

תורת החבורות 88-218-01 תשפ"א

הערות הרצאה 3

תזכורת 0.1. חבורה, תת-חבורה, חבורות ציקליות, פונקציות, חח"ע, על, יחס שקילות ומחלקות שקילות.

0.1 מחלקות

משפט 0.2 (לגראנז'). תהי G חבורה סופית, ותהי $H \leq G$ תת-חבורה שלה. אז $|H| \mid |G|$.

צריך לדעת מה זה יחס שקילות (יח"ש) \sim על קבוצה A . צריך להזכר שלכל $a \in A$ יש מחלקת שקילות תחת היחס הזה המוגדרת לפי $[a] = \{x \in A \mid a \sim x\}$. מחלקות שקילות הן זרות (אם הן שונות) והאיחוד שלהן הוא A .

הוכחה. בהנתן $H \leq G$, נגדיר שני יחסים על G :

$$\begin{aligned}x \sim_l y &\iff \exists h \in H, x = yh \\x \sim_r y &\iff \exists h \in H, x = hy\end{aligned}$$

כלומר $x \sim_l y$ אם ורק אם $y^{-1}x \in H$. נראה כי \sim_l הוא יח"ש (ההוכחה עבור \sim_r דומה):

1. (רפלקסיביות) לכל $x \in G$ מתקיים $x \sim_l x$ כי $x = x \cdot e$ והרי $e \in H$ מפני ש- H תת-חבורה.

2. (סימטריות) לכל $x, y \in G$ אם $x \sim_l y$, אז קיים $h \in H$ כך ש- $x = yh$. נכפיל ב- h^{-1} מימין ונקבל $y = xh^{-1}$. מפני ש- $h^{-1} \in H$ שהרי H סגורה להופכי, אז $y \sim_l x$.

3. (טרנזיטיביות) נניח $x \sim_l y$ וגם $y \sim_l z$, אזי קיימים $h_1, h_2 \in H$ כך ש- $x = yh_1$ וגם $y = zh_2$ אז נציב

$$x = yh_1 = zh_2h_1$$

ומפני ש- $h_2h_1 \in H$, אזי $x \sim_l z$.

לכן \sim_l יח"ש. נסמן את מחלקת השקילות של $a \in G$ בסימון $[a] = aH$. קיבלנו כי G היא איחוד זר של המחלקות האלו. נגדיר פונקציה $f_a: H \rightarrow aH$ לפי $f_a(h) = ah$ (הבינו שהיא מוגדרת היטב). אז נראה שהיא חח"ע ועל:

1. (חח"ע) אם $f_a(h_1) = f_a(h_2)$, אזי $ah_1 = ah_2$. מצמצום נקבל $h_1 = h_2$.

2. (על) יהי $x \in aH$. כלומר קיים $a \sim_l x$. לכן קיים $h \in H$ כך ש- $x = ah$. לכן $x = f_a(h)$.

לכן $|H| = |aH|$ לכל $a \in G$. מפני ש- G היא איחוד זר של מחלקות שכולן מאותו גודל, שהוא $|H|$, נסיק $|G| = |H|$. \square

הגדרה 0.3. תהי G חבורה, ותהי $H \leq G$ תת-חבורה, ויהי $a \in G$. אז נגדיר:

• המחלקה השמאלית של H ב- G לגבי a להיות מחלקת השקילות תחת היחס \sim_l :

$$aH = \{ah \mid h \in H\} \subseteq G$$

• המחלקה הימנית של H ב- G לגבי a להיות מחלקת השקילות תחת היחס \sim_r :

$$Ha = \{ha \mid h \in H\} \subseteq G$$

• את אוסף המחלקות השמאליות של H ב- G מסמנים G/H , ואת מספר המחלקות השמאליות מסמנים $[G : H] = |G/H|$. המספר הזה נקרא האינדקס של H ב- G .

לעיתים רחוקות נסמן $H \setminus G$ להיות אוסף המחלקות הימניות של H ב- G .

הערה 0.4. כמה אבחנות לגבי מחלקות:

1. עבור $a = e$, נקבל $eH = H = He$. כלומר H היא תמיד מחלקה שמאלית וימנית.

2. כל שאר המחלקות (שאינן H) הן לא תת-חבורות של G .

3. לכל $a \in G$ מתקיים $|aH| = |H| = |Ha|$.

4. ניסוח אחר ליחס \sim_l אומר שמתקיים $aH = bH$ אם ורק אם $a \sim_l b$ אם ורק אם $b^{-1}a \in H$. בפרט $aH = H$ אם ורק אם $a \in H$.

5. מתקיים $|G/H| = |H \setminus G|$. הסיבה היא שיש התאמה חח"ע ועל בין הקבוצות האלו לפי

$$Ha \mapsto a^{-1}H$$

כדי לראות שזה מוגדר היטב, שימו לב שאם $Ha = Hb$, אז צריך להראות $a^{-1}H = b^{-1}H$. מפני ש- $a \sim_r b$, קיים $h \in H$ כך ש- $a = hb$. לכן $b^{-1}a = b^{-1}hb = h$, ולכן $a^{-1} \sim_l b^{-1}$. בנוסף ההתאמה הזו הפיכה כי קיימת לה העתקה הופכית $H a^{-1} \leftarrow aH$.

מסקנה 0.5. תהי G חבורה כלשהי, ותהי $H \leq G$. מתקיים $|G| = [G : H] |H|$.
זה נכון בחשבון עוצמות, במקרה האינסופי זה שקול לאקסיומת הבחירה.

דוגמה 0.6. נבחר $G = \mathbb{Z}_8$, ונסתכל על $H = \langle 2 \rangle = \{0, 2, 4, 6\}$. אכן $|H| = 4 \mid 8 = |G|$.
המחלקות השמאליות הן

$$0 + H = H = \{0, 2, 4, 6\} = 2 + H = 4 + H = 6 + H$$

$$1 + H = \{1, 3, 5, 7\} = 3 + H = 5 + H = 7 + H$$

$$\text{מתקיים } |G| = 8 = 2 \cdot 4 = [G : H] |H|$$

דוגמה 0.7. ראינו $G \leq G$. מפני ש- G $y^{-1}x \in G$ לכל $x, y \in G$, אזי $x \sim_l y$. לכן יש רק מחלקה שמאלית אחת, והיא G . בסימונים שלנו $G/G = \{G\}$.

דוגמה 0.8. ראינו $\{e\} \leq G$. מתי $x \sim_l y$? אם ורק אם $y^{-1}x \in \{e\}$ אם ורק אם $y^{-1}x = e$. כלומר אם ורק אם $x = y$. לכן כל מחלקה שמאלית (וגם ימנית) היא יחידון מהצורה $\{x\}$. בסימונים שלנו $G/\{e\} = \{\{g\} \mid g \in G\}$.

דוגמה 0.9. נבחר $G = GL_n(\mathbb{R})$ ונבחר את $H = SL_n(\mathbb{R})$. נבדוק מתי $A \sim_l B$ עבור $A, B \in G$

$$B^{-1}A \in SL_n(\mathbb{R})$$

$$\det(B^{-1}A) = 1$$

$$\frac{\det(A)}{\det(B)} = 1$$

$$\det(A) = \det(B)$$

כלומר יש התאמה חח"ע ועל בין הדטרמיננטה לבין מחלקת השקילות. כלומר

$$\mathbb{R}^* \longleftrightarrow G/H = \{\{A \in GL_n(\mathbb{R}) \mid \det(A) = r\} \mid r \in \mathbb{R}^*\}$$

במקרה יצא שכל המחלקות הימניות שוות למחלקות השמאליות, למרות שהחבורות אינן אבליות.

דוגמה 0.10. תהי X קבוצה, ויהי $a \in X$. נבחר $G = S_X$ ואת $H = \text{stab}(a)$ שהוכחנו שהמייצב H הוא תת-חבורה. נבדוק מי הן המחלקות השמאליות ב- G/H : יהיו $\sigma, \tau \in S_X$. נרצה לבדוק מתי $\tau^{-1}\sigma \in H$.

$$\sigma \sim_l \tau \iff \tau^{-1}\sigma \in \text{stab}(a) \iff (\tau^{-1}\sigma)(a) = a \iff \tau^{-1}(\sigma(a)) = a \iff \sigma(a) = \tau(a)$$

כלומר $\sigma H = \tau H$ אם ורק אם σ, τ שולחות את a לאותו איבר של X (כלומר יש להן את אותה תמונה עבור a). יש התאמה חח"ע ועל בין

$$X \longleftrightarrow G/H$$

$$x \in X \mapsto \{\sigma \in S_X \mid \sigma(a) = x\}$$

תרגיל לבית: המחלקות הימניות הן שונות מהמחלקות השמאליות, אבל עדיין יש התאמה חח"ע ועל ל- X . רמז

$$X \longleftrightarrow G \setminus H$$

$$x \in X \mapsto \{\sigma \in S_X \mid \sigma(x) = a\}$$

מסקנה 0.11 (ממשפט לגראנז'). תהי G חבורה מסדר n . אז לכל $a \in G$ מתקיים $o(a) \mid n$.

הוכחה. ראינו כי $o(a) = |\langle a \rangle|$. לפי לגראנז' $|\langle a \rangle| \mid |G|$. סיימנו. \square

מסקנה 0.12. לכל $a \in G$ בחבורה סופית מתקיים $a^{|G|} = e$. (ראינו כי $a^k = e$ אם ורק אם $o(a) \mid k$).

טענה 0.13. יהי p מספר ראשוני, ותהי G חבורה מסדר p . אז G ציקלית, וכל איבריה הם יוצרים שלה, פרט ל- e .

הוכחה. נתון $|G| = p$. הסדר של כל איבר של G חייב לחלק את p . לכן האיברים הם מסדר 1 או p . האיבר היחיד מסדר 1 הוא איבר היחידה, וכל השאר הם מסדר p . לכן G ציקלית (כי היא סופית ויש לה איברים מהסדר שלה).

אגב, גם מצאנו מיון לתת-חבורות של G . יש רק את G ואת $\{e\}$, כי גם הסדר של תת-חבורה יכול להיות רק 1 או p . \square

0.2 היכרות עם מערכת הצפנה RSA

משפט 0.14 (משפט אוילר). לכל $a \in U_n$ מתקיים $a^{\varphi(n)} \equiv 1 \pmod{n}$.

הוכחה. זה מקרה פרטי של המסקנה ממשפט לגראנז' עבור $G = U_n$. הרי $|G| = \varphi(n)$. ראינו כי $a^{|G|} = e_G$. כלומר $a^{\varphi(n)} \equiv 1 \pmod{n}$. \square

דוגמה 0.15. יהי p מספר ראשוני. אז לכל $a \in U_p$ מתקיים $a^{p-1} \equiv 1 \pmod{p}$. כי $\varphi(p) = p - 1$. זה מוכר כמשפט פרמה הקטן. לפעמים רואים את זה בצורה $a^p \equiv a \pmod{p}$. לכל $a \in \mathbb{Z}_p$.

שימו לב למספרים פריקים לא תמיד מתקיים $a^{n-1} \equiv 1 \pmod{n}$. למשל עבור $n = 15$:

$$2^{14} \equiv 4 \not\equiv 1 \pmod{15}$$

טענה 0.16. יהיו p, q ראשוניים שונים, ונסמן $n = pq$. אז חישוב $\varphi(n)$ קשה כמו פירוק n לגורמים ראשוניים.

הוכחה. אם ידוע הפירוק $n = pq$, אז קל לחשב $\varphi(n) = \varphi(p)\varphi(q) = (p-1)(q-1)$. בכיוון השני, נניח ש- n ו- $\varphi(n)$ ידועים. אז

$$\varphi(n) = pq - p - q + 1 = (n + 1) - (p + q)$$

$$p + q = n + 1 - \varphi(n)$$

לכן p, q הם שורשים של הפולינום הריבועי

$$(x-p)(x-q) = x^2 - (p+q)x + pq = x^2 + (\varphi(n) - n - 1)x + n$$

אז מנוסחת השורשים זה מהיר לחשב

$$p, q = \frac{-(\varphi(n) - n - 1) \pm \sqrt{(\varphi(n) - n - 1)^2 - 4n}}{2}$$

כמו שרצינו.

ריבסט, שמיר ואדלמן מצאו שיטה להצפנה אסימטרית. אליס ובוב רוצים לשלוח הודעות מוצפנות זה לזה.

המטרה: בוב רוצה לשלוח לאליס הודעה באופן מוצפן.

יצירת מפתחות: אליס מגרילה שני ראשוניים גדולים p, q באקראי. היא מחשבת את $n = pq$ ואת $\varphi(n) = (p-1)(q-1)$. היא בוחרת מספר $e > 1$ שזר ל- $\varphi(n)$ שנקרא מעריך ההצפנה (בפועל $65537 + 1 = 2^{16} + 1$ או מספר קטן דומה). היא מוצאת הופכי כפלי d -ל- e בחבורה $U_{\varphi(n)}$. המספר d הוא המפתח הפרטי של אליס והמפתח הציבורי הוא (n, e) .

הפצת המפתח הציבורי: אליס שולחת באופן אמין לבוב (או לכל העולם) את המפתח הציבורי שלה, ושומרת בסוד אצלה את המפתח הפרטי.

הצפנה: בוב רוצה לשלוח לאליס הודעה בצורת מספר $0 < m < n$. אז הוא מצפין אותה בצורה

$$c \equiv m^e \pmod{n}$$

ושולח את c .

פענוח: אליס תפענח את ההודעה המוצפנת על ידי חישוב

$$c^d \equiv m^{ed} \equiv m \pmod{n}$$

הוכחת נכונות הפענוח: נעזרים באלגוריתם אוקלידס המורחב. לפי שלב יצירת המפתחות $de \equiv 1 \pmod{\varphi(n)}$. לכן קיים $k \in \mathbb{Z}$ כך ש- $de = k\varphi(n) + 1$. נחלק לשני מקרים:

• אם $\gcd(m, n) = 1$, אז $m^{\varphi(n)} \equiv 1 \pmod{n}$ לפי משפט אוילר. לכן

$$c^d \equiv m^{ed} \equiv m^{k\varphi(n)+1} \equiv m \pmod{n}$$

• אחרת, אם $\gcd(m, n) > 1$ (זה מקרה ממש נדיר הקורה בערך בהסתברות $\frac{1}{p} + \frac{1}{q} - \frac{1}{pq}$). לכן m הוא כפולה של p או של q , אבל לא של שניהם כי $m < n$. בלי הגבלת הכלליות, נניח $m = rp$ עבור $r \geq 0$. בפרט $\gcd(m, q) = 1$. לפי משפט פרמה הקטן $m^{q-1} \equiv 1 \pmod{q}$. נחשב

$$m^{k\varphi(n)} = (m^{\varphi(q)})^{\varphi(p)k} \equiv (m^{q-1})^{\varphi(p)k} \equiv 1 \pmod{q}$$

לכן קיים t כך ש- $m^{k\varphi(n)} = tq + 1$. בחישוב מודולו n נקבל

$$c^d \equiv m^{ed} \equiv m^{k\varphi(n)+1} \equiv (tq+1)m \equiv tqrp + m \equiv m \pmod{n}$$

□

הערה 0.17. עד n יש בערך $\frac{n}{\ln n}$ מספרים ראשוניים. אלגוריתמים לבדיקת ראשוניות כמו מילר-רבין או AKS.

0.3 הומומורפיזמים

הגדרה 0.18. תהינה $(G, *)$ ו- (H, \bullet) חבורות. העתקה $f: G \rightarrow H$ תקרא הומומורפיזם של חבורות אם היא שומרת על הפעולה. כלומר מתקיים

$$\forall x, y \in G, \quad f(x * y) = f(x) \bullet f(y)$$

אם בנוסף f היא חח"ע ועל, נאמר שהיא איזומורפיזם של חבורות. במקרה כזה נאמר כי G איזומורפית ל- H ונסמן $G \cong H$.

דוגמה 0.19. תהינה G, H חבורות. אז הפונקציה $f(g) = e_H$ לכל $g \in G$ היא ההומומורפיזם הטריוויאלי. קל לבדוק שזהו אכן הומומורפיזם:

$$\forall x, y \in G, \quad f(xy) = e_H = e_H e_H = f(x)f(y)$$

זהו איזומורפיזם אם ורק אם G ו- H שתיהן טריוויאליות.

דוגמה 0.20. תהי G חבורה, ותהי $H \leq G$. הפונקציה $f: H \rightarrow G$ המוגדרת לפי $f(h) = h$ נקראת השיכון של H ב- G . זהו הומומורפיזם. זהו איזומורפיזם רק אם $H = G$.

דוגמה 0.21. תהי G חבורה, ויהי $g \in G$ איבר קבוע. אז הפונקציה $f: \mathbb{Z} \rightarrow G$ המוגדרת לפי $f(n) = g^n$ הוא הומומורפיזם.

$$\forall n, m \in \mathbb{Z}, \quad f(n + m) = g^{n+m} = g^n g^m = f(n)f(m)$$

התמונה של f היא $\langle g \rangle$.

טענה 0.22 (תכונות). יהי $f: G \rightarrow H$ הומומורפיזם. אז

1. מתקיים $f(e_G) = e_H$ כי

$$f(e_G) = f(e_G * e_G) = f(e_G) \bullet f(e_G)$$

ועל ידי צמצום של $f(e_G)$ בחבורה H נקבל $f(e_G) = e_H$.

2. בעזרת אינדוקציה נקבל $f(g^n) = f(g)^n$ לכל $n \in \mathbb{N}$.

3. מתקיים $f(g^{-1}) = f(g)^{-1}$ כי

$$f(g^{-1}) \bullet f(g) = f(g^{-1} * g) = f(e_G) = e_H$$

ועל ידי כפל ב- $f(g)^{-1}$ מימין בחבורה H ולקבל את הדרוש. באינדוקציה וכמסקנה לתכונה הקודמת נקבל $f(g^n) = f(g)^n$ לכל $n \in \mathbb{Z}$.

4. אם f היא איזומורפיזם, אז הפיכה. הפונקציה ההופכית $f^{-1}: H \rightarrow G$ גם היא איזומורפיזם. בהנתן $w, z \in H$, נבדוק עבור $f^{-1}(w), f^{-1}(z) \in G$ מה קורה כשנפעיל את f :

$$f(f^{-1}(w) * f^{-1}(z)) = f(f^{-1}(w)) \bullet f(f^{-1}(z)) = w \bullet z$$

ומפני ש- f היא חח"ע, נקבל $f^{-1}(w \bullet z) = f^{-1}(w) * f^{-1}(z)$.

5. אם $G \cong H$, אז $|G| = |H|$.

דוגמה 0.23. קבוצת שורשי היחידה המרוכבים מסדר n היא

$$\Omega_n = \{z \in \mathbb{C} \mid z^n = 1\} = \left\{ \operatorname{cis} \frac{2\pi k}{n} = e^{\frac{2\pi i k}{n}} \mid k = 0, 1, \dots, n-1 \right\}$$

נסמן $\omega_n = e^{\frac{2\pi i}{n}}$. אז $\Omega_n = \langle \omega_n \rangle \leq \mathbb{C}^*$. נוכיח כי \mathbb{Z}_n (עם פעולת חיבור מודולו n) איזומורפית ל- Ω_n (עם פעולת הכפל). נגדיר פונקציה $f: \mathbb{Z}_n \rightarrow \Omega_n$ לפי הקביעה $f(1) = \omega_n$. כדי שבאמת יהיה מדובר בהומומורפיזם, צריך לבדוק כי

$$f(k) = f(1^k) = f(1 + \dots + 1) = f(1)^k = \omega_n^k = e^{\frac{2\pi i k}{n}}$$

ולכן זו פונקציה חח"ע ועל. נותר להוכיח שהיא הומומורפיזם

$$f(k+r) = \omega_n^{k+r} = \omega_n^k \omega_n^r = f(k)f(r)$$

ומכאן שהוכחנו כי $\mathbb{Z}_n \cong \Omega_n$.

טענה 0.24. תהינה G, H חבורות ציקליות סופיות. אז $G \cong H$ אם ורק אם $|G| = |H|$.

הוכחה. כיוון אחד קל לפי התכונות: נניח $|G| \neq |H|$, אז הן לא איזומורפיות כי לא תתכן פונקציה חח"ע ועל ביניהן. בכיוון השני, נניח $|G| = |H|$. יהי g יוצר של G ויהי h יוצר של H . נגדיר פונקציה מפורשת $f: G \rightarrow H$ לפי $f(g^k) = h^k$. בודקים שזהו הומומורפיזם שהוא חח"ע ועל, ומסיימים. \square

מסקנה 0.25. אנחנו מכירים חבורה ציקלית מכל סדר טבעי n , והיא \mathbb{Z}_n . לכן כל חבורה ציקלית מסדר n איזומורפית אליה. כל חבורה ציקלית אינסופית איזומורפית ל- \mathbb{Z} . כלומר יש רק חבורה ציקלית אחת מכל סדר, עד כדי איזומורפיזם.

דוגמה 0.26. נתבונן בחבורות $G = (\mathbb{R}, +)$ ו- $H = (\mathbb{R}_+, \cdot)$. נגדיר העתקה $f: G \rightarrow H$ לפי $f(x) = e^x$. אז f חח"ע (כי e^x היא מונוטונית עולה בממשיים החיוביים) וגם על (כי הטווח שלה הוא בדיוק $(0, \infty)$), ושומרת על הפעולה:

$$f(x+y) = e^{x+y} = e^x e^y = f(x)f(y)$$

לכן $G \cong H$.

דוגמה 0.27. החבורות \mathbb{Z} -ו- \mathbb{Q} אינן איזומורפיות. כי \mathbb{Z} ציקלית ואילו \mathbb{Q} אינה ציקלית.

הגדרה 0.28. הומומורפיזם שהוא חח"ע נקרא מונומורפיזם או שיכון. נאמר כי G משוכנת ב- H אם קיים שיכון $f: G \hookrightarrow H$.
 הומומורפיזם שהוא על נקרא אפימורפיזם. נאמר כי H היא תמונה אפימורפית של G אם קיים אפימורפיזם $f: G \twoheadrightarrow H$.

דוגמה 0.29. בתרגול תראו כי $\det: GL_n(F) \rightarrow F^*$ היא אפימורפיזם, אם $n = 1$ אז אפילו איזומורפיזם. בכיוון ההפוך, הפונקציה $f: F \rightarrow SL_n(F)$ המוגדרת לפי

$$f(\alpha) = \begin{pmatrix} 1 & 0 & \cdots & 0 & \alpha \\ & \ddots & & & 0 \\ & & \ddots & & \vdots \\ & & & \ddots & 0 \\ & & & & 1 \end{pmatrix}$$

היא מונומורפיזם. קצת יותר מתוחכם זה להראות כי $\varphi: \mathbb{R} \rightarrow GL_2(\mathbb{R})$ המוגדרת לפי

$$\varphi(\alpha) = \begin{pmatrix} \cos \alpha & -\sin \alpha \\ \sin \alpha & \cos \alpha \end{pmatrix}$$

היא הומומורפיזם. אכן,

$$\begin{aligned} \varphi(\alpha)\varphi(\beta) &= \begin{pmatrix} \cos \alpha & -\sin \alpha \\ \sin \alpha & \cos \alpha \end{pmatrix} \begin{pmatrix} \cos \beta & -\sin \beta \\ \sin \beta & \cos \beta \end{pmatrix} \\ &= \begin{pmatrix} \cos \alpha \cos \beta - \sin \alpha \sin \beta & -\cos \alpha \sin \beta - \sin \alpha \cos \beta \\ \cos \alpha \sin \beta + \sin \alpha \cos \beta & \cos \alpha \cos \beta - \sin \alpha \sin \beta \end{pmatrix} \\ &= \begin{pmatrix} \cos(\alpha + \beta) & -\sin(\alpha + \beta) \\ \sin(\alpha + \beta) & \cos(\alpha + \beta) \end{pmatrix} = \varphi(\alpha + \beta) \end{aligned}$$

אבל ברור שזהו לא אפימורפיזם, למשל כי באלכסון יש איברים זהים. היא גם לא מונומורפיזם, כי $\varphi(\alpha) = \varphi(\alpha + 2\pi)$ לכל α .

הערה 0.30. יש קשר לבעיית תת-החבורה החבויה. נתונה חבורה G , תת-חבורה $H \leq G$ וקבוצה X . נאמר שפונקציה $f: G \rightarrow X$ מחזיאה את H אם היא קבועה על מחלקות שמאליות של H . כלומר לכל $g_1, g_2 \in G$ מתקיים $f(g_1) = f(g_2)$ אם ורק אם $g_1 H = g_2 H$.

אלגוריתם שור לפירוק מספרים בחישוב קוונטי, למעשה פותר את שאלת תת-החבורה החבויה במקרה של חבורות אבליות סופיות.

0.4 מבוא מהיר לפעולות של חבורות על קבוצות

צריך להבדיל בין פעולה של חבורה (באנגלית operation), לבין פעולה של חבורה על קבוצה (action). אם $G = F$ שדה כלשהו ו- $X = V$ היא קבוצה של הוקטורים של מרחב וקטורי מעל F , אז כפל בסקלר מגדיר פעולה של חבורה על קבוצה.

הגדרה 0.31. פעולה של חבורה (G, \cdot) על קבוצה X היא פעולה בינארית $G \times X \rightarrow X$ שנסמנה $(g, x) \mapsto g * x$ המקיימת:

$$1. \quad (gh) * x = g * (h * x) \quad \text{לכל } g, h \in G \text{ ו-} x \in X.$$

$$2. \quad e * x = x \quad \text{לכל } x \in X.$$

הגדרה 0.32 (הגדרה שקולה). פעולה של חבורה G על קבוצה X היא הומומורפיזם $\varphi: G \rightarrow S_X$. כלומר לכל $g \in G$ מתאימים פונקציה $\varphi(g): X \rightarrow X$ שהיא חח"ע ועל, ולפונקציות האלו מתקיים $\varphi(g_1 g_2) = \varphi(g_1) \circ \varphi(g_2)$.

יש המון דוגמאות מעניינות, אבל כל זה בהרצאה הבאה.