הגדרה. תהי G חבורה שפועלת על קבוצה X. לכל $g \in G$ מסמנים ב$fix(g) = X^g = \{x \in X : gx = x\}$ נקודות השבת של g.

למה. הלמה של ברנסהייד: נניח שG פועלת על X. נסמן בk את מספר המסלולים בפעולה. אז מתקיים

$$|G|k = \sum_{g \in G} |fix(g)|$$

בפרט אם G חבורה סופית אז

$$k = \frac{1}{|G|} \sum_{g \in G} |fix(g)|$$

תרגיל. תהי G חבורה סופית לא טריוויאלית שפועלת טרנזיטיבית על קבוצה X בת יותר מאיבר. (כלומר, שיש רק מסלול אחד). הוכיחו שקיים $g \in G$ כך ש$fix(g) = \emptyset$.

פתרון. לפי הלמה של ברנסהייד

$$|G| = \sum_{g \in G} |fix(g)|$$

אם אין g כך ש$fix(g) = \emptyset$ זה אומר שלכל $g \in G$, $|fix(g)| \geq 1$, ומכיוון שזה שווה למספר האיברים בG, וזה שוויון של סכומים סופיים, אז נקבל שלכל $g \in G$ $|fix(g)| = 1$. אבל יודע ש$fix(e) = X$, ולפי ההנחה $|X| \geq 2$, סתירה.

משפט. משפט קיילי: תהי G חבורה שפועלת על קבוצה X. אז הפעולה מגדירה לנו הומומורפיזם

$$G \to S_{|X|}$$

ההומומורפיזם הנ"ל חח"ע אמ"ם הפעולה נאמנה (האיבר היחיד שפועל טריוויאלית, כלומר משאיר את כל האיברים במקום, הוא איבר היחידה).

אז כל פעם שיש לנו פעולה נאמנה של G על קבוצה X, נקבל שיכון $G \hookrightarrow S_{|X|}$.

לכל חבורה G יש פעולה נאמנה של G על עצמה, ע"י כפל משמאל. לכן תמיד יהיה שיכון

$$G \hookrightarrow S_{|G|}$$

לשיכון הנ"ל נקרא "שיכון קיילי"

דוגמה. $G = D_3$. $|G| = 6$, אז קיים שיכון $D_3 \hookrightarrow S_6$.

נמספר את איברי החבורה.

$$D_3 = \{e, \sigma, \sigma^2, \tau, \tau\sigma, \tau\sigma^2\}$$

הסדר שבו כתבנו הוא בעצם המספור שלהם.

נדגים לאן σ נשלח בשיכון קיילי.

$$\sigma e = \sigma$$

$$\sigma\sigma = \sigma^2$$

$$\sigma\sigma^2 = e$$

$$\sigma\tau = \tau\sigma^2$$

$$\sigma\tau\sigma = \tau$$

$$\sigma\tau\sigma^2 = \tau\sigma$$

$$\sigma \to (1,2,3)(4,6,5)$$

$$\tau \to (1,4)(2,5)(3,6)$$

הערה. (העידון של משפט קיילי) תהי G חבורה ו$H \leq G$. G פועלת על קבוצת המנה G/H ע"י

$$g * (xH) = gxH$$

ולכן נקבל הומומורפיזם

$$G \to S_{[G:H]}$$

אם הפעולה הזאת תהיה נאמנה אז ההומורפיזם יהיה שיכון.
הגרעין של ההומורפיזם הזה הוא $core(H)$. ולכן

$$G/core(H) \hookrightarrow S_{[G:H]}$$

הערה. תהי G חבורה פשוטה שפועלת על X. אז יש הומומורפיזם $G \to S_{|X|}$.
גרעין הוא תת חבורה נורמלית ולכן בגלל שG פשוטה $\ker = G \vee \{e\}$.
הגרעין יהיה שווה לכל G אם ורק אם כל $g \in G$ נשלח לתמורת הזהות. כלומר, הוא משאיר כל $x \in X$ במקום. שזה הפעולה הטריוויאלית: $gx = x$ לכל g ולכל x.
לכן אם יש פעולה לא טריוויאלית של G חבורה פשוטה על איזשהי קבוצה X, ההומורפיזם המתקבל הוא מונומורפיזם, והפעולה נאמנה.

תרגיל. תהי $H \leq A_n$ נאותה $(H \neq A_n)$ עבור $n \geq 5$. הוכיחו ש$[A_n : H] \geq n$.

פתרון. A_n היא פשוטה ולכן $core(H) = \{e\}$. אז נקבל שיכון $A_n \hookrightarrow S_{[A_n:H]}$. לכן $|A_n| \mid |S_{[A_n:H]}|$

$$\frac{n!}{2} \mid [A_n : H]!$$

בשביל שזה יקרה חייב להתקיים ש$n \geq [A_n : H]$. מש"ל.

מסקנה. לA_6 אין תתי חבורות מגודל 360 (אינדקס 2), 240 (אינדקס 3), 180 (אינדקס 4), 144 (אינדקס 5)

תרגיל. נניח שרוצים להכין דגלים שמורכבים מ6 פסים מקבילים כל אחד, ואפשר לצבוע כל פס באחד מקבוצה של 4 צבעים נתונים. תשימו לב שכל דגל ניתן לסובב ואולי לקבל דגל עם צביעה שונה. כמה דגלים שונים אפשר ליצור?

פתרון. הקבוצה X זה וקטורים מאורך 6, עם 4 אפשרויות בכל רכיב, זה שקול ל$\mathbb{Z}_4^6$.
החבורה G שפועלת היא $\mathbb{Z}_2$ כי יש לנו רק פעולה אחת מסדר 2 (להפוך את הדגל). אנחנו רוצים לספור כמה מסלולים שונים יש.

$$k = \frac{1}{2}(fix(0) + fix(1))$$

$$fix(0) = |\mathbb{Z}_4^6| = 4^6$$

1 שומר על הדגלים שבהם הפס הראשון והשישי שווים, הפס השני והחמישי שווים, והפס השלישי והרביעי שווים. כמה דגלים כאלה יש? 4^3.

$$k = \frac{1}{2}(4^6 + 4^3) = 2080$$

תרגיל. תהי G חבורה ו$H \leq G$ מאינדקס m. הוכיחו שיש לG תת חבורה נורמלית K, שמוכל בH, $[G : K] \mid m!$.

פתרון. נקח את $K = core(H) = \bigcap_{g \in G} gHg^{-1}$. אז ידוע ש$K \trianglelefteq G$, ו $K \subseteq H$. כעת מהעידון של משפט קיילי

$$G/K \hookrightarrow S_{[G:H]=m}$$

ולכן $|G/K| \mid |S_m| = m!$. ו$|G/K| = [G : K]$.

תרגיל. תהי G חבורה סופית וp הראשוני הקטן ביותר שמחלק את $|G|$. תהי $H \leq G$ כך ש: $[G : H] = p$. הוכיחו ש$H \trianglelefteq G$.

פתרון. נסמן את $core(H) = K$. אז ידוע ש$[G : K] \mid p!$. בנוסף, האינדקס של תת חבורה תמיד מחלק את גודל החבורה, לכן $[G : K] \mid |G|$.
אם $[G : K] \mid p!$ אז הראשוניים שמשתתפים בו הם מבין המספרים $\{1, ..., p\}$.
מצד שני, אם $[G : K] \mid |G|$ אז כל ראשוני שמחלק את $[G : K]$ מחלק גם את $|G|$.

לכן הראשוני היחיד שמשתתף ב$[G:H]$ הוא p. אבל שום חזקה גדולה מ1 של p לא יכולה לחלק את $p!$, ולכן $[G:K]=p$.

$K\subseteq H$ ומכיוון שיש להם אותו אינדקס נובע שהם שווים. ולכן $K=H$.

קיבלנו שH שווה לתת חבורה נורמלית, לכן H נורמלית. מש"ל.

תרגיל. תהי G חבורה מסדר $2n$ כאשר $(2,n)=1$. הוכיחו שיש לG תת חבורה מאינדקס 2. (ובפרט, כל חבורה מסדר $2n$ עבור n אי זוגי היא לא פשוטה)

פתרון. ראשית, קיים שיכון קיילי $G\hookrightarrow S_{2n}$. אז $G\cong f[G]$, אז מספיק להוכיח של$f[G]$ יש תת חבורה מאינדקס 2.

יש את פונקציית הסימן שמוגדרת $S_{2n}\to\{-1,1\}$.

אפשר להסתכל על הצמצום $f[G]\to\{-1,1\}$

פונקציית הסימן היא הומומורפיזם. צמצום של הומומופריזם הוא גם הומומורפיזם, אז קיבלנו הומומורפיזם

$$f[G]\to\{-1,1\}$$

אם הוא אפימורפיזם אז

$$f[G]/\ker\cong\{-1,1\}$$

ולכן הגרעין יהיה תת חבורה מאינדקס 2.

אז נותר להוכיח שההעתקה היא אכן אפימורפיזם. כלומר, שבתמונה של $f[G]$ יש גם תמורות זוגיות וגם תמורות אי זוגיות. איבר היחידה הוא תמורה זוגית. אז נותר להוכיח שיש תמורה איזוגית.

$|G|=2n$, זוגי, ולכן יש איבר מסדר 2 (עשינו באחד התרגולים). נסמן אותו בx.

נרצה להבין איזה תמורה x יוצר על איברי G ע"י הפעולה של הכפל משמאל.

נשים לב שאם

$$xg_1=g_2$$

אז

$$xg_2=x(xg_1)=x^2g_1=g_1$$

כי x מסדר 2.

אז x עושה חילופים (תמורות מאורך 2) על איברי G.

בנוסף אין איברים שx משאיר במקום, כי אם $xg=g$ אז $x=e$ בסתירה לכך שהוא מסדר 2.

קיבלנו שהתמורה שx יוצר היא מכפלה של n חילופים. הסימן של כל חילוף הוא -1. ומכיוון שיש מספר אי זוגי של חילופים, אז $sign(f(x))=(-1)^n=-1$.

כלומר, $f(x)$ היא תמורה אי זוגית.

מש"ל.

חבורות אוטומורפיזם

הגדרה. תהי G חבורה, $Aut(G)=\{f:G\to G:\text{isomorphism is f}\}$ זאת חבורה עם פעולת ההרכבה.

תרגיל. $Aut(\mathbb{Z}_2 \times \mathbb{Z}_2) = ?$

פתרון. $Aut(\mathbb{Z}_2 \times \mathbb{Z}_2) \cong S_3$. כל אוטומורפיזם משאיר את איבר היחידה במקום.
חוץ מאיבר היחידה יש 3 איברים. אנחנו צריכים להראות שכל תמורה שנעשה על שלושת האיברים הנותרים $(1,0),(0,1),(1,1)$ תגדיר הומומורפיזם.
כל האיברים מסדר 2. לכן לא משנה מה זה $f(x)$, בכל מקרה $f(x+x) = f(x) + f(x)$.
נשים לב שכל שניים מבין שלושת האיברים האלו- הסכום שלהם הוא האיבר השלישי. לכן, לא משנה איך נגדיר את $f(x)$ ו$f(y)$ כאשר xו y שונים, נקבל ש $x+y$ חייב ללכת לאיבר היחיד שנשאר, ואז

$$f(x) + f(y)$$

זה האיבר היחיד שנשאר מבין $(0,0), f(x), f(y)$. כלומר נקבל ש

$$f(x+y) = f(x) + f(y)$$

הגדרה. חבורת האוטומורפיזמים הפנימיים של G זה חבורת כל האוטומורפיזמים מהצורה γ_g

$$\gamma_g(x) = g^{-1}xg$$

האוטומורפיזמים שמתקבלים ע"י הצמדה. מסמנים ב$inn(G)$

$$inn(G) \cong G/Z(G)$$

תרגיל. חשבו את הגודל של $|inn(G)|$ עבור $G = \left\{ \begin{pmatrix} 1 & a & b \\ & 1 & c \\ & & 1 \end{pmatrix} : a,b,c \in \mathbb{Z}_3 \right\}$

פתרון. $|G| = 3^3 = 27$. G היא חבורת p. ראשית אנחנו יודעים שהמרכז לא טריוויאלי. $|Z(G)| = 3 \vee 9 \vee 27$. החבורה לא אבלית ולכן זה לא 27. ממשפט מהתרגול, לא ייתכן ש$G/Z(G)$ היא ציקלית לא טריוויאלית.
ולכן לא יכול להיות ש$|Z(G)| = 9$ כי אז $|G/Z(G)| = 3$ שזה אומר שזאת חבורה ציקלית לא טריוויאלית, וזה סתירה.
לכן נשאר רק $|Z(G)| = 3$ ומכאן $|inn(G)| = 9$