מבוא

שמות לקבוצות מוכרות:

$\mathbb{N}$ = המספרים הטבעיים.

$\mathbb{Z}$ = המספרים השלמים.

$\mathbb{Q}$ = המספרים הרציונאליים.

$\mathbb{R}$ = המספרים הממשיים.

$\mathbb{C}$ = המספרים המרוכבים.

A , קבוצת מספרים ממשיים, אז: A^+ = המספרים האי-שליליים ב- A .

A^- = המספרים האי-חיוביים ב- A .

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

אינדוקציה:

כדי להוכיח טענה עבור מספרים טבעיים יש:

- א. להוכיחה עבור $n=1$.

  ב. מתוך נכונות ל- k , להוכיח ל- $k+1$.

- א. להוכיחה עבור $n=1$.

  ב. מתוך נכונות לכל $n>k$, להוכיח נכונות ל- n .

אם א+ב מתקיימים, הטענה נכונה לכל n טבעי.

עיקרון הסדר הטוב: בכל תת קבוצה לא ריקה של המספרים הטבעיים יש איבר קטן ביותר.

תכונות של מספרים שלמים:

משפט פירוק יחיד לשארית: לכל שני מספרים $b<a$ קיימים q,r יחידים כך ש: $a=bq+r$ $(0\le r<a)$.

צירוף שלם: יהיו $a,b\in\mathbb{Z}$. המספר $\alpha a+\beta b$ נקרא צירוף שלם של a ו- b כאשר המקדמים שלמים.

משפט: לכל $b,a\in N$ מתקיים:

$$c\mid a\rightarrow\exists q_1:a=cq_1$$
$$c\mid b\rightarrow\exists q_2:b=cq_2$$
$$\alpha a+\beta b=\alpha cq_1+\beta cq_2=c(\alpha q_1+\beta q_2)\rightarrow c\mid\alpha a+\beta b$$

תוצאות מיידיות:

- לכל $a\in\mathbb{Z}$ מתקיים: $1\mid a$.
- לכל $a\neq 0$ מתקיים: $a\mid 0$.
- $a=\pm 1\leftarrow a\mid 1$
- $a\mid c\leftarrow\begin{cases}a\mid b\\ b\mid c\end{cases}$ (טרנזיטיביות).
- $a=\pm b\leftarrow\begin{cases}a\mid b\\ b\mid a\end{cases}$
- אם $a\mid b$ וגם $a\mid c$ אז: $a\mid\alpha b+\beta c$ עבור כל α,β.

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

משפט פירוק של מספרים טבעיים: יהא n טבעי גדול מ-1. אז: $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ כאשר $p_1, p_2, \ldots, p_k$ מספרים ראשוניים שונים. אז הפירוק הוא חד-ערכי.

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

טענה: הקבוצה Z_p הינה שדה אם"ם p ראשוני.

המחלק המשותף המקסימאלי (gcd): יהיו $a,b \in \mathbb{Z}$. אז הממג"ב (מחלק משותף גדול ביותר) שלהם יסומן: $(a,b) = \gcd(a,b) = d$ וגם מתקיים:

- $d > 0$.
- $d \mid a$ וגם $d \mid b$.
- אם $c \in \mathbb{Z}$ וגם $c \mid a,\ c \mid b$ אז: $c \mid d$.

דגש: d הוא תמיד מספר חיובי.

ביטוי ע"י פירוק לראשוניים: $(a,b) = p_1^{\min\{i_1,j_1\}} p_2^{\min\{i_2,j_2\}} \cdots p_k^{\min\{i_k,j_k\}}$.

הערה: $a,b \in \mathbb{Z}$ אם $(a,b) = 1$ אז a,b הם מספרים זרים.

טענה: a,b זרים אם"ם קיימים מספרים x,y כך שמתקיים: $ax + by = 1$.

האלגוריתם של אוקלידס:

$$b = aq_1 + r_1 \qquad (r_1 < a)$$
$$a = r_1 q_2 + r_2 \qquad (r_2 < r_1)$$
$$r_1 = r_2 q_3 + r_3 \qquad (r_3 < r_2)$$
$$\vdots$$
$$r_{k-2} = \boxed{r_{k-1}} q_k + r_k \,(=0)$$

יהיו $a,b \in \mathbb{Z}$ ונניח בה"כ ש: $0 < a < b$. אז:

האלגוריתם מסתיים כאשר מקבלים שארית אפס.

טענה: r_{k-1} הוא המחלק המשותף המקסימאלי.

משפט: אם $d = (a,b)$ אז קיימים $\alpha, \beta \in \mathbb{Z}$ כך ש: $d = \alpha a + \beta b$.

הכפולה המשותפת הקטנה ביותר (lcm): יהיו $a,b \in \mathbb{Z}$. אז הכמק"ב שלהם יסומן: $[a,b] = c$ וגם:

- $c > 0$.
- $a \mid c,\ \ b \mid c$.
- אם קיים $e \in \mathbb{Z}$ כך ש $a \mid e,\ b \mid e$ אז: $c \mid e$.

ביטוי ע"י פירוק לראשוניים: $(a,b) = p_1^{\max\{i_1,j_1\}} p_2^{\max\{i_2,j_2\}} \cdots p_k^{\max\{i_k,j_k\}}$.

יחס שקילות:

יחס שקילות בקבוצה A הוא "קשר" בין חלק מאברי הקבוצה, סימון: $R,\sim$. כך שמתקיים:

יחס רפלקסיבי: R נקרא יחס רפלקסיבי אם"ם: $\forall a\in A: aRa$ (a קשור לעצמו).

יחס סימטרי: R נקרא יחס סימטרי אם"ם: $aRb\to bRa$.

יחס טרנזיטיבי: R נקרא יחס טרנזיטיבי אם"ם: $aRb\wedge bRc\to aRc$.

דוגמא: תהי $A=Z$. נגדיר יחס על Z: $a\equiv b\left(\mathrm{mod}\,n\right)\Leftrightarrow n\mid a-b\Leftrightarrow a=b+kn$,

כלומר: ההפרש בין a ל- b מתחלק ל- n.

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

אומרים ש- a קונגרואנטי ל- b מודולו n ומסמנים: $a\equiv b\left(\mathrm{mod}\,n\right)\Leftrightarrow n\mid a-b$.

משפט: אם $a\equiv b\left(\mathrm{mod}\,n\right)$ ו- $c\equiv d\left(\mathrm{mod}\,n\right)$ אז:

א. $a+c\equiv b+d\left(\mathrm{mod}\,n\right)$.

ב. $a\cdot c\equiv b\cdot d\left(\mathrm{mod}\,n\right)$.

ג. $a^t\equiv b^t\left(\mathrm{mod}\,n\right)$, $t\in\mathbb{N}$.

ד. $\alpha a\equiv\alpha b\left(\mathrm{mod}\,n\right)$, $\alpha\in\mathbb{Z}$.

מחלקת שקילות:

יהי R יחס שקילות על קבוצה A ויהי $a\in A$. נסמן: $[a]=\{x\in A\mid aRx\}$ - מחלקת השקילות של a (וזוהי קבוצת כל האיברים שהם ביחס שקילות עם a).

טענה: $a\in[a]$ (כי יחס שקילות הוא רפלקסיבי).

משפט: יהי R יחס שקילות על קבוצה A.

1. לכל $a,b\in A$ מתקיים: $[a]=[b]$ או $[a]\cap[b]=\varnothing$.
2. {איחוד כל מחלקות השקילות הזרות} = A.

הופכי מודולו n: יהי $a\in\mathbb{Z}$. ל- a יש הופכי מודולו n אם קיים a' כך ש- $a\cdot a'=1\left(\mathrm{mod}\,n\right)$.

סימון: $a'=a^{-1}$.

דוגמא: ההופכי של 7 מודולו-12 הוא: $7\cdot a^{-1}=1\left(\mathrm{mod}\,12\right)\to a^{-1}=7$.

משפט: ל- a יש הופכי מודולו n אם"ם: $\left(a,n\right)=1$ (הם מספרים זרים).

מציאת המספר ההופכי: נמצא את הצירוף השלם של a ו- n שנותן-1. המקדם של a בצירוף הוא a^{-1}.

מספר נגדי: מספר נגדי של a הוא מספר b המקיים: $a+b=0$.

ב- Z_n הנגדי של a הוא: $n-a$ כי: $a+\left(n-a\right)=n\equiv 0$.

טענה: ב-Z_n יש בדיוק n מחלקות שקילות שונות.

נגדיר ב-Z_n שתי פעולות: $\begin{cases}\overline{a}\oplus\overline{c}=\overline{a+c}\\ \overline{a}\otimes\overline{c}=\overline{a\cdot c}\end{cases}$

- החיבור והכפל ב-Z_n נעשים מודולו n.
- החיבור והכפל אינם תלויים בבחירת הנציגים.

תכונות ב-Zn:

- קומוטטיביות בכפל ובחיבור.
- אסוציאטיביות בכפל ובחיבור.
- איבר אדיש חיבורי ב-Z_n - $\overline{0}$.
- איבר אדיש כפלי ב-Z_n - $\overline{1}$.
- איבר נגדי: הנגדי למחלקה $\overline{i}$ הוא $\overline{n-i}$.
- איבר הופכי בכפל לא תמיד קיים לכל איבר. קיים רק כאשר Z_p ו-p ראשוני.

מסקנה: ב-Z_n יש הופכי לאיבר i אם"ם $(i,n)=1$.

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

חבורות

הגדרת חבורה: תהי $G \neq \varnothing$ ותהי * פעולה בינארית המוגדרת על אברי G. G נקראת חבורה ביחס לפעולה * אם:

1. ב-G יש סגירות לפעולה *: $a,b \in G$ אז: $a*b \in G$.
2. הפעולה אסוציאטיבית: $a,b,c \in G$ אז: $(a*b)*c = a*(b*c)$.
3. קיים ב-G איבר "אדיש" לפעולה (איבר יחידה) המסומן ע"י e המקיים: $\forall a \in G : a*e = e*a = a$.
4. לכל $a \in G$ יש הופכי $a^{-1} \in G$ כך ש: $a^{-1}*a = a*a^{-1} = e$.

הערה: בד"כ $a*b \neq b*a$.

חבורה אבלית: אם $a*b = b*a$ לכל $a,b \in G$. נקראת גם חבורה קומוטטיבית.

דוגמאות חשובות לחבורות:

- לכל שדה F $(\mathbb{Q},\mathbb{R},\mathbb{C})$, $(F,+)$ היא חבורה אבלית. $e=0$, $x^{-1}=-x$.
- $F^* = F \setminus \{0\}$, $(F^*,\bullet)$ היא חבורה אבלית. $e=1$, $x^{-1}=\frac{1}{x}$.

הערה: הסגירות לא נפגעה כי לא תיתכן מכפלת מספרים שונים מ-0 שתהיה 0.

- לכל מרחב וקטורי V, $(V,+)$ היא חבורה אבלית.
- $(\mathbb{Z},+)$ היא חבורה אבלית. $e=0$, $x^{-1}=-x$.
- $(\mathbb{Z},\bullet)$ איננה חבורה (אבל כן אבלית). אין הופכי לאף איבר פרט ל± 1.
- nZ=הכפולות של n = $\{0,\pm n,\pm 2n,\ldots\}$. חבורה אבלית לגבי +.
- $A=\{x \in \mathbb{C} \mid |x|=1\}$, $(A,\bullet)$ היא חבורת שורשי היחידה (מספרים מרוכבים על מעגל ברדיוס 1 מהראשית).
- $B=\{f : F \to F \mid f \text{ is a function}\}$ ונגדיר: $(f+g)(x)=f(x)+g(x)$. אז: $(B,+)$ זו חבורה. $e=f(x)\equiv 0$, $f^{-1}(x)=-f(x)$.
- Z_n היא חבורה ביחס לחיבור מחלקות (מודולו n). $x^{-1}=n-x$, $e=0$.
- $U_n = \{a \in Z_n \mid (a,n)=1\}$. U_n היא חבורה אבלית ביחס לכפל מחלקות (מודולו n).

קיום הופכי נובע מהמשפט: $(a,n)=1 \leftrightarrow$ ל-a יש הופכי מודולו n.

- חבורת ה-4 של קליין: $\{e,a,b,a\cdot b\}$. $a^2=b^2=e$, $a\cdot b = b\cdot a$.
- $F^{m,n}$ - אוסף המטריצות מסדר $m\times n$ מעל F. $F^{m,n}$ חבורה אבלית ביחס לחיבור מטריצות.

חבורות לא קומוטטיביות:

- $GL(n,F)$ - אוסף המטריצות הממשיות ההפיכות מסדר $n\times n$. זו חבורה ביחס לכפל מטריצות.
- $SL(n,F)$ - כל המטריצות מסדר $n\times n$ עם דטרמיננטה שווה ל-1. חבורה לגבי כפל מטריצות.

תכונות בסיסיות בחבורה:

תהי G חבורה ביחס לפעולה $*$ אז:

1. האדיש הוא יחיד.
2. לכל איבר יש הופכי יחיד.
3. חוקי צמצום: $a*b=a*c \leftarrow b=c$ (צמצום משמאל).
   $a*c=b*c \leftarrow a=b$ (צמצום מימין).
   הערה: אם $a*b=b*c$ זה לא גורר $a=c$.
4. למשוואות: $\begin{cases} a*x=b & \xrightarrow{a^{-1}(\ )} \quad x=a^{1}*b \\ y*a=b & \xrightarrow{(\ )a^{-1}} \quad y=b*a^{-1} \end{cases}$ יש פיתרון יחיד.

חבורה סופית: G חבורה סופית אם מספר האיברים ב-G הוא סופי. הסדר של חבורה סופית הוא מספר האיברים בה.

דוגמאות: $|S_n|=n!$, $|Z_n|=n$, פונקציית אויילר- $|U_n|=\varphi(n)$.

חזקות: $\boxed{a^k=a^{k-1}*a}$ $a^0=e,\quad a^1=a,\quad a^2=a*a,\ \ldots,$

תכונות:

- $a^m*a^n=a^{m+n}$.
- $\left(a^m\right)^n=a^{m\cdot n}$.
- $\left(a^{-1}\right)^{-1}=a$
- $\left(a^{-1}\right)^m=\left(a^m\right)^{-1}$.
- $(a*b)^{-1}=b^{-1}*a^{-1}$ $((a*b)^n\neq a^n*b^n)$.

משפט: בטבלת כפל של חבורה סופית, מופיעים כל איברי החבורה פעם אחת בדיוק.

משפט: קבוצה G עם סגירות ואסוציאטיביות תהיה חבורה אם יתקיימו:

1. קיים $e\in G$ כך ש: $\forall a\in G,\ ae=a$.
2. לכל $a\in G$, קיים $b\in G$ כך ש: $ab=e$.

תמורות:

S_A - החבורה הסימטרית על A. אברי החבורה הן הפונקציות החח"ע ועל מ-A על A והפעולה היא הרכבת פונקציות. הערה: אם $A=\{1,2,3,\ldots,n\}$ אז מסמנים: $S_A=S_n$.

S_n היא חבורה לא אבלית ביחס להרכבת פרמוטציות. $(\theta\cdot\sigma)(i)=\theta(\sigma(i))$.

טענות לגבי הרכבת פונקציות:

- אם f,g הן חח"ע ועל אז גם $f\circ g$ היא חח"ע ועל.
- אסוציאטיביות: $f\circ(g\circ h)=(f\circ g)\circ h$.
- I-פונקצית הזהות, $(f\circ I)(x)=f(I(x))=f(x),\quad (I\circ f)(x)=I(f(x))=f(x)$.
- לכל f חח"ע ועל יש f^{-1} ועל כך ש: $f\circ f^{-1}=f^{-1}\circ f=I$.

תת-חבורה:

תהי G חבורה ביחס לפעולה $*$. תהי $H \neq \varnothing$ תת-קבוצה של G. H נקראת תת-חבורה של G אם H היא חבורה ביחס לפעולה $*$. סימון: $H \prec G$.

טענה-1: תהי G חבורה ביחס לפעולה $*$. H היא תת-חבורה אם:

1. $H \neq \varnothing$
2. ב-H יש סגירות לפעולה $a,b \in H \leftarrow a*b \in H$.
3. ב-H יש סגירות להופכי $a \in H \leftarrow a^{-1} \in H$.

טענה-2: תהי G חבורה ביחס לפעולה $*$. $H \subset G$ היא תת-חבורה אם:

1. $e \in H$ (נובע מכך ש-$H \neq \varnothing$).
2. H סגורה ל"חילוק" $a,b \in H \leftarrow a*b^{-1} \in H$ (כולל בתוכו סגירות להופכי וקיום אדיש).

תת-חבורה טריוויאלית: G ו-$\{e\}$.

דוגמא: ת"ח של $(\mathbb{Z},+)$: $n\mathbb{Z} = \{nx : x \in \mathbb{Z}\}$. ואלו הת"ח היחידות של $\mathbb{Z}$.

טענות חשובות:

- חיתוך של תת חבורות של G הוא גם תת-חבורה של G.
- אם H תת-חבורה של G ולוקחים איבר $g \in G$ אזי גם $g^{-1}Hg$ תת חבורה של G.

משפט: תהי G חבורה סופית. אז לכל $a \in G$ קיים $k \in \mathbb{N}$ כך ש-$a^{-1} = a^k$.

הערה: ולכן כדי שתת-קבוצה $H \neq \varnothing$ תהיה ת"ח של G, **מספיק לבדוק סגירות לפעולה** ואין צורך לבדוק סגירות להופכי.

חבורות ציקליות:

הגדרה: תהי G חבורה יהי $a \in G$, נגדיר: $< a >= \{a^s : s \in \mathbb{Z}\}$. כאשר G סופית, ניתן להשמיט חזקות שליליות: $< a >= \{e, a, a^2, \ldots, a^{o(a)-1}\}$.

טענה: $< a >$ היא ת"ח של G, והיא הת"ח המינימאלית המכילה את a, כלומר: כל ת"ח המכילה את a מכילה גם את $< a >$.

$< a >$ נקראת הת"ח הנוצרת ע"י a.

דוגמאות:

- $(\mathbb{Z},+)$: $\mathbb{Z} =< 1 >=< -1 >$ (כל מספר ב-$\mathbb{Z}$ ניתן ליצור ע"י חיבור של 1 או של -1).

  $\mathbb{Z}$ היא חבורה ציקלית אינסופית הנוצרת מ-1 או מ-1-.

  $n\mathbb{Z}$ היא ת"ח ציקלית אינסופית הנוצרת ע"י n.

- $(\mathbb{C},\bullet)$: $H = \{z \in C^* : z^n = 1\}$ - קבוצת שורשי היחידה מסדר n.

  $H =< \omega >$, $\omega = \cos\left(\frac{2\pi}{n}\right) + i\sin\left(\frac{2\pi}{n}\right)$ - ת"ח ציקלית מסדר n ($\{\omega, \omega^2, \omega^3, \ldots, \omega^n\}$).

- $U_{10} = \{1,3,7,9\}$. U_{10} היא חבורה ציקלית הנוצרת ע"י 3 וגם נוצרת ע"י 7.

  $< 3 >= 3^1 = 3,\ 3^2 = 9,\ 3^3 = 7,\ 3^4 = 1$ $\quad < 7 >= 7^1 = 7,\ 7^2 = 9,\ 7^3 = 3,\ 7^4 = 1$

משפט: תהי G חבורה ציקלית, אז כל ת"ח של G היא גם ציקלית.

משפט: תהי G חבורה ציקלית מסדר-n. אז לכל: $m \mid n$ יש ת"ח ציקלית מסדר m (והיא יחידה).

יצירת ת"ח מסדר m: $o\left(a^{n/m}\right)=\frac{n}{\left(n,n/m\right)}=\frac{n}{n/m}=m$ והיא נוצרת ע"י: $< a^{n/m} >$.

טענה: חבורה ציקלית היא חבורה אבלית.

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

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

דוגמא: $U_{10}=\{1,3,7,9\}$, $o(1)=1,\ o(3)=4,\ o(7)=4,\ o(9)=2$.

הערות:

- $o(a)=1$ אמ"מ: $a=e$.
- $o(a)=|<a>|$ (הסדר של a הוא מספר החזקות השונות של a עד שמגיעים שוב ל-e).
- אם $o(a)=|G|$ אז G ציקלית ו-a יוצר אותה.

טענה: אם $a^m=e$ אז: $o(a)\mid m$.

טענה: אם $|G|=n$, $o(a)=n$ אז: $o\left(a^k\right)=\frac{n}{(n,k)}$.

מסקנה: $o(a)=o\left(a^k\right)$ אמ"מ: $(n,k)=1$.

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

תכונות:

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

טענה: מספר היוצרים של חבורה ציקלית מסדר n הוא: $\varphi(n)$.

משפט לגרנז'

לגרנז:

משפט לגרנז': תהי G חבורה סופית ותהי $H \prec G$. אזי: $|H| \mid |G|$ (מספר האיברים ב- H מחלק את מספר האיברים ב- G).

הערה: למעשה- $|G| = |H| \cdot [G:H]$.

טענה: כל חבורה מסדר ראשוני היא ציקלית וכל איבר מהחבורה השונה מ- e הוא יוצר שלה.

מסקנה: G חבורה סופית, $a \in G$, אזי: $o(a) \mid |G|$.

קוסטים:

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

קוסט ימני (מחלקה ימנית) של H ב- G: $Ha = \{ha : h \in H\}$.

קוסט שמאלי (מחלקה שמאלית) של H ב- G: $aH = \{ah : h \in H\}$.

הערה: אם החבורה אבלית, קוסטים ימניים וקוסטים שמאליים הם זהים.

דוגמא: $G = (\mathbb{Z}, +)$, $H = 5\mathbb{Z}$, $a = 2$, $H + 2 = 5\mathbb{Z} + 2 = \{5m + 2,\ m \in \mathbb{Z}\}$ (זו לא ת"ח).

הגדרה: מספר הקוסטים הימניים של תת-חבורה H בחבורה G יסומן ב: $[G:H]$ וייקרא:

האינדקס של H ב-G.

טענה: $|Ha| = |H|$.

משפט: תהי G חבורה ו- H תת-חבורה של G. נגדיר יחס בין אברי G בצורה הבאה:

$a \sim b \leftrightarrow ab^{-1} \in H$. יחס זה הוא יחס שקילות ומתקיים כי מחלקת השקילות של a היא Ha.

מסקנות:

- $Ha = H$ אם"ם $a \in H$.
- $Ha = Hb$ אם"ם $ab^{-1} \in H$.
- $Ha \cap Hb \neq \varnothing$ אם"ם $Ha = Hb$.
- G שווה לאיחוד הקוסטים הימניים הזרים.

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

מסקנה: G חבורה סופית, $a \in G$ ונניח ש- $n \in \mathbb{N}$ כך ש: $a^n = e$ אזי: $o(a) \mid n$.

המשפט הקטן של פרמה: אם p ראשוני ו- $a \in \mathbb{Z}$ אזי: $a^p = a \pmod p \leftrightarrow p \mid a^p - a$.

משפט אויילר: יהא n מספר טבעי, $a \in \mathbb{Z}$, כך ש $(a,n) = 1$, אזי $a^{\varphi(n)} \equiv 1 \pmod n$

($\varphi(n)$ - פונקצית אויילר).

דוגמא: $|U_{15}|=\varphi(15)=8$ $U_{15}=\{1,2,4,7,8,11,13,14\}$. נגדיר: $H=\{1,4,7,13\}$ אז:

$o(7)=4\to H=<7>$. ולפי המשפט: $[U_{15}:H]=\frac{|U_{15}|}{|H|}=\frac{8}{4}=2$ כלומר: יש רק 2 קוסטים שונים:

$$\begin{cases} H=H1=H4=H7=H13 & =\{1,4,7,13\} \\ H2=H8=H11=H14 & =\{2,8,11,14\} \end{cases}$$

הצמדת איברים: תהי G חבורה, $a,b\in G$. a,b נקראים צמודים אם קיים $x\in G$ בחבורה כך ש-$x^{-1}ax=b$ (זוהי מעין הכללה של דמיון מטריצות).

הערה: יחס הצמידות הוא יחס שקילות ולמחלקות השקילות קוראים: מחלקות צמידות.

משפט: G חבורה סופית, $a\in G$, אז מספר האיברים הצמודים ל-a הוא מספר הקוסטים הימניים הזרים של a ב-G, כלומר: $[G:C_G(a)]$.

תת-חבורה נורמאלית:

הגדרה: תהי G חבורה ו-N תת-חבורה. אם לכל $g\in G$ ולכל $n\in N$ מתקיים: $g^{-1}ng\in N$ (סגירות להצמדה) אזי: N נקראת תת-חבורה נורמאלית. סימון: $N\lhd G$.

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

משפט: תהי G חבורה, אז 3 הטענות הבאות הן שקולות:

1. $N\lhd G$.
2. $\forall g\in G,\ g^{-1}Ng=N$.
3. $\forall g\in G,\ Ng=gN$.

טענה: אם $H\prec G$ ו-$[G:H]=2$ אז: $H\lhd G$ (ת"ח נורמאלית).

טענה: אם G חבורה קומוטטיבית, אז כל תת חבורה שלה היא נורמאלית.

הערה: אם G קומוטטיבית ו-H תת-חבורה כלשהי, $h\in H,\ g\in G$ אז: $g^{-1}hg=hg^{-1}g=h$ וזה שייך ל-H כלומר: כל צמוד של איברי H הוא ב-H ולכן: $H\lhd G$.

הרכז: הרכז של $a\in G$ מוגדר כ- $C_G(a)=\{x\in G: xa=ax\}$ (כל האיברים שמתחלפים עם a). זו תת-חבורה של G.

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

חבורת הפרמוטציות (התמורות)

הגדרות בסיסיות:

מעגל: תמורה שמסומנת $\sigma=(i_1,i_2,\ldots,i_k)\in S_n$ כאשר: $\sigma(\alpha_i)=\alpha_{i+1}$ (באופן מעגלי) ואם $j\notin\{i_1,i_2,\ldots,i_k\}$ אז: $\sigma(j)=j$.

דוגמא: $(1,4,2,6)\in S_7$ אז הפרמוטציה היא: $\begin{pmatrix}1&2&3&4&5&6&7\\4&6&3&2&5&1&7\end{pmatrix}$

מעגלים זרים: מעגלים שאין להם אף איבר משותף.

טענות חשובות:

- כל $\sigma\in S_n$ אפשר לרשום כמכפלה של מעגלים זרים.
- מעגלים זרים הם מתחלפים (קומוטטיביים). ($\alpha,\beta\in S_n$ זרים אז $\alpha\beta=\beta\alpha$).

משפט: הסדר של מעגל באורך k, הוא k (חזקה קטנה יותר לא תביא לתמורת הזהות).

דוגמא: $\sigma=(1,4,6,2)\quad\sigma^2=(1,2)(4,6)\quad\sigma^3=(1,6,2,4)\quad\sigma^4=(1)(4)(2)(6)=e$

משפט: תהא σ תמורה שהיא מכפלה של מעגלים זרים שאורכיהם $k_1,k_2,\ldots,k_s$, אזי הסדר של σ הוא הכפולה המשותפת הקטנה ביותר של $k_1,k_2,\ldots,k_s$ (ה-lcm).

הופכי של מעגל: $\sigma=(i_1,i_2,\ldots,i_{k-1},i_k),\quad\sigma^{-1}=(i_k,i_{k-1},\ldots,i_2,i_1)$.

הופכי של תמורה: שהיא מכפלה של מעגלים זרים:
$\varphi=(i_1,\ldots,i_k)(j_1,\ldots,j_k)=(i_1,\ldots,i_k)^{-1}(j_1,\ldots,j_k)^{-1}$ כי מעגלים זרים הם מתחלפים.

תמורות זוגיות ואי-זוגיות:

טרנספוזיציה: מעגל באורך 2.

טענה: לכל טרנספוזיציה α, $\alpha^2=e$ (בגלל שהסדר הוא-2 והעלאה בסדר מביאה ל-e).

משפט: כל תמורה ניתנת לכתיבה כמכפלה של טרנספוזיציות:
$(i_1,i_2,\ldots,i_k)=(i_1,i_2)(i_1,i_3)\cdots(i_1,i_k)$ (מעגל באורך k ניתן לרשום כ: k-1 טרנספוזיציות).

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

תמורה זוגית: תמורה שניתן לרשום אותה כמכפלה של מספר זוגי של טרנספוזיציות.

תמורה אי-זוגית: תמורה שניתן לרשום אותה כמכפלה של מספר אי-זוגי של טרנספוזיציות.

הגדרה נוספת: תמורה σ שמספר הזוגות $i<j$ כך ש: $\sigma(i)<\sigma(j)$ הוא מספר זוגי.

מסקנה: מעגל הוא תמורה זוגית אם"ם אורכו אי-זוגי.

טענות:

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

An: אוסף כל התמורות הזוגיות ב- S_n.

טענה: $A_n \lhd S_n$ ו- $|A_n| = \frac{n!}{2}$ (חצי מהתמורות הן זוגיות).

הערה: זו ת"ח נורמאלית בגלל ש $[S_n : A_n] = 2$.

הצמדה של מעגל: הצמדת המעגל $(i_1, i_2, \ldots, i_k)$ ע"י $\sigma \in S_n$ תמורה כלשהי:

$$\sigma(i_1, i_2, \ldots, i_k)\sigma^{-1} = (\sigma(i_1), \sigma(i_2), \ldots, \sigma(i_k)).$$

מכפלה של מעגלים:

$$\sigma(i_1, i_2, \ldots, i_k)(j_1, j_2, \ldots, j_k)\sigma^{-1} = (\sigma(i_1), \sigma(i_2), \ldots, \sigma(i_k))(\sigma(j_1), \sigma(j_2), \ldots, \sigma(j_k))$$

מסקנה-1: הצמדה של תמורה שומרת על מבנה המעגלים שלה.

מסקנה-2: תהי $N \lhd S_n$, אם N מכילה טרנספוזיציה כלשהי אז N מכילה את כל הטרנספוזיציות (בגלל הסגירות להצמדה בת"ח נורמאלית) ולכן $S_n = N$.

הומומורפיזם של חבורות

הגדרה: יהיו G_1,G_2 חבורות. e_1 הוא האיבר הניטראלי של G_1, e_2 הוא האיבר הניטראלי של G_2.
פונקציה $\varphi:G_1\to G_2$ נקראת הומומורפיזם אם: $\underbrace{\varphi(ab)}_{in\ G_1}=\underbrace{\varphi(a)\varphi(b)}_{in\ G_2}$ לכל $a,b\in G_1$.

גרעין: $Ker(\varphi)=\{a\in G_1:\varphi(a)=e_2\}$. $Ker(\varphi)\subseteq G_1$.

תמונה: $\mathrm{Im}(\varphi)=\{\varphi(a):\ a\in G_1\}$. $\mathrm{Im}(\varphi)\subseteq G_2$.

הומומורפיזם טריוויאליים:

הומומורפיזם הזהות: $I_G:G\to G$, $I_G(a)=a$.

הומומורפיזם הטריוויאלי: $\varphi:G_1\to G_2$, $\varphi(a)=e_2$ (שולח את כל האיברים ל-e_2).

איזומורפיזם: הומומורפיזם שהוא חח"ע ועל.
G_1 ו-G_2 נקראות איזומורפיות אם קיים איזומורפיזם ביניהן. סימון: $G_1\cong G_2$.
מונומורפיזם: הומומורפיזם חח"ע.
אפימורפיזם: הומומורפיזם על.

משפט: תהי $\varphi:G_1\to G_2$ הומומורפיזם. e_1,e_2 איברים ניטראלים בהתאמה. אז:

- $\varphi(e_1)=e_2$.
- לכל $a\in G_1$, $\varphi(a^{-1})=(\varphi(a))^{-1}$
- $Ker(\varphi)$ היא תת-חבורה נורמאלית של G_1.
- $\mathrm{Im}(\varphi)$ היא תת-חבורה של G_2.
- φ חח"ע אם"ם: $Ker(\varphi)=\{e_1\}$ (הגרעין מכיל רק את האיבר הניטראלי).
- φ על אם"ם $\mathrm{Im}(\varphi)=G_2$.
- לכל $x\in G_1$, $x^{-1}(\ker(\varphi))x\subseteq\ker(\varphi)$.
- לכל $x\in G_1$, $(\ker(\varphi))x=\{y\in G|\ \varphi(y)=\varphi(x)\}$.

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

משפט: כל חבורה ציקלית אינסופית היא איזומורפית ל-$\mathbb{Z}$ לגבי חיבור.

משפט: כל חבורה ציקלית מסדר n היא איזומורפית ל-Z_n.

משפט קיילי: תהא G חבורה סופית כך ש-$|G|=n$, אז G איזומורפית לתת-חבורה של S_n
(כלומר קיים איזומורפיזם שמתאים כל איבר ב-G לפונקציה חח"ע ועל).

חבורות מנה ומשפטי הומומורפיזם

חבורת מנה: תהי G חבורה ו- $N \lhd G$. נגדיר: $\frac{G}{N} = \{Ng : g \in G\}$ כלומר: אוסף הקוסטים של N ב- G. נגדיר פעולה בין קוסטים: $(Na)(Nb) = Nab, \quad a,b \in G$.

$\frac{G}{N}$ היא חבורה ביחס לפעולה הנ"ל. איבר היחידה: $Ne = N$, וההופכי של קוסט Na הוא: Na^{-1}.

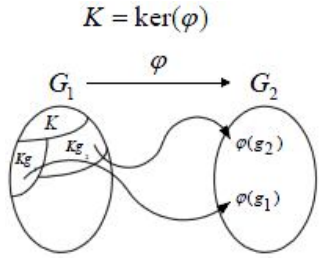
טענה: אם G חבורה סופית אז $\left|\frac{G}{N}\right| = \frac{|G|}{|N|}$.

הערה: אם G חבורה קומוטטיבית ו- H תת-חבורה ($H \lhd G$ כי G קומוטטיבית), אז $\frac{G}{H}$ מוגדרת וגם היא קומוטטיבית.

משפט: G חבורה ו- $H \lhd G$. נגדיר: $\varphi : G \to \frac{G}{H}$ כך: $\varphi(g) \to Hg$ (הפונקציה שולחת איבר ב G לקוסט שלו). אז: φ הומומורפיזם ו- $H = \ker(\varphi)$.

משפטי הומומורפיזמים:

משפט האיזומורפיזם הראשון: תהא $\varphi : G_1 \to G_2$ הומומורפיזם. אזי: $G_1 / \ker(\varphi) \cong \mathrm{Im}(\varphi)$.



דוגמאות:

- $\mathbb{Z}/n\mathbb{Z} \cong Z_n : \varphi : \mathbb{Z} \to Z_n, \ \varphi(a) = a \pmod n, \ \mathrm{Im}(\varphi) = Z_n, \ \ker(\varphi) = n\mathbb{Z}$.
- $\mathbb{C}^*/N = \{z : |z| = 1\} \cong \mathbb{R}^+ : \varphi : \mathbb{C}^* \to \mathbb{R}^*, \ \varphi(z) = |z|, \ \mathrm{Im}(\varphi) = \mathbb{R}^+, \ \ker(\varphi) = N$.
- $GL(n,\mathbb{R})/SL(n,\mathbb{R}) \cong \mathbb{R}^* : \varphi : GL(n,\mathbb{R}) \to \mathbb{R}^*, \ \varphi(A) = |A|, \ \ker(\varphi) = SL(n,\mathbb{R}), \mathrm{Im}(\varphi) = \mathbb{R}^*$.

משפט האיזומורפיזם השני: G חבורה, $N \lhd G$, H תת-חבורה. אז:

1. HN היא תת-חבורה.
2. $N \lhd NH$
3. $N \cap H \lhd H$
4. $\frac{HN}{N} \cong \frac{H}{H \cap N}$

משפט האיזומורפיזם השלישי: G חבורה, $N \lhd G$, $K \lhd G$ כך ש- $K \subseteq N$. אז: $\frac{G}{N} \cong \frac{\left(\frac{G}{K}\right)}{\left(\frac{N}{K}\right)}$.

שדות וחוגים-הגדרות

חוג: קבוצה R (Ring) עם שתי פעולות: $+,\bullet$ (חיבור וכפל). כל שמתקיימות הדרישות הבאות:

1. R חבורה קומוטטיבית לגבי + (אלה להן למעשה 5 מאקסיומות השדה).
   איבר ניטראלי יסומן: 0, הופכי של a לגבי + יסומן: $-a$.
2. R סגורה לגבי $\bullet$: אם $a,b\in R$ אז גם $ab\in R$.
3. $\bullet$ היא פעולה אסוציאטיבית. $a,b,c\in R$ אז: $(ab)c=a(bc)$.
4. פילוג: $a,b,c\in R$ אז: $(b+c)a=ba+ca$ $\quad a(b+c)=ab+ac$.

הערה: יש כאן 8 מתוך 11 האקסיומות של שדה.

חוג עם יחידה: חוג שיש בו איבר ניטראלי לגבי $\bullet$. איבר זה יסומן: 1 ו: $1\cdot a=a\cdot 1=a$ לכל $a\in R$.

חוג קומוטטיבי: חוג שבו $\bullet$ היא פעולה קומוטטיבית: $ab=ba$ לכל $a,b\in R$.

מחלק אפס: איבר $0\neq a\in R$ בחוג R כך שקיים $0\neq b\in R$ ומתקיים: $ab=0$ או $ba=0$.

תחום שלמות: חוג קומוטטיבי, עם יחידה ובלי מחלקי אפס.

איבר הפיך: בחוג עם יחידה R זה איבר $a\in R$ כך שקיים $b\in R$ המקיים: $ab=ba=1$.

חוג עם חילוק: חוג עם יחידה שבו כל איבר שונה מאפס הוא הפיך.

שדה: חוג קומוטטיבי עם חילוק (עם יחידה ובלי מחלקי אפס).

דוגמאות:

- $\mathbb{Z}$: חוג קומוטטיבי עם יחידה לגבי $+,\bullet$. זהו תחום שלמות. איברים הפיכים: $1,-1$.
- $2\mathbb{Z}$: חוג קומוטטיבי בלי יחידה לגבי $+,\bullet$. זה אינו תחום שלמות. אין בו איברים הפיכים.
- $\mathbb{R},\mathbb{Q},\mathbb{C}$: שדות. תחומי שלמות לגבי $+,\bullet$.
- $\mathbb{Z}_n$: חוג קומוטטיבי עם יחידה ביחס לחיבור וכפל מודולו n. האיברים ההפיכים הם המספרים הזרים ל-n. אם n לא ראשוני, אז זה לא תחום שלמות. (n ראשוני $\leftarrow$ $\mathbb{Z}_n$ שדה).
- קבוצת כל המספרים הרציונאליים מהצורה $\frac{a}{b}$ כאשר a,b הם שלמים זרים ו-b אי-זוגי: חוג קומוטטיבי לגבי $+,\bullet$ ויש בו יחידה.
- כל הפונקציות הממשיות הרציפות על $[0,1]$ עם הפעולות חיבור וכפל מטריצות: חוג קומוטטיבי עם יחידה. לא כל איבר הוא הפיך, יש בו מחלקי אפס ולכן זה אינו תחום שלמות.
- $M_n(F)$ - מטריצות $n\times n$ מעל השדה F: חוג עם יחידה= I, החוג אינו קומוטטיבי (כי כפל מטריצות הוא לא), האיברים ההפיכים- מטריצות עם דטרמיננטה $\neq 0$, זה אינו תחום שלמות כי יש בו מחלקי אפס.

משפט: R הוא חוג. אז מתקיימים הדברים הבאים:

1. 0 הוא יחיד.
2. $a\in R$ אז: $-a$ הוא יחיד.
3. $0a=a0=0$ לכל $a\in R$.

4. $a(-b)=(-a)b=-(ab)$ לכל $a,b\in R$.
5. $(-a)(-b)=ab$.
6. $(-1)a=-a$ אם R הוא חוג עם יחידה.

משפטים- תחום שלמות:

- אם D תחום שלמות ונתון ש: $ab=ac$ אז ניתן לצמצם ולקבל: $b=c$.
- בשדה אין מחלקי אפס, כלומר, כל שדה הוא תחום שלמות.

משפט: R הוא חוג. נתון: $x=x^2$ לכל $x\in R$. אז R הוא חוג קומוטטיבי.

משפטים- מספר איברים בשדה:

- מספר האיברים בשדה סופי הוא חזקה של מספר ראשוני.
- אם p ראשוני ו- n מספר טבעי, אז קיים שדה ובו p^n איברים.
- אם F שדה סופי אז: $|F|=p^n$ כאשר p הוא ראשוני ו- n הוא טבעי ($char(F)=p$).

מציין/אופיין של שדה:

מציין של שדה: F הוא שדה. המספר הקטן ביותר m כך ש- $\underbrace{1+1+\cdots+1}_{m}=0$ נקרא: **המציין של השדה** או **הקרקטריסטיקה של השדה** או **האופיין של השדה**. סימון: $char(F)$.

משפט: מציין של שדה הוא או אפס, או מספר ראשוני.

משפט: לכל שדה סופי יש תת-שדה מסדר: $char(F)$.

משפט: אם שדה סופי F מכיל תת-שדה K אז הסדר של F הוא חזקה של הסדר של K.

הערה: $\mathbb{Z}_p$ הוא שדה עם מציין שווה ל- p.

תת-חוג:

הגדרה: יהי R חוג ו- S תת-קבוצה לא ריקה של R. אם S היא בעצמה חוג ביחס לפעולות ב- R אז אומרים ש- S היא תת-חוג.

טענה: יהי R חוג ו- S תת-קבוצה של R אז S היא תת-חוג אם"ם:

1. $S\neq\varnothing$.
2. לכל $a,b\in S$ מתקיים: $a-b\in S$.
3. לכל $a,b\in S$ מתקיים: $a\cdot b\in S$.

הערה: לכל חוג יש שני תתי-חוגים טריוויאלים: החוג עצמו ו- $\{0\}$.

אידיאלים, הומומורפיזם של חוגים וחוגי מנה

אידיאלים:

אידיאל: R חוג. I זו קבוצה ב-R שנקראת **אידיאל** ומקיימת:

1. $I \neq \varnothing$.
2. $a,b \in I$ אז: $a+b \in I$ (סגירות ל +).
3. $a \in I$ אז: $-a \in I$ (סגירות לגבי נגדי בחיבור).
4. $a \in I$, $x \in R$ אז: $ax, xa \in I$ (בליעה).

*ניתן לאחד את (2) ו-(3) לסגירות לחיסור: $a,b \in I \to a-b \in I$

אידיאל משמש לאותו תפקיד בו משמשת תת-חבורה נורמאלית בחבורות.

הערות:

- כל אידיאל הוא תת-חוג (סגירות לחיסור וכפל).
- בכל חוג יש שני אידיאלים טריוויאלים: R ו-$\{0\}$ והם נקראים: **אידיאלים לא אמיתיים**.

טענה: אם R הוא חוג עם יחידה ואם I הוא אידיאל ב-R כך ש-$1 \in I$ אז: $I = R$ (נובע מבליעה: כפל ב-1 מכניס כל איבר ל-I).

משפט: אם F הוא שדה ו-$I \neq \{0\}$ הוא אידיאל ב-F אז בהכרח: $I = F$ (בשדה אין אידיאלים אמיתיים, אך ייתכן חוג שאינו שדה וגם בו אין אידיאלים אמיתיים).

משפט הפוך: יהי R חוג קומוטטיבי עם יחידה שאין בו אידיאלים אמיתיים. אז R הוא שדה.

אידיאל ראשי: R חוג קומוטטיבי, $a \in R$. נסמן: $(a) = \{ax \mid x \in R\}$. אז (a) הוא אידיאל והוא נקרא: **האידיאל הראשי הנוצר ע"י a**. דוגמא: ב-$\mathbb{Z}$, $(15) = 15\mathbb{Z}$.

הומומורפיזם:

הגדרה: פונקציה $\varphi : R_1 \to R_2$, R_1, R_2 חוגים כך ש:

$$\varphi(a+b) = \varphi(a) + \varphi(b)$$
$$\varphi(ab) = \varphi(a) \cdot \varphi(b)$$

גרעין של הומומורפיזם: $\ker(\varphi) = \{x \in R \mid \varphi(x) = 0\}$

- $\varphi(0) = 0$.
- $\varphi(-a) = -\varphi(a)$.
- φ חח"ע אם"ם $\ker(\varphi) = \{0\}$.

משפטים- תכונות: $\varphi : R_1 \to R_2$ הומומורפיזם, אז:

1. $\ker(\varphi)$ הוא תת-חבורה של R_1 לגבי +. והוא גם אידיאל ב-R_1.
2. $a \in \ker(\varphi)$, $x \in R_1$ אז מתקיימת בליעה: $xa, ax \in \ker(\varphi)$.
3. $\mathrm{Im}(\varphi)$ הוא תת-חוג של R_2.

חוג מנה:

חוג מנה: יהא I אידיאל בחוג R. יהא $b\in R$, נגדיר קוסט של b: $I+b=\{x+b \mid x\in I\}$. זוהי בדיוק הגדרת הקוסט בחבורות, מלבד זאת שהכפל נהפך ל+.

ומתקיים: $I+b=b+I$ כי + פעולה קומוטטיבית, ובפרט I תת-חבורה נורמאלית ב-R לגבי +.

נגדיר: $\frac{R}{I}=\{I+b \mid b\in R\}$ (אוסף כל הקוסטים של I ב-R).

משפט: R חוג, I אידיאל. אז $\frac{R}{I}$ הוא חוג ביחס לפעולות:

$$(I+a)+(I+b)=I+(a+b)$$
$$(I+a)\cdot(I+b)=I+ab$$

- אם יש ב-R יחידה אז: $I+1$ הוא היחידה של $\frac{R}{I}$.
- אם R קומוטטיבי אז גם $\frac{R}{I}$ הוא קומוטטיבי.
- אם R הוא חוג עם חילוק, אז גם $\frac{R}{I}$ הוא חוג עם חילוק.

<u>הערות:</u>

- אם R תחום שלמות, $\frac{R}{I}$ איננו בהכרח תחום שלמות ולהפך.
- אם I אידיאל, אז I הוא גרעין של איזשהו הומומורפיזם: $\varphi(a)=I+a$, $\varphi: R\to\frac{R}{I}$.

משפטי איזומורפיזם של חוגים:

משפט ראשון: $\varphi: R_1\to R_2$ הומומורפיזם. אז: $\frac{R_1}{\ker(\varphi)}\cong \mathrm{Im}(\varphi)$.

משפט שני: I,J הם אידיאלים בחוג R אז: $\frac{I+J}{I}\cong\frac{J}{I\cap J}$.

משפט שלישי: $R\supseteq I\supseteq J$, R חוג, I,J הם אידיאלים. אז: $\frac{R/J}{I/J}\cong\frac{R}{I}$ (כביכול מצמצמים ב-J).

משפט: כל אידיאל ב-$\mathbb{Z}$ הוא מהצורה $n\mathbb{Z}$ כאשר $n\in\mathbb{N}$. וגם מתקיים: $\frac{\mathbb{Z}}{n\mathbb{Z}}\cong\mathbb{Z}_n$.

הגדרה: $\varphi(a)=a\pmod n$ $\varphi:\mathbb{Z}\to\mathbb{Z}_n$ אז מתקיים כי φ הוא הומומורפיזם בין חוגים.

מסקנה: $\frac{\mathbb{Z}}{n\mathbb{Z}}$ הוא שדה אם"ם n הוא ראשוני.

משפט: R הוא חוג קומוטטיבי עם יחידה. אם $\{0\}$ ו-R הם האידיאלים היחידים, אז R הוא שדה.

משפט: יהיו שני חוגים R_1, R_2 איזומורפיים: $R_1 \cong R_2$. אם R_1 הוא שדה אז גם R_2 הוא שדה.
$\varphi(1)$ זה היחידה של R_2.

אידיאל מקסימאלי: יהי R חוג ו- I אידיאל ב- R. I נקרא אידיאל מקסימאלי אם I לא מוכל בשום אידיאל אחר פרט ל- I ו- R.

דוגמאות:

- ב- $\mathbb{Z}$: $6\mathbb{Z}$ הוא אידיאל לא מקסימאלי כי למשל: $6\mathbb{Z} \subset 3\mathbb{Z} \subset \mathbb{Z}$.
  אבל $5\mathbb{Z}$ הוא אידיאל מקסימאלי.

טענה: $n\mathbb{Z}$ הוא אידיאל מקסימאלי ב- $\mathbb{Z}$ אם"ם n ראשוני.

- $R[x]$ = חוג הפולינומים מעל R. נגדיר: $M = \{p(x) \in R[x] \mid p(1) = 0\}$. אז M הוא אידיאל מקסימאלי ב- $R[x]$.

משפט: יהי R חוג קומוטטיבי עם יחידה. יהי I אידיאל ב- R, אז: $\frac{R}{I}$ הוא שדה אם"ם I הוא אידיאל מקסימאלי.

חוג הפולינומים

הגדרה: F =שדה, $F[x]$ = אוסף כל הפולינומים עם מקדמים ב- F.

פולינום= $f(x)=a_0+a_1x+\cdots+a_nx^n$, $a_0,a_1,\ldots,a_n\in F$, x =משתנה ב- F.

מעלת הפולינום: אם $a_n\neq 0$ אז n נקרא המעלה של הפולינום $f(x)$. סימון: $\deg(f(x))$.

פולינום האפס: פולינום שכל מקדמיו שווים לאפס. מעלת פולינום האפס לא תוגדר.

טענה:
$$\deg(f(x)+g(x))\le\max\{\deg(f(x)),\deg(g(x))\}$$
$$\deg(f(x)\cdot g(x))=\deg(f(x))+\deg(g(x))$$

משפט: $F[x]$ זה חוג קומוטטיבי עם יחידה, בלי מחלקי אפס.

משפט: $f(x),g(x)\neq 0\in F[x]$. אז קיימים שני פולינומים $q(x),r(x)\in F[x]$ כך ש:
$f(x)=g(x)\cdot q(x)+r(x)$ וגם: $0\le\deg(r(x))<\deg(g(x))$.

אידיאלים ב-F[x]:

משפט: כל אידיאל בחוג $F[x]$ הוא אידיאל ראשי (כפולות של איזשהו פולינום).

חוג ראשי: חוג שכל אידיאל בו הוא ראשי (למשל: חוג הפולינומים).

משפט: יהא $f(x)\in F[x]$, $\deg(f(x))=n$, אז כל איבר ב- $\dfrac{F[x]}{(f(x))}$ ניתן להצגה באופן יחיד בצורה: $a_0+a_1x+\cdots+a_{n-1}x^{n-1}+(f(x))$ כאשר: $a_0,a_1,\ldots,a_{n-1}\in F$

הערה: המשמעות היא שניתן לכתוב את הקוסט של הפולינום (עם האידיאל $(f(x))$) ע"י פולינום ממעלה קטנה יותר באופן יחיד.

מסקנה: נניח ש- F שדה ובו q איברים. יהא $f(x)\in F[x]$ ממעלה n. אז מספר האיברים ב- $\dfrac{F[x]}{(f(x))}$ הוא: q^n.

אם $F=Z_p$ אז: $\left|\dfrac{Z_p[x]}{I}\right|=p^n$.

דוגמאות:

- $\dfrac{\mathbb{R}[x]}{(x^3+x+2)}$, $x^3+x+2+I=I$ כי $x^3+x+2\in I$ ולכן כאילו שווה לאפס.

  לא תמיד נמצא בביטוי את האידיאל במלואו, ולכן ניתן לכתוב: $x^3+I=-x-2+I$ (מעין העברת אגפים).

  נחשב מכפלה של קוסטים: $(x^2+2x+2+I)(x^2+3x+I)=(x^2+2x+2)(x^2+3x)+I$
  $=x^4+5x^3+8x^2+6x+I$

  נציב: $x^3=-x-2$ ונקבל: $(-x-2)x+5(-x-2)+8x^2+6x+I=7x^2-x-10+I$.

- $\dfrac{\mathbb{Q}[x]}{(x^2-5x+6)}$, נחשב: $(x-2+I)(x-3+I)=(x-2)(x-3)+I=x^2-5x+6+I=I$.

פריקות של פולינומים:

פולינום אי-פריק: $f(x)\in F[x]$ פולינום שמחלקיו היחידים הם: אברי F (סקלרים) וכפולותיהם באיבר מ- F (פולינום מאותה מעלה כמו של $f(x)$).

הערה: פולינום ממעלה 2 או 3 הוא פריק אם"ם יש לו שורש.

משפט: $\frac{F[x]}{(f(x))}$ הוא שדה אם"ם $f(x)$ הוא פולינום אי-פריק.

הערה: $I=(f(x))$ הוא אידיאל מקסימאלי אם"ם $a(x)$ אי-פריק ב-$F[x]$.

משפט: $f(x)\in F[x]$, $a\in F$, אז:

1. $f(x)=(x-a)q(x)+f(a)$.
2. $(x-a)\mid f(x) \leftrightarrow f(a)=0$.

מסקנה: $f(x)\in F[x]$, $\deg(f(x))\geq 2$. אם יש ל-$f(x)$ שורש ב- F אז $f(x)$ הוא פריק (כי אם a הוא שורש אז: $f(x)=(x-a)q(x)$).

הערה: המשפט ההפוך לא נכון. לא לכל פולינום פריק יש שורש בשדה.

משפט: $f(x)\in F[x]$, $\deg(f(x))$ שווה 2 או 3. אם $f(x)$ פריק, אז יש לו שורש ב- F.

מסקנה: $f(x)\in F[x]$ ממעלה 2 או 3, אז $f(x)$ אי-פריק מעל F אם"ם אין ל-$f(x)$ שורש ב- F.

משפטים על פריקות בשדות מסויימים:

- כל פולינום ממעלה גדולה מ-1 הוא פריק מעל $\mathbb{C}$ (לפי המשפט היסודי של האלגברה, לכל פולינום עם מקדמים ב-$\mathbb{C}$, יש שורש ב-$\mathbb{C}$).
- השורשים המרוכבים מופיעים בזוגות- שורש והצמוד שלו.
- כל פולינום ממעלה לפחות 3 ב-$\mathbb{R}[x]$ הוא פריק מעל $\mathbb{R}$.
- כל פולינום ממעלה אי-זוגית, יש לו שורש ממשי ב-$\mathbb{R}$ ולכן הוא פריק.
- יהא $f(x)=a_0+a_1x+a_2x^2+\cdots+a_nx^n$ פולינום עם מקדמים שלמים. נניח ש-$\frac{p}{q}$ הוא שבר מצומצם שהוא שורש של $f(x)$. אז: $p\mid a_0$ וגם: $q\mid a_n$.

משפט אייזנשטיין: נניח ש- $f(x)=a_0+a_1x+a_2x^2+\cdots+a_nx^n$ כאשר: $a_0,a_1,a_2,\ldots,a_n$ שלמים. ונניח שקיים מספר ראשוני p כך ש: $p\mid a_0, p\mid a_1, p\mid a_2,\ldots,p\mid a_{n-1}$ וגם: $p\nmid a_n,\ p^2\nmid a_0$. אם כל אלה מתקיימים אז $f(x)$ הוא אי פריק מעל $\mathbb{Q}[x]$.