אלגברה ב' 1 - הרצאה 8 - 20.9.12

<u>הגדרה</u>: תהי A חבורה אבלית (חיבורית).

I. החבורה $A^t := \{a \in A \mid o(a) > \infty\}$ נקראת תת-חבורת הפיתול של A.
II. אם $A = A^t$ נאמר ש-A חבורת פיתול ($Torison$).
III. A נקראת חסרת פיתול אם $A^t = \{0\}$.

<u>למה</u>: א. $A^t \le A$.
ב. A/A^t חסרת פיתול.
ג. אם A חבורת פיתול חילופית נוצרת סופית אז A סופית.

<u>הוכחה</u>: א. ברור ש-$0 \in A^t$. יהיו $a,b \in A^t$, אז יש $m,n \in \mathbb{N}$ כך ש $ma = nb = 0$. לפיכך,

$$mn(a+b) = mna + mnb = n(ma) + m(nb) = 0$$

לכן $a+b \in A^t$. כמו כן $m(-a) = -(ma) = 0$, לכן $-a \in A^t$.
ב. צריך להוכיח לכל $a \in A$: אם $a + A^t$ מסדר $n < \infty$ ב-A/A^t אז $a + A^t = A^t$, כלומר $a \in A^t$. ואכן, $n(a+A^t) = A^t$, לכן $na \in A^t$, כלומר קיים $m \in \mathbb{N}$ כך ש-$m(na) = 0$, ולכן $a \in A^t$.
ג. באינדוקציה על מספר היוצרים המינימלי של A. אם $A = \langle a \rangle$ אז קיים n כך ש-$na = 0$, אם ניקח n מינימלי כזה יתקיים $A \cong \mathbb{Z}_n$, כלומר A סופית. נניח $A = \langle a_1, ..., a_n \rangle$. לפי הנחת האינדוקציה החבורה $B = \langle a_1, ..., a_{n-1} \rangle$ סופית, ומאבליות A מתקיים $A = B + \langle a_n \rangle$. לכן, ממשפט האיזומורפיזם השני מתקיים $A/B \cong \langle a_n \rangle / B \cap \langle a_n \rangle$, ולכן $[A:B] \le |\langle a_n \rangle| < \infty$. ממשפט לגראנז', $|A| = |B| \cdot [A:B] < \infty$. ▨

<u>דוגמה</u>: חבורת פיתול שאינה סופית - $A \cong \{(a_1, a_2, ...) \mid a_i \in Z_2\} \cong \mathbb{Z}_2^{\aleph_0}$ עם חיבור איבר-איבר. הסדר של חבורה זו הוא $\aleph$, וכל איבר בחבורה הוא מסדר 2.

<u>דוגמה</u>: נתבונן ב-$\mathbb{Q}/\mathbb{Z} = \{q + \mathbb{Z} \mid q \in \mathbb{Q}\}$. אם $\frac{m}{n} + \mathbb{Z} \in \mathbb{Q}/\mathbb{Z}$, $n,m \in \mathbb{Z}$, אז $n(\frac{m}{n} + \mathbb{Z}) = m + \mathbb{Z} = \mathbb{Z}$. זו לא חבורה סופית כי כל האיברים $\frac{1}{n} + \mathbb{Z}$ שונים זה מזה עבור $n \ge 1$, אך זו חבורת פיתול.

<u>דוגמה</u>: החבורה $\mathbb{Z}_2 \oplus \mathbb{Z}$ זו חבורה "מעורבת". האיבר $(1,0)$ מסדר סופי, אך האיבר $(0,1)$ מסדר אינסופי.

הגדרה: תהא F חבורה אבלית. קבוצה של איברים $v_1,...,v_n \in F$ נקראת בסיס אם לכל $v \in F$ יש הצגה יחידה $v=\sum_{i=1}^{n}\alpha_i v_i$ כאשר $\alpha_i \in \mathbb{Z}$ לכל i. חבורה אבלית נקראת חופשית אם יש לה בסיס.

משפט: תהא F חבורה אבלית חופשית עם בסיס $v_1,...,v_n$, ותהא A חבורה אבלית, $a_1,...,a_n \in A$. קיים הומומורפיזם יחיד $\varphi: F \to A$ כך ש- $\forall 1\le i\le n: \varphi(v_i)=a_i$. בפרט, אם $A=\langle a_1,...,a_n\rangle$, אזי $A\cong F/\ker\varphi$.

הוכחה: נגדיר $\varphi: F\to A$ באופן הבא: לכל $v=\sum_{i=1}^{n}\alpha_i v_i$ יתקיים:

$$\varphi(v)=\sum_{i=1}^{n}\alpha_i\varphi(v_i)=\sum_{i=1}^{n}\alpha_i a_i$$

לפי הגדרת הבסיס, זוהי הגדרה טובה. ברור שמדובר בהומומורפיזם יחיד המקיים את התכונות הרצויות. אם $A=\langle a_1,...,a_n\rangle$, אזי $\operatorname{Im}\varphi = A$, ולכן לפי משפט ההומומורפיזם $A\cong F/\ker\varphi$. ▨

למה: תהא F חבורה אבלית, $v_1,...,v_n\in F$. $v_1,...,v_n$ בסיס אס"ם

- $F=\langle v_1\rangle\oplus\langle v_2\rangle\oplus...\oplus\langle v_n\rangle$
- $\forall 1\le i\le n: \langle v_i\rangle\cong\mathbb{Z}$

הוכחה: $F=\langle v_1\rangle\oplus\langle v_2\rangle\oplus...\oplus\langle v_n\rangle$ שקול ל:

- $F=\langle\langle v_1\rangle,\langle v_2\rangle,...,\langle v_n\rangle\rangle$, כלומר קיימת הצגה לכל $v\in F$, אולי אינה יחידה.
- $a_i a_j = a_j a_i,\ a_i\in\langle v_i\rangle,\ a_j\in\langle v_j\rangle$ עבור $i\ne j$.
- אם $m_1'v_1+m_2'v_2+...+m_n'v_n=m_1v_1+m_2v_2+...+m_nv_n$ אזי $m_i'v_i=m_iv_i$ לכל i.

$\forall 1\le i\le n: \langle v_i\rangle\cong\mathbb{Z}$ שקול ל- $ord(v_i)=\infty$, כלומר $k_iv_i=0 \Leftarrow k_i=0$, ולכן אם $m_i'v_i=m_iv_i$ אזי $m_i'=m_i$. כלומר, קיבלנו שתנאים אלו שקולים לקיום הצגה לכל $v\in F$, וליחידות הצגה זו. ▨

מסקנה: חבורה אבלית F היא חופשית אס"ם $F\cong\mathbb{Z}^n$.

תרגיל: תהי F אבלית חופשית עם בסיס $v_1,...,v_n$. יהיו $k_2,...,k_n\in\mathbb{Z}$, אז גם

$$v_1+k_2v_2+k_3v_3+...+k_nv_n, v_2, v_3, ..., v_n$$

בסיס.

הערה: הטענה נכונה גם עבור סדרת יוצרים, והוכחה זהה פרט לטענה על יחידות ההצגה, שאינה דרושה עבור סדרת היוצרים.

הוכחה: יהי $v\in F$. מספיק להוכיח שקיימים $m_1,...,m_n$ יחידים כך שמתקיים:

$$v=m_1(v_1+k_2v_2+...+k_nv_n)+m_2v_2+...+m_nv_n=m_1v_1+(m_1k_2+m_2)v_2+...+(m_1k_n+m_n)v_n$$

$v_1,...,v_n$ בסיס, לכן קיימים $r_1,...,r_n$ יחידים כך ש- $v=r_1v_1+r_2v_2+...+r_nv_n$. לפיכך, בהכרח מתקיים $r_1=m_1$, $\forall 2\le i\le n: r_i=m_1k_i+m_i$, כלומר $\forall 2\le i\le n: m_i=r_i-m_1k_i$, ולכן m_i נקבעים ביחידות. ▨

משפט: תהי F חבורת חסרת פיתול אבלית. אם F נוצרת סופית אז F חופשית.

הוכחה: יהי n מספר מינימלי עבורו יש סדרת יוצרים בת n איברים ל- F. נניח בשלילה שלא קיים בסיס ל- F. לכן, לכל סדרת יוצרים $v_1,v_2,...,v_n$ קיימים $m_1,...,m_n\in\mathbb{Z}$, לא כולם אפס, כך ש- $m_1v_1+m_2v_2+...+m_nv_n=0$. לכל סדרת יוצרים נסמן $\delta(v_1,v_2,...,v_n):=|m_1|+...+|m_n|$. נבחר סדרת יוצרים בת n איברים ל- F, $v_1,v_2,...,v_n$, כך ש- $\delta(v_1,v_2,...,v_n)$ מינימלי. אם קיים i יחיד עבורו $m_i\neq 0$, אזי $m_iv_i=0$, ומשום ש- F חסרת פיתול בהכרח $v_i=0$, בסתירה למינימליות גודל סדרת היוצרים. לפיכך, נניח שלפחות עבור שני ערכי i מתקיים $m_i=0$.

בה״כ נניח $m_1,m_2\neq 0$, $|m_1|\le|m_2|$, $0<m_1$. נחלק עם שארית: $m_2=qm_1+r, 0\le r<m_1$.

$$\Rightarrow m_1v_1+(qm_1+r)v_2+m_3v_3+...+m_nv_n=0$$
$$\Rightarrow m_1(v_1+qv_2)+rv_2+m_3v_3+...+m_nv_n=0$$

לפי התרגיל הקודם גם הסדרה $v_1+qv_2,v_2,v_3,...,v_n$ היא סדרת יוצרים. מתקיים:

$$\delta(v_1+qv_2,v_2,...,v_n)=|m_1|+|r|+|m_3|+...+|m_n|<|m_1|+|m_1|+...+|m_n|\le$$
$$\le|m_1|+|m_2|+...+|m_n|=\delta(v_1,v_2,...,v_n)$$

בסתירה למינימליות $\delta(v_1,v_2,...,v_n)$. ▨

משפט: אם $v_1,...,v_n$ בסיס לחבורה אבלית F ו- $u_1,...,u_k$ סדרת יוצרים ל- F אזי $n\le k$.

הוכחה: נרשום $v_i=m_{1i}u_1+...+m_{ki}u_k$ עבור כל $i\in\{1,...,n\}$. נניח בשלילה $n>k$ ונתבונן במטריצה $M=(m_{ij})_{n\times k}$. מכיוון ש- $n>k$ שורות המטריצה M תלויות לינארית (מעל $\mathbb{Q}$). לכן, קיימים $q_1,...,q_n\in\mathbb{Q}$, לא כולם אפס, כך ש- $q_1(m_{11},...,m_{k1})+...+q_n(m_{1n},...,m_{kn})=(0,...0)$, ולכן $q_1v_1+...+q_nv_n=0$, בסתירה לכך ש- $v_1,...,v_n$ בסיס. ▨

מסקנה: אם B_1,B_2 שני בסיסים שונים ל- F, שניהם עם אותו מספר איברים. למספר זה נקרא הדרגה של F, ונסמנו rkF.

<u>משפט</u> (משפט החבורות החלקיות של תת-החבורה החופשית F_n): תהי $H \le F_n$ תת-חבורה של חבורה חופשית אבלית מדרגה n, אז גם H חופשית. יתר על כן, קיים בסיס $v_1,...,v_n$ ל- F_n וקיימים $0 \le k \le n$, $\varepsilon_1,\varepsilon_2,...,\varepsilon_k \in \mathbb{N}$ כך ש- $\varepsilon_1 | \varepsilon_2 | \varepsilon_3 | ... | \varepsilon_k$ (כל איבר מחלק את עקבו), ו- $\varepsilon_1 v_1,...,\varepsilon_k v_k$ הוא בסיס ל- H.

<u>הוכחה</u>: אם $H = \langle 0 \rangle$ אז קבוצה ריקה של וקטורים מהווה בסיס ל- H, ולכן הטענה נכונה עבור $n=0$. נוכיח אינדוקטיבית על n.

טענת עזר I: קיימים $u_1,...,u_n \in F_n$ כך שעבור $0 \ne v \in H$ מתקיים $v = \sum_{i=1}^n m_i u_i$, $m_1 > 0$. ואכן, נבחר בסיס כלשהו $u_1,...,u_n \in F_n$ ו- $0 \ne v \in H$, לכן $v = \sum_{i=1}^n m_i u_i$ עבור $m_i \in \mathbb{Z}$ כלשהם, וקיים i עבורו $m_i \ne 0$. נחליף את u_1 ב- u_i כדי להניח $m_1 \ne 0$, ונחליף את u_i ב- $(-u_i)$ במידת הצורך כדי להניח $m_1 > 0$. נסמן עבור $0 \ne v \in H$, $\varepsilon_1 := \min\{m_1 | u_1,...,u_n \in F_n : v = \sum_{i=1}^n m_i v_i\}$.

טענת עזר II: יש בסיס $u_1,...,u_n \in F_n$ כך ש- $\varepsilon_1 u_1 \in H$.
נבחר $u_1,...,u_n, v \in F_n$, כך ש- $\varepsilon_1 = m_1$. נחלק עם שארית: $i \ge 2 : m_i = q_i \varepsilon_1 + r_i,\ \ 0 \le r_i < \varepsilon_1$.
נסמן $u_1' = u_1 + \sum_{i=2}^n q_i u_i$, וגם הקבוצה $u_1', u_2, ..., u_n$ בסיס של F_n (תרגיל מעמוד קודם), ומתקיים $v = \varepsilon_1 u_1' + \sum_{i=2}^n r_i u_i$. ε_1 מינימלי מבין כל הצירופים הלינארים המבטאים את v, לכן אם קיים i עבורו $r_i > 0$, לפי החלוקה בשארית $0 < r_i < \varepsilon_1$, ולכן ניתן להחליף את i ו-1 על מנת לקבל צירוף לינארי חדש, בו המקדם הראשון קטן יותר מ- ε_1, בסתירה למינימליות ε_1. לכן, $\forall 2 \le i \le n : r_i = 0$, ולכן $\varepsilon_1 u_1' = v \in H$ ומצאנו בסיס כנדרש.

יהי בסיס $u_1,...,u_n \in F_n$ כך ש- $\varepsilon_1 u_1 \in H$. נסמן:

$$F' = \langle u_2,...,u_n \rangle,\ \ H' = H \cap F'$$

מתקיים $F_n = \langle u_1 \rangle \oplus F'$, לכן F' אבלית חופשית מדרגה $n-1$ עם בסיס $u_2,...,u_n$.

טענת עזר III: $H = \langle \varepsilon_1 u_1 \rangle \oplus H'$, כאשר מדובר בסכום ישר פנימי.
ואכן, מתקיים $\langle \varepsilon_1 u_1 \rangle \cap H' = \{0\}$, אחרת יתקיים $\langle \varepsilon_1 u_1 \rangle \cap F' \ne \{0\}$ בסתירה לכך ש- $u_1,...,u_n$ בסיס. $H' \lhd H$ מאבליות, לכן נותר להראות $H = \langle \varepsilon_1 u_1 \rangle + H'$.

יהי $u = \sum_{i=1}^n m_i u_i$ איבר של H. נחלק עם שארית: $m_1 = q\varepsilon_1 + r,\ \ 0 \le r < \varepsilon_1$. מתקיים

$$u-q(\varepsilon_1 u_1)=ru_1+\sum_{i=2}^{n} m_i u_i$$

ו- $r=0$ ממזעריות ε_1. לכן $u-q(\varepsilon_1 u_1)=\sum_{i=2}^{n} m_i u_i \in H\cap F'=H'$ (שייכות ל- F' ברורה, ו- H מסגירות). לפיכך $u=q(\varepsilon_1 u_1)+\sum_{i=2}^{n} m_i u_i \in \langle \varepsilon_1 u_1\rangle + H'$, ולכן $H=\langle \varepsilon_1 u_1\rangle \oplus H'$.

לפי הנחת האינדוקציה, H' חופשית ויש בסיס $v_2,...,v_n$ ל- F', ו- $\varepsilon_2,...,\varepsilon_k\in\mathbb{N}$ כך ש: $\varepsilon_2\,|\,\varepsilon_3\,|\,...\,|\,\varepsilon_k$ ו- $\varepsilon_2 v_2,...,\varepsilon_k v_k$ בסיס של H'. יהי $v_1 := u_1$, אז $F=\langle v_1\rangle\oplus F'$, ולכן $v_1,...,v_n$, ו- $\varepsilon_1 v_1,...,\varepsilon_k v_k$ בסיס ל- H. נשאר להראות $\varepsilon_1\,|\,\varepsilon_2$. אכן, נכתוב $\varepsilon_2=q\varepsilon_1+r$, $0\le r<\varepsilon_1$, ונסמן $v_1'=v_1+qv_2$, ונקבל $v_1',v_2,...,v_n$ בסיס ל- F_n ומתקיים:

$$\varepsilon_2 v_2-\varepsilon_1 v_1\in H$$

$$\varepsilon_1 q v_2+rv_2-\varepsilon_1 v_1=-\varepsilon_1 v_1'+rv_2=-\varepsilon_1 v_1'+rv_2+0\cdot v_3+...+0\cdot v_n$$

ומשום ש- ε_1 מזערי אזי $r=0$, ולכן $\varepsilon_2=q\varepsilon_1$, כלומר $\varepsilon_1\,|\,\varepsilon_2$. ▨

<u>מסקנה</u>: אם F חופשית, $H\le F$, אז $rkH\le rkF$.

המבנה של חבורה אבלית נוצרת סופית

<u>המטרה</u>: להראות שכל חבורה אבלית נוצרת סופית היא סכום ישר של חבורות חופשיות (כלומר, סכום של כמה עותקי $\mathbb{Z}$ ושל חבורות ציקליות סופיות).

<u>טענה</u>: תהא $G_1 \times G_2 \times \ldots \times G_n = G$, ולכל $1 \le i \le n$ נניח $N_i \lhd G_i$. נסמן $N = N_1 \cdot N_2 \cdot \ldots \cdot N_n$.
הוכח: $G/N \cong G_1/N_1 \times G_2/N_2 \times \ldots \times G_n/N_n$.

<u>הוכחה</u>: באינדוקציה, מספיק להראות ל- $n=2$. נגדיר העתקה $\varphi : G \to (G_1/N_1 \times G_2/N_2)$ על ידי: $\varphi(g_1, g_2) = (g_1N_1, g_2N_2)$. קל להראות שזהו אפימורפיזם.

$$\ker\varphi = \{(g_1, g_2) \mid (g_1N_1, g_2N_2) = (N_1, N_2)\} =$$
$$= \{(g_1, g_2) \mid g_1 \in N_1, g_2 \in N_2\} = N_1 \cdot N_2 = N$$

ולפי משפט האיזומורפיזם הראשון $G/N \cong G_1/N_1 \times G_2/N_2$. ▨

<u>המשפט היסודי של חבורות אבליות נוצרות סופית</u>: כל חבורה אבלית נוצרת סופית A היא סכום ישר של חבורות ציקליות, וליתר דיוק $A \cong \mathbb{Z}_{\varepsilon_1} \times \mathbb{Z}_{\varepsilon_2} \times \ldots \times \mathbb{Z}_{\varepsilon_k} \times \overbrace{\mathbb{Z} \times \ldots \times \mathbb{Z}}^{r}$,
כאשר $\varepsilon_1 \mid \varepsilon_2 \mid \ldots \mid \varepsilon_k$, $r, k \ge 0$, ומספרים אלו נקבעים ביחידות.

<u>הוכחה</u>: נסמן $A = \langle a_1, .., a_n \rangle$. תהא חבורה חופשית F_n מדרגה n, ויהי $u_1, \ldots, u_n$ בסיס שלה. לפי משפט שהוכחנו, ההעתקה $\varphi : F \to A$, $\varphi(u_i) := a_i$ היא הומומורפיזם ויחידה, ומתקיים $A \cong F_n / \ker\varphi$. נסמן $H = \ker\varphi$. לפי משפט החבורות החלקיות של החבורה החילופית החופשית F_n, קיים בסיס $v_1, \ldots, v_n$ של F_n כך ש:

$$F_n = \langle v_1 \rangle \oplus \ldots \oplus \langle v_k \rangle \oplus \langle v_{k+1} \rangle \oplus \ldots \oplus \langle v_n \rangle$$
$$H = \langle \varepsilon_1 v_1 \rangle \oplus \ldots \oplus \langle \varepsilon_1 v_k \rangle = \langle \varepsilon_1 v_1 \rangle \oplus \ldots \oplus \langle \varepsilon_1 v_k \rangle \oplus \underbrace{\langle 0 \rangle \oplus \ldots \oplus \langle 0 \rangle}_{n-k}$$

כאשר $\varepsilon_1 \mid \varepsilon_2 \mid \ldots \mid \varepsilon_k$, $k \le n$. לפי הטענה האחרונה מתקיים:

$$A \cong F/H \cong \langle v_1 \rangle / \langle \varepsilon_1 v_1 \rangle \oplus \langle v_2 \rangle / \langle \varepsilon_2 v_2 \rangle \oplus \ldots \oplus \langle v_k \rangle / \langle \varepsilon_k v_k \rangle \oplus \langle v_{k+1} \rangle / \langle 0 \rangle \oplus \ldots \oplus \langle v_n \rangle / \langle 0 \rangle$$

אולם $\langle v_1 \rangle \cong \mathbb{Z}$, לכן $\langle v_1 \rangle / \langle \varepsilon_1 v_1 \rangle \cong \mathbb{Z}_{\varepsilon_1}$, וכנ"ל עבור $i = 2, \ldots, k$. $\langle v_{k+1} \rangle / \langle 0 \rangle \cong \langle v_{k+1} \rangle \cong \mathbb{Z}$, וכנ"ל עבור $i = k+2, \ldots, n$. נסמן $r = n-k \ge 0$. קיבלנו:

$$A \cong \mathbb{Z}_{\varepsilon_1} \times \mathbb{Z}_{\varepsilon_2} \times \ldots \times \mathbb{Z}_{\varepsilon_k} \times \overbrace{\mathbb{Z} \times \ldots \times \mathbb{Z}}^{r}$$

▨