הרצאה 6

29 באפריל 2019

1 חבורות ציקליות - סיום

נזכיר כי הגדרנו את החבורה הציקלית להיות חבורה $G=\{e,g,g^2,\dots,g^{n-1}\}$ כך ש-$g^n=e$ ואנו אומרים ש-g הוא היוצר של G.

הערה 1. תת חבורה של חבורה ציקלית, היא ציקלית.
לדוגמה, למדנו כי אם $H<\mathbb{Z}$, כלומר תת חבורה של השלמים, אז היא מהצורה $k\mathbb{Z}$, כלומר עבור $k=5$ נקבל כי $H=\{\dots,-5,0,5,10,15,\dots\}$.

הוכחה. ניתן להניח כי $G=\mathbb{Z}_n$ (כי ראינו שכל חבורה ציקלית היא איזומורפית ל-$\mathbb{Z}_n$, ולכן הן למעשה אותו דבר וההוכחה שקולה).
תהא $H<\mathbb{Z}_n$. יהא k האיבר המינימאלי ב-H ששונה מ-0 . נראה ש-k יוצר של H.
ברור שמתקיים: $0,k,k+k,k+k+k,\dots$ כולם בתוך H, שכן היא תת חבורה ולכן סגורה לפעולה (חיבור במקרה שלנו כי אנחנו תת חבורה של $\mathbb{Z}_n$).
אם נראה שכל איבר $h\in H$ הוא מהצורה $m\cdot k$, פירושו שכל איבר h נוצר על ידי k.
נרשום: $h=m\cdot k+r$ כאשר $r<k$. נרצה להראות שהשארית r שווה ל-0. נניח בשלילה כי $r>0$. אזי מתקיים $r=h-m\cdot k$, ולכן מסגירות לפעולה $r\in H$. אך זו סתירה לכך ש-k היה מינימאלי, שונה מ-0 ב-H.
לכן $r=0$ ו-k הוא באמת יוצר כנדרש. ■

הערה 2. החבורה $\mathbb{Z}_2\oplus\mathbb{Z}_3$ציקלית.

הוכחה. נראה שהאיבר $(1,1)$ יוצר. קל להראות זאת על ידי מעבר על כל האיברים ב-$\mathbb{Z}_2\oplus\mathbb{Z}_3$ (זה אפשרי כי החבורה קטנה יחסית) ולהראות כי קיים k כך ש-$(1,1)^k$ שווה להם:
$(1,1),(1,1)+(1,1)=(0,2),3\cdot(1,1)=(1,0),4\cdot(1,1)=(0,1),5\cdot(1,1)=(1,2)$. ■

משפט 3. $\mathbb{Z}_a\oplus\mathbb{Z}_b\cong\mathbb{Z}_{ab}$ אם $(a,b)=1$.

הוכחה. ניקח כיוצר את $(1,1)$ ונראה כי הסדר שלו הוא $n=a\cdot b$.
נניח בשלילה כי $s=o(1,1)<n$. מתקיים: $(s,s)=s\cdot(1,1)=(0,0)$ משום ש-$(s\cdot mod(a),s\cdot mod(b))=(0,0)$, שפירושו $a|s$ וכן $b|s$.
לכן s הוא כפולה של a,b ולכן $s\geq[a,b]=ab$, וזו סתירה להנחה ש-$s<n$. ■

2 חבורות לא אבליות \ קומטטיביות

דוגמה ראשונה לחבורה שכזו היא חבורת התמורות של n איברים.

באלגברה לינארית, למדנו כי מטריצה A היא למעשה טרנספורמציה במסווה. כלומר היא מגדירה $T:\mathbb{R}^n\to\mathbb{R}^m$ ע"י $T\overline{x}=A\overline{x}$.

במובן של מכפלת מטריצות, אם יש לנו 2 מטריצות A,B שמגדירות טרנספורמציות S,T, אזי מכפלת המטריצות היא הרכבת הטרנספורמציות: $S(T(\overline{x}))=(B\cdot A)\overline{x}$.

לא בהכרח שההרכבה של 2 הטרנספורמציות תצא אותו דבר, דהיינו המכפלה של המטריצות , או ההרכבה של הטרנספורמציות (ושל פונקציות בכללי) היא אינה קומטטיבית.

2.1 חבורת התמורות עם פעולת ההרכבה

הגדרה 4. נסמן $[n]=\{1,2,\dots n\}$. לשתי פונקציות: $f,g:[n]\to[n]$ נגדיר $f\circ g:[n]\to[n]$ להיות $f\circ g(k)=f(g(k))$.

הגדרה 5. נסמן: I - פונקצית הזהות. כלומר $I(k)=k$.

לכן יתקיים $f\circ I=I\circ f=f$. זה למעשה יהיה האיבר האדיש שלנו בחבורה.

הגדרה 6. פונקציה $f:[n]\to[n]$ נקראת תמורה, אם f חח"ע ועל.

אם f תמורה אז קיימת ההופכית שלה f^{-1}המוגדרת על ידי: $f^{-1}=\{(j,i):(i,j)\in f\}$ (בכתיב יחסים). או אם $f(i)=j$ אז $f^{-1}(j)=i$. מתכונה זו יתקיים $f(f^{-1}(i))=i$ ולכן $f\circ f^{-1}=I$.

נשים לב שמכל ההגדרות האלה למעשה הרכבנו חבורה ביחס לפעולת ההרכבה של התמורות.

הגדרה 7. חבורת התמורות על n איברים ($[n]$) נקראת החבורה הסימטרית על $[n]$ ומסומנת ב: S_n.

דוגמה. עבור $n=1$. החבורה הסימטרית היא קבוצה המכילה אך ורק את I ולכן $|S_1|=1$.

עבור $n=2$ יש לנו 3 תמורות שטובות ל-S_2 ולכן $|S_2|=3$.

הגדרה. נסמן סימון זמני (ופרמטיבי) לתמורות בעזרת:

$$\begin{pmatrix} 1 & 2 & \cdots & n \\ \alpha(1) & \alpha(2) & \cdots & \alpha(n) \end{pmatrix}$$

.

ב-S_3 יהיו לנו 6 מטריצות כאלה ולכן 6 תמורות שונות.

הגדרה. הסימון המעגלי לתמורות. מהתכונה שהרכבת α שוב ושוב נחזור בחזרה למקור (כלומר ניצור מעין מעגל) ניתן לסמן את התמורה באופן הבא: $S_6=(1,2,4,6)\cdot(3,5)$ כאשר $\alpha(1)=2,\alpha(2)=4,\alpha(4)=6,\alpha(6)=1$. באופן דומה $\alpha(3)=5,\alpha(5)=3$. כל האיברים שלא מופיעים בכל המעגלים הם למעשה "מעגל משל עצמם" או "נשארים במקומם".

מעניין לראות כי הכפל בסימון בין הוקטורים הוא באמת כפל תמורות. בנוסף, הכפל הוא אינו קומטטיבי כמובן מאליו, רק במקרים מסויימים:

דוגמה. עבור $\alpha \in S_3 : (1,2)$ ועבור $\beta \in S_3 : (1,3)$ מתקיים כי $\alpha\beta \neq \beta\alpha$. מעניין לראות כי אם ניקח $\alpha \in S_4 : (1,2)$ ואת $\beta \in S_4 : (3,4)$ נקבל כי $\alpha\beta = \beta\alpha$ כלומר המכפלה כן קומטטיבית. זה נובע מהעובדה כי המעגלים "זרים". עוד מקרה מעניין בו הכפל קומטטיבי: $\alpha = (1,2,3)$ מתקיים $(1,2,3)\,(1,2,3) = (1,3,2)$.

הערה. נזכיר את המונח צמוד או הצמדה. נאמר ש-α צמודה לתמורה β אם $\alpha\beta\alpha^{-1} = \beta$.

טענה. אם מתקיים $\beta(i) = j$ אז $\alpha\beta(i) = \alpha(j)$ או $\alpha\beta\alpha^{-1}(\alpha(i)) = \alpha(j)$

טענה. אם $\beta = (1,2)(3,4,5)(6,7)$. אז הצמדה שלה לתמורה α מקיימת: $\alpha\beta\alpha^{-1} = (\alpha(1),\alpha(2))\cdot(\alpha(3),\alpha(4),\alpha(5))\cdot(\alpha(6),\alpha(7))$. כלומר בכתיבה מעגלית $\alpha\beta\alpha^{-1}$ מתקבל מ-β על ידי החלפת כל i ב-$\alpha(i)$.

3 סדר של תמורות

מהו הסדר של $\beta = (1,2,3,4,5)$? ניתן לראות מחישוב קצר כי $\beta^5(i) = i$ לכל $i \in \beta$ ולכן $\beta^5 = I$, כלומר $o(\beta) = 5$.

דוגמה נוספת: $\beta = (1,2)(3,4,5)$. מתקיים: $\beta^2 = (1,2)(3,4,5)(1,2)(3,4,5) = (1,2)(1,2)(3,4,5)(3,4,5) = (1,2)^2(3,4,5)^2$. עבור $(1,2)^2 = I$ אך $(3,4,5)^2 \neq I$.

מהדוגמה לעיל ניתן לראות כי במקרה כזה הסדר יהיה ה-$gcd(i,j)$.

טענה 8. אם $\beta = (c_1)(c_2)\ldots(c_t)$ מכפלה של t מעגלים זרים. אזי $o(\beta) = l.c.m(|c_1|,|c_2|,\ldots,|c_t|)$