סיכומי קורס במבנים אלגבריים 1
מרצה: ענר שלו

סיכם: שיר פלד
ותודה ל: OpenOffice שהביאנו עד הלום, לדינה זיל על האירוח באתר שלה, ליותם דרקסלר, אורן בקר, יאיר יצחקי וליאור ינובסקי על התיקונים

<u>שיעור ראשון</u>

הגדרה: חבורה היא קבוצה לא ריקה G עם פעולה דו מקומית $G\times G\to G$ כך שמתקיים:
0. סגירות, כלומר $x,y\in G\Rightarrow xy\in G$
1. אסוציאטיביות: $(xy)z=x(yz)$
2. איבר יחידה: יש איבר יחידה $1\in G$ כך ש $x\cdot 1=1\cdot x=x$
3. קיום הופכי: לכל $x\in G$ יש $x^{-1}\in G$ כך שמתקיים $x\,x^{-1}=x^{-1}x=1$

קיימות חבורות קומוטטיביות. (=חבורות אבליות, ע"ש הנריק אבל)

<u>דוגמאות</u>
1. יהי F שדה, $(F,+,0)$ היא החבורה החיבורית של השדה, קל להראות מיידית (כאשר ההופכי הכפלי של החבורה הוא הנגדי החיבורי של השדה).
2. $(F\setminus 0,\cdot,1)$ היא החבורה הכפלית של השדה.
3. $\mathbb{Z}_n$ השאריות מודולו n. אזי $(\mathbb{Z}_n,+,0)$ היא חבורה חיבורית בגודל n (יתכן שזהו אינו שדה).
4. נסמן $\mathbb{Z}_n^*=\{0<k<n:gcd(k,n)=1\}$ כלומר המספרים הזרים ל n. ואז נקבל $(\mathbb{Z}_n^*,\cdot,1)$ חבורה כפלית שגודלה $\phi(n)$. החבורה מ 4 עבור n=8 היא הקבוצה (1,3,5,7) ומעניין שבה לפולינום $x^2=1$ יש 4 פתרונות – כל האיברים.
5. המטריצות $n\times n$ מעל שדה F כאשר הדטרמיננטה אינה 0. זוהי חבורה ביחס לכפל מטריצות, מטריצת היחידה היא איבר היחידה, והשאר מאלגברה לינארית.
6. תת קבוצה של 5, המטריצות שהדטרמיננטה שלהן היא 1. סגירות – מחוקי דטרמיננטה ושאר האקסיומות נובעות באופן ישיר מ 5.
7. החבורה הסימטרית - S_n כל התמורות על $1,\dots,n$ (סימטריה היא העתקה חח"ע ועל מקבוצה לעצמה), הפעולה הדו מקומית תהיה הרכבת פונקציות או הרכבת תמורות, העתקת הזהות תהיה איבר היחידה. עבור המקרה הכללי – נקבל חבורה הנקראת $Sym(X)=\{f:X\to X\}$ כאשר f חח"ע ועל.

ידוע ש $|S_n|=n!$, פירוק למחזורים (לעבור על זה בבית), זוגיות של תמורות.
ניזכר ב $A_n=\{\sigma\in S_n:sg(\sigma)=1\}$ קבוצת התמורות הזוגיות.
אזי $|A_n|=\frac{n!}{2}$ ומסיבות של כפל תמורות זוגיות ודברים שראינו באלגברה – גם A_n היא חבורה.

תרגיל – חבורה בה $x^2=1$ לכל x היא קומוטטיבית. (בבית)

טענה: בחבורה – איבר היחידה הוא יחיד.
הוכחה: נניח שקיימים שניים ונוכיח שהם שווים.
טענה: תהי G חבורה אזי:
1. ההופכי של כל איבר הוא יחיד
2. $(x\,y)^{-1}=x^{-1}y^{-1}$
3. $(x^{-1})^{-1}=x$

הוכחה:
1. נניח שיש a שהוא גם הופכי ואז
$$a=1\cdot a=(x^{-1}x)a=x^{-1}(xa)=x^{-1}$$
2. מראים ש $(xy)\cdot(y^{-1}x^{-1})=1$
3. נראה ששניהם הופכיים של x^{-1} ומיחידות ההופכי מסתדרים.

טענה: תהי G חבורה, נקבע $g\in G$
אז:
1. ההעתקה $X\to g\cdot X$ היא תמורה על G.
2. כנ"ל עבור ההעתקה $X\to X\cdot g$
הוכחה:
1. חח"ע: $g\,x=g\,y$
$$x=1\,x=(g^{-1}g)x=g^{-1}(g\,x)=g^{-1}(g\,y)=(g^{-1}g)\,y=1\,y=y$$
על:
בהנתן $h\in G$ נראה שהוא בתמונה.
$x=g^{-1}h$ נציב את x בהעתקה ונקבל את המבוקש.

2. אותו הדבר.

מסקנה: למשוואה $g\,x=h$ בחבורה יש פתרון יחיד (כנ"ל עבור $x\,g=h$)

<u>חזקות בחבורה</u>
חזקות טבעיות מוגדרות באופן שהיינו מצפים.
$X^0=1$
ועבור n טבעי נגדיר $x^{-n}=(x^n)^{-1}$

קל לוודא חוקי חזקות בסיסיים:
$x^n\cdot x^m=x^{n+m}\ ,\ (x^n)^m=x^{nm}$

<u>הגדרה – הסדר של איבר X</u> בחבורה מוגדר כ n>0 המינימלי כך ש $x^n=1$ אם אין כזה אז נאמר של X סדר אינסופי.

למשל ב $\mathbb{Z}_8^*$ סדרי האיברים מלבד 1 הם 2. נראה בהמשך שהסדרים מחלקים את גודל החבורה תמיד.

טענה: אם חבורה G סופית אז לכל איבר ב G סדר סופי.

הוכחה: יהי $x\in G$ נתבונן בחזקותיו $1\,,x\,,x^2,\dots x^n,\dots$
זו סדרה אינסופית שאיבריה בקבוצה סופית לכן אפשר לבחור את n כך שיהיה m<n המקיים $x^n=x^m$ כופלים ב x^{-m}
ומכאן נובע $x^{n-m}=x^{m-m}=x^0=1$

מנגד נסתכל ב $\mathbb{R}^*$ עם פעולת הכפל ו 1 כאיבר היחידה, ל 1 ול -1 סדר 1 ולכל שאר האיברים סדר אינסופי.

טענה: תהי G חבורה, $x\in G$ איבר מהסדר n אז $n|m\Leftrightarrow x^m=1$
הוכחה:
כיוון 1 נניח $n|m$ ואז $m=nk$
$$x^m=x^{nk}=(x^n)^k=1^k=1$$
כיוון 2 נניח $x^m=1$ אבל $n\nmid m$ כלומר $m=nk+r$ כאשר r חיובי.
כלומר $1\le r\le n-1$
$$1=x^m=x^{nk+r}=x^{nk}\cdot x^r=1\cdot x^r=x^r$$
וזו סתירה למינימליות הסדר.

<u>שיעור שני – 5.11.08</u>

משפט: תהי G חבורה אבלית סופית. אז לכל $x\in G$ מתקיים $x^{|G|}=1$
במילים אחרות: הסדר של x מחלק את גודל החבורה.
הערה: המשפט נכון ללא הנחת אבליות – לכל חבורה סופית נוכיח עתה לאבליות ובהמשך לחבורות כלליות.
הוכחת המשפט:
נניח $G=\{x_1,\dots,x_n\}$
נתבונן בסדרה $x\cdot x_1, x\cdot x_2, \dots, x\cdot x_n$
ראינו שכפל באיבר קבוע משרה תמורה.
נובע שיש תמורה $\sigma\in S_n$ כך ש $\forall i=1\dots n \;:\; x\cdot x_i=x_{\sigma(i)}$
לכן:

$$(x\cdot x_1)(x\cdot x_2)\cdot\dots\cdot(x\cdot x_n)=x_{\sigma(1)}\cdot\dots\cdot x_{\sigma(n)}$$

מאחר ש G קומוטטיבית נובע ש:

$$x_{\sigma(1)}\cdot\dots\cdot x_{\sigma(n)}=x_1\cdot\dots\cdot x_n=x^n\cdot(x_1\cdot\dots\cdot x_n)$$

נכפול את שני האגפים במכפלת ההופכיים של $x_1,\dots,x_n$ ונקבל:

$$x^n=1$$

מסקנה – משפט פרמה הקטן

$$x^P\equiv x \bmod P \quad , \quad \forall x\in\mathbb{N}\wedge prime\ P$$

הגדרה:
$a\equiv b \bmod p$ אם $p|(a-b)$ ז"א יש ל a,b אותה שארית בחלוקה ב p.

הוכחה
נתבונן בחבורה הכפלית $\mathbb{Z}_P^*$
גודל החבורה הוא P-1
מהמשפט שהוכחנו נובע:

$$\forall x\in\mathbb{N}, P\nmid x, x^{P-1}=1 \;\Rightarrow\; x^P\equiv x \bmod P$$

והשוויון האחרון ברור שנכון כאשר P מחלק את x (אז נקבל אפסים).
ומכאן הטענה.

הכללה
n כללי (לאו דווקא ראשוני)
$G=\mathbb{Z}_n^*$ שאריות זרות ל n עם כפל מודולו n
פונקציית אוילר $|G|=\phi(n)$
לכן

$$x\in\mathbb{Z}_n^* \quad \text{לכל} \quad x^{\phi(n)}=1$$

כלומר אם x טבעי זר ל n אז מתקיים $x^{\phi(n)}\equiv 1 \bmod n$

תתי חבורות
הגדרה תהי G חבורה. קבוצה חלקית $H\subseteq G$ נקראת תת חבורה (או חבורה חלקית) אם היא מהווה חבורה ביחס לכפל ולאיבר היחידה של G.
כלומר:
$1\in H$ (ניתן להמיר זאת בדרישה לכך שהיא תהיה לא-ריקה, ואז היחידה תנבע מהסגירות להופכי ולכפל)
סגירות H לכפל
סגירות H להופכי

(אסוציאטיביות נובעת בפרט מאסוציאטיביות ב G)

הערות:

1. נסמן תת חבורה ע"י $H \leq G$
2. אם G סופית אז הסגירות של H להופכי נובעת משתי הדרישות הקודמות, כי ל x סדר סופי ולכן $x^{|x|-1}=x^{-1}$ ומסגירות לכפל נובע ישירות ש $x^{-1}\in H$
3. $H \subset G$ תת חבורה אם"ם $H \neq \emptyset$ וגם $x, y \in H \Rightarrow x y^{-1} \in H$ (לא קשה להראות, תרגיל לבית)

<u>דוגמאות</u>

$$A_n \leq S_n$$
$$SL_n(F) \leq GL_n(F)$$

<u>10.11.08 – שיעור שלישי</u>

הערה: נזכיר ש $\phi(n)=n \cdot \prod_{p|n \ , \ p \ prime} (1-\frac{1}{p})$

דוגמה לתת-חבורה, בהנתן $x \in G$ נתבונן ב $\langle x \rangle = \{\dots, x^{-2}, x^{-1}, 1, x^1, x^2, \dots\}$
קל לראות למה זו תת חבורה.
מתקיים $|\langle x \rangle| = |x|$ (אולי ∞)
אם $|x|=n$ $x^n=1$
זה גורר $\langle x \rangle = \{1, x, \dots, x^n\}$

<u>הגדרה:</u> $\langle x \rangle$ <u>תקרא תת החבורה הנוצרת ע"י x, וחבורה כנ"ל תקרא **ציקלית**. נוצרת ע"י איבר אחד.</u>
דוגמא:
$(\mathbb{Z}, +, 0)$ חבורה ציקלית אינסופית נוצרת ע"י 1.
$(\dots -2, -1, 0, 1, 2, \dots)$
$(\mathbb{Z}_n, +, 0)$ חבורה ציקלית מסדר n , עם החיבור מודולו n.
אלה כל החבורות הציקליות (עד כדי איזומורפיזם)

<u>מחלקות של תת-חבורה</u>
תהי G חבורה ו $H \leq G$ תת חבורה.
<u>הגדרה:</u> **מחלקה שמאלית** של H היא קבוצה מהצורה $gH = \{gh : h \in H\}$ עבור $g \in G$ נתון.
מחלקה ימנית, Hg באותו אופן.
הערה: אם $h \in H$ אז $Hh=H \wedge hH=H$ שכן כפל משמאל או מימין משרה תמורה של איברי החבורה.
לעומת זאת אם $g \notin H$ אז בהכרח $gH \neq H$ כי $g=g \cdot 1 \in gH$ וכאמור $g \notin H$
(כמובן אם G אבלית אז $gH=Hg$)

<u>דוגמא</u>

$$G=(\mathbb{Z}_6, +, 0)$$
$$H=\{0,2,4\}$$

המחלקות של H:

$$0+H=H$$

$$1+H=\{1,3,5\}$$
$$2+H=\{0,2,4\}$$
$$3+H=\{1,3,5\}$$
$$4+H=\{0,2,4\}$$
$$5+H=\{1,3,5\}$$

נשים לב ש G היא איחוד זר של מחלקות.

<u>טענה</u> : תהי G חבורה כלשהי, $H\leq G$ תת חבורה
יהיו $g_1,g_2\in G$
אזי או שמתקיים $g_1H\cap g_2H=\emptyset$
או ש- $g_1H=g_2H$
כלומר מחלקות שמאליות שונות הן זרות. (כמובן כנ"ל לגבי מחלקות ימניות)
<u>הוכחה</u>:
נניח ש $g_1H\cap g_2H\neq\emptyset$ ונוכיח $g_1H=g_2H$
ניקח איבר בחיתוך הנ"ל אז אפשר לכתוב אותו $g_1h_1=g_2h_2$
כאשר $h_1,h_2\in H$
נבחר איבר כלשהו $g_1h\in g_1H$

$$g_1h=g_1h_1\cdot h^{-1}h=g_2\underbrace{h_2h^{-1}}_{\in H}h\in g_2H$$

ומכאן $g_1H\subseteq g_2H$
מטעמי סימטריה לא משנה עם מי התחלנו ולכן אפשר להראות את אותה הכלה בכיוון השני ומכאן
$g_1H=g_2H$
❑

<u>משפט</u>: תהי G חבורה, $H\leq G$ תת חבורה
יהיו $g\in X$, gH כל המחלקות השמאליות השונות זו מזו של H ב G.
(X מוגדרת להיות קבוצה של נציגים אשר יוצרים ע"י פעולת מחלקה על H – מחלקות שונות זו מזו)
אז $G=\coprod_{g\in X}gH$ (איחוד זר)
<u>הוכחה</u>
המחלקות $gH_{g\in X}$ הן שונות ע"פ הגדרת X, לכן הן זרות זו לזו עפ"י הטענה הקודמת.
מכאן שהאיחוד הוא זר כנדרש.
נותר להראות שהאיחוד הוא G ואמנם יהי $g\in G$ נתבונן במחלקה gH היא מופיעה כאחת המחלקות מהצורה g_1H כאשר $g_1\in X$ ואמנם

$$g\in gH=g_1H\Rightarrow g\in g_1H\,(g_1\in X)$$

לכן g באיחוד.

<u>הגדרה:</u> ה**אינדקס** של תת חבורה H בחבורה G מוגדר כמספר המחלקות השמאליות השונות של H (זה בעצם $|X|$ לפי הגדרת X כמקודם).
הוא יסומן $|G:H|$
הערה: כנ"ל ניתן להגדיר אינדקס כמספר המחלקות הימניות השונות
טענה – שני האינדקסים יתלכדו.
<u>למה</u>: ההעתקה $gH\to Hg^{-1}$ היא העתקה חח"ע ועל בין המחלקות השמאליות לימניות של G.

הוכחה:
ראשית נשים לב $H g^{-1}=(g H)^{-1}$:
$(g H)^{-1}=H^{-1}g^{-1}=H g^{-1}$ $(g h)^{-1}=h^{-1}g^{-1}\in H g^{-1}$
מכאן שקודם כל נובע שההעתקה $g H\to H g^{-1}$ מוגדרת היטב – לא תלויה בנציגים:
$g_1 H=g_2 H \Rightarrow (g_1 H)^{-1}=(g_2 H)^{-1} \Rightarrow H g_1^{-1}=H g_2^{-1}$
חח"ע:
נניח $H g_1^{-1}=H g_2^{-1}$
$\Rightarrow (H g_1^{-1})^{-1}=(H g_2^{-1})^{-1} \Rightarrow (g_1^{-1})^{-1}H^{-1}=(g_2^{-1})^{-1}H^{-1} \Rightarrow g_1 H=g_2 H$
על:
ניקח מחלקה ימנית $H g$ ונראה שהיא בתמונה:
$H g=H(g^{-1})^{-1}$
$g^{-1}H\to H g$
הוכחנו את הלמה ומכאן הטענה
❑

הערה: האינדקס יהיה תמיד סופי אם G סופית
אם G אינסופית האינדקס $|G:H|$ יכול להיות סופי או אינסופי ואז הוא מוגדר – עוצמת קבוצת המחלקות.

דוגמאות
$G=\mathbb{Z}_6 \quad H=\{0,2,4\} \Rightarrow |G:H|=2$
(כי היו שתי מחלקות)
עבור החבורה החיבורית $\mathbb{Z}$ נסתכל ב H כקבוצת הכפולות של 10. ואז $|G:H|=10$

טענה: תהי G חבורה סופית, אז $|G|=|G:H|\cdot|H|$
הוכחה
ראינו $G=\bigcup_{g\in X} g H$ כאשר $|g H|=|H|$ ו X היא קבוצת הנציגים למחלקות.
לכן
$|G|=\sum_{g\in X}|g H|=|X|\cdot|H|$
לבסוף
$|X|=|G:H| \Rightarrow |G|=|G:H|\cdot|H|$
בחבורות סופיות האינדקס הוא פשוט $\frac{|G|}{|H|}$ ונובע מכך כמובן שהגודל של H מחלק את הגודל של G.

משפט לגרנג': בחבורה סופית גודל תת חבורה מחלק את גודל החבורה
$H\le G \Rightarrow |H| \mid |G|$
מסקנה: בחבורה סופית סדר כל איבר בחבורה מחלק את גודל החבורה.
$X\in G\Rightarrow |X| \mid |G|$

הוכחה:
ניקח $H=\langle X\rangle$ החבורה הציקלית הנוצרת ע"י X.
אז ראינו ש - $|H|=|X|$
וממשפט לגרנג' נובע ש $|H| \mid |G|$ ולכן $|X| \mid |G|$

שימושים
לחבורה הסימטרית S_{10} אין תת חבורה בגודל 11.

זאת כי $|S_{10}|=10!$ וברור ש $11\nmid 10!$ כי 11 ראשוני.

<u>תתי חבורות נורמליות</u>

הגדרה: תת חבורה $N\leq G$ תקרא **תת חבורה נורמלית ב G** ותסומן $N\lhd G$
אם מתקיים $g^{-1}Ng=N$ לכל $g\in G$

<u>הערות:</u>

1.

תנאי שקול הוא $gNg^{-1}=N$
לכל $g\in G$ ע"י הצבת g^{-1} במקום g.

2.

תנאי שקול נוסף, טבעי יותר, הוא $gN=Ng$ לכל $g\in G$ כי $g(g^{-1}Ng)=Ng$ ולפי תנאי הנורמליות זה גם gN.
כלומר N נורמלית אם"ם כל מחלקה ימנית היא גם שמאלית עם אותו נציג.

3.

בחבורה אבלית G כל תת חבורה היא נורמלית

4.

בכל חבורה G מתקיים – תת החבורה הטריוויאלית (איבר היחידה) היא נורמלית, וכן G נורמלית בעצמה.

5.

דוגמא לחבורה לא נורמלית, נניח $G=S_3$ $H=\langle(12)\rangle=\{1,(12)\}$
אבל נקבל $(123)^{-1}(12)(123)=(13)\notin H$ לכן H לא נורמלית ב G, וזו אינה דוגמא יוצאת דופן.
בדרך כלל בחבורות לא אבליות, רוב תתי החבורות הן לא נורמליות. (כאשר "רוב" ו"בדרך כלל" הן הגדרות די עמומות, אבל כדי להמחיש פרינציפ).

6.

עוד הגדרה שקולה לנורמליות $g^{-1}Ng\subseteq N$ לכל $g\in G$ (משתמשים בה לעיתים כי יש לבדוק רק הכלה בכיוון אחד וזה קל יותר).
נראה כי הכלה גוררת שוויון:
נכפול משמאל ב g ומימין ב g^{-1} ונקבל $N\subseteq gNg^{-1}$ ואז נציב במקום g את g^{-1} ונקבל $N\subseteq g^{-1}Ng$
מההכלה הדו כיוונית קיבלנו את השוויון $g^{-1}Ng=N$
הערה: נעדיף לעיתים להשתמש בהכלה כיוון שזו דרישה יותר חלשה, במילים אחרות – פחות עבודה להוכיח אותה עבור מקרה מסויים.

הערה של תלמיד: אפשר גם בתנאי 2 לדרוש הכלה חלשה במקום שוויון?
ענר: כן, כי זה בדיוק אותו רעיון וההכלה גוררת שוויון

<u>שיעור רביעי</u>

<u>דוגמאות</u>

$A_n\lhd S_n$

הוכחה: צ"ל $g^{-1}A_ng\subseteq A_n$ לכל $g\in S_n$
כלומר ניקח $h\in A_n$ צ"ל $g^{-1}hg\in A_n$
<u>הערה-הגדרה:</u> $g^{-1}hg$ נקרא h **<u>מוצמד</u>** ע"י g ומסומן גם h^g ולעיתים ${}^gh$ (<u>הצמדה</u>)
ואמנם:

$$sgn(g^{-1}hg)=sgn(g^{-1})sgn(h)sgn(g)=sgn(g)^{-1}sgn(h)sgn(g)=\underbrace{sgn(g)^{-1}sgn(g)sgn(h)}_{\text{Sign is commutative}}=\underbrace{1\cdot sgn(h)}_{h\in A_n}=1$$

נוכיח טענה קצת יותר כללית – אנחנו יודעים ש $|S_n : A_n| = \frac{|S_n|}{|A_n|} = 2$, נראה שהנורמליות פה היא לא "במקרה".

<u>טענה:</u> תהי G חבורה כלשהי, $H \leq G$ תת חבורה מאינדקס 2, אז $H \lhd G$

הוכחה: ל H יש 2 מחלקות שמאליות, נקבע $g \in G$, $g \notin H$
וגם 2 מחלקות ימניות H , Hg gH , H
מכיוון ש G היא איחוד זר של מחלקות ימניות (שמאליות) אז
$$G = H \uplus gH = H \uplus Hg \Rightarrow gH = G \setminus H \ , \ Hg = G \setminus H \Rightarrow gH = Hg$$

לעומת זאת אם $g \in H$ אז אפילו קל יותר – $gH = H = Hg$
קל לחשוב על זה באופן הבא: אם יש שתי מחלקות – אז לכפול משמאל חבורה באיבר ומימין בהופכי שלו זה כמו להזיז את המחלקה הראשונה לשניה וחזרה (אם האיבר הוא לא מהחבורה) או לא לעשות כלום (אם האיבר הוא כן מהחבורה), ובכל מקרה קיבלנו שוב את החבורה שהתחלנו איתה.
❑

<u>הגדרה: חבורת מנה</u>
תהי G , כאשר $N \lhd G$ נגדיר חבורה שתסומן G/N ותקרא **חבורת המנה של G מודולו N**.
(זה באמת דומה למה שקורה כשלוקחים מספרים מודולו משהו סופי, אבל זה הרבה יותר כללי ואולי לא קומוטטיבי.)
$$G/N = \{Ng : g \in G\}$$
זהו למעשה אוסף המחלקות הימניות של N.
זה כמובן שווה למחלקות השמאליות, כי תת החבורה היא נורמלית.

היופי הוא שהנורמליות מאפשרת לנו להגדיר כפל על איברי G/N
נגדיר את הכפל כך:
$$Na \cdot Nb = Na \cdot b$$
כלומר מכפלת שתי מחלקות ימניות היא המחלקה הימנית הנוצרת ע"י מכפלת הנציגים.
האם זה מוגדר היטב? (כלומר האם לא משנה באיזה נציגים נשתמש – אם המחלקות אותן מחלקות – נקבל אותה תוצאה)
כן, כי:
$$Nab = (Na)(Nb)$$
כמכפלת קבוצות, נראה שזה נכון:
$$(Na)(Nb) = N(aN)b = N(Na)b = (NN)ab = Nab$$
ומשום שמכפלת קבוצות מוגדרת היטב (ומטבעה תלויה רק ב"מי הקבוצות") אזי הביטוי שלנו מוגדר היטב.

<u>הגדרת מכפלת קבוצות בחבורה G:</u>
$$X, Y \subseteq G$$
$$XY = \{xy : x \in X, y \in Y\}$$
זו מכפלה אסוציאטיבית
$$(XY)Z = X(YZ)$$
אם X תת חבורה אז $XX = X$

תכונות כפל המחלקות:
אסוציאטיביות:
$$(NaNb)Nc = Na(NbNc) \quad (Nab)Nc = Na(Nbc) \quad N(ab)c = Na(bc)$$

איבר יחידה: $N(=N1)$

$$NaN=NNa=Na$$

יש הופכי:

$$NaNa^{-1}=Naa^{-1}=N1=N=Na^{-1}Na$$

כלומר הופכי של Na הוא Na^{-1}

<u>מסקנה</u>: G/N **<u>עם פעולת הכפל הנ"ל היא חבורה (= חבורת המנה)</u>**

דוגמה:
$G=\mathbb{Z}$
$N=10\mathbb{Z}$ (ענר: סתם אני לוקח את 10 כמשל, יכול להיות גם 9)
$G/N=\{10\mathbb{Z}+i : i=0,1,..,9\}$
$(N+i)+(N+j)=N+i+j$
כביכול התוספת חורגת מ 10, אבל למעשה יוצא שנקבל חיבור מודולו 10.
ואז G/N איזומורפית ל $\mathbb{Z}_{10}$

איזומורפיזם = העתקה חח"ע ועל ששומרת על הפעולה בחבורה.

<u>שיעור חמישי – 17.11.08</u>

לדוגמה, בהמשך לשיעור הקודם, לכל n נסתכל בחבורה הנורמלית $n\mathbb{Z}$ כתת חבורה של החבורה החיבורית, ובחבורת המנה $G/N=\mathbb{Z}/n\mathbb{Z}$ (כל המחלקות הימניות של $n\mathbb{Z}$, כדאי לשחק קצת עם החיבור של המחלקות הללו כדי לראות את המשפט הבא)
אם נחבר שני איברים בחבורת המנה – זה מזכיר גם בחיבור וגם באיברים חבורה מוכרת – $\mathbb{Z}_n=\{0,...,n-1\}$
נראה בהמשך $\mathbb{Z}/n\mathbb{Z}$ איזומורפית ל $\mathbb{Z}_n$
לשם כך נזדקק להגדרות נוספות.

<u>הגדרה</u>: יהיו G, H חבורות.
העתקה $f:G\to H$ תקרא **<u>הומומורפיזם</u>** אם $f(xy)=f(x)f(y)$ (נשים לב שבתוך הסוגריים זהו כפל ב G ומחוץ לסוגריים כפל ב H)

שימור יחידה והופכי נובעים מהדרישה הקודמת.
טענה: $f:G\to H$ הומומורפיזם אז:
1. $f(1_G)=1_H$
2. $f(x^{-1})=f(x)^{-1}$

הוכחה:
1. $f(1)=f(1\cdot 1)=f(1)\cdot f(1) \Rightarrow 1=f(1)$
2. $1=f(1)=f(x\cdot x^{-1})=f(x)\cdot f(x^{-1}) \Rightarrow f(x)^{-1}=f(x^{-1})$

ענר: כאן זה אפילו יותר קל מאלגברה לינארית

<u>הגדרה</u>:
1. הומומורפיזם שהוא חח"ע יקרא **<u>מונומורפיזם</u>** (=שיכון)
2. הומומורפיזם שהוא על יקרא **<u>אפימורפיזם</u>**
3. הומומורפיזם שהוא חח"ע ועל יקרא **<u>איזומורפיזם</u>**

<u>דוגמאות</u>

.1

אם $H \le G$ אז ההעתקה $f: H \to G$ המוגדרת $f(h)=h$ היא מונומורפיזם.

.2

תהי $N \lhd G$ נגדיר העתקה $\Pi: G \to G/N$ ע"י $\Pi(g)=Ng$

אז Π העתקה כפלית. כי $\Pi(gh)=Ngh=Ng\,Nh=\Pi(g)\Pi(h)$

ענר: אולי זה קצת מופשט, אבל בקור רוח אפשר לראות שזה הומומורפיזם

Π היא על: כל מחלקה Ng היא בתמונה.

ענר: כל כך אין פה מה להוכיח שזה כמעט עלבון לאינטיליגנציה

<u>מסקנה</u>: Π הוא אפימורפיזם מ G ל G/N ולעיתים הוא נקרא **<u>ההטלה הקנונית</u>** מ G על G/N

<u>תת-דוגמה</u>

$$\Pi: \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$$
$$\Pi(i)=n\mathbb{Z}+i$$

.3

נתבונן בחבורות G,H:

$G=(\mathbb{Z}_2, +, 0)=\{0,1\}$ (חיבור מוד 2)

$H=\{1,-1\}$ עם כפל

נבנה איזומורפיזם $f: G \to H$

$$f(0)=1,\ f(1)=-1$$
$$f(x+y)=f(x)f(y)$$

התלמיד הנודניק יוודא זאת בעצמו.

.4

דוגמה נוספת לאיזומורפיזם:

$$f: \mathbb{Z}_n \to \mathbb{Z}/n\mathbb{Z}$$
$$i \to n\mathbb{Z}+i$$

שומר על פעולת החיבור מוד n.

ברור שהיא חח"ע ועל ולכן היא איזומורפיזם.

סימון $G \cong H$ אם G איזומורפית ל H.

<u>תמונה וגרעין של הומומורפיזם</u>

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

נגדיר $Image(f)=\{f(x): x \in g\}$

$$Ker(f)=\{x \in G: f(x)=1\}$$

<u>טענה:</u>

1.התמונה היא תת חבורה של H

2. הגרעין הוא תת חבורה נורמלית של G

<u>הוכחה</u>:

.1

$1 \in Image(f)$ כי $f(1_G)=1_H$

נניח ש $a, b \in Image(f)$ ונראה $ab \in Image(f)$

יש $x,y\in G$ כך ש $a=f(x)\ ,b=f(y)$ ואז $ab=f(x)\cdot f(y)=f(xy)\in Image(f)$
סגירות להופכי נובעת מכך ש $f(x^{-1})=f(x)^{-1}$

.2
$1\in Ker(f)$ כי $f(1)=1$
$$x,y\in Ker(f)\ \Rightarrow\ f(x)=1,\ f(y)=1\ \Rightarrow\ f(xy)=f(x)f(y)=1\ \Rightarrow\ xy\in Ker(f)$$
$$x\in Ker(f)\Rightarrow f(x)=1\Rightarrow f(x^{-1})=f(x)^{-1}=1^{-1}=1\ \Rightarrow\ x^{-1}\in Ker(f)$$
נורמליות הגרעין:
נניח $x\in Ker(f)$
ו $g\in G$ כלשהו
צ"ל $g^{-1}xg\in Ker(f)$
אבל על סמך כפליות:
$$f(g^{-1}xg)=f(g^{-1})f(x)f(g)=f(g^{-1})f(g)=f(g^{-1}g)=f(1)=1\ \Rightarrow\ g^{-1}xg\in Ker(f)$$
❑

<u>טענה</u>: כל תת חבורה נורמלית היא גרעין של הומומורפיזם.
נניח אם $N\lhd G$ נגדיר $\Pi:G\to G/N$ ההטלה הקנונית
אז
$$\Pi(g)=Ng\quad Ker(\Pi)=\{g\in G:Ng=N\}=\{g\in N\}=N$$

<u>משפטי איזומורפיזם</u>
<u>משפט האיזומורפיזם ה I</u>
יהי $f:G\to H$ הומומורפיזם, אז $G/Ker(f)\cong Image(f)$
נסמן $K=Ker(f)$ אז $K\lhd G$ נגדיר $\phi:G/K\to Image(f)$ ע"י $\phi(Kg)=f(g)$ ואז נראה ש:
1.זה מוגדר היטב
2.זה הומומורפיזם
3. ϕ חח"ע ועל ולכן זה איזומורפיזם
הוכחה:
.1
$Kg=Kg'$ אז $K=Kg'g^{-1}$ ולכן $g'g^{-1}\in K$ כלומר $f(g'g^{-1})=1$
אבל
$$1=f(g'g^{-1})=f(g')f(g^{-1})=f(g')f(g)^{-1}\ \Rightarrow\ f(g)=f(g')$$

.2
נראה כפליות.
$$\phi(Kg\cdot Kg')=\phi(Kgg')=f(gg')=f(g)f(g')=\phi(Kg)\phi(Kg')$$
ענר: תעשו לי טובה אם אתם מוכיחים את זה במבחן אז תשתמשו ב x ו y

3. ϕ חח"ע:
$$\phi(Kx)=\phi(Ky)\ \Rightarrow\ f(x)=f(y)\Rightarrow\ f(x\cdot y^{-1})=f(x)f(y)^{-1}=1$$
$$xy^{-1}\in Ker(f)=K\ \Rightarrow\ Kxy^{-1}=K\ \Rightarrow\ Kx=Ky$$
ϕ על:

כל איבר בתמונה של f הוא מהצורה $f(x)$ ל $x\in G$ כלשהו.
ו $f(x)=\phi(K\,x)$
הוא בתמונה של ϕ

<u>דוגמאות ושימושים</u>
.1
נתבונן ב $sgn:S_n\to\{\pm1\}$ (סימן התמורה)
$$sgn(\sigma\circ\tau)=sgn(\sigma)\cdot sgn(\tau)$$
ולכן sgn היא הומומורפיזם של חבורות.
$$Image(sgn)=\{\pm1\}$$
$Ker(sgn)=A_n$ התמורות הזוגיות.
$$S_n/Ker(sgn)\cong Image(sgn)$$
$$S_n/A_n\cong(\pm1\,,\,\cdot)\cong\mathbb{Z}_2$$

.2
$$G=GL_n(F)$$
מטריצות הפיכות מעל שדה F כלשהו עם כפל מטריצות.
$$det:G\to F^*$$
(F^* החבורה הכפלית של השדה)
$$det(A)=|A|$$
$$det(A\,B)=det(A)\,det(B)$$
מכאן שהדטרמיננטה היא הומומורפיזם מהחבורה $GL_n(F)$ לחבורה F^*
ולכן:
$Ker(det)=\{A\in GL_n(F):det(A)=1\}=SL_n(F)$ (המטריצות עם דטרמיננטה 1)
$Image(det)=F^*$ כי לכל λ ניקח מטריצת יחידה ונחליף את האיבר הפינתי ב λ ונקבל את דטרמיננטה שהיא בדיוק λ .
$$GL_n(F)/Ker(det)=Image(det)\quad\Rightarrow\quad GL_n(F)/SL_n(F)\cong F^*$$

.3
$f:\mathbb{Z}\to\mathbb{Z}_n$ ע"י $f(i)\to i\bmod n$
$$Image(f)=\mathbb{Z}_n\qquad Ker(f)=\{i\in\mathbb{Z}:i\equiv0\bmod n\}=n\mathbb{Z}$$
$$\mathbb{Z}/Ker(f)\cong Image(f)\quad\mathbb{Z}/n\mathbb{Z}\cong\mathbb{Z}_n$$

<u>שיעור שישי 19.11.08</u>
נוכיח טענה שקשורה למשפט האיזומורפיזם השני.
<u>טענה</u>:
יהיו $H\,,K\le G$
1.אז $HK=\{h\cdot k:h\in H\,,k\in K\}$ היא תת חבורה אם"ם $HK=KH$
2. אם $K\lhd G$ אז לכל $H\le G$ מתקיים HG=GH ולכן HK תת חבורה

הוכחה (הראינו גם בתרגיל אבל נראה זאת שוב)
.1
אם HK תת חבורה אז היא סגורה להופכי ולכן $HK=(HK)^{-1}$
מצד שני מאחר ש $(h\,k)^{-1}=k^{-1}h^{-1}$ נובע $(HK)^{-1}=K^{-1}H^{-1}=K\,H$
בכיוון השני: נניח HK=KH נוכיח HK חבורה:

$1 \in HK$ ברור כי $1 = 1 \cdot 1$

$(hk)^{-1} = k^{-1}h^{-1} \in \underbrace{KH = HK}_{given}$ (סגירות להופכי)

סגירות לכפל:

$(HK)(HK) = H(KH)K = H(HK)K = (HH)(KK) = HK$ (ככפל קבוצות)

2.

אם $K \triangleleft G$ אז $gK = Kg$ לכל $g \in G$

ולכן $HK = KH$ לכל תת חבורה (ואפילו תת קבוצה) H

<u>משפט האיזומורפיזם השני</u>

תהינה H, K תתי חבורות של G, כאשר $K \triangleleft G$

אז

$K \triangleleft HK$, $H \cap K \triangleleft H$ ומתקיים

$$HK/K \simeq H/(H \cap K)$$

<u>הוכחה:</u>

ראשית ברור ש HK תת חבורה של G עפ"י הטענה הקודמת

$K \triangleleft G$ ובפרט $K \triangleleft HK$

נראה כעת ש $(H \cap K) \triangleleft H$

ברור ש $H \cap K \leq G$ (חיתוך של תתי חבורות הוא חבורה)

ניקח $x \in H \cap K$ ו $h \in H$ אז

$h^{-1}xh \in K$ (כי $x \in K$ ו K נורמלית ב G)

כמו כן $x \in H$ ולכן

$h^{-1}xh \in H$

ומכאן קבלנו $h^{-1}xh \in H \cap K$ לכן $H \cap K \triangleleft H$

להוכחת האיזומורפיזם נתבונן בהטלה הקנונית $\Pi : G \to G/K$

$\Pi(g) = gK$

$\phi = \Pi_{|H} : H \to G/K$ (זה יהיה הסימון שלנו לצמצום תחומה של Π ל H)

הרעיון: נבדוק את הגרעין והתמונה של העתקה זו ונשתמש במשפט האיזומורפיזם ה I.

$$Ker\,\phi = \{h \in H : \phi(h) = 1_{G/K}\} = \{h \in H : \Pi(h) = 1_{G/K}\} = \{h \in H : h \in \underbrace{Ker(\Pi)}_{K}\} = \{h \in H : h \in K\} = H \cap K$$

כלומר $Ker(\phi) = H \cap K$

נסתכל בתמונה:

$$Image(\phi) = \{\phi(h) : h \in H\} = \{\Pi(h) : h \in H\} = \{hK : h \in H\} = HK/K$$

ממשפט האיזומורפיזם I נקבל:

$$H/Ker(\phi) \cong Image(\phi) \;\Rightarrow\; H/(H \cap K) \cong HK/K$$

<u>משפט האיזומורפיזם ה III</u>

(לקראת סוף השיעור, אחרי הרבה שאלות) ענר: הצלחתם למנוע את הוכחת משפט האיזומורפיזם השלישי אבל לא תצליחו למנוע ניסוח שלו:

תהי G חבורה, $K, H \triangleleft G$ תתי חבורות נורמליות

נניח בנוסף לכך $K \subseteq H$
אז:

$$H/K \lhd G/K$$

ומתקיים

$$(G/K)/(H/K) \cong G/H$$

<u>הוכחה</u>
נגדיר העתקה $f: G/K \to G/H$ ע"י $f(gK) = gH$
1. f מוגדרת היטב (אי תלות בנציגים)
צ"ל שאם $xK = yK$ אז $xH = yH$
ואמנם $xK = yK$ גורר $y^{-1}x \in K$ ולכן $y^{-1}x \in H$ (כי K מוכלת ב H)
ולכן $xH = yH$

2. f הומומורפיזם, כלומר כפלית:
$$f(xK \cdot yK) = f(xyK) = xyH = xHyH = f(xK) \cdot f(yK)$$
3.
נחשב את $Ker(f)$:
$$\{xK : f(xK) = 1_{G/H}\} = \{xK : xH = H\} = \{xK : x \in H\} = H/K$$

מהי תמונת ההעתקה? $Image(f) = G/H$
כי כל מחלקה gH מתקבל כ $f(gK)$

4. נשתמש במשפט האיזומורפיזם הראשון:
$$(G/K)/Ker(f) \cong Image(f) \Rightarrow (G/K)/(H/K) \cong G/H$$
הערה: עוד קודם מסיקים ש $G/K \lhd H/K$ כגרעין של הומומורפיזם.

<u>דוגמה</u>
$S^1 = \{z \in \mathbb{C} : |z| = 1\}$ $\mathbb{C}^*/S^1 \cong (\mathbb{R}^*_{pos}, \cdot)$ (S_1 היא מעגל היחידה)
ואכן ניקח את $f(z) = |z|$

<u>מכפלות ישרות של חבורות</u>
תהיינה G,H חבורות
נגדיר $G \times H = \{(g,h) : g \in G, h \in H\}$
ונגדיר גם כפל רכיב-רכיב:
$$(g_1, h_1)(g_2, h_2) = (g_1 g_2, h_1 h_2)$$

זה כפל אסוציאטיבי עם יחידה $(1_G, 1_H)$ ועם הופכי $(g,h)^{-1} = (g^{-1}, h^{-1})$
<u>מסקנה</u> $G \times H$ היא חבורה והיא נקראת **המכפלה הישרה של G ו H**

באופן דומה מגדירים מכפלות ישרות עם יותר קבוצות $G \times H \times K$

דוגמאות:
1.

$\mathbb{Z}\times\mathbb{Z}$ - סריג הנקודות השלמות במישור עם חיבור וקטורי.

2. $\mathbb{Z}_4\times\mathbb{Z}_5\cong\mathbb{Z}_{20}$

כללית אם m,n טבעיים זרים זה לזה אז מתקיים $\mathbb{Z}_m\times\mathbb{Z}_n\cong\mathbb{Z}_{mn}$

הוכחה ע"י משפט השאריות הסיני:
נניח m,n זרים, אז לכל $0\le i<m,\ 0\le j<n$
קיים k יחיד $0\le k<mn$ כך ש:
$k\equiv i \bmod m$
$k\equiv j \bmod n$
ואז לכל $i\in\mathbb{Z}_m\ \ j\in\mathbb{Z}_n$ נגדיר $f(i,j)=k$

זו סקיצה של ההוכחה, ללא כל הפרטים, אבל נשלים את חומר הרקע הדרוש בתרגול.

הערה: ללא הנחת הזרות אי אפשר לומר זאת כי חבורת המכפלה אינה ציקלית ואינה איזומורפית לשום חבורה חיבורית כלשהי בשלמים.

<u>יוצרים של חבורות</u>
תהי G חבורה, $X\subseteq G$ תת קבוצה, נשאל מהי תת החבורה הנוצרת ע"י X?
היא מוגדרת ע"י $\langle X\rangle=\bigcap_{X\subseteq H\le G} H$
הערות:
1. $\langle X\rangle$ היא תת חבורה (כחיתוך תתי חבורות)
2. מינימליות – אם H תת חבורה שמכילה את X אז H מכילה את תת החבורה הנוצרת ע"י X (די טבעי)

ניתן לאפיין את $\langle X\rangle$ כתת החבורה המינימלית של G שמכילה את X.

אפיון נוסף של $\langle X\rangle$:
נסגור את X לכפל ולהופכי כך שתהפוך לתת חבורה.
איך?
$x_1^{\varepsilon_1}\cdot x_2^{\varepsilon_2}\cdot\ldots\cdot x_n^{\varepsilon_n}\quad n\ge 0, x_i\in X,\ \varepsilon_i=\pm 1$
קל לראות שאוסף זה כבר סגור לכפל, הופכי ומכיל את 1 ולכן תת חבורה שמכיל את X.
מינימלית:
כל תת חבורה $H\le G$ שמכילה את X חייבת להכיל את הביטויים מהצורה הנ"ל ולכן H מכילה את תת החבורה הנ"ל שבנינו.

מכאן נובע שתת החבורה המינימלית כפי שהגדרנו היא בדיוק $\langle X\rangle$

<u>הגדרה:</u> נאמר ש $X\subseteq G$ היא <u>**קבוצת יוצרים**</u> ל G (או – <u>**יוצרת את G**</u>) אם $\langle X\rangle=G$

דוגמאות:
1.
G ציקלית אם יש לה קבוצת יוצרים בת איבר אחד.
עד כדי איזומורפיזם יש חבורה ציקלית יחידה מכל גודל $\mathbb{Z}_n$ מגודל n, ו $\mathbb{Z}$ עבור חבורה אינסופית.

.2
$G=\mathbb{Z}$
$X=\{4,5\}$
$\langle X\rangle=\mathbb{Z}$ כי $5-4=1$ ו $\mathbb{Z}=\langle 1\rangle$

יותר כללי:
אם m,n זרים אז $\langle m,n\rangle=\mathbb{Z}$ כי יש a,b שלמים $a\,m+b\,n=1$ וכאמור 1 הוא יוצר של השלמים.

עוד יותר כללי:
לכל $m,n\in\mathbb{Z}$ מתקיים $\langle m,n\rangle=gcd(m,n)\mathbb{Z}$ למשל $\langle 8,10\rangle=2\mathbb{Z}$

ראינו למשל בתרגיל 1 ש S_n נוצרת ע"י שני איברים $(12),(12\ldots n)$

<u>אוטומורפיזמים של חבורה</u>
הגדרה: G חבורה, $f:G\to G$ נקרא אוטומורפיזם של G אם הוא איזומורפיזם מ G לעצמו.
נגדיר $Aut\,G$ כאוסף האוטומורפיזמים של G. נגדיר כפל ע"י הרכבה ונקבל חבורה.

דוגמאות:
1.העתקת הזהות היא תמיד אוטומורפיזם.
2. $G=\mathbb{Z}$ אז $x\to -x$ אוטומורפיזם, קל לראות מהפיכות.

תרגיל:
$Aut\,\mathbb{Z}=\{Id_{\mathbb{Z}},-Id_{\mathbb{Z}}\}$

<u>אוטומורפיזמים פנימיים</u>
נקבע $g\in G$ נגדיר $\phi_g:G\to G$ ע"י $\phi_g(x)=g\,x\,g^{-1}$
טענה: $\phi_g\in Aut\,G$ לכל $g\in G$
<u>הוכחה</u>:
ϕ_g הומומורפיזם, נבדוק כפליות.
$\phi_g(x\,y)=g\,x\,y\,g^{-1}=g\,x\,g\,g^{-1}\,y\,g^{-1}=\phi_g(x)\,\phi_g(y)$
חח"ע:
$\phi_g(x)=\phi(y)\ /\cdot g^{-1}\cdot\ldots\cdot g\ \Rightarrow\ g^{-1}\cdot(g\,x\,g^{-1})\,g=g^{-1}\cdot(g\,y\,g^{-1})\,g\ \Rightarrow\ x=y$
על:
$\phi_g(g^{-1}\,x\,g)=g\,(g^{-1}\,x\,g)\,g^{-1}=x$
הערה $x\to g\,x$ גם חח"ע ועל אך לא הומומורפיזם לכל $g\neq 1$

<u>הגדרה:</u>
אוסף ה**אוטומורפיזמים הפנימיים** של G יסומן ב $Inn\,G$

<u>טענה</u>
$Inn\,G$ היא תת חבורה נורמלית של $Aut\,G$
<u>הוכחה:</u>
יחידה:
$Id\in Inn\,G$ באופן טבעי ע"י הצמדה עם 1
סגירות לכפל:

$$\phi_g \circ \phi_h(x)=\phi_g(\phi_h(x))=g(h\,x\,h^{-1})g^{-1}=(g\,h)x(g\,h)^{-1}=\phi_{g\,h}(x)$$
$$\Rightarrow\ \phi_g \circ \phi_h=\phi_{g\,h}\in Inn\,G$$
סגירות להופכי:
$$(\phi_g)^{-1}=\phi_{g^{-1}}\in Inn\,G$$
קל לוודא זאת.

נראה נורמליות:
ניקח $\phi_g\in Inn\,G$ ונצמיד אותו עם $\psi\in Aut\,G$
צ"ל: $\psi^{-1}\phi_g\psi\in Inn\,G$
זה שקול ל:
$\forall\,\psi\in Aut\,G\ \ \psi\,\phi_g\,\psi^{-1}\in Inn\,G$ ועם זה קצת יותר נוח לעבוד.

$$(\psi\,\phi_g\psi^{-1})(x)=\psi(\phi_g(\psi^{-1}(x)))=\psi(g\,\psi^{-1}(x)g^{-1})=\psi(g)\psi(\psi^{-1}(x))\psi(g^{-1})=\psi(g)\,x\,\psi(g)^{-1}=\phi_{\psi(g)}(x)$$
ומכאן המסקנה (כי זה מוכל ב Aut G):
$$\psi\,\phi_g\,\psi^{-1}=\phi_{\psi(g)}\in Inn\,G\quad\Rightarrow\quad Inn\,G\triangleleft Aut\,G$$

<u>המשך – שיעור 8, 26.11</u>
<u>דוגמה:</u>
G אבלית – אז – $Inn\,G=\{1\}=\{Id_G\}$

<u>מרכז</u>
הגדרה תהי G חבורה, **המרכז** שלה $Z(G)$ מוגדר על ידי:
$$Z(G)=\{g\in G:\forall\,x\in G:g\,x=x\,g\}$$
כלומר המרכז הוא אוסף אברי G שמתחלפים עם **<u>כל</u>** אברי G.

דוגמה:
$G=GL_n(F)$ המטריצות ההפיכות
$Z(G)=\{\lambda\,I:\lambda\in F^*\}$ המטריצות הסקלאריות (וראינו בלינארית שהן אכן מתחלפות עם האחרות)

דוגמה נוספת:
$Z(S_n)=\{1\}$ עבור $n\geq 3$

<u>טענה</u>: $Z(G)\triangleleft G$

<u>הוכחה</u>
אפשר להוכיח ישירות [תרגיל]
ניתן הוכחה קצרה ואלגנטית, נראה: המרכז הוא גרעין של הומומורפיזם כלשהו מ G לאנשהו.

נגדיר:
$f:G\to Inn\,G$ ע"י $f(g)=\phi_g$
מתקיים:
$$f(g\,h)=\phi_{g\,h}=\phi_g\,\phi_h=f(g)\,g(h)$$
כלומר זהו אכן הומומורפיזם.
$$Kerf=\{g\in G:\phi_g=1\}$$

ואז:
$$\phi_g = Id \Leftrightarrow \ \phi_g(x)=x \ \forall x\in G \ \Leftrightarrow \ g x g^{-1}=x \ \forall x\in G \ \Leftrightarrow \ g x = x g \ \ \forall x\in G \ \Leftrightarrow \ g\in Z(G)$$

מסקנה: $Ker f = Z(G)$
בפרט נובע $Z(G)\triangleleft G$

טענה: $G/Z(G)\simeq Inn G$
הוכחה: על סמך משפט האיזומורפיזם הראשון – $Image(f)=Inn\,G \quad Ker f = Z(G)$
מסקנה: $Z(G)=\{1\}\Rightarrow \ Inn\,G\cong G$
הוכחה: $G/\{1\}\cong G$
בפרט $Inn\,S_n\cong S_n \quad (n\geq 3)$

<u>הגדרה</u>:
$Out\,G = Aut\,G/Inn\,G$
חבורת האוטומורפיזמים החיצוניים. נשים לב שאלו לא אוטומורפיזמים, אלא מחלקות של חבורת האוטומורפיזמים הפנימיים.

דוגמה: ידוע (קשה ולכן זה <u>לא תרגיל</u>)
$n\geq 5, n\neq 6$
$Aut\,S_n = Inn\,S_n$
כלומר כל אוטומורפיזם של S_n הוא פנימי ולכן $Aut\,S_n\cong S_n$
$Out\,S_n=\{1\}$ עבור n כנ"ל.

<u>הגדרה</u>: חבורה G נקראת **<u>חבורה פשוטה</u>** אם
$N\triangleleft G \Rightarrow N=G \ \vee \ N=\{1\}$

דוגמאות:
1. $\mathbb{Z}_p$ עבור p ראשוני
2. A_n עבור $n\geq 5$ (דורש הוכחה)

עובדה:
חבורות פשוטות סופיות אבליות הן איזומורפיות ל $\mathbb{Z}_p$
החבורות הלא-אבליות מויינו במהלך בערך מאה שנה, סגרו את הפינה הזו בשנות ה 80 של המאה שעברה, וההוכחה המפורטת תופסת 15,000 עמודים.

מיון החבורות הפשוטות הסופיות Classification of Finite Simple Group
דוגמה החבורה $PSL_n(\mathbb{Z}_p)$ המוגדרת כך:
$PSL_n(\mathbb{Z}_p)=SL_n(\mathbb{Z}_p)/Z(SL_n(\mathbb{Z}_p))$
לחלק מהחפ"סות (להלן – חבורות פשוטות סופיות) G יש התכונה שכל האוטומורפיזמים שלהן הם פנימיים, כלומר
$Aut\,G = Inn\,G$
החפ"סות הן "אבני בניין" של החבורות הסופיות כולן.

ענר: למען הגילוי הנאות, במיון הראשון של 1980 היו גם 900 עמודים שמעולם לא פורסמו, כי היתה בהם טעות...
היום יש כבר דור שלישי של המיון - הוכחה מלאה ובה 5,000 עמודים.

<u>**פעולות של חבורות על קבוצות**</u>

דוגמה:
G חבורה, נגדיר X=G

$g\in G$ יפעל על X ע"י $g\,x=g\cdot x$ כאשר באגף ימין זהו כפל בחבורה.

<u>תכונות הפעולה</u>

1. $g(h\,x)=(g\cdot h)\,x$
2. $1\,x=x$

קיבלנו העתקה $G\times X\to X$
המקיימת את 1,2

(נשים לב שלא בהכרח הפעולה צריכה להיות על איברי החבורה, סתם במקרה בחרנו את X להיות בדיוק איברי G)

<u>הגדרה: **פעולה של חבורה G על קבוצה X**</u> (לאו דווקא G עצמה) היא העתקה $G\times X\to X$ המקיימת את 1 ו 2.

<u>שיעור תשיעי, 1.12.08</u>

המשך פעולות על חבורות של קבוצות -
נניח שנתונה פעולה כנ"ל.
לכל $g\in G$ נגדיר (בדומה לשיעור הקודם) $\tau_g:X\to X$ ע"י $\tau_g(x)=g\,x$
נראה שהיא חח"ע ועל.
חח"ע:

$$\tau_g(x)=\tau_g(y)\ \Rightarrow\ g\,x=g\,y\ \Rightarrow\ g^{-1}(g\,x)=g^{-1}(g\,y)\ \Rightarrow\ (g^{-1}\cdot g)x=(g^{-1}g\cdot g)\,y\ \Rightarrow\ x=y$$

על:

$$\tau_g(g^{-1}x)=g\,(g^{-1}x)=(g\,g^{-1})\,x=x\ \Rightarrow\ x\in Image(\tau_g)$$

מכאן ש τ היא תמורה (העתקה חח"ע ועל) על X.

תזכורת:

$$Sym(X)=\{\underbrace{\Pi:X\to X}_{\text{one-to-one and onto}}\}$$

החבורה הסימטרית על X ביחס לפעולת ההרכבה.

התאמנו לכל $g\in G$ העתקה כלשהי בחבורה הסימטרית.
נגדיר:

$$\phi:G\to Sym(X)\qquad \phi(g)=\tau_g$$

נראה ש ϕ הומומורפיזם.
צ"ל $\phi(g\,h)=\phi(g)\phi(h)$
כלומר:

$$\tau_g\circ\tau_h=\tau_{g\,h}$$
$$(\tau_g\circ\tau_h)x=g(h\,x)=(g\,h)x=\tau_{g\,h}(x)$$

מסקנה: בהנתן פעולה של G על X מקבלים הומומורפיזם

$$\phi:G\to Sym(X)$$

נראה שגם ההיפך נכון - בהנתן ϕ כנ"ל נבנה פעולה של G על X.

$$G\times X\to X$$
$$(g,x)\to \underbrace{\phi(g)}_{\in Sym(X)}\,x$$

נבדוק שאקסיומות 1 ו 2 מתקיימות עם הפעולה $g\,x=\phi(g)(x)$

$$1\,x=\phi(1)(x)=Id\,(x)=x$$
$$g(h\,x)=\phi(g)(\phi(h)(x))=(\phi(g)\circ\phi(h))(x)=\phi(g\,h)(x)=(g\,h)x$$

לסיכום – פעולה של G על X שקולה להומומורפיזם $G \to Sym(X)$

<u>דוגמה</u>

G=X – כפי שהגדרנו בסוף השיעור הקודם
נקבל הומומורפיזם $\phi : G \to Sym(G)$
ϕ חח"ע, כי:
$Ker(\phi) = \{g : \phi(g) = Id_G\} = \{1\}$
<u>הערה</u>: לכל הום' ϕ של חבורות מתקיים ϕ חח"ע $\Leftrightarrow$ $Ker\,\phi = \{1\}$
הוכחה: תרגיל.

הום' חח"ע נקרא שיכון.

<u>משפט קיילי כל חבורה ניתן לשיכון בחבורת תמורות</u>
ביתר פירוט: יש שיכון מהחבורה G לחבורת התמורות $Sym(G)$
ניסוח שקול:
כל חבורה G היא איזומורפית לתת חבורה של חבורת התמורות $Sym(G)$

הסיבה: ϕ חח"ע $\Leftarrow$ $\phi(G) \cong G$

תרגיל: עבור חבורות G בגודל n לבנות את ϕ הנ"ל $\phi : G \to S_n$ ואז נקבל $G \subseteq S_n$,

<u>למשל</u>
$G = \mathbb{Z}_3$
$\phi : G \to S_3$
$0 \to Id \quad 1 \to (123) \quad 2 \to (132)$

לכן $G \cong \{Id, (123), (132)\} \subseteq S_3$

באופן דומה ניקח $G = \mathbb{Z}_2 \times \mathbb{Z}_2$ ונחפש $\phi : G \to S_4$
ניתן לוודא ש $G \cong \langle (12)(34), (13)(24) \rangle$
$1 \quad (0,0)$
$2 \quad (0,1)$
$3 \quad (1,0)$
$4 \quad (1,1)$
$(0,0) \to Id$
$(0,1) \to (12)(34)$
$(1,0) \to (14)(23)$
$(1,1) \to (14)(23)$
לחבורה זו קוראים חבורת קליין.

אלגוריתם לייצוג חבורה בגודל n כתת חבורה של S_n
1.
נכנה את איברי החבורה G בשמות 1 עד n
2.

לכל איבר $g\in G$
נתבונן בהעתקה $\{1,\dots n\}\to\{1,\dots,n\}$ שהוא משרה ע"י כפל משמאל $x\to g\,x$
נקבל תמורה $\tau_g\in S_n$
.3
אוסף התמורות $\{\tau_1,\dots,\tau_n\}$
מהווה תת חבורה של S_n שאיזומורפית ל G.
<u>תרגיל</u>
בצעו זאת עבור $G=S_3$, נקבל שיכון ב S_6 כי $|G|=6$
$\phi: S_3\to S_6$

הדוגמה הראשונה שהבאנו לפעולה של G על G נקראת לפעמים **הפעולה הרגולרית**.

דוגמאות נוספות לפעולות:
.2
$G=S_n$
$X=\{1,\dots,n\}$
$g\,x=g(x)$

.3
G כלשהי
X=G עם פעולת ההצמדה:
$g\,x=g\cdot x\cdot g^{-1}$ (שוב – מימין זו פעולה בתוך החבורה)
$\phi(g)(x)=g\cdot x\cdot g^{-1}$
$\phi(g)$ הוא האוטומורפיזם הפנימי של G המושרה ע"י g.

<u>הגדרה</u>
פעולה של G על X תקרא **<u>נאמנה</u>** (faithfull) אם ההומומורפיזם המתאים $\phi: G\to Sym(X)$ הוא חח"ע.

בדוגמת הפעולה הרגולרית ראינו ש ϕ חח"ע ולכן נאמנה.
בדוגמה 2 – גם נאמנה (לבדוק לבד בבית) ובעצם כאן ϕ זהו איזומורפיזם מ S_n ל S_n

דוגמה 3 – לא תמיד ϕ חח"ע, למשל G אבלית ואז:
$\phi(g)(x)=g\,x\,g^{-1}=x\ \Rightarrow\ \phi(g)=Id_G\ \ \forall\, g$
ולכן ϕ היא "הכי לא חח"ע שאפשר" כי היא מעתיקה את כולם להעתקת הזהות, והפעולה ודאי לא נאמנה.

$$\text{הפעולה נאמנה}\ \Leftrightarrow\ Ker\,\phi=\{1\}\ \Leftrightarrow\ \left[(\forall\, x: g\,x=x)\ \Rightarrow\ g=1\right]$$

הגדרה:
1. **המסלול (Orbit=) של נקודה** $x\in X$ מוגדר ע"י $O(x)=\{g\,x: g\in G\}$
2. **המייצב (Stabilizer=) של נקודה** מוגדר ע"י $G_X=\{g\in G: g\,x=x\}$

טענה:
שני מסלולים $O(x),O(y)$ הם או זהים או זרים.
<u>הוכחה</u>
נניח שאינם זרים אז יש $z\in O(x)\cap O(y)$
לכן יש $g,h\in G$ כך ש – $z=g\,x=h\,y$

לכן $(h^{-1}g)x=h^{-1}(gx)=h^{-1}(hy)=...=y$
ולפיכך $y\in O(x)$ ומכאן נובע $O(y)\subseteq O(x)$
כי:
$$g_1 y=g_1(h^{-1}gx)=(g_1h^{-1}g)x$$
מטעמי סימטריה אותו הדבר יעבוד בכיוון השני ולכן $O(x)\subseteq O(y)$
ולכן $O(y)=O(x)$ כנדרש ❑

מסקנה: X היא איחוד זר של מסלולים
$$X=\coprod\{O(x):x\in X\}$$

הגדרה הפעולה נקראת **טרנזיטיבית** אם יש מסלול יחיד, כלומר X היא מסלול.

טענה: המייצב G_X הוא תת חבורה של G.
הוכחה:
ברור ש $1\in G_X$ כי $1x=x$
בנוסף:
$$g,h\in G_X \Rightarrow gx=x, hx=x$$
$$(gh)x=g(hx)=gx=x \Rightarrow gh\in G_X$$
וגם:
$$g\in G_X \Rightarrow gx=x \Rightarrow g^{-1}x=g^{-1}(gx)=x \Rightarrow g^{-1}\in G_X$$

טענה: יש העתקה חח"ע ועל $f:O(x)\to \underbrace{G/G_X}_{\text{קבוצת המחלקות השמאליות}}$
נשים לב ל abuse of notation כיוון שלא אמרנו ש G_X נורמלית וזו אינה חבורת המנה כי אם קבוצת המחלקות השמאליות של G_X ב G.

הוכחה
נגדיר $f(hx)=hG_X$
נבדוק ש f מוגדרת היטב כלומר $hx=kx \Rightarrow hG_X=kG_X$ ואמנם:
$$hx=kx \Rightarrow h^{-1}kx=x \Rightarrow h^{-1}k\in G_X \Rightarrow h^{-1}kG_X=G_X \Rightarrow hh^{-1}kG_X=hG_X \Rightarrow hG_X=kG_X$$
f חח"ע:
צ"ל $hG_X=kG_X \Rightarrow hx=kx$
הוכחה – ע"י הפיכת כיווני הגרירה בהוכחה הקודמת.

f על – מיידי כי כל איבר של G/G_X הוא מהצורה- hG_X כלומר $f(hx)$

שיעור עשירי 3.12.08

טענה:
גודל המסלול הוא האינדקס של המייצב, כלומר:
$$|O(x)|=|G:G_x|$$
(שימוש עיקרי יהיה כשהכל סופי, אך זה נכון גם למקרה האינסופי במובן של עוצמות)

הוכחה: כי יש העתקה חח"ע בין $O(x)$ ל G/G_x ו $|G/G_x|=|G:G_x|$

מסקנה: תהי G חבורה סופית הפועלת על קבוצה X
אזי – גודל כל מסלול מחלק את גודל החבורה, וזה ברור מהטענה הקודמת כי כבר אמרנו שאינדקס של תת חבורה מחלק את גודל החבורה.

(הערה: הפעולה הטריוויאלית היא כאשר אנחנו מגדירים שחבורה G פועלת על קבוצה X ע"י $g\,x=x$ לכל g ו x)

דוגמאות:
.1
תהי G חב' בגודל 7 שפועלת לא טריויאלית על קבוצה X בגודל 9.
מה גדלי המסלולים?
3 מסלולים שגדליהם – 1,1,7

הוכחה:
גודל כל מסלול מחלק את 7 כפי שראינו ולכן הוא 7 או 1.
יש חלוקה X=איחוד זר של מסלולים, ולכן סכום גדלי המסלולים הוא 9.
לכאורה היינו יכולים לבחור $1+1+1+1+1+1+1+1+1=9$ אבל זו הפעולה הטריוויאלית ומכאן מתחייבת המסקנה.

איבר טיפוסי של החבורה עד כדי שינוי שמות הנקודות יהיה $(9)(8)(7\ldots 1\,2)$

.2
$|G|=6$
$|X|=5$
ונניח שאין מסלולים בגודל 1, נובע שיש שני מסלולים בגדלים 2,3 מנימוק דומה לדוגמה הקודמת.

טענה: $h\,G_x\,h^{-1}=G_{h\,x}$ כאשר $h\in G\,,\,x\in X$
הוכחה: $g\in G_{h\,x} \Leftrightarrow g(h\,x)=h\,x \Leftrightarrow (g\,h)\,x=h\,x \Leftrightarrow h^{-1}(g\,h)\,x=x$
$\Leftrightarrow (h^{-1}\,g\,h)\,x=x \Leftrightarrow h^{-1}\,g\,h\in G_x \Leftrightarrow g\in h\,G_x\,h^{-1}$ ❑

מסקנות
1. צמוד של מיצב נקודה הוא גם מיצב של נקודה (אולי אחרת)
2. מייצבים של 2 נקודות x,y באותו מסלול הם צמודים
3. בפרט לכל מייצב של נקודות שהן באותו מסלול יהיה אותו גודל (אפשר היה בעצם להסיק זאת קודם מ $|O(x)|=|G:G_x|$ ו $|O(y)|=|G:G_y|$ ולכן $|G_x|=|G_y|$)

<u>פעולה טרנזיטיבית</u>
פעולה בה יש מסלול יחיד, כלומר לכל $x\,,y\in X$ יש $g\in G$ כך ש $g\,x=y$
<u>דוגמאות</u>
.1
$G=S_n$ על $\{1\ldots n\}$
.2
$G=A_n$ על אותו X לכל $n\neq 2$
.3
הפעולה הרגולרית (תזכורת: ע"י כפל משמאל) של G על G

<u>אנטי-דוגמה:</u>
פעולה לא-טרנזיטיבית היא למשל פעולת ההצמדה.
כי היחידה תמיד עוברת לעצמה, ובכל חבורה שיש בה יותר מאיבר אחד – לא יתכן שזה המסלול היחיד (כי אי אפשר להצמיד את 1 ע"י איבר כלשהו ולקבל משהו שאינו 1, מכאן שהיחידה במסלול משלה).

<u>טענה</u>: תהי G חבורה הפועלת טרנזיטיבית על קבוצה X.
יהי $H=G_x$ עבור $x\in X$ כלשהו ואז:
1. $|X|=|G:H|$
2. מייצבי הנקודות הם צמודי H (כלומר gHg^{-1})
3. אם $\phi:G\to Sym(X)$ הוא ההומומורפיזם המתאים אז $Ker\,\phi=\bigcap_{g\in G} g\,H\,g^{-1}$

<u>הוכחה</u>:
1.
כי $X=O(x)$ (כי יש מסלול אחד) ו $H=G_x$ ולכן נציב בנוסחה הקודמת: $|O(x)|=|G:G_x|$ ונקבל את המבוקש.
2.
נובע מכך שאם ניקח $y\in X$ כלשהו יש $g\in G$ כך ש $g\,x=y$ ואז:
$$G_y=G_{g\,x}=g\,G_x\,g^{-1}=g\,H\,g^{-1}$$
3.
$$a\in Ker\,\phi \;\Leftrightarrow\; \phi(a)(y)=y\;\;\forall\, y\in X \;\Leftrightarrow\; a\,y=y \;\Leftrightarrow\; a\in\bigcap_{y\in X} G_y \;\Leftrightarrow\; a\in\bigcap_{g\in G} g\,H\,g^{-1}$$

<u>שיעור 11 , 8.12.08 (ארז לפיד מחליף את ענר)</u>

דוגמה לפעולה על חבורה, נניח $H\le G$ ו G/H המחלקות השמאליות
אז G פועלת על G/H על ידי $g\cdot(x\,H)=(g\,x)\,H$
קל לראות שזה מוגדר היטב (כלומר אינו תלוי בנציג x) וכבר עשינו זאת בעבר.

עבור $g=1$ מקבלים את העתקת הזהות (וזה מקיים את האקסיומה הראשונה של פעולה של חבורה על קבוצה) ואסוציאטיביות כאן מושרית מאסוציאטיביות של כפל בחבורה.

נשים לב כי G פועלת טרנזיטיבית על G/H כי לכל $a\,,b\in G$ אם קיימות $aH\,,bH$ אז:
$(b\,a^{-1})\,a\,H=b\,H$ ולכן הן באותו מסלול.

מהם המייצבים?
נסמן את H בתור מחלקה בחבורת המנה ע"י eH
ואז:
$$G_{e\,H}=\{g\in G: g\,e\,H=e\,H\}=\{g\in G: g\,H=H\}=H$$
$$G_{x\,H}=G_{x\,e\,H}=x\,G_{e\,H}\,x^{-1}=x\,H\,x^{-1}$$
אם נסמן X = G/H אז הפעולה מגדירה הומומורפיזם $\phi:G\to Sym(X)$
נניח שהגודל של X, כלומר האינדקס של H – הוא $|X|=[G:H]=n$
$\phi:G\to S_n$
מה הגרעין של ϕ ?
$$Ker\,\phi=\bigcap_{x\in X} G_x \;\Rightarrow\; Ker\,\phi=\bigcap_{x\in G} x\,H\,x^{-1}$$
נשים לב ש $x\,H\,x^{-1}$ תלוי ב $x\,H$ ולא ב x, כלומר הוא פועל יוצא של בחירת מחלקה ולא בחירת נציג מסויים דווקא.

<u>טענה:</u>

$Core(H)=\bigcap_{g\in G} g H g^{-1}$ היא תת החבורה הנורמלית המקסימלית של G שמוכלת ב H.

<u>הוכחה</u>:
באחד התרגילים הקודמים (כנראה תרגיל 3)

<u>מסקנה</u>: אם ל G יש תת חבורה מאינדקס n אזי ל G יש תת חבורה נורמלית מאינדקס המחלק את $n!$

<u>הוכחה</u>: נסתכל על הגרעין של $\phi: G\to S_n$ ראינו ש $Core(H)=Ker\,\phi \triangleleft G$
כיוון ש $|S_n|=n!$
$G/Ker\,\phi \simeq Image(\phi)$ ולכן $[G:Ker\,\phi]\,|\,n!$ לפי משפט לגראנז'

בפרט אם n>1 ואם $|G|<n!$
או ש $|G|\nmid n!$ אז G אינה פשוטה.

הוכחה: נניח בשלילה ש G פשוטה, אם $|G|>n!$
מהמסקנה קיימת תת חבורה נורמלית K מאינדקס המחלק את $n!$
כיוון ש G פשוטה – K=G או $K=\{1\}$ לא יתכן ש K היא היחידה כי האינדקס של חבורת היחידה הוא $|G|$
אבל מהבניה של K נובע $K=Core(H)=\bigcap_{g\in G} g H g^{-1}\subseteq H$
לא יתכן ש K=G אלא אם H=G.

למשל - A_5 חבורה פשוט שגדלה 60.
לא קיימת ל A_5 חבורה מסדר 20.

נראה את החלק השני –כלומר שאם G פשוטה אז $|G|\,|\,n!$
הוכחה: כיוון ש G פשוטה אז $Ker\,\phi=\{1\}$ ואז ממשפט האיזומורפיזם $G/Ker\,\phi\simeq Image(\phi)$ ומכיוון שזו תת חבורה ב S_n אז האינדקס שלה מחלק את הגודל של S_n וצד שמאל הוא G, ולכן היא איזומורפית לתת חבורה ב S_n וממשפט לגראנז' קיבלנו את הרצוי.

הערה: אם H תת חבורה מאינדקס 2 אז H נורמלית (כי $[G:Core(H)]/2!=2$)

דוגמאות נוספות של פעולות של חבורה על קבוצה:
G המטריצות ההפיכות מעל F במימד n.
G פועלת על F^n ע"י כפל וקטורים ומטריצות.

X קבוצה כלשהי
S_n פועלת על $X^n=X\times X\times ...\times X$ על ידי:
$\sigma\in S_n$
$\sigma(x_1,...,x_n)=(x_{\sigma^{-1}(1)},x_{\sigma^{-1}(2)},...,x_{\sigma^{-1}(n)})$
למה זו פעולה?
הפעולה עבור תמורת הזהות ברורה ולכן האקסיומה הראשונה.
ולכל $\tau\in S_n$ נקבל:
$\tau(\sigma(x_1,...,x_n))=\tau(x_{\sigma^{-1}(1)},...,x_{\sigma^{-1}(n)})$
נסמן $y_k=x_{\sigma^{-1}(k)}$ ואז:
$(\tau\sigma)(x_1,...,x_n)=(x_{(\tau\sigma)^{-1}(1)},...)=(x_{\sigma^{-1}(\tau^{-1}(1))},...,x_{\sigma^{-1}(\tau^{-1}(n))})=(y_{\tau^{-1}(1)},...,y_{\tau^{-1}(n)})=$

פעולה נוספת:
H – חציו העליון של המישור המרוכב כלומר $H=\{z=x+iy: y>0\}$
נגדיר פעולה של המטריצות עם דטרמינטה 1 בגודל 2×2 על ידי:
$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} z=\frac{az+b}{cz+d}\in H$$
העתקות מביוס.
להוכיח שזו פעולה – תרגיל לבית.

טבעי בהקשר זה לשאול מתי שתי פעולות הן שקולות.
<u>הגדרה</u>
נניח ש G פועלת על X ועל X'
נאמר ש**<u>הפעולות הן שקולות</u>** אם קיימת העתקה חח"ע ועל $f: X\to X'$ כך שלכל $x\in X$ ו $g\in G$
$$f(gx)=gf(x)$$
באגף ימין זו הפעולה על X' ובאגף שמאל זו הפעולה על X

כלומר זו אותה פעולה עד כדי שינוי שמות האיברים ב X.

דוגמה:
X כלשהי
S_n פועלת על X^n כמקודם.
אם X' קבוצה אחרת ו $f: X\to X'$ חח"ע ועל.
אז הפעולות של S_n על X^n ועל X'^n שקולות ע"י $f^n: X^n\to X'^n$ העתקה קואורדינטה-קואורדינטה.

דוגמה:
הפעולה הרגולרית השמאלית של G שקולה לפעולה הרגולרית הימנית.
אם הרגולרית הימנית היא כפל בצמוד מימין, אז ברור שההעתקה $T(x)=x^{-1}$ עושה את העבודה.

שאלה של תלמיד: האם יש מצב שבו יש איזומורפיזם בין הקבוצות אבל פעולות אינן שקולות.
ארז: בוודאי, קח את G והפעולה הטריוויאלית שלה על עצמה, ומצד שני פעולה לא טריוויאלית.

<u>טענה</u>: נניח ש G פועלת טרנזיטיבית על X.
תהי $x_0\in X$
אז הפעולה של G על X שקולה לפעולה של G על G/G_{x_0}
<u>הוכחה:</u>
למעשה זה הוכח כבר בעבר, הגדרנו איזומורפיזם בין $O_{x_0}=X$ ובין G/G_{x_0} (X טרנזיטיבית לכן המסלול של איבר הוא כל הקבוצה) ע"י:
$$gG_{x_0}\to gx_0$$
נותר לבדוק ש f היא שקילות של פעולות.
אכן אם $g'\in G$ אז:
$$f(g'\cdot(gG_{x_0}))=f(g'gG_{x_0})=g'gx_0$$
מצד שני:
$$g'f(gG_{x_0})=g'(gx_0)=(g'g)x_0$$
ולכן הפעולות שקולות. ❑
שתי הערות:

1. המיצב G_{x_0} תלוי ב x_0 אבל אם $x_0' \in X$ אז $G_{x_0'}$ צמוד ל G_{x_0}
2. הפעולות של G על G/H הן שקולות G/H' אם ורק אם קיים $g \in G$ כך ש $H' = g H g^{-1}$

<u>מה קורה אם הפעולה אינה טרנזיטיבית?</u>

למשל G פועלת על עצמה ע"י הצמדה, $(g,x) \to g x g^{-1}$
המסלולים הם מחלקות הצמידות.
נתעניין מה מספר המסלולים (=מחלקות הצמידות)?

למה (Burnside, Cauchy):
נניח ש G פועלת על X.
מספר המסלולים של X = המספר הממוצע של נקודות שבת של $g \in G$.

<u>הגדרה</u>: **x נקראת נקודת שבת של** $g \in G$ **אם** $g x = x$
נסמן $Fix(g) = \{x \in X : g x = x\}$

כלומר ניסוח הטענה אומר שמספר המסלולים הוא:

$$\frac{1}{|G|} \sum_{g \in G} |Fix(g)|$$

בפרט:

$$|G| \| \sum_{g \in G} |Fix(g)|$$

<u>הוכחה</u>
נספור את נקודות השבת.
נגדיר:

$$A = \{(g,x) \in G \times X : g x = x\}$$

נמנה את איברי A בשתי צורות, נקבע את g ונקבע את x, כל אחד בנפרד.

מצד אחד:

$$A = \bigcup_{g \in G} \{g\} \times Fix(g) \;\Rightarrow\; |A| = \sum_{g \in G} |Fix(g)|$$

מצד שני:

$$A = \bigcup_{x \in X} G_x \times \{x\} \;\Rightarrow\; |A| = \sum_{x \in X} |G_x|$$

נניח שהמסלולים של G על X הם האיחוד הזר $O_1 \cup \ldots \cup O_n$ ואז ניתן להחליף את הסכימה על כל $g \in G$ לסכימה על כל ה $g \in O_i$ לכל i בנפרד.

$$\sum_{x \in O_i} |G_x| = \sum_{x \in O_i} \frac{|G|}{[G : G_x]} \qquad reminder : [G : G_x] = |O_i| \quad \Rightarrow \quad \sum_{x \in O_i} \frac{|G|}{|O_i|} = |O_i| \cdot \frac{|G|}{|O_i|} = |G|$$

כאשר מסכמים על כל ה $i = 1, \ldots, n$

$$\sum_{x \in X} |G_x| = \sum_{i=1}^{n} \left(\sum_{x \in O_i} |G_x| \right) = |G| \cdot n$$

ובסופו של דבר קיבלנו ש

$$\sum_{g\in G}|Fix(g)|=|G|\cdot|\text{המסלולים}|$$

ומכאן הטענה:

$$\text{מספר המסלולים}=\frac{1}{|G|}\sum_{g\in G}|Fix(g)|$$

❑

מסקנה: אם G פועלת טרנזיטיבית אז המספר הממוצע של נק' שבת של $g\in G$ הוא 1, בפרט אם $1<|X|=n$ ו G פועלת באופן נאמן (יש שיכון של G ב S_n) אז קיים $g\neq 1$ ללא נק' שבת (על X).
הוכחה: ל g=1 יש n נקודות שבת, אבל הממוצע הוא 1 ולכן קיים g עם פחות מנקודת שבת אחת ולכן ללא נק' שבת.

<u>דוגמה:</u>
למשל S_n פועלת על X^n נניח ש $X=\{0,1\}$ מספר המסלולים $=(n+1)!$
$(y_1,\dots,y_n)\sim(x_1,\dots,x_n)\Leftrightarrow\sum x_i=\sum y_i$

<מכאן קצת איבדתי אותו, למרות שזאת כנראה דוגמה מעניינת, אבל מכיוון שזו רק דוגמה, נסתפק בזה>

<u>שיעור 12 – עם ארז לפיד, 10.12.08</u>
נסמן $r=r(\sigma)$ (למשל $r(id)=n$)
הראינו:

$$n+1=\frac{1}{n!}\cdot\sum_{\sigma\in S_n}2^{r(\sigma)}$$

G פועלת על X, נניח $X=\coprod_{i=1}^{l}O_i$
O_i המסלולים הזרים (כיוון שאלו מחלקות שקילות)

$$|X|=\sum_{i=1}^{l}|O_i|$$

נסמן $x_1,\dots,x_l$ נציגים למסלולים.

$$|O_i|=[G:G_{x_i}]=\frac{|G|}{|G_{x_i}|}$$

לכן:

$$|X|=\sum_{i=1}^{l}\frac{|G|}{|G_{x_i}|}\quad *$$

נסתכל על פעולת ההצמדה של G על X=G כלומר $g\cdot x=g\,x\,g^{-1}$

המסלולים הם מחלקות הצמידות.
$x\in X=G$ מחלקת הצמידות של $x^G=\{g\,x\,g^{-1}:g\in G\}$
$|x^G|=[G:G_x]$

למה: $G_x=\{g\in G:g\,x=x\,g\}$
הוכחה:

$$g\cdot x=x\Leftrightarrow g\in G_x\Leftrightarrow g\,x\,g^{-1}=x\Leftrightarrow g\,x=g\,x\,g^{-1}=x\,g$$
❑

נסמן את הרכז של x ב G ע"י $C_G(x)=\{g\in G: g\,x=x\,g\}$
מסקנה:

1. $\forall\, x\in G \quad |x^G|=\frac{|G|}{|C_G(x)|}$
2. אם $x_1,\ldots,x_h$ נציגים למחלקות הצמידות של G, כאשר h מספר מחלקות הצמידות של G. אז:
$$1=\sum_{i=1}^{h}\frac{1}{|C_G(x_i)|}$$ (נובע מהסכום הקודם *)

דוגמאות:

1. אם G אבלית אז $h=|G|=n$ לכל $x\in G$ $C_G(x)=G$ ואז $1=\sum_{i=1}^{n}\frac{1}{n}$
2. $G=S_3$ יש 3 מחלקות צמידות (בגדלים 1,2,3) ואז נקבל $1=\frac{1}{6}+\frac{1}{3}+\frac{1}{2}$

הערה:
יש שוויון מהצורה:
$$1=\frac{1}{m_1}+\frac{1}{m_2}+\ldots+\frac{1}{m_2} \qquad m_1=n\geq m_2>\ldots\geq m_h$$
ניתן להוכיח (ארדש-טוראן) כי $h>\log\log n$
בפרט יש רק מספר סופי של חבורות סופיות עם מספר מחלקות צמידות נתון.

עוד הערה: מצד שני, כל חבורה חסרת פיתול (= כל $x\neq 1$ *בה הוא מסדר אינסופי) ניתנת לשיכון בחבורה בעלת שתי מחלקות צמידות, כלומר שבה כל שני איברים שונים מ 1 הם צמודים.*

נמשיך, אמרנו ש $1=\sum_{i=1}^{h}\frac{1}{|C_G(x_i)|}$
נגדיר את הנציג הראשון להיות היחידה בחבורה, ואז $C_G(x_1)=G$
נשאל מתי $C_G(x)=G$ באופן כללי?
זה קורה אם"ם $x\in Z(G)$ (כלומר x מתחלף עם כולם)

נניח ש $\{x_1,\ldots,x_h\}=Z(G)$
כל איבר במרכז מהווה מחלקת צמידות (כי הוא מתחלף עם כולם, ההצמדה מצטמצמת והוא נשאר בודד במחלקתו)
נקבל: $|G|=|Z(G)|+\sum_{i>k}\frac{|G|}{|C_G(x_i)|}$
זוהי **משוואת המחלקות**
מכיוון שהמרכז לעולם לא ריק (היחידה בו) נובע גם מיידית $\left|\bigcup_{i>k}C_G(x_i)\right|<|G|$

<u>משפט Cauchy</u>
אם $p\|G|$ (p ראשוני)
אז קיים ב G איבר מסדר p.

(כלומר G מכילה תת חבורה ציקלית מסדר p)
הערה: מספיק להוכיח שקיים איבר מסדר המתחלק ב p
כי אז x מסדר m ו $p|m$ ואז $x^{\frac{m}{p}}$ הוא איבר מסדר p.

הוכחה: באינדוקציה על מספר האיברים.
בסיס האינדוקציה – טענה ריקה (n=1)
שלב האינדוקציה:
מקרה א' – נניח ש G אבלית
ניקח $1\neq x_0\in G$ כלשהו מסדר m ונתבונן בתת החבורה שהוא יוצר $H=\langle x_0\rangle$ ונסמן $|H|=m$
אם $p|m$ סיימנו (מההערה לעיל).
אחרת – $p||G|=[G:H][H]$ כלומר $p||[G:H]$
כיוון ש G אבלית אז $H\lhd G$
ולכן $p||G/H|<|G|$
לפי הנחת האינדוקציה קיים איבר $y\in G/H$ מסדר p.
אם העתקת המנה היא $\phi:G\to G/H$ כך ש $\phi(g)=gH$
אז קיים $x\in G$ כך ש $\phi(x)=y$ הסדר של y מחלק את הסדר של x.
לפי הנחה הסדר של y הוא p ולכן הסדר של x מתחלק ב p.
סיימנו לפי ההערה.

הסבר קטן לריענון: לכל $\phi:G_1\to G_2$ הומומורפיזם של חבורות, הסדר של $\phi(x)$ מחלק את הסדר של x לכל $x\in G_1$, כי .

מקרה ב' – המקרה הכללי בו G לא בהכרח אבלית.
נשתמש במשוואת המחלקות:
$$|G|=|Z(G)|+\sum_{i>k}\frac{|G|}{|C_G(x_i)|}$$
אם $p||Z(G)|$ אז לפי המקרה הקודם יש איבר מסדר p ב $Z(G)$ ואז סיימנו.
אחרת:
$p||G|$ אבל $p\nmid|Z(G)|$ לכן $p\nmid\sum_{i>k}^{h}\frac{|G|}{|C_G(x_i)|}$
לכן קיים i>k כך ש $p\nmid\frac{|G|}{|C_G(x_i)|}$
כיוון ש $p||G|$ בהכרח $p||C_G(x_i)||G|$ (נובע מכך שבהנחת אי ההתחלקות – המנה באגף ימין שלמה, ולכן אי התחלקות, בהנתן התחלקות המונה, אפשרית רק אם גם המכנה מתחלק, אחרת היה אפשר עדיין לחלק ב p ולקבל משהו שלם)
הוא תת חבורה ממש של G (כי $x_i\notin Z(G)$) לפי הנחת האינדוקציה הוא לפיכך מכיל איבר מסדר p.
וסיימנו.

❑

<u>15.12.08 – שיעור 13 – שובו של הענר</u>
נזכיר שכאשר G פועלת על G/H נקבל פעולה <u>טרנזיטיבית</u> על קבוצה בגודל $|G/H|=n$
כל הפעולות הטרנזיטיביות של G על קבוצה בגודל n שקולות לפעולה כנ"ל.
בהנתן פעולה טרנזטיבית כלשהי על קבוצה X בגודל n, ניקח H מייצב נקודה ואז ראינו שיש התאמה חח"ע ועל בין X ו G/H

ששומרת על הפעולה, ולכן הפעולה על X שקולה לפעולה על המחלקות השמאליות של H.

<u>הלמה של ברנסייד</u>
מס' נקודות השבת של g על X = $fix(g)$
מס' המסלולים = N
אז
$$N=\frac{1}{|G|}\sum_{g\in G} fix(g)$$
מספר המסלולים = ממוצע מספר נקודות השבת
בפרט נובע: אם הפעולה טרנזיטיבית ו $1<|X|$ אז N=1 ונובע שיש $g\in G$ עם $fix(g)=0$
$fix(1)=|X|>1$

<u>משפט קושי</u>
תהי G חבורה סופית
p ראשוני, $p\|G|$ אז יש ב G איבר מסדר p

הוכחה 1 – מסתמכת על משוואת המחלקות:
$$|G|=Z(G)+\sum_i |G:C_G(x_i)|$$
נציגי מחלקות צמידות לא מרכזיות
$C_G(x)=\{g\in G: g\,x=x\,g\}$
זהו הרכז של X, ואז
$[G:C_G(x)]=|x^G|$
באגף ימין זו מחלקת הצמידות של x כלומר $\{x^g: g\in G\}$

הערה: באופן דומה G פועלת על תת חבורות על ידי הצמדה:
$(g,H)\to H^g=g\,H\,g^{-1}$

המסלול של H = כל החבורות הצמודות ל H
המיצב $\{g\in G: H^g=H\}$ בפעולה זו נקרא גם המשמר של H ומסומן $N_G(H)$ ואז $H\triangleleft N_G(H)$
וזו תת החבורה המקסימלית של G כך ש H נורמלית בתוכה.
נזכיר ש $|O(x)|=[G:G_x]$
מסקנה:
$$\left|\{H^g: g\in G\}\right|=[G:N_G(H)]$$
מקרה פרטי – $H\triangleleft G$ אז $N_G(H)=G$ כי $H^g=H$ תמיד.

נזכיר את שלבי ההוכחה למשפט קושי.
מקרה 1 – G אבלית, ואז עושים אינדוקציה על הגודל של G.
מקרה 2 – G לא אבלית, משתמשים במשוואת המחלקות.

<u>הוכחה 2</u>
נגדיר:
$$X=\{(g_1,\dots,g_p): g_i\in G, g_1\cdot\dots\cdot g_p=1\}$$
נשים לב שלולא התנאי השני, גודל הקבוצה היה $|G|^p$

טענה 1: $|X|=|G|^{p-1}$ כי ניתן לבחור את כל האיברים עד g_{p-1} בחופשיות, והאחרון מאולץ להיות ההופכי של המכפלה, כלומר יש p-1 דרגות חופש.
טענה 2: X סגורה להזזות ציקליות, לדוגמה
$(g_1,\dots,g_p)\in X \Rightarrow (g_2,\dots,g_p,g_1)\in X$
וכו'
מדוע? נבחר $1\le k\le p$ ואז $(g_1\cdot\ldots\cdot g_k)=(g_{k+1}\cdot\ldots\cdot g_p)^{-1}$ ולכן הם מתחלפים ועדיין מקבלים
$g_{k+1}\cdot\ldots\cdot g_p\cdot g_1\cdot\ldots\cdot g_k=1$
כל ההזזות הציקליות מתקבלות ע"י בחירת k כנ"ל ולכן האינווריאנטיות.

כעת תהי $\mathbb{Z}_p$ החבורה הציקלית בגודל זה, ניתן לה לפעול על X ע"י הזזות ציקליות:
$i(g_1,\dots,g_p)=(g_{i+1},\dots,g_{i+p})$
כמובן ההזזות הן מודולו p.

קל לראות שזו פעולה ולכן גדלי המסלולים מחלקים את $|\mathbb{Z}_p|=p$ ולכן הם 1 או p.
המסלול של וקטור ב X הוא בעל מסלול בגודל 1 אם"ם כל האיברים בו שווים, והאיבר לפיכך אינווריאנטי תחת הזזה.
$\vec{g}=(g_0,g_0,g_0,\dots,g_0)$

נניח ש X מתפרקת ל k מסלולים בגודל p ו l מסלולים בגודל 1
אז $|X|=k\,p+l$
הערה 1: $p\|X|$ כי $p|G$ ולפי טענה 1 קיבלנו $|X|=|G|^{p-1}$

הערה 2: $l=|X|-k\,p \Rightarrow p|l$ לפי הערה 1

כל מסלול בגודל 1 מתאים לאיבר ב G (כי הוא מסלול של וקטור יחיד בו כל הקואורדינטות שוות) המקיים $g^p=1$
$l=\left|\{g\in G: g^p=1\}\right|$
יש לפחות 1 כזה כי $1^p=1$ ולפי הערה 2 נקבל ש p מחלק את l, ולכן בהכרח $l\ge p$

<u>מסקנה</u>
יש לפחות p איברים $g\in G$ המקיימים $g^p=1$ ובפרט יש לפחות $p-1$ כנ"ל השונים מ 1.
לכן יש ב G לפחות $p-1$ איברים מסדר p ובפרט יש איבר כנ"ל.

הערה: אפשר לומר שמספר האיברים מסדר p ב G שקול ל -1 מודולו p.

<u>הגדרה</u>
p ראשוני
חבורה (סופית או אינסופית) נקראת **<u>חבורת p-</u>** אם לכל איבר בה סדר p^k עבור k כלשהו שתלוי אולי באיבר.

במובן מסויים חבורות p הן אבני בניין של תורת החבורות.
דוגמאות לחבורות סופיות כנ"ל:
1.
כמובן $\mathbb{Z}_p$
2.
$\mathbb{Z}_p\times\mathbb{Z}_p$
3.

$\mathbb{Z}_{p^n}$

<u>טענה:</u> חבורה סופית G היא חבורת-p אם"ם $|G|=p^n$ עבור n כלשהו.
בחלק מהספרים זו הגדרה חליפית, אבל אנחנו נעסוק גם בחבורות p אינסופיות ועל כן נישאר עם ההגדרה שלנו.

<u>הוכחה:</u> $\Rightarrow$
סדר איבר $x\in G$ מחלק את $|G|$ שהוא p^n ולכן הוא p^k ($0\le k\le n$) וזה נובע ממשפט לגרנז'.
$\Leftarrow$
אם $|G|$ לא חזקת p אז יש ראשוני $q\neq p$ אשר מקיים $q\|G|$.
ממשפט קושי נובע שיש $x\in G$ מסדר q (ששונה מ p^k לכל $k\neq 0$) בסתירה.

<u>משפט</u>:
תהי G חבורת-p סופית שהיא לא טריוויאלית.
אז $Z(G)\neq\{1\}$ כלומר המרכז של G לא טריוויאלי.
<u>הוכחה</u>:
על פי משוואת המחלקות.
$$|G|=Z(G)+\sum_i|G:C_G(x_i)|$$
כאשר i עובר על נציגי מחלקות צמידות לא מרכזיות.

$C_G(x_i)<G$ תת חבורה ממש, ולכן $1<[G:C_G(x_i)]\|G|$
מהטענה הקודמת $|G|=p^n$
ולכן
$[G:C_G(x_i)]=p^k$ (עבור $1\le k\le n$ כלשהו)

מסקנה:
$p|[G:C_G(x_i)]$ לכל i נציג מחלקת צמידות לא מרכזית כנ"ל.
מאחר שגם $p\|G|$ נובע ממשוואת המחלקות שגם $p\|Z(G)|$
ובפרט $Z(G)\neq\{1\}$
❑

הערה: יש חבורות p <u>אינסופיות</u> עם מרכז טריוויאלי

<u>טענה</u>: חבורת-p סופית היא פשוטה $\Leftrightarrow$ היא $\cong$ $\mathbb{Z}_p$

<u>הוכחה</u>:
כיוון 1 הוא די פשוט כי ראינו ש $\mathbb{Z}_p$ פשוטה והיא כמובן חבורת p סופית.

בכיוון השני:
תהי G חבורת p פשוטה סופית, נראה $G\cong\mathbb{Z}_p$
G לא טריוויאלית (נזכיר שהחבורה הטריוויאלית לא נחשבת פשוטה)
מהמשפט הקודם נקבל $Z(G)\neq\{1\}$
ברור ש $Z(G)\triangleleft G$
מפשטות G נובע $Z(G)=G$ ולכן G אבלית.
ממשפט קושי יש $x\in G$ מסדר p.
נתבונן בחבורה שיוצר x, דהיינו ב $\langle x\rangle$.

זו תהיה חבורה בגודל p, והיא נורמלית ב G כי G אבלית, אבל מפשטות G נובע שהיא כל החבורה.
ולכן $G\cong\mathbb{Z}_p$ (כי ראינו $\langle x\rangle\cong\mathbb{Z}_p$)

<u>משפטי סילו (יש שלושה)</u>

<u>משפט סילו I</u>
תהי G חבורה סופית, יהי p ראשוני, ותהי p^n המקסימלית כך ש $p^n\|G|$
אז יש ל G תת חבורה P בגודל p^n

הערות
1. P חבורת-p
2. אין ל G תתי חבורות גדולות יותר שהן חבורות p כי $p^{n+1}\nmid|G|$

נסמן $|G|=p^n\cdot m\quad p\nmid m$
<u>למה</u>
נניח $p\nmid m$ אז $\binom{p^n\cdot m}{p^n}$ לא מתחלק ב p.
<u>הוכחה</u>
$$\binom{p^n\cdot m}{p^n}=\frac{(p^n\cdot m)!}{p^n!\cdot(p^nm-p^n)!}=\frac{p^nm}{p^n}\cdot\frac{p^nm-1}{p^n-1}\cdot\ldots\cdot\frac{p^nm-i}{p^n-i}\cdot\ldots\cdot\frac{p^nm-p^n+1}{1}$$
נראה שחזקת p המירבית המחלקת את p^nm-i היא חזקת p המרבית המחלקת את p^n-i

$p^k|p^nm-i$ נשים לב ש $1\le i<p^n$ ולכן $p^n\nmid p^nm-i$ לכן $k<n$
$p^k|p^nm$ ולכן $p^k|i$ מכאן $p^k|p^n-i$
הראינו:
חזקת p מחלקת את המונה אז היא מחלקת את המכנה. גם ההיפך נכון, אבל לא נשתמש בזה ולכן זה פחות חשוב כרגע.
כל חזקת p במונים של המכפלה תצטמצם ע"י המכנים ונובע $p\nmid\binom{p^nm}{p^n}$

<u>שיעור 14 – 17.12.08</u>
נסמן:
$Syl_p(G)=\{P\le G:|P|=p^n\}$
$|G|=p^nm\quad p\nmid m$
P כנ"ל נקראות חבורות p-סילו של G ו $Syl_p(G)$ אוסף החבורות כנ"ל.

משפט סילו I :
$Syl_p(G)\neq\emptyset$
משפט סילו II :
$|Syl_p(G)|\equiv1\ mod\ p$
משפט סילו III:
כל שתי חבורות p-סילו ב G הן צמודות ב G, כלומר אם יש $P,Q\in Syl_p(G)$ אז יש $g\in G$ כך ש
$Q=gPg^{-1}$
<u>דוגמאות פשוטות לחבורות p-סילו</u>

1.
$p\nmid|G|$ אזי חבורת היחידה היא חבורת p-סילו (יחידה)
2.
$p^n=|G|$ אזי G חבורת p-סילו (יחידה)
3.
S_3 חבורת 3-סילו היא $\langle(123)\rangle$ בגודל 3, יחידה.
חבורת 2-סילו היא $\langle(12)\rangle$ אבל היא לא יחידה כי אפשר לקחת גם את $\langle(23)\rangle$

<u>הוכחת משפט סילו I</u>
נגדיר $X=\{B\subseteq G:|B|=p^n\}$ כאשר $|G|=p^n m$ אבל $p\nmid m$ כלומר n היא החזקה המקסימלית של p שנכנסת בגודל של G.

ברור ש $|X|=\binom{p^n m}{p^n}$ אבל הוכחנו קודם לכן שזה לא מתחלק ב p ועל כן $p\nmid|X|$
ניתן ל G לפעול על X ע"י הזזה משמאל, זאת אומרת:
$$(g,B)\to gB=\{gb:b\in B\}\quad\text{and still}\quad|gB|=|B|=p^n$$
מאחר שכאמור p אינו מחלק את הגודל של X יש מסלול $Y\subset X$ של G בפעולה זו כך ש $p\nmid|Y|$
מדוע? אם הסדר של הקבוצה כולה אינו מתחלק ב p אז יש מסלול שאינו מתחלק ב p, אחרת כולם היו מתחלקים ב p והגודל של X הוא סכום גדלי המסלולים ומכאן היה נובע $p\|X|$ בסתירה.

נניח $Y=O(B)$ עבור $B\in X$ (נזכיר $|B|=p^n$, $B\subseteq G$)

תהי $P=G_B$ המייצב של B.

אז $P=\{g\in G:gB=B\}$ תת חבורה של G כמובן.

אינדקס המייצב = גודל המסלול
ולכן $[G:P]=[G:G_B]=|O(B)|=|Y|$
ומצאנו תת חבורה שהאינדקס שלה אינו מתחלק ב p.
$$[G:P]=\frac{|G|}{|P|}=\frac{p^n m}{|P|}\quad\text{ולכן}\quad p\nmid[G:P]$$
מכאן ש $p^n\|P|$ אחרת היה נשאר במונה p^k כלשהו והביטוי כולו היה מתחלק ב p.

בפרט $|P|\geq p^n$
אם נוכיח אי שוויון חלש מהכיוון השני – נסיים.

לשם כך נקבע $b\in B$ כלשהו ונתבונן ב $P_b=\{gb;g\in P\}$ נקבל $P_b\subseteq B$ ולכן $|P_b|\leq|B|=p^n$
($gb\in B$ כי $gB=B$ כי P המייצב של B)
אבל $|P_b|=|P|$ כי זו הזזה של איברי החבורה.

מכאן שמצאנו תת חבורה מסדר p^n כנדרש.
❑

להוכחת משפטי סילו II ו III נזדקק ללמה הבאה:

<u>למה 1</u>:
תהי G חבורה סופית. P,Q תתי חבורות של G שהן חבורות p (לא בהכרח p סילו).
נניח $Q\not\subseteq P$ ו – Q משמרת את P : $xPx^{-1}=P$ לכל $x\in Q$
(N_G המשמר, המכונה גם מנרמל, אז הדרישה לעיל שקולה ל $Q\subseteq N_G(P)$)
<u>אז</u> PQ היא חבורת p ב G שמכילה ממש את P.
<u>הוכחה:מנרמל</u>
$xP=Px$ לכל $x\in Q$ (כי Q משמרת את P) ובפרט $QP=PQ$ ומכאן PQ תת חבורה (ראינו בעבר).

כפי שראינו בתרגיל $|PQ|=\frac{|P||Q|}{|P\cap Q|}$
ואז אם נסמן:
$|P|=p^k$
$|Q|=p^l$
$|P\cap Q|=p^m$
ואז $|PQ|=p^{k+l-m}$ חזקה של p.
ולכן PQ היא אכן חבורת p.
נתון ש $Q\not\subseteq P$ ובפרט $PQ\not\subseteq P$
בנוסף $P\subseteq PQ$ (כדי להשתכנע נתבונן בזוגות במכפלה כאשר בוחרים $1\in Q$)
לכן PQ מכילה את P אך לא מוכלת בה, מכאן שמכילה ממש את P כנדרש.
❑

<u>דוגמאות נוספות</u>
.1
$G=\mathbb{Z}_{35}$
p-ים רלוונטיים הם 5 ו 7.
$5|G$ חזקה מקסימלית ולכן צריכה להיות חב' 5-סילו בגודל 5:
$P_5=\{0,7,14,21,28\}$ וגם $P_7=\{0,5,10,15,20,30\}$
.2
תרגיל – $GL(z,p)=G$ מטריצות הפיכות מעל $\mathbb{Z}_p$
למצוא G חבורת p-סילו

<u>שיעור 15</u>
<u>למה 2</u>
תהי $\emptyset\neq T\subseteq Syl_P(G)$ קבוצה חלקית אינווריאנטית תחת פעולת ההצמדה של G.
כלומר -

$$P\in T \;\Rightarrow\; \forall x\in G:{}^xP\in T$$

(נסמן מעתה ${}^xP=xPx^{-1}$)

<u>אז</u> $|T|\equiv 1 \bmod p$

<u>הוכחה</u>
ניקח $Q\in T$ וניתן לה לפעול על T ע"י הצמדה.
T אינווריאנטית תחת G ולכן T אינווריאנטית תחת Q (לפעולת ההצמדה בשני המקרים).

נחלק את T למסלולים תחת פעולת Q.

$\{Q\}$ מסלול בגודל 1, נראה שהוא יחיד מגודל זה.
נניח בשלילה שגם $\{P\}$ מסלול בגודל 1 כאשר $P\neq Q$.
אז $P=P^x$ לכל $x\in Q$ ולפיכך Q משמרת את P.
$Q\not\subseteq P$ כי $P\neq Q$ והגדלים שלהן שווים (שתיהן חבורות p-סילו).
לכן מתקיימים בדיוק התנאים של <u>למה 1</u> ולכן נקבל ש $PQ\leq G$ היא חבורת p שמכילה ממש את P, בסתירה לכך ש P חבורת p-סילו ולכן אין חבורות-p גדולות ממנה ב G.
מכאן ש $\{Q\}$ אכן מסלול יחיד בגודל 1.

שאר המסלולים גדולים מ 1 וגדלם מחלק את $|Q|$ (גודל החבורה הפועלת) וזוהי חזקה של p, ולכן סכימת המסלולים תיתן שארית 1 מודולו p וזה מה שרצינו להראות. ❑

<u>הוכחת משפט סילו II</u>
ניקח $T=Syl_p(G)$ ברור ש T אינווריאנטית תחת הצמדה באיברי G וכן T לא ריקה (לפי משפט סילו 1).
עפ"י למה 2 נובע $|T|\equiv 1 \bmod p$ כלומר $|Syl_p(G)|\equiv 1 \bmod p$
❑

<u>הוכחת משפט סילו III</u>
כל שתי חבורות p-סילו הן צמודות ב G.

ניקח $P,Q\in Syl_p(G)$ ומה שאנחנו רוצים להראות הוא שפעולת ההצמדה של G על $Syl_p(G)$ היא טרנזיטיבית (=יש מסלול יחיד).

נניח בשלילה שאין מסלול יחיד, כלומר נוכל למצוא שני מסלולים שונים שיסומנו להלן T_1, T_2
אלו קבוצות לא ריקות ואינווריאנטיות תחת הצמדה (כי מסלול הוא מחלקת צמידות) ולכן מלמה 2 נקבל:
$$|T_1|\equiv 1 \bmod p$$
$$|T_2|\equiv 1 \bmod p$$
$$|T_1\cup T_2|\equiv 1 \bmod p$$
כי גם האיחוד הוא קבוצה אינווריאנטית ולא ריקה.
אבל מאידך T_1 ו T_2 מסלולים שונים ולכן החיתוך שלהם ריק וגודל האיחוד הוא סכום הגדלים.
מכאן נובע כי:
$$|T_1\cup T_2|=2 \bmod p$$
בסתירה...
ענר: הוכחה יפה, נכון?

הערות:
.1
משפט 2 גורר את משפט 1, אבל מצד שני מסתמך עליו ולכן אין פה יתירות.
.2
נובע ממשפט 3 ש $|Syl_p(G)|\|G|$ כי תחת פעולת ההצמדה קבוצת חבורות p-סילו היא מסלול.
ננסח לכן את **<u>משפט סילו II מחוזק</u>**
מספר חבורות p-סילו ב G שקול ל 1 מודולו p ומחלק את $|G|$

<u>טענה</u>
ל-G חבורת p-סילו יחידה ⇔ ל-G חבורת p-סילו נורמלית
<u>הוכחה:</u>

$\Leftarrow$

מיידי, כי אם P חבורת p-סילו יחידה אז בהכרח לכל x מתקיים $^{x}P=P$ (כי גם זו חבורת p-סילו) ולכן $P \lhd G$

$\Rightarrow$

נובע ממשפט סילו 3, כי אם P נורמלית, לפי סילו 3 כל השאר מתקבלות ממנה על ידי הצמדה, אבל היא אינווריאנטית תחת הצמדה ולכן יחידה.

נסמן: n_p = מספר חבורות p סילו של G
אז $n_p \| |G|$
וגם $n_p \equiv 1 \, mod \, p$

<u>שעשועים מספריים</u>
נניח $|G|=35$
<u>טענה</u>: חבורות 5-סילו ו 7-סילו הן נורמליות.
מספיק להראות $n_7=n_5=1$ ולפי הטענה האחרונה זה שקול לנורמליות.

<u>הוכחה</u>
$$n_5 | 35 \quad \wedge \quad n_5 \equiv 1 \, mod \, 5$$

המספרים שהם 1 מודולו 5 הם:
1,6,11,16,21,26,31
ומתוכם מחלק את 35 רק 1, ולכן $n_5=1$

בנוסף:
$$n_7 | 35 \quad \wedge \quad n_7 \equiv 1 \, mod \, 7$$
המספרים שהם 1 מודולו 7 הם:
...,1,8,15
ומתוכם רק 1 מחלק את 35 ולכן גם $n_7=1$
ומכאן הטענה.
❑

הערה: ניתן להראות שיש חבורה יחידה מסדר 35 עד כדי איזומורפיזם והיא $\mathbb{Z}_{35}$
הוכחה:
הרעיון הוא שאנחנו יודעים שהחבורות p-סילו שמצאנו לעיל הן איזומורפיות ל $\mathbb{Z}_5, \mathbb{Z}_7$ כי הן מגודל ראשוני, והחיתוך שלהן טריוויאלי כי גודל החיתוך כתת חבורה של שניהם צריך לחלק את גדלי שתי החבורות, ואלו ראשוניים שונים.
מכאן נובע שהמכפלה הישרה של שתי החבורות p-סילו היא כל החבורה.
ראינו בתרגול שעבור שתי חבורות נורמליות הנחתכות טריוויאלית מתקיים $NM \cong N \times M$
$$|NM| = \frac{|N||M|}{|N \cap M|}$$
ולכן חבורת המכפלה של חבורות הסילו היא תת חבורה של G בגודל 35, ולכן היא שווה לה.

<u>טענה</u>
חבורה בגודל 30 אינה פשוטה.
<u>הוכחה</u>
תהי G חבורה בגודל 30 ונניח בשלילה כי היא פשוטה.
נתבונן ב n_5 וב n_3

$n_5>1$ אחרת חבורת 5-סילו היתה נורמלית בסתירה לפשטות.
$n_5|30 \quad \wedge \quad n_5\equiv 1 \, mod \, 5$
האפשרויות הן 1,6,11,16,21,26
אבל רק 1 ו 6 מחלקים את 30 וששללנו את 1 לכן $n_5=6$
$n_3>1$ כמקודם
ושוב נדרוש:
$n_3|30 \quad \wedge \quad n_3\equiv 1 \, mod \, 3$
והברירות הן: 4,7,10,13,... מתוכם רק 10 מחלק את 30 ולכן $n_3=10$
נראה שכתוצאה כך יש "יותר מדי איברים ב G".
יש 6 חבורות 5-סילו, נסמנן $p_1, \dots, p_6$
גדלן הוא 5 וחיתוך כל שתיים הוא טריוויאלי, כי כל אחת מהן היא ציקלית בהיותה חבורה מסדר ראשוני.
זה אומר שהקבוצות $p_i \backslash \{1\}$ זרות.
ולכן $\coprod_{i=1}^{6}(p_i\backslash\{1\})=6\cdot 4=24$
קיבלנו כך 24 איברים שונים ב G מסדר 5.
מתוך שיקול דומה לגבי החבורות 3-סילו שמצאנו נקבל 20 איברים מסדר 3 ב G, כלומר יש 44 איברים שונים ב G ולכן הסתירה המבוקשת (כי $|G|=30$).
לכן החבורה היא בהכרח פשוטה.

<u>הערה</u>:
בעצם הוכחנו שבחבורה בגודל 30, או שחבורת 5-סילו נורמלית או שחבורת 3-סילו היא נורמלית.

<u>טענה 3</u>
אין חבורה פשוטה בגודל 36
הוכחה: תרגיל
רמז: ניקח P חבורת 3-סילו של G, נקבל $|P|=3^2=9$ נתבונן באוסף המחלקות השמאליות של P, שיסומן G/P.
כמובן $|G/P|=4$
G פועלת על G/P על ידי כפל משמאל, כלומר $g\cdot(aP)=(ga)P$ וזה מגדיר הומומורפיזם $\phi: G\to S_4$
כדאי להשתמש ב ϕ כדי למצוא תת חבורה נורמלית ב G שאינה 1 ואינה כל החבורה, ע"י גרעין הפעולה.
נקבל שהגרעין נורמלי ב G ושונה מחבורת היחידה.
מדוע? ההעתקה היא מקבוצה בגודל 36 לקבוצה בגודל 24, לכן היא לא חח"ע והגרעין לא טריוויאלי.
הגרעין גם מוכל ב P (כי הוא ה Core ולכן עפ"י הגדרה הוא חיתוך ההצמדות ב P) שמוכלת ממש ב G.
מכאן שהגרעין הוא חבורה נורמלית חלקית שאיננה $\{1\}$.

<u>שיעור 16</u>

<u>משפט</u>
תהי G חבורה סופית, P ראשוני ונניח ש $p^k||G|$ אז יש ל G תת חבורה בגודל p^k
<u>הערה</u>: זה מכליל את משפט סילו I (שמדבר על k מקסימלי כנ"ל) וגם את משפט קושי (שמבטיח עבור k=1)

<u>הוכחה</u>:
נרשום $|G|=p^n\cdot m$ כאשר $p\nmid m$ אז $k\le n$
נגדיר:
$X=\{B\subseteq G:|B|=p^k\}$

אז $|X|=\binom{p^n m}{p^k}$

<u>טענה</u>

$p^{n-k} \nmid \binom{p^n m}{p^k}$

<u>הוכחה</u>

דומה למקרה שהראינו כאשר $n=k$:

$$\binom{p^n m}{p^k}=\frac{p^n m}{p^k}\cdot\frac{p^n m-1}{p^k-1}\cdot\ldots$$

בביטויים באגף ימין, החל מהביטוי השני – כולם לא מתחלקים בחזקות של p אבל הביטוי הראשון מתחלק בדיוק ב p^{n-k}
(כדאי להסתכל שוב בהוכחה למשפט סילו, שם זה יותר מפורט)

<u>מסקנה</u>:

$p^{n-k+1} \nmid |X|$

ניתן ל G לפעול על X ע"י $g\,,\,B\to g\,B$

נחלק את X למסלולים, יש מסלול Y שגודלו לא מתחלק ב p^{n-k+1}

תהי $B\in Y$ ותהי $Q=G_B=\{g\in G: g\,B=b\}$

<u>טענה</u>

$|Q|=p^k$ ו Q תת חבורה, אם נוכיח זאת – נקבל את תת החבורה המבוקשת.

<u>הוכחה</u>

$$|Y|=|O(B)|=[G:G_B]=[G:Q]$$

$$p^{n-k+1} \nmid |Y|=\frac{|G|}{|Q|}=\frac{p^n m}{|Q|}$$

$$\downarrow$$

(1) $p^k \| |Q|$

מצד שני ניקח $b\in B$ אז $Qb\subseteq B$ כי $G_B=Q$ המייצב.

(2) $|Q|=|Qb|\le|B|=p^k$

מצירוף הטענות 1 ו – 2 נקבל כי $|Q|=p^k$ כנדרש.

❑

<u>משפט</u>

כל תת חבורה של G שהיא חבורת p מוכלת בחבורת p-סילו כלשהי של G.

לשם המחשה – נניח חבורה בגודל 36 כמקודם, אזי חבורת p-סילו שלה היא מגודל 3^2 , המשפט אומר שכל חבורה מסדר 3 ניתן להרחיב לחבורת p-סילו כנ"ל.

בסימונים:

$$|P|=p^n \quad Q\le P \;:\; \exists P\in Syl_p(G) \quad \Rightarrow \quad |Q|=p^k \quad Q\le G$$

<u>הוכחה</u>

ניתן ל Q הנ"ל לפעול על $Syl_p(G)$ ע"י הצמדה.
המסלולים הם בגודל 1 או בגודל שמתחלק ב p כי גודל מסלול מחלק את $|Q|=p^k$
מכאן נובע שיש מסלול בגודל 1, אחרת גדלי כל המסלולים מתחלקים ב p ולכן $p\left||Syl_p(G)|\right.$ (סתירה למשפט סילו II שמכתיב שארית של 1 בחלוקה ב p)

יהי $\{P\}$ מסלול כנ"ל, אז P חבורת p-סילו ו $^xP=P$ לכל $x\in Q$
לכן Q משמרת את P ו PQ היא חבורת p ב-G (מלמה שראינו)

לא יתכן $P<PQ$ כי P חבורת p-סילו וע"פ הגדרה אין חבורות p גדולות ממנה ב G.
לכן $PQ=P \Leftarrow Q\subseteq P$ (אחרת – לפי למה 2 שהוזכרה נקבל $P\subset PQ$, הכלה ממש)

<u>שיעור 17</u>
<u>עוד על סילו</u>
דוגמה:
ניקח את החבורה $GL_d[p]$ (מטריצות $d\times d$ מעל שדה עם p איברים)
נמצא חבורת p-סילו בחבורה זו:
P – אוסף המטריצות המשולשיות עליונות, כך שעל האלכסון יש 1 ומעליו כל הקומבינציות.

<u>חבורות p</u>

<u>טענה 1</u>: תהי P חבורה מסדר p^n אז לכל $0\le k\le n$ יש ל P תת חבורה מסדר p^k .
<u>הוכחה</u>: זה מקרה פרטי של סוף השיעור הקודם.

<u>טענה 2</u>: כל חבורה מסדר p^2 היא אבלית.
<u>הוכחה</u>:
תהי P חבורה מסדר p^2 , יהי $Z(P)$ המרכז שלה
ראינו שהמרכז לא טריוויאלי, ולכן המרכז הוא p או p^2 .
אם p^2 אז P אכן אבלית כי המרכז הוא כל החבורה.

נתבונן ב $P/Z(P)$ היא חבורת מנה, שגודלה P, ולכן איזומורפית ל $\mathbb{Z}_p$ ובפרט חבורת המנה הזו היא חבורה ציקלית.
השלמת ההוכחה ע"י הלמה הבאה:

<u>למה</u>
תהי G חבורה כך ש $G/Z(G)$ ציקלית, אז G אבלית. (ולכן $G/Z(G)=\{1\}$)
<u>הוכחה</u>
נסמן $Z=Z(G)$ ויהי gZ יוצר של החבורה הציקלית G/Z.

מכיוון שכל מחלקה hZ (כך ש $h\in G$) היא חזקה של היוצר אזי $hZ=(gZ)^k=g^kZ$
מכאן: כל $h\in G$ ניתן לכתיבה כ- g^kz כאשר $z\in Z$
ניקח שני איברים של G, הם ניתנים לכתיבה כחזקה של g כפול איבר מהמרכז, ולכן הם מתחלפים באופן טריוויאלי.

וזה משלים את הוכחת טענה 2.
❑

<u>הערה</u> חבורות בגודל p^3 אינן בהכרח אבליות.

למשל – מטריצות בשדה מגודל p שצורתן $\begin{pmatrix} 1 & a & c \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix}$
לא קשה למצוא שתיים שאינן מתחלפות והן מצורה זו.

<u>טענה 3</u>
G חבורת-p סופית
$H<G$ (תת חבורה ממש)
אז
$H<N_G(H)$ (כלומר המשמר של H מכיל ממש את H)
תזכורת:
$N_G(H)=\{g\in G: g\,H\,g^{-1}=H\}$

<u>הוכחה</u>
תהי
$X=\{g\,H\,g^{-1}: g\in G\}$ = כל צמודי H
G פועלת על X ע"י הצמדה וכך גם H.
אם $H\lhd G$ אז $G=N_G(H)$ ולפי ההנחה G מכילה ממש ומתקיימת הטענה.

לפיכך נניח בשלילה כי H איננה נורמלית ב G.
אז $N_G(H)<G$ (מוכל ממש)
נזכור כי ראינו בשבוע שעבר כי:
$|X|=[G: N_G(H)]>1$

G היא חבורת p ולכן $[G: N_G(H)]$ חזקת p גדולה מ 1 ולכן גודל זה מתחלק ב p.
ולפיכך $p\|X|$
נחלק את X למסלולים על פי פעולת H על X.
אז גדלי המסלולים הם 1 או כפולות של p (כי H חבורת p).
יש מסלול בגודל 1 – זהו פשוט H.

אם היה מסלול יחיד בגודל 1 היה נובע $|X|=k\,p+1$ בסתירה לכך ש p מחלק את $|X|$.
מכאן שיש עוד מסלול בגודל 1, כלומר $H\neq\{g\,H\,g^{-1}\}$
אז
$\forall\, h\in H \quad h\,g\,H\,g^{-1}h^{-1}=g\,H\,g^{-1}$
כי תחת פעולת ההצמדה – איבר במסלול בגודל 1 יעבור רק לעצמו.

$\forall\, h\in H \quad g^{-1}h\,g\,H\,g^{-1}h^{-1}g=H$
ולכן:
$g^{-1}H\,g\subseteq N_G(H)$
ראינו
$H\neq g\,H\,g^{-1} \;\Rightarrow\; g^{-1}H\,g\neq H$
אבל לשתי החבורות האחרונות אותו גודל, ולכן קיים $t\in g^{-1}H\,g\subseteq N_G(H)$ כך ש $t\notin H$
ואז $t\in N_G(H)\setminus H$ ולכן H מוכל ממש $N_G(H)$
❑

<u>טענה 4</u>
תהי G חבורת p סופית ותהי H תת חבורה מקסימלית של G.
(תת חבורה מקסימלית היא תת חבורה ממש שאינה מוכלת ממש באף תת חבורה ממש אחרת)
אז $H \lhd G$ וגם $[G:H]=p$

<u>הערות</u>
.1
$|G|=p^n \Rightarrow |H|=p^{n-1}$
לפי הטענה
.2
קיום תת חבורה H מסדר p^{n-1} כבר ידוע לנו, וקל לראות ש H כנ"ל היא מקסימלית (ביחס להכלה). החידוש הוא ש**<u>כל</u>** תת-חבורה מקסימלית היא בגודל p^{n-1} ונורמלית.

<u>הוכחת טענה 4</u>
נשתמש בטענה 3:
$H<G \Rightarrow H<N_G(H)$
ממקסימליות של H נובע ש $N_G(H)=G$ ולכן $H \lhd G$ (כי המשמר הוא הכל)

נותר להראות ש $[G:H]=p$
נתבונן ב G/H , זו חבורת מנה כי הראינו ש H נורמלית.
זוהי חבורת p, אם גודלה גדול מ p אז יש בה חבורה K כך ש:
$H/H<K/H<G/H$ (הכלות ממש)

נעיר כי כל תת חבורה של חבורת המנה היא מהצורה K/H כך ש H<K<G

ננסח משפט שדילגנו עליו במועד מוקדם יותר:
<u>משפט ההתאמה</u>
אם $H \lhd G$ אז יש התאמה חח"ע ועל בין חבורות חלקיות של חבורת המנה G/H ובין חבורות חלקיות של G שמכילות את H.
ההתאמה ניתנת ע"י:
$H \le K \le G \rightarrow K/H \le G/H$
הוכחה: תרגיל.

בחזרה להוכחה:
מסקנה: אם $p<|G/H|$ אז יש חבורה חלקית K כך ש H<K<G בסתירה למקסימליות של H.
לכן $|G/H|=p \Rightarrow [G:H]=p$
וסיימנו.
❑

<u>סדרות נורמליות וסדרות הרכב</u>

<u>הגדרה:</u>
תהי G חבורה..

סדרה נורמלית ב G היא סדרה מהצורה $1=G_n \triangleleft ... \triangleleft G_2 \triangleleft G_1 \triangleleft G_0=G$

כאשר כל G_i היא תת חבורה (לאו דווקא נורמלית) של G, אשר היא נורמלית ב G_{i-1}
אורך סדרה כנ"ל מוגדר כמספר ההכלות בדרך – כלומר n.
מותרות חזרות (יתכן $G_i=G_{i-1}$).

הגורמים של הסדרה כנ"ל יוגדרו כחבורות המנה G_i/G_{i+1} כאשר $0\le i\le n-1$

שתי סדרות נורמליות תקראנה **שקולות** אם יש להן אותם גורמים עד כדי סדר ואיזומורפיזם.

בנוסף אם $\{H_i\}_{i=0}^m$ היא סדרה נורמלית של G, נאמר שהיא עידון של $\{G_i\}_{i=0}^m$ אם כל G_j מופיע בקבוצה $\{H_i\}_{i=0}^m$, ז"א H_i מתקבלת מ G_j על ידי (אולי) תוספת חבורות חלקיות באמצע.

דוגמאות:
.1
בכל חבורה G ניתן לבנות סדרה נורמלית באורך 1: $\{1\}=G_1 \triangleleft G_0=G$

.2
$G=\mathbb{Z}_{30}=\langle x\rangle=\{x^k : 0\le k<30\}$
נוכל לבנות באופן הבא:
$G=G_0=\langle x\rangle \triangleright \langle x^2\rangle \triangleright \langle x^6\rangle \triangleright \langle x^{30}\rangle=1$

מי יהיו גורמי הסדרה?
$\langle x\rangle/\langle x^2\rangle \cong \mathbb{Z}_2$
$\langle x^2\rangle/\langle x^6\rangle \cong \mathbb{Z}_3$
$\langle x^6\rangle/\langle x^{30}\rangle \cong \mathbb{Z}_5$
סדרה אחרת:

$$G=G_0=\langle x\rangle \triangleright \langle x^3\rangle \triangleright \langle x^{15}\rangle \triangleright \{1\}$$

כיוון שהגורמים אותם גורמים – שתי הסדרות שהצגנו שקולות.

<u>שיעור 18</u>
נשים לב שהגורמים של הסדרה הנורמלית שהוצגה לעיל הם איזומורפיים ל $\mathbb{Z}_p$ כאשר p גורמים של $|G|$.
נכליל זאת:
ניקח $G=\mathbb{Z}_m=\langle x\rangle$
$m=p_i\cdot ...\cdot p_k$ כאשר p_i ראשוניים (לאו דווקא שונים)
אז ניתן לבנות סדרה נורמלית:
$$G=G_0=\langle x\rangle \triangleright \langle x^{p_1}\rangle \triangleright \langle x^{p_1 p_2}\rangle \triangleright ... \triangleright \langle x^{p_1 p_2 \cdot ... \cdot p_k}\rangle=\{1\}$$
$$\tilde{\mathbb{Z}}_{p_1} \quad \tilde{\mathbb{Z}}_{p_2} \quad \tilde{\mathbb{Z}}_{p_3} \quad \tilde{\mathbb{Z}}_{p_4}$$
נראה בהמשך שבכל סדרת הרכב (מושג שיוגדר בהמשך) ל G יופיעו גורמים אלה.

דוגמה נוספת:
G חבורת-p בגודל p^n אז יש ל-G סדרה נורמלית:

$$G=G_0\triangleright G_1\triangleright\ldots\triangleright G_n=\{1\}$$

כאשר $\mathbb{Z}_p\cong G_i/G_{i+1}$

בניה: ניקח G_1 תת חבורה מקסימלית של G ואז הוכחנו שמתקיים $G/G_1\cong\mathbb{Z}_p$ נמשיך באופן אינדוקטיבי.

<u>טענה:</u> אם $G=G_0\triangleright G_1\triangleright\ldots\triangleright G_n=\{1\}$ סדרה נורמלית ב G אז:

$$|G|=\prod_{i=0}^{n-1}|G_i/G_{i+1}|$$

<u>הוכחה:</u> באינדוקציה על $n\geq 1$

$n=1$ מיידי בשרשרת $G\triangleright\{1\}$

מעבר:

$G_1\triangleright\ldots\triangleright G_n=\{1\}$ באורך $n-1$

מהנחת האינדוקציה $|G_1|=\prod_{i=1}^{n-1}|G_i/G_{i+1}|$ וברור ש $|G|=|G/G_1|\cdot|G_1|$ ונציב את הגודל של G_1 בשוויון האחרון ונקבל את הטענה.

<u>הגדרה</u>

סדרת הרכב היא סדרה נורמלית בחבורה G כך ש- G_{i+1} תת חבורה נורמלית מקסימלית של G_i לכל i.

תנאי שקול – הגורמים כולם פשוטים.

<u>הוכחת השקילות</u>: ממשפט ההתאמה $G\triangleright N$ נורמלית מקסימלית $\Leftrightarrow$ אין חבורה נורמלית $N\triangleleft K\triangleleft G$ $\Leftrightarrow$ G/N פשוטה.

מדוע? נסתכל על חבורות המנה והנורמלית לעיל שקולה ל $\{1\}\triangleleft K/N\triangleleft G/N$.

<u>הערה</u>

בסדרת הרכב אין חזרות, אחרת אחד הגורמים היה חבורת היחידה שאינה פשוטה (זו בעצם הגדרה).
הדוגמאות שנתנו לסדרות נורמליות שניתנו לעיל היו סדרות הרכב.

<u>שאלות</u>

1. האם לכל חבורה יש סדרת הרכב?
2. האם היא יחידה?

<u>תשובות</u>

1. כן אם G סופית, לא תמיד – אם G אינסופית
2. לא, אך כן עד כדי שקילות של סדרות

חשיבות: להתאים לחבורה סופית כללית סדרת חבורות סופיות פשוטות שהן הגורמים של סדרת הרכב שלה, זה מקביל לפירוק לראשוניים.

<u>משפט</u>: לכל חבורה סופית G יש חבורת הרכב.

<u>הוכחה</u>: נגדיר $G_0=G$ ואילו G_1 תהיה תת חבורה נורמלית מקסימלי ב G_0 שקיומה מובטח מסופיות G.

אם $G_1=\{1\}$ סיימנו.

אחרת – ניקח G_2 נורמלית מקסימלית ב G_1 וכן הלאה, התהליך סופי כי G סופית.

<u>רעיון הוכחה שונה</u>: מכל הסדרות הנורמליות של G ללא חזרות, ניקח אחת עם אורך מקסימלי, נקבל G_{i+1} נורמלית מקסימלית ב G_i - אחרת ניתן לעדן ולמצוא $G_i \rhd K \rhd G_{i+1}$ ולהאריך את הסדרה.

<u>דוגמה</u>
$\mathbb{Z}$ חבורה ללא סדרת הרכב.
הוכחה: נניח בשלילה שקיימת סדרת הרכב סופית כך ש
$\mathbb{Z} = G_0 \rhd G_1 \rhd \ldots \rhd G_n = \{0\}$

סדרת הרכב ל $\mathbb{Z}$.

אזי מהטענה שהראינו קודם $\infty = |\mathbb{Z}| = \prod_{i=0}^{n-1} |G_i / G i+1|$

ולכן יש i כך ש G_i / G_{i+1} אינסופית., אבל היא גם פשוטה וגם אבלית (אפילו ציקלית).
<u>למה מיידית</u> – חבורה פשוטה אבלית היא סופית ולכן $\mathbb{Z}_p$, וזו סתירה כי נובע G_i / G_{i+1} סופית.

<u>שיעור 19</u>
נראה כעת **<u>יחידות של סדרת הרכב עד כדי סדר הגורמים ואיזומורפיזם</u>**.
(<u>משפט ז'ורדן-הלדר, 1868</u>)

<u>למה של זסנהאוס (?193)</u>
תהי G חבורה
$A, B, A^*, B^* \leq G$

נניח:
$B \lhd A$

$D \lhd C$

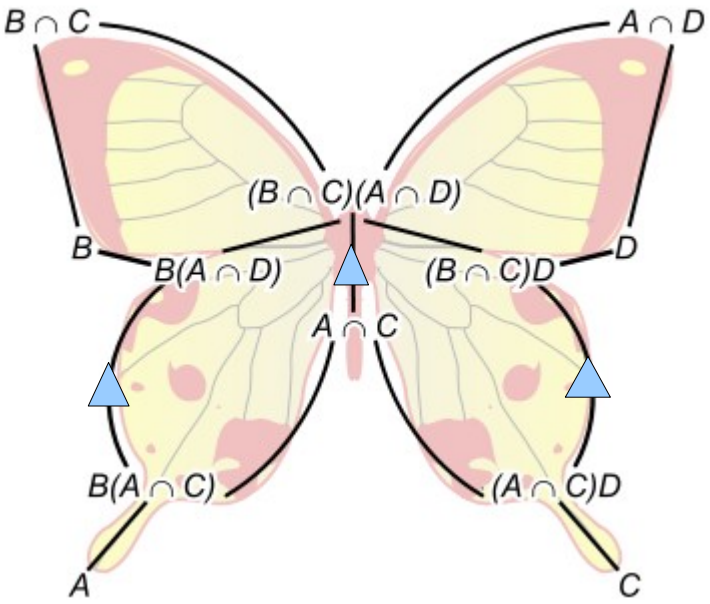
אז:
1.
$B(A \cap D) \lhd B(A \cap C)$

$D(B \cap C) \lhd D(A \cap C)$

2.
$$\frac{B(A \cap C)}{B(A \cap D)} \cong \frac{D(A \cap C)}{D(B \cap C)}$$

<u>הוכחה:</u> בתרגיל הפרונטלי.

++++
מתוך התרגיל:



(מתוך הערך בויקיפדיה באנגלית)
המשולשים הכחולים מסמנים נורמליות.
את ההוכחה המלאה אפשר למצוא שם, זה לא יהיה במבחן וזה טכני כמו המוות.
++++

<u>משפט העידון של שרייר (1928)</u>
לכל שתי סדרות נורמליות יש עידונים שקולים.
כלומר:
אם $\{B_i\}_{i=0}^{m}$ $\{A_i\}_{i=0}^{n}$ סדרות נורמליות של G אז יש עידון $\{C_i\}_{i=0}^{r}$ ל $\{A_i\}_{i=0}^{n}$
ועידון $\{D_i\}_{i=0}^{w}$ של $\{B_i\}_{i=0}^{m}$ כך שהסדרות הנורמליות $\{C_i\}_{i=0}^{r}$ ו $\{D_i\}_{i=0}^{w}$ שקולות (בפרט r=w).

<u>הוכחה</u>
נעדן את $\{A_i\}$ ע"י הוספת $A_{i+1}(A_i\cap B_j)$ עבור $j=0...m$ בין A_i ל A_{i+1}
נשים לב שזה בסדר כי:
$$A_i=A_{i+1}(A_i\cap \underbrace{B_0}_{G})\triangleright A_{i+1}(A_i\cap B_1)\triangleright A_{i+1}(A_i\cap B_2)\triangleright ...\triangleright A_{i+1}(A_i\cap \underbrace{B_m}_{1})=A_{i+1}$$
נבצע תהליך דומה לעדן את $\{B_i\}$ ע"י $B_{i+1}(B_i\cap A_j)$ כמקודם כאשר $j=0...n$ וכמובן:
$$B_i=B_{i+1}(B_i\cap \underbrace{A_0}_{G})\triangleright B_{i+1}(B_i\cap A_1)\triangleright B_{i+1}(B_i\cap A_2)\triangleright ...\triangleright B_{i+1}(B_i\cap \underbrace{A_n}_{1})=B_{i+1}$$
כעת נראה ששתי הסדרות המעודנות כנ"ל שקולות.
נשתמש בלמה של זסנהאוס כדי להסיק ש:
$$\frac{A_{i+1}(A_i\cap B_j)}{A_{i+1}(A_i\cap B_{j+1})}\cong\frac{B_{j+1}(B_j\cap A_i)}{B_{j+1}(B_j\cap A_{i+1})}$$
באופן זה יוצרים התאמה חח"ע ועל בין גורמי שתי הסדרות שמתאימה לגורם – גורם שהוא איזומורפי לו.

<u>הוכחת ז'ורדן הלדר</u>
תהיינה $\{B_i\}_{i=0}^{m}$ $\{A_i\}_{i=0}^{n}$ סדרות הרכב של G, נמצא להן (ע"פ שרייר) עידונים שקולים.

נצמצם חזרות וסיימנו (לא קיימים עידונים מלבד חזרות לסדרת הרכב).
❑

<u>הגדרה</u>
גורמי ההרכב של חבורה G הם **<u>ה</u>**גורמים של סדרת הרכב של G.
על סמך משפט **<u>ז'ורדן הלדר</u>** זה לא תלוי בסדרה ולכן זה מוגדר היטב.

כל חבורה סופית מוגדרת בעצם ע"י חבורות פשוטות סופיות שהן גורמי ההרכב שלה, ולכן אמרנו בעבר שהאחרונות הן אבני הבניין של כל החבורות הסופיות.
<u>דוגמאות</u>

1. G פשוטה $\Leftarrow$ G גורם ההרכב היחיד של G, כי הסדרה היא $G \triangleright \{1\}$
2. G פשוטה , נסתכל בחבורה $G \times G \times G$ אזי יש לה 3 גורמי הרכב איזומורפיים ל G.
3. $G = S_n$ עבור $n \geq 5$ יתקבל $S_n \triangleright A_n \triangleright 1$ גורמי הרכב $\mathbb{Z}_2, A_n$
4. $|G| = p^n$ ראינו שיש ל-G סדרת הרכב עם גורמים $\mathbb{Z}_p$ (n פעמים) ולכן יש גורם הרכב יחיד $\mathbb{Z}_p$ בריבוי.

מסקנה ממשפט ז'ורדן-הלדר:
המשפט היסודי של האריתמטיקה – פירוק מספר טבעי למכפלת גורמים ראשוניים היא יחידה עד כדי סדר הגורמים.

הוכחה:
$G = \mathbb{Z}_n$
$n = p_1 \cdot \ldots \cdot p_k$
ראינו שיש סדרת הרכב ל-G שגורמיה הם $\mathbb{Z}_{p_1} \ldots \mathbb{Z}_{p_k}$
ממשפט ז'ורדן הלדר – אם קיים פירוק אחר $n = t_1 \cdot \ldots \cdot t_l$ אזי נקבל גורמי הרכב $\mathbb{Z}_{t_1} \ldots \mathbb{Z}_{t_l}$
ממשפט ז'ורדן הלדר מתחייב k=l ועד כדי שינוי סדר כל גורם בראשון איזומורפי לגורם בשני, ולכן קיים סידור שעבורו לכל i מתקיים $p_i = t_i$ וסיימנו.

<u>חבורות פתירות</u>
הגדרה: חבורה G נקראת **<u>פתירה</u>** אם יש לה סדרה נורמלית עם גורמים אבליים.
מקור השם: קשור לפתרון משוואות פולינומיאליות.
לכל פולינום מתאימים חבורה (חבורת גלואה) ואז הוא פתיר $\Leftrightarrow$ החבורה פתירה.

<u>טענה:</u>
תהי G פתירה, אז:

1. כל חבורה חלקית $H \leq G$ פתירה
2. כל חבורת מנה G/H היא פתירה (כמובן H נורמלית)

<u>הגדרה:</u>
סדרה נורמלית עם גורמים אבליים תיקרא **<u>סדרה פתירה</u>**.

<u>הוכחת הטענה:</u>
ניקח סדרה פתירה עבור G, לפי הנתון G_i / G_{i+1} אבליות.
בהנתן $H \leq G$ נתבונן ב $H = H \cap G \triangleright H \cap G_1 \triangleright H \cap G_2 \triangleright \ldots \triangleright H \cap G_n = 1$
זו סדרה נורמלית עבור H.
נראה ש<u>הגורמים אבליים</u>:

$$H\cap G_i/H\cap G_{i+1}\cong\frac{\overbrace{G_{i+1}}^{S}\overbrace{(H\cap G_i)}^{T}}{G_{i+1}}$$

$$\underbrace{ST/S\cong T/S\cap T}_{\text{משפט האיזומורפיזם השני}}\quad(\text{נשים לב כי}\quad G_i\cap G_{i+1}=G_{i+1}\quad)$$

נתון ש G_i/G_{i+1} אבלית ולכן $\frac{G_{i+1}(H\cap G_i)}{G_{i+1}}$ אבלית (כתת חבורה)

לכן:
$H\cap G_i/H\cap G_{i+1}$ אבלית והסדרה שהגדרנו פתירה

מכאן - H פתירה כנדרש.

.2
ניקח $H\lhd G$ ונראה ש G/H פתירה.

ניקח סדרה פתירה עבור G ונתבונן בסדרה הנורמלית $G\rhd H\rhd 1$ ע"פ משפט העידון של שרייר יש ל-2 סדרות אלה עידונים שקולים, בפרט יש עידון שלה שגורמיו כולם אבליים (כי הוא שקול לעידון של סדרה פתירה – שכל גורמיו אבליים).
כלומר קיים עידון שנראה כך: $G=A_0\rhd A_1\rhd\ldots\rhd(A_k=H)\rhd H_1\rhd\ldots\rhd H_l$ שהוא סדרה פתירה ל G.

עקרון חשוב: *עידון של סדרה פתירה הוא סדרה פתירה.*
הסיבה: גורם של העידון איזומורפי לחבורת מנה של חבורה חלקית של גורם של הסדרה המקורית.

כעת נסתכל על הסדרה שמצאנו עד H מודולו H, כלומר על:
$$G/H=A_0/H\rhd A_1/H\rhd\ldots\rhd A_k/H=1$$

ואז ממשפט האיזומורפיזם השלישי:
$$\frac{A_i/H}{A_{i+1}/H}\cong A_i/A_{i+1}$$

ולכן באגף השמאלי קיבלנו חבורה אבלית, וזה נכון לכל הגורמים בסדרה של G/H ולכן G/H פתירה.

חבורת מנה של חבורה חלקית = **גזרה (Section)**

גורמים של סדרה מעודנת הם <u>גזרות</u> של גורמים של הסדרה המקורית.

<u>טענה-דוגמה</u>
כל חבורת-p סופית היא פתירה.
הוכחה:
ניקח לה סדרת הרכב, הגורמים יהיו $\mathbb{Z}_p$ ולכן אבליים ואכן החבורה פתירה.

<u>שיעור 20</u>

<u>דוגמאות:</u>
חבורות אבליות, חבורות p-סופיות, S_4

ראינו G פתירה אז כך גם חבורות חלקיות וחבורות מנה שלה.

<u>טענה</u>
תהי G חבורה
$H \le G$
נניח:
$H \lhd G$, H פתירה, G/H פתירה
אז G פתירה.

<u>הוכחה</u>
ניקח סדרה פתירה $\{H_i\}_{i=0}^{n}$ עבור H.
ניקח גם סדרה פתירה עבור G/H, שהיא בהכרח מהצורה $\{G_j/H\}_{j=0}^{m}$ כאשר $H \le G_j \le G$
$G/H = G_0/H \rhd G_1/H \rhd \ldots \rhd G_m/H = 1$

ואז
$G = G_0 \rhd G_1 \rhd \ldots \rhd G_m = H$

נמשיך סדרה זו ע"י
$G_m = H = H_0 \rhd H_1 \rhd \ldots \rhd H_n = 1$

וקיבלנו סדרה נורמלית עבור G.
זו סדרה פתירה כי H_i/H_{i+1} אבלית וגם

$$\frac{G_j/H}{G_{j+1}/H} \underbrace{\cong}_{\text{משפט האיזומורפיזם השלישי}} G_j/G_{j+1} = \text{חבורה אבלית}$$

כי $\{G_j/H\}$ סדרה פתירה.

<u>מסקנה</u>
G,H פתירות $\Leftarrow$ $G \times H$ פתירה
מדוע? כי $1 \times H \lhd G \times H$ וגם $(G \times H)/(1 \times H) \cong G$
ולכן יש לנו תת חבורה פתירה שגם חבורת המנה בה פתירה.

<u>משפט</u>
חבורת-p סופית היא פתירה
<u>הוכחה</u>
ראינו הוכחה אחת, ניתן אחרת באינדוקציה על גודל החבורה.

$|G| = 1$ ברור
מעבר האינדוקציה:
$|G| > 1 \Leftarrow |Z(G)| > 1$ (ראינו זאת בעבר)
אולם כעת $Z(G)$ אבלית ולכן פתירה.
$|G/Z(G)| = |G|/|Z(G)| < |G|$
חבורת המנה גם היא חבורת p, מדוע? גדלה כידוע הוא האינדקס של המרכז. אם האינדקס של המרכז הוא 1 – סיימנו כי החבורה אבלית, אחרת – האינדקס של המרכז מתחלק ב p (ממשפט לגראנז') ולא בשום מספר אחר.
מהנחת האינדוקציה $G/Z(G)$ פתירה (כי גם היא חבורת-p וקטנה ממש מ G) ומהטענה האחרונה נובע כי G פתירה.

<u>למה</u>
חבורה פשוטה אבלית היא בהכרח $\mathbb{Z}_p$ עבור p ראשוני כלשהו.
<u>הוכחה</u>
תהי G אבלית פשוטה (לא בהכרח סופית)
אז $G\neq 1$, ניקח $1\neq x\in G$ ונתבונן ב $\langle x\rangle \leq G$ אזי נובע מאבליות ש $\langle x\rangle \lhd G$ ומפשטות $\langle x\rangle = G$, נסיק כי G היא אף ציקלית.
אם G ציקלית אינסופית נקבל סתירה כי $G=\langle x\rangle \rhd \langle x^2\rangle \neq 1$ בסתירה לפשטות (באמצע זו תת חבורה ממש נורמלית)
מכאן נובע ש G ציקלית סופית, לכן איזומורפית לחבורת מודולו-n כלשהי וכל מחלק של n יגדיר תת-חבורה נורמלית.
(אם $d|n$ אז $\langle x^d\rangle$ מגדיר תת חבורה ממש נורמלית) ולכן n=p ראשוני ואכן $G\cong \mathbb{Z}_p$

<u>טענה</u>
חבורה סופית היא פתירה $\Leftrightarrow$ יש לה סדרת הרכב עם גורמים ציקליים מסדרים ראשוניים: $\mathbb{Z}_{p_1}, \mathbb{Z}_{p_2}, \ldots, \mathbb{Z}_{p_k}$

<u>הוכחה</u>
$\Rightarrow$: גורמים ציקליים הם אבליים. לכן סדרת ההרכב הנ"ל היא סדרה פתירה ו-G פתירה.
$\Leftarrow$: ניקח סדרה פתירה עבור G, ניקח סדרת הרכב עבור G, לפי משפט שרייר יש לשתי הסדרות עידונים שקולים. גורמי העידונים הם מצד אחד אבליים (כעידון של סדרה פתירה) ומצד שני פשוטים או $\{1\}$ (כעידון של סדרת הרכב).
בהנתן הלמה – הגורמים של העידונים הם כולם $\mathbb{Z}_p$ או 1 ולכן גורמי סדרת ההרכב המקורית הם $\mathbb{Z}_p$.

הערה:
G פתירה סופית $\Leftarrow$ ל-G סדרת הרכב עם גורמים $\mathbb{Z}_{p_i}$ בפרט ציקליים $\Leftarrow$ יש סדרה נורמלית עם גורמים ציקליים.
אם G פתירה אינסופית לא בהכרח יש סדרה נורמלית עם גורמים ציקליים.
למשל $G=\mathbb{Z}^\infty=\mathbb{Z}\times\mathbb{Z}\times\ldots$ או חבורת הרציונליים עם 0 וחיבור.

<u>שיעור 21</u>

<u>חבורת הקומוטטור והחבורה הנגזרת</u>

קומוטטור $[x,y]=xyx^{-1}y^{-1}$

$$xy=yx\Leftrightarrow [x,y]=1$$
$$[x,y]^{-1}=yxy^{-1}x^{-1}=[y,x]$$
החבורה הנגזרת= $G'=\langle [x,y]: x,y\in G\rangle$

היתה השערה שאם G פשוטה סופית לא אבלית, כל $g\in G$ הוא קומוטטור $g=[x,y]$ הוכח ב 2008 (ע"י צוות של ארבעה מתמטיקאים, ביניהם ענר)

תכונות G' :
1. $G'\lhd G$
2. G/G' אבלית
3. אם $N\lhd G$ וגם G/N אבלית אזי $G'\subseteq N$ כלומר – מבחינת הכלה G' היא מינימלית עבור תכונה זו.

דוגמאות ל G' :

$S_n' = A_n$
אם G פשוטה – אם היא אבלית $G'=1$ אם לא - $G'=G$

הסדרה הנגזרת (Derived Series)

הגדרה
בהנתן חבורה G, נגדיר סדרה $G^{(i)}$ ($i \geq 0$) על ידי:

$$G^{(0)}=G$$
$$G^{(1)}=G'$$
$$\vdots$$
$$G^{(i+1)}=(G^{(i)})'$$

נראה בהמשך כי $G^{(i)} \triangleleft G$ לכל i.

אם היינו רוצים להוכיח את זה באינדוקציה, זה היה קשה, כי נורמליות הוא לא יחס טרנזיטיבי, ולכן צעד האינדוקציה לא יהיה פשוט. לצורך זה ולצרכים אחרים נגדיר תת חבורה אפיינית.

תת חבורה אפיינית (Characteristic)

$H \leq G$ אפיינית אם"ם $\phi(H) \leq H$ לכל $\phi \in AutG$
ואז נסמן $H \; char \; G$

תכונות של תתי חבורות אפייניות:

1. $H \; char \; G \Rightarrow H \triangleleft G$ כי ניקח אוטומורפיזם פנימי של הצמדה ב g ונקבל ${}^gH \leq H$ לכל $g \in G$
   וזה יגרור $H \triangleleft G$
2. $H \; char \; G \Rightarrow \phi(H)=H \; \forall \phi \in AutG$ כי $\phi^{-1} \in AutG$ ולכן $\phi^{-1}(H) \leq H$ ואז $H \leq \phi(H)$ ואז מהיחס הדו כיווני נובע $\phi(H)=H$
3. טרנזיטיביות – כלומר: $H \; char \; G \wedge K \; char \; H \Rightarrow K \; char \; G$

הוכחת הטרנזיטיביות:
יהי $\phi \in AutG$
ראינו $\phi(H)=H$ ולכן $\phi_{|H} \in AutH$
$Kchar \; H \Rightarrow \phi(K)=\phi_{|H}(K) \leq K$

טענה: $G^{(i)} charG$ לכל i.
הוכחה: באינדוקציה על i
עבור i=0 זה מיידי, עבור i=1 צ"ל $G' \; char \; G$
אז: $\phi \in AutG$ ולכן אם ניקח $G'=\langle [x,y] : x,y \in G \rangle$

$$\phi(G')=\langle \phi([x,y]) : x,y \in G \rangle$$
$$\phi([x,y])=\phi(xyx^{-1}y^{-1})=\phi(x)\phi(y)\phi(x)^{-1}\phi(y)^{-1}=[\phi(x),\phi(y)]$$

ולכן $\phi(G')$ נוצר ע"י קומוטטורים ומכאן $\phi(G') \leq G'$
מעבר האינדוקציה:
נניח $G^{(i)} char \; G$ ואז נוכיח $G^{(i+1)} char \; G$
מדוע? $G^{(i+1)}=(G^{(i)})'$ וכבר ראינו שחבורת הנגזרת אפיינית $(G^{(i)})' \; char \; G^{(i)}$
מכיוון שזהו יחס טרנזיטיבי נקבל $G^{(i+1)} char \; G$

מסקנה – בפרט $G^{(i)} \triangleleft G$ לכל i.

משפט
תהי G חבורה
G פתירה $\Leftrightarrow$ קיים n שעבורו $G^{(n)}=\{1\}$
הוכחה
$\Rightarrow$
נניח $G^{(n)}=1$
אזי $\{G^{(i)}\}_{i=0}^{n}$ סדרה נורמלית.
הגורמים שלה הם אבליים, לפי תכונה 2 של החבורה הנגזרת.
$G^{(i)}/G^{(i+1)}=G^{(i)}/(G^{(i)})'$
לכן זו סדרה פתירה ומכאן – G פתירה כנדרש.
$\Leftarrow$
נניח G פתירה ותהי $\{G_i\}_{i=0}^{n}$ סדרה פתירה עבור G.
אז נראה שלכל $0 \le i \le n$ נקבל $G^{(i)} \le G_i$
נוכיח זאת באינדוקציה על i.
בסיס: $G^{(0)}=G_0=G$
מעבר: נניח $G^{(i)} \le G_i$
אז
$G^{(i+1)}=(G^{(i)})' \le (G_i)'$
מפתירות G_i/G_{i+1} אבלית, ולכן $(G_i)' \subseteq G_{i+1}$ (G/N אבלית $\Leftrightarrow$ $G' \subseteq N$)
מכאן $G^{(i+1)} \le G_{i+1}$ כדרוש.

נשתמש בזה ל i=n ואז $G^{(n)} \le G_n=\{1\}$ ולכן $G^{(n)}=\{1\}$

לסיכום
הראינו שבחבורות פתירות – הסדרה הנגזרת היא הסדרה הפתירה הקטנה ביותר (ביחס להכלה).

הגדרה
אורך נגזר של חבורה פתירה G הוא ה-n המינימלי כך ש $G^{(n)}=\{1\}$

דוגמאות:
1. ל-G אורך נגזר 1 $\Leftrightarrow$ G אבלית.
2. G נקראת מטא-אבלית אם יש לה אורך נגזר קטן או שווה ל 2. זה שקול ל $G''=\{1\}$ למשל S_3

ניתוח S_n :
1,2 אורך נגזר 0,1
3 אורך נגזר 2 כי $A_3'=1 \Rightarrow S_3''=1$, $S_3'=A_3$
4 אורך נגזר 3 (לא בטוח, כדאי לבדוק בבית)
>4 S_n לא פתירה, ולכן לא מוגדר אורך נגזר. $(S_n)^{(i)}=A_n$

הערה

<u>חבורות מילוליות</u>

נוצרות ע"י $\langle x^n : x \in G \rangle$ *עבור* n *נתון, חבורות אלו הן אפייניות.*

<u>משפט הבסיס לחבורות אבליות סופיות</u>

G אבלית סופית $\Leftrightarrow$ $G \cong \mathbb{Z}_{n_1} \times \ldots \times \mathbb{Z}_{n_k}$ מכפלה ישרה של חבורות ציקליות.

ניתן גם לדרוש $n_1 | n_2 | \ldots | n_k$

נראה את ההוכחה בתרגיל. (משפט מתורת החבורות, אבל ההוכחה שלו היא קצת קומבינטורית)

עד כאן בנוגע לחבורות ונתחיל עם חוגים.

תורת החוגים

הגדרה

$(R,+,\cdot,0,1)$ יקרא **חוג** אם:

1. חיבור וכפל יהיו פעולות דו מקומיות על R ו $0,1\in R$

2. R עם חיבור ו 0 הוא חבורה קומוטטיבית.

3. R עם כפל ו 1 הוא מונואיד עם יחידה, כלומר הכפל אסוציאטיבי ו 1 איבר יחידה עבור הכפל.

4. הכפל לא בהכרח קומוטטיבי ואין הופכי בהכרח (עבור כפל)

5. חוקי פילוג $x(y+z)=xy+xz$ $(x+y)z=xz+yz$

הערה: חוג הוא כמו שדה בלי דרישה לקומוטטיביות בכפל וקיום הופכי לכל איבר שונה מ 0.

חוג נקרא **קומוטטיבי** אם הכפל בו קומוטטיבי.

חוג נקרא **חוג חילוק** אם לכל $x\neq 0$ יש הופכי כפלי – חוג חילוק קומוטטיבי נקרא **שדה**

דוגמאות

1. $(\mathbb{Z},+,\cdot,0,1)$ השלמים הוא חוג קומוטטיבי אך אינו חוג חילוק שכן $2^{-1}\notin\mathbb{Z}$
2. כל שדה F
3. חוג המטריצות $M_n(F)$
4. $M_n(\mathbb{Z})$
5. כללית בהנתן חוג R ניתן להגדיר את $M_n(R)$ ולקבל חוג.
6. חוגי פולינום $F[x]$, וכללית $R[x]$
7. $\mathbb{Z}_n$ הוא גם חוג
8. $\{f:\mathbb{R}\to\mathbb{R}\}$
$(f+g)(x)=f(x)+g(x)$
$(f\cdot g)(x)=f(x)g(x)$
$0_R=f_0$
$1_R=f_1$

הגדרה

יהי R חוג, אזי $a\in R$ נקרא **מחלק אפס** אם כפולה מסויימת שלו באיזה $b\neq 0$ היא 0: כלומר $ab=0$ או $ba=0$.

למשל ב $\mathbb{Z}_6$, 2 הוא מחלק 0 כי $2\cdot 3=0$, וכללית ב- $\mathbb{Z}_n$ כל k שלא זר ל n הוא מחלק אפס.

מחלקי אפס בדוגמה 8 יהיו:

כל פונקציה f שמתאפסת בנקודה כלשהי היא מחלק אפס, כי נגדיר פונקציה אחרת שהיא אפס על כל הישר מלבד נקודה זו, ומכפלתן תהיה פונקציית האפס.

אם $f(x)\neq 0$ לכל $x\in R$ אז קיים $\frac{1}{f}(x)=\frac{1}{f(x)}$, שהוא הופכי כפלי לפונקציה (כי מכפלתן תיתן פונקציה קבועה 1) ו f לא מחלק אפס.

לכן בחוג נתון, אם איבר a כלשהו הוא הפיך (דו צדדית) אזי a אינו מחלק אפס.

חוג הקווטרניונים

$\mathbb{R}\subseteq\underbrace{\mathbb{C}}_{\text{חוג חילוק}}$

מהם חוגי החילוק מעל $\mathbb{R}$? אנחנו יודעים שהמרוכבים, אבל האם יש עוד?
בשבת אחת ב 1843 המילטון, מתמטיקאי אירי מדבלין, הסתובב לו בדבלין וכשהיה על אחד הגשרים – עלה על הפתרון וחרט אותו על הגשר: $i^2=j^2=k^2=ijk=-1$
קוראים להם H על שם המילטון, או לחילופין Q.
$$H=\{a\cdot 1+b\cdot i+c\cdot j+d\cdot k : a,b,c,d\in\mathbb{R}\}$$
וזה מרחב וקטורי ממימד 4 מעל $\mathbb{R}$ עם בסיס $\{1,i,j,k\}$
כפל ב H נקבע ע"י כפל איברי הבסיס, כאשר 1 נייטרלי, ונוסחאות הכפל מהגשר מגדירות באופן מלא את טבלת הכפל של איברי הבסיס.
עוזר לעיתים לצייר זאת במעגל (הכפל אנטי קומוטטיבי):
$$ij=k\ ,\ jk=i\ ,\ ki=j$$
$$ji=-k\ ,\ kj=-i\ ,\ ik=-j$$

<u>שיעור 23</u>

נאמר שאיבר a הוא הפיך אם יש $b\in R$ כך ש ab=ba=1, ואז מסמנים $b=a^{-1}$
אוסף האיברים ההפיכים בחוג מהווה חבורה ביחס לכפל.

לדוגמה: כל שדה בלי איבר האפס הוא חבורה.

עוד דוגמה: אם $R=M_n(F)$ חוג המטריצות אז $R^*=GL_n(F)$ חבורת המטריצות ההפיכות, (נשים לב שהוא אינו חוג כי אינו שומר על סגירות תחת חיבור).

ניזכר במחלקי אפס – 0 תמיד מחלק 0.

<u>טענה פשוטה</u>:
a הפיך $\Leftarrow$ a אינו מחלק אפס
<u>הוכחה</u>:
נניח ab=0 עבור $b\neq 0$ כלשהו, נניח קיום הפכי ונכפיל $b=a^{-1}(ab)=a^{-1}0=0$ בסתירה.

ראינו דוגמה לנקודה הזו בשיעור שעבר כאשר החוג היה פונקציות ממשיות (דוגמה 8).
מחלקי האפס יהיו במקרה זה כל הפונקציות המתאפסות, כלומר כל הפונקציות שהן איברים לא-הפיכים (לא לא-הפיכים במובן של הרכבה, אלא במובן הכפלי – שלא קיימת עבורם פונקציה שפונקציית המכפלה קבועה על 1).

הערה: לו היינו מגדירים את חוג הפונקציות עם פעולת ההרכבה – היינו מאבדים דיסטריביוטיביות מימין, כי לא בהכרח
$$h\circ(f+g)=h\circ f+h\circ g$$

נעיר גם שאי-הפיכות אינה שקולה להיותו של איבר מחלק אפס, אע"פ שהראינו גרירה בכיוון אחד.
למשל בחוג השלמים – 2 אינו הפיך ואינו מחלק אפס.

<u>חוג הקווטרניונים H</u>
טענה – זהו חוג חילוק (=שדה בלי קומוטטיביות בחיבור)
<u>הוכחה</u> נגדיר צמוד $\overline{a+bi+cj+dk}=a-bi-cj-dk$ ואז מתקיים: $x\bar{x}=(a^2+b^2+c^2+d^2)1$ (לבדוק לבד)
נשים לב שאם $x\neq 0$ אזי אחד מהמקדמים לפחות אינו 0.
ואז המקדמים בריבוע הם אי שליליים ולפחות אחד מהם ממש חיובי, ולכן $x\bar{x}>0$
ואז:

$$x^{-1}=\frac{1}{a^2+b^2+c^2+d^2}\cdot\overline{x}$$

כפי שציינו בשיעור הקודם – זו הדוגמה הראשונה מ 1843 לחוג חילוק לא קומוטטיבי.

אפשר להגדיר נורמה על ידי $|x|=\sqrt{a^2+b^2+c^2+d^2}$
ומקבלים שהנורמה היא כפלית (כמו במרוכבים) $|xy|=|x||y|$
אולי קשה להעריך את זה – אבל זה לא פשוט וקשור ישירות ללוח הכפל בדיוק כפי שהוגדר.
חוג חילוק מעל $\mathbb{R}$ *, הגדרה זמנית - מ"ו ממימד סופי מעל* $\mathbb{R}$ *, מכיל את* $\mathbb{R}$ *ואיבריו מתחלפים עם כל איברי החוג.*
משפט (שלא נוכיח): חוגי החילוק היחידים מעל $\mathbb{R}$ הם $\mathbb{R},\mathbb{C},H$
(יש גם חוג ממימד 8, אבל אז מאבדים לא רק קומוטטיביות אלא גם אסוציאטיביות)

<u>הגדרה</u>: יהי R חוג, ה**<u>מרכז</u>** של R, יסומן ע"י $Z(R)$ והוא מוגדר על ידי:
$$Z(R)=\{a\in R: ab=ba\ \forall\, b\in R\}$$
<u>הערה</u> $Z(R)$ מכיל את האפס והיחידה, סגור לחיבור וכפל ומהווה **<u>תת חוג</u>**
באשר: תת חוג $S\subseteq R$ קבוצה חלקית שמכילה את 0, 1 ומהווה חוג ביחס לפעולות של R.

R חוג חילוק מעל $\mathbb{R}$ אם $\mathbb{R}\subseteq Z(R)$
R חוג חילוק
$dim_{\mathbb{R}} R<\infty$

נחזור לכמה טענות פשוטות על חוגים:
יהי R חוג
<u>טענה:</u>
1. $a\in R$ לכל $a\cdot 0=0\cdot a=0$
2. $a(-b)=(-a)b=-ab$
3. $(-a)(-b)=ab$

נוכיח את 1 – והשאר בהעתקה לינארית מאלגברה 1 וההוכחות מאקסיומות השדה:
$$a\cdot 0=a(0+0)=a0+a0\ \Rightarrow\ a0=0$$

<u>שיעור 24</u>
<u>הגדרה</u>
<u>תחום שלמות</u> הוא חוג קומוטטיבי בו 0 הוא מחלק 0 היחיד [לעיתים נאמר במקרה זה שהחוג "ללא מחלקי אפס"]

<u>דוגמאות</u>
1. שדה F
2. חוג הפולינומים מעל שדה
3. פולינומים מעל תחום שלמות כלשהו
4. $\mathbb{Z}$

<u>אנטי דוגמאות:</u>
1. $M_2(F)$ לא תחום שלמות (יש מחלקי אפס, אין קומוטטיביות)
2. $\mathbb{Z}_n$ עבור n לא-ראשוני

<u>טענה</u>
תחום שלמות סופי הוא שדה
<u>הוכחה</u>

יהי R תחום שלמות סופי.
יהי $a\neq 0\in R$ ומספיק להראות שקיים a^{-1}
נתבונן ב $f:R\to R$ המוגדרת ע"י $f(x)=ax$
נראה f חח"ע.

נניח ש $f(x)=f(y)$ אז $ax=ay$ ולכן $a(x-y)=0$ ומכיוון ש R תחום שלמות נובע מיידית כי $x-y=0$
ולכן x=y וקיבלנו חח"ע כנדרש.

מכיוון ש R קבוצה סופית – נובע ש f היא גם על, ולכן קיים $f(x)=1$ ואז $ax=1$ ומקומוטטיביות זה גם שווה ל xa
ולכן x ממש הופכי של a.

<u>הומומורפיזמים ואידיאלים</u>
<u>הגדרה</u>
יהיו R ו-S חוגים
העתקה $\phi:R\to S$ תקרא הומומורפיזם אם:
$$\phi(x+y)=\phi(x)+\phi(y)$$
$$\phi(xy)=\phi(x)\phi(y)$$
$$\phi(1_R)=1_S$$
הערות
הדרישה הראשונה אומרת ש ϕ הוא הומומורפיזם של חבורות מהחבורה החיבורית של R לחבורה החיבורית של S, ומכאן נובע $\phi(0)=0$ ואף $\phi(-x)=-\phi(x)$ כזכור לנו מחבורות.

התכונה $\phi(1_R)=1_S$ לא נובעת משתי האחרות, כי למשל אם $\phi=0$ זהותית, מתקיימות שתי הראשונות אבל לא השלישית (זה כמובן נכון רק אם $0_S\neq 1_S$, ואחרת $S=\{0\}$ וזה לא מעניין)

<u>דוגמאות להומומורפיזמים</u>
1. $\phi:\mathbb{Z}\to Q$ ע"י $\phi(x)=x$
2. $\phi:\mathbb{C}\to M_2(\mathbb{R})$ על ידי $a+bi\to\begin{pmatrix}a & b\\ -b & a\end{pmatrix}$
3. $\phi:\mathbb{Z}\to\mathbb{Z}_n$ על ידי $nq+r\to r$ (העתקת השארית מודולו n)

<u>הגדרה</u>
יהי $\phi:R\to S$ הומומורפיזם של חוגים.
1. ϕ נקרא מונומורפיזם אם הוא חח"ע
2. ϕ נקרא אפימורפיזם אם הוא על
3. באותו אופן הוא איזומורפיזם אם הוא חח"ע ועל

בדוגמאות שנתנו – 1 ו-2 הם מונו ו-3 הוא אפי
ענר: רק לי מותר לקצר, אם תכתבו בבחינה "מונו" ו"אפי" ירדו לכם נקודות.

<u>תמונה וגרעין</u>
$$Image\,\phi=\{\phi(x):x\in R\}\subseteq S$$
$$Ker\,\phi=\{x\in R:\phi(x)=0\}$$

תכונות:

1. $Image\,\phi$ הוא תת חוג של S
2. $Ker\,\phi$ הוא תת חבורה חיבורית של $(R,+,0)$ שסגור לכפל מימין ומשמאל בכל $a\in R$ (כאילו תת-חוג בלי יחידה...)

<u>הוכחת התכונות</u>

התמונה של ϕ סגורה לחיבור כי $\phi(x+y)=\phi(x)+\phi(y)$ סגור לנגדי מכיוון ש $\phi(-x)=-\phi(x)$

$0=\phi(0)\in Image\,\phi$

סגור לכפל:

$\phi(x)\,\phi(y)=\phi(xy)\in Image\,\phi$

$1=\phi(1)\in Image\,\phi$

<u>הערה</u>

הגרעין סגור לכפל אך 1 בדרך כלל לא בגרעין (למעשה הוא בגרעין רק אם בטווח $1_S=0_S$ וכאמור זה לא מעניין במיוחד), ולכן הגרעין לא בהכרח תת-חוג.

הגרעין תת חבורה חיבורית, זה נובע ישירות מתכונות של הומומורפיזם והוכחנו דברים דומים כבר כמה פעמים בעבר.

סגירות לכפל "חיצוני":

יהי $a\in R$ ונניח $x\in Ker\,\phi$

אז $\phi(ax)=\phi(a)\,\phi(x)=\phi(a)\cdot 0=0\ \Rightarrow\ ax\in Ker\,\phi$

ובאופן דומה גם $xa\in Ker\,\phi$

<u>הגדרה</u>

<u>אידיאל</u> בחוג R היא קבוצה חלקית $I\subseteq R$ המהווה תת חבורה חיבורית של $(R,+,0)$ הסגורה לכפל מימין ומשמאל בכל איברי R.

אם דורשים סגירות רק לכפל חיצוני מימין – I מכונה **<u>אידיאל ימני</u>**.

אם דורשים סגירות רק לכפל חיצוני משמאל – I מכונה **<u>אידיאל שמאלי</u>**.

אם I אידיאל שמאלי וימני אז הוא נקרא **<u>אידיאל</u>** או **<u>אידיאל דו-צדדי</u>**.

<u>דוגמאות</u>

1.

R חוג קומוטטיבי, $a\in R$ ונגדיר $(a)=aR=\{ar:r\in R\}$ וזה יהיה אידיאל.

2.

$\{0\}$ אידיאל בכל חוג

3.

R עצמו הוא אידיאל ב-R

$3\frac{1}{2}$

כל אידיאל שמכיל את 1 הוא R

4.

R חוג לא קומוטטיבי אז aR אידיאלי ימני, אבל לא בהכרח שמאלי.

Ra אידיאל שמאלי.

מגדירים $RaR=\{\sum r_i a s_i : r_i, s_i\in R\}$

זה אידאל דו-צדדי (בפרט – הקטן ביותר שמכיל את a)

<u>הגדרה</u>

בחוג קומוטטיבי R אידיאל מהצורה aR נקרא **<u>אידיאל ראשי</u>** (הנוצר ע"י a).

דוגמה: $n\mathbb{Z}$ אידיאל ראשי ב $\mathbb{Z}$

<u>טענה</u>
כל אידיאל ב $\mathbb{Z}$ הוא ראשי.
<u>הוכחה</u>
יהי I אידיאל ב $\mathbb{Z}$.
אם $I=\{0\}$ אז $I=0\mathbb{Z}$ ראשית וסיימנו.
נניח כעת $I\neq\{0\}$ ולכן יש ב I איזה איבר שאינו 0, ובפרט קיים $n>0$ (ניקח את זה שאינו 0 או את הנגדי החיבורי שלו)
לכל קבוצת מספרים שלמים חיוביים יש מינימום (עיקרון הסדר הטוב) ולכן קיים $n>0$ מינימלי ב I.
נראה כעת כי $I=n\mathbb{Z}$ עבור n זה.

ההכלה $n\mathbb{Z}\subseteq I$ ברורה, כי $n\in I$ ולכן $nz\in I$ לכל $z\in\mathbb{Z}$

נראה את הכיוון השני:
יהי $m\in I$ ונחלק אותו ב n עם שארית r, כלומר $m=nq+r$ כאשר $0\leq r<n$
$nq\in I, m\in I$ ולכן $m-nq\in I$ כלומר $r\in I$
אם $r>0$ נקבל סתירה למינימליות של n.
מסקנה $m=nq$ ולכן $I\subseteq n\mathbb{Z}$

מההכלה הדו-כיוונית מתקבלת הטענה כנדרש.

<u>הגדרה</u>
תחום שלמות בו כל אידיאל הוא ראשי נקרא לעיתים **<u>תחום ראשי</u>** או **<u>חוג ראשי</u>**.
למשל $\mathbb{Z}$, בהמשך נראה שגם $F[x]$ הוא תחום ראשי.

נסביר קצת את השם "אידיאל":
בשלמים – כל אידיאל מתאים למספר כלשהו (כי הוא מגדיר אידיאל ע"י $n\mathbb{Z}$ *)*
לכן ראו באידיאל הכללה של מספר.
בתורת המספרים מופיעים חוגים בהם לא כל אידיאל הוא ראשי.

<u>עוד תכונות של אידיאלים</u>
.1
$\emptyset\neq I\subseteq R$ סגור לחיבור וסגור לכפל חיצוני דו-צדדי $\Leftarrow$ I אידיאל
כי יהי $x\in I$ ומכיל את 0, כי הוא סגור לכפל חיצוני.
$y\in I$ אז $-y=(-1)y\in I$ (סגירות לנגדי)
מסקנה: I תת חבורה חיבורית של $(R,+,0)$ ולכן (בהנתן סגירות לכפל חיצוני) I אכן אידיאל.

.2
חיתוך אידיאלים מהווה אידיאל.
I,J אידיאלים אז $I\cap J$ אידיאל.
ובכלל אם I_α אידיאלים ב R, אז $\cap I_\alpha$ אידיאל

.3
I,J אידיאלים ב R אז
$I+J=\{a+b:a\in I, b\in J\}$ גם כן אידיאל ב R.

.4
אם נגדיר כפל באופן הבא:
$$I\cdot J:=\{\sum a_i b_i : a_i\in I\,,\, b_i\in J\}$$
נקבל שגם זה אידיאל.

נסיים את השיעור בבניה של חוג מנה.

<u>חוג מנה</u>
יהי R חוג, I אידיאל ב R.
נגדיר את **<u>חוג המנה</u>** R/I להיות חבורת המנה החיבורית $\{a+I : a\in R\}$, $(a+I)+(b+I)=(a+b)+I$
עם כפל שמוגדר ע"י $(a+I)(b+I)=ab+I$
$0+I$ נייטרלי לחיבור ב R/I
$1+I$ נייטרלי לכפל

הגדרת הכפל בלתי תלויה בנציגים:
$$a+I=a_1+I$$
$$b+I=b_1+I$$
אז:
$$a_1=a+x\,,\, b_1=b+y \qquad x\,,\, y\in I$$
ונקבל
$$a_1 b_1+I=(a+x)(b+y)+I=ab+\underbrace{ay}_{\in I}+\underbrace{xb}_{\in I}+\underbrace{xy}_{\in I}+I=ab+I$$
ונובעת בקלות הטענה הבאה:
<u>טענה</u>
$$(R/I\,,+,\cdot\,,0+I\,,1+I)$$
הוא חוג (לפי הדברים שהראינו לעיל)

תרגילון לסיום:
חוג המנה $\mathbb{Z}/n\mathbb{Z}$ איזומורפי ל $\mathbb{Z}_n$ כחוג.

<u>שיעור 25</u>
נזכיר:
I אידיאל ב R אם הוא תת חבורה חיבורית של R (עם אותה פעולת חיבור) וסגור לכפל מימין ומשמאל באברי R.
נסמן $I\lhd R$

חוג מנה:
$$R/I=\{a+I : a\in R\}$$
עם חיבור וכפל ע"פ נציגים, מקבלים חוג ובו $0+I$ הוא הנייטרלי החיבורי ו $1+I$ הנייטרלי הכפלי.

<u>נגדיר</u>
<u>ההטלה הקנונית</u>
$$f: R\to R/I$$
$$f(a)=a+I$$
אז f היא הומומורפיזם של חוגים:
$$f(a+b)=a+b+I=a+I+b+I=f(a)+f(b)$$

$$f(ab)=ab+I=(a+I)(b+I)=f(a)f(b)$$
$$f(1)=1+I$$

f הוא על – אפימורפיזם, והוא בדרך כלל לא חח"ע כי $Ker(f)=I$
בפרט יוצא:
כל גרעין של הומומורפיזם הוא אידיאל
כל אידיאל הוא גרעין של הומומורפיזם

<u>משפטי איזומורפיזם לחוגים</u>

<u>משפט איזומורפיזם I לחוגים</u>

יהיו R,S חוגים
$f:R\to S$ הומומורפיזם של חוגים
ואז:
$$R/Ker(f)\cong Image(f)$$

<u>הוכחה</u>:
נגדיר $I=Ker(f)$ ואז כמובן $I\lhd R$
נגדיר גם כן: $\phi:R/I\to Image(f)$
על ידי: $\phi(a+I)=f(a)$
נראה אי-תלות בנציגים (כלומר ϕ מוגדרת היטב):
$$a+I=b+I\Rightarrow a-b\in I\Rightarrow f(a-b)=0=f(a)-f(b)\Rightarrow f(a)=f(b)$$
היפוך חצי הגרירה בשורה האחרונה תיתן חח"ע.
היות הפונקציה על מתקבל מיידית מכך שאנחנו מסתכלים על התמונה של הפונקציה, ושמירת הפעולות קלה להוכחה.

<u>דוגמה</u>
נגדיר $f:\mathbb{Z}\to\mathbb{Z}_n$
כפי שהגדרנו בהוכחה לכך של $\mathbb{Z}$ יש רק אידיאלים ראשיים, כלומר: $kn+r\to r$
זהו הומומורפיזם, הגרעין הוא $n\mathbb{Z}$ ונסיק על פי המשפט כי:
$$\mathbb{Z}/n\mathbb{Z}=\mathbb{Z}/Ker(f)\cong Image(f)=\mathbb{Z}_n$$

<u>משפט האיזומורפיזם II</u>

יהי R חוג, S תת חוג, I אידיאל ב R.
אז S+I תת חוג של R, $I\lhd(S+I)$, $S\cap I\lhd S$

והעיקר:
$$S/(S\cap I)\cong(S+I)/I$$

<u>הוכחה:</u>
נתבונן בהטלה הקנונית $f:R\to R/I$
נצמצם אותה ל-S:
$$\phi=f_{|S}:S\to R/I$$
אז $Ker(\phi)=S\cap I$ ו $Image(\phi)=\underbrace{(S+I)/I}_{\subseteq R/I}$ (כלומר אלו המחלקות של I עם נציג מ S)

נשתמש במשפט האיזומורפיזם I ונקבל כי:

$$S/Ker(\phi) \cong Image(\phi)$$
$$S/(S \cap I) \cong (S+I)/I$$

מדוע S+I תת חוג?
סגור לפעולות ומכיל את 0 ו 1.
(בדיקה קטנה שאפשר לעשות לבד)

<u>משפט האיזומורפיזם III</u>
יהי R חוג, $J \subset I$ אידיאלים ב R.
נגדיר $I/J = \{a+J : a+I\}$
זה <u>לא</u> חוג מנה (כי I אינו חוג) ולכן הוא מכונה <u>אידיאל מנה</u>.
נוכל להשתמש בפעולות של R/J כי הוא קבוצה חלקית של R/J.
אז:
$$I/J \lhd R/J \quad \wedge \quad (R/J)/(I/J) \cong R/I$$

נגדיר $f : R/J \to R/I$ על ידי $f(a+J) = a+I$

נראה אי-תלות בנציגים:
$$a+J = b+J \;\Rightarrow\; a-b \in J \;\Rightarrow\; a-b \in I \;\Rightarrow\; a+I = b+I$$
$\subseteq I$

קל לוודא כי f הומומורפיזם של חוגים, באופן טבעי הוא אפימורפיזם (=על), ולכן $Image(f) = R/I$
הגרעין הוא: $\{a+J : a+I = I\} = \{a+J : a \in I\} = I/J$
מכאן ש $R/J \lhd I/J$ כי הוא גרעין של הומומורפיזם.

וכעת על סמך <u>משפט האיזומורפיזם I</u> מתקבל:
$$(R/J)/Ker(f) \cong Image(f)$$
$$(R/J)/(I/J) \cong R/I$$

ענר: אם אין שאלות נעשה את משפט ההתאמה וזה באמת יהיה שיא של ארבע משפטים חשובים בשלושת-רבעי שעה.

<u>משפט ההתאמה:</u>
יש התאמה חח"ע ועל בין אידיאלים בחוג המנה R/I לבין אידיאלים ב R שמכילים את I.
נניח ש $I \subseteq J \lhd R$ ואז נגדיר: $f(J) \to J/I$
הטענה היא שזו התאמה חח"ע ועל, נראה את זה בתרגיל.

<u>שיעור 26</u>
הגדרה: חוג R נקרא **<u>פשוט</u>** אם יש בו רק שני אידאלים שונים – החוג כולו ו $\{0\}$.

הערה: החוג $\{0\}$ לא נחשב פשוט כי יש בו רק אידאל 1.
לכן בחוג פשוט $0 \neq 1$ ו $\{0\} \neq R$

<u>טענה</u> חוג קומוטטיבי R הוא פשוט $\Leftrightarrow$ R הוא שדה

<u>הוכחה</u>: בכיוון אחד – יהי R=F שדה, כדי להראות ש F פשוט די להוכיח שאידאל $I \neq \{0\}$ הוא כל F.
ניקח $a \neq 0 \in I$ יש הופכי ל a בשדה ולכן $a^{-1}a = 1 \in I$ וכבר ראינו שאם אידיאל מכיל את 1 הוא מכיל את הכל, כי הוא סגור לכפל חיצוני.

בכיוון השני – נניח R פשוט ונוכיח שהוא שדה. די להוכיח שלכל $a\neq 0$ יש הופכי a^{-1} .
נתבונן באידיאל $Ra=(a)=I$ ($a\neq 0$ ולכן $I\neq\{0\}$) ומפשטות נובע I=R ובפרט $1\in I$ ולכן יש $r\in R$ כך ש $ra=1$ ולכן $r=a^{-1}$ וסיימנו.

ולכן R שדה.

<u>חוגים פשוטים לא קומוטטיביים:</u>

1. חוג חילוק (אותה הוכחה כמו לשדה), למשל H הקווטרניונים.
2. חוגי מטריצות מעל שדה.

<u>טענה</u>: $M_n(F)$ פשוט
<u>הוכחה</u>:
יהי $I\neq\{0\}$ אידיאל (דו-צדדי) ב $R=M_n(F)$, ניקח $0\neq A\in I$ כלשהי.
קיימים i_0, j_0 כלשהם (מיקום של תא בתוך המטריצה הנ"ל) כך ש $a_{i_0,j_0}\neq 0$ (כלומר תא שאינו אפס) כאשר $A=(a_{i,j})$
נזכיר ש $e_{i,j}$ הם איברי הבסיס של החוג (=מרחב וקטורי במקרה זה) ואז מתקיים לכל i ו j:

$$e_{i,i_0}Ae_{j_0,j}=a_{i_0,j_0}e_{i,j}\in I$$

$$a_{i_0,j_0}^{-1}\in F$$

$$e_{i,j}=(a_{i_0,j_0}^{-1}I_d)a_{i_0,j_0}e_{i,j}\in I$$

ומכאן ברור שכל מטריצה שייכת ל I, כי היא נפרשת ע"י מטריצות הבסיס הסטנדרטי.

ב $M_n(F)$ אין אידיאלים דו צדדיים שונים מ 0 ומהכל אבל יש אידיאלים חד צדדיים כאלה.

<u>אידיאלים מקסימליים</u>
<u>הגדרה</u>
יהי R חוג, אידיאל $I\in R$ נקרא **<u>אידיאל מקסימלי</u>** אם $I\subset R$ (הכלה ממש) ואין אידיאל J שמקיים $I\subset J\subset R$ (הכלה ממש)

<u>טענה</u>
I ב R אידיאל מקסימלי ⇔ R/I הוא חוג פשוט.
<u>הוכחה</u>
ממשפט ההתאמה – יש התאמה חח"ע ועל בין אידיאלים של R/I לאידיאלים $J\in R$ שמכילים את R.

$$J\to J/I\lhd R/I$$

.

R/I פשוט אם"ם יש בו שני אידיאלים:

$$I/I=\{0\} \text{ ו } R/I$$

⇔
יש רק 2 אידיאלים ב R שמכילים את I, וברור שאלו I ו R, וזה נכון אם"ם I אידיאל מקסימלי ב R.

נרצה לאפיין אידיאלים מקסימליים:
<u>מסקנה (מצירוף עם הטענה הקודמת שהוכחנו לגבי חוגים פשוטים)</u>
יהי R חוג קומוטטיבי, ו I אידיאל ב R, אז I אידיאל מקסימלי ⇔ R/I הוא שדה.

דוגמה: $R=\mathbb{Z}$
$I=p\mathbb{Z}$ אידיאל מקסימלי ולכן
$R/I=\mathbb{Z}/p\mathbb{Z}=\mathbb{Z}_p$
מדוע המקסימליות? אם נוסיף עוד איבר a ל $p\mathbb{Z}$ הוא בהכרח יהיה זר ל p ולכן ה gcd שלהם יהיה 1 ואז קיימים x,y כך ש $xa+yp=1$ ולכן $(a)+p\mathbb{Z}=\mathbb{Z}$ והאידיאל מקסימלי.

<u>קיום אידיאלים מקסימליים</u>

<u>משפט</u>
יהי R חוג, אז כל אידיאל $I\neq R$ ניתן להרחבה לאידיאל מקסימלי $I\subseteq J$.

לפני ההוכחה – נקבל מכך מסקנה – שבכל חוג $R\neq\{0\}$ יש אידיאלים מקסימליים.
מדוע? ניקח $I=\{0\}$ ונרחיבו לאידיאל מקסימלי לפי המשפט שנוכיח.

נזכיר מונח מתורת הקבוצות:
<u>הלמה של צורן (1904) – לא נוכיח זאת במסגרת הקורס</u>
תהי X קבוצה לא ריקה סדורה חלקית.
כלומר קיים יחס $\leq$ שהוא טרנזיטיבי, רפלקסיבי ואנטי-סימטרי.
נניח שלכל שרשרת $x_1\leq x_2\leq\ldots\leq x_n\leq\ldots$ יש חסם מלעיל $x\in X$ כך ש $x\geq x_i$ לכל i.
<u>אז</u> יש ב X איבר מקסימלי y, כלומר שאין גדול ממנו (לא בהכרח שבסדר החלקי הוא גדול מכולם, אלא שאין איבר שהוא על פי יחס הסדר גדול ממנו).
במילים אחרות – <u>אין</u> $y\neq z\in X$ כך ש $y<z$.

נשתמש כאן ביחס הסדר של הכלה ובלמה של צורן כדי להוכיח את המשפט שלנו, נעיר כי ללא אקסיומת הבחירה (השקולה ללמה של צורן) לא ניתן להוכיח את קיום האידיאלים המקסימליים תמיד.

יהי I אידיאל ממש ב R.
נגדיר:
$$X=\{J\supseteq I:\ \underbrace{J}_{\text{אידיאל}}\subset R\}$$
נגדיר סדר חלקי על X ע"י הכלה.
נראה שלכל שרשרת ב X יש חסם מלעיל:
תהי הסדרה $I_1\subseteq I_2\subseteq\ldots\subseteq I_n\subseteq\ldots$
ונגדיר $J=\bigcup_{n\geq 1} I_n$
כעת J אידיאל, מדוע?
$x,y\in J\ \Rightarrow\ x\in I_n,\ y\in I_m$
בה"כ נניח n>m ואז נובע ששניהם מוכלים ב I_n ולכן סכומם גם כן.

ברור ש $I\subseteq I_1$ כי $I_1\in X$ ולכן $I\subseteq J$ ו J אידיאל.
נותר להראות $J\neq R$ אחרת 1 מוכל באחד האידאלים בסדרה, ולכן אידיאל זה הוא כבר כל R, בסתירה לכך שאידיאלים ב X מוכלים ממש ב R.

הוכחנו ש X מקיימת את תנאי הלמה של צורן עם יחס ההכלה ולכן יש איבר מקסימלי J ב X, המכיל את I ואין אידיאל שמכיל אותו שאיננו R עצמו.
❑

<u>מסקנות</u>
1. לכל חוג R שאינו $\{0\}$ יש מנה פשוטה.
הוכחה – ניקח I אידיאל מקסימלי ב R ונקבל R/I חוג מנה פשוט.
2. לכל חוג קומוטטיבי שאינו $\{0\}$ יש מנה שהיא שדה (באופן דומה) ומכאן שיש אפימורפיזם:
$\phi: R \to F$
(תמיד ניתן להשתמש בשדה הנוצר ע"י R/I ואז מקבלים איזומורפיזם, בפרט אפימורפיזם)

<u>שאלה</u>
אילו חוגים קומוטטיביים ניתנים לשיכון בשדה?

תנאי הכרחי: אין מחלקי אפס, כי בשדה אין מחלקי אפס והשיכון משמר תכונות אלגבריות.

<u>טענה</u>: כל תחום שלמות (=חוג קומוטטיבי ללא מחלקי אפס) ניתן לשיכון בשדה
אם נוכיח זאת בעצם נענה על השאלה כי אין עוד חוגים קומוטטיביים הניתנים לשיכון בשדה מלבד תחומי שלמות)

<u>הוכחה</u>:
בניית שדה שברים, כמו שבונים את $\mathbb{Q}$ מ $\mathbb{Z}$.
מגדירים את כל הזוגות:
$\{(a,b): a \in R, b \neq 0 \in R\}$
ואז אומרים ש $(a,b) \sim (a_1,b_1)$ אם $a\,b_1 = b\,a_1$
בודקים : זה יחס שקילות.
ואז מסמנים $\frac{a}{b}$ כמחלקת השקילות של (a,b) (כפי שחצי שקול ל $\frac{2}{4}, \frac{9}{18}$ וכו')
מגדירים פעולות:
$$\frac{a}{b} + \frac{a_1}{b_1}$$

$$\frac{a}{b} \cdot \frac{a_1}{b_1}$$

כמו ב $\mathbb{Q}$, בודקים אי-תלות בנציגים ומקבלים חוג ובעצם שדה כי $\left(\frac{a}{b}\right)^{-1} = \frac{b}{a}$

יש מונומורפיזם המוגדר ע"י $a \to \frac{a}{1}$
וזו בעצם הכללה של הרציונליים עבור כל תחום שלמות.

השתמשנו בכך שאין מחלקי אפס בהגדרת הכפל, כי אחרת מתקבל $\frac{a\,a_1}{b\,b_1}$ והמכנה עלול להיות 0, ואז זה לא מוגדר (כי הגדרנו שבר ע"י $b \neq 0$) באופן דומה מגדירים חיבור ע"י מכנה משותף וגם הוא אסור שיתאפס.

<u>מסקנה</u>
חוג R הוא תחום שלמות $\Leftrightarrow$ הוא ניתן לשיכון בשדה

<u>חלוקה בין איברים</u>

יהי R תחום שלמות, $a,b\in R$ שונים מ 0.
אז נגדיר $a|b$ אם קיים $c\in R$ כך ש $b=ac$

נגדיר a חבר של b אם $a|b$ ו $b|a$ –
זה שקול ל $b=au$ כי u הפיך ב R
למשל 5 ו -5 חברים ב $\mathbb{Z}$

מדוע השקילות?
בכיוון הראשון כי נובע $b=au$ ו $u^{-1}\in R$
בכיוון השני נניח ששניהם מחלקים זה את זה ע"י $a=bd,b=ac$ ונקבל:
$b=(bd)c=b(dc)\Rightarrow b(1-dc)=0\Rightarrow 1-dc=0\Rightarrow dc=1$
ולכן c ו d איברים הפוכים.

<u>הגדרה</u>
$a\neq 0\in R$ יקרא אי-פריק אם a אינו הפיך ו $a=xy$ גורר x הפיך או y הפיך.
<u>תנאי שקול</u>
כל מחלק של a הוא הפיך או חבר של a.

<u>הגדרה</u>
$a\neq 0\in R$ יקרא <u>ראשוני</u> אם a לא הפיך ו
$a|xy\Leftarrow a|x$ או $a|y$
<u>דוגמה:</u>
בשלמים אי פריקות שקולה לראשוניות.

<u>שיעור 27</u>

<u>הגדרה</u>
a **מחלק ממש** את b אם $b=ac$ וגם c אינו הפיך.
אם $a|b$ לא ממש אז a,b חברים.

נזכיר כי (x) הוא האידיאל הנוצר ע"י x.

<u>טענה</u>
1. $a|b\Leftrightarrow(b)\subseteq(a)$
2. a מחלק ממש של b $\Leftrightarrow$ מתקיים $(b)\subset(a)$ (הכלה ממש)
3. a,b חברים $\Leftrightarrow$ $(a)=(b)$

<u>הוכחת הטענה</u>:
1.
$(b)\subseteq(a)\Rightarrow b\in(a)\Rightarrow b=ac\Rightarrow a|b$
$a|b\Rightarrow b=ac\Rightarrow b\in(a)\Rightarrow(b)\subseteq(a)$
2, 3 מוכחים באופן דומה.

נזכיר כי:
$a\neq 0$ לא הפיך

a נקרא אי-פריק אם a=xy כאשר x הפיך או y הפיך.
זה שקול : כל מחלק ממש של a הוא הפיך וגם ל: כל מחלק של a הוא חבר של a או הפיך.

a נקרא ראשוני אם:
$a|xy \Rightarrow a|x \vee a|y$
<u>טענה</u>: בכל תחום שלמות, כל איבר ראשוני הוא אי-פריק.

<u>הוכחה</u>:
יהי a ראשוני, נניח a=xy, צ"ל x או y הפיכים.
ברור ש $a|xy$, a ראשוני ולכן $a|x$ או $a|y$.
בה"כ $a|x$ לכן יש $c \in R$ כך ש- $x=ac$ נציב:
$a=xy=(ac)y=a(cy) \Rightarrow a(1-cy)=0$
וכיוון ש $a \neq 0$ נובע $1-cy=0$ כלומר $1=cy$ ומכאן y הפיך כי $c=y^{-1}$

<u>טענה</u>: a ראשוני $\Leftrightarrow$ חוג המנה $R/(a)$ הוא תחום שלמות

<u>הוכחה</u>: נסמן $R'=R/(a)$ ו $x'=x+(a) \in R'$ וכו'.
אז $x'y'=0 \Leftrightarrow (xy)'=0 \Leftrightarrow xy \in (a)$
נניח a ראשוני – ואז מכך ינבע (הפעם נתחיל משמאל לימין):
$a|xy \Leftrightarrow a|x \vee a|y \Rightarrow y \in (a) \vee x \in (a) \Leftrightarrow x'=0 \vee y'=0$
להפך: נניח $R/(a)$ תחום שלמות, נראה a ראשוני.
נניח $a|xy$ אז $xy \in (a)$ ולכן $(xy)'=0'$ לכן $x'=0' \vee y'=0'$ ואז $x \in (a) \vee y \in (a)$
כלומר $a|x \vee a|y$ כנדרש.

<u>טענה</u>
יהי R תחום ראשי: אז $a \in R$ הוא אי-פריק $\Leftrightarrow$ (a) הוא אידיאל מקסימלי $\Leftrightarrow$ $R/(a)$ שדה.

<u>הוכחה</u>
נניח a אי-פריק. נראה שהאידיאל הנוצר על ידו הוא אידיאל מקסימלי.
יהי (b) אידיאל שמכיל את (a).
ראינו שמכאן נובע $b|a$ ומאי-פריקות a נובע ש b חבר של a או הפיך.
אם חבר – הראינו שבמקרה זה נובע a=b ואם הוא הפיך אז הוא הכל, מסגירות לכפל חיצוני (נכפול בהפכי ונקבל 1 ואז נקבל את הכל.

להיפך: נניח (a) אידיאל מקסימלי, נוכיח a אי-פריק.
צ"ל: אם $b|a$ אז b חבר של a או הפיך.
זה שקול ל $(a)=(b)$ או $(b)=R$ וזה נובע ממקסימליות (a) .

הוכחנו את השקילות הראשונה בטענה, והשני כבר הוכח כי I מקסימלי אם"ם R/I שדה (ראינו זאת בשיעור קודם).

<u>טענה</u>
בתחום ראשי כל איבר אי-פריק הוא ראשוני.
a אי פריק $\Leftarrow$ $R/(a)$ שדה $\Leftarrow$ $R/(a)$ תחום שלמות $\Leftarrow$ a ראשוני

מסקנה: אם R תחום ראשי, $a \in R$ אז a אי-פריק $\Leftrightarrow$ a ראשוני.
למשל בשלמים, וגם ב $F[x]$ חוג פולינומים מעל שדה (גם הוא תחום ראשי, נוכיח זאת בתרגיל)

מטרה: פריקות חד-ערכית של איברים כמכפלת אי-פריקים בתחום ראשי.

הכנות:
משפט
יהי R תחום ראשי, אז כל שרשרת עולה של אידיאלים ב R מתייצבת.
כלומר – אם יש:
$I_1 \subseteq I_2 \subseteq \ldots \subseteq I_n \subseteq \ldots$
אז יש m כך ש $I_n = I_m$ לכל $n > m$.
הערה: חוג עם תכונה זו נקרא **חוג נתר**. ע"ש אמי נתר (Noether).

הוכחת המשפט
תמיד כשיש שרשרת הטריק הוא לקחת את האיחוד של איברי השרשרת וגם הוא אידיאל.
נגדיר $I = \bigcup_{n \geq 1} I_n$ ואז I אידיאל. לכן I ראשי, כלומר $I = (a)$ לאיזה $a \in R$.
$a \in I$ ולכן a שייך לאחד המאוחדים, כלומר עבור I_m לאיזה m, ולכן $I = (a) \subseteq I_m$ וההכלה בכיוון השני טריוויאלית (כי I הוא איחוד של כולם) ולכן $I_m = I$, כלומר החל מ m השרשרת מתייצבת וכל סימני ההכלה הופכים לסימני שוויון.

מסקנה: תחום ראשי הוא חוג נתר.
תוצאה: תחום ראשי מקיים את תנאי שרשרת המחלקים שאומר:
אין סדרה אינסופית כך ש: $a_1, a_2, \ldots, a_n, \ldots$ כאשר a_{n+1} מחלק ממש את a_n
(מדוע? ניקח סדרת אידאלים הנוצרת ע"י הסדרה ונקבל שהיא מתייצבת, ולכן ממקום מסויים אין הכלות ממש)

שיעור 28
הערה: בעצם הראינו שכל חוג נתר מקיים את תנאי שרשרת המחלקים.

למה 1: יהי R תחום שלמות המקיים תנאי שרשרת המחלקים – אז כל $0 \neq a \in R$ לא הפיך מתחלק באיבר אי-פריק.
הוכחה
אם a עצמו אי-פריק גמרנו.
אחרת – יש ל a מחלק ממש לא-הפיך.
תזכורת: a אי-פריק $\Leftrightarrow$ אין ל-a מחלק ממש לא הפיך.
אם a_1 אי-פריק גמרנו, אחרת יש ל a_1 מחלק ממש לא הפיך a_2 . נמשיך כך ונקבל סדרה כך שכל איבר בה מחלק ממש את קודמו. מתנאי שרשרת המחלקים נובע שהסדרה סופית ולכן קיים a_n קונקרטי אי-פריק ו $a_n | a$ כנדרש אי-פריק.

למה 2: יהי R תחום שלמות המקיים את תנאי שרשרת המחלקים, אז כל $0 \neq a \in R$ לא-הפיך ניתן להצגה כמכפלה של איברים אי-פריקים.

הוכחה
עפ"י למה 1 יש אי-פריק p_1 כך ש $p_1 | a$ ואז נכתוב $a = p_1 a_1$. אם a_1 הפיך אז $a = a_1 p_1$ גם כן אי-פריק, ($a \sim p_1$ במקרה זה וחבר של אי-פריק הוא אי-פריק) ואין מה להוכיח.
לכן נניח ש a_1 לא אי-פריק ואז מלמה 1 יש $p_2 | a_1$ אי-פריק, ונכתוב $a_1 = p_2 a_2$.
אם a_2 הפיך אז a_1 אי פריק (חבר של p_2) ו $a = p_1 a_1$ מכפלת אי-פריקים, אחרת נמשיך באותו אופן ונקבל סדרות p_n a_n כך ש $a_{n-1} = p_n a_n$ ולכן a_n מחלק ממש של a_{n-1} .
מתנאי שרשרת המחלקים זו תהיה סדרה סופית ולכן באיזהשהו שלב יסתיים התהליך ונקבל שקיים n כלשהו כך ש a_n

הפיך ומתקיים -
$a=p_1a_1=p_1(p_2a_2)=\ldots=p_1p_2\ldots p_na_n$
ולכן במכפלה האחרונה נקבל מכפלת אי-פריקים, $p_1\cdots p_{n-1}$ ברור למה, ואילו p_na_n אי פריק כחבר של אי-פריק.

הוכחנו <u>קיום</u> הצגה של איבר כמכפלת אי-פריקים (בחוג נתרי) נעסוק ב<u>יחידות</u> הפרוק עד כדי חברות.

<u>למה 3</u>: יהי R תחום שלמות בו כל איבר אי-פריק הוא ראשוני.
נניח $\prod_{i=1}^{n}p_i=\prod_{i=1}^{m}q_i$ כאשר p_i,q_j אי-פריקים אז n=m ועד כדי שינוי סדר $p_i\sim q_i$.
<u>הוכחה</u>:
אינדוקציה על $n\geq 1$.
עבור $n=1$
$p_1=\prod_{i=1}^{m}q_i$
הערה:
p ראשוני אז $p|x_1\cdot\ldots\cdot x_m$ גורר $p|x_i$ לאיזהשהו i.
ל $m=2$ זוהי ממש הגדרה של איבר ראשוני, ול $m>2$ זה קל להראות באינדוקציה.

p_1 אי-פריק ולכן ראשוני (מההנחה על R) ומתקיים $p_1|\prod_{i=1}^{m}q_i$ ולכן קיים i כך ש $p_1|q_i$
בה"כ (אחרת נשנה את סדר המכפלה – שזה מותר כי ההוכחה היא עד כדי שינוי סדר) נניח i=1.
כלומר $p_1|q_1$
q_1 אי-פריק, p_1 מחלק לא הפיך של q_1 ולכן חבר של q_1 , $p_1\sim q_1$

$$p_1=q_1\underbrace{u}_{\text{הפיך}}=q_1(q_2q_3\ldots q_m)\ \Rightarrow\ \underbrace{q_1}_{\neq 0}\underbrace{(q_2q_3\ldots q_m-u)}_{=0}=0$$

ואז נובע שהמכפלה הפיכה (כי u הפיך והם שווים)/
אם $m\geq 2$ נקבל סתירה כי $q_2,\ldots,q_m|u$ ולכן גם הם הפיכים ואם כך – לא אי-פריקים.
מסקנה $m=1$ ולכן $p_1\sim q_1$ זה מוכיח את תחילת האינדוקציה עבור n=1.

נניח n>1 ואז נקבל $p_1\cdot\ldots\cdot p_n=q_1\cdot\ldots\cdot q_m$ ואז p_1 מחלק את המכפלה ולכן מחלק אחד מאיברי המכפלה, בה"כ הראשון, ומכך שגם q_1 אי פריק ונובע כמקודם $p_1\sim q_1$

$q_1=p_1\underbrace{u}_{\text{הפיך}}$ ונוכל להציב:
$\cancel{p_1}\cdot\ldots\cdot p_n=(\cancel{p_1}u)\cdot\ldots\cdot q_m$
$p_2\cdot\ldots\cdot p_n=\underbrace{(p_2u)}_{\text{אי פריק}}\cdot\ldots\cdot q_m$
וקיבלנו בשני האגפים מכפלות באורך n-1 ו m-1 ומהנחת האינדוקציה נובע כי עד כדי שינוי סדר מתקיימת הטענה.
ולכן n=m וגם $p_i\sim q_i$ לכל i. (עבור i=2 נשתמש ב $p_2\sim uq_2q_2$ ובטרנזיטיביות החברות)

<u>משפט</u>
יהי R תחום שלמות המקיים את תנאי שרשרת המחלקים בו כל אי-פריק הוא ראשוני אז לכל איבר איבר ב R שהוא לא הפיך ושונה מאפס יש הצגה כמכפלת אי-פריקים והצגה זו יחידה עד כדי שינוי סדר וחברות.

<u>הוכחה</u>
למה 2 נותנת קיום, למה 3 נותנת יחידות.
<u>סימון</u> נקרא לתכונה הנ"ל **<u>פריקות חד-ערכית</u>**

מסקנה – בתחום ראשי יש פריקות חד-ערכית.

דוגמאות:
1. $\mathbb{Z}$ השלמים
2. $F[x]$ - חוג פולינומים מעל שדה.

בפרט: כל פולינום הוא מכפלה של פולינומים אי-פריקים.

$F[x,y]$ חוג הפולינומים מעל שדה F ב 2 משתנים. איבריו הם $\sum a_{i,j}x^i y^j$ כאשר $a_{i,j}\in F$
זהו לא תחום ראשי, למשל האידיאל הנוצר ע"י x ו y (כפולינומים) אינו ראשי (לא קשה במיוחד והראינו בתרגיל) בכל זאת ניתן להראות שיש פריקות חד-ערכית בחוג $F[x,y]$.

<u>סימון כללי לאידיאל הנוצר</u>
בחוג קומוטטיבי R אם $a_1,\dots a_n$ איברים בחוג, מסמנים את האידיאל הנוצר על ידם באופן הבא:

$$(a_1,\dots,a_n)=a_1R+\dots+a_nR=\left\{\sum_{i=1}^{n}a_ib_i \;:\; b_i\in R\right\}$$

זהו אידיאל הנוצר ע"י האיברים הללו והוא המינימלי (ביחס להכלה) המכיל אותם.

<u>פולינומים ושורשיהם</u>
חילוק עם שארית ב $F[x]$
לכל f,g אם $g\neq 0$ יש q ו r יחידים כך ש:
$$f=q\cdot g+r$$
$$deg(r)<deg(g)$$
כאשר מוגדר
$$deg(0)=-\infty$$
ונזכיר כי
$$deg(fg)=deg(f)+deg(g)$$

למה 1:
יהי $f(x)\in F[x]$, $a\in F$ אז
1. $f(x)=(x-a)q(x)+f(a)$ ל $q(x)\in F[x]$
2. $f(a)=0\Leftrightarrow x-a\,|\,f(x)$

<u>הוכחה</u>
נחלק את $f(x)$ ב $x-a$ עם שארית ונקבל: $f(x)=(x-a)q(x)+r(x)$ ואז $deg(r)<deg(x-a)=1$
ולכן יתכן ש r הוא מקדם חופשי או פולינום האפס, ובכל מקרה הוא פולינום קבוע, נסמן את ערכו בכל נקודה c.
נציב x=a בחלוקה בשארית שרשמנו ונקבל:
$$f(a)=(a-a)q(x)+c=c$$
2 ברור ונובע מההצבה האחרונה (השארית היא בדיוק $f(a)$)

<u>טענה</u> – ל $f(x)$ יש לכל היותר n שורשים אם $n=deg(f)$

<u>הוכחה</u> : אינדוקציה על $n\geq 0$
$n=0, f(x)=c$
אז יש 0 שורשים (עבור c שונה מאפס)

מעבר האינדוקציה:
נניח $n\geq 1$ אם אין שורשים ל f סיימנו, אחרת יהי a שורש אז $x-a|f(x)$ ולכן $f(x)=(x-a)\cdot q(x)$ כך ש
$deg(q)=n-1$ ובאינדוקציה יש ל q לכל היותר n-1 שורשים.
שורשי f הם שורשי q וכן a ולכל לכל היותר n שורשים.

<u>משפט</u> – יהי F שדה סופי, אז החבורה הכפלית F^* היא ציקלית. רעיון ההוכחה – שימוש בטענה הקודמת.
בשיעור הבא נראה איך בונים שורש לפולינום בשדה הרחבה.

<u>שיעור 29</u>
נגדיר כי **<u>מעריך=אקספוננט של חבורה</u>** הוא ה m המינימלי שעבורו לכל $x\in G$ מתקיים $x^m=1$, זוהי גם הכפולה המשותפת המינימלית של סדרי האיברים.
כמובן $m||G|$ כי $x^{|G|}=1$ לכל x.

נמשיך את הוכחת המשפט מסוף השיעור הקודם:
תהי G החבורה הכפלית של F.
יהי m המעריך של G.
אז כל איבר ב G מקיים $x^m-1=0$ ב F (שהרי G היא F בלי 0). קיבלנו פולינום ממעלה m עם לפחות $|G|$ שורשים ב F. ממשפט קודם נובע $|G|\leq m$ ולכן $|G|=m$ (כי גם $m\leq|G|$ לפי טענה קודמת).
<u>מסקנה</u>: G היא חבורה אבלית סופית שהמעריך שלה = גודל שלה
<u>תרגיל</u>: חבורה כנ"ל היא בהכרח ציקלית.
<u>תוצאה</u>: $\mathbb{Z}_p^*$ ציקלית לכל p ראשוני, למשל $\mathbb{Z}_7^*$ - 3 הוא יוצר שלה.

<u>טענה</u> יהי $p(x)\in F[x]$ פולינום אי-פריק.
יהי $E=F[x]/(p(x))$ אז E הוא שדה, ו $F\subseteq E$ (כשיכון טבעי), ו E הוא מרחב וקטורי מעל F ממימד $d=deg(p)$

<u>הוכחה</u>
ראינו שבכל תחום ראשי R, אם $a\in R$ אי-פריק אז (a) הוא אידיאל מקסימלי ולכן $R/(a)$ הוא שדה. בפרט $E=F[x]/(p(x))$ הוא שדה. איבריו הם:
$$a_0+a_1x+...+a_{d-1}x^{d-1}+(p(x)) \qquad a_i\in F \qquad d=deg(p)$$
ניתן לזהותם עם הפולינומים ממעלה קטנה מ d מעל F עם פעולות מודולו $p(x)$ ולכן ניתן לשכן את F ב E, ומתקיים ש $\{1,x,...,x^{d-1}\}$ בסיס ל E מעל F.

כפל בסקלר לא תלוי בנציגים כי עבור $\lambda\in F$ מתקיים ש:
$$\lambda(g(x)+(p(x)))=\lambda g(x)+(p(x))$$

<u>משפט</u>
יהי $p(x)$ פולינום אי-פריק, נגדיר $E=F[x]/(p(x))$ כמקודם, אז יש $\alpha\in E$ כך ש $p(\alpha)=0$, כלומר E

הוא שדה הרחבה ל F בו יש ל $p(x)$ שורש.

<u>הוכחה</u>
ניקח $\alpha = x + (p(x)) \in E$
אם $p(x) = \sum_{i=0}^{d} b_i x^i$

$$p(\alpha) = \sum b_i \alpha^i = \sum b_i (x + p(x))^i = \sum b_i (x^i + p(x)) = (\sum b_i x^i) + (p(x)) = p(x) + (p(x)) = (p(x)) = 0$$

<u>מסקנה:</u> לכל פולינום לא קבוע יש שורש בשדה הרחבה כלשהו ממימד סופי.
<u>הוכחה</u>: נכתוב אותו כמכפלת אי-פריקים, נמצא שדה לפי המשפט הקודם בו לראשון מביניהם יש שורש ונקבל שזה מאפס את הפולינום שלנו.

<u>משפט קרוניקר</u>
לכל פולינום לא קבוע $f(x) \in F[x]$ יש שדה הרחבה ממימד סופי $F \subseteq E$ (גם כאן זה שיכון ולא הכלה) כך שמעליו f יהיה מכפלת גורמים ליניאריים, כלומר $n = deg(f)$ $f(x) = c(x_1 - \alpha_1) \cdot \ldots \cdot (x - \alpha_n)$

<u>הוכחה</u>
באינדוקציה על הדרגה של הפולינום.
עבור n=1 זה מתקיים כי f בעצמו ליניארי.
מעבר האינדוקציה: נשתמש במסקנה הקודמת למצוא $F \subseteq E_1$ ו $\alpha_1 \in E_1$ כך ש $f(\alpha_1) = 0$ ואז ידוע שבחוג הפולינומים $E_1[x]$ מתקיים $x - \alpha_1 | f(x)$, כלומר: $f(x) = (x - \alpha_1) f_1(x)$ עבור $f_1(x) \in E_1[x]$ כלשהו.
$Deg(f_1) < n$ ולכן נשתמש בהנחת האינדוקציה ו f_1 יתפצל לגורמים ליניאריים בשדה הרחבה של E_1 כלשהו שנסמנו E . ואז מחד יתקיים ש $F \subseteq E$ ומאידך:
$f = (x - \alpha_1) c (x - \alpha_2) \cdot \ldots \cdot (x - \alpha_n)$
במקרה זה אומרים ש f <u>מתפצל</u> מעל E או ש-E הוא <u>שדה פיצול</u> של f.