הגדרה: תהי G חבורה ו$x_1, ..., x_n \in G$. התת חבורה שנוצרת ע"י האיברים

$$\langle x_1, ..., x_n \rangle = \bigcap_{\{x_1,...,x_n\} \subseteq H \leq G} H$$

בניה מפורשת: זה בעצם כל ה"מילים" שאפשר ליצור ב$x_1, ..., x_n$ ובהופכיים.
למשל:

$$x_1 x_1 x_1 x_2^{-1} x_4 (x_3)^{-1} (x_3)^{-1}$$

שימו לב שיכול להיות שיש "מילים" שנכתבות שונה, אבל הן בעצם אותו איבר בחבורה (משתמשים בכללי הכפל).
למשל, אם החבורה אבלית אז

$$x_1 x_2 = x_2 x_1$$

הגדרה: חבורה G נקראת "נוצרת סופית" אם יש

$$x_1, ..., x_n \in G$$

כך ש:

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

לדוגמא:
1. כל חבורה סופית היא נוצרת סופית (ע"י כל איברי החבורה).
2. כל חבורה ציקלית היא נוצרת סופית.
3. $\mathbb{Z} \times \mathbb{Z}$ נוצרת ע"י $(1,0), (0,1)$.

$$(n, m) = n(1,0) + m(0,1)$$

אפשר ליצור את $\mathbb{Z} \times \mathbb{Z}$ ע"י איברים נוספית, למשל: $(1,0), (1,1)$
תזכורת: בשיעור הקודם הגדרנו את חבורת שורשי היחידה, $\Omega_\infty = \{x \in \mathbb{C}. \exists n : x^n = 1\}$
תרגיל: הוכיחו שΩ_∞ אינה נוצרת סופית.
הוכחה: נניח בשלילה שיש קבוצה סופית $x_1, ..., x_n$ שיוצרת את Ω_∞. נקח את המכפלה של כל סידרי האיברים. נקרא לה m. כלומר, לכל i, $x_i^m = 1$. מכיוון שהחבורה אבלית, וכן סדר של איבר שווה לסדר של ההופכי, אז כל איבר בתת חבורה שנוצרת על ידיהם, הסדר שלו קטן שווה מm.
בΩ_∞ יש איבר מכל סדר, אז ניתן לבחור איבר מסדר יותר גבוה מm, הוא לא נמצא בתת החבורה שנוצרת ע"י האיברים האלו.
הערה: חבורה נוצרת סופית היא בת מניה (לכל היותר $\aleph_0$).
תרגיל: האם $(\mathbb{Q} \setminus \{0\}, \cdot)$ נוצרת סופית?

פתרון: לא. נניח בשלילה שיש

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

כל אחד מx_i וy_i הוא מכפלה של מס' סופי של ראשוניים.
כל איבר שאפשר ליצור על ידם הוא מכפלה של עליהם ושל ההופכיים, ולכן המונה והמכנה שלו יהיו כפולות של $x_1, ..., x_1, y_1, ..., y_n$ ולכן של הגורמים הראשוניים שלהם.
יש אינסוף ראשוניים, אז נקח ראשוני שלא מופיע בפירוק, p, הוא לא מופיע בתת החבורה הנוצרת על ידם.
תרגיל: הוכיחו שכל תת חבורה נוצרת סופית של $\langle \mathbb{Q}, + \rangle$ היא ציקלית.
הוכחה: נסתכל על

$$\langle \frac{x_1}{y_1}, ..., \frac{x_n}{y_n} \rangle$$

$$\frac{2}{15}, \frac{3}{20}$$

$$\frac{3}{20} - \frac{2}{15} = \frac{1}{60}$$

$$m\frac{x_1y_2}{y_1y_2} + l\frac{x_2y_1}{y_2y_1} = \frac{m(x_1y_2) + l(x_2y_1)}{y_1y_2} = \frac{k \cdot gcd(x_1y_2, x_2y_1)}{y_1y_2}$$

כי ידוע שהצירופים הלינאריים של שני מספרים זה כל הכפולות של הgcd שלהם.
נוכיח את הטענה באינדוקציה.
נראה שאם התת חבורה נוצרת ע"י n איברים, אז היא ציקלית.
בסיס: $n = 1$- ברור.
נניח שהטענה ידועה לn, ונוכיח ל$n + 1$.

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

כל צירוף של שני האיברים האחרונים, הוא צירוף

$$\frac{gcd(x_ny_{n+1,}y_nx_{n+1})}{y_ny_{n+1}}$$

ולכן אפשר להחליף את שניהם באיבר היחיד הזה.
קיבלנו שהתת חבורה נוצרת ע"י n איברים, מהנחת האינדוקציה היא ציקלית.

חבורה דיהדרלית

מסמנים בD_3 את החבורה הבאה:

יהיו σ, τ שני איברים שמקיימים את היחסים הבאים:

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

$$\sigma/\tau\sigma = \sigma^{-1}\tau/\sigma^{-1}$$

$$\sigma\tau = \tau\sigma^2$$

D_3 היא כל מה שאפשר ליצור ע"י שני האיברים והתכונות שציינו.

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

מי ההופכי של $\tau\sigma$?

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

באותו אופן

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

$$(\tau\sigma)(\tau\sigma^2) = \tau(\sigma\tau)\sigma^2 = \tau(\tau\sigma^2)\sigma^2 = \sigma^4 = \sigma$$

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

ראינו שD_3 הוא אוסף הסיבובים והשיקופים על משולש משוכלל.
הכללה: D_n הוא אוסף השיקופים והסיבובים על מצולע משוכלל עם n צלעות. נוצר ע"י:

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

האיברים הם:

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

בD_n יש $2n$ איברים.
וD_n תמיד לא אבלית ($n \geq 3$)
טענה: לכל n ולכל $k < n$, בחבורה D_n מתקיים:

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

הוכחה:

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

נוכיח ש

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

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

הומומורפיזמים

הגדרה:

$$f : G \to H$$

נקראת הומומורפיזם אם לכל $x, y \in G$

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

אפימורפיזם: הומומורפיזם על.
מונומורפיזם: הומומורפיזם חח"ע.
איזומורפיזם: הומומורפיזם חח"ע ועל.
דוגמאות:
1.

$$f : \Omega_n \to {}_n$$

$$f(cis(\frac{2\pi k}{n})) = k$$

$$f(cis(\frac{2\pi k}{n})cis(\frac{2\pi m}{n})) = f(cis(\frac{2\pi(k+m)}{n})) = k+m = f(cis(\frac{2\pi k}{n}))+cis(\frac{2\pi m}{n})$$

שימו לב שהפעולה אכן מוגדרת מודולו n.

על: המקור של k הוא $cis(\frac{2\pi k}{n})$. וזה קבוצות סופיות עם אותו מספר איברים, אז פונקציה על היא חח"ע.

2.

$$f : GL_n(\mathbb{F}) \to \mathbb{F} \setminus \{0\}$$

$$f(A) = |A|$$

ידוע שהפוקנציה כיפלית. זה אפימורפיזם, כי ניתן לראות שהיא על.

3.

$$f : GL_n(\mathbb{F}) \to \mathbb{F} \setminus \{0\}$$

$$f(A) = tr(A)$$

בכלל לא מוגדרת, כי יש מטריצות הפיכות עם טרייס 0.

4.

$$f : GL_n(\mathbb{F}) \to (\mathbb{F}, +)$$

$$f(A) = tr(A)$$

לא הומומורפיזם, כי

$$tr(AB) \neq tr(A) + tr(B)$$

5.

$$f : M_n(\mathbb{F}), + \to \mathbb{F}, +$$

$$f(A) = tr(A)$$

אפימורפיזם, למשל

$$\begin{pmatrix} x & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

מקור של x. ניתן לראות שהיא לא חח"ע.

תכונות:

1. $f(e_G) = e_H$
2. $f(g^n) = (f(g))^n$
3. $f(g)^{-1} = f(g^{-1})$

תרגיל: מה הקשר בין הסדר של g לסדר של $f(g)$?

פתרון: נסמן $o(g) = n, o(f(g)) = m$.

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

לכן $m|n$.
אי אפשר להשיג יותר מזה.
תרגיל המשך: אם f מונומורפיזם, אז $o(g) = o(f(g))$
כיוון אחד ראינו.
עכשיו

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

מכיוון שהפונקציה חח"ע, ומתכונה 1 ידוע שe נשלח לe, אז אם g^m נשלח לe, הוא חייב להיות שווה לe. לכן $g^m = e$. לכן $n|m$.
הגדרה: הגרעין של הומומורפיזם:

$$\ker f = \{g \in G : f(g) = e\}$$

תרגיל: הוכיחו שגרעין של הומומורפיזם הוא תת חבורה.
הוכחה:
1. איבר יחידה: $f(e) = e$ מתכונה 1, לכן $e \in \ker f$.
2. סגירות לפעולה: נניח ש$g, h \in \ker$, אז

$$f(gh) = f(g)f(h) = e \cdot e = e$$

לכן $gh \in \ker$
3. סגירות להופכי: נניח ש$g \in \ker$, אז:

$$f(g^{-1}) = f(g)^{-1} = e^{-1} = e$$

לכן $g^{-1} \in \ker$.
הגדרה:

$$Im(f) = \{h \in H : \exists g \in G, f(g) = h\}$$