<u>הצגות של חבורות סופיות</u>

ⓒ ארזים

8 בדצמבר 2016

1 חוג חבורה

הגדרה 1.1 תהי G חבורה ויהי R חוג קומוטטיבי עם יחידה. נגדיר את <u>חוג החבורה</u>:

$$R[G] = \left\{ \sum_{s \in G} a_s \cdot s \mid a_s \in R \right\}$$

את הכפל נגדיר על ידי

$$a_s s \cdot a_t t = a_s a_t st$$

עבור G אבלית נקבל חוג קומוטטיבי, ועבור G לא אבלית - חוג לא קומוטטיבי (זה נקרא גם אלגברת החוג).

אנחנו נתבונן במקרה הפרטי $\mathbb{C}[G]$. זוהי $\mathbb{C}$ אלגברה, לאו דווקא קומוטטיבית, עם יחידה. ניתן להגדיר תורה אנלוגית לתורת ההצגות, עם מודולים מעל אלגברה, אבל אנחנו לא נעשה את זה.

מטרתנו - בהינתן כל ההצגות האי פריקות של G, לאפיין במדוייק את $\mathbb{C}[G]$. נרצה להראות כי $\mathbb{C}[G]$ איזומורפית למכפלת אלגבראות מטריצות. במדוייק, יהיו $\rho_i : G \to GL(W_i)$ כל ההצגות האי פריקות השונות של G. נסמן $n_i = \dim W_i$. אזי בבירור

$$\mathrm{End}(W_i) \cong M_{n_i}(\mathbb{C})$$

כעת נוכל להגדיר לפי לינאריות, בהנתן ρ_i:

$$\tilde{\rho}_i : \mathbb{C}[G] \to \mathrm{End}(W_i)$$
$$\tilde{\rho}_i \left(\sum a_s s \right) = \sum a_s \rho_i(s)$$

ועכשיו נוכל להגדיר:

$$\tilde{\rho} : \mathbb{C}[G] \to \prod_i \mathrm{End}(W_i)$$
$$\tilde{\rho} \left(\sum a_s s \right) = \left(\tilde{\rho}_i \left(\sum a_s s \right) \right)_i$$

טענה 1.2 $\tilde{\rho}$ היא איזומורפיזם.

הוכחה: בבירור זו העתקה לינארית, וקל לראות שמימד המרחב $\mathbb{C}[G]$ הוא $|G|$ בעוד מרחב המכפלה הוא

$$\sum_i n_i^2 = |G|$$

ולכן מספיק להוכיח כי $\tilde{\rho}$ על. אחרת, קיימת תבנית לינארית לא טריוויאלית על

$$\prod_i \mathrm{End}(W_i)$$

שמתאפסת על כל התמונה.
$\tilde{\rho}$ נותנת לנו למעשה $\sum n_i^2$ מספרים מרוכבים, שהם $\rho_i^{k,l}(s)$ (הכניסה (k,l) של המטריצה $\rho_i(s)$). ראינו מיחסי אורתוגונליות:

$$\left(\rho_i^{k,l}, \rho_{i'}^{k',l'}\right) = \frac{1}{n_i}\delta_{i,i'}\delta_{k,k'}\delta_{l,l'}$$

לכן בפרט מתקבלת סדרה אורתוגונלית, ולכן בלתי תלויה לינארית - לכן לא ייתכן יש קומבינציה לינארית שלהם שמתאפסת. לכן $\tilde{\rho}$ אכן על, וסיימנו. ■

טענה 1.3 (נוסחת היפוך פורייה) יהי $(u_i)_{1\le i\le n}$ איבר של $\prod \mathrm{End}(W_i)$, כך שמתקיים $u = \sum u(s)s \in \mathbb{C}[G]$. אזי המקדם $u(s)$ של u באיבר s הוא

$$u(s) = \frac{1}{|G|}\sum_i n_i \mathrm{Tr}_{W_i}\left(\rho_i\left(s^{-1}\right)u_i\right)$$

הוכחה: לפי לינאריות, מספיק להניח כי $u = t \in G$. אזי $u(s) = \delta_{t,s}$. כמו כן, $u_i = \tilde{\rho}_i(u) = \rho_i(t)$. אזי מתקיים

$$\mathrm{Tr}_{W_i}\left(\rho_i\left(s^{-1}\right)u_i\right) = \mathrm{Tr}_{W_i}\left(\rho_i\left(s^{-1}\right)\rho_i(t)\right) = \mathrm{Tr}_{W_i}\left(\rho_i\left(s^{-1}t\right)\right) = \chi_i\left(s^{-1}t\right)$$

לכן נשאר להראות

$$\delta_{t,s} = \frac{1}{|G|}\sum_i n_i\chi_i\left(s^{-1}t\right)$$

ואת הנוסחה הזו הוכחנו בעבר, כשעסקנו בתורת הכרטקטרים. אם $s = t$, נקבל

$$1 = \frac{1}{|G|}\sum_i n_i\chi_i(1) = \frac{1}{|G|}\sum_i n_i^2 = 1$$

ואם $s \neq t$ נקבל

$$0 = \sum_i n_i\chi_i(s)$$

כפי שראינו. ■

1.1 המרכז של $\mathbb{C}[G]$

הגדרה 1.4 המרכז של $\mathbb{C}[G]$, $\mathrm{Cent}\mathbb{C}[G]$ הוא אוסף כל האיברים המתחלפים עם כל איברי $\mathbb{C}[G]$ (באופן שקול, עם כל איברי G).

דוגמא ניקח מחלקת צמידות C של G. ניקח את

$$e_C = \sum_{s \in C} s$$

זהו איבר מרכזי, שכן

$$te_Ct^{-1} = t\left(\sum_{s\in C} s\right)t^{-1} = \sum_{s\in C} tst^{-1} = \sum_{u\in C} u = e_C$$

יהי $\mathrm{Cent}\mathbb{C}[G] \ni u_s s \sum$. ברור לחלוטין שהיא פונקציית מחלקות על G, שכן

$$t\left(\sum u_s s\right)t^{-1} = \sum u_s s$$

לכן e_C שהגדרנו קודם יהוו בסיס, כאשר ניקח כל מחלקת צמידות. לכן המרכז הוא מרחב ווקטורי מעל C ממימד h (כמות מחלקות הצמידות).
כעת, בהינתן $\rho_i : G \to GL(V)$ הצגה אי פריקה, ראינו את ההרחבה הלינארית $\tilde{\rho}_i : \mathbb{C}[G] \to \mathrm{End}(W_i)$.

טענה 1.5 ההומומורפיזם $\tilde{\rho}$ מעביר את $\mathrm{Cent}\mathbb{C}[G]$ לקבוצת ההומותטיות של W_i, ומגדיר הומומורפיזם של אלגבראות

$$\omega_i : \mathrm{Cent}\mathbb{C}[G] \to \mathbb{C}$$

אם $u = \sum u(s)\, s \in \mathrm{Cent}\mathbb{C}[G]$, אז

$$\omega_i(u) = \frac{1}{n_i}\mathrm{Tr}_{W_i}(\tilde{\rho}_i(u)) = \frac{1}{n_i}\sum_{s\in G} u(s)\,\chi_i(s)$$

הוכחה: ההעתקה $\tilde{\rho}_i$ בבירור על, ולכן מעבירה את המרכז למרכז - והמרכז של $\mathrm{End}(W_i)$ הוא בדיוק ההומותטיות. עבור החישוב המדוייק של הקבוע, כל איבר במרכז הוא פונקציית מחלקות, וראינו שעבור פונקציית מחלקות f, ההעתקה

$$\rho_f = \sum f(t)\,\rho_t$$

היא הומותטיה עם קבוע

$$\lambda = \frac{1}{n_i}\sum_{t\in G} f(t)\,\chi_i(t)$$

כמו שרצינו. ■

טענה 1.6 המשפחה ω_i, עבור $1 \le i \le h$, נותנת איזומורפיזם

$$\mathrm{Cent}\mathbb{C}\left[G\right] \cong \mathbb{C}^h = \mathbb{C} \times \mathbb{C} \times \cdots \times \mathbb{C}$$

הוכחה: נוכל לזהות את $\mathbb{C}\left[G\right]$ עם

$$\prod_{i=1}^{h} \mathrm{End}\left(W_i\right)$$

ולכן נוכל לזהות את המרכזים. המרכז של $\mathrm{End}\left(W_i\right)$ הוא בדיוק אוסף ההומותטיות, שאיזומורפי למרחב $\mathbb{C}$, ולכן המרכז של המכפלה הוא מכפלה של כל אלה ־ כלומר $\mathbb{C}^h$. ברור כי ω_i נותנות את האיזומורפיזם הזה. ■

1.2 שלמות ותכונות בסיסיות של איברים שלמים

למה 1.7 תהי A חבורה אבלית נוצרת סופית. תהי $B \le A$ תת חבורה. אזי גם B אבלית ונוצרת סופית.

זו טענה מאלגברה ב1, שלא נוכיח.

הגדרה 1.8 יהי R חוג קומוטטיבי ויהי $x \in R$. אומרים כי x <u>שלם</u> מעל $\mathbb{Z}$ אם יש $1 \le n \in \mathbb{Z}$ וגם $a_1, \ldots, a_n \in \mathbb{Z}$ כך שמתקיים

$$x^n + a_1 x^{n-1} + \cdots + a_n = 0$$

דוגמאות $\sqrt{2} \in \mathbb{R}$ שלם:

$$x^2 - 2 = 0$$

לעומת זאת, $\sqrt{\frac{1}{2}}$ אינו שלם (אולי נראה את ההוכחה מאוחר יותר). גם $\frac{1}{2}$ אינו שלם. 2 כן שלם.

הגדרה 1.9 מספר מרוכב $z \in \mathbb{C}$ השלם מעל $\mathbb{Z}$ נקרא <u>מספר שלם אלגברי</u>.

למה 1.10 יהי $x \in \mathbb{Q}$. אם x שלם אלגברי, אזי $x \in \mathbb{Z}$.

הוכחה: נניח בשלילה כי $x \notin \mathbb{Z}$. נכתוב

$$x = \frac{p}{q}$$

כאשר $p, q \in \mathbb{Z}$, $q \ge 2$, $\gcd\left(p, q\right) = 1$. אם כן, מקבלים כי קיימים שלמים עבורם

$$p^n + a_1 q p^{n-1} + \cdots + a_n q^n = 0$$

מכאן רואים כי $q \mid p^n$, אבל $\gcd\left(p, q\right) = 1$, ולכן זו סתירה. ■

מסקנה 1.11 (פיתגורס) $\sqrt{2}\notin\mathbb{Q}$.

הוכחה: $\sqrt{2}$ שלם אלגברי, לכן אם היה רציונאלי הוא היה שלם. אבל ברור כי $2 \neq (\pm1)^2 , 0^2$, ולכל $x\in\mathbb{Z}$ אחר מתקיים $x^2\geq 4$, ולכן אין פיתרון בתוך $\mathbb{Z}$ עבור $x^2-2=0$. ■

טענה 1.12 יהי R חוג קומוטטיבי המכיל את $\mathbb{Z}$, ויהי $x\in R$. נסמן

$$\mathbb{Z}\left[x\right]=\{b_0+b_1x+\cdots+b_mx^m \mid b_0,\ldots,b_m\in\mathbb{Z}\}$$

אזי התנאים הבאים שקולים:

1. x שלם מעל $\mathbb{Z}$.
2. תת החוג $\mathbb{Z}\left[x\right]$ של R, הנוצר על ידי x, הוא נוצר סופית כחבורה אבלית.
3. קיימת תת חבורה נוצרת סופית $A\subseteq R$ כך שמתקיים

$$A\supseteq\mathbb{Z}\left[x\right]$$

הוכחה: $3 \Leftarrow 2$: ברור, ניקח $A=\mathbb{Z}\left[x\right]$.
$2 \Leftarrow 3$: $\mathbb{Z}\left[x\right]$ נוצרת סופית כתת חבורה של חבורה אבלית נוצרת סופית.
$2 \Leftarrow 1$: x שלם, כלומר קיימים שלמים עבורם

$$x^n+a_1x^{n-1}+\cdots+a_n=0$$

נגדיר $g_0=1$, $g_1=x$, $g_2=x^2$, וכן הלאה עד $g_{n-1}=x^{n-1}$. כל האיברים הללו שייכים לחבורה $\mathbb{Z}\left[x\right]$. אזי נקבל כי

$$x^n\in\langle g_0,g_1,\ldots,g_{n-1}\rangle$$

כמו כן,

$$x^{n+1}=x^n\cdot x\in\langle g_0,\ldots,g_{n-1}\rangle$$

לכן באינדוקציה $\mathbb{Z}\left[x\right]=\langle g_0,\ldots,g_{n-1}\rangle$.
$1 \Leftarrow 2$: נגדיר

$$R_n=\left\langle 1,x,\ldots,x^{n-1}\right\rangle$$

כמובן מתקיים $R_n\subseteq R_{n+1}$, וכן

$$\bigcup_{n=1}^{\infty}R_n=\mathbb{Z}\left[x\right]$$

מההנחה, $\mathbb{Z}[x]$ היא חבורה אבלית נוצרת סופית. ניקח $g_1,\dots,g_r$ יוצרים. כעת, לכל i קיים n_i כך שמתקיים $g_i \in R_{n_i}$. נגדיר

$$m = \max n_i$$

אזי $m \geq n_i$ לכל i, ולכן

$$R_m \supseteq R_{n_i} \ni g_i$$

לכל i. לכן $R_m = \mathbb{Z}[x]$. כלומר $\{1, x, \dots, x^{m-1}\}$ יוצרים את $\mathbb{Z}[x]$, ובפרט

$$x^m = a_0 + a_1 x + \dots + a_{n-1} x^{n-1}$$

ולכן x שלם מעל $\mathbb{Z}$. ■

דוגמא נסתכל על $\mathbb{Z}[x]$. זהו תת חוג של $\mathbb{R}$.נרצה לדעת האם הוא נוצר סופית. עבור $\sqrt{2}$ כן, ועבור $\frac{1}{2}$ לא. גם ברור כי עבור $\sqrt{\frac{1}{2}}$ החוג לא נוצר סופית, כי הוא מכיל את זה של $\frac{1}{2}$.

מסקנה 1.13 אם R חוג שמכיל את $\mathbb{Z}$ ונוצר סופית כחבורה אבלית, אזי כל איבר של R הוא שלם מעל $\mathbb{Z}$.

הוכחה: יהי $x \in R$. אזי $\mathbb{Z}[x] \subseteq R$, ולכן תנאי 3 מהטענה הקודמת מתקיים, ולכן x שלם מעל $\mathbb{Z}$. ■

מסקנה 1.14 האיברים של R שהם שלמים מעל $\mathbb{Z}$ מהווים תת חוג של R. כלומר אם x, y שלמים מעל $\mathbb{Z}$, אז גם $x \pm y$, $x \cdot y$ שלמים מעל $\mathbb{Z}$.

הוכחה: יהיו $x, y \in R$. נגדיר $\mathbb{Z}[x,y]$ - תת החוג המינימלי המכיל את x, y, כלומר כל האיברים מהצורה

$$\sum_{i,j} a_{i,j} x^i y^j$$

נניח כי x, y שלמים מעל $\mathbb{Z}$. אזי $\mathbb{Z}[x] = \langle 1, x, \dots, x^{n-1} \rangle$, וכן $\mathbb{Z}[y] = \langle 1, y, \dots, y^{m-1} \rangle$. אז נקבל

$$\mathbb{Z}[x,y] = \langle x^i y^j \mid 0 \leq i \leq n, 0 \leq j \leq m \rangle$$

זו חבורה נוצרת סופית ולכן כל איבריה שלמים - כולל $x \pm y, x \cdot y$. ■

טענה 1.15 יהי χ כרקטר של הצגה ρ של חבורה סופית G. אזי $\chi(s)$ הוא מספר שלם אלגברי לכל $s \in G$.

הוכחה: החבורה סופית, ולכן הכרקטר הוא סכום של שורשי יחידה - בפרט שלם אלגברי כסכום של שלמים אלגבריים. ■

טענה 1.16 נסתכל על החוג הקומוטטיבי $\mathrm{Cent}\mathbb{C}[G]$ וניקח בו איבר $u = \sum u(s)\, s$. נניח כי כל $u(s)$ שלמים אלגבריים, אזי u שלם מעל $\mathbb{Z}$.

הוכחה: ניקח את מחלקות הצמידות C_i של G, עבור $1 \le i \le h$. נכתוב

$$e_i = \sum_{s \in C_i} s \in \mathrm{Cent}\mathbb{C}[G]$$

אזי, עבור s_i נציגים של C_i, מתקיים

$$u = \sum u(s_i)\, e_i$$

$u(s_i)$ שלמים אלגבריים מההנחה, נותר להראות כי e_i שלמים אלגבריים. נגדיר

$$R = \mathbb{Z}e_1 + \cdots + \mathbb{Z}e_h$$

זהו תת חוג נוצר סופית. לכן כל e_i שלם אלגברי, כאיבר של תת חוג נוצר סופית. ■