

תזכורת: בסוף התרגול הקודם הגדרנו מה זה חבורה נוצרת סופית. אם G היא חבורה ו x_1, \dots, x_n איברים ב G , אז החבורה שנוצרת על ידם מסומנת ב

$$\langle x_1, \dots, x_n \rangle$$

והיא שווה לחיתוך של כל תתי החבורות שמכילות אותם. למעשה האיברים ב $\langle x_1, \dots, x_n \rangle$ הם כל ה"מילים" שאפשר לכתוב עם x_1, \dots, x_n וההופכיים שלהם, (כמובן תוך התחשבות בלוח הכפל).

G נקראת "נוצרת סופית" אם יש קבוצה סופית של איברים $x_1, \dots, x_n \in G$, כך ש

$$G = \langle x_1, \dots, x_n \rangle$$

הבאנו את הדוגמאות הבאות:

1. $\mathbb{Z} \times \mathbb{Z}$ נוצרת סופית.

2. Ω_∞ לא נוצרת סופית.

תרגיל: האם $(\mathbb{R}, +)$ נוצרת סופית?

פתרון: למעשה נגיד משהו יותר כללי.

חבורה נוצרת סופית היא בהכרח בת מניה.

הסבר: האיברים בחבורה הם מילים ב x_1, \dots, x_n וההופכיים שלהם, באורך סופי.

אז מכל אורך מספר המילים האפשרי הוא סופי.

יש כל אורך אפשרי, לכן זה איחוד בן מניה של קבוצות סופיות, אז הוא בן מניה.

(שימו לב שזה לא איחוד זר, כי יכול להיות מילים שונות ששוות בחבורה לאותו איבר).

לכן עוצמת החבורה קטנה שווה מעוצמת האיחוד.

תרגיל: האם $(\mathbb{Q} \setminus \{0\}, \cdot)$ נוצרת סופית?

פתרון: נקח קבוצה סופית ונוכיח שהיא לא יוצרת את כל \mathbb{Q} .

$$\frac{x_1}{y_1}, \dots, \frac{x_n}{y_n}$$

נציג את כל השברים בצורה מצומצמת.

לכל אחד מהמספרים $x_1, \dots, x_n, y_1, \dots, y_n$ יש פירוק יחיד למספר סופי של גורמים ראשוניים.

אם נאחד את כל הראשוניים שמופיעים באיזשהו פירוק נקבל קבוצה סופית של ראשוניים, P .

האיברים בחבורה שנוצרת ע"י $\frac{x_1}{y_1}, \dots, \frac{x_n}{y_n}$ הם מכפלות של $\frac{x_1}{y_1}, \dots, \frac{x_n}{y_n}$ ושל ההופכיים שלהם.

ולכן אפשר להגיע רק לשברים שהמונה והמכנה שלהם מורכב מהגורמים הראשוניים בקבוצה P .

נקח ראשוני $p \notin P$, אז $\frac{p}{1}$ לא נמצא בתת חבורה שנוצרת ע"י

$$\frac{x_1}{y_1}, \dots, \frac{x_n}{y_n}$$

תרגיל: הוכיחו שבחבורה $(\mathbb{Q}, +)$ כל תת חבורה נוצרת סופית היא ציקלית.

פתרון:

$$\langle \frac{1}{2}, \frac{1}{3} \rangle = \langle \frac{1}{6} \rangle$$

$$\frac{1}{2} \in \langle \frac{1}{6} \rangle$$

$$\frac{1}{2} = \frac{1}{6} + \frac{1}{6} + \frac{1}{6}$$

$$\frac{1}{3} \in \langle \frac{1}{6} \rangle$$

$$\frac{1}{3} = \frac{1}{6} + \frac{1}{6}$$

ולכן

$$\langle \frac{1}{2}, \frac{1}{3} \rangle \subseteq \langle \frac{1}{6} \rangle$$

$$\frac{1}{6} = \frac{1}{2} - \frac{1}{3}$$

ולכן

$$\frac{1}{6} \in \langle \frac{1}{2}, \frac{1}{3} \rangle$$

ולכן

$$\langle \frac{1}{2}, \frac{1}{3} \rangle \supseteq \langle \frac{1}{6} \rangle$$

$$\frac{x_1}{y_1}, \frac{x_2}{y_2}$$

$$\frac{\gcd(x_1, x_2)}{\text{lcm}(y_1, y_2)}$$

$$\frac{2}{35}, \frac{4}{21}$$

$$\frac{2}{105}$$

$$\frac{6}{105}, \frac{20}{105}$$

ראשית, נוכיח שתת חבורה שנוצרת ע"י 2 איברים היא ציקלית.

$$\langle \frac{x_1}{y_1}, \frac{x_2}{y_2} \rangle$$

האיברים בחבורה הזאת הם מהצורה הבאה :

$$m \frac{x_1}{y_1} + n \frac{x_2}{y_2}$$

כאשר $m, n \in \mathbb{Z}$

$$= \frac{mx_1y_2 + nx_2y_1}{y_1y_2}$$

למעשה במונה יש צירוף לינארי כלשהו של המספרים x_1y_2 ו x_2y_1 .
הצירוף הלינארי הכי קטן הוא $\gcd(x_1y_2, x_2y_1)$. לכן

$$\frac{\gcd(x_1y_2, x_2y_1)}{y_1y_2} \in \left\langle \frac{x_1}{y_1}, \frac{x_2}{y_2} \right\rangle$$

מצד שני,

$$x_1y_2 = \gcd(x_1y_2, x_2y_1) \cdot k_1$$

$$\frac{x_1}{y_1} = k_1 \frac{\gcd(x_1y_2, x_2y_1)}{y_1y_2}$$

ובאותו אופן

$$x_2y_1 = \gcd(x_1y_2, x_2y_1) \cdot k_2$$

$$\frac{x_2}{y_2} = k_2 \frac{\gcd(x_1y_2, x_2y_1)}{y_1y_2}$$

אז קיבלנו

$$\left\langle \frac{x_1}{y_1}, \frac{x_2}{y_2} \right\rangle = \left\langle \frac{\gcd(x_1y_2, x_2y_1)}{y_1y_2} \right\rangle$$

נוכיח שתת חבורה שנוצרת ע"י n איברים נוצרת ע"י איבר אחד, באינדוקציה :
נניח שהטענה נכונה ל n . נוכיח ל $n + 1$. אז יש לנו תת חבורה שנוצרת ע"י $n + 1$ איברים :

$$\left\langle \frac{x_1}{y_1}, \dots, \frac{x_n}{y_n}, \frac{x_{n+1}}{y_{n+1}} \right\rangle$$

לפי הנחת האינדוקציה, כל מה שנוצר ע"י n האיברים הראשונים שקול למה שנוצר ע"י איזשהו

$$\frac{x}{y}$$

איבר יחיד $\frac{x}{y}$.
כלומר התת חבורה נוצרת ע"י

$$\left\langle \frac{x}{y}, \frac{x_{n+1}}{y_{n+1}} \right\rangle$$

ראינו שכל תת חבורה שנוצרת ע"י שני איברים היא ציקלית.

חבורות דיהדרליות

נציג את D_3 :

$$e, \tau, \sigma : \tau^2 = e, \sigma^3 = e, \tau\sigma = \sigma^{-1}\tau$$

$$\sigma^{-1} = \sigma^2$$

$$\sigma\tau, \tau\sigma^2$$

האם הם איברים שונים:

$$\tau\sigma^2 = (\tau\sigma)\sigma = (\sigma^{-1}\tau)\sigma = \sigma^{-1}(\tau\sigma) = \sigma^{-1}\sigma^{-1}\tau = \sigma\tau$$

איברי החבורה הם:

$$\{e, \sigma, \sigma^2, \tau, \tau\sigma, \tau\sigma^2\}$$

נחשב כמה כפולות:

$$(\tau\sigma)\tau = (\sigma^{-1}\tau)\tau = \sigma^{-1} = \sigma^2$$

$$(\tau\sigma^2)(\tau\sigma^2) = (\sigma\tau)(\sigma\tau) = \sigma(\tau\sigma\tau) = \sigma\sigma^2 = e$$

הכללה:

D_n היא חבורת הסיבובים והשיקופים על מצולע משוכלל עם n צלעות.

$$\sigma, \tau, \sigma^n = e, \tau^2 = e, \tau\sigma = \sigma^{-1}\tau$$

$$D_n = \{e, \sigma, \dots, \sigma^{n-1}, \tau, \tau\sigma, \dots, \tau\sigma^{n-1}\}$$

ב D_n יש תמיד $2n$ איברים. והיא לא אבלית לכל $n \geq 3$.
טענה: ב D_n תמיד מתקיים:

$$\tau\sigma^k = \sigma^{-k}\tau$$

הסבר: כל פעם נחליף σ אחת עם τ והיא תהפוך ל- σ^{-1}

$$(\tau\sigma)\sigma^{k-1} = \sigma^{-1}(\tau\sigma^{k-1}) = \sigma^{-1}\sigma^{-(k-1)}\tau = \sigma^{-k}\tau$$

למעשה:

$$\sigma^{-k} = \sigma^{n-k}$$

הסבר:

$$(\sigma^k)(\sigma^{n-k}) = \sigma^n = e$$

הומומורפיזמים

תיזכורת: יהיו G, H חבורות. פונקציה

$$f: G \rightarrow H$$

נקראת הומומורפיזם אם לכל $x, y \in G$

$$f(xy) = f(x)f(y)$$

אם f על-אפימורפיזם
 אם f חח"ע-מונומורפיזם
 אם f חח"ע ועל-איזומורפיזם
 תכונות:

$$1. f(e_G) = e_H$$

$$2. f(g^n) = f(g)^n$$

$$3. f(g^{-1}) = (f(g))^{-1}$$

שאלה: מה הקשר בין $o(g)$ ל- $o(f(g))$?
 תשובה:

$$o(f(g)) | o(g)$$

הוכחה: נסמן $n = o(g)$. אז

$$e = f(e) = f(g^n) = (f(g))^n$$

ולכן

$$o(f(g)) | n$$

טענה: אם f מונומורפיזם אז $o(f(g)) = o(g)$.
הוכחה: נסמן $n = o(f(g))$

$$f(g^n) = (f(g))^n = e$$

בגלל ש f חח"ע, האיבר היחיד שנשלח ל e , זה e בעצמו. לכן $g^n = e$.
ולכן $n | o(g)$

$$\mathbb{Z} \rightarrow \mathbb{Z}_n \times \mathbb{Z}_m$$

כאשר n, m זרים

$$f(x) = (x \bmod n, x \bmod m)$$

חשבו גרעין ותמונה.
גרעין:

$$x \in \ker f \iff x \bmod n = 0 \wedge x \bmod m = 0$$

$$\iff n|x \wedge m|x \iff \text{lcm}(m, n)|x \iff mn|x$$

כלומר

$$\ker f = mn\mathbb{Z}$$

ממשפט השאריות הסיני f על.