

הרצאה 4

סדר של איבר ושל חבורה

הגדרה

• סדר של חבורה הוא מס' האיברים בה.
• סדר של איבר g בחבורה הוא

$$o(g) = \begin{cases} \min\{k \in \mathbb{N} : g^k = 0\} \\ \infty \text{ if there is no such } k \end{cases}$$

דוגמא

$$o(9) = 2, o(3) = 4 \text{ מתקיים } U_{10} = \{1, 3, 7, 9\}$$

$$o(1) = \infty \text{ מתקיים } (\mathbb{Z}, +)$$

טענה

$$a^k = e \Leftrightarrow o(a) | k$$

הוכחה

בכיוון ראשון

$$o(a) | k \Rightarrow \exists q \in \mathbb{Z} : k = o(a) * q \Rightarrow a^k = (a^{o(a)})^q = e^q = e$$

בכיוון הנגדי

$$a^k = e \Rightarrow o(a) < k$$

נתייחס לפירוק מקסימלי: $0 \leq r < o(a), k = o(a) * q + r$

$$e = a^k = (a^{o(a)})^q a^r \Rightarrow a^r = e$$

אבל בהתאם למינימליות e של הסדר $o(a)$, ולכן $r=0$, ולכן $k=o(a)q$

הערה

תמונה הומומורפית של חבורה צקלית היא חבורה צקלית.

$$f: \overset{=<a>}{\vec{G}} \rightarrow H \Rightarrow H = \langle f(a) \rangle$$

הוכחה

$$\forall G \in G : g = a^i \rightarrow f(a)^i \Rightarrow \text{Im}(f) = H = \langle f(a) \rangle$$

משפט

$$\forall n, m \in \mathbb{Z} : (n, m) = 1 \Leftrightarrow \mathbb{Z}_n \times \mathbb{Z}_m \cong \mathbb{Z}_{nm}$$

הוכחה

← הוכחנו באמצעות CRT.

⇒

$$\mathbb{Z}_n \times \mathbb{Z}_m \cong \mathbb{Z}_{nm} = \langle i \rangle \Rightarrow \exists (a, b) \in \mathbb{Z}_n \times \mathbb{Z}_m : o(a, b) = nm$$

$$\Rightarrow (a, b)^{[n, m]} = ([n, m]a, [n, m]b) = (nq_1a, mq_2b) = (0, 0)$$

$$o(a, b) = nm \leq [n, m] \Rightarrow nm = [n, m] \Leftrightarrow (n, m) = 1$$

מיון חבורת ציקליות

משפט

תהא $G = \langle a \rangle$ חבורה ציקלית, אזי :

- א. אם $G \cong \mathbb{Z}$ אינסופית, אזי $G \cong \mathbb{Z}$
- ב. אם G מסדר n , אזי $G \cong \mathbb{Z}_n$

הוכחה

א. נגדיר $f: \mathbb{Z} \rightarrow G : k \mapsto a^k$

$$f(m+n) = a^{m+n} = a^m a^n = f(m)f(n)$$

לכן f הומו' (משמר פעולה).

כיוון שניתן להגיע לכל חזקה שלמה של a , $Im(f) = \langle a \rangle = G$, כלומר f אפי' (על). בנוסף אם $m \neq n$ אז בהכרח $a^m \neq a^n$ שכן אחרת G הייתה סופית (חזקות חוזרות על עצמן נכנסים ללולאה סופית) בסתירה לנתון, מכאן f מונו' ובסה"כ איזו'.

ב. שוב נגדיר את ההעתקה $f: \mathbb{Z}_n \rightarrow G : k \mapsto a^k$

שימור פעולה: $\forall k_1, k_2 \in \mathbb{Z}_n : k_1 \oplus k_2 = k_1 + k_2 - \alpha n$

$$f(k_1 \oplus k_2) = a^{k_1 \oplus k_2} = a^{k_1 + k_2 - \alpha n} = a^{k_1} a^{k_2} (a^{-\alpha n}) = a^{k_1} a^{k_2} = f(k_1)f(k_2)$$

כיוון שכל חזקה $0 \leq k \leq n-1$ מתאפשרת בתמונה, כלומר כל G נפרשת, כלומר f על, ומתוך כך f הוא מונו' (כי $|\mathbb{Z}_n| = |G| = n$).

דוגמא

$$\mathbb{Z} \cong \langle 1+i \rangle \leq \mathbb{C}$$

$$|1+i| \neq 1$$

חבורה ציקלית אינסופית.

באופן כללי, החבורה $G = \langle z = re^{i\theta} \in \mathbb{C} \rangle$ לגבי כפל סופית אם $r=1, \frac{\theta}{\pi} \in \mathbb{Q}$

$$\frac{\theta}{\pi} \in \mathbb{Q} \Leftrightarrow \theta k \in 2\pi\mathbb{Z} \Leftrightarrow (cis(\theta))^k = cis(k\theta) = 1$$

מיון תת-חבורות של חבורה צקלית

טענה

צקליות היא תכונה תורשתית, כלומר אם G צקלית אזי כל ת"ח $H \leq G$ צקלית

הוכחה

בהינתן $G = \langle a \rangle$, צ"ל $H = \langle a^k \rangle$, $\exists k \in \mathbb{N}$

אם $H = \{e\}$ אזי $H = \langle e \rangle$

אחרת נגדיר $k := \min\{i \in \mathbb{N} : a^i \in H\}$ ונראה כי $H = \langle a^k \rangle$

אכן יהא $a^t \in H$ ונתייחס לפרוק $t = kq + r$ כאשר $0 \leq r < k$. ע"פ הסגירות נקבל $a^r = a^{t-kq} \in H$
אבל $r < k$, בסתירה למנמליות, ולכן $r=0$, ולכן $t = kg$ ולכן $a^t \in \langle a^k \rangle$

טענה 1

תהא חבורה G ואיבר $a \in G$ כך ש $o(a) = n$, אזי :

$$\forall d \leq n : o(a^d) = \frac{n}{(d,n)}$$

דוגמא

$$1 \in \mathbb{Z}_6, o(1^d) = o(d) = \frac{6}{(d,6)}$$

הוכחה

1. התיכנות $(a^d)^{\frac{n}{(d,n)}} = (a^n)^{\frac{d}{(d,n)}} = e$

2. מינימליות : נניח כי $(a^d)^t = e$ אזי $a^{dt} = e$. ידוע כי $o(a) = n$ ולכן $n | dt$ מכאן שגם:

$$t \geq \frac{n}{(d,n)} \mid \frac{dt}{(d,n)} \text{ אבל } \left(\frac{n}{(d,n)} \mid \frac{d}{(d,n)} \right) \text{ ולכן } \frac{n}{(d,n)} \mid t$$

תרגיל נחמד:

תהא $G = \langle a \rangle$, כמה איברים ב- G יוצרים את כל G (כל אחד בנפרד)?

פתרון

$$G = \langle a^k \rangle \Leftrightarrow o(a^k) = n = \frac{n}{(n,k)} \Leftrightarrow (n,k) = 1$$

לדוגמא $\mathbb{Z}_6 = \langle 1 \rangle$ ולכן התשובה היא $\varphi(n)$

תרגיל

נניח ש U_n חבורה צקלית, כמה איברים יפרשו אותה כל אחד לבד?

$$\varphi(|U_n|) = \varphi(\varphi(n))$$

טענה 2:

נניח שבחבורה G מתקיים עבור $g, h \in G$

$$\begin{aligned} & gh = hg \quad .1 \\ & (o(g), o(h)) = 1 \quad .2 \end{aligned}$$

אזי $o(gh) = o(g) o(h)$

הוכחה

נסמן $o(gh) = m, o(g) = n, o(h) = k$

צ"ל $m = nk$

$$(gh)^{nk} = (g^n)^k (h^k)^n = ee = e \text{ היתכנות: } e$$

$$g^{mk} = g^{mk} e = g^{mk} h^{mk} = (gh)^{mk} = ((gh)^m)^k = e \Rightarrow n|mk$$

אבל $(n, k) = 1$ ולכן $n|m$ ובאותו אופן $k|m$ ומכאן ש $[n, k] | m$ אבל $[n, k] = nk$ ולכן $m \geq nk$ ולכן $m = nk$

טענה

יהיו 2 איברים a, b בחבורה כך ש:

$$o(a) = n, o(b) = m, ab = ba$$

אזי

$$o(ab^{(n,m)}) = \frac{[n, m]}{(n, m)}$$

הוכחה

$$o(a^{(n,m)}) = \frac{n}{(n,m)} : 1 \text{ מתוך טענה 1}$$

$$o(b^{(n,m)}) = \frac{m}{(n, m)}$$

$$o(ab^{(n,m)}) = o(a^{(n,m)} b^{(n,m)}) = \frac{nm}{(n,m)^2} = \frac{[n,m]}{(n,m)} : 2 \text{ ולכן ע"פ טענה 2: } \left(\frac{n}{(n,m)}, \frac{m}{(n,m)} \right) = 1 \text{ אבל}$$

קבוצת יוצרים של חבורה

הגדרה

בהינתן חבורה G , תת קבוצה $A \subset G$ נקראית קבוצת יוצרים של G אם $\langle A \rangle = G$.
אם A סופית אז נאמר כי G נוצרת סופית.

$$\text{למשל } \mathbb{Z}^2 = \langle (1,0), (0,1) \rangle$$

הערה:

אם G נוצרת סופית אז $|G| \leq \aleph_0$

נחליט על כלשהו של היוצרים, יוצרים אלו הם הא"ב של כל אוסף המילים הסופיות שיכולות להיווצר כיוון שהא"ב סופי ניתן לסדר את כל המילים לפי סדר לקסיקוגרפי.

הערה

ניתן אבל חבורה בת מניה שאינה נוצרת סופית $(\mathbb{Q}^*, *)$

הגדרה

הדרגה של חבורה G : $\text{rank}(G)$ היא המס' המינימלי של פורשים יחד את כל G .

$$\text{למשל } \text{rank}(\mathbb{Z}^n) = n$$

חבורה חופשית

כל חבורה ניתנת לכתיבה כקבוצת האיברים היוצרים אותה וקבוצת היחסים ביניהם.

$$C_n = \langle a : a^n = e \rangle \text{ לדוגמא}$$

$$D_n = \overbrace{\{a, b\}}^{\text{יוצרים}} \mid \overbrace{b^2 = e, a^n = e, ab = b^n a^{n-1}}^{\text{יחסים}}$$

הגדרה

יחס טריוויאלי הוא שוויון בין איברי חבורה שנובע מאקסיומות של חבורה, למש $aa^{-1} = e, a^3 a^4 = a^7$

הגדרה

קבוצה חופשית (מעל קבוצה X) היא קבוצה הנוצרת ע"י איברי X כך שאין ביניהם שום יחסים ביניהם שום יחסים לא טריוויאליים.

$$\text{סימון } G = F(X)$$

$$\text{לדוגמא } G = F(\{a, b\}) = \{a, a^2, ab, ba, bbaba\}$$

הגדרה

חבורה אבלית חופשית מעל קבוצה X היא חבורה הנוצרת מאיברי X יחד עם יחס הקומוטטיביות.

מסמנים חבורה אבלית חופשית מעל X היא $G = A(X)$

$$G = A(\{a, b\}) \cong \mathbb{Z}^2$$
 לדוגמא

$$G = A(X) \cong \mathbb{Z}^{|X|}$$
 באופן כללי

האיזו' מופיע ע"י סידור מסוים של יוצרים, וקיבוץ כל היוצרים בנפרד על שכל מילה מתוארת ע"י

וקטור של חזקות בגודל n .