תזכורת:

G,H חבורות $f:G\to H$ הומומורפיזם אם לכל $g_1,g_2\in G$

מתקיים $f(g_1g_2)=f(g_1)f(g_2)$

הגדרנו גרעין של הומומורפיזם:

$$\ker f=\{g\in G : f(g)=e_H\}\underset{\substack{\text{תת חבורה}\\\text{נורמלית}}}{\trianglelefteq} G$$

לכל $h\in f(G)$ $\quad f^{-1}(h)=g\cdot(\ker f)$ כאשר $g\in f^{-1}(h)$

הגדרות:

יהי $f:G\to H$ הומומורפיזם. הוא נקרא:

1) מונומורפיזם אם f חח"ע

2) אפימורפיזם אם f על

3) איזומורפיזם אם f חח"ע ועל

הגדרה:

חבורות G,H נקראות איזומורפיות אם ק"מ איזומורפיזם $f:G\to H$. מסמנים $G\simeq H$

תרגיל:

אם f איזומורפיזם, הפונקציה ההפוכה f^{-1} גם איזומורפיזם

דוגמאות:

1) $G=\mathbb{Z}_2=\{[0],[1]\}$ (חיבור), $\quad H=\{\pm1\}=U(\underbrace{\mathbb{Z}}_{\substack{\text{מינוויך}\\\text{תחת כפל}}})$ (כפל)

נראה ש $G\simeq H$

צריך לבנות $f: G \to H$ איזו'

$f([0]) = 1$

$f([1]+[0]) = f([1]) = -1 = f([0]) \cdot f([1])$

$f([1]) = -1$

טבלאות כפל:

$\mathbb{Z}_2$	$[0]$	$[1]$
$[0]$	$[0]$	$[1]$
$[1]$	$[1]$	$[0]$

$\{\pm 1\}$	1	-1
1	1	-1
-1	-1	1

שתי החבורות איזומורפיות אם יש להן אותה טבלת כפל
עד כדי החלפת שמות האיברים

2) יהי $f: G \to H$ הומ' חח"ע (מונומורפיזם). אזי $G \simeq f(G)$
הוכחה:

f עצמו נותן לנו העתקה $f': G \to f(G)$

f' הומ' כי f הומ'

f' על לפי ההגדרה

f' חח"ע כי f חח"ע

3) $f: \mathbb{Z}_2 \to \mathbb{R}^*$, $f(\mathbb{Z}_2) = \{\pm 1\}$

$[0] \to 1$

$[1] \to -1$

f גורר איזו' $\mathbb{Z}_2 \xrightarrow{\sim} \{\pm 1\} = f(\mathbb{Z}_2)$

משפט: (קיילי)

תהי G חבורה סופית. יהי $n=|G|$. אזי G איזומורפית לתת חבורה של S_n. כלומר, קיימת תת-חבורה $H\le S_n$ כך ש $G\simeq H$

הוכחה:

לפי הבחנה הקודמת, מספיק למצוא הומ׳ חח״ע $f:G\to S_n$ כי אז $G\simeq f(G)$. אך $f(G)$ תת-חבורה, כפי שהוכחנו בשיעור הקודם. נזכור כי G פועלת על עצמה על ידי כפל משמאל
$A=G$ $\quad g*a=ga$ (בדקנו שזו אכן פעולה)

אבל ראינו בשיעור הקודם שמכל פעולה של חבורה G על קבוצה A מקבלים הומ׳ $f:G\to S_A=\{\varphi:A\to A$ חח״ע ועל$\}$, $(f(g)=f_g,\ f_g(a)=g*a)$

במקרה שלנו, $|A|=|G|=n$. נקבע מספור של האיברים של $G=A$
כלומר נקבע התאמה חח״ע בין הקבוצות:

$G=A\longleftrightarrow\{1,\dots,n\}$

אחרי שזיהינו G עם $\{1,\dots,n\}$ זיהינו $S_G=S_A$ עם S_n

מקבלים $f:G\to S_n$. נשים לב כי $f_g(e)=g*e=g$
בפרט, אם $g_1\ne g_2$, אזי $f_{g_1}(e)\ne f_{g_2}(e)$, לכן $f_{g_1}\ne f_{g_2}$
לכן $f:G\to S_n$ הינו חח״ע.
$(f(g)=f_g)$

דוגמה 1 למשפט קיילי:

יהי $G=\mathbb{Z}_2\times\mathbb{Z}_2$. לפי המשפט, G איזומורפית לתת״ח של S_4

נבנה את האיזו׳

צריך למספר את האיברים של $\mathbb{Z}_2\times\mathbb{Z}_2$

$([0],[0])$ 2

$([0],[1])$ 3

$([1],[0])$ 1

$([1],[1])$ 4

לכל $g\in\mathbb{Z}_2\times\mathbb{Z}_2$:

פונקצית הזהות $f_{([0,0])}(g)=([0],[0])*g=g$

$$
\begin{aligned}
f_{([1],[0])}:\ & 1\,([1],[0]) \mapsto ([1],[0])*([1],[0]) = ([0],[0])\,2\\
& 2\,([0],[0]) \mapsto ([1],[0])*([0],[0]) = ([1],[0])\,1\\
& 3\,([0],[1]) \mapsto ([1],[0])*([0],[1]) = ([1],[1])\,4\\
& 4\,([1],[1]) \mapsto ([1],[0])*([1],[1]) = ([0],[1])\,3
\end{aligned}
$$

$$
\begin{aligned}
f_{([0],[1])}:\ & 1\,([1],[0]) \mapsto ([0],[1])*([1],[0]) = ([1],[1])\,4\\
& 2\,([0],[0]) \mapsto ([0],[1])*([0],[0]) = ([0],[1])\,3\\
& 3\,([0],[1]) \mapsto ([0],[1])*([0],[1]) = ([0],[0])\,2\\
& 4\,([1],[1]) \mapsto ([0],[1])*([1],[1]) = ([1],[0])\,1
\end{aligned}
$$

הוכחנו ש $g\mapsto f_g$ הוא הומומורפיזם. לכן,

$$f_{([1],[1])} = f_{([1],[0])([0],[1])} = f_{([1,0])}\circ f_{([0],[1])} =$$

$= (1\ 2)(3\ 4)(1\ 4)(2\ 3) = (1\ 3)(2\ 4)$

קיבלנו הומ׳ חח״ע $f: \mathbb{Z}_2 \times \mathbb{Z}_2 \to S_4$

$([1],[0]) \mapsto e$

$([0],[0]) \mapsto (1\ 2)(3\ 4)$

$([0],[1]) \mapsto (1\ 4)(2\ 3)$

$([1],[1]) \mapsto (1\ 3)(2\ 4)$

מסקנה:

$f(\mathbb{Z}_2 \times \mathbb{Z}_2) = \{e, (1\ 2)(3\ 4), (1\ 4)(2\ 3), (1\ 3)(2\ 4)\}$

הינה תת חבורה של S_4

הערה: שתי חבורות מאותו סדר אינן בהכרח איזומורפיות!!!

טענה:

תהי G חבורה אבלית, $f: G \to H$ הומ׳ (לא בהכרח חח״ע) אז׳ $f(G)$ תת-חבורה אבלית של H

הוכחה:

יהיו $h_1, h_2 \in f(G)$, אזי קיימים $g_1, g_2 \in G$ כך ש $f(g_1) = h_1$ ו- $f(g_2) = h_2$. לכן,

$$h_1 h_2 = f(g_1) f(g_2) = f(g_1 g_2) = f(g_2 g_1) = f(g_2) f(g_1) = h_2 h_1$$

טענה: $|\mathbb{Z}_6| = 6 = |S_3|$ אבל $\mathbb{Z}_6 \not\cong S_3$

כי $\mathbb{Z}_6$ אבלית אבל S_3 לא אבלית

טענה:

יהי $f:G\to H$ הומ'. יהי $g\in G$ איבר מסדר סופי. אזי $o(f(g))|o(g)$

הוכחה:

יהי $n=o(g)$ אזי

$$(f(g))^n=f(g^n)=f(e_G)=e_H \Rightarrow o(f(g))|n$$

(כי $g^n=e$ $\Leftarrow$ $o(g)|n$)

תוצאה:

יהי $f:G\to H$ איזומורפיזם. לכל $g\in G$ $o(g)=o(f(g))$

הוכחה:

לפי הטענה הקודמת $o(f(g))|o(g)$

אבל f^{-1} גם איזו' לכן:

$$o(g)=o(f^{-1}(f(g)))|o(f(g))$$

לכן $o(g), o(f(g))$ הם מספרים טבעיים שמחלקים אחד את השני, לכן שווים.

תוצאה:

$\mathbb{Z}_4\neq\mathbb{Z}_2\times\mathbb{Z}_2$ למרות ששתיהן חבורות אבליות מסדר 4

הוכחה:

ב-$\mathbb{Z}_4$ יש איברים מסדר 4 (כמו $[1]$ ו-$[3]$)

ב-$\mathbb{Z}_2\times\mathbb{Z}_2$ כל האיברים מסדר 1 או 2.

טענה:

תהי G חבורה כלשהי, $g\in G$. העתקה $\varphi_g: G\to G$

$\varphi_g(x)=gxg^{-1}$ הינה איזומורפיזם

הוכחה:

לכל $x,y\in G$

$$\varphi_g(x)\varphi_g(y) = gxg^{-1}gyg^{-1} = gxyg^{-1} = \varphi_g(xy)$$

בנוסף,

$$(\varphi_{g^{-1}}\circ\varphi_g)(x) = \varphi_{g^{-1}}(gxg^{-1}) = g^{-1}gxg^{-1}g = x$$

לכן $\varphi_{g^{-1}}\circ\varphi_g$ העתקת הזהות

כמו כן גם $\varphi_g\circ\varphi_{g^{-1}}$ העתקת הזהות

לכן ל- φ_g יש הופכית, לכן φ_g חח"ע ועל. לכן φ_g איזומורפיזם

הגדרה: איזומורפיזם $f:G\to G$ נקרא אוטומורפיזם

תרגיל:

הקבוצה של כל האוטומורפיזמים של G, תחת הרכבה, הינה חבורה

מסמנים אותה $Aut(G)$

אוטו מן הצורה $x\mapsto gxg^{-1}$ נקרא אוטו פנימי. האוטו

הפנימיים מהווים תת חבורה של $Aut(G)$, מסמנים אותה $Inn(G)$

הגדרה: יהי n מספר טבעי. חלוקה של n הינה סדרה לא עולה

$a_1,\dots,a_r$ של מס' חיוביים כך ש $a_1+\dots+a_r=n$

יהי $P(n)$ מספר החלוקות של n

$$P(4)=5 \Leftarrow 4, 31, 22, 211, 1111$$

תהי $\sigma\in S_n$ תמורה. ניתן לפרק את σ באופן יחיד למכפלה של

מחזורים זרים, עד כדי שינוי סדר הגורמים.

מבנה המחזורים של σ הינו החלוקה של n המתקבלת מן האורכים של המחזורים הזרים

למשל: $\begin{pmatrix}1&2&3&4&5&6&7&8&9\\4&1&3&2&6&7&8&5&9\end{pmatrix}=(142)(3)(5678)(9)$

המבנה המחזורי של $\sigma\in S_9$ הנ"ל הינו $4,3,1,1$

תזכורת:

כל חבורה G שפועלת על עצמה על ידי הצמדה $g*a=gag^{-1}$

המסלולים של הפעולה הזאת נקראים מחלקות צמידות.

כלומר: $a,b\in G$ צמודים אם"ם קיים $g\in G$ כך ש $gag^{-1}=b$

טענה:

יהיו $\sigma,\tau\in S_n$ הן צמודות $\Longleftrightarrow$ יש להן אותו מבנה מחזורי

הוכחה:

נשים לב שאם $\sigma\in S_n$ תמורה, $(a_1\dots a_r)\in S_n$ מחזור מאורך r, אזי

$$\sigma(a_1\dots a_r)\sigma^{-1}=(\sigma(a_1)\dots\sigma(a_r))$$

$$\sigma(a_2)\mapsfrom a_2\mapsfrom a_1\mapsfrom\sigma(a_1)$$

$(\Leftarrow)$ נניח כי σ,τ צמודים, אזי קיימת תמורה $\rho\in S_n$ כך ש $\tau=\rho\sigma\rho^{-1}$

הפירוק של σ למחזורים זרים:

$$\sigma=(a_1\dots a_r)(b_1\dots b_s)\dots$$

$$\tau=\rho\sigma\rho^{-1}\underset{\text{הומ׳ }\varphi_\rho}{=}\rho(a_1\dots a_r)\rho^{-1}\rho(b_1\dots b_s)\rho^{-1}\dots=$$

$$=(\rho(a_1)\dots\rho(a_r))(\rho(b_1)\dots\rho(b_s))\dots$$

לכן ל-σ ול-τ יש אותו מבנה מחזורי

$(\Leftarrow)$ נניח של σ,τ אותו מבנה מחזורי

$\sigma=(a_1 \dots a_r)(b_1 \dots b_s)\dots$

$\tau=(a_1' \dots a_r')(b_1' \dots b_s')\dots$

תהי ρ התמורה:

$a_1 \mapsto a_1'$
$\vdots$
$a_r \to a_r'$
$b_1 \mapsto b_1'$
$\vdots$
$b_s \mapsto b_s'$

אזי $\tau=\rho\sigma\rho^{-1}$ לפי הנ"ל

דוגמא:

$\sigma=(12345)(67)(89)$

$\tau=(14789)(36)(25)$

$$\rho=\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 1 & 4 & 7 & 8 & 9 & 3 & 6 & 2 & 5 \end{pmatrix}=(1)(248)(376)(59)$$

אזי $\tau=\rho\sigma\rho^{-1}$

הגדרה: תהי $\sigma\in S_n$ תמורה. מספר ההיפוכים של σ הינו
$inv(\sigma)=|\{(ij) : i<j,\ \sigma(i)>\sigma(j)\}|$

למשל: $\sigma=(134)\in S_4$

12	$\xrightarrow{\sigma}$	32 ✓
13		34
14		31 ✓
23		24
24		21 ✓
34		41 ✓

$inv(134)=4$

טענה:

ההעתקה $sgn: S_n \to \{\pm 1\}$ $\quad sgn(\sigma)=(-1)^{inv(\sigma)}$ הינה הומומורפיזם.

הוכחה:

נזכור מן התרגול כי S_n פועלת על קבוצת הפולינומים במשתנים $x_1,\dots,x_n$ $\quad x_i \mapsto x_{\sigma(i)}$

נגדיר את הפולינום הבא: $\quad \Delta_n = \prod_{1\le i<j\le n} (x_j - x_i)$

לדוגמא:

$$\Delta_4 = (x_2-x_1)(x_3-x_1)(x_4-x_1)(x_3-x_2)(x_4-x_2)(x_4-x_3)$$

נשים לב ש $\sigma * \Delta_n = (-1)^{inv(\sigma)} \Delta_n$

אכן: σ מעביר זוגות לזוגות. אם i,j זוג לא נהפך על ידי σ $\quad (x_j - x_i) \to \underbrace{(x_{\sigma(j)} - x_{\sigma(i)})}_{\text{גורם של } \Delta_n}$

אם $i<j$ כן נהפך $\quad (x_j - x_i) \mapsto (x_{\sigma(j)} - x_{\sigma(i)}) = (-1)(\text{גורם מ-}\Delta_n)$

לכן, הפעולה של σ על Δ_n מכניסה -1 לכל גורם שמתאים לזוג נהפך

$$(1\,3\,4) * \Delta_4 = \overset{-1}{(x_2-x_3)}(x_4-x_3)\overset{-1}{(x_1-x_3)}(x_4-x_2)\overset{-1}{(x_1-x_2)}\overset{-1}{(x_1-x_4)} = (-1)^4 \Delta_4$$

לכן,

$$(-1)^{inv(\sigma\tau)} \Delta_n = \sigma\tau * \Delta_n = \sigma * (\tau * \Delta_n) = \sigma * ((-1)^{inv(\tau)} \Delta_n) =$$

$$= (-1)^{inv(\tau)} (\sigma * \Delta_n) = (-1)^{inv(\tau)} (-1)^{inv(\sigma)} \Delta_n$$

לכן $\quad (-1)^{inv(\sigma\tau)} = (-1)^{inv(\tau)} (-1)^{inv(\sigma)}$

$$sgn(\sigma\tau) = sgn(\sigma)\, sgn(\tau)$$

טענה:

כל מחזור הינו מכפלה של חילופים, לא בהכרח זרים.

הוכחה:

$(a_1 \dots a_r) = (a_1\, a_2)(a_2\, a_3)\dots(a_{r-2}\, a_{r-1})(a_{r-1}\, a_r)$

$(1\,2\,3\,4) = (1\,2)(2\,3)(3\,4)$

תוצאה:

כל $\sigma \in S_n$ הינו מכפלה של חילופים

הוכחה:

σ היא מכפלה של מחזורים זרים, כל מחזור הינו מכפלה של חילופים (לפי הטענה הקודמת).

יש הרבה דרכים להציג את σ כמכפלה של חילופים.

לדוגמא: $(1\,3) = (2\,3)(1\,2)(2\,3) = (1\,2)(2\,3)(1\,2)$

טענה:

תהי $\sigma \in S_n$. בכל הצגה של σ כמכפלה של חילופים תמיד יהיה מספר זוגי של גורמים אם $sgn(\sigma)=1$ ומספר אי זוגי של גורמים אם $sgn(\sigma)=-1$

הוכחה:

נוכיח תת טענה:

יהי $\tau=(a\,b)$ חילוף. אזי $sgn(\tau)=-1$

הוכחה:

יהי $\tau=(a\,b)$, נניח $a<b$. יהי $i<j$ זוג.

אם $\{i,j\}\cap\{a,b\}=\emptyset$ אזי σ לא הופך בלום לזוג i,j

הזוגות הנהפכים הם: $a<j$ כאשר $j<b$

$a,j \Leftarrow b,j$. יש $b-a-1$ כאלה

גם a,b נהפך. לכן $inv((ab))=2(b-a-1)+1$

אי זוגי ולכן $sgn((ab))=(-1)^{2b-2a-1}=-1$

כיוון ש sgn הוא הומ׳, ו σ היא מכפלה של m חילופים אזי $sgn(\sigma)=(-1)^m$

$sgn(\sigma)=1 \Rightarrow m$ זוגי

$sgn(\sigma)=-1 \Rightarrow m$ אי זוגי

הגדרה: σ הינה תמורה זוגית אם $sgn(\sigma)=1$ ואי זוגית אם $sgn(\sigma)=-1$

הגדרה: החבורה המתחלפת הינה $A_n=\ker(sgn:S_n\to\{\pm1\})$

$A_n=\{$ כל התמורות הזוגיות ב-S_n $\}\trianglelefteq S_n$

טענה:

יהי $(a_1\dots a_r)$ מחזור מאורך r. אזי $sgn(\tau)=(-1)^{r-1}$

הוכחה:

$$(a_1\dots a_r)=(a_1a_2)(a_2a_3)\dots(a_{r-1}a_r)$$

יש כאן $r-1$ גורמים

מסקנה:

יהי $r_1,\dots,r_s$ מבנה המחזורי של $\sigma\in S_n$ $(r_1+\dots+r_s)=n$

אזי $\sigma\in A_n \iff (r_1-1)+\dots+(r_s-1)=n-s$ הינו מספר זוגי.