שיעור חבורות – מחנה אביב תשע"ד – קבוצת ירדן

מטרות

1. להכיר את המושג חבורה.
2. לראות דוגמאות חשובות של חבורות.
3. לפתור חידות עם קשר לחבורות.

מהלך

הקדמה לשיעור –

הנושא שנלמד היום הינו מחוץ לסילבוס של האולימפיאדה. ברגע שנאמרת אמירה כזו צריכה לעלות השאלה: "אז למה יש הרצאה בנושא?". ובכן, אני מתכוון לתת שתי תשובות לשאלה הזאת.

א) מי שכותבים את האולימפיאדות הם מתמטיקאים והם יודעים מה זאת חבורה. יותר מזה, הם בונים חידות שהניסוח שלהן אלמנטרי (וניתן לפתור אותן באופן אלמנטרי) שמסתתרות בהן חבורות. לכן הכלי הזה מסוגל להיות לעזר.
ב) חבורות הן הכללה שעוזרת להבין תוצאות שמוכרות לכם מתורת המספרים וקומבינטוריקה בלי "לעבוד קשה".
ג) יש חידות שזה יעזור לכם לפתור, ויותר מזה, אחרי שתכירו מספר חבורות חידות מסוימות יקפצו לכם ישר כקשורות לחבורות.

<u>אקספוזיציה</u>:

- בסדרת האנימציה פיוצ'רמה, פרק 98 עונה 6, הפרופסור ואיימי בונים מכונה שמחליפה מוחות בין גופים. הבעיה במכונה, היא שאם היא החליפה בין שני אנשים היא לא יכולה לבצע חילוף בין אותו זוג של אנשים בדיוק. לאחר שהחליפו 10 אנשים מוחות ביניהם הם ניסו לתקן את הבעיה.
  האם אפשר לסדר את המוחות מחדש באמצעות המכונה עם עוד אדם אחד שיתנדב לעזור?
  האם אפשר לסדר מחדש באמצעות שני אנשים?
- מה התוצאה של $7^{130} \bmod 1020$?
- נתון פאון משוכלל עם n קודקודים וk פאות סביב כל קודקוד. נסכום את כמות הקודקודים שמופיעים בכל מישור סימטריה של הפאון. כמה יוצא הסכום?

כל השאלות הנתונות פה דנות ביצור מיוחד מאד במתמטיקה שנקרא **<u>חבורה</u>**.

הגדרות ודוגמאות

אז מה זאת חבורה?

<u>חבורה:</u> נתונה קבוצה של איברים G ופעולת "כפל" בין האיברים הללו $_\cdot_ : G\times G\to G$ כך שהתנאים הבאים מתקיימים –

א) לכל שלושה איברים $(a\cdot b)\cdot c = a\cdot(b\cdot c)$. – אסוציאטיביות.
ב) קיים איבר שנסמנו e שמקיים $a\cdot e = e\cdot a = a$ לכל $a\in G$ - קיום נייטרלי.
ג) לכל איבר $a\in G$ יש איבר $a^{-1}\in G$ שמקיים $aa^{-1} = a^{-1}a = e$ - קיום הפכי.

אנחנו בשיעור היום נדבר (בעיקר) על חבורות סופיות ($|G|<\infty$).

<u>הדוגמאות הקלאסיות לחבורות מגיעות מעולם הסימטריה, ובכלל, חבורות מעניינות כי הן פועלות על קבוצות (או עצמים).</u>

- <u>חבורה דיהדרלית</u>: כל הסימטריות של מצולע משוכלל. (ומה חבורת הסימטריה של פאון?) <u>חבורה דיהדרלית ויקי</u>
- <u>חבורת סימטריה (תמורות)</u>: כל הדרכים לסדר n אנשים בשורה. <u>חבורה סימטרית ויקי</u>

- השלמים, חשבון שאריות. חבורה ציקלית ויקי
- הזזות, שיקופים וסיבובים במרחב. איזומטריות

כעת החידה הראשונה מקבלת ניסוח מדוייק יותר – האם ניתן למצוא הפכי לתמורה כלשהי ב S_{10} שלא משתמשת באיברים מ S_{10} בתוך S_{11}? ובתוך S_{12}?

די ברור ש S_{10} חיה בתוך S_{11} שחיה בתוך S_{12}.

זה מיד מעלה את השאלה איזה חבורות קטנות יותר חיה בתוך חבורה מסויימת?

לתופעה הזאת קוראים – **תת-חבורה**.

הגדרה מדוייקת: תת חבורה של חבורה G זאת תת קבוצה H שהיא חבורה ביחס לאותה פעולת כפל.

דוגמא: חבורת הסיבובים בתוך החבורה הדיהדרלית.

דוגמא חשובה: החזקות של כל איבר $a \in G$ הן חבורה ומסומנת $\left\{e, a, a^2, ..., a^t\right\} = \left\langle a \right\rangle \leq G$. למספר האיברים בחבורה הזאת קוראים "הסדר של a".

עכשיו, אם יש לנו תתי חבורות, אנחנו יכולים לשאול את השאלה הבאה על איברים: בהנתן שני איברים $x, y \in G$ האם יש איבר בתת חבורה שמעביר אותם אחד לשני מימין, כלומר - $\exists h \in H : x = yh$. מסמנים זאת ב $x \equiv_L y \bmod H$

די קל לראות שהתכונה הזאת מחלקת את החבורה ל"מחלקות שקילות" (מחלקות שקילות זה חלוקה של החבורה לקבוצות זרות).

נראה כי זה יחס שקילות:

רפלקסיביות -

$e \in H$ ולכן $x = ex$ כלומר $x \equiv_L x \bmod H$.

סימטריה -

נניח $x \equiv_L y \bmod H$ אזי $\exists h \in H : x = yh$. H תת חבורה אז יש בה את h^{-1}. נכפול את שני האגפים ב h^{-1} מימין ונקבל – $xh^{-1} = y$. לכן $y \equiv_L x \bmod H$.

טרנזיטיביות – $x \equiv_L y, y \equiv_L z$. אזי $x = yh_1; y = zh_2$ לכן $x = zh_2h_1$ ולכן $x \equiv_L z$.

לכל נציג של מחלקת שקילות כזאת קוראים מחלקה שמאלית של H (left co-set) ומסמנים אותו בתור $xH = \left\{y \in G \mid \exists h \in H : y = xh\right\}$, באופן דומה מגדירים מחלקות ימניות.

דוגמאות למחלקות ביחס לתת חבורות:

- השלמים ביחס לשלמים כפול 5. (מראה סימון מקובל של מודולו)
- $\left\{0, 4\right\} \leq C_8$.

תוצאה נוספת - שנובעת ישירות מההגדרה של מחלקות ביחס לתת חבורה היא שלכולן יש בדיוק אותה עוצמה (אותה כמות איברים).

נראה זאת:

נגדיר פונקציה $\varphi: H \to xH$ באופן הבא $\varphi(h) = xh$. זה מוגדר היטב כי כפל מוגדר היטב. זה הפיך (לכן חח"ע ועל) כי נכפול בx^{-1} ונקבל את ההפכית.

העובדה הזאת על המחלקות גוררת ישירות את המשפט החשוב הבא שנקרא על שם המתמטיקאי מהמאה ה18 לגראנז':

משפט לגראנז'

מספר האיברים בתת חבורה מחלק את כמות האיברים בחבורה.

לכמות הקוסטים קוראים האינדקס של תת החבורה ומסמנים אותו ב$[G:H]$. מתקיים $|G| = |H| \cdot [G:H]$.

תרגיל

כל חבורה עם מספר ראשוני של איברים היא חבורת החזקות של איבר מסויים (השם של חבורות כאלה הוא ציקליות – כמו חבורת הסיבובים של המצולעים).

תרגיל

נובע גם שהסדר של כל איבר מחלק את גודל החבורה.

מסקנה מהתרגיל

תהא G חבורה. יהא $a \in G$ כלשהוא. אזי $a^{|G|} = e$.

אחרי כל ההגדרות וההבנות שהבנו על חבורות אנחנו מגיעים לחקור את החבורות הספציפיות שעלו באקספוזיציה:

חבורת השאריות מודולו

השאלה המרכזית עליה נענה בחלק זה היא – בהנתן n כלשהו. מהו המספר שבוודאות יקיים $a^{\lambda(n)} \equiv 1 \bmod n$ לכל a שזר ל n.

נקבע n מספר שלם.

נביט בקבוצה $\frac{\mathbb{Z}}{n\mathbb{Z}} = \{\overline{0}, \overline{1}, ..., \overline{n-1}\}$.

ביחס לחיבור זאת חבורה עם הנייטרלי 0.

ביחס לכפל זאת לא חבורה (כי ל0 אין הפכי).

בכל זאת, נסמן בU_n את כל האיברים ההפיכים ביחס לכפל ב$\frac{\mathbb{Z}}{n\mathbb{Z}}$ (כלומר כל האיברים שזרים לn מתוך קבוצת האיברים).

זאת תהיה חבורה ביחס לכפל והנייטרלי שלה יהיה 1.

דוגמא $U_8=\{1,3,5,7\}$.

כעת, ב $\frac{\mathbb{Z}}{n\mathbb{Z}}$ ברור כמה איברים יש, אבל ב U_n לא ברור במבט ראשון כמה איברים יש.

כמה יהיה ב U_{10}? וב U_{100}?

השאלה הזאת שקולה לשאלה כמה איברים זרים ל n ב $\frac{\mathbb{Z}}{n\mathbb{Z}}$?

לפונקצייה שלכל מספר n אומרת כמה איברים יש ב U_n נקראת פונקציית אויילר ומסמנים אותה ב $\varphi(n)$.

אחרי שנגלה איך מחשבים בדיוק את הפונקציה הזאת נקבל בחינם את **משפט אויילר:**

משפט אויילר

אם $\gcd(a,n)=1$ אז $a^{\varphi(n)}\equiv 1 \bmod n$.

אם n ראשוני כמה שווה $\varphi(n)$? זה קל, כל איבר חוץ מ0 זר ל n ולכן $\varphi(n)=n-1$.

שימו לב שזה גורר לי ישר (בלי שום מאמץ) את **המשפט הקטן של פרמה**:

משפט – הקטן של פרמה

אם $\gcd(a,n)=1$ ו- n ראשוני אזי $a^{n-1}\equiv 1 \bmod n$.

אם $n=p^k$ ו- p ראשוני כמה שווה $\varphi(n)$?

זה שוב לא קשה מדי:

איבר יהיה זר ל p^k אם הוא זר ל p.

בין כל p איברים רצופים יש בדיוק אחד שהוא כפולה של p.

לכן יש סך הכל p^{k-1} איברים שלא זרים ל p.

ולכן $\varphi(n)=p^k-p^{k-1}=n\left(1-\frac{1}{p}\right)$.

ועבור n כללי מה יהיה $\varphi(n)$?

באמצעות משפט השאריות הסיני אפשר להוכיח כי $U_{mn}=U_m\times U_n$ כאשר $\gcd(m,n)=1$ (כלומר m ו- n זרים).

כלומר, אם אומרים לי כמה שווה $x \bmod 3$ וכמה שווה $x \bmod 17$ אני אדע ישר לומר לכם למה שווה $x \bmod 51$.

לכן עבור $n=p_1^{t_1}\dots p_k^{t_k}$ נקבל $U_n=U_{p_1^{t_1}\dots p_k^{t_k}}=U_{p_1^{t_1}}\times\dots\times U_{p_k^{t_k}}$ ובפרט

$$\varphi(n)=|U_n|=\left|U_{p_1^{t_1}}\right|\cdot\dots\cdot\left|U_{p_k^{t_k}}\right|=\prod_{i=1}^{k}p_i^{t_i}\left(1-\frac{1}{p_i}\right)=n\prod_{i=1}^{k}\left(1-\frac{1}{p_i}\right).$$

לדוגמא עבור 100 - $\varphi(100)=100\cdot\left(1-\frac{1}{2}\right)\left(1-\frac{1}{5}\right)=100\cdot\frac{1}{2}\cdot\frac{4}{5}=40$.

ישר נובע מזה שכל איבר מודולו 100 אם נעלה אותו בחזקת 40 נקבל 1.

מהי $\varphi(1020)$?

$1020=3\cdot4\cdot5\cdot17$ ולכן $\varphi(1020)=1020\cdot\frac{1}{2}\cdot\frac{2}{3}\cdot\frac{4}{5}\cdot\frac{16}{17}=256$. אז $7^{256}\equiv1\bmod1020$ אבל עוד אין לנו מושג לגבי 7^{130} ...

עבור 8 כל איבר ב U_8 הוא מסדר 2 למרות ש $\varphi(8)=8\cdot\frac{1}{2}=4$. השאלה האם יש פונקצייה שמוצאת בדיוק מה החזקה שמקיימת שכל איבר בחזקת התוצאה מודולו n יהיה 1?

לפונקצייה זו קוראים פונקציית למבדה ומחשבים אותה באופן הבא:

$$\lambda\left(2^s p_1^{t_1}\ldots p_k^{t_k}\right)=\begin{cases}lcm\left(2^{s-2},\left(p_i-1\right)p_i^{t_i-1}\right), s>2\\ lcm\left(2^{s-1}\left(p_i-1\right)p_i^{t_i-1}\right), s=1,2\\ lcm\left(\left(p_i-1\right)p_i^{t_i-1}\right), s=0\end{cases}.$$

קל להבין למה היא נכונה אם מאמינים לפירוק ממקודם $U_n=U_{p_1^{t_1}\ldots p_k^{t_k}}=U_{p_1^{t_1}}\times\ldots\times U_{p_k^{t_k}}$ ואומרים שמספיק לנו לקבל 1 בכל קואורדינטה.

אז מי זאת $\lambda(1020)$?

$\lambda(1020)=lcm(2,2,4,16)=16$ ולכן $7^{16}\equiv1\bmod1020$ והפתרון לחידה מתחילת השיעור ברור.

החבורה הדיהדרלית ומשפט ברנסייד

כפי שאמרתי בתחילת השיעור, חבורה היא מעניינת כי היא פועלת על קבוצה –

הגדרה

יהיו G חבורה ו- X קבוצה.

אם כל איבר ב G מגדיר תמורה על X,

<u>ומתקיים</u>: $e=Id_X$, $g\circ g^{-1}=Id_X$,

נאמר כי G פועלת על X.

עכשיו אפשר לשאול את השאלות המעניינות הבאות:

1. עבור $x\in X$ כלשהו מי האיברים שאליהם x נשלח?
2. עבור $x\in X$ כלשהו מי האיברים של החבורה שלא מזיזים אותו?
3. עבור $g\in G$ מי האיברים שהוא לא מזיז?

התשובה לשאלה הראשונה נקראת "המסלול של x" מסומן $Orb(x)$, התשובה לשאלה השנייה נקראת "המייצב של x" מסומן $stab(x)$, התשובה לשאלה השלישית נקראת "נקודות השבת של g" ומסומנת ב- $Fix(g)$.

טענה

נניח G חבורה שפועלת על הקבוצה X. אזי לכל $x \in X$ $stab(x)$ היא תת חבורה של G.

הוכחה

תרגיל

משפט

מספר האיברים במסלול של איבר שווה לאינדקס של המייצב שלו בחבורה. כלומר $|Orb(x)| = [G : stab(x)]$.

הוכחה

יהא $x \in X$. נראה כי כל קוסט של התת חבורה $stab(x)$ נותן איבר יחיד במסלול:

אם $g \in stab(x)$ אז לפי הגדרה $g(x) = x$ ולכן אף אחד מהם לא תורם למסלול איברים.

יהא $h \notin stab(x)$. אזי מהגדרה $h(x) = y \neq x$ אבל y במסלול של x.

לכל איבר $g \in h \cdot stab(x)$ מתקיים $g = hs : s \in stab(x)$ ולכן $g(x) = h \cdot s(x) = h(x) = y$.

מזה למדנו שלכל קוסט יש רק איבר אחד שמקבלים והוא לא x.

לכן כמות הקוסטים היא בדיוק אורך המסלול וכמות הקוסטים היא האינדקס $[G : stab(x)]$.

<u>עכשיו גם אפשר לענות די בקלות על השאלה שלנו של הפאון:</u>

קודם כל נראה שחבורת הסימטריות שפועלת על הפאון היא מהצורה הבאה – כל קודקוד אפשר לקחת לכל קודקוד (סה"כ n אפשרויות) ואז סביב כל קודקוד יש k פאות שביניהן אפשר להפעיל כל פעולה של החבורה הדיהדרלית D_k. לכן סך הכל יש $2nk$ סימטריות על פאון כנ"ל.

ניתן לתרגם כעת את השאלה לשאלה על מייצבים: איזה שיקופים מייצבים קודקוד מסויים?

תרגמנו את השאלה מספירה לפי מישורים לספירה לפי קדקודים (שתי דרכים לספור).

כעת, אם קודקוד מסויים נשאר במקום נשאר להפעיל את D_k על הפאות שלו. מתוך D_k יש k שיקופים (שהם, אם לא הזזנו את הקודקוד הנ"ל, מישורי סימטריה של המצולע).

לכן סך הכל הסכום יוצא nk.

הרבה פעמים חשוב לנו לספור כמה מסלולים יש בפעולה של חבורה על קבוצה. דוגמה קלאסית –

<u>יש כרטיסי ניקוב 3X3. כמה דרכים יש לנקב אותם בלי שיהיה אפשר להפוך ולסבוב כרטיס אחד לאחר?</u>

התשובה תהיה באמצעות המשפט הבא.

ברנסייד

תהי G חבורה הפועלת על קבוצה X .

נסמן $\mathrm{Fix}(g) = \{x \in X | g(x) = x\}$, כלומר כל האברים ש g משאיר במקום.

כמו כן, נסמן ב N את מספר ה[מסלולים] .

אזי מתקיים:

$$N = \frac{1}{|G|} \sum_{g \in G} |\operatorname{Fix}(g)|$$

כלומר - מספר המסלולים הוא ה[ממוצע] של גדלי הFix.

הוכחה

ההוכחה למשפט הזה משתמשת במושג האהוב עלינו כל כך מעולם האולימפיאדות: "שתי דרכים לספור".

ניקח את קבוצת כל הזוגות (g,x) שמקיימים $g(x)=x$. כלומר, מבחינת x האיבר g במייצב ומבחינת g האיבר x נקודת שבת.

סימון מקובל: $A=\{(g,x) \mid g \in G, x \in X, g(x)=x\}$.

כעת נספור כמה איברים יש בA: אפשר לספור זאת כשרצים על כל הx-ים ואפשר כשרצים על כל הg-ים. כלומר-

$$\sum_{g \in G} |Fix(g)| = |A| = \sum_{x \in X} |stab(x)| .$$

המייצב של איבר הוא תת חבורה ולכן הוא תמיד מגודל החבורה חלקי האינדקס, כלומר $|stab(x)| = \frac{|G|}{[G : stab(x)]}$.

מצד שני, אמרנו כבר כי אורך המסלול הוא בדיוק האינדקס של תת חבורה ולכן $|stab(x)| = \frac{|G|}{|Orb(x)|}$.

לכן - $\sum_{g \in G} |Fix(g)| = \sum_{x \in X} \frac{|G|}{|Orb(x)|}$.

נחלק ב$|G|$ ונקבל - $\frac{1}{|G|} \sum_{g \in G} |Fix(g)| = \sum_{x \in X} \frac{1}{|Orb(x)|} = \sum_{[x] \text{ an orbit}} \underbrace{\left(\frac{1}{|Orb(x)|} + \ldots + \frac{1}{|Orb(x)|} \right)}_{|Orb(x)| \text{ times}} = N$

חידה

תהא G חבורה סופית. מה ההסתברות ששני איברים שנבחרו באקראי Gמ יתחלפו (יקיימו $ab = ba$)? (השתמשו בפעולת ההצמדה של החבורה על עצמה כלומר כל איבר פועל על החבורה באופן הבא: $g(h) = g^{-1}hg$). הנוסחא להסתברות משתמשת רק בגודל החבורה ובמספר המסלולים ביחס להצמדה.

פתרון

נביט במרחב ההסתברות – זוגות של איברים Gמ שהסדר משנה. ונביט בפעולה של G על עצמה לפי הצמדה (כלומר $g(h) = g^{-1}hg$)

אזי זוג $g,h\in G$ יתחלף אם אמ"מ $g\in Fix(h)$ וגם $h\in Fix(g)$. נראה זאת –

$$g\in Fix(h)\Leftrightarrow h(g)=g\Leftrightarrow h^{-1}gh=g\setminus h\cdot\Leftrightarrow gh=hg.$$

לכן אפשר לספור את כל הזוגות שמקיימים את התנאי הזה באופן הבא - $\sum_{g\in G}|Fix(g)|$.

מצד שני, יש סך הכל $|G\times G|=|G|^2$ זוגות. לכן ההסתברות היא: $\frac{N}{|G|}=_{Burnside}\frac{\sum|Fix(g)|}{|G|^2}$.

חידה

ניקח מצולע משוכלל עם p צלעות (p ראשוני גדול מ3). כמה משולשים יש במצולע עד כדי סימטריה?

פתרון

בעצם אנחנו צריכים לבדוק כמה מסלולים יש לצביעה של כל 3 קודקודים של המצולע. כלומר:

X= קבוצת כל השלישיות של מספרים (קודקודים) בין 1 לp בלי חשיבות לסדר.

G= D_p.

ב D_p יש p-1 סיבובים והם ודאי לא משאירים אף שלישייה במקום (אחרת המרחק בין כל שני קודקודים היה שווה ואז p היה כפולה של 3).

הזהות משאירה את כולם במקום (כולם זה $\binom{p}{3}=\frac{p(p-1)(p-2)}{6}$)

שיקופים משאירים את כל המשולשים השווי שוקיים שהקודקוד שאינו על הבסיס שלהם נמצא על ישר השיקוף. נספור כמה כאלה יש לפי קודקודים:

אם קודקוד מסויים נמצא על ישר שיקוף, יש לו $\frac{p-1}{2}$ זוגות של קודקודים שיחד איתו ייצרו משולש שוו"ש.

יש p קודקודים כאלו (ואי אפשר לספור פעמיים אף אחד אחרת היה משולש שוו"צ ואין כזה מהטיעון של הסיבובים).

לכן יש - $p\cdot\frac{p-1}{2}$ נקודות שבת ביחס לשיקופים.

סך הכל קיבלנו - $\sum|Fix(G)|=\frac{p(p-1)}{2}+\frac{p(p-1)(p-2)}{6}$ ו- $|G|=2p$. לכן –

$$N=\frac{\frac{p(p-1)}{2}+\frac{p(p-1)(p-2)}{6}}{2p}=\frac{3(p-1)+(p-1)(p-2)}{12}=\frac{p^2-1}{12}.$$

תוצאה מעניינת (וקלה לבדיקה) היא ש $\frac{p^2-1}{12}$ הוא מספר שלם לכל ראשוני גדול מ3.

חידה

נתונה טבלה 7X7 מהצורה $\begin{pmatrix} 1 & 2 & \dots & 7 \\ 7 & 1 & \dots & 6 \\ \dots & & & \\ 2 & 3 & \dots & 1 \end{pmatrix}$.

כמה דרכים יש לסדר אותה מהחלפת שורות ועמודות?

פתרון

<u>דרך א'</u>:

מקיימת חוק המלבנים (סכום האלכסונים מודולו 7 קבוע) ולכן אם קבעת שורה ראשונה ועמודה ראשונה קבעת את כל הטבלה (!7!6)

<u>דרך ב'</u>:

יש $S_7 \times S_7$ פעולות על הטבלה (פרמוטציות על העמודות והשורות).

אנחנו מחפשים מה אורך המסלול של האיבר הנתון (הטבלה דלעיל).

לפי התנאי $|Orb(x)|=\left[G:stab(x)\right]$ מספיק לגלות מי המייצב של הטבלה. יש לפחות 7 איברים במייצב כי כל סיבוב של הטבלה ביחס לעמודות ולשורות נותן איבר במייצב ויש 7 כאלה.

קל לבדוק שלאן שנשלח את השורה הראשונה יהיו חילופי עמודות ושורות שיחזירו אותנו למצב המקורי ויש רק אוסף אחד כזה של פעולות. לכן יש 7 איברים במייצב וזהו. לכן $|Orb(x)|=\frac{(7!)^2}{7}$.

תמורות

דרכים יעילות להציג תמורות.

פירוק תמורות למעגלים.

פירוק תמורות לחילופים.

פתרון לחלק א' של פיוצ'רמה

אי אפשר באמצעות אדם אחד נוסף למצוא הפכי.

למה? כי ברגע שנשים את האדם החדש (נסמנו x) בגוף כלשהו הוא כלוא שם. אי אפשר להחזיר אתה המוח של x לגוף שלו כי זה חילוף שהשתמשנו בו ואי אפשר להעביר אותו לגוף אחר כי זה חילוף מהקבוצה שאסור להשתמש בה.

פתרון לחלק ב' של פיוצ'רמה

/http://www.gadial.net/2010/09/14/futurama_and_group_theory

חידה

p_k מספר התמורות על n איברים עם k נקודות שבת.

תוכיחו

א) $\sum kp_k = n!$.

ב) $\sum_{k=0}^{n}\binom{k}{l}l!\,p_k = n!$ עם $1 \le l \le n$ קבוע.

פתרון

נפתור את א' בשתי דרכים. ב' יישאר כתרגיל:

<u>דרך ראשונה</u>: "שתי דרכים לספור"

נשים לב כי אם אנחנו רוצים לספור את "כל המופעים של נקודת שבת בכל התמורות" אפשר לעשות את זה לפי תמורות ולפי נקודות.

לפי תמורות, בכל תמורה מסוג p_k יש k נקודות שבת. לכן כדי לספור את כל המופעים צריך לרוץ על כל הkים ולקבל - $\sum_{k=0}^{n} kp_k$.

מצד שני אם נספור לפי נקודות, אם נקודה מסויימת נשארת במקום יש עוד $(n-1)!$ סידורים של השאר. לכן כל נקודה מופיעה ב $(n-1)!$ תמורות כנקודת שבת ואם סוכמים על כל הנקודות מקבלים $n\cdot(n-1)! = n!$.

<u>דרך שנייה</u>: ברנסייד

נשים לב שחבורת התמורות S_n פועלת על הקבוצה $\{1,\dots,n\}$ באופן טבעי.

לפי ברנסייד: $N \mid S_n \mid = \sum_{g\in S_n}\left|Fix(g)\right|$.

לכל נקודה יש תמורה שמעבירה אותה לכל נקודה אחרת ולכן יש מסלול יחיד $(N=1)$

כמות האיברים ב S_n הוא $n!$.

ולכל תמורה שנמצאת ב p_k יש k נקודות שבת ולכן $\sum_{g\in G}\left|Fix(g)\right| = \sum_{k=0}^{n}\sum_{g\in p_k} k = \sum_{k=0}^{n} kp_k$.

סך הכל $n! = \sum_{k=0}^{n} kp_k$.

סעיף ב' הוא באותו כיוון וברנסייד פותר אותו עבור פעולה של S_n על קבוצות אחרות (חשבו איזה קבוצה מתאימה לכל l).

חידה

נתון מעגל עם נקודות כחולות ואדומות עליו. בכל תור מותר להוריד ממנו נקודה כחולה וזה משנה את שתי הנקודות שלצידו לצבע הנגדי להן או להוסיף נקודה כחולה וזה משנה את שתי הנקודות שלצידו לצבע הנגדי להן.

הוכיחו כי לא ניתן להגיע ממצב של שתי נקודות כחולות למצב של שתי נקודות אדומות באמצעות הפעולות הללו.

פתרון

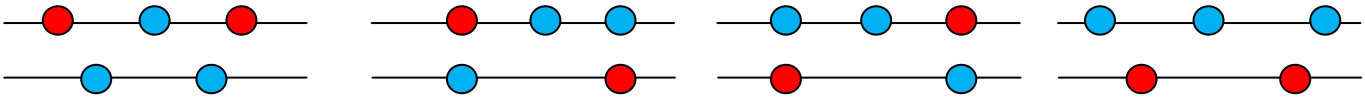
<u>חידות מסוג זה מסוגלות להיות תמימות עם איזה אינווריאנט פשוט. אך לא זו. מסתתרת פה חבורה באופן עמוק.</u>

תחילה, ניתן לשים לב כי הזוגיות של הנקודות האדומות היא אינווריאנט של המערכת.

אבל זה לא פותר את החידה.

מי שחד מאד שם לב כי יש את האינווארינט הבא: הלוח מתחלק לתחומים לפי הנקודות האדומות. הסכום המתחלף של מספר הנקודות הכחולות בכל התחומים לפי סדר היא אינווארינט מודולו 3. כעת קל לראות שבמצב הראשון יש לנו 2mod3 ובמצב השני 0mod3. אבל מאיפה הגיע האינווארינט המשוגע הזה?!

<u>קודם כל נראה שזה נכון</u>:



אלו כל המעברים האפשריים (אפשר לעבור מלמעלה למטה ולהיפך). תבדקו ותראו שהם שומרים על האינווארינט.

אבל איך כל זה קשור לחבורות?!

תחילה נשים לב כי אפשר במקום כחול ואדום לדבר על איברים של חבורות על מעגל.

נזכר בחבורה הדיהדרלית של המשולש. אמרנו שיש בה סיבוב a ושיקוף σ ושהקשר ביניהם הוא $\sigma a = a^2\sigma, a^3 = e, \sigma^2 = e$. נשים לב שהשוויונות הבאים מתקיימים עליהם:

$$I.\ aaa = e = \sigma\sigma$$
$$II.\ \sigma a\sigma = \sigma\sigma a^2 = aa$$
$$III.\ \sigma aa = a\sigma$$
$$IV.\ aa\sigma = a^2\sigma = \sigma a$$

זה בדיוק השקילות על נקודות כחולות ואדומות שלנו!!!! כשסיבוב זו נקודה כחולה ושיקוף אדומה.

כלומר, אם נסתכל על מעגל כמכפלה של איברי חבורה לפי הצבעים, הפעולות לא משנות את האיבר. אבל מאיפה צריך להתחיל לכפול את המעגל? כלומר אם יש רק נקודה כחולה ואדומה לא ברור אם המילה היא σa או $a\sigma = \sigma a^2$?!?!?!

זה לא הורס לנו את האינווריאנט לגמרי, כי המקום בו נתחיל לא משנה את "מחלקת הצמידות" של האיבר שמצאנו, נראה זאת: $a \cdot word \sim a^{-1} \cdot a \cdot word \cdot a = word \cdot a$, $\sigma \cdot word \sim \sigma \cdot \sigma \cdot word \cdot \sigma = word \cdot \sigma$.

לכן מצאנו אינווריאנט של החבורה! הפעולה לא יכולה לשנות את מחלקת הצמידות של המילים שהמעגל מבטא!

אז בואו נראה שמחלקת הצמידות של σ^2 היא לא אותה מחלקה כמו של a^2 וסיימנו: $\sigma^2 = e$ ולכן הוא האיבר היחיד במחלקת הצמידות של עצמו, $a^2 \neq e$ ולכן הוא לא שם.