גירסה 1.02 – 26.7.2004

אלגברה מודרנית - סיכום נקודות

ניר אדר

Nir Adar
Email: underwar@hotmail.com
Home Page: http://underwar.livedns.co.il

אנא שילחו תיקונים והערות אל המחבר

<u>גרסאות</u>

גירסה 1.02 – 26.7.2004
- שינויי ניסוח ועיצוב שונים למסמך.
- שיפורי ניסוח עבור ההגדרות והמשפטים השונים.
- תיקונים של מספר משפטים והגדרות.

גירסה 1.01 - 26.7.2002
- תוקנו שגיאות כתיב שונות במסמך.
- תוקן הניסוח של המשפט היסודי של האריתמטיקה.
- תוקנה ההגדרה של קוסט שמאלי.

גירסה 1.00 - 31.5.2002
- גירסה ראשונה למסמך

שמות לקבוצות מוכרות

$\mathbb{N}$ - קבוצת המספרים הטבעיים
$\mathbb{Z}$ – המספרים השלמים
$\mathbb{Q}$ – המספרים הרציונליים
$\mathbb{R}$ – המספרים הממשיים
$\mathbb{C}$ – המספרים הקומפלקסים

$\mathbb{R},\mathbb{Q},\mathbb{C}$ הם שדות.

עיקרון הסדר הטוב

בכל תת קבוצה לא ריקה של המספרים הטבעיים יש איבר קטן ביותר.
עיקרון זה שקול לאינדוקציה.

יחסי שקילות

יחס שקילות בקבוצה A הוא "קשר" בין חלק מאברי הקבוצה, סימון $\sim$, כך שמתקיימות 3 דרישות:

1. רפלקסיביות: $\forall a \in A, a \sim a$
2. סימטריות: $a \sim b \Leftarrow b \sim a$
3. טרנזיטיביות: $\left.\begin{matrix} a \sim b \\ b \sim c \end{matrix}\right\} \Rightarrow a \sim c$

הגדרה

יהי $\sim$ יחס שקילות ב-A. ניקח $a \in A$ ונסמן:

$$[a] = \{x \in A \mid x \sim a\}$$

$[a]$ נקראת מחלקת השקילות של a.

משפט

$\sim$ הוא יחס שקילות בקבוצה A, אזי:
א. $[a]=[b]$ או $[a]\cap[b]=\phi$.
ב. האיחוד של מחלקות השקילות השונות הוא כל A.

חלוקת המספרים השלמים

יהיו a ו- b שלמים ($b \neq 0$), אזי קיימים q שלם ו- r אי שלילי יחידים כך ש:

$$a = bq + r$$
$$0 \le r \le |b|$$

אם $r = 0$ נאמר כי b מחלק את a, ונסמן $b \mid a$.
הסימון הבא אומר: b אינו מחלק את a: $b \nmid a$.

תוצאות מיידיות

1. $\forall a \in \mathbb{Z}, 1 \mid a$
2. $\forall a \neq 0, a \mid 0$
3. $a \mid 1 \Leftarrow a = \pm 1$
4. $\begin{cases} a \mid b \\ b \mid c \end{cases} \Leftarrow a \mid c$ (טרנזיטיביות).
5. $\begin{cases} a \mid b \\ b \mid a \end{cases} \Leftarrow a = \pm b$
6. אם $a \mid b$ וגם $a \mid c$ אזי $a \mid \alpha b + \beta c$ עבור כל α, β.

הגדרה

מחלק משותף גדול ביותר (ממג"ב):
יהיו a ו- b לא שניהם 0 ויהי $c > 0$ כך ש:

1. $c \mid a, c \mid b$
2. אם קיים d כך ש $\begin{cases} d \mid a \\ d \mid b \end{cases} \Leftarrow d \mid c$

במקרה זה c יקרא ממג"ב ונסמן: $c = (a,b)$

דגש

c הוא תמיד מספר חיובי.

משפט

המחלק המשותף הגדול ביותר של שני מספרים a,b שלא שניהם 0 קיים והוא יחיד.
יתרה מזאת, ניתן למצוא m,n שלמים כך ש- $c = ma + nb$.

אלגוריתם החילוק של אוקלידס

בלי הגבלת כלליות $a > b$.

$$0 \le r \le |b|$$

$$a = bq_1 + r_2$$

אם $r_1 = 0 \Leftarrow$ הממג"ב שווה b. אחרת: $0 \le r_2 < r_1$

$$b = r_1 q_2 + r_2$$

אם $r_2 = 0 \Leftarrow$ הממג"ב שווה r_1.
אחרת: $0 \le r_3 < r_2$

$$r_1 = r_2 q_3 + r_3$$

...

$$r_{t-2} = r_{t-1} \cdot q_t + r_t, 0 \le r_t < r_{t+1}$$

$$r_{t-1} = r_t \cdot q_{t+1}$$

ומתקיים כי r_t הוא הממג"ב.

הגדרה

אם $(a,b)=1$ אזי אומרים ש- a,b זרים. דוגמא: (3,5), (6,35).

טענה

a,b זרים אמ"מ קיימים מספרים x,y כך שמתקיים $ax+by=1$.

הגדרה

הכפולה המשותפת הקטנה ביותר (כמק"ב) של a ו- b היא מספר d המקיים:
1. $a\mid d,\ b\mid d$.
2. אם $a\mid f,\ b\mid f$ אזי גם $d\mid f$.

כלומר d הוא המספר הקטן ביותר ש- a,b מחלקים.
הסימון של הכמק"ב: $d=[a,b]$.

דוגמא

a=5, b=12. הכמק"ב הוא $[a,b]=60$.

טענה

$$(a,b)\cdot[a,b]=a\cdot b$$

טענה

$o(g)=n$, אזי $o(g^k)=\dfrac{n}{(n,k)}$

מספרים ראשוניים

הגדרה

מספר ראשוני p הוא מספר גדול מ-1 המתחלק רק ב- $\pm1,\pm p$.

טענה

אם מתקיים כי $a\mid bc$ וגם $(a,b)=1$ אזי נובע כי $a\mid c$.

המשפט היסודי של האריתמטיקה

יהא n טבעי גדול מ-1. אזי n ניתן לפירוק בצורה יחידה כלהלן:

$$n=p_1^{\alpha_1}\cdot p_2^{\alpha_2}\cdot\ldots\cdot p_r^{\alpha_r}$$

קבוצת השאריות מודולו n הינה הקבוצה $Z_n=\{0,1,2,\ldots,n-1\}$.

טענה

הקבוצה $Z_p=\{0,1,2,\ldots,p-1\}$ הינה שדה אמ"מ p ראשוני.

קונגרואנציה

$a,b\in\mathbb{Z}$, n טבעי. נסמן את השארית של חלוקת a ב-n כך: a(mod n)

הגדרה

$a,b\in\mathbb{Z}$ n טבעי. אומרים ש-a קונגרואנטי ל-b מודולו n ומסמנים $a\equiv b(\mathrm{mod}\,n)\Leftrightarrow n\mid a-b$

דוגמא מכשילה

$-51\equiv\_\_(\mathrm{mod}\,5)$

$-51\equiv 4(\mathrm{mod}\,5)$

טענה

$a\equiv b(\mathrm{mod}\,n)\Leftrightarrow a$ ל- ו- b אותה שארית בחלוקה ב- n.

טענה

אם $a\equiv b(\mathrm{mod}\,n)$ וגם $c\equiv d(\mathrm{mod}\,n)$ אזי:

1. $a\pm c\equiv b\pm d(\mathrm{mod}\,n)$
2. $a\cdot c\equiv b\cdot d(\mathrm{mod}\,n)$
3. $\forall m\in N, a^m\equiv b^m(\mathrm{mod}\,n)$
4. $k\in z, ka\equiv kb(\mathrm{mod}\,n)$

טענה

ב- z_n יש בדיוק n מחלקות שקילות שונות.

הגדרה

נגדיר ב- z_n 2 פעולות.

$$\begin{cases}\bar{a}\oplus\bar{c}=\overline{a+c}\\ \bar{a}\otimes\bar{c}=\overline{a\cdot c}\end{cases}$$

- החיבור והכפל ב- z_n מוגדרים היטב. הם אינם תלויים בבחירת הנציגים.
- החיבור והכפל ב- z_n נעשים מודולו n.

תכונות ב z_n:

- קומוטטיביות בכפל ובחיבור.
- אסוציאטיביות בכפל ובחיבור.
- איבר אדיש חיבורי ב- z_n ($\bar{0}$)
- איבר אדיש כפלי ב- z_n ($\bar{1}$)
- איבר נגדי: הנגדי למחלקה $\bar{i}$ הוא $\overline{n-i}$.
- איבר הופכי בכפל לא תמיד קיים. ב- z_5 קיים הופכי לכל איבר. ב- z_6 קיים הופכי רק ל- $\bar{1}$ ול- $\bar{5}$.
- מסקנה: ב- z_n יש הופכי לאיבר i אמ"מ $(i,n)=1$.

<u>טענה</u>

אם $\begin{cases} x \equiv a(\mathrm{mod}\, n) \\ (x,n)=1 \end{cases}$ אזי גם $(a,n)=1$.

<u>חבורות</u>

<u>הגדרה</u>

תהיי G קבוצה לא ריקה ונניח שעל G מוגדרת פעולה • כך שמתקיימות 4 הדרישות הבאות:

1. סגירות: $\forall a,b \in G, a \cdot b \in G$
2. אסוציטיביות: $\forall a,b \in G, (a \cdot b) \cdot c = a \cdot (b \cdot c)$
3. קיום איבר יחידה $\forall a \in G, a \cdot e = e \cdot a = a$
4. לכל $a \in G$ קיים $a^{-1} \in G$ כך ש: $a \cdot a^{-1} = a^{-1} \cdot a = e$

אזי G עם הפעולה הנ"ל נקראת חבורה.

<u>הגדרה</u>

תהי G חבורה ונניח כי מתקיים $\forall a,b \in G, a \cdot b = b \cdot a$. אזי G נקראת חבורה קומוטטיבית או חבורה אבלית.

<u>דוגמאות חשובות</u>

1. כל שדה הוא חבורה אבלית לגבי הפעולה +. אם נוריד את ה-0, אזי כל שדה הוא גם חבורה קומוטטיבית לגבי •.
2. כל מרחב ווקטורי הוא חבורה אבלית לגבי הפעולה +.
3. $(\mathbb{Z},+)$ היא חבורה (אבלית). $e=0$. $-3="3^{-1}"$.
4. $(\mathbb{Z},\cdot)$ איננה חבורה (אבל כן אבלית). אין הופכי לאף איבר פרט ל ± 1.
5. $(\mathbb{Q},+)$ היא חבורה (אבלית). שדה בחיבור מקיים אף יותר מתכונות החבורה הדרושות.
6. $(\mathbb{Q},\cdot)$ איננה חבורה (אבל כן אבלית), כי ל0 אין הופכי.
7. $(\mathbb{Q}^*,\cdot) \Leftarrow (\mathbb{R}^*,\cdot),(\mathbb{C}^*,\cdot)$ קבוצת הרציונליים פרט ל-0, היא חבורה. חבורות.

– לא פגענו בסגירות כשהוצאנו את 0 מהקבוצה, כי לא תיתכן מכפלת מספרים שונים מ-0 שתהיה 0.

<u>הגדרה</u>

נאמר ש- G היא חבורה סופית אם G חבורה וגם ל- G מספר סופי של איברים.
מספר איברי החבורה יסומן על ידי $|G|$.

<u>הגדרה</u>

נסמן ב- U_n את כל איברי z_n שיש להם הופכי. כלומר כל האיברים שזרים ל- n.
למשל: $U_{10} = \{1,3,7,9\}$.

<u>טענה</u>

U_n היא תמיד חבורה אבלית לגבי כפל מודולו n.

<u>הגדרה</u>

פונקצית אויילר $\varphi(n)$: $\varphi(n)=\left|U_n\right|$, כלומר $\varphi(n)$ סופרת את מספר האיברים ב z_n הזרים ל-n.

<u>תכונות</u>

1. $\varphi(P)=P-1 \Leftarrow$ P ראשוני
2. $\varphi(P^{\alpha})=(P-1)P^{\alpha-1} \Leftarrow$ P ראשוני
3. $\varphi(ab)=\varphi(a)\cdot\varphi(b) \Leftarrow (a,b)=1$

<u>משפט אויילר</u>

יהא n מספר טבעי, $a\in\mathbb{Z}$, כך ש $(a,n)=1$, אזי $a^{\varphi(n)}\equiv 1(\mathrm{mod}\, n)$

<u>הערות</u>

1. מגדירים בחבורה $a^0=e,\forall a\in G$.
2. נגדיר בחבורה את a^n באופן הבא: $a^n=\underbrace{a\cdot a\cdot a\cdot\ldots\cdot a}_{\text{n times}}$.
3. נגדיר בחבורה את a^{-n} באופן הבא: $a^{-n}=\underbrace{a^{-1}\cdot a^{-1}\cdot a^{-1}\cdot\ldots\cdot a^{-1}}_{\text{n times}}$.
4. בחבורות חיבוריות המשמעות של a^n היא $a+a+\ldots+a=na$.

<u>תוצאות מהגדרת חבורה</u>

תהי G חבורה כלשהי, אזי:

א. איבר היחידה e הינו יחיד.

ב. לכל $a\in G$, קיים $a^{-1}\in G$ יחיד.

ג. $(a^{-1})^{-1}=a$

ד. $(a\cdot b)^{-1}=b^{-1}\cdot a^{-1}$

ה. $\left(a^{-1}\right)^n=\left(a^n\right)^{-1}$

ו. $a^{n+m}=a^n\cdot a^m$

ז. $\left(a^n\right)^m=a^{nm}$

ח. $ab=ac\Rightarrow b=c$

ט. $ab=cb\Rightarrow a=c$

<u>תמורות</u>

תהא A קבוצה. לפונקציה $f:A\to A$ ח.ח.ע. ועל נקרא תמורה.

<u>טענה</u>

חבורת S_n לכל $n\geq 3$ איננה אבלית.

<u>טענה</u>

$\left|S_n\right|=n!$

תת חבורות

תהי $(G,\cdot)$ חבורה, ותהיי $\phi \neq H \subseteq G$.
אומרים ש-H היא תת חבורה של G אם H מהווה חבורה ביחס לאותה פעולה שהוגדרה ב-G ועם אותה משמעות של פעולה.

דוגמאות

1. $(Q_i^*,\cdot) \subseteq (R_i^*,\cdot)$ תת חבורה.
2. $(Z_4,+),(Z_5,+)$ Z_4 איננה תת חבורה של Z_5 (פעולת החיבור שונה!) כל אחד מהביטויים הינו חבורה אולם הם אינם תת חבורה אחד של השני.

משפט

תהי G חבורה ו $\phi \neq H \subseteq G$ אזי H ת"ח של G אמ"מ:
1. מתקיימת סגירות: $\forall h_1,h_2 \in H, h_1 \cdot h_2 \in H$.
2. קיום הופכי: $\forall h \in H, h^{-1} \in H$.

הערה

אם H היא תת חבורה של G, אזי איבר היחידה e של H הוא אותו איבר יחידה e של החבורה G.

הגדרות

GL(n.F) אוסף מטריצות הפיכות ביחס לכפל מטריצות.
SL(n,F) מטריצות ב-GL(n,F) שהדטרמיננטה שלהם שווה 1.

משפט

תהי G חבורה סופית. אזי קיים n טבעי או אפס כך ש- $a^{-1} = a^n$

הוכחה

נרשום כל החזקות של a: $a, a^2, a^3, a^4, a^5, a^6, \ldots$
רשימת החזקות הינה סופית, כיוון שכל החזקות הן בתוך G ו-G סופית. כלומר יש k ו-l טבעיים כך ש $a^k = a^l$.
נניח בלי הגבלת כלליות כי $k < l$.
מכאן:

$$\underbrace{a \cdot a \cdot a \cdot \ldots \cdot a}_{k \text{ times}} = \underbrace{a \cdot a \cdot a \cdot \ldots \cdot a}_{l \text{ times}}$$

נצמצם ב-a k פעמים.
מכאן:

$$e = a^{l-k}$$
$$a \cdot a^{l-k} = e \Rightarrow$$
$$a^{l-k} \equiv a^{-1}$$

הגדרה

בחבורה סופית לכל איבר a קיים m טבעי כך שמתקיים $a^m = e$.
ה-m המינימלי עבורו מתקיים $a^m = e$ נקרא הסדר של a והסימון הוא $o(a)$.

משפט

תהיה G חבורה, $\phi \neq H \subseteq G$ כאשר H סופית, אזי H תת חבורה של G אמ"מ מתקיימת סגירות.

דוגמא

תהי G חבורה.

$$Z(G) = \{x \in G \mid xy = yx, \forall y \in G\}$$

- Z(G) נקרא המרכז של G.
- Z(G) הוא תת חבורה של G.

טענות חשובות

1. לכל חבורה G יש שתי ת"ח טריוויאליות: G, $\{e\}$.
2. כל תת קבוצה של Z מהצורה mz (m טבעי) היא תת חבורה של Z. יתרה מזו, (mz) הינן תת החבורות היחידות של Z.
3. חיתוך של תת חבורות של G הוא גם תת חבורה של G.
4. אם H תת חבורה של חבורה G ולוקחים איבר $g \in G$ אזי גם $g^{-1}Hg$ תת חבורה של G.

חבורות ציקליות

תהי G חבורה, ויהי איבר $a \in G$.
נגדיר $< a >$:

$$< a >= \{a^0 = e, a^{\pm 1}, a^{\pm 2}, a^{\pm 3}, ...\}$$

כאשר G סופית, אזי

$$< a >= \{a^0 = e, a^1, a^2, a^3, ...a^{O(a)-1}\}$$

הגדרה וטענה

$< a >$ נקראת החבורה הציקלית הנוצרת על ידי a. $< a >$ היא תמיד תת חבורה.

משפט

תת חבורה של חבורה ציקלית היא ציקלית.

משפט

תהי G חבורה ציקלית מסדר n. יהי m מספר שמחלק את n, אזי קיימת ב-G תת חבורה מסדר m.

טענה

חבורה ציקלית היא חבורה אבלית.

משפט לגרנג'

אם G חבורה סופית, ו-H תת חבורה, אזי מספר האיברים ב-H מחלק את מספר האיברים ב-G.

<u>משפט</u>

בחבורה ציקלית מסדר n יש תת חבורה יחידה מכל סדר d המחלק את n.

<u>טענה</u>

אם $G=<g>$ חבורה ציקלית מסדר n, וגם $d \mid n$, אזי $o\left(g^{\frac{n}{d}}\right)=d$.

<u>טענה</u>

אם $G=<g>$ חבורה ציקלית מסדר n, אזי g^i יוצר את G אמ"מ $(i,n)=1$

<u>הגדרה</u>

G חבורה ו-H תת חבורה של G.
לכל $a \in G$ נגדיר:

$$Ha=\{ha \mid h \in H\}$$

Ha נקרא מחלקה ימנית (קוסט ימני) של H ב-G.

<u>הגדרה</u>

מספר הקוסטים הימניים השונים של תת חבורה H בחבורה G, יסומן $|G:H|$ ונקרא האינדקס של H ב-G.

<u>הגדרה</u>

תהי G חבורה ותהי H תת חבורה של G. לכל $a \in G$ נגדיר:

$$aH=\{ah \mid h \in H\}$$

aH נקרא מחלקה שמאלית (קוסט שמאלי) של H ב-G.

אם החבורה אבלית, קוסטים ימניים וקוסטים שמאליים הם זהים.

<u>משפט</u>

תהי G חבורה, ו-H תת חבורה של G. נגדיר יחס בין אברי G בצורה הבאה:
$a \sim b$ אמ"מ $a \cdot b^{-1} \in H$.
יחס זה הוא יחס שקילות ומתקיים כי מחלקת השקילות של a היא Ha.

<u>מסקנה</u>

G חבורה, H תת חבורה, אזי:
א. $Ha=H$ אמ"מ $a \in H$.
ב. $Ha=Hb$ אמ"מ $a \cdot b^{-1} \in H$.
ג. $Ha \cap Hb \neq \phi$ אמ"מ $Ha=Hb$.
ד. G שווה לאיחוד הקוסטים הימניים הזרים.

משפט לגרנג'

G חבורה סופית ו-H תת חבורה של G, אזי:

$$|G| = |H| \cdot |G:H|$$

משפט

תהא G חבורה מסדר ראשוני. G חבורה ציקלית וכל איבר מהחבורה השונה מ-e הוא יוצר שלה.

מסקנה

G חבורה סופית, $a \in G$, אזי $O(a) \| |G|$

טענה

מספר היוצרים של חבורה ציקלית מסדר n הוא $\varphi(n)$ (כאשר $\varphi(n)$ היא פונקצית אויילר).

משפט

n טבעי, (a,n)=1, a שלם. אזיי $a^{\varphi(n)} = 1 (\mathrm{mod}\, n)$, כאשר $\varphi(n)$ זוהי פונקצית אויילר.

המשפט הקטן של פרמה

אם p ראשוני ו $a \in \mathbb{Z}$ אזי $ap = a (\mathrm{mod}\, p)$.

משפט

G חבורה סופית, $a \in G$, אזי $a^{|G|} = e$

הצמדת איברים

נניח ש-G חבורה, $a,b \in G$. a,b נקראים צמודים אם יש $x \in G$ בחבורה כך ש $x^{-1} \cdot a \cdot x = b$.
זוהי מעין הכללה של דמיון מטריצות.

נשים לב שיחס הצמידות הוא יחס שקילות.

הגדרה: מעגל באורך k או k-מעגל

מעגל זוהי תמורה שמסומנת: $F = (\alpha_1, \alpha_2, ..., \alpha_k) \in S_n$ כך ש $F(\alpha_i) = \begin{cases} \alpha_{i+1} & i < k \\ \alpha_1 & i = k \end{cases}$ וכמו כן אם קיים $\beta \neq \alpha_1, \alpha_2, ..., \alpha_k$ אזי $F(\beta) = \beta$.

הגדרה

אומרים ששני מעגלים הם זרים, אם אין להם אף איבר משותף.

משפט

אם $\alpha, \beta \in S_n$ שני מעגלים זרים, אזי $\alpha\beta = \beta\alpha$.

הגדרה

2 מעגל נקרא חילוף (טרנספורמציה).

טענה

לכל טרנספורמציה α, מתקיים $\alpha^2 = e$.

הערה

כל תמורה ניתנת לכתיבה בתור מעגלים זרים.

משפט

הסדר של מעגל באורך k הוא k.

משפט

$\alpha \in S_n$, אזי α ניתנת להצגה כמכפלת מעגלים זרים.

מסקנה נוספת ממשפט לגרנג'

G חבורה סופית וקיים $a \in G$.
נניח ש-n הוא מספר טבעי כך ש $a^n = e$, אזי $o(a) \mid n$.

משפט

תהא σ תמורה שהיא מכפלה של מעגלים זרים שאורכיהם $k_1, k_2, ..., k_s$, אזי הסדר של σ הוא הכפולה המשותפת הקטנה ביותר של $k_1, k_2, ..., k_s$.

הגדרה

מעגל באורך 2 נקרא טרנספוזיציה.

משפט

כל תמורה ניתנת לכתיבה כמכפלה של טרנספוזיציות.

משפט

ניקח $\sigma \in S_n$ תמורה. אם נרשום את כל האופנים של הצגת σ כמכפלת טרנספוזיציות, אז מספר הטרנספוזיציות יהיה או זוגי בכולן או אי זוגי בכולן.

הגדרה

תמורה נקראת זוגית אם ניתן לרשום אותה כמכפלה של מספר זוגי של טרנספוזיציות.
תמורה נקראת אי זוגית אם ניתן לרשום אותה כמכפלה של מספר אי זוגי של טרנספוזיציות.

מעגל באורך k

$$(\alpha_1\ \alpha_2\ \dots\ \alpha_k)=(\alpha_1\ \alpha_k)(\alpha_1\ \alpha_{k-1})\dots(\alpha_1\ \alpha_3)(\alpha_1\ \alpha_2)$$

המעגל מורכב מ-k-1 טרנספוזיציות.

מעגל באורך k - תמורה זוגית אם k אי זוגי
מעגל באורך k - תמורה אי זוגית אם k זוגי.

טענה

תמורה זוגית כפול תמורה זוגית הינה תמורה זוגית.
תמורה אי זוגית כפול תמורה אי זוגית הינה תמורה זוגית.
תמורה זוגית כפול תמורה אי זוגית הינה תמורה אי זוגית.

טענה

התמורה תהיה זוגית אמ"מ מספר המעגלים הזרים בעלי אורך זוגי הוא זוגי. (מספר התמורות האי זוגיות הוא זוגי).

הגדרה

אוסף כל התמורות הזוגיות ב S_n נקרא A_n . (החבורה האלטרנטיבית).
A_n היא תת קבוצה בחבורה הסופית S_n .

הערה

קבוצת התמורות האי זוגיות ב S_n , שנסמנה ב B_n , אמנם איננה תת חבורה, אך היא קוסט ימני של A_n ב S_n .

הצמדה של איבר בחבורה

G חבורה וניקח $x\in G$ ויהי $a\in G$:
האיבר $a^{-1}xa$ נקרא הצמדת x על ידי a.
אם החבורה אבלית מתקיים $a^{-1}xa=x$.

טענה

אם $\sigma=(a_1,\dots,a_k)$ מעגל ו $\psi\in S_n$ תמורה כלשהי, אזי הצמדת המעגל σ על ידי ψ תיתן :
$$\psi\sigma\psi^{-1}=\psi(a_1,\dots,a_k)\psi^{-1}=(\psi(a_1),\psi(a_2),\dots,\psi(a_k))$$

הערה

הצמדת מעגלים זרים שומרת על מבנה המעגלים.

הגדרה

G_1,G_2 חבורות. e_1 הוא האיבר הניטראלי של G_1 , e_2 הוא האיבר הניטראלי של G_2 .
פונקציה $\varphi:G_1\to G_2$ נקראת הומומורפיזם אם $\varphi(ab)=\varphi(a)\varphi(b)$ לכל $a,b\in G_1$.
אם φ היא גם חד חד ערכית ועל, היא נקראת איזומורפיזם.

מילון שמות

הומומורפיזם ח.ח.ע. נקרא מונומורפיזם.
הומומורפיזם על נקרא אפימורפיזם.
הומומורפיזם ח.ח.ע. ועל נקרא איזומורפיזם.

הגדרה

הגרעין של הומומורפיזם φ מסומן ב $Ker(\varphi)$ והגדרתו: $Ker(\varphi)=\{a\in G_1 \mid \varphi(a)=e_2\}$

סימון: אם G_1,G_2 הן איזומורפיות, אזי נסמן $G_1\cong G_2$,

טענה

אם הגרעין מכיל רק את איבר היחידה, הפונקציה היא חד חד ערכית.

טענה

יהי $\varphi:G_1\to G_2$ הומומורפיזם על, אזי: אם G_1 קומוטטיבית, אזי גם G_2 קומוטטיבית, ואם G_1 ציקלית אזי גם G_2 ציקלית.

הומומורפיזם טריוויאליים

$\varphi:G_1\to G_2$
$\varphi(\forall g\in G)=e_2$

זהו הומומורפיזם. ומכאן, בין כל שתי חבורות קיים הומומורפיזם.
האם φ על? אם G_2 כוללת רק את איבר היחידה, אזי היא על.
האם φ חד חד ערכית? אם G_1 כוללת רק איבר אחד, אזי היא חד חד ערכית.

$\varphi:G\to G$
$\forall g\in G,\varphi(g)=g$

זוהי פונקצית הזהות, והיא הומומורפיזם.

משפט

תהי $\varphi:G_1\to G_2$ הומומורפיזם. e_1 הוא האיבר הניטראלי של G_1. e_2 הוא האיבר הניטראלי של G_2.
אזי:

1. $\varphi(e_1)=e_2$. הגרעין אף פעם לא ריק!
2. $\left(\varphi(a)\right)^{-1}=\varphi(a^{-1}),\forall a\in G_1$
3. $Ker(\varphi)$ היא תת חבורה של G_1.
4. התמונה של φ היא תת חבורה של G_2.
5. φ חד חד ערכית אמ"מ $\ker(\varphi)=\{e_1\}$
6. $x\in G_1$ אזי $x^{-1}Ker(\varphi)x\subseteq Ker(\varphi)$ לכל $x\in G_1$.
7. $x\in G_1$ אזי $\left(\ker(\varphi)\right)x=\{y\in G_1\mid \varphi(y)=\varphi(x)\}$

הגדרה

תהי G חבורה ו-N תת חבורה.
אם לכל $x \in G$ מתקיים $x^{-1}Nx \subseteq N$ אזי N נקראת תת חבורה נורמלית.
ההכלה $x^{-1}Nx \subseteq N$ פירושה $\begin{cases} x^{-1}nx \in N \\ \forall n \in N \end{cases}$.

הערה

לפי המשפט הקודם, נובע כי הגרעין של הומומורפיזם הוא תת חבורה נורמלית.

משפט

תהי G חבורה ו- N תת חבורה של G, אז התנאים הבאים שקולים:
1. N נורמלית ב- G (מסמנים: $N \lhd G$).
2. $\forall n \in N,\ x^{-1}nx \in N$
3. $\forall x \in G,\ x^{-1}nx = N$
4. $\forall x \in G,\ Nx = xN$

משפט

כל חבורה ציקלית אינסופית היא איזומורפית ל- $\mathbb{Z}$ (השלמים) לגבי חיבור.

משפט

כל חבורה ציקלית מסדר m היא איזומורפית ל- $\mathbb{Z}_n$.

משפט (משפט קיילי)

תהא G חבורה סופית, אזי G איזומורפית לתת חבורה של S_G.
S_G היא חבורת כל התמורות על איברי G.

טענה

אם G חבורה קומוטטיבית, אזי כל תת חבורה שלה היא נורמלית.

הערה

לכל חבורה יש שתי תתי חבורות נורמליות טריוויאליות: G כולה ו $\{e\}$.

הערה

אם $|G:N| = 2$ אזי N תת חבורה נורמלית.

הערה

המרכז, המוגדר כ: $z(G) = \{x \in G \mid xg = gx, \forall g \in G\}$ הוא תת חבורה נורמלית של G.

<u>משפט - חבורת המנה</u>

G חבורה ו-N תת חבורה נורמלית של G.

נסמן ב- $\frac{G}{N}$ את אוסף הקוסטים של N ב-G.

נגדיר פעולה בקבוצה $\frac{G}{N}$:

$$(Na)(Nb) = Nab, \quad a,b \in G$$

אזי $\frac{G}{N}$ היא חבורה.

איבר היחידה בה הוא $Ne = N$.

ההופכי של קוסט Na הוא Na^{-1} .

<u>משפט ההומומורפיזם הראשון</u>

תהא $\varphi : G_1 \to G_2$ הומומורפיזם. אזי $\frac{G_1}{\ker(\varphi)} \cong \mathrm{Im}(\varphi)$.

EOF