi : \mathbb{Z} \rightarrow \mathbb{Z}_m$  כאשר  $n \rightarrow n \pmod{m}$ ,  $m \in \mathbb{N}$ . אזי,  $\ker(\varphi) = m \cdot \mathbb{Z}$ , ולכן, מהמשפט,  $\mathbb{Z}_m \cong \mathbb{Z}/m \cdot \mathbb{Z}$ .
  - תהי  $\det : GL_2(\mathbb{F}) \rightarrow \mathbb{F}^*$  כאשר  $\det \begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix} = a \in \mathbb{F}^*$ . אזי  $\ker(\det) = \{A \in GL_2(\mathbb{F}) | \det(A) = 1\} = SL_2(\mathbb{F})$ , ולכן, מהמשפט,  $\mathbb{F}^* \cong GL_2(\mathbb{F})/SL_2(\mathbb{F})$ .
  - תהי  $sign : S_n \rightarrow \{\pm 1\}$  אפימורפיזם המתאים לתמורה את הזוגיות שלה (כפי שהגדרנו בדיון קודם). אזי  $\ker(sign) = A_n$ , אוסף התמורות הזוגיות, ולכן, מהמשפט,  $S_n/A_n \cong \{\pm 1\}$ .
  - תהי  $\varphi : \mathbb{R}_+ \rightarrow S^1 = \{z \in \mathbb{C} | |z| = 1\}$  כלומר  $\varphi : \mathbb{R}_+ \rightarrow S^1$  הוא מעגל היחידה עם פעולת הכפל, כאשר  $\varphi(x) = e^{2\pi i x}$ . אזי  $\ker(\varphi) = \mathbb{Z}$ , ולכן  $\mathbb{R}_+/ \mathbb{Z} \cong S^1$ .
- למה 1.75** אם  $G$  חבורה,  $N, H \leq G$ , וכמו כו  $N \triangleleft G$ , אזי  $NH = HN$  היא חבורה חלקית, כאשר  $NH = \{n \cdot h | n \in N, h \in H\}$ .
- הערה 1.76** אזהרה - אם  $H_1, H_2 \leq G$  חבורות חלקיות, אזי  $H_1 H_2$  אינה בהכרח ח"ח!  
**הוכחה:** נוכיח כי  $NH = HN$  ע"י הכלה דו כיוונית:

$$nh = h(h^{-1}nh) \in HN \Rightarrow NH \subseteq HN$$

$$hn = (hnh^{-1})h = ((h^{-1})^{-1}n(h^{-1}))h \in NH$$

כאשר המעברים הם מכיוון  $N$  נורמלית (ולכן  $h^{-1}nh, hnh^{-1} \in N$ ). נראה כי  $NH = HN$  היא חבורה חלקית. נראה סגירות ביחס לכפל: יהיו  $n_1, n_2 \in N$ ,  $h_1, h_2 \in H$ ,  $h_i, n_i \in HN$  נחשב:

$$(h_1 n_1)(h_2 n_2) = \left( \underbrace{(h_1 h_2)}_{\in H} \underbrace{(h_2^{-1} n_1 h_2)}_{\in N} \underbrace{n_2}_{\in N} \right) \in HN$$

ולסיום, נראה קיום הופכי:

$$(hn)^{-1} = n^{-1}h^{-1} \in NH = HN$$

■

היחידה נמצאת כי היא גם ב- $H$  וגם ב- $N$ .

#### ניסוח מחדש של המשפט:

**משפט 1.77** יהי  $\varphi : G \rightarrow N$  הומומורפיזם כלשהוא כך ש- $\ker(\varphi) = N$ . אזי, קיים הומומורפיזם יחיד כך  $\tilde{\varphi} = G/N \rightarrow H$  כך שהדיאגרמה הבאה קמוטטיבית:

$$G \xrightarrow{\varphi} H, \quad G \xrightarrow{\pi} G/N \xrightarrow{\exists! \tilde{\varphi}} H \Rightarrow \tilde{\varphi} \circ \pi = \varphi, \quad \forall g \in G \quad \tilde{\varphi}(\pi(g)) = \varphi(g)$$

ובפרט  $\text{Im}(\varphi) \cong G/\ker(\varphi)$ .

#### 1.7.4 משפט ההומומורפיזם השני

15/11/2010

**משפט 1.78** תהי  $G$  חבורה,  $N, H \leq G$ , כך ש- $N \triangleleft G$ . אזי  $H \cap N \triangleleft H$ , ומתקיים:

$$HN/N \simeq H/H \cap N$$

**הערה 1.79** נזכור כי ראינו כי  $HN = NH$ , והיא ח"ח של  $G$ .

**הערה 1.80** בפרט אנו טוענים כי אם  $N, H \leq G$ , כך ש- $N \triangleleft G$ , אזי  $H \cap N \triangleleft H$ .

**הוכחה:** ברור שגם  $H, N \leq HN$  - מההגדרות:

$$HN = \{hn | h \in H, n \in N\} \supseteq H = \{he | h \in H, e \in N\}$$

וכמו כן  $N \triangleleft HN$ , כי נתון ש- $N \triangleleft G$ . לכן  $HN/N$  מוגדרת, ויש הומומורפיזם  $\pi : HN \rightarrow HN/N$ . נצמצם את  $\pi$  ל- $H$  ונסמנו ב- $\pi_0$ :

$$\pi_0 : H \rightarrow HN/N$$

**טענה 1.81**  $\pi_0$  היא אפימורפיזם, כלומר על, וכמו כן,  $\ker(\pi_0) = H \cap N$ .

בהנחה שטענת העזר נכונה, נקבל כי  $\pi_0$  הוא איזומורפיזם מ- $H/H \cap N$  ל- $HN/N$ , ולכן, ממשפט ההומומורפיזם הראשון,  $HN/N \cong H/H \cap N$ . נוכיח את הטענה, ונסיים: **הוכחה:** תהא  $gN$  מחלקה של  $N$  ב- $HN$ . לכן  $g \in HN$ , כלומר קיימים  $h_1 \in H$ ,  $n_1 \in N$ , כך ש- $g = h_1 n_1$ . אזי:

$$gN = h_1 n_1 N = h_1 N \Rightarrow gN = h_1 N = \pi(h_1) = \pi_0(h_1)$$

ולכן  $\pi_0$  היא על.

נמצא את  $\ker(\pi_0)$ :

$$\ker(\pi_0) = \{h \in H \mid \pi_0(h) = eN\} = \{h \in H \mid hN = eN\} = \{h \in H \mid h \in N\} = H \cap N$$

■

וסיימנו.

■

**הערה 1.82** נשים  $\heartsuit$  כי מהוכחת הקרנל של  $\pi_0$  נובע  $H \cap N \triangleleft H$ , כי ראינו שגרעין של הומומורפיזם הוא נורמלי במקור. תרגיל - הוכיחו ישירות כי  $H \cap N \triangleleft H$ .

### 1.7.5 משפט ההתאמה

**משפט 1.83** יהי  $\varphi: G \rightarrow H$  אפימורפיזם. אזי יש התאמה  $\psi$  חח"ע ועל בין ח"ח של  $H$  ובין ח"ח של  $G$  המכילה את  $\ker(\varphi) = N$ . נסמן  $N \leq K \leq G, L \leq H$ . אזי, ההתאמה ניתנת באופן הבא:

$$\psi(L) = \{g \in G \mid \varphi(g) \in L\} (= \varphi^{-1}(L))$$

ובכיוון ההפוך, קיימת  $\psi'$  כך ש:

$$\psi'(K) = \varphi(K) = \{\varphi(k) \mid k \in K\}$$

למעשה, אנו טוענים:

1.  $\psi(L)$  היא ח"ח המכילה את  $N$ .

2.  $\psi'(K)$  ח"ח.

3.  $\psi \circ \psi' = id, \psi' \circ \psi = id$ , כלומר  $\psi, \psi'$  היא חח"ע ועל.

4.  $L \triangleleft H$  אמ"מ  $\psi(L) \triangleleft G$ .

5.  $K \triangleleft G$  אמ"מ  $\psi'(K) \triangleleft H$ .

כאשר שתי הטענות האחרונות נוספות (ולא קשורות לתחילת המשפט).

**הוכחה:** נוכיח כל תת טענה:

1. נבדוק קודם ש- $\psi(L)$  ח"ח - מספיק להראות שאם  $x, y \in \psi(L)$  אזי גם  $xy^{-1} \in \psi(L)$ , כלומר  $\varphi(xy^{-1}) \in L$ . נחשב:

$$\varphi(xy^{-1}) = \varphi(x) \cdot \varphi(y^{-1}) = \varphi(x) \cdot \varphi(y)^{-1} \in L$$

כי  $\varphi(x), \varphi(y) \in L$  ונתון ש- $L$  ח"ח. לכן  $\psi(L)$  ח"ח, ולכן היא מכילה את  $\psi(\{e\}) = N$  שהרי  $\{g \in G \mid \varphi(g) = e\} = N$ .

2.  $\psi'(K) = \varphi(K)$ ,  $\varphi$  הומומורפיזם, וכבר ראינו שהומומורפיזם מעביר ח"ח לח"ח - ולכן גם  $\psi'(K)$  גם ח"ח.

3. תהא  $K$  ח"ח של  $G$  המכילה את  $N$ . נחשב:

$$(\psi \circ \psi')(K) = \psi(\psi'(K)) = \psi(\varphi(K)) = \{g \in G \mid \varphi(g) \in \varphi(K)\}$$

נראה שמה שהתקבל הוא בדיוק  $K$  - נניח  $g \in G$ , וקיים  $k \in K$  כך ש- $\varphi(g) = \varphi(k)$ .  
 לכן  $\varphi(gk^{-1}) = e$ , כלומר  $gk^{-1} \in N \leq K$ , ולכן  $gk^{-1} \in K$ . כלומר, קיים  $k_0 \in K$   
 כך ש- $gk^{-1} = k_0$ , ולכן  $g = k_0k \in K$ , ולכן  $\psi \circ \psi' = id$ . מצד שני, תהא  $L \leq H$ . נחשב:

$$\psi' \circ \psi = \psi'(\{g \in G \mid \varphi(g) \in L\}) = \{\varphi(g) \mid \varphi(g) \in L, g \in G\} = L$$

כאשר השיויון נובע מכך שלכל איבר  $d \in L$  קיים  $g \in G$  כך ש- $\varphi(g) = d$ , כי  $\varphi$  על.

לסיים, מספיק אם נוכיח את הכיוון  $\Leftarrow$  לשתי הטענות האחרונות - מדוע? הסיבה מושארת כתרגיל.

את הקטע הזה יש להשלים - לא מופיע מסודר במחברת...  
 נניח  $L \triangleleft H$ , ויהי  $g \in G$ ,  $x \in \psi(L)$ , כלומר, קיים  $x_1 \in L$  נרצה להוכיח  $g^{-1}xg \in \psi(L)$ , כלומר  $\varphi(g^{-1}xg) \in L$ . אזי:

$$\varphi(g^{-1}xg) = \varphi^{-1}(g) \cdot \varphi(x) \cdot \varphi(g) \in L$$

■ מצד שני, נניח כי  $K \triangleleft G$ , ונוכיח כי  $\psi'(K) \triangleleft H$ .

**הערה 1.84** ניסוח אחר למשפט ההתאמה:

תהא  $G$  חבורה,  $N \triangleleft G$ , ויהי  $\pi: G \rightarrow G/N$  האפימורפיזם הטבעי. אזי יש התאמה חח"ע ועל בין הח"ח של  $G/N$  ובין הח"ח של  $G$  המכילות את  $N$ . התאמה זו ניתנת כך:  
 אם  $L \leq G/N$ , אזי:

$$\psi(L) = \{g \in G \mid \pi(g) \in L\} = \{g \in G \mid gN \in L\}$$

ואם  $N \leq K \leq G$ , ובפרט  $N \triangleleft K$ , אזי:

$$\psi'(K) = K/N \leq G/N$$

וכמו כן  $\psi \circ \psi' = id$ , והן חח"ע ועל, ומתקיים

$$K/N \triangleleft G/N \Leftrightarrow K \triangleleft G, \psi(L) \triangleleft G \Leftrightarrow L \triangleleft G/N$$

**1.7.6 משפט ההומומורפיזם השלישי**

**משפט 1.85** יהיו  $N \triangleleft G$ ,  $N \leq K \triangleleft G$ . אזי:

$$(G/N)/(K/N) \simeq G/K$$

**הוכחה:** יש לפרמל ההוכחה - נוסח לא מפורט מהכיתה:  
נגדיר הומומורפיזם  $\eta: G/N \rightarrow G/K$  ע"י  $\eta(gN) = gK$ . נוכיח כי ההעתקה זו מוגדרת היטב, וכן שהיא הומומורפיזם - מושאר לקורא השקדן.  
 $\eta$  היא על - טריוויאל. כמו כן:

$$\ker(\eta) = \{gN | gK = eK\} = K/N$$

ולכן, לפי משפט ההומומורפיזם הראשון:

$$(G/N)/(K/N) \simeq G/K$$

■

כנדרש.

17/11/2010

## 1.8 סדרות נורמליות, סדרות הרכב

22/11/2010

### 1.8.1 למת צננהאוס

**למה 1.86** תהי  $G$  חבורה,  $A, B, A^*, B^*$  חבורות חלקיות של  $G$  כך ש- $A \triangleleft A^*, B \triangleleft B^*$ . אזי:

1.

$$B(B * \cap A) \triangleleft B(B * \cap A^*), A(A * \cap B) \triangleleft A(A * \cap B^*)$$

2.

$$A \cdot (A^* \cap B^*) / A \cdot (A^* \cap B) \cong B \cdot (B^* \cap A^*) / B \cdot (B^* \cap A)$$

### 1.8.2 סדרות נורמליות

**הגדרה 1.87** תהי  $G$  חבורה. אזי:

$$\{e\} = G_l \triangleleft G_{l-1} \triangleleft \dots \triangleleft G_1 \triangleleft G_0 = G$$

תקרא סדרה נורמלית.

**הערה 1.88** נשים  $\heartsuit$  כי  $G_i \triangleleft G_{i-1}$  לכל  $1 \leq i \leq l$ , ולא דווקא  $G_i \triangleleft G$ !

**הערה 1.89** נסמן את הסדרה הנ"ל ב- $(*)$ .

**הערה 1.90** ייתכן ו- $G_i = G_{i-1}$ .

**הגדרה 1.91** הסדרה:

$$\{e\} = H_m \triangleleft H_{m-1} \triangleleft \dots \triangleleft H_0 \triangleleft G$$

תקרא שקולה ל- $(*)$  אם  $l = m$ , ואם קיימת תמורה:

$$\sigma : \{1, \dots, l\} \rightarrow \{1, \dots, l\}$$

כך שלכל  $1 \leq i \leq l-1$  מתקיים:

$$G_{i-1}/G_i \simeq H_{\sigma(i-1)}/H_{\sigma(i)}$$

**הערה 1.92** נסמן סדרה זו ב- $(**)$ .

**הגדרה 1.93** הסדרה  $(**)$  תקרא עידון ל- $(*)$  אם הסדרה  $G_l, G_{l-1}, \dots, G_0$  היא תת סדרה של  $H_m, H_{m-1}, \dots, H_0$ .

**משפט שרייר**

24/11/2010

**משפט 1.94** תהי  $G$  חבורה. אזי לכל שתי סדרות נורמליות יש עידונים שקולים.

**הוכחה:** נשתמש בסימוני  $(*)$  ו- $(**)$ , ונגדיר:

$$H_{-1} = G_{-1} = G, \quad H_{l+1} = G_{l+1} = \{e\}$$

אזי  $G_{ij} = G_{i+1} (G_i \cap H_j)$  עבור  $0 \leq i \leq m, 0 \leq j \leq l$  היא הסדרה:

$$\dots \triangleleft G_{12} \triangleleft G_{11} \triangleleft G_{10} = G_1 \triangleleft G_{0,m-1} \triangleleft \dots \triangleleft G_{0,2} \triangleleft G_{0,1} \triangleleft G_{00} = G_0 = G$$

ונגדיר  $H_{ij} = H_{j+1} (H_j \cap G_i)$  נקבל:

$$\dots \triangleleft H_{2,1} \triangleleft H_{1,1} \triangleleft H_{0,1} = H_1 \triangleleft H_{l-1,0} \triangleleft \dots \triangleleft H_{2,0} \triangleleft H_{1,0} \triangleleft H_{0,0} = H_0 = G$$

אם נסמן  $A^* = G_i, A = G_{i+1}, B^* = H_{j-1}, B = H_j$ . התנאים של הלמה של צצנהאוס מתקיימים, ולכן נקבל:

$$G_{ij} = G_{i+1} (G_i \cap H_j) \triangleleft G_{i+1} (G_i \cap H_{j-1}) = G_{i,j-1}$$

נשים לב כי ישנם מעברים שהלמה לא מסבירה. נוכיח אותם:

$$G_{i-1,m} = G_i (G_{i-1} \cap H_m) = G_i (G_{i-1} \cap \{e\}) = G_i$$

כלומר, במעברים אלו מדובר באותן החבורות, ולכן החבורה  $G_{i-1,m}$  נורמלית בעצמה. בסה"כ קיבלנו כי זהו עידון! באותו האופן:

$$H_{i+1,j-1} = H_j (H_{j-1} \cap G_{i+1}) \triangleleft H_j (H_{j-1} \cap G_i) = H_{i,j-1}$$

אז זהו עידון של  $(**)$ . אזי, מהלמה של צצנהאוס, מתקיים:

$$H_{i,j-1}/H_{i+1,j-1} \simeq G_{i,j-1}/G_{i,j}$$

כלומר שני העידונים שקולים, כנדרש!

■

### 1.8.3 סדרות הרכב

הוכחה:

29/11/2010

■

### 1.8.4 משפט ג'ורדן הולדר

**משפט 1.95** כל שתי סדרות הרכב בחבורה  $G$  שקולות.

**הוכחה:** על פי משפט שרייר, יש להם עידונים שקולים. עידונים שכאלו ישאירו את חבורות המנה המקוריות (שהן לא טריוויאליות), ויוסיפו רק מנות טריוויאליות, ולכן אם שקולות לאחר העידון, הן היו שקולות לפני העידון.

■

**אזהרה!** לא לכל חבורה יש סדרת הרכב. אבל בחבורה סופית תמיד יש סדרת הרכב.  
**הוכחה:** באינדוקציה על הסדר על  $G$ .

■

## 1.9 חבורות פתירות

**הגדרה 1.96** חבורה  $G$  נקראת פתירה אם יש לה סדרה נורמלית סופית כך שכל המנות  $G_{i-1}/G_i$  הן חבורות אבליות לכל  $i = 1, \dots, l$ .

תזכורת מהתרגיל -

**הגדרה 1.97** בהנתן חבורה  $G$ , נסמן:

$$G' = [G, G] = \langle \{g^{-1}h^{-1}gh \mid g, h \in G\} \rangle$$

זוהי חבורת הקומוטטור\חבורת הנגזרת, כאשר  $(g, h) = g^{-1}h^{-1}gh$  הקומוטטור של  $g$  ו- $h$ .  
תכונותיה:

1.  $G' \triangleleft G$ .

2.  $G/G'$  אבלית.

3. אם  $N \triangleleft G$  ו- $N/G'$  אבלית, אזי  $G' \leq N$ .

**הגדרה 1.98** הסדרה הנגזרת תהיה, בסימונים של ההגדרה הקודמת:

$$G_{(0)} = G, G_{(1)} = G', G_{(2)} = G'_{(1)}, \dots, G_{(i+1)} = G'_{(i)}$$

**טענה 1.99** חבורה היא פתירה אם"מ קיים  $l$  כך ש- $G_{(l)} = \{e\}$ .

■

**הוכחה:**  $\Rightarrow$  נניח ש- $G_{(l)} = \{e\}$ . אזי:

**טענה 1.100** חבורה סופית  $G$  היא פתירה אם"מ כל גורמי ההרכב שלה הן חבורות ציקליות מסדר ראשוני.

**משפט 1.101** ל- $n \geq 5$ ,  $A_n = \text{Alt}(n)$  חבורת התמורות הזוגיות על  $n$  עצמים, היא חבורה פשוטה.

### 1.10 פעולה של חבורה $G$ על קבוצה $X$

**הגדרה 1.102** פעולה של חבורה  $G$  על קבוצה  $X$ . היא פונקציה  $\alpha : G \times X \rightarrow X$ , כך ש:

1.

$$\alpha(e, x) = x$$

2.

$$\alpha(g_1 g_2, x) = \alpha(g_1, \alpha(g_2, x))$$

#### 1.103 מסקנה

$$\alpha(g^{-1}g, x) = \alpha(e, x) = x$$

ומצד שני:

$$\alpha(g^{-1}g, x) = \alpha(g^{-1}, \alpha(g, x))$$

**טענה 1.104** אם  $\alpha : G \times X \rightarrow X$  פעולה של  $G$  על  $X$ , אזי, ההעתקה  $\varphi : G \rightarrow \text{Sym}(X)$  המוגדרת כך ש:  $(\varphi(g))(x) = \alpha(g, x)$  היא הומומורפיזם.

**הערה 1.105** לכל  $g \in G$  -  $\varphi(g)$  תמורה, כלומר חח"ע ועל, כי קיים הפכי:

$$\varphi(g^{-1}) \cdot \varphi(g) = \varphi(g^{-1})(\alpha(g, x)) = \alpha(g^{-1}, \alpha(g, x)) = \alpha(g^{-1}g, x) = \alpha(e, x) = x$$

**טענה 1.106** בהנתן הומומורפיזם  $\varphi : G \rightarrow \text{Sym}(X)$ , נגדיר  $\alpha : G \times X \rightarrow X$  באופן הבא:

$$\alpha(g, x) = (\varphi(g))(x)$$

אזי,  $\alpha$  מגדירה פעולה של  $G$  על  $X$ .

**נסמן** בקיצור  $\alpha(g, x) = g.x$ .

**נשים**  $\heartsuit$  -  $G$  יכולה לפעול על  $X$  בצורות שונות.

**לדוגמא,**  $G$  פועלת על עצמה בשלוש צורות:

1.

$$\alpha : G \times G \rightarrow G, \alpha(g, x) = g \cdot x$$

נראה כי זו אכן פעולה, כלומר כי שני התנאים מתקיימים:

$$1. \alpha(e, x) = e \cdot x = x$$

$$2. \alpha(g_1 g_2, x) = (g_1 g_2) x = g_1 (g_2 x) = g_1 \cdot \alpha(g_2, x) = \alpha(g_1, \alpha(g_2, x))$$

כאשר המעבר השני הוא בגלל אסוציאטיביות.

2.

$$\beta : G \times G \rightarrow G, \beta(g, x) = x \cdot g^{-1}$$

3.

$$\gamma : G \times G \rightarrow G, \gamma(g, x) = x g x^{-1}$$

**הערה 1.107** נשים  $\heartsuit$  שהפעולה  $\gamma$  מעלה מגדירה הומומורפיזם  $\varphi : G \rightarrow \text{Sym}(G)$  כך ש- $\varphi(g(x)) = x g x^{-1}$ , ולמעשה  $\text{Im}(G) \leq \text{Aut}(G) \leq \text{Sym}(G)$ . זה לא נכון בסעיפים 1,2.

**הגדרה 1.108** אם  $G$  פועלת על  $X$ , ו- $x_0 \in X$ , המסלול של  $x_0$  ביחס ל- $G$  הוא הקבוצה:

$$[x_0] = G.x_0 = \{g.x_0 | g \in G\}$$

**דוגמאות:**

המסלולים של הפעולות בדוגמא הקודמת הם:

1.

$$[x_0] = X = G$$

2.

$$[x_0] = X = G$$

3.  $[x_0]$  היא מחלקת הצמידות של  $x_0$ .

**טענה 1.109** תהי  $G$  חבורה הפועלת על  $X$  לכל  $x, y \in X$ . אזי:  
או  $[x] \cap [y] = \emptyset$ , או  $[x] = [y]$ .

**מסקנה 1.110** תהי  $G$  פועלת על  $X$ , ונגדיר  $x \sim y$  אם קיים  $g \in G$  כך ש- $g.x = y$ . זהו יחס שקילות, ומחלקות השקילות הן בדיוק המסלולים.

**הגדרה 1.111** תהי  $G$  פועלת על  $X$ . נגדיר את המייצב של  $x_0 \in X$  להיות:

$$G_{x_0} = \{g \in G \mid g.x_0 = x_0\}$$

**טענה 1.112** אם  $G$  פועלת על  $X$ , ו- $x_0 \in X$ , אזי יש התאמה חח"ע ועל בין איברי המסלול  $[x_0]$  למחלקות השמאליות של המייצב של  $x_0$ , הניתנת ע"י:

$$\eta = gH \rightarrow g.x_0$$

**מסקנה 1.113** תהי  $G$  פועלת על  $X$ , ונניח כי  $G.x_0 = [x_0]$  המסלול של  $x_0$  הוא סופי. אזי,  
 $|[x_0]| = [G : G_{x_0}]$ .

**מסקנה 1.114** בפרט, אם  $G$  סופית ופועלת על  $X$ , אזי אורך כל מסלול מחלק את הסדר של  $G$ .

**מסקנה 1.115** מסקנה מהמסקנה הקודמת - אם  $G$  חבורה סופית, אזי הסדר של כל מחלקת צמידות מחלק את הסדר של החבורה.

לדוגמא, עבור  $G = S_n$ ,  $|S_n| = n!$ , והסדר של מחלקת הצמידות, כלומר החילופים, הוא  $\binom{n}{2} \cdot n!$  ואכן  $\binom{n}{2} \mid n!$ .

**הגדרה 1.116** תהי  $G$  פועלת על  $X$ . אזי  $x_0 \in X$  נקרא נקודת שבת, אם לכל  $g \in G$  מתקיים  $g.x_0 = x_0$ . כלומר:

$$[x_0] = \{x_0\} \Leftrightarrow G_{x_0} = G$$

**דוגמא** תהי  $G$  הפועלת על עצמה על ידי הצמדה. מהם נקודות השבת? בדיוק המרכז  $Z(G)$ .

תזכורת - לפעולה הזו:

$x_0 \in Z(G)$  הוא  $Center = Merkaz$  אמ"מ  $gx_0g^{-1} = x_0$  לכל  $g \in G$ , כלומר האיברים שלכל  $g \in G$  הפעלת הפעולה עליהם משאירה אותם כפי שהיו. המרכז  $Centralizer = Merakez$  הוא הקבוצה:

$$G_{x_0} = \{g \in G | gx_0g^{-1} = x_0\} = C_G(x_0)$$

**מסקנה 1.117** אם  $G$  חבורה סופית,  $Z(G)$ , ונניח  $c_1, c_2, \dots, c_l$  מחלקות צמידות ב- $G$  של איברים לא מרכזים. אזי:

$$|G| = |Z(G)| + \sum_{i=1}^n |c_i|$$

ואם נסמן  $x_1, x_2, \dots, x_l$  מייצגי מחלקות הצמידות הלא מרכזיות, אזי אם נציב, נקבל את המשוואה החיבורית של  $G$ :

$$|G| = |Z(G)| + \sum_{i=1}^l [G : C_G(x_i)]$$

**הגדרה 1.118** יהא  $p$  מספר ראשוני. חבורה סופית נקראת חבורת  $p$ , אם לאיזשהו  $n \in \mathbb{N}$ .

**משפט 1.119** אם  $G$  חבורת  $p$ , אזי  $Z(G) \neq \{1\}$ .

**מסקנה 1.120** כל חבורת  $p$  סופית היא פתירה.

**משפט 1.121** תהי  $G$  חבורה סופית ו- $p$  ראשוני, ונניח  $|G| = p^r$ . אזי יש ב- $G$  איבר  $x \neq e$  כך ש- $x^p = 1$ . כלומר, יש איבר מסדר  $p$ .

8/12/2010

**1.11 משפט סילוא - Sylow**

**משפט 1.122** תהי  $G$  חבורה סופית מסדר  $|G| = p^r \cdot m$ , כאשר  $p$  ראשוני,  $r \geq 1$ ,  $(m, p) = 1$ . אזי:

1. יש ל- $G$  חבורה חלקית מסדר  $p^r$ .

**הגדרה 1.123** חבורה כזו נקראת חבורת  $p$ -סילוא של  $G$ . היא מאופיינת בכך שזו חב'  $p$  שהאינדקס שלה זר ל- $p$ .

2. כל חבורת  $p$  המוכלת ב- $G$  מוכלת באיזשהי חבורת  $p$ -סילוא.

3. כל חבורות  $p$ -סילוא של  $G$  צמודות זו לזו.

4. נסמן ב- $l$  את מספר חבורות ה- $p$ -סילוא השונות ב- $G$ . אז  $l \equiv 1 \pmod{p}$  וגם  $l|m$ .

**הגדרה 1.124**  $G$  חבורה,  $M$  ח"ח של  $G$ . נסמן:

$$Y = \{gMg^{-1} | g \in G\}$$

זהו אוסף החבורות החלקיות הצמודות ל- $M$  ב- $G$ .

נשים ♡ שלא בהכרח הח"ח שנקבל שונות אחת מהשניה.