ביה״ס למדעי המחשב ומתמטיקה. תשס״ה, 19.07.2005
מבנים אלגבריים. סמסטר ב׳, מועד א׳.
שם המרצה: פרופ׳ מ. מוזיצ׳וק.
משך המבחן: 2.5 שעות.

אפשר להשתמש רק במחשיבון ובדפי עזר המצורפים לטופס הבחינה.

חלק א׳: בחלק זה יש לכתוב במחברת תשובה מלאה על כל אחת מהשאלות.

1. 14 נקודות.

א. הוכח שלכל מספר טבעי n הקבוצה $n\mathbf{Z}=\{nx \mid x\in \mathbf{Z}\}$ היא תת-חבורה של $(\mathbf{Z},+)$.

ב. הוכח ש $n\mathbf{Z}\subseteq m\mathbf{Z}$ אם ורק אם $m\mid n$.

2. 14 נקודות

יהי $f:G\to H$ הומומורפיזם חבורות. אז

א. $f(e_G)=e_H$.

ב. $\forall g\in G \quad f(g^{-1})=(f(g))^{-1}$.

ג. $\forall g\in G \quad \forall n\in \mathbf{Z} \quad f(g^n)=(f(g))^n$.

3. 14 נקודות

אם $f(x),g(x)\in F[x]$ שני פולינומים כלשהם, $g(x)\neq 0(x)$, אז קיימים שני פולינומים $q(x),r(x)\in F[x]$ כך ש:

$$f(x)=q(x)\cdot g(x)+r(x)$$
$$\deg(r(x))<\deg(g(x))$$

4. 14 נקודות

יהי $(R,+,\cdot)$ חוג כלשהו. נגדיר A כקבוצה של כל האיברים $r\in R$ שמקיימים

$$\forall x\in R \; xr=rx$$

הוכח ש A תת-חוג קומוטטיבי של R.

חלק ב': יש לענות על 5 שאלות. <u>תשובות לחלק זה ייבדקו רק בטופס הבחינה</u>.

5. 10 נקודות.

שתי תמורות של הקבוצה $\mathbf{Z}_7 = \{0,1,2,3,4,5,6\}$ מוגדרות ע"י הנוסחאות הבאות:

$f = (0,5,3,1)(2,4,6),\ g^{-1}(x) = \begin{cases} \frac{2x+5}{5x+3}, x \neq 5 \\ 6, x = 5 \end{cases}, x \in \mathbf{Z}_7$ (הפעולות מתבצעות ב-$\mathbf{Z}_7$).

א. חשב את gf^2:	
ב. פרק את gf^2 למכפלה של מחזורים זרים:	
ב. מצא את הסדר של gf^2	
ג. פרק את gf^2 למכפלה של חילופים:	

6. 10 נקודות.

חשב את המחלק המשותף הגדול ביותר של הפולינומים הבאים:

$a(x) = x^4 + 3x^3 + 2 \in \mathbf{Z}_5[x],\ b(x) = x^3 + 2x^2 + 4 \in \mathbf{Z}_5[x]$.

$\gcd(a(x), b(x)) =$

7. 10 נקודות.

מצא את פתרון פרטי של המשוואה $374x + 238y = 34$ בשלמים.

$x =$	$y =$

8. 10 נקודות.

נתונה חבורה סימטרית S_4.

רשום 4 מחלקות ימניות שונות של S_4 לפי תת-החבורה $H = \{id, (1,2,3), (3,2,1)\}$.

9. 10 נקודות.

נתונה חבורת מטריצות $G = \left\{ \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \;\middle|\; a,b,c \in \mathbf{Z}_2 \right\}$. רשום את כל האברים של החבורה ומול כל איבר רשום את הסדר שלו.

בהצלחה!

1. יש לדעת להוכיח את הטענות המסומנות באותיות גדולות.
2. בתשובות הוכחה יש לציין את הטענות השימושיות ע"י הפניה למספר הרצאה ומספר טענה.

הרצאה 1.

<u>הגדרה 1.</u> תהי A קבוצה כלשהי עם פעולה בינרית $*$. איבר $e \in A$ נקרא <u>איבר-יחידה</u> כלפי $*$ אם לכל $a \in A$ הוא מקיים $a*e=e*a=a$.

<u>טענה 1</u>. תהי A קבוצה כלשהי עם פעולה בינרית $*$. אם ב-A קיים איבר-יחידה כלפי $*$, אז הוא יחיד.

<u>הגדרה 2.</u> תהי A קבוצה כלשהי עם פעולה בינרית $*$. פעולה $*$ נקראת פעולה <u>אסוציאטיבית</u> אם לכל שלושה איברים $a \in A, b \in A, c \in A$ מתקיים:

$$a*(b*c)=(a*b)*c$$

<u>הגדרה 3.</u> פעולה בינרית $*$ המוגדרת מעל קבוצה A נקראת <u>קומוטטיבית</u> אם לכל שני איברים $a \in A, b \in A$ מתקיים:

$$b*a=a*b$$

<u>טענה 2 (חוק אסוציאטיבי מורחב).</u>
תהי A קבוצה כלשהי עם פעולה בינרית ואסוציאטיבית $*$. אז לכל n איברים $a_1 \in A, \dots, a_n \in A$ ערך הביטוי $a_1 * a_2 * \dots * a_{n-1} * a_n$ לא תלוי במיקום של סוגריים.

<u>הגדרה 4.</u> קבוצה A יחד עם פעולה בינארית אסוציאטיבית $*$ נקראת <u>חבורה למחצה.</u> חבורה למחצה עם איבר-היחידה נקראת <u>מונויד.</u>

<u>הגדרה 5</u>. תהי A קבוצה עם פעולה בינרית $*$ כלשהי. נניח שקיים איבר-היחידה $e \in A$ ביחס ל-$*$. איבר $a \in A$ <u>נקרא הפוך לאיבר</u> $b \in A$ אם הם מקיימים את התנאי הבא: $a*b=b*a=e$. איבר שיש לו הפוך נקרא <u>הפיך</u>.

<u>**טענה 3**</u>. יהי $(A,*)$ מונויד עם איבר-היחידה $e \in A$. אם $a \in A$ הפיך אז יש לו הפוך אחד בלבד.

<u>הגדרה 6.</u> קבוצה A יחד עם פעולה בינרית $*$ נקראת <u>חבורה</u> אם היא מקיימת את האקסיומות הבאות:
1G. (סגירות) לכל שני איברים $a,b \in G$ קיים איבר $a*b \in G$.
2G. (אסוציאטיביות) $(a*b)*c=a*(b*c)$ $\forall a \in A \forall b \in A \forall c \in A$.
3G. (קיום איבר היחידה) קיים איבר $e \in A$ כך ש-$a*e=e*a=a$ $\forall a \in A$.
4G. (קיום איבר הפוך) $a*b=b*a=e$ $\forall a \in A \exists b \in A$ (איבר הפוך ל-$a \in A$ יסומן כ-a^{-1}). חבורה נקראת חבורה <u>קומוטטיבית</u> (או <u>אבלית</u>) אם $*$ היא פעולה קומוטטיבית.

<u>הגדרה 7.</u> תהי $(A,*)$ חבורה כלשהי עם איבר-היחידה e. לכל איבר $a \in A$

נבחר n מספר טבעי כלשהו. נגדיר יחס בינארי $\equiv_n$ מעל הקבוצה $\mathbf{Z}$:

$$x \equiv_n y \quad \Leftrightarrow \quad \frac{x-y}{n} \in \mathbf{Z} \qquad (1.1)$$

טענה 1.
יחס $\equiv_n$ הוא יחס שקילות מעל $\mathbf{Z}$.

נסמן כ- $[a]_n$ מחלקת שקילות של מספר $a \in \mathbf{Z}$ ביחס השקילות $\equiv_n$.
לכל שני מספרים שלמים a ו b מתקיים :

$$[a]_n = [b]_n \quad \Leftrightarrow \quad a \equiv_n b \qquad (1.2)$$

טענה 2.
ליחס $\equiv_n$ יש n מחלקות שקילות והן $[0]_n, [1]_n, \dots, [n-1]_n$.

פעולות בין האיברים של $\mathbf{Z}_n$ מוגדרות ע"י הנוסחאות הבאות :

$$\begin{aligned} [a]_n + [b]_n &= [a+b]_n \\ [a]_n \cdot [b]_n &= [a \cdot b]_n \end{aligned} \qquad (1.3)$$

<u>טענה 3</u>. פעולות ב-(1.3) מוגדרות היטב, כלומר
$[a]_n = [a']_n \ \wedge \ [b]_n = [b']_n \Rightarrow [a+b]_n = [a'+b']_n \ \wedge \ [a \cdot b]_n = [a' \cdot b']_n$

<u>טענה 4</u>. קבוצה $\mathbf{Z}_n$ יחד עם שתי פעולות חיבור וכפל המוגדרות ע"י (1.3) היא חוג קומוטטיבי (החוג הזה נקרא חוג שאריות מודולו n).

<u>הגדרה 2</u>. חוג R נקרא <u>טריביאלי</u> אם $|R|=1$.

טענה 5. יהי R חוג כלשהו. אז
א. $a+b=a+c \Leftrightarrow b=c \quad \forall a \in R \ \forall b \in R \forall c \in R$
ב. $\forall a \in R \ a \cdot 0 = 0 = 0 \cdot a$.
ג. $\forall a \in R \ \forall b \in R \ (-a) \cdot b = -(a \cdot b)$.
ד. $\forall a \in R \ \forall b \in R \ (-a) \cdot (-b) = a \cdot b$.

<u>מסקנה 6</u>. חוג R יהיה טריביאלי אם ורק אם $1 = 0$.
<u>הוכחה.</u>

<u>הגדרה 3</u>. איבר $b \in R$ נקרא <u>הפוך ימני</u> לאיבר $a \in R$ אם $ab = 1$.
איבר $b \in R$ נקרא <u>הפוך שמאלי</u> לאיבר $a \in R$ אם $ba = 1$. איבר $b \in R$ נקרא <u>הפוך</u>

לאיבר $a \in R$ אם $ab = ba = 1$.
איבר $a \in R$ נקרה <u>הפיך ימני(שמאלי)</u> אם יש לו הפוך ימני (שמאלי), בהתאם.
איבר $a \in R$ נקרה <u>הפיך</u> אם יש לו הפוך.

איבר הפוך ל- $a \in R$ יסומן כ- a^{-1}.

<u>טענה 7</u>. קבוצה R^* של כל האיברים ההפיכים של החוג R היא חבורה ביחס לכפל.

חבורה $(R^*,\cdot)$ נקראת <u>חבורה כפלית</u> של החוג.

<u>הגדרה 4</u>. איבר $a \in R\setminus\{0\}$ נקרא <u>מחלק אפס</u> אם לפחות לאחת מהמשוואות $ax = 0, xa = 0$ קיים פתרון לא טריביאלי ב- R (לא טריביאלי = שונה מאפס).

<u>טענה 8</u>. אם $a \in R\setminus\{0\}$ מחלק אפס אז הוא איננו הפיך.

<u>הגדרה 5</u>. חוג קומוטטיבי שבו כל איבר שונה מ-0 הפיך נקרא <u>שדה</u>.

<u>טענה 9</u>. איבר $[a]_n \in \mathbf{Z}_n$ יהיה הפיך אם ורק אם $\gcd(a,n) = 1$.

<u>הגדרה 5</u>. חוג קומוטטיבי שבו כל איבר שונה מ-0 הפיך נקרא <u>שדה</u>.

<u>טענה 10</u>. חוג $\mathbf{Z}_n$ יהיה שדה אם ורק אם n מספר ראשוני.

הרצאה 4

<u>הגדרה 1.</u> תהיינה G,H שתי חבורות כלשהן. פונקציה שלמה $f:G\to H$ נקראת <u>הומומורפיזם</u> אם לכל $g_1,g_2\in G$ מתקיים $f(g_1 *_G g_2)=f(g_1)*_H f(g_2)$ (כאן $*_G$ ו $*_H$ הן פעולות בינאריות ב- G ו H בהתאם). הומומורפיזם $f:G\to H$ נקרא <u>איזומורפיזם</u> אם f פונקציה הפיכה. שתי חבורות G,H נקראות <u>איזומורפיות</u> (סימון, $G\cong H$) אם קיים איזומורפיזם ביניהן.

<u>טענה 1.</u> $\cong$ זה יחס שקילות בין חבורות.

<u>טענה 2.</u> יהי $f:G\to H$ הומומורפיזם חבורות. אז

א. $f(e_G)=e_H$.

ב. $f(g^{-1})=(f(g))^{-1}$ $\forall g\in G$.

ג. $f(g^n)=(f(g))^n$ $\forall n\in \mathbf{Z}$ $\forall g\in G$.

<u>הערה.</u> הומומורפיזם $f:G\to H$ ניקרא <u>טריביאלי</u> אם $\mathrm{Im}(f)=\{e_H\}$.

<u>טענה 3.</u> יהי $f:G\to H$ הומומורפיזם חבורות. אז

א. לכל תת-חבורה $A\le G$ מתקיים $f(A)\le H$.

ב. לכל תת-חבורה $B\le H$ מתקיים $f^{-1}(B)\le G$.

תת-חבורה $f(G)$ נקראת <u>תמונה</u> של f ומסומנת כ- $\mathrm{Im}(f)$. תת-חבורה $f^{-1}(e_H)$ נקראת <u>גרעין</u> של f ומסומנת כ- $\mathrm{Ker}(f)$.

<u>טענה 4.</u> יהי $f:G\to H$ הומומורפיזם חבורות כלשהו. אז

א. $g_1*(g_2)^{-1}\in \mathrm{Ker}(f) \Leftrightarrow f(g_1)=f(g_2)$ $\forall g_2\in G$ $\forall g_1\in G$.

ב. f חד-חד-ערכית אם ורק אם $\mathrm{Ker}(f)=\{e_G\}$.

<u>טענה 5.</u> הומומורפיזם $f:G\to H$ יהיה איזומורפיזם אם ורק אם $\mathrm{Im}(f)=H,\mathrm{Ker}(f)=\{e\}$.

<u>הגדרה 2.</u> תהיינה R,S שני חוגים כלשהם. פונקציה שלמה $f:R\to S$ נקראת <u>הומומורפיזם חוגים</u> אם לכל $r_1,r_2\in R$ מתקיים

א. $f(r_1 +_R r_2)=f(r_1)+_S f(g_2)$.

ב. $f(r_1 \cdot_R r_2)=f(r_1)\cdot_S f(g_2)$.

ג. $f(1_R)=1_S$.

(כאן אינדקסים $_R$ ו $_S$ מסמנים פעולות ב- R ו S בהתאם).

הומומורפיזם $f:R\to S$ נקרא <u>איזומורפיזם</u> אם f פונקציה הפיכה. שני חוגים R,S נקראים <u>איזומורפיים</u> (סימון, $R\cong S$) אם קיים איזומורפיזם ביניהם.

קבוצה $f(R)$ נקראת <u>תמונה</u> של f ומסומנת כ- $\mathrm{Im}(f)$.

קבוצה $\mathrm{Ker}(f):=\{r\in R\mid f(r)=0\}$ נקראת <u>גרעין</u> של f .

<u>הערה.</u> שני שדות נקראים <u>איזומורפיים</u> אם הם איזומורפיים כחוגים.

הרצאה 6

<u>הגדרה 1</u>. חבורה G נקראת חבורה <u>ציקלית</u> אם קיים איבר $g\in G$ כך שכל איבר $x\in G$ ניתן לקבל כחזקה של g, כלומר $\forall x\in G\ \exists n\in \mathbf{Z}\quad x=g^n$. איבר g נקרא <u>יוצר</u> של G.

תהי G חבורה כלשהי עם פעולה בינארית $*$. לכל איבר $g\in G$ נסמן כ- $<g>$ את הקבוצה של כל החזקות של g, כלומר $<g>=\{g^n\mid n\in \mathbf{Z}\}$.

טענה 1. לכל $g\in G$ הקבוצה $<g>$ היא תת-חבורה ציקלית עם יוצר g.

<u>הגדרה 2</u>. איבר $g\in G$ נקרא <u>איבר מסדר אין-סופי</u> אם $g^n\neq e$ לכל מספר טבעי n, אחרת איבר g <u>נקרא איבר מסדר סופי</u>.

<u>הגדרה 3</u>. יהי $g\in G$ איבר מסדר סופי כלשהו. מספר טבעי מינימלי n שמקיים $g^n=e$ נקרא <u>סדר</u> של g ויסומן כ- $o(g)$. אם $g\in G$ איבר מסדר אי-סופי, אז נכתוב $o(g)=\infty$.

איבר $g\in G$ הוא איבר מסדר n אם ורק אם

$$\boxed{(6.1)\qquad g^n=e \text{ ו } g^m\neq e \text{ לכל } 1\le m\le n}$$

טענה 2. אם $g\in G$ איבר סופי מסדר n, אז לכל מספר שלם m מתקיים:
$g^m=e\Leftrightarrow n\mid m$.

טענה 3. אם $g\in G$ איבר מסדר סופי, אז $|<g>|=o(g)$ ו
$<g>=\{g^0,g^1,\dots,g^{o(g)-1}\}$.

מסקנה 4. אם G חבורה סופית, אז
א. $o(g)\mid |G|$.
ב. $g^{|G|}=e$.

מסקנה 5.
א. לכל מספר שלם a זר למספר טבעי n מתקיים $a^{\varphi(n)}\equiv_n 1$ (משפט Euler)
ב. לכל מספר ראשוני p ולכל מספר a שלא מתחלק ב- p מתקיים $a^{p-1}\equiv_p 1$ (המשפט הקטן של Fermat).
<u>הערה</u>: כאן $\varphi(n)$ מספר איברים של $\mathbf{Z}_n$ הזרים ל- n, כלומר $\varphi(n)=|\mathbf{Z}_n^*|$

<u>טענה 6</u>. יהי $g\in G$ איבר כלשהו. אז
א. אם $o(g)=\infty$ אז $(<g>,*)\cong(\mathbf{Z},+)$.
ב. אם $o(g)=n<\infty$ אז $(<g>,*)\cong(\mathbf{Z}_n,+)$.

טענה 7. כל תת-חבורה של חבורה ציקלית היא גם חבורה ציקלית.

<u>הפולינום</u>. פולינום שכל מקדמיו שווים לאפס נקרא <u>פולינום-אפס</u> ויסומן כ- $0(x)$.
קבוצה של כל הפולינומים מעל R תסומן כ- $R[x]$.

אם $f(x)=\sum_{i=0}^{n} a_i x^i$ פולינום שונה מפולינום-אפס, אז <u>מעלה</u> $\underline{\deg(f(x))}$ <u>של</u> $f(x)$ מוגדרת כ- $\deg(f(x)) := \max\{i \mid a_i \neq 0\}$. אם $f(x)$ פולינום-אפס, אז $\deg(f(x)) := -\infty$. בהמשך אנו מניחים ש- $-\infty + n = -\infty$ ו $-\infty < n$ לכל מספר שלם n.

<u>הגדרה 3</u>. שני פולינומים $f(x)=\sum_{i=0}^{n} f_i x^i$ ו $g(x)=\sum_{i=0}^{m} g_i x^i$ שווים אם ורק אם הם מקיימים את התנאים הבאים:
א. $\deg(f(x)) = \deg(g(x))$.
ב. $g_i = f_i$ לכל $0 \le i \le \deg(f(x))$.

במילים אחרות שני פולינומים שווים אם ורק אם אחד מהם מתקבל מהשני ע"י

הוספה של מספר כלשהו של איברים מהצורה $0x^i$, למשל
$x^2+x^1+0x^0 = 0x^4+0x^3+x^2+x^1+0x^0$.

אם $f(x)=\sum_{i=0}^{n} f_i x^i \in R[x]$ פולינום כלשהו שונה מאפס, אז המקדם $f_{\deg(f)}$ נקרא <u>המקדם המוביל</u> של $f(x)$. פולינום ניקרא <u>פולינום מתוקן</u> אם המקדם המוביל שלו שווה ל-1.

יהיו $f(x)=\sum_{i=0}^{n} f_i x^i \in R[x]$ ו $g(x)=\sum_{i=0}^{m} g_i x^i \in R[x]$ שני פולינומים כלשהם. בלי הגבלת הכלליות אפשר להניח ש- $m \le n$. <u>סכום</u> $f(x)+g(x)$ מוגדר כפולינום
$\sum_{i=0}^{m}(f_i+g_i)x^i + \sum_{i=m+1}^{n} f_i x^i$.

$$\boxed{\deg(f(x)+g(x)) \le \max(\deg(f(x)),\deg(g(x))) \qquad (7.2)}$$

יהיו $f(x)=\sum_{i=0}^{n} f_i x^i \in R[x]$ ו $g(x)=\sum_{i=0}^{m} g_i x^i \in R[x]$ שני פולינומים כלשהם. <u>מכפלה</u> $f(x)\cdot g(x)$ מוגדרת כפולינום הבא: $f(x)\cdot g(x) := \sum_{k=0}^{m+n} h_k x^k \in R[x]$ כאשר המקדמים h_i מוגדרים ע"י הנוסחה:

$$\boxed{h_k = \sum_{j=0}^{k} g_j f_{k-j} \qquad (7.3)}$$

הרצאה 8

בהרצאה זו נניח ש- F שדה.

<u>הגדרה 1.</u> שני פולינומים $f(x),g(x)\in F[x]$ נקראים <u>פרופורציונאליים</u> (סימון, $f(x)\sim g(x)$) אם קיים $a\in F\setminus\{0\}$ כך ש- $f(x)=ag(x)$.

<u>הגדרה 2.</u> פולינום $f(x)\in F[x]$ <u>מחלק את</u> פולינום $g(x)\in F[x]$ (סימון, $f(x)\mid g(x)$) אם קיים $h(x)\in F[x]$ כך ש- $g(x)=f(x)\cdot h(x)$.

<u>טענה 1.</u> אם $f(x),g(x)\in F[x]$ שני פולינומים שונים מפולינום-אפס, אז $f(x)\mid g(x)\wedge g(x)\mid f(x)\Leftrightarrow f(x)\sim g(x)$.

<u>טענה 2. (חילוק עם שארית).</u>

אם $f(x),g(x)\in F[x]$ שני פולינומים כלשהם , $g(x)\neq 0(x)$, אז קיימים שני פולינומים $q(x),r(x)\in F[x]$ כך ש :

$$\boxed{\begin{aligned} &f(x)=q(x)\cdot g(x)+r(x) \\ &\deg(r(x))<\deg(g(x)) \end{aligned} \qquad (8.1)}$$

<u>הערה:</u> פולינום $r(x)$ נקרא <u>שארית</u> ופולינום $q(x)$ נקרא <u>מנה חלקית</u> של החילוק $f(x)$ ב- $g(x)$.

<u>הגדרה 3.</u> פולינום $d(x)\in F[x]$ נקרא <u>מחלק משותף</u> של פולינומים $f(x),g(x)\in F[x]$ אם $d(x)\mid f(x)\wedge d(x)\mid g(x)$. קבוצה של כל המחלקים המשותפים של $f(x),g(x)\in F[x]$ תסומן כ- $\mathrm{Div}(f(x),g(x))$.
מחלק משותף $d(x)\in \mathrm{Div}(f(x),g(x))$ בעל מעלה מקסימלית <u>מחלק משותף הגדול ביותר</u> (קיצור - מ.מ.ג) של הפולינומים $f(x),g(x)$. מ.מ.ג. של $f(x),g(x)$ שהוא גם פולינום מתוקן נקרא $\gcd(f(x),g(x))$.

<u>טענה 3.</u> יהיו $f(x),g(x)\in F[x],g(x)\neq 0(x)$ שני פולינומים כלשהם, אז :

א. קיים מ.מ.ג. $d(x)$ של $f(x),g(x)$.
ב. $d(x)$ שלהם שניתן להציג אותו כצירוף ליניארי $d(x)=u(x)\cdot f(x)+v(x)\cdot g(x),u(x),v(x)\in F[x]$.
ב. $d(x)$ הוא בעל מעלה מקסימלית בין כל המחלקים המשותפים.
ג. כל מחלק משותף הגדול ביותר של $f(x),g(x)$ פרופורציונאלי ל- $d(x)$.

תמורות ומספרים מרוכבים

<u>הגדרה 1</u>. קבוצה של כל התמורות של הקבוצה $\{1,2,\ldots,n\}$ נקראת <u>חבורה סימטרית</u> מדרגה n ומסומנת כ- S_n.

<u>הגדרה 2</u>. תמורה מהצורה $(i_1, i_2, \ldots, i_k)$ נקראת <u>מחזור</u>. מספר k נקרא <u>אורך המחזור</u>.

<u>טענה 1</u>. כל תמורה $f \in S_n$ ניתן לפרק באופן יחיד למכפלה של מחזורים זרים.

<u>טענה 2</u>.
א. סדר המחזור שווה לאורכו.
ב. סדר של תמורה $f \in S_n$ שווה ל- $\operatorname{lcm}(n_1, \ldots, n_k)$ כאשר $n_1, \ldots, n_k$ אורכים של המחזורים של f.

<u>הגדרה 3</u>. מחזור מאורך 2 נקרא <u>חילוף</u>.

<u>טענה 3</u>. כל תמורה $f \in S_n$ אפשר לקבל כמכפלה של חילופים.

<u>הגדרה 4</u>. תמורה שהיא מכפלה של מספר זוגי של חילופים נקראת <u>תמורה זוגית</u>.
קבוצה של כל התמורות הזוגיות מסומנת כ- A_n.

<u>טענה 4</u>. $A_n \le S_n$ ו $|A_n| = \frac{n!}{2}$.