נכתב ע"י ספיר ביתן

מבנים אלגבריים – ד"ר ארז שיינר

הערה: הסיכום נכתב בלשון נקבה (לעיתים ברבות/רבים) אך כמובן פונה לכולן/ם.
ראשית, כי אני אישה אין שום סיבה שאכתוב בלשון זכר :)
סיבה נוספת היא שהוכח מחקרית שנשים מצליחות יותר במבחנים כשפונים אליהן בלשון נקבה (גם במבחן וגם בקורס/סיכום/וואטאבר) 😊

עוד מחקר מעניין בנושא, נשים מצליחות יותר כאשר הטמפרטורה בחדר גבוהה (אצל גברים זה הפוך – ככל שהיא נמוכה יותר כך הם מצליחים יותר) :
https://journals.plos.org/plosone/article?id=10.1371%2Fjournal.pone.0216362&fbclid=IwAR1oYInLz2jmplmX9F5xppmIJaYXsraViQRAPYeLGGPNIlBJ6rIV0ggb3_k

עד לכאן, השיעור במגדר 😉

ייתכנו טעויות בסיכום, לא להסתמך על מה שכתוב כאן מבלי לראות את ההרצאות!

שיהיה בהצלחה לכולן/ם!

הרצאה 1 – 29.10.19

שלושה סוגי מבנים אלגבריים (עליהם נלמד):

- חבורה
- חוג
- שדה

יישומים למבנים האלגבריים:

- זיהוי ותיקון שגיאות
- הצפנה (הסתרה, אימות זהות הצדדים, להבטיח את שלמות ואמינות המידע).

חבורה

הגדרה: חבורה היא קבוצה G יחד עם פעולה $\cdot$ כך שמתקיימים התנאים הבאים:

- סגירות – לכל $a,b \in G$ מתקיים: $a \cdot b \in G$
- קיבוץ (אסוציאטיביות) – לכל $a,b,c \in G$ מתקיים: $a \cdot (b \cdot c) = a \cdot (b \cdot c)$
- איבר יחידה/ניטרלי – קיים $e \in G$ כך שלכל איבר בחבורה מתקיים $a \cdot e = e \cdot a = a$.
- הופכיים – לכל $a \in G$ קיים $a^{-1} \in G$ כך ש$a \cdot a^{-1} = a^{-1}a = e$.

חבורה שמקיימת את חוק החילוף נקראת חילופית(אבלית, קומוטטיבית).

דוגמא:
נסתכל על קבוצת הטבעיים $\mathbb{N} = \{1,2,3 \dots\}$. האם $\mathbb{N}$ יחד עם חיבור חבורה. אין איבר יחידה (0 לא קיים בטבעיים הנ"ל). עם 0 – אין נגדי, גם לא חבורה.

לעומת זאת, אם נסתכל על השלמים $\mathbb{Z} = \{\dots -2, -1,0,1,2 \dots\}$ עם הפעולה $+$ - חבורה.

$(\mathbb{Z},\cdot)$ לא חבורה(אין הופכי). $(\mathbb{Q},\cdot)$ לא חבורה(אין הופכי ל0).

דוגמא: $GL_n(\mathbb{R})$ = אוסף המטריצות הממשיות בגודל $n \times n$ הפיכות. האם חבורה?

1. סגירות: כפל מטריצות הפיכות – מטריצה הפיכה.
2. אסוציאטיביות – כפל מטריצות הוא אסוציאטיבי.
3. I הפיכה והיא איבר היחידה
4. הופכיים: לכל $A \in GL_n(\mathbb{R})$ קיימת A^{-1} וכמובן ש A^{-1} הפיכה ולכן $A^{-1} \in GL_n(\mathbb{R})$.

סה"כ חבורה. אך הקבוצה אינה חבורה חילופית (חילוף מטריצות הפיכות מביא תוצאה שונה).

חוג

הגדרה: חוג R הוא קבוצה יחד עם שתי פעולות $+,\cdot$ כך שמתקיימים התנאים הבאים:

- $(R,+)$ חבורה אבלית
- הכפל סגור, אסוציאטיבי, וקיים איבר יחידה כפלי.
- פילוג(דיסטריביוטיביות) – לכל $a,b,c \in R$ מתקיים
  $a \cdot (b+c) = a \cdot b + a \cdot c, (b+c) \cdot a = ba + ca$

דוגמא:

אוסף המטריצות $R^{n \times n}$ עם חיבור וכפל מטריצות הוא חוג.

$\mathbb{Z}$ עם כפל וחיבור – חוג.

הגדרה: יהי $n \in \mathbb{N} \leq 2$ נגדיר את $\mathbb{Z}_n = \{\bar{0}, \bar{1} \dots \overline{n-1}\}$ ונגדיר פעולות $\bar{a} + \bar{b} = (a+b)\ mod\ n$, $\bar{a} \cdot \bar{b} = a \cdot b\ mod\ n$.

האם $\mathbb{Z}_n$ חוג? כן.

דוגמא: $\mathbb{Z}_7 = \{\bar{0} \dots \bar{6}\}$

$\bar{2} + \bar{5} = 0$ ולכן 5 נגדי ל2.

<u>שדה</u>

<u>הגדרה</u>: שדה F הוא קבוצה עם שתי פעולות $(+,\cdot)$ כך שמתקיימים התנאים הבאים:

- $(F,+)$ חבורה אבלית.
- $\left(\frac{F}{\{o\}}, \cdot\right)$ חבורה אבלית.
- פילוג – לכל $a,b,c \in F$ מתקיים $a \cdot (b+c) = ab + ac$.

שאלה: האם $\mathbb{Z}_n$ שדה? אם ורק אם n ראשוני.

נוכיח בהמשך הקורס...

דוגמא: נביט ב$\mathbb{Z}_4$,
$\bar{0} = \bar{2} \cdot \bar{0}, \bar{2} \cdot \bar{1} = \bar{2}$, $\bar{2} \cdot \bar{2} = \bar{0}$, $\bar{2} \cdot \bar{3} = \bar{2}$. אין הופכי.

שאלה: האם יתכנו שני איברים שונים בחבורה שהם איברי יחידה?

הוכחה: נניח $e_1, e_2 \in G$ איברי יחידה. $e_1 \cdot e_2 = \boldsymbol{e_1} = e_2 \cdot e_1 = \boldsymbol{e_2}$ בסתירה לכך שהם שני איברים שונים.

תכונה של חבורות: (תכונת הצמצום) תהי חבורה G ויהיו $a,b,c \in G$ כך ש$ab = ac$ אזי $b = c$.

הוכחה: $ab = ac$ נכפיל בהופכי משני הצדדים(מובטח שיש הופכי כיוון שG חבורה):
$b = a^{-1} \cdot a \cdot b = a^{-1} \cdot a \cdot c = c$.

הרצאה 2 – 5.11.19

תזכורת: חבורה היא קבוצה עם פעולה סגורה, אסוציאטיבית, עם איבר יחידה והופכיים.

<u>הדוגמא החשובה ביותר</u>

תהי A קבוצה כלשהי, נגדיר את S_A להיות אוסף הפונקציות ההפיכות מA לA.
S_A יחד עם פעולת ההרכבה היא חבורה. החבורה הסימטרית/ חבורת התמורות.
S_n קבוצת הפונקציות ההפיכות מקבוצה בגודל n לעצמה.
כל פעולה ניתן להציג כהרכבה של פונקציות (כל חבורה הינה תת חבורה של החבורה הזו).

נוכיח כעת כי S_A חבורה:

- סגירות – תהיינה $f,g \in S_A$ שתי פונקציות הפיכות אז $f \circ g \in S_A$.
- קיבוץ (אסוציאטיביות) – הרכבת פונקציות היא אסוציאטיבית.
- איבר יחידה/ניטרלי – פונקציית הזהות הינה הפיכה ולכן בהכרח נמצאת בS_A ומהווה איבר יחידה $(I_A \circ f = f \circ I_A)$.
- הופכיים – תהי $f \in S_A$ לכן f הפיכה לכן קיימת f^{-1}. כיוון שf^{-1} הפיכה אזי $f^{-1} \in S_A$.

<u>הגדרה</u>: תהי חבורה G, H נקראת תת חבורה של G אם מתקיימים:

- $H \subseteq G$
- H חבורה ביחס לפעולה של G.

קריטריון מקוצר לבדיקת תת חבורה: תהי חבורה G ותהי $H \subseteq G$ אזי H תת חבורה של G אם"ם מתקיימים:

- $e_G \in H$ – איבר היחידה של G נמצא בH.
- לכל $a,b \in H$ מתקיים $a \cdot b^{-1} \in H$.

הוכחה:
$\Leftarrow$ נניח שH תת חבורה, צ"ל את שני התנאים:

1. H חבורה ולכן $e_G \in H$:

$$e_H \cdot e_H = e_H$$
$$e_G \cdot e_H = e_H$$
$$e_H e_H = e_G e_H \rightarrow e_H = e_G \rightarrow e_G \in H$$

2. יהיו $a,b \in H$ צ"ל $a \cdot b^{-1} \in H$
נסמן ב$c \in H$ את ההופכי של b בH ולכן: $c \cdot b = e_H = e_G$.
$$b^{-1} \cdot b = e_G \rightarrow c \cdot b = b^{-1} b \rightarrow c = b^{-1}$$

$\Rightarrow$ נתון שמתקיימים שני התנאים. צ"ל שH תת חבורה.
נתון:

1. $e_G \in H$
2. לכל $a,b \in H$ מתקיים $a \cdot b^{-1} \in H$

נוכיח חבורה:

אסוציאטיביות: הפעולה על G אסוציאטיבית לכל איבר בG ובפרט לכל איבר בH.
איבר יחידה: נתון $e_G \in H$, e_G איבר יחידה בG ולכן בפרט גם בH.
הופכי: יהי $a \in H$ צ"ל $a^{-1} \in H$. נתון $e_G \in H$ ולכן לפי (2) $e_G \cdot a^{-1} \in H$ ולכן $a^{-1} \in H$.
סגירות: יהיו $a,b \in H$ צ"ל ש$a \cdot b \in H$.
$b \in H$ ולכן $b^{-1} \in H$, ולפי (2) $a \cdot (b^{-1})^{-1} \in H$. כעת $(b^{-1})^{-1} = b$ וקיבלנו $a \cdot b \in H$.

דוגמאות:

$GL_n(\mathbb{R})$= מטריצות הפיכות עם כפל.
$SL_n(\mathbb{R}) \subseteq GL_n(\mathbb{R})$ = כל המטריצות עם דטרמיננטה 1.

נוכיח שמדובר בתת חבורה:

1. $|I| = 1$ כי $I \in SL_n(\mathbb{R})$
2. תהיינה $A, B \in SL_n(\mathbb{R})$, צ"ל $A \cdot B^{-1} \in SL_n(\mathbb{R})$. צ"ל $|A \cdot B^{-1}| = 1$

$$|A \cdot B^{-1}| = |A| \cdot |B^{-1}| = \frac{|A|}{|B|} = \frac{1}{1} = 1$$

דוגמא: נביט בחבורה $GL_2(\mathbb{R})$ ונביט בקבוצה $A = \left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \middle| a^2 + b^2 \neq 0 \right\}$.
$\begin{vmatrix} a & b \\ -b & a \end{vmatrix} = a^2 + b^2$ ולכן $A \subseteq GL_2(\mathbb{R})$ אפשר להוכיח שA תת חבורה.

$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix} \cdot \begin{pmatrix} c & d \\ -d & c \end{pmatrix} = \begin{pmatrix} ac - bd & ad + bc \\ -(ad + bc) & ac - bd \end{pmatrix}$$

$A = \frac{\mathbb{C}}{\{0\}}$ חבורה ביחס לכפל.

שאלה: כיצד נסמן את התוצאה של הפעלת הפעולה על איבר עם עצמו n פעמים?

<u>הגדרה</u>: תהי חבורה G, לכל n טבעי נגדיר: $a^n = \underbrace{a \dots a}_{n}$ (כמו שלמדנו בתרגול). $a^0 = e_G$.
$a^{-n} = (a^{-1})^n = (a^n)^{-1}$.

<u>הגדרה + טענה</u>: תהי חבורה G ויהי $a \in G$ נגדיר את *תת החבורה הציקלית*(צריך להוכיח שהיא תת חבורה ! נוכיח בשיעור הבא) $< a \geq \{a^n | n \in \mathbb{Z}\}$.

דוגמא: נביט בחבורה $(\mathbb{Z}, +)$, $< 2 \geq \{\dots -4, -2, 0(e_G), 2, 4, 6, 8 \dots\}$.

הרצאה 3 – 19.11.19

תזכורת: תהי חבורה G, ויהי $a \in G$ אזי $a^n = \underbrace{a \dots a}_{n}$, $a^{-n} = \underbrace{a^{-1} \dots a^{-1}}_{n}$, $a^0 = e$.

<u>הגדרה</u>: תהי חבורה G ויהי $a \in G$ נגדיר: $< a > = \{a^n | n \in \mathbb{Z}\} \subseteq G$ ***תת החבורה הציקלית.***

נוכיח שהקבוצה $< a >$ היא תת חבורה של G.

הוכחה:

1. $a^0 \in < a >$ ולכן איבר היחידה נמצא בתת החבורה הציקלית.
2. יהיו $a^k, a^n \in < a >$, צ"ל ש $a^k * (a^n)^{-1} \in < a >$,
   אבל $a^k * (a^n)^{-1} = a^k * (a^{-1})^n = a^{k-n} \in < a >$.

מ.ש.ל

<u>הגדרה</u>: תהי G חבורה ויהי $a \in G$ חבורה נגדיר את ***הסדר*** של a להיות המספר החיובי n הקטן ביותר עבורו $a^n = e$ מסומן $o(a) = n$. אם לא קיים מספר כזה אומרים ש $o(a) = \infty$.

דוגמא: נביט בחבורה $(\mathbb{C}\backslash\{0\}, \cdot)$: ... $1,2,4,8,16 \dots \geq 2 > \cdots \frac{1}{8}, \frac{1}{4}, \frac{1}{2}$ האם חזרנו לאיבר היחידה? לא, ולכן $o(2) = \infty$.

- שאלה: האם כל איבר בחבורה אינסופית חייב להיות מסדר אינסוף? איבר היחידה תמיד לא, הסדר של איבר היחידה הוא תמיד $o(e) = 1$.
  שאלה נוספת: מלבד איבר היחידה האם כל איבר בחבורה אינסופית חייב להיות מסדר אינסוף? לא.

נסתכל על: $1, -1 \geq -1 >$, קל לראות ש $0(-1) = 2$. ועל: $< i \geq 1, i, -1, -i$ והסדר: $o(i) = 4$.

טענה: תהי חבורה G ויהי $a \in G$ אזי הגודל של תת החבורה הציקלית: $o(a) = | < a > |$.
הערה: לכן, נהוג לקרוא לגודל של תת חבורה הסדר שלה.

משפט(חלוקה עם שארית): יהי $n \in \mathbb{N}$ ו $k \in \mathbb{Z}$ קיימים q, r יחידים כך ש:

1. $k = q \cdot n + r$
2. $0 \leq r \leq n - 1$

הוכחת הטענה:

מקרה 1: $o(a) = n \in \mathbb{N}$ סופי.
צ"ל $n = | < a > |$.

ראשית, נוכיח $< a \geq e, a, a^2 \dots a^{n-1}$.
שנית, נוכיח שכל שני איברים מבין $e, a, a^2 \dots a^{n-1}$ הם שונים ולכן $| < a > | = n$.

$\supseteq$ ברור שהקבוצה $e, a, a^2 \dots a^{n-1}$ מוכלת ב $< a >$=אוסף כל החזקות של a.

כעת, נוכיח הכלה בכיוון ההפוך. יהי $a^k \in a$ צ"ל שהוא שייך ל $\{e, a, a^2 \dots a^{n-1}\}$. נחלק את k ב n ונקבל ש $k = q \cdot m + r$(לפי משפט חלוקה עם שארית).
לדוגמא $-8 = -2 \cdot 7 + 6$. השארית היא 6.

$\subseteq$ נזכור ש $a^n = e$ כי $o(a) = n$. וידוע לנו ש $a^k = a^{q \cdot n + r} = a^{q \cdot n} \cdot a^r = (a^n)^q \cdot a^r = e^q \cdot a^r = a^r$ לכן $0 \leq r \leq n - 1 < a \geq e, a, a^2 \dots a^{n-1}$ שזה החלק הראשון של ההוכחה.

נניח בשלילה שקיים $0 \leq r_1 < r_2 < n - 1$ כך ש $a^{r_1} = a^{r_2}$.

נכפול את שני הצדדים בa^{-r_1} ונקבל: $e = a^{r_2-r_1}$. $0 < r_2 - r_1 \leq r_2 \leq n-1$ כלומר, מצאנו חזקה חיובית קטנה מn כך ש$a^n = e$ בסתירה לכך ש$o(a) = n$.

מקרה 2: נניח $o(a) = \infty$.

צ"ל $\infty = |< a >|$.

נניח בשלילה ש $|< a >|$ סופי. לכן קיימים $0 < r_1 < r_2$ כך ש$a^{r_1} = a^{r_2}$. נכפול בa^{-r_1} ונקבל $e = a^{r_2-r_1}$. קיבלנו שקיימת חזקה חיובית עבורה $a^{r_2-r_1} = e$ בסתירה לכך ש$o(a) = \infty$.

שאלה: ראינו שבחבורה אינסופית יתכן $o(a) = n, o(a) = \infty$. האם גם בחבורות סופיות זה אפשרי?
לא.
טענה: תהי G חבורה סופית ויהי $a \in G$ אזי $o(a)$ סופי.
הוכחה: $\underset{\text{סופי}}{G} > |< a >| = o(a)$.

תזכורת: *חבורת התמורות* S_n היא חבורת כל הפונקציות ההפיכות מקבוצה בגודל n לעצמה עם הרכבה.(תזכורת: החבורה החשובה ביותר כי כל חבורה בעולם היא במובן מסוים תת חבורה של חבורת התמורות).

דוגמא: בS_3 נסמן פונקציות (תמורות) בצורה הבאה (דוגמא):
$$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$$

כלומר – בשורה הראשונה נרשום כל איבר בקבוצה ובשורה השנייה נרשום לאן כל איבר הולך(לדוגמא $2 \to 3$).

כמה איברים יש בS_n(או בצורה אחרת – כמה פונקציות הפיכות יש בS_n)? שקול לשאלה בכמה דרכים ניתן לסדר n איברים? והתשובה היא כמובן $n!$ (ההוכחה היא מקומבינטוריקה – באינדוקציה). לכן, כמות התמורות היא $|S_n| = n!$.

דוגמא: $S_3 = \left\{ I, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \right\}$.

(הערה: כיוון שהפונקציה היא על כל האיברים אמורים להופיע בשורה השנייה, וכיוון שהיא חח"ע כל אחד מופיע בדיוק פעם אחת, לכן ההבדל בין פונקציה אחת לאחרת היא באיזה סדר המספרים מופיעים).

<u>הגדרה</u>: נסמן ב$(a_1, a_2 \dots a_k) \in S_k$ את התמורה f המוגדרת ע"י:
אם $i \neq a_1 \dots a_k$ אז $f(i) = i$.
אחרת, אם קיים $0 \leq j < k-1$ אזי $f(a_j) = a_{j+1}$ וגם $f(a_k) = a_k$.

דוגמא: $(7\ 1\ 2) \in S_7$, $f = \begin{pmatrix} 1 & 2 & 34 & 56 & 7 \\ 2 & 7 & 34 & 56 & 1 \end{pmatrix}$.

האם כל תמורה היא מחזור? לא. אבל כל תמורה ניתן להציג כהרכבה של מחזורים זרים.
דוגמא: נביט ב$(12)(34) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$. זה לא מחזור אך כן הרכבה של מחזורים זרים.

<u>הגדרה</u>:

תהי $f \in S_n$, נגדיר את *סימן התמורה* ע"י

$$sign(f) = \prod_{\text{זוגות } i,j} \frac{X_{f_i} - X_{f_j}}{X_i - X_j}$$

כאשר $X_1 \dots X_n$ משתנים.

דוגמא: נביט בפונקציה $f = \begin{pmatrix}1 & 2 & 3\\ 3 & 1 & 2\end{pmatrix} = (1,3,2) \in S_3$, ונרצה לדעת מה הסימן של התמורה הזו.

$$sign(f) = \frac{X_3 - X_1}{X_1 - X_2} \cdot \frac{X_1 - X_2}{X_2 - X_3} \cdot \frac{X_3 - X_2}{X_1 - X_3} = -1 \cdot -1 = 1$$

בעצם המשוואה הזו סופרת כמה שינויים היו וקובעת את סוג הסימן לפי מספר השינויים(הסבר בהמשך).

$$sign(f) = \pm 1$$

אם $sign(f) = 1$ אומרים שf זוגית או חיובית ואם $sign(f) = -1$ אומרים שf אי-זוגית או שלילית.

שאלה (חשובה ביותר): $sign(f \circ g) =$?

תשובה: $sign(f \circ g) = sign(f) \cdot sign(g)$(הוכחה בהרצאה הבאה).

דוגמא(די חשוב): $sign(I) = \prod_{i,j \text{ זוגות}} \frac{X_i - X_j}{X_i - X_j} = 1$ תמיד!

<u>הגדרה</u>: מחזור באורך 2 נקרא חילוף.

דוגמא: נחשב את הסימן של חילוף:

$$sign\big((1\ 2)\big) = \frac{X_2 - X_1}{X_1 - X_2} \cdot \frac{X_2 - X_3}{X_1 - X_3} \cdot \dots \cdot \frac{X_2 - X_n}{X_1 - X_n} \cdot \frac{X_1 - X_3}{X_2 - X_3} \cdot \frac{X_1 - X_4}{X_2 - X_4} \cdot \dots \cdot \frac{X_1 - X_n}{X_2 - X_n} \cdot \frac{X_3 - X_4}{X_3 - X_4} \cdot \dots \cdot \frac{X_{n-1} - X_n}{X_{n-1} - X_n} = -1$$

(שמות האיברים בקבוצה חסרי משמעות, לכן ניתן לקרוא להם 1,2)

הרצאה 4 – 26.11.2019

תזכורת: אנו עוסקים כרגע בחבורת התמורות S_n(הפונקציות ההפיכות)
הגדרנו לכל תמורה $f \in S_n$:

$$sign(f) = \prod_{\text{זוגות } i,j} \frac{X_{f_i} - X_{f_j}}{X_i - X_j}$$

והוכחנו $sign\Big((a_i, a_j)\Big) = -1$.

משפט: $sign(f \circ g) = sign(f) \cdot sign(g)$.
הוכחה:

$$sign(f \circ g) = \prod_{\text{זוגות } i,j} \frac{X_{f(g(i))} - X_{f(g(j))}}{X_i - X_j}$$

$$= \underbrace{\prod_{\text{זוגות } i,j} \frac{X_{f(g(i))} - X_{f(g(j))}}{X_{g(i)} - X_{g(j)}}}_{sign(f)} \cdot \underbrace{\frac{X_{g(i)} - X_{g(j))}}{X_i - X_j}}_{sign(g)} = sign(f) \cdot sign(g)$$

במכנה רצים על כל הזוגות האפשריים ומעל כל זוג – f של האיבר הזה ולכן סה"כ החלק הראשון של המכפלה שווה ל$sign(f)$. והחלק השני של המכפלה ברור.

כעת נרצה להראות שניתן להציג כל מחזור כחילופים.

טענה: $(a_1 \dots a_k) = (a_1\ a_2)(a_2\ a_3) \dots (a_{k-1}a_k)$

דוגמא: נביט במחזור $(7\ 1\ 2\ 4) = (24)(12)(71)$

הוכחת הטענה: עבור $x \neq a_1 \dots a_k$ מתקיים: $(a_1 \dots a_k)_{(x)} = x$ וגם $(a_1\ a_2) \dots (a_{k-1}\ a_k)_{(x)} = x$
כעת, נביט ב$1 \leq i \leq k-1$, $x = a_i$ מתקיים: $(a_1 \dots a_k)_{(a_i)} = a_{i+1}$ וגם:
$(a_1\ a_2)(a_2\ a_3) \dots (a_{i-1}\ a_i)(a_i\ a_{i+1}) \dots (a_{k-1}\ a_k)_{(a_i)} = a_{i+1}$.

רק מהעובדה שהמחזור חח"ע ועל ניתן להגיד שגם a_k מגיע למקומו($k-1$ איברים הגיעו למקום הנכון ולכן יש רק מקום אחד אליו a_k יכול להגיע) אבל נוכיח בכל זאת:

עבור a_k: $(a_1 \dots a_k)_{(a_k)} = a_1$ וגם: $(a_1\ a_2)(a_2\ a_3) \dots . (a_{k-1}\ a_k)_{(a_k)}$

מסקנה:

$$sign\big((a_1 \dots a_k)\big) = sign\big((a_1\ a_2)(a_2\ a_3) \dots (a_{k-1}\ a_k)\big)$$
$$= sign\big((a_1\ a_2)\big) \cdot \dots sign\big((a_{k-1}\ a_k)\big) = (-1)^{k-1}$$

דוגמא: $sign(7\ 1\ 2\ 4) = (-1)^3 = -1$.

דוגמא: $f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 7 & 4 & 1 & 2 & 3 & 6 & 3 \end{pmatrix} = (1\ 7\ 5\ 3)(2\ 4) \rightarrow sign(f) = (-1) \cdot (-1) = 1$.

הומומורפיזמים ואיזומורפיזמים

הגדרה: תהיינה שתי חבורות G, H ותהי פונקציה $f: G \rightarrow H$, אזי f נקראת *הומומורפיזם* אם לכל $a, b \in G$ מתקיים $f(a \cdot b) = f(a) \cdot f(b)$ כאשר הפעולה בצד שמאל היא של G ובצד ימין של H.

כמו כן, *הומומורפיזם* הפיך נקרא *איזומורפיזם*.

אזהרה 😉 : החלק הבא נכתב לפי ההסבר שארז נתן בע"פ, יכול להיות שזה לא כל כך מדויק ושפספסתי חלק, מומלץ לבדוק 😊

מה זה איזומורפיזם?
הוא אומר שG,H הם "אותה גברת בשינוי אדרת" (לפי ארז 😉)
דוגמא:

$$G = \{Elad, Erez, Dana, Alice\}, e_G = Erez$$

$$Elad \cdot Erez = Elad$$

$$H = \{Bob, Sponge, Dorin, Sandy\}$$

$$f = \begin{pmatrix} Elad & Erez & Dana & Alice \\ Bob & Sponge & Dorin & Sandy \end{pmatrix}$$

כעת, לפי ההגדרה של איזומורפיזם, אם מתקיים $Elad \cdot Erez = Elad$ אזי בחבורה החדשה צריך להתקיים: $Bob \cdot Sponge = Bob$ו $e = Bob$.

ולפי הומומורפיזם $\{Elad, Erez, Dana, Alice\} \to Boy, Girl$(כשהשליחה היא לפי שמות של זכר ונקבה). הקבוצה אליה נשלח איבר היחידה היא איבר היחידה(נוכיח בהמשך) ולכן במקרה הזה איבר היחידה יהיה $e = Boy$.

אם $Elad \cdot Dana = Alice$ אזי $Boy \cdot Girl = Girl$

הומומורפיזם אומר נחלק את האיברים לקבוצות והקבוצות יתנהגו כמו החבורה השנייה.

<u>טענה</u>: יהי הומומורפיזם $f: H \to G$ אזי

1. $f(e_G) = e_H$
2. לכל $a \in G$ מתקיים $f(a^{-1}) = \big(f(a)\big)^{-1}$ (הסוגריים חשובים, לא נכון לכתוב $(f^{-1}(a)$)

הוכחה:

1. $f(e_G) = f(e_G e_G) = f(e_G) \cdot f(e_G)$, נכפיל את שני הצדדים בהופכי של $f(e_G)$ ונקבל: $e_H = f(e_G)$(מותר להכפיל בהופכי כיוון שזו חבורה).
2. צ"ל שההופכי של $f(a)$ הוא $f(a^{-1})$.
כלומר, צ"ל $f(a) \cdot f(a^{-1}) = f(a^{-1}) \cdot f(a) = e_H$.
$f(a)f(a^{-1}) = f(a \cdot a^{-1}) = f(e_G) = e_H$
והצד השני דומה.

הערה: אם $a, b \in G$ ו$a \cdot b = e$ אזי $b = a^{-1}$.

<u>הגדרה</u>: יהי $f: G \to H$ הומומורפיזם נגדיר $Im(f) = \{f(a) | a \in G\} \subseteq H$.
$\ker(f) = \{a \in G | f(a) = e_H\} \subseteq G$.

ההומומורפיזם יהיה חח"ע אם הגרעין מכיל רק את איבר היחידה.

<u>טענה</u>: יהי f הומומורפיזם אזי התמונה היא תת חבורה של H והגרעין הוא תת חבורה של G.

נוכיח עבור התמונה:

1. צ"ל שמתקיים $e_H \in Im(f)$
אכן $f(e_G) = e_H$ ולכן $e_H \in Im(f)$
2. יהיו $h_1, h_2 \in Im(f)$ צ"ל $h_1^{-1}h_2 \in Im(f)$.
קיימים $g_1, g_2 \in G$ כך ש$f(g_1) = h_1 . f(g_2) = h_2$
$h_1^{-1}h_2 = f((g_1))^{-1}f(g_2) = f(g_1^{-1})f(g_2) = f(g_1^{-1}g_2) \in Im(f)$

<u>משפט קיילי</u>

כל חבורה איזומורפית לתת חבורה של חבורת תמורות(כל חבורה היא במידה מסוימת תת חבורה של חבורת התמורות).

<u>שיכון קיילי</u>

תהי חבורה G ונביט בחבורת התמורות S_G. רוצים להתאים לכל איבר $a \in G$ פונקציה $f_a \in S_G$.

$f_a: G \to G$, נגדיר את f_a ע"י : $f_a(x) = a \cdot x$.

צ"ל f_a הפיכה על מנת ש$f_a \in S_G$

ונגדיר את שיכון קיילי: $\varphi: G \to S_G$ כך שמתקיים $\varphi(a) = f_a$.

נוכיח שf_a הפיכה(חח"ע ועל); אם G סופית, חח"ע גורר על ולכן אין צורך להוכיח גם וגם.

חח"ע: יהיו $x_1, x_2 \in G$ כך ש$f_a(x_1) = f_a(x_2) \to ax_1 = ax_2 \to x_1 = x_2$

על: יהי $y \in G$ צריך למצוא מקור $x \in G$ כך ש$f_a(x) = y$. כלומר, $ax = y$. אז נבחר $x = a^{-1}y$ ולכן $f(a^{-1}y) = y$.

דוגמא: $G = (\mathbb{Z}_3, +)$
$\varphi: G \to S_G$.

בחבורה G ישנם 3 איברים ולכן בS_G יש 6 פונקציות. נבחר 3 פונקציות איזומורפיות לחבורה G.

$$G = \bar{0}, \bar{1}, \bar{2}$$

$$S_G\{I, \begin{pmatrix} 0 & 1 & 2 \\ 0 & 2 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 2 \\ 1 & 0 & 2 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 2 \\ 1 & 2 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 2 \\ 2 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 2 \\ 2 & 1 & 0 \end{pmatrix}\}$$

שיכון קיילי:

$$\varphi(\bar{0}) = f_{\bar{0}}$$

$$f_{\bar{0}}(x) = \bar{0} + x = x \to f_0 = I$$

באופן דומה: $\varphi(1) = f_1$, $f_{\bar{1}}(x) = \bar{1} + x \to f_1 = \begin{pmatrix} 0 & 1 & 2 \\ 1 & 2 & 0 \end{pmatrix}$

ו$f_{\bar{2}}(x) = \bar{2} + x = \begin{pmatrix} 0 & 1 & 2 \\ 2 & 0 & 1 \end{pmatrix}$,

כעת נביט ב$\bar{0} = \bar{1} + \bar{2}$ וקל לראות שההרכבה של שתי הפונקציות f_1, f_2 תיתן את f_0.

הרצאה 5 – 3.12.19

תזכורת: הגדרנו את שיכון קיילי $f: G \to S_G$

$$\varphi(a) = f_a = a \cdot x$$

אכן $f_a \in S_G$

נוכיח ששיכון קיילי הוא הומומורפיזם וחח"ע.

ואז $\varphi: G \to Im(\varphi)$ איזומורפית ולכן G איזומורפית ל$Im(\varphi)$ שהיא תת חבורה של חבורת התמורות (משפט קיילי).

נוכיח שφ הומומורפיזם:

יהיו $a, b \in G$ צ"ל $\varphi(a \cdot b) = \varphi(a) \circ \varphi(b)$. כלומר, צ"ל $f_{ab} = f_a \circ f_b$.

יהי $x \in G$ צ"ל ש$(ab)x = f_{ab}(x) = f_a(x) \circ f_b(x) = f_a\big(f_b(x)\big) = a(bx)$ כיוון שG אסוציאטיבית מתקיים: $(ab)x = a(bx)$.

נוכיח שφ חח"ע:

יהיו $a, b \in G$ כך ש$\varphi(a) = \varphi(b)$ צ"ל $a = b$.

נתון $f_a = f_b$, לכן $f_a(e) = f_b(e)$ ומתקיים $a = ae = be = b$.

משפט קיילי: תהי חבורה G אזי היא איזומורפית לתת חבורה של S_G.
הוכחה: $\varphi: G \to Im(\varphi)$ היא איזומורפיזם.

משפט לגראנז'

דוגמא: החבורה $\mathbb{Z}_6 = \bar{0} \dots \bar{5}$, נביט בתת החבורה הציקלית: $< \bar{3} \geq \bar{0}, \bar{3}$.

הגדרה: תהי חבורה G ותהי תת חבורה H ויהי $a \in G$, נגדיר את *המחלקה* $a \cdot H = \{a \cdot h | h \in H\}$.

($eH = H$ תמיד).

נראה את המחלקות בדוגמא: $\bar{0} + H = \{\bar{0}, \bar{3}\} = \bar{3} + H$, $\bar{1} + H = \{\bar{1}, \bar{4}\} = \bar{4} + H$,
$\bar{2} + H = \{\bar{2}, \bar{5}\} = \bar{5} + H$.

האם המחלקה היא תמיד תת חבורה? לא, אין את איבר היחידה.

קל לראות מהדוגמא שגודל תת החבורה חייב לחלק את גודל החבורה(בערך מה שמשפט לגראנז' אומר – נראה בהמשך הגדרה מדויקת).

טענה: תהי חבורה G ותהי תת חבורה H נגדיר יחס על G $aRb \Leftrightarrow a^{-1}b \in H$. אזי R יחס שקילות וכמו כן $[a]_R = aH$.

מסקנה: המחלקות זרות ומכסות את כל G.

נדגים באמצעות הדוגמא הקודמת: $\bar{1}R\bar{4} \Leftrightarrow \bar{3} = \bar{5} + \bar{4} \in H$ - מתקיים, אבל $\bar{4}R\bar{5} \Leftrightarrow \bar{2} + \bar{5} \in H$ ולכן לא מתקיים – $1 \notin H$.

הוכחת הטענה:
ראשית, נוכיח שמדובר ביחס שקילות:

- רפלקסיבי: יהי $a \in G$ צ"ל aRa, כלומר צ"ל $a^{-1}a \in H$ וזה נכון כיוון ש$a^{-1}a = e \in H$.
- סימטרי: יהיו $a, b \in G$ כך שaRb צ"ל bRa:
  נתון: $a^{-1}b \in H$, צ"ל $b^{-1}a \in H$. $a^{-1}b \in H$ ולכן $b^{-1}a = (a^{-1}b)^{-1} \in H$.

- טרנזיטיבי: יהיו $a,b,c \in G$ כך ש aRb, bRc צ"ל aRc.
  נתון: $a^{-1}b \in H, b^{-1}c \in H$ צ"ל $a^{-1}c \in H$:
  $a^{-1}c = (a^{-1}b)(b^{-1}c) \in H$

כעת נוכיח שלכל $a \in G$ מתקיים $[a]_R = aH$

ניזכר מה היא מחלקת שקילות:
$$[a]_R\{b \in G | aRb\} = \{b | a^{-1}b \in H\} = \{b | \exists\, h \in H, a^{-1}b = h\} = \{b | \exists h \in H : b = aH\}$$
$$= \{ah | h \in H\} = aH$$

נזכור את המסקנה: המחלקות aH מחלקות את G לקבוצות זרות.

נותר להוכיח שלכל $a \in G$ מתקיים $|aH| = |H|$

נבנה $f: H \to aH$ שהיא חח"ע ועל: $f(h) = ah$ צ"ל שf חח"ע ועל.

הוכחה: על: יהי aH במחלקה, המקור שלו הוא h.
חח"ע: יהיו $h_1, h_2 \in H$ כך ש$f(h_1) = f(h_2)$, צ"ל $h_1 = h_2$.
נתון: $a \cdot h_1 = a \cdot h_2 \to h_1 = h_2$.

<u>הגדרה</u>: תהי חבורה G ותהי H תת חבורה אזי כמות המחלקות שH מייצרת נקראת *האינדקס* ומסומנת $[G:H]$.

בדוגמא: $G = \mathbb{Z}_6, H = \bar{0}, \bar{3}$, ו$[G:H] = 3$. קל לראות ש $|G| = [G:H] \cdot |H|$.

<u>משפט לגראנז'</u>: תהי חבורה סופית G ותהי תת חבורה H אזי $|G| = [G:H] \cdot |H|$
הוכחה: ראינו שH מחלקת את G ל$[G:H]$ מחלקות זרות שכולן בגודל $|H|$.

מסקנות:

- תהי G חבורה סופית ותהי H תת חבורה אזי *הסדר* של H ($|H|$) מחלק את *הסדר* של G.
- תהי G חבורה סופית ויהי $a \in G$ אזי הסדר של a מחלק את הסדר של G.
  הוכחה: $o(a) = |< a >|$ ו$|< a >|$ מחלק את G.

<u>הגדרה</u>: חבורה נקראת ציקלית אם היא נוצרת ע"י איבר אחד, כלומר: $a \in G$ וגם $G \geq < a >$

דוגמא: נביט בחבורה $\mathbb{Z}_6 = \bar{0} \dots \bar{5}$, האם היא חבורה ציקלית? כן, כיוון ש$\mathbb{Z}_6 \geq < \bar{1} >$.
הערה: נכון לכל $\mathbb{Z}_n$.

דוגמא: $\mathbb{Z}_2 X \mathbb{Z}_2 = (0,0), (1,0), (0,1), (1,1)$

$$< (0,0) \geq \{(0,0)\}, < 1,0 \geq (0,0), (1,0)$$

באופן דומה, אפשר לראות שהחבורה לא נוצרת מאף איבר יחיד.

<u>טענה</u>: תהי G חבורה מסדר ראשוני, אזי G ציקלית.
הוכחה: ניקח $a \neq e \in G$, מתקיים: $o(a)$ מחלק את $|G|$ ולכן $o(a) = |G| \vee o(a) = 1$ אבל $a \neq e$ ולכן $o(a) = |G|$. וכיוון ש $G \geq < a > \to |G| = | < a > | = o(a). < a > \subseteq G$.

כיוון שהחבורות סופיות G היא ציקלית.

דוגמא: $\mathbb{Z}_7 = \bar{0}, \bar{1} \dots \bar{7}$, $< \bar{3} \geq < \bar{0}, \bar{3}, \bar{6}, \bar{2}, \bar{5}, \bar{1}, \bar{4}$

מסקנה: כל החבורות מסדר ראשוני ציקליות ואיזומורפיות ל$\mathbb{Z}_n$. כי כל תתי החבורות הציקליות מגודל מסוים איזומורפיות אחת לשנייה.

משפט חלוקה עם שארית: יהי $n \in \mathbb{Z}$ ויהי $k \in \mathbb{Z}$ אזיק יימים $q, r \in \mathbb{Z}$ <u>יחידים</u> כך ש$k = q \cdot n + r$ וגם $0 \leq r \leq n - 1$.

r נקראת שארית וq נקראת מנה.

דוגמאות:

$$20 = 2 \cdot 7 + 6, -20 = -3 \cdot 7 + 1$$

הוכחה:

<u>קיום</u>: מקרה ראשון: $k \geq 0$. נעשה אינדוקציה על k.
עבור $k = 0$: $0 = 0 \cdot n + 0$. הטענה נכונה עבור $k = 0$.
יהי k עבורו הטענה נכונה, צריך להוכיח עבור $k + 1$.
נתון: $k = q \cdot n + r$, נוסיף 1 לשני האגפים ונקבל: $k + 1 = q \cdot n + r + 1$.

אם $0 \leq r < n - 2$ אזי $1 \leq r + 1 \leq n - 1$ ומצאנו את החלוקה בשארית.
אחרת, $r = n - 1$ אז $k + 1 = q \cdot n + r + 1 = q \cdot n + n = n \cdot (q + 1) + 0$

מ.ש.ל

מקרה שני: $k < 0$, לכן $-k > 0$ וניתן להציג אותו כך: $-k = q \cdot n + r$ כך ש$0 \leq r \leq n - 1$.

$$k = (-q)n + (-r)$$

אם $r = 0$ אז סיימנו. אחרת, אם $1 \leq r \leq n - 1$ אז נוסיף n ונחסר n ונקבל
$k = (-q)n + n + (n - r) = (-q)(n + 1) + (n - r)$, $1 \leq n - r \leq n - 1$.קיבלנו חלוקה עם שארית.

<u>יחידות</u>: $k = q_1 n + r_1 = q_2 n + r_2$, צ"ל $q_1 = q_2, r_1 = r_2$

נתון: $q_1 n - q_2 n = r_2 - r_1$ נוציא n ונקבל: $n(q_1 - q_2) = r_2 - r_1$, $-(n - 1) \leq r_2 - r_1 \leq n - 1$

ו... $n(q_1 - q_2) = \cdots -2n, -n, 0, n, 2n$ וההתנגשות היחידה היא ב0. ולכן שני הצדדים שווים 0,
כלומר $q_1 = q_2, r_1 = r_2$.
מ.ש.ל

הרצאה 6 – 10.12.2019

תזכורת: למדנו משפט חלוקה עם שארית. אם $k \in \mathbb{Z}, n \in \mathbb{N}$ קיימים $q, r \in \mathbb{N}$ יחידים כך ש $k = q \cdot n + r$ ו$0 \le r \le n - 1$.

נזכור את יחס השקילות מוד n, $a \equiv bmodn$, אם"ם $a = p \cdot n + b$.
בפרט אם r היא השארית של החלוקה של k בn, אז $k \equiv rmodn$

שאלה: נניח $a \equiv r_a modn, b \equiv r_b modn$, האם $a \cdot b \equiv r_a r_b modn$ כן?
הוכחה: נכפיל ונקבל: $a = q_a n + r_a, b = q_b n + r_b$,
$$ab = (q_a n + r_a) \cdot (q_b n + r_b) = q_a q_b n^2 + q_a n r_b + q_b n r_b + r_a r_b$$
$$= n(q_a q_b + q_a r_b + q_b r_a) + r_a r_b \to ab \equiv r_a r_b modn$$

ולכן $a^k \equiv r_a^k modn$

שאלה: נניח $a \equiv bmodn$ האם $c^a \equiv c^b modn$
דוגמא: $4 \equiv 1mod3, 2^4 \equiv 1mod3, 2^1 \not\equiv 1mod3$ - הפרכה.

<u>הגדרה</u>: יהיו n, k טבעיים, נגדיר את $gcd(n,k)$ להיות הטבעי הגדול ביותר שמחלק את n וגם את k.
דוגמא: $gcd(6,15) = 3$

<u>הגדרה</u>: k, n נקראים זרים אם $gcd(n,k) = 1$.

<u>טענה</u>: יהיו $k < n \in \mathbb{N}$ כך ש$gcd(k,n) = gcd(k, n-k)$
דוגמא: $gcd(6,15) = gcd(6,9) = gcd(6,3) = gcd(3,3) = 3$
הוכחת הטענה: נוכיח שקבוצת המחלקים המשותפים של n, k שווה לקבוצת המחלקים המשותפים של $k, n-k$.
בכיוון אחד אם a מחלק את n וגם את k, צ"ל שa מחלק את $n-k$. כיוון שn הוא כפולה שלמה של a $(n = ta)$ וגם k הוא כפולה שלמה של a $(k = sa)$, אז מתקיים $n - k = (t-s) \cdot n$, גם הוא כפולה שלמה של a.
בכיוון שני, אם a מחלק את $k, n-k$ כלומר: $k = ta, n-k = sa$ אז $n = (t+s) \cdot a$ ולכן a מחלק גם את n.

<u>טענה</u>: יהיו $l, k \in \mathbb{N}$ אזי קיימים $a, b \in \mathbb{Z}$ כך ש$an + bk = gcd(n,k)$.
הוכחה: נעשה אינדוקציה על $n + k$.
אם $n + k = 2$ אז צריך למצוא a, b כך ש$an + bk = \gcd(n,k) = a \cdot 1 + b \cdot 1 = 1$, ניקח $a = 1, b = 0$.
יהי m עד אליו הטענה נכונה. צריך להוכיח עבור $k + n = m$: אם $k = n$ אז $gcd(n,k) = n$. קל לראות שעבור $a = 0, b = 1$ מתקיים: $0 \cdot k + 1 \cdot n = n$.

כעת נניח $n > k$ (עבור $k > n$ דומה):$gcd(n,k) = gcd(k, n-k)$ כעת $k + n - k < k + n = m$ לכן לפי הנחת האינדוקציה קיימים a, b כך ש$gcd(k, n-k) = a \cdot k + b \cdot (n-k)$. קיבלנו שמתקיים: $gcd(k,n) = ak + b(n-k) = k(a-b) + bn$. מ.ש.ל

הערה: אלגוריתם אוקלידס

דוגמא: מצאי a, b כך ש$gcd(6,15) = a \cdot 6 + b \cdot 15$.

$$gcd(6,15) = gcd(6,3) \quad 3 = 15 - 2 \cdot 6$$

$$gcd(6,3) = gcd(3,3) = 3 \quad 3 = 6 - 3$$

$$3 = 1 \cdot 3 + 0 \cdot 3 = 1 \cdot (6-3) + 0 \cdot 3 = 1 \cdot 6 + (-1) \cdot 3$$

$$= 1 \cdot 6 - 1 \cdot (15 - 2 \cdot 6) = -1 \cdot 15 + 3 \cdot 6$$

למסתבכות/ים - המסומנים באדום הם n, k ובשחור a, b 😊

<u>טענה</u>: בחוג $(\mathbb{Z}_n, +, \cdot)$, $k \in \mathbb{Z}_n$ הפיך אם"ם k, n זרים.
דוגמא: ב$\mathbb{Z}_{12}$ ההפיכים הם: 1,5,7,11, ב$\mathbb{Z}_{15}$ ההפיכים: 1,2,4,7,8,11,13,14.
הוכחת הטענה:

מקרה 1: k, n אינם זרים. צ"ל שk אינו הפיך ב$\mathbb{Z}_n$. כלומר $gcd(k,n) = a > 1$. כעת a מחלק את $n, k \to n = ta, k = sa$, כאשר: $2 \leq t \leq^{*} n-1$ **, כלומר $0 \neq t \in \mathbb{Z}_n$.
$t \neq n$* אחרת $a = 1$.

**למי שלא מבינה למה - הסבר בהרצאה https://www.youtube.com/watch?v=ZT1GI7XtRZM דקה 59:56.

כעת $tk = tsa = sn \equiv 0 mod n$. נב"ש(נניח בשלילה) k הפיך ב$\mathbb{Z}_n$:

$$\bar{t}\bar{k} = \bar{0} \ /k^{-1}$$

$$\bar{t} = \bar{0}$$

בסתירה לכך ש$t \neq 0$.

מקרה 2: k, n זרים. צ"ל k הפיך. נתון $gcd(k,n) = 1$, קיימים $a, b \in \mathbb{Z}$ כך ש$ak + bn = 1$.
$ak \equiv 1 mod n$ נסמן בr_a את השארית של a חלקי n, ולכן $r_a k \equiv 1 mod n$, כלומר $r_a = k^{-1}$ ($r_a \in \mathbb{Z}_n$).
דוגמא: $3 \cdot (-2) + 1 \cdot 7$, רוצים למצוא את ההופכי של 3 ב$\mathbb{Z}_7$. ולכן $-2 \cdot 3 \equiv 1 mod 7$
$5 = 3^{-1}$. ולכן $5 \cdot 3 \equiv 1 mod 7$.

מסקנה: החוג $\mathbb{Z}_n$ הוא שדה אם"ם n ראשוני.
הוכחה: $\mathbb{Z}_n$ שדה $\Leftrightarrow$ $(\mathbb{Z}_n \backslash \{0\}, \cdot)$ חבורה חילופית {סגירות וחילופיות ואיבר יחידה יש} $\Leftrightarrow$ ב$\mathbb{Z}_n \{0\}$ כולם הפיכים $\Leftrightarrow$ ב$\mathbb{Z}_n \{0\}$ כולם זרים לn $\Leftrightarrow$ n ראשוני. אם n ראשוני אז $1,2 \dots n-1$ זרים לו כיוון שאינם מתחלקים בn ולכן $\mathbb{Z}_n$ שדה. אם n אינו ראשוני, אזי $n = km, 1 < k, m < n$, k, m אינם זרים לn ולכן אינם הפיכים ו$\mathbb{Z}_n$ אינו שדה.

<u>הגדרה</u>: נגדיר את U_n להיות קבוצת כל המספרים $1 < k < n$ שזרים לn. יחד עם כפל מוד n היא חבורה הנקראת חבורת אוילר.

דוגמא: $U_{12} = 1,5,7,11$. הקבוצה איזומורפית ל$\mathbb{Z}_2 x \mathbb{Z}_2$.

הרצאה 7 – 17.12.2019

תזכורת: למדנו על החוג $\mathbb{Z}_n$ כשהחיבור והכפל הם $modn$, וההפיכים הם בדיוק המספרים שזרים לn ולכן $\mathbb{Z}_n$ שדה אם"ם n ראשוני.
הגדרנו גם את U_n – קבוצת כל המספרים הטבעיים שקטנים או שווים לn וזרים לו.
זו נקראת חבורת אוילר יחד עם כפל $modn$.

דוגמא: $U_{15} = 1,2,4,7,8,11,13,14$.

<u>הגדרה</u>: נסמן ב$\varphi(n)$ את פונקציית אוילר, שהיא כמות הטבעיים שקטנים או שווים לn וזרים לו. לכן $\varphi(n) = |U_n|$.

משפט אוילר: יהי $n \in \mathbb{N}$ ויהי $a < n$ וזר לn, אזי $a^{\varphi(n)} \equiv 1 modn$.

הוכחה: $a < n$ וזר לn ולכן $a \in U_n$. $o(a)|o(U_n)$ - הסדר של a מחלק את הסדר של U_n כלומר את $\varphi(n)$. כלומר, $\varphi(n) = t \cdot o(a)$. ולכן $a^{\varphi(n)} = a^{t \cdot o(a)} = \left(a^{o(a)}\right)^t \equiv 1 modn$.

<u>משפט פרמה הקטן</u>

יהי p מספר ראשוני ויהי $a < p$ אזי $a^{p-1} \equiv 1 modp$.
דוגמא: $p = 7, a = 2$. $2^6 \equiv 1 mod7$.
הערה: $a^p \equiv a modp$ לכל $a \in \mathbb{N}$.(p מספר ראשוני).

הוכחת משפט פרמה הקטן: p ראשוני ולכן $a < p$ זר לp. לפי אוילר, $a^{\varphi(p)} = 1 modp$. אבל $U_p = 1 \dots p-1$, לכן $\varphi(p) = p - 1$. מ.ש.ל

<u>הצפנה</u>

כמו שלמדנו בתחילת הסמסטר ישנן 3 מטרות להצפנה:

- הסתרת העברת מידע
- הבטחת זהות השולח
- אמינות ושלמות המידע

סוגים שונים של הסתרת מידע:

- הצפנה סימטרית – מפתח שמתואם מראש(לדוגמא, שני אנשים שמסכימים על סיסמא מראש).
- הצפנה פומבית
- פרקטית – מתאמים מפתח להצפנה סימטרית באמצעות הצפנה פומבית.

דוגמא: נרצה לשלוח כסף בדואר מבלי שיגנבו את הכסף, נשלח את תיבת הכסף בדואר עם מנעול, כעת המקבלת תנעל את התיבה עם מנעול משלה ותשלח את התיבה לשולחת, השולחת תפתח את המנעול שלה ותשלח חזרה – ככה המקבלת יכולה לפתוח את התיבה בעצמה.
הדוגמא הזו קצת שונה מתהליך *RSA*, דוגמא שיותר דומה ל*RSA* היא שהמקבלת תשלח מנעול מראש לשולחת(וכמובן תשאיר את המפתח אצלה), השולחת תנעל את התיבה במנעול של המקבלת ותשלח אותה.

אל תנסו את זה בבית(מילותיו של ארז):

מטה-דאטה (מה זה מטה דאטה? דוגמא – נעשתה שיחת טלפון, המידע היא השיחה עצמה(הקלטה של השיחה), מטה-דאטה זה מי דיבר עם מי, מתי, כמה זמן דיברו וכו')
דוגמא למטה-דאטה שכדאי להצפין:

1. כמה פעמים אותו מידע נשלח
2. מי דיבר עם מי ומתי?
3. אורך המידע(על מנת להסתיר את אורך המידע בדר"כ מרפדים באפסים)

4. זמן ההצפנה – כמה זמן זה לקח להצפין את המידע

בעצם מטה דאטה הוא "מידע על המידע" והרבה פעמים באמצעות מטה דאטה ניתן לגלות דברים על המידע עצמו.

<u>ההצפנה המושלמת</u>

שני הצדדים מתאמים מפתח שהוא רצף אקראי של ביטים: 1010001

1111111 – המידע שנרצה להעביר

נעשה XOR עם המפתח על מנת להסתיר את המידע ונקבל: 0101110

הצד השני יעשה XOR עם המפתח ויקבל: 1111111

מה הבעיה בהצפנה הזו?
נסביר באמצעות דוגמא:
נשלחו שתי הודעות: v_1, v_2, לרצף הביטים האקראי שלנו נקרא u, כעת נבצע XOR בין ההודעות לבין u, ונקבל: $v_1 \oplus u = x_1, v_2 \oplus u = x_2$, כעת מישהו יירט את שתי ההודעות, כל מה שהוא צריך לעשות על מנת לשבור את ההצפנה זה XOR בין ההודעות: $x_1 \oplus x_2 = v_1 \oplus v_2$. אלו אומנם לא ההודעות עצמן, אך זה שלב קרוב מאוד אליהן – וזה לא טוב.

<u>*RSA*</u>

אליס בוחרת שני ראשוניים גדולים(סדר גודל 2^{4096}) p, q. ואז מחשבת:

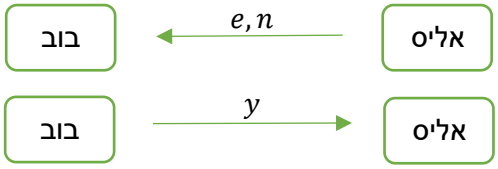
$$n = p \cdot q, m = (p-1)(q-1)$$

אליס מגרילה מספר e שזר לm. אליס מפרסמת את e, n (מפתח פומבי).
בוב רוצה לשלוח מידע $x < n$ לאליס. בוב מחשב את: $y = x^e (mod n)$.

הערה: השורש הדיסקרטי(מודולו) נחשב לבעיה קשה ולכן זו הצפנה טובה.

אליס מחשבת את $d = e^{-1} (mod m)$(הראנו בהרצאה הקודמת כיצד לעשות זאת, יש הסבר גם בתרגול) ומחשבת $y^d (mod n) = x$.

<u>תרשים</u>:



הערה: בדר"כ המפתח של אליס פשוט מפורסם וכל התקשורת היא בוב שולח הודעה לאליס והחלק הראשון כמעט ולא קורה.

הסבר **שגוי**: $y^d = (x^e)^d = x^{ed} = x^1$, למה שגוי? כי כל הפעולות חושבו $mod n$ ו$mod m$.

טענה: יהיו p, q ראשוניים וn המכפלה שלהם, אזי $\varphi(n) = \underbrace{(q-1)(p-1)}_{m}$

הוכחה: $\varphi(n)$ הוא כמות הטבעיים עד n שזרים לn.ניתן לומר ש:
כמות המספרים שלא זרים לn $\varphi(n) = n - n$.
$n = p \cdot q$, שני מספרים זרים אם"ם אין להם גורם ראשוני משותף. לכן המספרים שלא זרים לn מתחלקים בp או בq.

המספרים שמתחלקים בp עד n הם: $p, 2p, 3p \dots q \cdot p$, ועבור q: $q, 2q \dots p \cdot q$,
אילו מספרים יופיעו בשתי השורות? מספרים שמתחלקים גם בp וגם בq, ולכן מתחלקים

ב$n = p \cdot q$, כלומר, רק $p \cdot q$ חוזר על עצמו. לכן בשתי השורות יחד יש $p + q - 1$ מס' שונים, לכן
$\varphi(n) = n - (p + q - 1) = p \cdot q - p + q + 1 = (p - 1)(q - 1)$

הרצאה 8 – 24.12.19

תזכורת: אליס בוחרת ראשוניים p,q. מחשבת $n=p\cdot q$. ומחשבת $m=\varphi(n)=(p-1)(q-1)$.
אליס בוחרת מספר e זר לm ואליס מחשבת את $d=e^{-1}(modm)$. אליס שולחת את הזוג e,n לבוב. בוב מחשב את $y=x^e(modn)$ ואת זה הוא שולח לאליס($x<n$). אליס מחשבת את $y^d(modn)=x$.

נוכיח שאכן $y^d\equiv x(modn)$. לכן $x^e\equiv y(modn)$ $(x^e)^d\equiv y^d(modn)$ (אם שני מספרים הם שקולים גם החזקה שלהם שקולה מודולו). לכן צ"ל $(x^e)^d\equiv x(modn)$.
$d=e^{-1}(modm)\to de=1(modm)$.

הסבר **שגוי**: $(x^e)^d=x^{ed}\equiv x^1=x$. כבר הראנו דוגמא בהרצאה הקודמת ש $1\equiv 4(mod3), 2^1\not\equiv 2^4(mod3)$. כלומר, אם היה מדובר באותו מודולו($m=n$) אז זה לא היה נכון, אבל במקרה הזה $m=(p-1)(q-1)\neq n$.

מקרה 1: x זר לn. לפי משפט אוילר $x^{\varphi(n)}\equiv 1modn$. אז $d\cdot e=km+1$ $x^{ed}=x^{k\cdot m+1}=x\cdot\left(\underbrace{x^m}_{\equiv 1}\right)^k\equiv xmodn$.

מקרה 2: x לא זר לn. לכן x מתחלק בp או בq ולא בשניהם($x<n$). נניח שx מתחלק בp ולא מתחלק בq(במקרה ההפוך ההוכחה דומה). לכן $x=h\cdot p$ וx זר לq.
לפי פרמה הקטן $x^{q-1}\equiv 1(modq)$. נסתכל על
$$x^{km}=x^{k(p-1)(q-1)}=(x^{q-1})^{k(p-1)}\equiv 1(modq)$$
כיוון ש$x^{km}\equiv 1(modq)$ אזי $x^{km}=tq+1$.
$$x^{ed}=x^{km+1}=x^{km}\cdot x=(1+tq)\cdot x=x+tq\cdot\underbrace{x}_{hp}=x+tq\cdot hp=x+thn\equiv x(modn)$$
מ.ש.ל

לסיכום:

בוחרים $p.q$ ראשוניים גדולים $\Leftarrow$ $p\cdot q$ קל לחשב $\Leftarrow$ $d=e^{-1}modm$ קל לחשב באמצעות $gcd(e,m)\Leftarrow x^d,x^e$ נראה בהמשך שקל לחשב(קל=יעיל, זמן החישוב בערך $log(n)$).

עובדה: כמות הראשוניים עד n היא **בערך** $\frac{n}{log(n)}$ – לא נוכיח. מה הסיכוי בהגרלת מספר מ1 עד n שהוא יהיה ראשוני?$\frac{1}{\log(n)}=\frac{\frac{n}{\log(n)}}{n}$ כלומר, סה"כ הסיכוי להגריל מספר ראשוני סביר.

כיצד נקבע האם p ראשוני?
רעיון: ידוע שלכל $a<p$ אם p ראשוני אזי $a^{p-1}\equiv 1modp$(לפי פרמה). נבדוק האם 8 ראשוני:
$2^7\not\equiv 1mod8$ כמובן שזה לא נכון, כי $2^7\equiv 0mod8$ בסתירה.
הרעיון יכול לעזור על מנת **לפסול לא ראשוניים** אך לא יעיל למציאת ראשוניים.
האם למספרים שאינם ראשוניים $a^{p-1}\neq 1modp$? למעשה, יש מספרים שכמעט לכל a מקיימים $a^{n-1}\equiv 1modn$.

<u>אלגוריתם מילר-רבין לבדיקת ראשוניות</u>

נתון מספר n אי-זוגי, האם הוא ראשוני? נציג את $n-1=2^s\cdot r$ כאשר r אי-זוגי, כלומר, נציג כחזקה של 2 כפול מספר אי-זוגי.

<u>הגדרה</u>: יהי n מספר טבעי ויהי $a<n$, a נקרא <u>עד חזק</u> לראשוניות של n אם אחד מהתנאים הבאים מתקיים:

- $a^r\equiv 1modn$
- לאחד מבין הערכים $0\leq k\leq s-1$ מתקיים $a^{2^k\cdot r}=(n-1)modn$

דוגמא: נבדוק אם 2 הוא <u>עד חזק</u> לראשוניות של 9. $9-1=8=2^3\cdot 1$ כלומר, $r=1,s=3$.
לכן, צריך לחשב את המספרים הבאים: a^r,a^{2r},a^{4r}. נחשב: $mod9$ $2^1=2,2^2=4,2^4=16$.
אף אחד מהם לא שקול ל$8mod9$. ולכן 2 אינו עד חזק לראשוניות של 9.

<u>טענה</u>: אם n ראשוני אז כל $1\le a<n$ הם עדים חזקים לכך.
<u>טענה</u>(ללא הוכחה): אם n אינו ראשוני לכל היותר רבע מבין המספרים $1\le a<n$ הם עדים חזקים לראשוניות של n.

<u>האלגוריתם</u>

נגריל k מספרים $1\le a<n$ ונבדוק האם הם עדים חזקים בהינתן שn אינו ראשוני. מה הסיכוי שכל העדים יטענו שהוא ראשוני?$\frac{1}{4^k}$.

סיכומון:
נגריל 1000 מספרים, על כל מספר נגריל $1000(k)$ עדים ועל כל עד פוטנציאלי נבדוק האם הוא עד חזק לראשוניות (1000 פעולות בערך).

הרצאה 9 – 31.12.19

תזכורת: $a < n$ הוא עד חזק לראשוניות של n אם אחד מהתנאים הבאים מתקיים:

- $a^r \equiv 1 mod n$
- קיים $0 \leq k \leq s-1$ עבורו $a^{2^k r} \equiv n-1 mod n$

כאשר $2^s r = n-1$.

אם n אינו ראשוני לכל היותר רבע מבין המספרים $1 \leq a < n$ הם עדים חזקים לראשוניותו.

משפט: יהי p ראשוני אזי לכל $1 \leq a < p$ a עד חזק לראשוניות של p.

טענה: יהי p ראשוני ויהי $x \in U_p$ כך ש$x^2 = 1$, כלומר $x^2 \equiv 1 mod p$, אז $x = 1$ או $x = -1$ $(x = p-1)$.
הוכחה: כיוון שp ראשוני, $\mathbb{Z}_p$ הוא שדה. $x \in \mathbb{Z}_p$, נתון $x^2 = 1$ ולכן $(x-1)(x+1) = x^2 - 1 = 0$.
בשדה אין מחלקי 0 ולכן $x-1 = 0 \vee x+1 = 0$.
הסבר(למה אין מחלקי 0 בשדה): נניח בשלילה $x \pm 1 \neq 0$. נכפול בהופכי של $x-1$ ונקבל $(x-1)(x+1) = 0/(x-1)^{-1}$ ולכן $x+1 = 0$ בסתירה.
לכן, $x = 1 \vee x = -1$. שימו לב: אם $x \equiv -1 mod p$ אז $x \equiv p-1 mod p$.

דוגמא: $n = 8$. $(3-1)(3+1) = 0 mod 8$, $3^2 = 1 mod 8$, במספר לא ראשוני מצאנו מספר שהוא לא 1 ולא 7(1-).

הוכחת המשפט: יהי p ראשוני ויהי $1 \leq a < p$ אז צ"ל שa עד חזק לראשוניות של P. נסמן $p-1 = 2^s r$. צ"ל $a^r \equiv 1 mod p$ או שאחד מבין $a^r, a^{2r} \dots a^{2^{s-1} r} \equiv p-1 mod p$.
לפי פרמה הקטן $a^{p-1} \equiv 1 mod p$, כלומר $a^{2^s r} \equiv 1 mod$ נשים לב ש$(a^r)^2 = a^{2r}, (a^{2r})^2 = a^{2^2 r}, \dots \left(a^{2^{s-1} r}\right)^2 = a^{2^s r} = a^{p-1} \equiv 1 mod p$. לפי טענה קודמת, כיוון שp ראשוני, אם $x^2 \equiv 1 mod p$ אזי $x \equiv \pm 1 mod p$. נניח בשלילה שa אינו עד חזק, לכן $a^r \not\equiv 1$ $a^r, \dots a^{2^{s-1} r} \not\equiv -1$.
בסתירה לכך ש$\left(a^{2^{s-1} r}\right)^2 \equiv 1$(כי מתישהו היה מספר שאינו ± 1 ובריבוע הפך ל1).

דוגמא: האם 9 ראשוני? נבדוק האם 3 עד חזק. $9 - 1 = 8 = 2^3 \cdot 1$. נבדוק את $3^1, 3^{2 \cdot 1}, 3^{4 \cdot 1} mod 9$ (לעולם לא נקבל מינוס 1 אלא את ההופכי של 1, כלומר 8 במקרה הזה) קל לראות שאף מספר לא מקיים, כלומר 3 אינו עד חזק ו9 אינו ראשוני. נבדוק האם 4 עד חזק: $4^1, 4^2, 4^3$.
$4^1 \neq 1,8, 4^2 \neq 8, 4^4 \neq 8$ ולכן גם 4 אינו עד חזק.
תזכורת: בפועל, צד אחד מגדיל "סוד כמוס" ושולח לצד השני בהצפנה פומבית ואז שניהם עוברים להצפנה סימטרית. יכולתי להעביר מידע כרצוני.

בניגוד לכך *שיטת דיפי-הלמן* היא שיטה לתיאום סוד בין שני הצדדים בלי להעביר אותו(בלי להעביר מידע מוצפן), כלומר, שיטה לתיאום מפתח בלבד!

תהליך דיפי הלמן

אליס מגרילה ראשוני גדול p, בוחרת יוצר של החבורה U_p $(< g \geq U_p)$ או לפחות איבר מסדר גדול מאוד, נסמנו g. אליס שולחת את g ואת p לבוב. כעת, אליס מגרילה מספר $a < p$ ובוב מגריל מספר $b < p$. אליס מחשבת את $g^a mod p$ ושולחת לבוב, בוב מחשב את $g^b mod p$ ושולח לאליס.
צופה מהצד יודע: $g, p, g^a mod p, g^b mod p$. בלי המודולו: היינו עושים $log_g(g^a)$. מודולו p נקרא הלוג הדיסקרטי וזו נחשבת בעיה קשה.

צופה מהצד לא יודע: a, b.

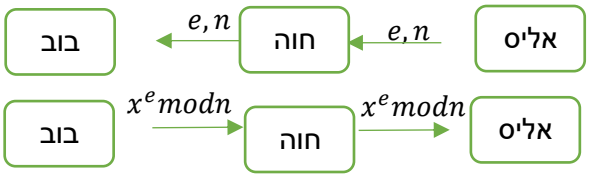
אליס מעלה את g^b שהיא קיבלה מבוב בa ומקבלת: $\left(g^b\right)^a = g^{ab} mod p$. בוב עושה אותו דבר ומקבל $g^{ab} mod p$. ויצרנו סוד משותף שרק שניהם יודעים.

פרקטית כיצד נמצא יוצר g או לפחות איבר מסדר גבוה. הגרלנו p ראשוני, $|U_p| = p - 1$. נגריל $g < p$. כיצד נדע מה הסדר של g?
לכן, נגריל "ראשוני בטוח" $(safe\ prime)$. כלומר, ראשוני מהצורה $p = 2q + 1$ כאשר q ראשוני.
לכן $|U_p| = 2q$. לכן בסדר של כל איבר $g \in U_p$ הוא אחד מהבאים: $1,2,q,2q$. אם הסדר הוא $2q$ אז זה היוצר וזה מעולה. לבחור את 1 זה לא טוב(הסדר הוא 1). אם הסדר הוא 2 זה אומר ש$g^2 = 1$ וכיוון שp ראשוני זה אומר ש$g = -1$. לכן לכל $g \neq \pm 1$ הסדר הוא לפחות q או שg יוצר.

<u>הבטחת זהות הכותב ושלמות ואמינות המידע</u>

איך עם RSA ניתן להבטיח את זהות הצד השני?

אבחר x סודי, אצפין ואשלח לאליס $x^e mod n$ ואליס תחזיר x.
יכול להיות מקרה נוסף(*woman in the middle*):



כך שבוב חושב שהוא מדבר עם אליס, אך בעצם הוא מדבר עם חוה. זו מתקפה שקשה לעקוף אותה.

הרצאה 10 – 15.01.20

הבטחת שלמות ואמינות המידע

מייקרוסופט יצרו עדכון גרסה, נבצע גיבוב ($hash$) על עדכון הגרסה ונקבל ערך מגובב x.
למייקרוסופט יש n, e ידועים מה*RSA*. מייקרוסופט תשלח את העדכון גרסה יחד עם $x^d mod n$. אני מחשבת את
$x = x^{d^e} mod n$. מבצעת בעצמי גיבוב לעדכון ומקבלת x.
הסיבה שאנחנו מבצעים גיבוב היא כי x הוא מספר גדול מדי להעלות בחזקת d.

העלאה בחזקות גבוהות

נרצה לחשב את x^{35}, נתחיל בלחשב את x^2 ולאחר מכן נחשב $x^4 = (x^2)^2$, ומשם את x^8 וכן הלאה עד x^{32}, כעת כדי למצוא את x^{35} נחשב: $x \cdot x^2 \cdot x^{32}$. וכך ביצענו 7 פעולות במקום 35, הסיבוכיות היא בערך $2\log n$.

<u>הגדרה</u>: תהי חבורה G ותהי H תת חבורה של G, H נקראת *תת חבורה נורמלית* של G אם לכל איבר בG מתקיים $aH = Ha$. לכן, אם החבורה חילופית, כל תת חבורה היא תת חבורה נורמלית.

הערה: אם נרצה לחשוב על חבורה כללית שהיא לאו דווקא חילופית נחשוב על תמורות, כי הוכחנו שכל חבורה בעולם היא תת חבורה של חבורת התמורות. עצה למבחן מארז: לחשוב על חבורת התמורות.

דוגמא: חבורת התמורות $S_3 = \{I, (1\ 2\ 3), (1\ 3\ 2), (1\ 2), (1\ 3), (2\ 3)\}$, נסתכל על $H =< (1\ 2) >= \{I, (1\ 2)\}$(תזכורת: תמיד בתת חבורה ציקלית נמצא איבר היחידה).

נסתכל על $H(1\ 3) = \{(1\ 3), (3\ 1\ 2)[= (1\ 2\ 3)]\}$. נחשב $H(1\ 3) = \{(1\ 3), (1\ 3\ 2)\}$

*חישוב מפורט יותר למי שמתקשה: $(1\ 2\ 3) = (3\ 1\ 2) = (1\ 2)(1\ 3)$,עבור $(1\ 3)(1\ 2)$ נבצע את אותו דבר: $(1\ 3\ 2) = (2\ 1\ 3) = (1\ 3)(2\ 1)$.

$H(1\ 3) \neq (1\ 3)H$ ולכן H אינה נורמלית.

דוגמא: $H =< (1\ 2\ 3) >= \{I, (1\ 2\ 3), (1\ 3\ 2)\}$, $|H| = |aH|$ ולכן אם f אי-זוגית(שלילית),
$fH = \{3\text{ תמורות שליליות}\} = \{(1\ 2), (1\ 3), (2\ 3)\}$
לעומת זאת, אם f זוגית: $fH = H = Hf$

<u>הגדרה</u>: תהי חבורה G ותהי H תת חבורה נורמלית, נגדיר את $G/_H := \{aH | a \in G\}$.
לדוגמא: $S_3/_{< (1\ 2\ 3) >} = \{H, \{(1\ 2), (1\ 3), (2\ 3)\}\}$.

<u>הגדרה</u>: נגדיר פעולה ל$G/_H$: $(aH)(bH) = \{ahbk | h, k \in H\}$
שאלה: האם $(aH)(bH) \in G/_H$?

<u>משפט</u>: תהי G חבורה ותהי H תת חבורה נורמלית אזי $(aH)(bH) = (ab)H$.
הוכחה: יהי $abh \in (ab)H$, צ"ל $\underbrace{abh}_{=aebh} \in (aH)(bH)$, וכמובן שמתקיים $bh \in bH, ae \in aH$ והוכחנו.
יהי $ahbk \in (aH)(bH)$ צ"ל $ahbk \in (ab)H$. $hb \in Hb = bH \to hb \in bH \to hb = bt, t \in H$.
$ahbk = ab\underbrace{tk}_{\in H} \in (ab)H$

הקדמה לאיזומורפיזם #1

משפט האיזומורפיזם הראשון במידה מסוימת מבהיר לנו מה זה הומומורפיזם.
$f: G = \{Bob, Sponge, Boba, Sponga\} \to H = \{Boy, Girl\}$

אם נקבץ את הבנים יחד ונקבץ את הבנות יחד החבורה הראשונה תתנהג כמו החבורה השנייה, כלומר קבוצת הבנים תתנהג כמו בן אחד וקבוצת הבנות תתנהג כמו בת אחת, ואם בן הוא איבר היחידה מכפלה בין בן לבת תיתן לנו בת.

משפט האיזומורפיזם הראשון: יהי $f: G \to H$. הומומורפיזם בין שתי חבורות אזי $Imf \cong {}^{G}/_{kerf}$.

דוגמא: $f: \mathbb{Z} \to \mathbb{Z}_3$ עם הפעולות חיבור וחיבור מודולו 3 בהתאמה כך ש
שארית החלוקה של a ב-3 $\coloneqq f(a)$. ללא הוכחה f הומומורפיזם.
לדוגמא: $f(4) = 1, f(-1) = 2, f(30) = 0$.$kerf = 3\mathbb{Z}$,${}^{\mathbb{Z}}/_{3\mathbb{Z}} = \{0 + 3\mathbb{Z}, 1 + 3\mathbb{Z}, 2 + 3\mathbb{Z}\}$

$$1 + 3\mathbb{Z} + (2 + 3\mathbb{Z}) = 0 + 3\mathbb{Z}$$

הרצאה 11 – 21.01.20

המטרה של קידוד: זיהוי שגיאות ו**אולי** תיקון שגיאות.
נניח ונרצה להעביר לצד השני את המידע הבא: 101101, לצד המקבל אין שום מושג אם המידע שהוא קיבל תקין או שנפלה בו טעות, לכן נוסיף ביטי יתירות $\underbrace{101101}_{\text{מידע}}\underbrace{101101}_{\text{יתירות}}$ – במקרה הזה אנו שולחים פעמיים את המידע ובמידה ונוצרה שגיאה אחת הצד השני **יזהה** את השגיאה כיוון שלא קיבלנו את אותו המספר פעמיים.
על מנת שנוכל **לתקן** שגיאה אחת נשלח 3 פעמים את המידע, אבל במקרה כזה נשלח מידע ארוך פי 3 שזה לא יעיל במיוחד.

נשאלת השאלה – האם אפשר לעשות את זה בפחות מקום?
דוגמא: *parity bit/parity check*
הערה: כל המידע הם וקטורים מעל השדה $\mathbb{Z}_2$.
בהינתן המידע: 101101, ה*parity bit* הוא סכום כל הביטים לפניו ובמקרה הזה: 0.
כיצד נתאר שגיאה באופן אלגברי? חיבור 1 לאחד הביטים.
במילה המקורית סכום הביטים כולל ביט ה*parity*(זוגיות) הוא 0, אם נפלה שגיאה **אחת** סכום הביטים (לא כולל ביט ה*parity*) יהיה 1 וביט ה*parity* יהיה 0 וכך סכום הביטים יהיה 1, כלומר חלה שגיאה.
לסיכום, ה*parity* יודע לזהות כל מספר אי-זוגי של שגיאות ולא מזהה כל מספר זוגי של שגיאות והוא לא יודע לתקן באף אחד מהמקרים.

קידוד לינארי

אורך המידע – n
אורך היתירות – k
אורך מילה מקודדת – $n+k$

תהי מטריצה בינארית A בגודל $k \times n$, היא מגדירה *קוד לינארי*:

$$G = \binom{I_n}{A}, H = (A \mid I_k)$$

בהינתן וקטור מידע v באורך n, Gv הוא המילה המקודדת(באורך $n+k$). הצד השני מקבל את Gv (אולי יחד עם שגיאות) וכופל אותו בH, ומצהיר שהמילה חוקית אם"ם הוא קיבל וקטור אפסים.

דוגמא #1: $A = (1\ 1\ 1\ 1)$, מכאן ניתן להסיק שהמטריצה $G = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 \end{pmatrix}$. אורך המידע $n = 4$, אורך היתירות: $k = 1$
מידע לדוגמא: $v = 1010$, $Gv = (\underbrace{1\ 0\ 1\ 0}_{\text{המידע}}\ \underbrace{0}_{\text{יתירות}})$, קידוד זה הוא *parity check*, ולכן ניתן לומר ש*parity check* הוא מקרה פרטי של קידוד לינארי.
שימו לב: $Gv = \binom{I}{A}v = \binom{Iv}{Av} = \binom{v}{Av}$.

דוגמא #2: $A = \begin{pmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \end{pmatrix}$. $n = 4, k = 3$, $v = 1010$. $Gv = (\underbrace{1\ 0\ 1\ 0}_{\text{מידע}}\ \underbrace{1\ 0\ 1}_{\text{יתירות}})$

$$H = \begin{pmatrix} 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ \underbrace{1 & 1 & 0 & 1}_{A} & \underbrace{0 & 0 & 1}_{I} \end{pmatrix}$$

על מנת להקל על עצמנו בהכפלה, נסתכל על הוקטור Gv ונראה שבעצם התוצאה של Hv היא סכום העמודות ה1,3,5,7 ונקבל: $(0\ 0\ 0)$.
נניח נפלה שגיאה בביט השלישי, $H(1\ 0\ 0\ 0\ 1\ 0\ 1)$, ונקבל: $(0\ 1\ 0)$, לא קיבלנו וקטור אפסים ולכן ניתן להסיק שקרתה שגיאה. אם נסתכל על התוצאה שקיבלנו היא אומרת לנו איפה נפלה טעות.

<u>משפט</u>: תהי מילה x באורך $n+k$ אזי x היא מילה חוקית(מידע מקודד) אם"ם $Hx=0$.
<u>הוכחה</u>: ראשית, מילה חוקית היא מילה מהצורה $x=\begin{pmatrix} v \\ Av \end{pmatrix}$, (שימו לב היתירות החוקית היא יחידה)
תהי מילה כלשהי $x=\begin{pmatrix} v \\ u \end{pmatrix}$, x חוקית אם"ם $u=Av$.
נזכור $H=(A\mid I)$, ולכן $Hx=(A\mid I)\begin{pmatrix} v \\ u \end{pmatrix}=Av+Iu=Av+u$ ולכן $Hx=0$ אם"ם $Av=u$,
(ב$\mathbb{Z}_2$ סכום של שני דברים מתאפס רק אם הם שווים).
שימו לב: כל טעות או מספר טעויות ביתירות יזוהו.

כיצד טעות משפיעה על התהליך? שימו לב Gv עם טעות בביט הi היא בעצם $Gv+ei$ (ei היא 1 במקום הi, 0 בכל מקום אחר).

$$H(Gv+ei)=\underbrace{HGv}_{0}+Hei=C_i(H)$$

*$C_i(H)$ היא העמודה הi בH.
מסקנה: ניתן לזהות שגיאה אחת אם"ם אין עמודת אפסים בH אם"ם אין עמודות אפסים בA.

כיצד משפיעות שתי שגיאות?

$$H(Gv+ei+ej)=0+Hei+Hej=C_i(H)+C_j(H)$$

נקבל 0 אם"ם שתי העמודות זהות.
מסקנה: אם בH אין עמודת אפסים אזי אפשר לזהות שתי שגיאות אם"ם אין בH שתי עמודות זהות.

הערה: אם אין עמודת אפסים ואין שתי עמודות זהות, ניתן לתקן שגיאה יחידה.

דוגמא: נחזור למטריצה $H=\begin{pmatrix} 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{pmatrix}$ ($\underbrace{\quad A \quad}$ $\underbrace{\quad I \quad}$) ולמילה המקודדת: $G\begin{pmatrix} 1 \\ 0 \\ 1 \\ 0 \end{pmatrix}=\begin{pmatrix} 1 \\ 0 \\ 1 \\ 0 \\ 1 \\ 0 \\ 1 \end{pmatrix}$

$$x=\begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 1 \\ 0 \\ 1 \end{pmatrix}=Gv+e_2+e_3\rightarrow Hx=C_2(H)+C_3(H)=\begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix}$$

דוגמא: $\begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \\ 1 \\ 0 \\ 1 \end{pmatrix}=Gv+e_1\rightarrow Hx=C_1(H)=\begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix}$.

שימו לב: אם רוצים להיות מסוגלים לתקן שגיאה אחת ולזהות 2, צריך שלא תהיה עמודת אפסים בH ושלא תהיינה שתי עמודות זהות.

בהינתן k ביטי יתירות, אורך המידע המקסימלי הוא $\underbrace{1}_{\text{עמודת האפסים}} - \underbrace{k}_{\text{מספר עמודות ה}I} - 2^k$.

<u>הגדרה</u>: יהיו שני וקטורים בינאריים נגדיר את מרחק המינג ביניהם להיות כמות הביטים השונים.
דוגמא: $d\big((1\ 1\ 0\ 1),(0\ 1\ 1\ 1)\big) = 2$.

<u>הגדרה</u>: יהי קוד לינארי נגדיר את d_{min} להיות המרחק המינימלי בין שתי מילים חוקיות כלשהן.
דוגמא: אם $d_{min} = 1$, אזי יש שתי מילים חוקיות במרחק 1, כלומר Gv חוקית ו$Gv + ei$ גם חוקית, לכן לא ניתן להבטיח זיהוי של שגיאה, וזה קורה אם"ם העמודה הi היא עמודת אפסים.

אם $d_{min} = 5$ ניתן לתקן 2 שגיאות.

הסבר טוב של ארז למה זה קורה ב1:27:00:
https://www.youtube.com/watch?v=E9GOdfhk7wM

<u>הרצאה 12 – 28.01.20</u>

<u>קודים פולינומיים וציקליים</u>

IP/TCP/UDP – Checksum

Ethernet – crc32

נביט בפולינומים עם מקדמים מ$\mathbb{Z}_2$. מדובר בחוג.

בהינתן וקטור המידע 11010 נמיר אותו לפולינום: x^4+x^3+x.

קוד פולינומי מוגדר על ידי פולינום g מדרגה k. הוא מוסיף יתירות של k ביטים למידע.
בהינתן פולינום מידע f, נכפול אותו בx^k(זה מוסיף k אפסים – שם נשים את ביטי היתירות).
דוגמא: $110 = x^2+x \to x^3(x^2+x) = x^5+x^4$.
נחלק את $x^k f$ בפולינום g חלוקה עם שארית. דרגת השארית r היא ככל היותר x^{k-1}, והיא בעצם מייצגת את k ביטי היתירות.
המילה המקודדת היא: $x^k \cdot f + r$.

<u>שימו לב</u>: ב$\mathbb{Z}_2$ חיבור וחיסור הם אותה פעולה. כאילו חיסרנו את השארית . מילה היא חוקית אם"ם היא מתחלקת בg ללא שארית.

הערה: קל להוכיח שסכום הקידודים שווה לקידוד הסכומים, לכן קידוד פולינומי הוא בעצם סוג של קוד לינארי, נזכור מלינארית שכל העתקה לינארית היא כפל במטריצה, בהנחה שהגבלנו את דרגת הפולינומים.

דוגמא: נקודד את המידע 110 בקוד הפולינומי המוגדר ע"י $g = x^3+x+1$. פולינום המידע הוא $f = x^2+x$, נכפול את f בx^3 ונקבל $x^3 \cdot f = x^5+x^4$. $x^5+x^4 = x^2+x+1+\frac{1}{x^3+x+1}$(חילוק $\frac{x^5+x^4}{x^3+x+1}$ פולינומים) לכן השארית היא 1. סה"כ המילה המקודדת: $110001 \to x^5+x^4+1$.

שאלה מוזרה: האם לאחר הזזה ציקלית אחת שמאלה של מילה חוקית נקבל מילה חוקית?
נבדוק בדוגמא: $100011 = x^5+x+1$, כעת נחשב: $x^2+1+\frac{x^2}{x^3+x+1} = \frac{x^5+x+1}{x^3+x+1}$, קיבלנו שארית ולכן המילה לא חוקית.

<u>הגדרה</u>: בהינתן פולינום g מסדר k ומידע באורך n, הקוד נקרא ציקלי אם כל הזזה ציקלית של מילה חוקית שמאלה נותנת מילה חוקית. כלומר, אם $a_1, a_2 \dots a_{n+k}$ מילה חוקית אזי $a_2 \dots a_{n+k}a_1$ גם חוקית.
דוגמא: נביט בדוגמא הקודמת: $110 \to 110001$, $0110 \to 0110001$, ההזזה היא 1100010.
נבדוק האם חוקי:x $x^3+x^2+x = \frac{x^6+x^5+x}{x^3+x+1}$, קיבלנו מילה חוקית – אבל זה לא אומר שהיא ציקלית!

מה היתרון בקוד ציקלי?

<u>טענה</u>: בקוד ציקלי כל כמות של שגיאות בטווח של k ביטים תהפוך מילה חוקית ללא חוקית.
למשל ב$Ethernet$ משתמשים בg מדרגה 32.

<u>הוכחה</u>: נניח ש$a_1 \dots a_{n+k}$ מילה חוקית כלשהי. נבחר בטווח $a_m \dots a_{m+k-1}$ שנחליף ל $b_m \dots b_{m+k-1}$. קיבלנו את המילה $a_1 \dots a_{m-1}b_m \dots b_{m+k-1}a_{m+k} \dots a_{n+k}$. צ"ל שזו מילה שאינה חוקית. נבצע הזזות ציקליות עד שנקבל $a_{m+k} \dots a_{n+k}a_1 \dots a_{m-1}b_m \dots b_{m+k-1}$. מילה זו חוקית אם"ם המילה הקודמת חוקית. המילה $a_{m+k} \dots a_{m+k-1}$ חוקית כהזזה של מילה חוקית. כיוון ששארית החלוקה יחידה לא יתכן ששתי המילים מתחלקות בg.

כיצד נדע האם g מייצר קוד ציקלי עבור מידע באורך n?

<u>משפט</u>: פולינום g מדרגה k מייצר קוד פולינומי ציקלי עבור מידע מאורך n אם"ם g מחלק את $x^{n+k}+1$ ללא שארית.

דוגמא: $110 \to 110001$ לא ציקלי כי $x^3 + x + 1$ לא מחלק את $x^6 + 1$.

$0110 \to 0110001$ ציקלי כי $x^7 + x + 1$ אכן מחלק את $x^7 + 1$.

<u>הערה</u>: הפולינום של *Ethernet* מחלק את $x^{2^{32}-1} + 1$. כלומר עם הפולינום של *Ethernet* ניתן לקודד עד בערך 4 מיליארד ביטים של מידע והקוד עדיין יישאר ציקלי.

<u>הסבר המשפט</u>: הכפלה בx מזיזה את הביטים שמאלה, כלומר
$$h \leftrightarrow a_1 \dots a_{n+k} \to xh \leftrightarrow a_1 \dots a_{n+k}0$$

אם $a_1 = 0$ אכן xh מייצג את ההזזה הציקלית שמאלה. כלומר, לוקחים רק את $n + k$ הביטים הימניים. אם h מתחלק בg בוודאי xh מתחלק בg.
אם $a_1 = 1$ אז $xh + x^{n+k} + 1 = a_2 \dots a_{n+k}a_1$(מחקנו את הביט a_1 והוספנו אחד – כלומר הפכנו את ה0 בביט האחרון ל1).
אם g מחלק את $x^{n+k} + 1$ אז המילה החדשה חוקית.
מצד שני, אם המילה חוקית אז $x^{n+k} + 1$ גם מתחלק בg.

מבנה המבחן:
4 שאלות(כל שאלה 28 נקודות):

- שאלה ראשונה – חופשית, הרבה פעמים משפט האיזומורפיזם
- שאלה שנייה – משפט קיילי ותמורות
- שאלה שלישית – הצפנה (*RSA*, דיפי הלמן, מילר רבין, חתימה)
- שאלה רביעית – קידוד (פולינומי או לינארי)