23-10-2006

מבנים אלגבריים - שעור מס' 1

המרצה: שחר מוזס
משרד: חדר 1 במבנין איינשטיין.

חבורות

הגדרה: חבורה היא שלשה $(G,\cdot,e)$

כאשר: G קבוצה

• הפעולה, היא פונקציה מ- $G\times G$ לתוך G: $G\times G \longmapsto G$

$(a,b) \longmapsto a\cdot b$

$e\in G$ איבר ב-G

כך שמתקיימות התכונות הבאות:

אלו הן האקסיומות של החבורה

Ⓐ אסוציאטיביות: לכל $a,b,c\in G$ $(a\cdot b)\cdot c = a\cdot(b\cdot c)$

Ⓑ e הוא איבר יחידה: לכל $g\in G$ $e\cdot g = g\cdot e = g$

Ⓒ קיום הופכי: לכל $g\in G$ קיים איבר שנסמנו $g^{-1}\in G$ כך ש: $g^{-1}g = g\cdot g^{-1} = e$

Ⓒ' (דרך נוספת לרשום את Ⓒ): לכל $g\in G$ קיים $h\in G$ יחיד כך ש: $h\cdot g = g\cdot h = e$

למה: עבור כל $g\in G$ יש איבר הופכי יחיד כלומר יש רק איבר $h\in G$ יחיד

כך ש: $hg = gh$

הוכחה: נניח כי $h_1, h_2\in G$ ויהי $g\in G$ כלשהו כך ש: $h_1\cdot g = g\cdot h_1 = e$

וגם: $h_2 g = g h_2 = e$

אזי: $(h_1\cdot g)h_2 = e\cdot h_2 = h_2$

$\| $ אסוציאטיביות

$h_1(gh_2) = h_1\cdot e = h_1$

וקיבלנו $h_1 = h_2$

▨

הגדרה: חבורה בה מתקיים כי לכל $a,b\in G$ $ab=ba$ תקרא חבורה קומוטטיבית (חילופית)

וגם חבורה אבלית (Abelian) (Abel על שם)

דוגמאות: (לכל מיני חבורות)

א) $(\mathbb{Z},+,0)$ $\quad \mathbb{Z}=\{\dots,-3,-2,-1,0,1,2,3\dots\}$

ב) $(\mathbb{R},+,0)$ אוסף כל המספרים הממשיים.

ג) $(\mathbb{Q},+,0)$ $\mathbb{Q}$ רציונליים

ד) $(\mathbb{R}^*,\cdot,1)$ $\quad \mathbb{R}^*=\{x\in\mathbb{R} \mid x\neq 0\}$

ה) אם F שדה אזי $(F^*,\cdot,1)$ היא חבורה

ו) $(\mathbb{Q}^*,\cdot,1)$

ז) יהי $1<n\in\mathbb{N}$

$\mathbb{Z}/n\mathbb{Z}$ - נציגים של שאריות מודולו n $\{\bar{0},\bar{1},\bar{2},\dots\overline{n-1}\}$

נתבונן ב $(\mathbb{Z}/n\mathbb{Z},+,0)$ כאשר $a+b$ היא שארית הסכום מודולו n

למשל אם $n=10$ אז $\mathbb{Z}/10\mathbb{Z}$ אז $\bar{7}+\bar{5}=\bar{2}$

דוגמא נוספת, יותר מעניינת:

נסמן ב- $(\mathbb{Z}/n\mathbb{Z})^*$ נציגים מודולו n של מספרים טבעיים אשר זרים ל-n

שוב ניקח $n=10$ $\quad \mathbb{Z}/10\mathbb{Z}=\{0,1,2,3,4,5,6,7,8,9\}$

$\mathbb{Z}/10\mathbb{Z}^*=\{\bar{1},\bar{3},\bar{7},\bar{9}\}$

(הערה: אם $n=p$ כאשר p ראשוני אז $\mathbb{Z}/n\mathbb{Z}$ שדה)

$g.c.d$ = מחלק משותף מירבי.

בהינתן זוג מספרים טבעיים a,b (לא שניהם אפס) המחלק המשותף המירבי שלהם הוא המספר הטבעי (השלם) הגדול ביותר אשר מחלק גם את a וגם את b.

טענה: לכל $n>1$ טבעי $((\mathbb{Z}/n\mathbb{Z})^*,\cdot,1)$ היא חבורה.

נתבונן בדוגמא בלוח הכפל של $(\mathbb{Z}/10\mathbb{Z})^*$

$\cdot$	1	3	7	9
1	1	3	7	9
3	3	9	1	7
7	7	1	9	3
9	9	7	3	1

הוכחה: ① סגירות: (סגירות פירושה שהכפל מגדיר העתקה
$$(\mathbb{Z}/n\mathbb{Z})^*\times(\mathbb{Z}/n\mathbb{Z})^*\longrightarrow(\mathbb{Z}/n\mathbb{Z})^*$$
וזה נובע מקיום ויחידות פירוק לגורמים ראשוניים.

(כל מספר טבעי m ניתן להצגה באופן יחיד (עד כדי שינוי סדר) כמכפלה של ראשוניים $m=p_1^{e_1}p_2^{e_2}\cdots p_k^{e_k}$ כאשר p_i ראשוניים ו- $e_i\in\mathbb{N}$))

* זוג מספרים הם זרים אם אין להם גורם ראשוני משותף.

המשך בעמ' הבא:

אז אם $\bar{a},\bar{b}\in(\mathbb{Z}/n\mathbb{Z})^*$ יהיו $a,b\in\mathbb{Z}$ נציגים שלהם.

אז $a=p_1^{e_1}\cdot p_2^{e_2}\cdot\ldots\cdot p_k^{e_k}$

$b=q_1^{r_1}\cdot q_2^{r_2}\cdot\ldots\cdot q_l^{r_l}$

אנו יודעים כי אף אחד מהראשוניים p_i,q_j אינו גורם של n

ולכן:

$$a\cdot b=p_1^{e_1}\cdot p_2^{e_2}\cdot\ldots\cdot p_k^{e_k}\cdot q_1^{r_1}\cdot q_2^{r_2}\cdot\ldots\cdot q_l^{r_l}$$

$\Leftarrow$ אף גורם ראשוני של $a\cdot b$ אינו גורם ראשוני של n ולכן השארית של $a\cdot b$ מודולו n היא איבר ב- $(\mathbb{Z}/n\mathbb{Z})^*$

② קיום הפכי: נותר להוכיח קיום הפכי כלומר נתון $\bar{a}\in(\mathbb{Z}/n\mathbb{Z})^*$. נציג שארית $a\in\mathbb{Z}$ זר ל-n וצריך להראות קיום $\bar{b}\in(\mathbb{Z}/n\mathbb{Z})^*$ כך ש $\bar{a}\cdot\bar{b}=\bar{1}$

לדוגמא: צריך להראות כי ל- $\bar{7}$ יש הפכי ב- $(\mathbb{Z}/10\mathbb{Z})^*$, למשל צריך להראות כי ל- 17 יש כפולה המשאירה שארית 1 מחלוקה ב- 10.

טענה 1: יהיו $m,n\in\mathbb{N}$ ויהי $d\in\mathbb{N}$ המחלק המשותף המקסימלי שלהם,

אז קיימים $r,s\in\mathbb{Z}$ כך ש: $r\cdot m+s\cdot n=d$

{ בדוגמא שלנו: $(17,10)=1 \Leftarrow$ קיימים $r,s\in\mathbb{Z}$ כך ש: $r\cdot 17+s\cdot 10=1$ }

טענה שמשתמשים בה בהמשך נוכיח:

טענה 2:

אם $a\in\mathbb{Z}$ זר ל-n ו $b\in\mathbb{Z}$ נותן את אותה השארית בחלוקה ב n אז:

$b\equiv a \bmod n$ (כלומר n מחלק את $a-b$)

אז גם b זר ל-n.

הוכחת טענה 2: קיים $k\in\mathbb{N}$ כך ש- $a-b=k\cdot n$

ולכן $a=b+k\cdot n$.

נניח כי b אינו זר ל-n כלומר יש $1<d\in\mathbb{N}$ כך ש $d|b$

$d|n \Leftarrow d$ מחלק גם את $a=b+kn$ ולכן גם a אינו זר ל-n

מסתירה להנחה.

$\blacksquare$

הוכחת טענה 1: איך נמצא מחלק משותף מירבי?

דרך א': לפרק את m ואת n לגורמים ראשוניים ולחשב מהם את המחלק המשותף המירבי. זוהי דרך לא טובה במובן הפרקטי.

דרך ב': אלגוריתם אוקלידס

נתונים $m,n \in \mathbb{N}$ טבעיים ונניח ב.ה.כ. כי $m>n$

נחשב את השארית של m בחלוקה ב-n אז: $m=k_1+q_1\cdot n$

טענה: המחלק המשותף המירבי של k_1 ו-n שווה למחלק המשותף המירבי של m,n.

$0<k_1<n$ אם $k_1=0$ סיימנו, אחרת:

$$n=k_2+q_2k_1$$

מה טענתיים ראינו? $m=k_1+q_1\cdot n$ (קצת חזרה על השורות הקודמות)

$$\gcd(m,n)=\gcd(n,k)$$

אם $k_2=0$ אז k_1 הוא המחלק המשותף המירבי של m,n

$$k_1=m-q_1\cdot n$$

אם $k_1=k_3+q_3\cdot k_2$

אם $k_3=0$ אז k_2 הוא המספר המבוקש

$$k_2=n-q_2k_1=n-q_2(m-q_1n)=(1+q_1q_2)n-q_2m$$

התהליך יפסק בשלב מסוים השארית היא אפס ואז ניתן לחזור אחורה ולמצוא את הצרוף עם m,n. ▨

נחזור להוכחה של קיום ההפכי:

מסקנה: נניח כי a,n זרים כלומר המחלק המשותף המקסימלי שלהם הוא 1

אז יש $r,s\in\mathbb{Z}$ כך ש: $1=ra+sn$ ולכן שארית r מודולו n

היא ההפכי ל-a מודולו n ב $(\mathbb{Z}/n\mathbb{Z})^*$

מתקיימים סגירות + קיום הפכי ולכן זוהי חבורה

▨

הגדרה: תת-חבורה

תהי G חבורה. תת-קבוצה (לא ריקה) H של G תקרא תת-חבורה

אם:
⓪ H אינה ריקה
① H סגורה לכפל כלומר לכל $h_1, h_2 \in H$ $h_1 \cdot h_2 \in H$
② לכל $h \in H$ אז $h^{-1} \in H$

ובעצם נובע $\Downarrow$

③ $e \in H$

סימון לתת-חבורה

הגדרה: תהי $H<G$ תת-חבורה

מחלקות ימניות של H הן הקבוצות מהצורה $Hg=\{hg \mid h \in H\}$ כאשר $g \in G$

מחלקה שמאלית: $gH=\{gh \mid h \in H\}$

הערה 1: $H<G$ תת-חבורה של G

כל שתי מחלקות ימניות הן זרות או זהות (אותה הטענה נכונה גם לגבי מחלקות שמאליות)

הוכחה: יהיו $g_1, g_2 \in G$ נתבונן ב- Hg_1, Hg_2

צריך להראות כי אם $Hg_1 \cap Hg_2 \neq \emptyset$ אזי $Hg_1 = Hg_2$

נניח כי $g \in Hg_1 \cap Hg_2$ מכאן קיימים $h_1, h_2 \in H$ כך ש:

$$g = h_1 g_1$$
$$g = h_2 g_2$$
$$\Downarrow$$
$$h_1 g_1 = h_2 g_2 \quad / h_1^{-1}\text{-נכפול משמאל ב}$$
$$g_1 = h_1^{-1} \cdot h_2 g_2$$

כעת, יהי $x \in Hg_1$ אזי קיים $h_x \in H$ כך ש:

$$x = h_x g_1 = h_x(h_1^{-1} h_2 g_2) = \underbrace{(h_x h_1^{-1} h_2)}_{H} g_2 \in Hg_2$$

כלומר $Hg_1 \subset Hg_2$

ובאותו האופן $Hg_2 \subseteq Hg_1$

ולכן מתקבל השוויון: $Hg_1 = Hg_2$

▨

אותו דבר נכון לגבי מחלקות שמאליות: או $g_1H = g_2H$ או $g_1H \cap g_2H = \emptyset$

טענה: $H<G$ תת-חבורה.

ללא הוכחה

כל שתי מחלקות ימניות של H הן שוות עצמה

כלומר לכל $g_1,g_2 \in G$ יש העתקה חח"ע ועל: $\varphi: Hg_1 \longrightarrow Hg_2$

מסקנה: (משפט לגראנז'): תהי G חבורה סופית ותהי $H<G$ תת-חבורה אזי

$|H|$ מחלק את $|G|$

הוכחה: איחוד $\bigcup_{g\in G} Hg = G$ הוא פירוק של G לקבוצות זרות שוות גודל ולכן $|H| \mid |G|$

מסקנות: ① יהי p ראשוני, אז לכל $a\in\mathbb{Z}$ $a^p \equiv a \pmod p$ (משפט פרמה הקטן)

② משפט אוילר: אם $1<n\in\mathbb{N}$ ו-a זר ל-n אזי:

$$a^{\phi(n)} \equiv 1 \bmod n$$

$\phi(n) = |(\mathbb{Z}/n\mathbb{Z})^*|$ = מס' המספרים שקטנים מ-n וזרים לו.

תרגיל: מהו $\phi(n)$?

רמז: $\phi(p_1^{e_1}\cdot p_2^{e_2}\cdot\ldots\cdot p_k^{e_k})$

ספרים מומלצים:

* עמיצור

* Topics in Algebra / Herstein

* Rotman

* Lang

(הכל) מדפים 22-24 בספריה למתמטיקה.

25-10-2006

מבנים אלגבריים - שעור מס' 2

(הוכחות מסודרות ס) משפט לגראנז' והלמה שהזכרנו בסוף השעור שעבר)

משפט לגראנז': תהי G חבורה סופית ותהי $H<G$ תת-חבורה אזי, הסדר של H (מספר איברי H: $\#H$, $|H|$) מחלק את הסדר של G.

הוכחה: נתבונן במחלקות השמאליות של H, כלומר, בתתי הקבוצות של G מהצורה $gH=\{gh \mid h\in H\}$ כאשר $g\in G$.

ראינו כי כל שתי מחלקות שמאליות הן או זרות או זהות.

כל איבר $g\in G$ שייך לאיזשהי מחלקה שמאלית. $ge=g\in gH$.

לכן G הוא איחוד זר של מחלקות שמאליות של H: $G=\dot{\bigcup}_{i=1}^{k} g_iH$

כלומר - קיימים $g_1,\dots,g_k\in G$: $G=\dot{\bigcup}_{i=1}^{k} g_iH$

הערה: k נקרא האינדקס של H ב-G.

למה: לכל חבורה G ותת-חבורה H ולכל $x,y\in G$ המחלקות השמאליות Hx, yH שוות עצמה. כלומר יש העתקה חח"ע ועל מ-xH ל-yH.

הוכחה: צריכים להראות קיום $\varphi: xH\to yH$ חח"ע ועל.

נגדיר $\varphi(z)=yx^{-1}z$

עבור $z\in xH$ קיים $h\in H$ כך ש: $z=xh$.

$$\varphi(z)=\varphi(xh)=yx^{-1}xh=yh\in yH$$

לכן φ העתקה מ-xH לתוך yH.

בדיקה לחח"ע: נניח כי $z_1,z_2\in xH \leftarrow$ $yx^{-1}z_1=\varphi(z_1)=\varphi(z_2)=yx^{-1}z_2$

נכפול משמאל ב: $(yx^{-1})^{-1}$ ונקבל כי:

$$z_1=ez_1=(yx^{-1})^{-1}(yx^{-1})z_1=(yx^{-1})^{-1}(yx^{-1})z_2=e\cdot z_2=z_2$$

כלומר $z_1=z_2$ וההעתקה היא חד-חד ערכית.

בדיקה לעל: בהינתן איבר $\overset{yh}{\omega}\in yH$ צריך להוכיח קיום $z\in xH$ כך ש: $\omega=\varphi(z)$

בהינתן $\omega=yh$ נתבונן ב $z=xh$

$$\varphi(z)=yx^{-1}xh=yh=\omega$$

כלומר קיימת העתקה חח"ע ועל ומכאן כי המחלקות שוות עצמה.

מכאן נובע כי: $|H|\,\big|\,|G|$ - משפט לגרנז'

מסקנה: יהי $1<n\in\mathbb{N}$ ויהי $a\in\mathbb{Z}$ זר ל-n אזי: $a^{\phi(n)}\equiv 1 \bmod n$

$\phi(n)=(\mathbb{Z}/n\mathbb{Z})^*$ = מספר השארית של n הזרות ל-n

תהי G חבורה ויהי $g\in G$ איבר כלשהו בחבורה.
מעוניינים בתת-החבורה המינימלית המכילה את g

$$g\in\langle g\rangle=\{g^n \mid n\in\mathbb{Z}\}\neq\phi$$

נשים לב כי הקבוצה סגורה תחת כפל: $g^n\cdot g^m=g^{n+m}$

תחת הופכי: $(g^{-n})g^n=g^0=e$

הגדרה: חבורה מהצורה $\{g^n \mid n\in\mathbb{Z}\}$ תקרא חבורה ציקלית.

תהי G חבורה סופית ויהי $g\in G$ איבר ב-G.
נתבונן בתת-החבורה (הציקלית) הנוצרת ע"י g - הסדר שלה הוא סופי-
משום ש- $\langle g\rangle\subset G$ ו-G סופית $\Leftarrow$ לכן, בסדרת האיברים $g_1,g_2,\dots$
יש חזרות כלומר, קיימים $k,l\in\mathbb{N}$ $l<k$ כך ש: $g^k=g^l \Leftarrow g^{k-l}=e$
(הכפלת $g^k=g^l$ ב-g^{-l}).
ולכן, לכל איבר $g\in G$ בחבורה סופית יש $m\geq 1$ טבעי כך ש- $g^m=e$.
ה- m המינימאלי הזה נקרא הסדר של g ונסמנו ב: $o(g)$.

הערה: הסדר של g הוא גודל תת-החבורה הנוצרת ע"י g.

$H=\{e,g,g^2,\dots,g^{m-1}\}$ אלה הם m איברים שונים, וקל לראות מכך ש: $g^m=e$ ונקבל כי $H=\{g^n \mid n\in\mathbb{Z}\}$.

כל $n\in\mathbb{Z}$ ניתן לרשום כ: $0\leq r\leq m-1$ $n=r+my$

$$g^n=g^{r+my}=g^r\cdot(g^m)^y=g^r\cdot e^y=g^r$$

25-10-2006 ②

מסקנה (אוילר): יהי $1<n\in\mathbb{N}$ ויהי $a\in\mathbb{Z}$ זר ל- n אזי: $a^{\phi(n)}\equiv 1 \bmod n$

הוכחה:

למה: תהי G חבורה סופית ויהי $g\in G$ איבר כלשהו בחבורה
אזי $g^{|G|}=e$

הוכחת הלמה: קיים $m=o(g)=|\langle g\rangle|$ כך ש: $g^m=e$

ממשפט לגרנז' $\Leftarrow$ $|G|=s\cdot m$ ולכן:

$$g^{|G|}=g^{s\cdot m}=(g^m)^s=e^s=e$$

עבור המסקנה, נתבונן במקרה הפרטי בו: $G=(\mathbb{Z}/n\mathbb{Z})^*$:

לכל $\bar{a}\in(\mathbb{Z}/n\mathbb{Z})^*$ מתקיים $\bar{a}^{\phi(n)}\equiv 1$ כאשר $\phi(n)=(\mathbb{Z}/n\mathbb{Z})^*$

ולכן לכל $a\in\mathbb{Z}$ זר ל- n מתקיים $a^{\phi(n)}\equiv 1 \bmod n$ $\square$

מסקנה (משפט פרמה הקטן): עבור p ראשוני, $a\in\mathbb{Z}$ $a^p\equiv a \bmod p$

$$\phi(p)=|(\mathbb{Z}/p\mathbb{Z})^*|=p-1$$

ומאוילר עבור a זר ל- p $a^{\phi(p)}=a^{p-1}\equiv 1 \bmod p$

$\Leftarrow$ $a^p\equiv a \bmod p$ עבור a זר ל- p

אם a אינו זר ל- p פרט המקרה כי $p|a$ ולכן $a^p\equiv 0\equiv a \bmod p$

בשעור הקודם הוכחנו את משפט לגרנג' וראינו מסקנות ממנו:

* אם G חבורה סופית אז $\forall g\in G$ $g^{|G|}=e$ (איבר בחזקת סדר החבורה שווה לאיבר היחידה)

* פונקצית אוילר

$$\forall n\in\mathbb{N}\ \forall a\ (a,n)=1 \Longrightarrow a^{\phi(n)}\equiv 1 \pmod n$$

חבורה ציקלית היא חבורה הנוצרת ע"י איבר אחד, כלומר חבורה מהצורה:

$$\{g^n \mid n\in\mathbb{Z}\}$$

דוגמאות: $\mathbb{Z}$

$\mathbb{Z}/_n\mathbb{Z}$ עבור $n\in\mathbb{N}$

טענה: אם G חבורה סופית מסדר ראשוני אזי G ציקלית (סדר החבורה הוא מספר האיברים בחבורה)

הוכחה: יהי $e\neq a\in G$ (שונה מאיבר היחידה) ונתבונן בתת החבורה הנוצרת ע"י a.

נסמנה ב- H. $H=\{a^n \mid n\in\mathbb{Z}\}$ ציקלית (כי נוצרת ע"י a)

היות ו $a,e\in H$ $|H|\geq 2$

ממשפט לגרנג' אנו יודעים כי $|H|\,\big|\,|G|$ לכן היות ו- $|G|$ ראשוני

נובע $|H|=|G|$ $\Leftarrow$ $H=G$

$\boxtimes$

משפט קושי: תהי G חבורה סופית מסדר $n=|G|$

יהי p ראשוני המחלק את n אזי יש ב-G איבר מסדר p

כלומר קיים $e\neq a\in G$ כך ש: $a^p=e$

הערה: אם $a\in G$ ו $a\neq e$, p ראשוני ו $a^p=e$

אזי לכל $1\leq i<p$ $a^i\neq e$

ניח בשלילה כי יהי $i\leq p$ מינימלי כך ש $a^i=e$

אזי $a^i=e$ $a^p=e$

הוכחה! $1<i<p$ נתבונן בחלוקת p ב-i עם שארית

$$0<s<i$$
$\uparrow$ כי p ראשוני

$$p=r\cdot i+s$$

$$e=a^p=a^{r\cdot i+s}=(a^i)^r\cdot a^s=e^r\cdot a^s=a^s$$

סתירה כי $1\le s<i$

הוכחת משפט קושי:

נסמן ב-$\Omega\subset G^p$ את אוסף כל ה-p-יות של איברי G שמכפלתן e

$$\Omega=\{(g_1,g_2,g_3,\dots,g_p)\mid g_1\cdot g_2\cdots g_p=e\}$$

$\Omega\neq\emptyset$ כי $(e,e,\dots,e)\in\Omega$

$$|\Omega|=|G|^{p-1}=n^{p-1}$$

(כי אם נבחר את $p-1$ האיברים הראשונים ב p-יה אז יש איבר שמשלים רק להגיע למכפלה e והאיבר הזה הוא יחיד.)

הסבר של המורה

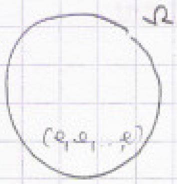
שכן יש לנו n^{p-1} אפשרויות לבחור $g_1,g_2,\dots,g_{p-1}\in G$ עם סדר

לכל בחירה כזו יש איבר יחיד $g_p\in G$ כך ש: $g_1\cdot g_2\cdots g_{p-1}\cdot g_p=e$

(והוא האיבר $g_p=(g_1 g_2\cdots g_{p-1})^{-1}$)

נשים לב כי המשפט טוען כי קיים ב-Ω איבר מהצורה $(\underbrace{a,a,\dots,a}_{p\text{ פעמים}})$

כאשר $a\neq e$.



נשים לב כי p מחלק את Ω כי $p\mid n$! $|\Omega|=n^{p-1}$

(כי $1\le p-1$!)

כמו כן נשים לב כי אם $(x_0,x_1,x_2,\dots,x_{p-1})\in\Omega$

$$\Longrightarrow (x_{p-1},x_0,x_1,x_2,\dots,x_{p-2})\in\Omega$$

ומאותה סיבה: $(x_{p-2},x_{p-1},x_0,x_1,\dots,x_{p-3})\in\Omega$

וכן הלאה

$\vdots$

30-10-2006

(2)

שכן אם $x_0 \cdot x_1 \cdot \ldots \cdot x_{p-1} = e$

אזי נכפול ב x_{p-1} משמאל ונקבל

$$x_{p-1} \cdot x_0 \cdot x_1 \cdot \ldots \cdot x_{p-1} = x_{p-1} \cdot e = x_{p-1}$$

נכפול ב: x_{p-1}^{-1} מימין ונקבל

$$x_{p-1} \cdot x_0 \cdot x_1 \cdot \ldots \cdot x_{p-2} = x_{p-1} \cdot x_0 \cdots x_{p-2} \cdot x_{p-1} \cdot x_{p-1}^{-1} =$$
$$= x_{p-1} \cdot x_{p-1}^{-1} = e$$

למה: (נוכח מהטעשם)

יהי p ראשוני

אם $(x_0, x_1, \ldots, x_{p-1})$ מינה מהצורה $x_0 = x_1 = x_2 = \ldots = x_{p-1}$

אזי כל p ה-p-יות $(x_i, x_{i+1}, \ldots, x_{p-1}, x_0, x_{i-1})$

$0 \leq i \leq p-1$ שונות זו מזו.

נדחה לרגע את הוכחת הלמה ונדגיש כי הלמה נכונה רק אם p ראשוני.

נאמר כי שני איברים $(x_0, \ldots, x_{p-1}), (y_0, \ldots, y_{p-1}) \in \Omega$

שקולים אם הם מתקבלים אחד מהשני ע"י סיבוב

הלמה אומרת כי מחלקות השקילות הן או מגודל 1 בדיוק כאשר האיבר מהצורה

$(a, a, \ldots a) \in \Omega$ או מגודל p.

הפירוק של Ω למחלקות שקילות מחלק אותה לקבוצות מגודל p או 1

היות וגודל Ω מתחלק ב-p הרי שמס' המחלקות מגודל 1 חייב להתחלק ב-p

היות ו! $(e, e, \ldots, e) \in \Omega$ הרי שיש לפחות חוק 1 מגודל 1 ולכן יש לפחות p רחוקים

מגודל 1 ולכן יש $e \neq a \in G$ כך ש: $\underbrace{(a, a, \ldots, a)}_{\text{פעמים}} \in \Omega$ כלומר $a^p = e$

$\square$

נעבור עתה להוכחת הלמה:

הוכחת הלמה:

תהי $\varphi_0 = (x_0, x_1, \dots, x_{p-1})$

סדרה מאורך p.

נתבונן באוסף כל הסיבובים שלה.

נחשוב על $(x_0, x_1, \dots, x_{p-1})$ כהעתקה

$$\varphi_0 : \mathbb{Z}/p\mathbb{Z} \longrightarrow G$$

$$\varphi_0(j) = x_j$$

הסיבובים הן הפונקציות $\varphi_r : \mathbb{Z}/p\mathbb{Z} \longrightarrow G$

$$\varphi_r(j) = \varphi_0(j+r)$$

צריך להראות כי או <u>א</u> φ_0 פונקציה קבועה או

<u>ב</u> $\varphi_0, \varphi_1, \dots, \varphi_{p-1}$ פונקציות שונות זו מזו

נניח כי <u>ב</u> אינו מתקיים כלומר לאיזשהם $r \neq s \in \mathbb{Z}/p\mathbb{Z}$

$$\varphi_r = \varphi_s$$

כלומר לכל j ב- $\mathbb{Z}/p\mathbb{Z}$

$$x_{r+j} = \varphi_r(j) = \varphi_s(j) = x_{s+j}$$

$\Longleftarrow$ עבור $t = r - s \neq 0 \in \mathbb{Z}/p\mathbb{Z}$

לכל j $\quad x_j = x_{j+t}$

$$x_0 = x_t = x_{2t} = x_{3t} = \dots = x_{(p-1)t} \quad (= x_{pt})$$

נזכור כי כל איבר $t \neq 0$ ב- $\mathbb{Z}/p\mathbb{Z}$ יוצר את $\mathbb{Z}/p\mathbb{Z}$

ולכן נובע כי $x_i = x_j$ לכל i, j ב- $\mathbb{Z}/p\mathbb{Z}$ ∎

30-10-2006

5

הומומורפיזם

הגדרה: תהיינה G ו L חבורות.

הומומורפיזם מ- G ל L הוא העתקה: $\varphi: G \longrightarrow L$

רק שלכל $a,b \in G$ $\varphi(ab)=\varphi(a)\cdot\varphi(b)$.

הומומורפיזם $\varphi: G \longrightarrow L$ יקרא **איזומורפיזם** אם φ חח"ע ועל.

דוגמאות:

א) $G=\mathbb{Z}$

$L=\mathbb{Z}/n\mathbb{Z}$

$\varphi(k)=(k+n\mathbb{Z})=k \bmod n$

ב) $G=\mathbb{Z}^2=\{(x,y) \mid x,y \in \mathbb{Z}\}$ (חיבור)

$L=\mathbb{Z}$

$\varphi((x,y))=x+3y$

ג) $L=(\mathbb{R}^*,\cdot)$

$\mathbb{R}^*=\{x \in \mathbb{R} \mid x \neq 0\}$

$G=(\mathbb{R},+)$

$\varphi: G \longrightarrow L$

$x \longmapsto e^x$

$\varphi(x)=e^x$

$\varphi(x+y)=e^{x+y}=e^x \cdot e^y=\varphi(x)\cdot\varphi(y)$

דוגמא: $G=GL_n(\mathbb{R})=\{A\in M_n(\mathbb{R})\mid det(A)\neq 0\}$

"מטריצות רגולריות, מטריצות הפיכות.

יהי V מרחב וקטורי n מימדי מעל $\mathbb{R}$

נתבונן באוסף כל הטרנספורמציות הלינאריות מ- V ל- V

נסמן ב- $Hom_{\mathbb{R}}(V,V)$. מוגדרת עליו פעולת הרכבה של פונקציות.

אם קובעים / בוחרים בסיס $v_1,\dots,v_n\in V$

אזי לכל טרנספורמציה $T:V\to V$ מתאימה מטריצה $A\in M_n(\mathbb{R})$

הרכבת טרנספורמציות לינאריות $\overset{\text{מתאימה:}}{\rightsquigarrow}$ כפל מטריצות.

אוסף כל הטרנספורמציות הלינאריות ההפיכות מ- V ל- V $Aut_{\mathbb{R}}(V)$

מהווה חבורה תחת הרכבת פונקציות.

$GL_n(\mathbb{R})$ מהווה חבורה ביחס לפעולה של כפל מטריצות כאשר איבר היחידה

הוא $I=\begin{pmatrix}1 & & 0\\ & \ddots & \\ 0 & & 1\end{pmatrix}$

נשים לב כי בהינתן בסיס קבוע $v_1,\dots v_n\in V$ ההעתקה המתאימה

$$\Phi: Aut_F(V)\to GL_n(F)$$
$$T\to A$$

המתאימה ~~את~~ ל- T את המטריצה ביחס לבסיס הנתון היא איזומורפיזם.

טענה: ההעתקה $det: GL_n(\mathbb{R})\to\mathbb{R}^*$

$A\longmapsto det(A)$ היא <u>הומומורפיזם</u>

משפט: תהיינה G ו- L חבורות ו $\varphi:G\to L$ הומומורפיזם

אזי תמונת G $\varphi(G)=\{\varphi(g)\mid g\in G\}$. היא תת-חבורה של L

הוכחה: $e_G\in G$, $\varphi(e_G)\in L \Leftarrow$ L אינה ריקה

נשים לב כי $\varphi(e_G)=e_L$ כי, הוכחה:

נתבונן ב- $e_G\cdot e_G=e_G$

אז $\varphi(e_G)=\varphi(e_G\cdot e_G)\underset{\text{הומומורפיזם}}{=}\varphi(e_G)\varphi(e_G)$

נכפיל מימין ב- $\varphi(e_G)^{-1}$

ונקבל $e_L=\varphi(e_G)\cdot\varphi(e_G)^{-1}=\varphi(e_G)\cancel{\varphi(e_G)}\varphi(e_G)^{-1}=e_L$

30-10-2006

$= \varphi(G_G) e_L = \varphi(e_G)$

המשך ההוכחה:

$\varphi(G)$ סגורה לכפל כי אם $x', y' \in \varphi(G)$

אז קיימים $x, y \in G$ כך ש: $\varphi(x) = x'$

$\varphi(y) = y'$

$$x'y' = \varphi(x)\varphi(y) = \varphi(xy) \in \varphi(G)$$

קיום הפכי:

נניח $x' \in \varphi(G)$ אז קיים $x \in G$ כך ש $\varphi(x) = x'$

נשים לב כי

$$\varphi(x^{-1})\varphi(x) = \varphi(x^{-1}x) = \varphi(e_G) = e_L$$

$$\Longrightarrow (x')^{-1} = \varphi(x)^{-1} = \varphi(x^{-1}) \in \varphi(G)$$

הגדרה: גרעין (Kernel) של הומומורפיזם $\varphi: G \longrightarrow L$ הוא:

$$Ker(\varphi) = \{g \in G \mid \varphi(g) = e_L\}$$

משפט: גרעין של הומומורפיזם $\varphi: G \longrightarrow L$ הוא תת-חבורה של G

הוכחה: נשים לב כי היות $\varphi(e) = e$ נובע כי $e \in Ker(\varphi)$

נניח כי $x, y \in Ker\varphi$

אז: $\varphi(xy) = \varphi(x)\varphi(y) = e \cdot e = e$

$\Leftarrow$ $xy \in Ker\varphi$

נניח עתה $x \in Ker\varphi$ אז $\varphi(x^{-1}) = \varphi(x)^{-1} = e^{-1} = e$

$\Longrightarrow x^{-1} \in Ker\varphi$ $\square$

שאלה: נתון מרחב וקטורי V ותת מרחב W (נניח שם סטטור מימד סופי)

האם ~~קיימת~~ קיים מרחב U והעתקה לינארית $T: V \longrightarrow U$

כך שגרעין T הוא W?

למה: תהי $\varphi: G \longrightarrow L$ הומומורפיזם.

נסמן $N=\mathrm{Ker}\varphi$ אזי לכל $g\in G$ ולכל $n\in N$

$g^{-1}ng \in N$ הצמדת n ע"י g

הוכחה: צריך להראות כי הצמדה היא איבר מגרעין

$g^{-1}ng$

$$\varphi(g^{-1}ng)=\varphi(g^{-1})\varphi(n)\varphi(g)=$$

$$=\varphi(g)^{-1}e\varphi(g)=\varphi(g)^{-1}\varphi(g)=e$$

הגדרה: תת חבורה N של G תקרא נורמלית אם לכל $g\in G$ ולכל $n\in N$

$g^{-1}ng\in N$

משפט: $N\lhd G$ תת חבורה נורמלית $\Longleftrightarrow$ לכל $g\in G$ $g^{-1}Ng=N$ $\Longleftrightarrow$ $\forall g\in G\ gN=Ng$

(שיוויון מחלקות ימניות ושמאליות)

1-11-2006

מבנים אלגבריים - שעור מס' 4

חבורות, תתי חבורות ...

גרעין: אם $\varphi: G \longrightarrow L$ הומומורפיזם אז

$$\ker\varphi = \{g \in G \mid \varphi(g) = e\}$$

גרעין של הומומורפיזם הוא תת-חבורה נורמלית.

$N \lhd G$ תקרא נורמלית אם:

$$\forall g \in G,\ \forall n \in N \quad g^{-1}ng \in N$$

טענה: התכונות הבאות שקולות:

Ⓐ $\forall g \in G,\ \forall n \in N \quad g^{-1}ng \in N$

$(\forall g \quad gNg^{-1} \subset N)$

Ⓑ $\forall g \in G \quad g^{-1}Ng = N$

Ⓒ $\forall g \in G \quad Ng = gN$ (שיוויון מחלקות ימניות ושמאליות)

הערות: אם G חבורה, $A, B \subset G$ תתי-חבורות

אז: $AB = \{ab \mid a \in A,\ b \in B\}$ $\quad Ag = \{ag \mid a \in A\}$

$$gA = \{ga \mid a \in A\}$$

הוכחה: א' ⇐ ב': נתון כי $g^{-1}Ng \subset N \Longleftarrow N = g(g^{-1}Ng)g^{-1} \subset gNg^{-1}$

ולכן $g \in G$ $\quad N \subset gNg^{-1}$

אנחנו כופלים את שני האגפים ב- g משמאל וב- g^{-1} מימין

קיבלנו כי לכל $g \in G$ $\quad N \subset g^{-1}Ng \Longleftarrow N = g^{-1}Ng$

ב' ⇐ ג': נתון כי $g^{-1}Ng = N$, $\forall g \in G$

$\Longleftarrow Ng = g(g^{-1}Ng) = Ng \ \forall g \in G$ (כפלנו את שני האגפים משמאל ב- g^{-1})

ג' ⇐ א': נתון כי $Ng = gN$ לכל $g \in G$

$\Longrightarrow \forall g \in G,\ g^{-1}Ng = g^{-1}gN = N$

(שוב, כפל של שני האגפים משמאל ב- g^{-1})

$\blacksquare$

תרגיל: התבוננו בחבורה S_3 ותהי $H<S_3$

תת חבורה שמקיימת $H(3)=3$ בדקו שחבורה זו אינה נורמלית.

למה: תהי $N \triangleleft G$ תת-חבורה נורמלית, אזי לכל $x,y \in G$ $(Nx)(Ny)=xyN$

הוכחה: $$Nx \cdot Ny = N\underbrace{(xN)}_{Nx}y = \underbrace{N \cdot N}_{N}xy = Nxy = xyN$$

הערה: היות ו-N תת-חבורה היא סגורה לכפל כלומר לכל $n,m \in N$ $N \cdot N \subset N$

ומצד שני $N \ni$ לכן $e \in N$ $N \subset N \cdot N$ ולכן השיוויון.

הגדרה: תהי G חבורה, N תת-חבורה נורמלית אזי קבוצת המחלקות (שמאליות = ימניות)

$G/N=\{gN \mid g \in G\}$ מהווה חבורה ביחס לכפל של תתי קבוצות מ-G.

G/N נקראית חבורת המנה של G מודולו N.

נראה כי זו אכן חבורה:

* ראשית נראה סגירות לכפל:

לכל $xN, yN \in G/N$ מכפלתן שווה ע"פ הלמה $xy \cdot N \in G/N$

ולכן מתקיימת סגירות.

* אסוציאטיביות: אם $aN, bN, cN \in G/N$

$$((aN)(bN))(cN) = (abN) \cdot cN = abcN = a(bc)N =$$

$$= aN(bcN) = aN((bN)(cN))$$

* קיום איבר יחידה: איבר היחידה הוא $N \in G/N$ כי לכל $aN \in G/N$ מתקיים:

$$NaN = aNN = aN$$

* קיום הפכי: עבור $aN \in G/N$

$$(a^{-1}N)(aN) = aa^{-1}N = N$$

האקסיומות אכן מתקיימות ולכן זוהי חבורה.

בהינתן N תת-חבורה נורמלית, קיים הומומורפיזם (טבעי)

$$\varphi: G \longrightarrow G/N$$
$$g \longrightarrow gN$$

<u>תרגיל</u>: בידקו כי זהו אפימורפיזם (על סמך הלמה)

<u>טענה</u>: $N \triangleleft G$, גרעין ההומומורפיזם הטבעי הוא N.

<u>הוכחה</u>: $\mathrm{Ker}\varphi = \{g \in G \mid \varphi(g) = N\} =$

$$= \{g \in G \mid g \cdot N = N\} = \{g \in G \mid g \in N\} = N$$

<u>טענה</u>: יהי $\varphi: G \longrightarrow L$ הומומורפיזם אזי:

(א) φ חח"ע $\iff$ $\mathrm{Ker}\varphi = \{e\}$

(ב) עבור כל $z \in \varphi(G) \subset L$

$$\varphi^{-1}(z) = \{g \in G \mid \varphi(G) = z\} = xN$$

כאשר: $N \in \mathrm{Ker}\varphi$, $\varphi(x) = z$

<u>הוכחה</u>: די להראות את (ב):

יהי $x \in G$, $\varphi(x) = z \in L$

נניח כי $y = \varphi^{-1}(z)$ כלומר $\varphi(y) = z$

נתבונן ב:

$$\varphi(yx^{-1}) = \varphi(y)\cdot\varphi(x^{-1}) = \varphi(y)\varphi^{-1}(x) = z \cdot z^{-1} = e$$

ולכן $\varphi^{-1}(z) \subset Nx$

מצד שני עבור כל $n \in N$ $\varphi(nx) = \varphi(n)\varphi(x) = e \cdot z = z$

$\Longleftarrow$ $n \in \varphi^{-1}(z)$

$\Longleftarrow$ $Nx \subset \varphi^{-1}(z)$

$$\Longrightarrow \varphi^{-1}(z) = Nx$$

▨

טענה: יהי $\varphi: G\longrightarrow L$ הומומורפיזם ותהי K תת-חבורה של L

אז: $\{g\in G \mid \varphi(g)\in K\} = \varphi^{-1}(K)$

היא תת-חבורה של G המכילה את $Ker\varphi$

הוכחה: נשים לב כי $Ker\varphi \subset \varphi^{-1}(K)$ ולכן בפרט $\varphi^{-1}(K)$ אינו ריק.

אם $x,y\in\varphi^{-1}(K)$ אז: סגור לכפל: $\varphi(x\cdot y)=\underset{K}{\varphi(x)}\cdot\underset{K}{\varphi(y)}\in K$

$\Longrightarrow x\cdot y\in\varphi^{-1}(K)$

סגור להפכי: $\varphi(x^{-1}) = \varphi(x)^{-1}\in K$ $\quad \forall x\in\varphi^{-1}(x)$

☒

הערה: אם G חבורה קומוטטיבית אז כל תת-חבורה שלה היא נורמלית

משפט: תהי G חבורה אבלית סופית מסדר n ויהי d טבעי אשר מחלק את n

אז יש ל-G תת-חבורה מסדר d

הוכחה: באינדוקציה על $n=|G|$ (הסדר של G)

אם $n=1$ אז זה ברור.

תהי G חבורה קומוטטיבית מסדר n ומניחים את המשפט על חבורות מסדר קטן יותר.

יהי $d|n$; אם $d=1 \Longrightarrow$ ברור

אחרת יהי p ראשוני המחלק את d ולכן גם את n.

ממשפט קושי נובע כי קיימת תת חבורה N ב-G מסדר p. היות ו-G קומוטטיבית,

N נורמלית ולכן נוכל להתבונן בחבורת המנה $\bar{G}=G/N$ זוהי חבורה

סופית מסדר $n/p>1$ ולכן מאינדוקציה יש לה תת-חבורה $\bar{H}<\bar{G}$ מסדר $\frac{d}{p}$.

נתבונן ב $\varphi^{-1}(\bar{H})$ וזוהי תת-חבורה של G מסדר d

כאשר $\varphi: G\to\bar{G}$ ההומומורפיזם הטבעי.

☒

6-11-2006

מבנים אלגבריים - שעור מס' 5

נזכר בכמה דברים שעשינו בשעור הקודם ונתקן כמה דברים.

ניזכר בהגדרה של חבורה נורמלית: G חבורה, N תת-חבורה של G אם $gNg^{-1}=N$ $\forall g\in G$ ונסמן $N\lhd G$.

הגדרה: חבורה G תקרא פשוטה אם אין לה תתי-חבורות נורמליות לא טריוויאליות (כלומר פרט ל-G ול-$\{e\}$)

מיון חבורות פשוטות סופיות

* $\mathbb{Z}/p\mathbb{Z}$ החבורה הציקלית בת p (ראשוני) איברים.

* A_n חבורת חבורת התמורות הזוגיות על קב' בת n איברים כאשר $n\geq 5$

ישנו מספר סופי של משפחות (אינסופיות) של חבורות פשוטות.

בשעור הקודם גם הגדרנו חבורת מנה:

$N\lhd G$ אזי לאוסף המחלקות (השמאליות) של G G/N יש מבנה של חבורה.

קיים הומומורפיזם $\varphi: G\to G/N$

כמו כן ראינו טענה:

אם $\varphi: G\to L$ הומומורפיזם על ו- $N=\ker\varphi$

אזי לכל K תת-חבורה $K<L$ $\varphi^{-1}(K)\supset\ker\varphi$ היא תת-חבורה של G.

כאשר φ על אזי מקבלים התאמה חח"ע ועל בין תתי-חבורות של L לבין תתי חבורות של G המכילות את $\ker\varphi$.

משפט: תהי G חבורה אבלית סופית. אז לכל d המחלק את $|G|=n$ יש ל-G תת-חבורה מסדר d.

הוכחה בשעור הבא

הוכחה: נוכיח באינדוקציה.

אם $d=1$ זה ברור.

נוכיח באינדוקציה על n. עבור $n=1$ זה ברור. יהי n כך שלכל $m<n$ לכל חבורה אבלית מסדר m יש תת-חבורות מכל גודל המחלק את m.

יהי p ראשוני המחלק את d. היות ו- $d|n$ גם $p|n$

ולכן לפי משפט קושי יש ל- G תת-חבורה N מסדר p.

היות ו- G אבלית N היא תת-חבורה נורמלית ולכן נוכל לדבר על חבורת המנה.

נתבונן ב- $\bar{G} = G/N = \{gN \mid g\in G\}$

זוהי חבורה מסדר $\frac{n}{p} < n$, כמו כן נשים לב כי $\frac{d}{p}$ מחלק את $\frac{n}{p}$

לכן לפי הנחת האינדוקציה יש תת-חבורה $\bar{H}$ של $\bar{G} = G/N$ מסדר $\frac{d}{p}$.

נתבונן ב ההומומורפיזם הטבעי $\varphi: G \longrightarrow G/N = \bar{G}$ $\varphi(g) = gN$.

המקור של $\bar{H}$ הוא תת-חבורה $\varphi^{-1}(\bar{H})$ ב- G

היות וההעתקה φ היא p ל- 1 (כלומר לכל איבר בתמונה יש בדיוק p מקורות)

$$|\varphi^{-1}(\bar{H})| = p|\bar{H}| = p\cdot\frac{d}{p} = d$$

∎

משפטי ההומומורפיזם

משפט ההומומורפיזם הראשון: (מוכר כמשפט האיזומורפיזם השני בספרים מסוימים)

תהינה G,L חבורות $\psi: G \longrightarrow L$ הומומורפיזם על $(\psi(G)=L)$

$N=\ker\psi$ אזי קיים איזומורפיזם (טבעי):

$$\tilde{\psi}: G/N \longrightarrow L$$

הנתון על ידי $\bar{\psi}(gN) = \psi(g)$

הערה: מובלעת כאן הטענה שההעתקה $\bar{\psi}$ מוגדרת היטב. כלומר אם $gN=g'N$ אזי $\psi(g)=\psi(g')$ ואכן אם $gN=g'N$ אזי קיים $n\in N$ כך ש: $g=g'n$

$$\psi(g) = \psi(g'n) = \psi(g')\cdot\psi(n) = \psi(g')e = \psi(g')$$

הוכחה: $\bar{\psi}$ היא הומומורפיזם.

יהיו $g_1N, g_2N \in G/N$

$$\bar{\psi}((g_1N)(g_2N)) \overset{\text{כפל ב- } G/N}{=} \bar{\psi}(g_1g_2N) \overset{\text{הגדרת } \bar{\psi}}{=}$$

$$= \psi(g_1g_2) \overset{\psi \text{ הומומורפיזם}}{=} \psi(g_1)\psi(g_2) = \bar{\psi}(g_1N)\bar{\psi}(g_2N)$$

6-11-2006

$\bar{\Psi}$ על: יהי $g\in L$ אזי קיים $g_0\in G$ כך ש $\Psi(g_0)=g$

כי Ψ על ולכן $\bar{\Psi}(g_0N)=\Psi(g_0)=g$

$\bar{\Psi}$ חח"ע: כדי להראות חח"ע די להראות כי הגרעין הוא מינימלי

נניח כי $\bar{\Psi}(gN)=e$

פירוש הדבר $e=\bar{\Psi}(gN)=\Psi(g)$ $\Longleftarrow$ $g\in \ker\Psi=N$

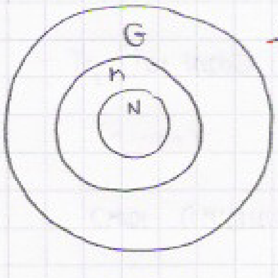
$\Longleftarrow$ $gN=N$

ולכן $\bar{\Psi}^{-1}(e)=\{N\}$

$\bar{\Psi}$ הוא חח"ע $\Longleftarrow$ $\bar{\Psi}$ איזומורפיזם.

■

משפט האיזומורפיזם השני (האיזומורפיזם הראשון):



תהי G חבורה ותהיינה $K,N\triangleleft G$ תתי-חבורות נורמליות

ב- G ונניח כי N מוכלת ב- K אזי N נורמלית ב- K

ומתקיים: $G/K \cong (G/N)/(K/N)$

כלומר $\bar{K}=K/N$ היא תת-חבורה נורמלית ב- $G/N=\bar{G}$

וקיים $\bar{G}/\bar{K}\cong G/K$

הוכחה:

היות ו- $N\triangleleft G$ נובע $N\triangleleft K$ כי: $N\triangleleft G \Longleftrightarrow gNg^{-1}=N \quad \forall g\in G$

$N\triangleleft K \Longleftrightarrow kNk^{-1}=N \quad \forall k\in K$

לכן מוגדרות חבורות המנה: G/N, K/N ! G/K

נגדיר העתקה: $\rho: G/N \to G/K$

ע"י: $\rho(gN)=gK$

צריך לבדוק שזה מוגדר היטב כי ניתן היה לרשום

$$\rho(gN)=g\cdot N\cdot K=g(\underbrace{NK}_{K})=gK$$

לחילופין ניתן היה לנסח זאת באופן הבא: נניח $gN=g'N$ אזי קיים $n\in N$ כך ש: $g=g'n$

ולכן $gK=g'nK=g'K$

(כי $n\in K$ ו K תת-חבורה)

צריך להוכיח כי ρ הומומורפיזם ו- ρ היא על G/K ולכן $G/K \cong {(G/N)}/{\ker\rho}$

וצריך להוכיח גם $\ker\rho \cong K/N$.

(א) ρ היא הומומורפיזם. יהיו $g_1N, g_2N \in \bar{G}$

$\rho(g_1N \cdot g_2N) \underset{\text{כפל ב-} \bar{G}}{=} \rho(g_1g_2N) \underset{\text{הגדרת } \rho}{=} g_1g_2K \underset{\text{כפל ב-} G/K}{=} g_1K \cdot g_2K = \rho(g_1N)\rho(g_2N)$ כלומר זהו הומומורפיזם.

(ב) ρ על $G/K \ni gK$

נבחר $g' \in gK$ $g' = gk'$ אזי: $\rho(g'N) = g'K = gK$, $g'K = gk'K$

נותר לחשב את גרעין ρ = $\ker\rho = \{gN \in G/N \mid \rho(gN) = K\}$ (איבר היחידה ב- G/K)

$= \{gN \mid gK = K\} = \{gN \mid g \in K\} \underset{\text{ההגדרה}}{=} K/N$

לכן לפי משפט ההומומורפיזם הראשון נובע כי $G/K \cong {(G/N)}/{(K/N)}$

(תוספת):

כאשר האיזומורפיזם מ- ${(G/N)}/{(K/N)}$ נתון ע"י

$\bar{\rho}\,((gN)(K/N)) = gK$

נובע ע"פ ההוכחה שנתנו למשפט ההומומורפיזם הראשון.

משפט ההומומורפיזם השלישי: (האיזומורפיזם השני)

תהי G חבורה. תהי $N \lhd G$ תת-חבורה נורמלית. $A < G$ תת-חבורה (לא מניחים שום יחס הכלה בין N ו- A)

אזי קיים איזומורפיזם $A/(A\cap N) \cong AN/N$

הערות: (1) אם $N \lhd G$ תת-חבורה נורמלית ו- $A < G$ תת-חבורה

אזי $AN = \{an \mid {a\in A \atop n \in N}\}$ תת-חבורה ב- G

נשים לב כי $N \subset AN$, $\{en \mid n \in N\}$

היות ו- N נורמלית ב- G היא תת-חבורה נורמלית גם ב- AN ולכן ניתן להתבונן בחבורת המנה AN/N.

6-11-2006 ③

② חיתוך תתי חבורות הוא תת-חבורה.

וכאשר N נורמלית ב-G נוכיח כי $A\cap N$ נורמלית ב-A.

צריך להראות כי אם $a\in A$ ו $x\in A\cap N$ אזי $axa^{-1}\in A\cap N$

נבדוק: נתון $a\in A$ $x\in A\cap N$ נתבונן ב- axa^{-1}

$x\in N$ ולכן היות ו $G\rhd N$ $axa^{-1}\in N$ $a\in A$ $x\in A \Rightarrow axa^{-1}\in A$

$\Rightarrow axa^{-1}\in A\cap N$

הוכחה: (משפט ההומומורפיזם השלישי = משפט האיזומורפיזם השני)

נבנה הומומורפיזם מ-A על AN/N ונראה כי הגרעין שלו הוא $A\cap N$.

יהי: $\psi: A\longrightarrow AN/N$

$$\psi(a)=aN\in AN/N$$

ברור כי ψ הומומורפיזם: $\psi(ab)=abN=aNbN=\psi(a)\psi(b)$

- צריך להראות כי ψ היא על:

יהי $\bar{x}\in AN/N$ אזי $\bar{x}$ הוא מהצורה $(an)N$ כאשר $a\in A$ $n\in N$

ולכן $\bar{x}=aN$ כלומר $\bar{x}=\psi(a)$.

נותר לחשב את גרעין ψ.

$$\ker\psi=\{a\in A\mid \psi(a)=\overset{\text{יחידה ב-}AN/N}{N}\}=$$

$$=\{a\in A\mid aN=N\}=\{a\in A\mid a\in N\}=A\cap N$$

נתייחס עכשיו להערה מס ①:

טענה: תהי G חבורה ותהיינה $H,K<G$ תתי-חבורות של G אזי HK היא תת-חבורה

אם ורק אם $HK=KH$ (התכונה כאן היא כקבוצות, זה לא אומר שהאיברים מתחלפים איבר איבר)

כלומר: $HK=\{hk\mid h\in K\ \ k\in K\}$

$KH=\{kh\mid k\in K,\ h\in H\}$

$HK=KH \Longleftrightarrow$ לכל $h_1\in H$ $k_1\in K$

קיימים $h_2\in H$ $k_2\in K$ כך ש: $h_1k_1=k_2h_2$

הוכחת הטענה: נניח $HK=KH$. נשים לב כי $e\in HK\neq\emptyset$.

יהיו $x,y\in HK$ אזי:

$$xy\in HK\cdot HK=H(KH)K=$$

$$=H(HK)K=H\cdot H\cdot K\cdot K=HK$$

אז יש סגירות

זה סגור להפכי כי אם $x \in HK = KH$ לכן קיימים $h \in H$, $k \in K$

ומתקיים $x = kh \Leftarrow x^{-1} = h^{-1}k^{-1} \in HK$

כיוון שני: אם HK תת-חבורה אזי $KH = HK$ (תרגיל).

הוכחת הערה ג'

אם N נורמלית ב-G אזי לכל $g \in G$ $gN = Ng$ בפרט לכל $a \in A$ $aN = Na$

$$AN = \bigcup_{a \in A} aN = \bigcup_{a \in A} Na = NA$$

מבנים אלגבריים - שיעור מס' 6

הגדרה:

G חבורה , $X \subset G$ תת-קבוצה. אזי תת-החבורה הנוצרת ע"י X היא תת-החבורה המינימלית H של G כך ש $X \subset H$.

נסמן תת-חבורה כזו כ: $\langle X \rangle$

הערה: $\langle X \rangle$ קיימת:

ניתן לזה שם

$$\langle X \rangle = \bigcap_{\substack{K \in G \\ X \subset K}} K = A$$

$$\emptyset \neq \{K \mid K<G \text{ תת-חבורה}, \ K \text{ מכילה את } X\}$$

נשים לב כי:

A היא תת-חבורה ו- A היא מינימלית מבין כל תתי-החבורות המכילות את X

כי מהגדרה של A לכל $X \subset K < G$ השתתפה בחיתוך (ידוע כי חיתוך של תתי-חבורות הוא תת-חבורה) ולכן $A \subset K$.

כי: $a,b \in \bigcap_{K \in \Omega} K \Leftarrow$ לכל $K \in \Omega$ $a,b \in K$ (Ω היא הקבוצה של תתי-החבורות)

$\Leftarrow$ לכל $K \in \Omega$ $ab \in K$, $a^{-1} \in K$

$\Leftarrow$ $ab \in \bigcap_{K \in \Omega} K$, $a^{-1} \in \bigcap_{K \in \Omega} K$

דרך לבנית תת-החבורה המינימלית המכילה את X:

תהי $X \subset G$ תת-קבוצה:

נתבונן ב: $B = \{x_1^{\varepsilon_1} x_2^{\varepsilon_2} \cdots x_s^{\varepsilon_s} \in G \mid x_i \in X, \ \varepsilon_i \in \{\pm 1\}, \ s \in \mathbb{N} \cup \{0\}\}$

כאשר את המכפלה הריקה $(s=0)$ נפרש כמסמנת את איבר היחידה של G

נשים לב כי B היא תת חבורה של G:

① $e \in B$ ② אם $x_1^{\varepsilon_1} x_2^{\varepsilon_2} \cdots x_n^{\varepsilon_n} \in B$, $y_1^{\alpha_1} \cdots y_m^{\alpha_m} \in B$ $\Leftarrow$ $x_1^{\varepsilon_1} \cdots x_n^{\varepsilon_n} \cdot y_1^{\alpha_1} \cdots y_m^{\alpha_m} \in B$

③ $x_1^{\varepsilon_1} \cdots x_n^{\varepsilon_n} \in B \Leftarrow x_1^{-\varepsilon_1} \cdots x_n^{-\varepsilon_n} \in B$

כי: $x_1^{\varepsilon_1} \cdots x_n^{\varepsilon_n} \cdot x_1^{-\varepsilon_1} \cdots x_n^{-\varepsilon_n} = e$

קיבלנו כי:

$$\langle X\rangle \subset \{x_1^{\epsilon_1}\cdots x_n^{\epsilon_n} \mid n\geq 0,\ x_i\in X,\ \epsilon_i\in\{\pm1\},\ 1\leq i\leq n\}$$

מאידך ברור כי אם H תת-חבורה של G ו- $X\subset H$

אזי לכל $n\geq 0$ ולכל $x_1,\ldots,x_n\in X$ ו- $\epsilon_1,\ldots,\epsilon_n\in\{\pm1\}$

מתקיים $x_1^{\epsilon_1}\cdots\cdots x_n^{\epsilon_n}\in H$

ולכן $\langle X\rangle \supset \{x_1^{\epsilon_1}\cdots x_n^{\epsilon_n} \mid \ldots\ldots\}$

מתקיימת הכלה דו-כיוונית ולכן מתקיים שוויון

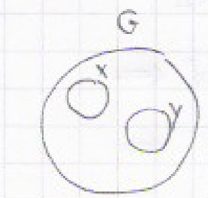
נשאל: מה מספר האיברים המינימלים כדי לייצר את G:

תהי G חבורה. נסמן ב- $d(G)$ את העוצמה ("הגודל") המינימלית של קבוצת יוצרים של G.

$$\min\{|X| \mid \langle X\rangle = G \quad X\subset G\}$$

אם יש ל-G קבוצת יוצרים סופית אזי (נאמר ש-G נוצרת סופית)

ונסמן $d(G) =$ גודל מינימלי של קבוצת יוצרים של G; אחרת $d(G)=\infty$.



$|X| \quad \langle X\rangle = G$

$|Y| \quad \langle Y\rangle = G$

דוגמא: תהי $G=S_n$ חבורת התמורות על n איברים. $n\geq 3$

$d(S_n)=2$ כי: $\sigma=(1,2,\ldots,n)$ $\tau=(1,2)$

$$\langle \tau,\sigma\rangle = S_n$$

$$\Downarrow$$

$$d(S_n)\leq 2$$

$$d(S_n)\geq 2 \quad 3\leq n$$

כי S_n עבור $n\geq 3$ אינה אבלית $\Leftarrow$ אינה ציקלית.

8-11-2006

②

דוגמא נוספת:

$$S=\{(1,2),(2,3),\ldots\ldots,(n-1,n)\}$$

$$\langle S\rangle = S_n$$

תרגיל: כל תת-קבוצה ממש של S אינה יוצרת את S_n.

טענה: תהיינה G,L חבורות נוצרות סופית ונניח כי קיים הומומורפיזם $\varphi: G\longrightarrow L$ על

אזי $d(G)\geq d(L)$

הוכחה: תהי $X\subset G$ קבוצת יוצרים מגודל מינימלי כלומר $|X|=d(G)$

אז היות ו- $\varphi(G)=L$ (כי φ על) ו- $\langle X\rangle=G$ נובע כי $\underset{L}{\varphi(G)}=\langle\varphi(X)\rangle$

לכן $\varphi(X)$ קבוצת יוצרים של L

ולכן $d(L)\leq|\varphi(X)|\leq \underset{d(G)}{|X|}$ $\Leftarrow$ $d(L)\leq d(G)$

הסבר: $\varphi(G)\supset\varphi(X)$ היא תת-חבורה

$\Leftarrow$ $\varphi(G)\supset\langle\varphi(X)\rangle$

כל $g\in G$ הוא מהצורה $g=x_1^{\varepsilon_1}\cdots\cdots x_n^{\varepsilon_n}$

והיות וזה הומומורפיזם: $\varphi(g)=\varphi(x_1)^{\varepsilon_1}\cdots\cdots\varphi(x_n)^{\varepsilon_n}\in\langle\varphi(X)\rangle$

שאלה: (א) האם יש חבורה G כך שלכל חבורה L כך ש: $d(L)=7$

יש הומומורפיזם מ- G על L?

סימון כללי: L_1,L_2 חבורות כלשהן. האם יש חבורה G כך שיש הומומורפיזמים $\varphi_i: G\longrightarrow L_i$ $\quad i=1,2$

התשובה: כן!

נתבונן במכפלה הישרה של L_1 ו- L_2

$$G=L_1\times L_2=\{(g_1,g_2)\mid g_i\in L_i\}$$

עם כפל קואורדינטה קואורדינטה

$$(g_1,g_2)(g_1',g_2')=(g_1g_1',g_2g_2')$$

אזי $\varphi_i: L_1\times L_2\longrightarrow L_i$

$$\varphi_i(g_1,g_2)=g_i$$

נחזור לשאלה המקורית (*)

אפשר להתבונן במכפלה הישרה של כל החבורות הנוצרות ע"י 7 איברים.

(נמשיך לדבר על זה בשיעור הבא)

הגדרה: תהי X קבוצה כלשהי. החבורה החופשית הנוצרת ע"י X שתסומן ב- $F(X)$ היא החבורה G כך שמתקיימות התכונות הבאות:

(א) $X \subset G$

(ב) לכל חבורה H ולכל העתקה $\alpha : X \longrightarrow H$

קיים הומומורפיזם יחיד $\varphi : G \longrightarrow H$ כך ש: $\varphi|_X = \alpha$

גם על הגדרה זו נמשיך לדבר בשיעור הבא

13-11-2006

חבורה חופשית

תהי X קבוצה. החבורה החופשית הנוצרת ע"י X תהיה החבורה G רק שמתקיים:

① $X \subset G$

② לכל חבורה H והעתקה (כלשהי) $f: X \longrightarrow H$
קיים הומומורפיזם יחיד $\varphi: G \longrightarrow H$ כך ש: $\varphi|_X = f$

נסמן חבורה כזו ב-$F(X)$.

צריך להראות כי קיימת חבורה כזו G ו-G יחידה (עד כדי איזומורפיזם)

טענה: תהי X קבוצה. אם G_1, G_2 הן חבורות המקיימות את התנאים $1, 2$ אז הן איזומורפיות.

הוכחה: נתבונן בהעתקה $id = f_1 : X \longrightarrow X$ (הזהות)

$f_1(x) = x$ $\quad f_1(x)=x$

היות ו-G_1 מקיימת את 2 יש הומומורפיזם יחיד $\varphi_1: G_1 \longrightarrow G_2$
כך ש: $\varphi_1|_X = f_1 = id$

מאידך אם נתבונן בהעתקת הזהות מ-X ל-X כהעתקה $f_2: X \longrightarrow G$, $x \longmapsto x$

אז מההנחה לגבי G_2 קיים הומומורפיזם יחיד $\varphi_2|_X = id$ $\varphi_2 : G_2 \longrightarrow G_1$

נתבונן בהרכבה $\varphi_2 \circ \varphi_1$ זהו הומומורפיזם $\varphi_2 \circ \varphi_1 : G_1 \longrightarrow G_1$

נשים לב ש: $id_G = \varphi_2 \circ \varphi_1$ שכן $\varphi_2 \circ \varphi_1|_X = id_X$

לפי 2 לגבי G_1 יש רק הומומורפיזם יחיד מ $G_1 \longrightarrow G$

אשר צמצומו ל-X הוא הזהות על X.

היות והעתקת הזהות $id_{G_1}: G_1 \longrightarrow G_1$ אף היא הומומורפיזם שצמצומו ל-X הוא הזהות על X, נובע כי $\varphi_2 \circ \varphi_1 = id_{G_1}$.

באופן דומה מקבלים $\varphi_1 \circ \varphi_2 = id_{G_2} \Longleftarrow G_1, G_2$ איזומורפיות

∎

טענה: X יוצרת את $F(X)$

הוכחה: נסמן ב-H את תת-החבורה של G הנוצרת על ידי X.
(הגדרה התחרה) נוכיח צורה לאחר שנראה קיום.

קיום

תהי X קבוצה. נסמן ב- $\Sigma = X \uplus \bar{X}$ כאשר $\bar{X} = \{\bar{x} \mid x \in X\}$

(אלו הם איברים חדשים שלא היו קודם ב-X, לכל $x \in X$ מתאים $\bar{X}$) אלו הם סמלים, כי עדיין לא הוגדרה לכן עדיין לא מדברים על הכל.

נסמן ב: $\Sigma^* = \left\{ \begin{array}{c} \text{מילים סופיות} \\ \text{באורך } 0 \leq \\ \text{מאותיות } \Sigma \end{array} \right\}$

$= \left\{ a_1 a_2 \dots a_n \,\middle|\, \begin{array}{l} n \geq 0 \\ a_i \in \Sigma \end{array} \right\}$

כאשר עבור $n=0$, המילה הריקה, נסמנה ב- e.

דוגמא: נניח $X = \{a, b\}$

$\bar{X} = \{\bar{a}, \bar{b}\}$

$\Sigma = \{a, b, \bar{a}, \bar{b}\}$

$\Sigma^* = \{a, \bar{a}, b, \bar{b}, \bar{a}b, abb\bar{b} \dots\}$

על Σ^* יש לנו פעולה של שרשור (שרשור של שתי מילים)

נגדיר על Σ^* יחס שקילות המוגדר הבא:

שתי מילים $w_1, w_2 \in \Sigma^*$ יקראו שקולות אלמנטרית אם ניתן לעבור מאחת לשניה

על ידי צמצום של $x\bar{x}$ או $\bar{x}x$

או $w_1 = \begin{cases} u\bar{x}xv \\ ux\bar{x}v \end{cases}$

כאשר $u, v \in \Sigma^*$ $x \in X$

! $w_2 = uv$

או להיפך $w_2 = \begin{cases} ux\bar{x}v \\ u\bar{x}xv \end{cases}$

! $w_1 = uv$

⋮

נעיר: שתי מילים w, w' יקראו שקולות $w \sim w'$

אם ניתן לעבור מאחת לשניה על ידי סדרה סופית כלשהי של

שקילויות אלמנטריות

הגדרה: מילה $w \in \Sigma^*$ תקרא מצומצמת אם היא לא מכילה $x\bar{x}$ או $\bar{x}x$

לאף $x \in X$. קל לראות כי כל מילה שקולה למילה מצומצמת.

למה: אם $w_1 \sim w_1'$
ב Σ^*
$w_2 \sim w_2'$

אזי $w_1 w_2 \sim w_1' w_2'$ (להוכיח לבד, זה לא קשה)

לכן, פעולת השרשור על Σ^* משרה פעולה שתקרא שרשור / כפול על $\Sigma^*/_\sim$

כאשר $\Sigma^*/_\sim =$ אוסף מחלקות השקילות ב-Σ^*.

נסמן ב- $[w]$ את מחלקת השקילות של המילה w.

משפט:

א) $\Sigma^*/_\sim$ עם פעולה זו היא חבורה.

ב) זוהי החבורה החופשית הנוצרת ע"י X; לשם הדיוק היה צריך לרשום $[X] = \{[x] \mid x \in X\}$

כדי לפשט סימונים נשמיט את [ ]

הערה: כדי להצדיק מהלך זה (השמטת הסוגריים) צריך גם להראות כי אם $a, b \in X$

!$a \neq b$ אזי $a \nsim b$!$[a] \neq [b]$.

הוכחה: א) בהינתן שני איברים ב $\Sigma^*/_\sim$ $[w], [w']$ הרי שהם מוגדר להיות $[ww']$

ונשים לב שזה מוגדר היטב (כי זה לא תלוי הנציגים)

אסוציאטיביות: ברורה, מאסוציאטיביות של שרשור מילים.

יחידה: מחלקת השקילות של המילה הריקה, נסמן אותה ב e

קיום הופכי: בהינתן $[w] \in \Sigma^*/_\sim$

נבחר $w \in [w]$ $w = a_1 a_2 \dots a_n$ $a_i \in \Sigma$

נגדיר $V = b_n b_{n-1} \dots b_1$ מאיזון הנאי: $1 \leq i \leq n$

$$b_i = \begin{cases} \bar{x} & a_i = x \\ x & a_i = \bar{x} \end{cases}$$

$$[w][v] = [wv] = [\text{מילה ריקה}] = e$$

$$wv = a_1 a_2 \dots a_n b_n b_{n-1} \dots b_1 \sim$$

אז $a_n b_n = \begin{cases} x\bar{x} \\ \bar{x}x \end{cases}$ ולכן ניתן לצמצם צמצום

$\sim a_1 a_2 \dots a_{n-1} b_{n-1} \dots b_1$ (ושוב ניתן לצמצם)

$\sim$
$\vdots$

מילה ריקה $\sim a_1 b_1 \sim$ (אם יש הכי).

נחדד את ההגדרה האחרונה שכתבנו (לפני השמטת הסוגריים):

בהינתן $w \in \Sigma^*$ נגדיר $P_w : X \longrightarrow \mathbb{Z}/2\mathbb{Z}$

$$P_w(x) = \left(\left(\text{מס' ההופעות של } x \text{ ב-} w \right) - \left(\text{מס' ההופעות } \bar{x} \text{ ב-} w \right) \right)_{\text{מודולו } 2}$$

לדוגמא: $X = \{a, b, c\}$ $\quad w = aab\bar{a}b\bar{b}cab\bar{a}cc$

$P_w(a) = 1$

$P_w(b) = (3) - 1 = 2 = 0 \bmod 2$

$P_w(c) = 1$

טענה: אם $w = w'$ אזי $P_w = P_{w'}$ כלומר לכל $x \in X$ $P_w(x) = P_{w'}(x)$

נשים לב כי עבור $x \in X$ $P_x(y) = \begin{cases} 1 & y = x \\ 0 & y \neq x \end{cases}$ $y \in X$

מסקנה: עבור $a, b \in X$ $a \neq b \Longrightarrow P_a \neq P_b$ כי לדוגמא

$$P_a(a) = 1 \neq 0 = P_b(a)$$

ולכן אם הטענה נכונה נובע כי a ו b אינם שקולים.

הוכחת הטענה: די לבדוק כי $P_{w_1} = P_{w_2}$ כאשר w_1 ו w_2 שקולות אלמנטרית.

עבור שקילות אלמנטרית ברור, כי מתווספים (או נעלמים) x אחד ו $\bar{x}$ אחד

13-11-2006

③ (ב) כדי להראות כי $G=\Sigma^*/_\sim$ היא החבורה החופשית הנוצרת על ידי X. צריך להראות קיום דרישות 1 ו- 2 מההגדרה.

לפי ההסכמה שלנו לזהות בין אברי X ומחלקות השקילות שלהם $X\subset G$.

עתה, תהי H חבורה כלשהי ! $f: X \longrightarrow H$ פונקציה שרירותית.

נגדיר פונקציה $\psi: \Sigma^* \longrightarrow H$

$$\psi(\text{מילה ריקה}) = \text{יחידה ב-}H$$

$$\psi(a_1a_2\dots a_n) = h_1h_2\dots h_n$$

כאשר:

$$h_i = \begin{cases} f(x) & a_i = x \\ f(x)^{-1} & a_i = \bar{x} \end{cases}$$

נשים לב כי: $\psi(vw) = \psi(v)\psi(w)$

וכן נבדוק כי אם $w\sim w'$ אזי $\psi(w)=\psi(w')$

הוכחה: די לבדוק עבור מילים שקולות אלמנטרית $w_1 = ux\bar{x}v$

$w_2 = uv$

$$\psi(w_1) = \psi(u)\psi(x)\psi(\bar{x})\psi(v) = \psi(u)f(x)f(x)^{-1}\psi(v) =$$

$$= \psi(u)\psi(v) = \psi(uv) = \psi(w_2)$$

לכן הפונקציה ψ משרה הומומורפיזם $\varphi: \underbrace{\Sigma^*/_\sim}_{G} \longrightarrow H$

נותר להראות כי φ כן יחיד.

לפי נובע מהטענה הבאה: אם G חבורה, $X\subset G$ קבוצה היוצרת את G.

H חבורה.

$\varphi_1: G\longrightarrow H$ $\quad \varphi_2: G\longrightarrow H$ הומומורפיזם

$$\varphi_1=\varphi_2 \Longleftarrow \varphi_1|_X = \varphi_2|_X$$

הוכחת הטענה: נתבונן ב- $g\in G$. היות ו- G נוצרת ע"י X. יש $a_1\dots a_n$

כך ש $a_i\in X$ $\quad \varepsilon_1\dots\varepsilon_n$ ב $\{\pm 1\}$

כך ש: $g=a_1^{\varepsilon_1}a_2^{\varepsilon_2}\cdots a_n^{\varepsilon_n}$

$$\varphi_1(g) = \varphi_1(a_1^{\varepsilon_1}a_2^{\varepsilon_2}\cdots a_n^{\varepsilon_n}) =$$

$$= \varphi_1(a_1)^{\varepsilon_1}\varphi_1(a_2)^{\varepsilon_2}\cdots\varphi_1(a_n)^{\varepsilon_n} = \varphi_2(a_1)^{\varepsilon_1}\varphi_2(a_2)^{\varepsilon_2}\cdots\varphi_2(a_n)^{\varepsilon_n} =$$

$$= \varphi_2(a_1^{\varepsilon_1}\cdots a_n^{\varepsilon_n}) = \varphi_2(g)$$

הערה: מהטענה רואים ש X יוצרת את $\overset{F(X)}{G}$.

נוכיח כי X יוצרת את $F(X)$ ישירות מההגדרה:

תהי $G=F(X)$ מקיימת תכונות 1 ו-2 בהגדרה

תהי L תת-החבורה של G הנוצרת ע"י X.

$$X \subset L < G$$

נראה כי לכל חבורה H והעתקה $f: X \to H$ יש הומומורפיזם יחיד ρ

מ-L ל-H כך ש: $\rho|_X = f$.

קיים הומומורפיזם ρ כזה, כי לפי ההנחה עבור G קיים הומומורפיזם (יחיד)

$\varphi: G \to H$ כך ש- $\varphi|_X = f$. נגדיר ρ להיות הצמצום של φ ל-L $\rho = \varphi|_L$.

היות ו- X יוצרת את L נובע כי ההומומורפיזם ρ נקבע ביחידות ע"י f

לכן L מקיימת את התכונות האוניברסליות של חבורה חופשית ולכן L איזומורפית ל-G.

ניתן להראות שהן שוות (כלומר שהן אותה תת-חבורה)

נשים לב כי יש לנו הומומורפיזם יחיד $\varphi_1: L \to G$ כך ש: $\varphi_1|_X = id_X$

ישנו גם הומומורפיזם יחיד $\varphi_2: G \to L$ כך ש: $\varphi_2|_X = id_X$

כלומר קיבלנו $\psi = \varphi_1 \circ \varphi_2 : G \to G$ (הומומורפיזם כך שצמצומו ל X הוא id_X)

נשים לב כי (א) φ_1 הוא הכלה של L. כלומר השיכון של L ב G.

(ב) $\psi = id_G \Longleftarrow \psi$ על ולכן גם φ_1 על

ולכן $L=G$

$\blacksquare$

15-11-2006 ①

מבנים אלגבריים - שעור מס' 8

דיברנו בשיעור הקודם על החבורה החופשית, ואמרנו כי

חבורה חופשית היא:

X קבוצה

$\bar{X}=\{\bar{x} \mid x\in X\}$. הגדרנו את $\Sigma = X\cup\bar{X}$

ואז הגדרנו את: $\Sigma^* \stackrel{def}{=} \{$מילים מאורך סופי ≥ 0 מעל $\Sigma\}$

~ יחס שקילות.

הראינו כי: $\Sigma^*/\sim$ עם פעולת שרשור היא חבורה חופשית נוצרת ע"י X.

ω מילה מצומצמת אם אין מופיעה ב-ω תת מילה מהצורה $x\bar{x}$ או $\bar{x}x$ $x\in X$

עובדה: (שדורשת הוכחה אבל נשמיט אותה כרגע):

בכל מחלקת שקילות יש בדיוק מילה מצומצמת אחת.

ניתן לזהות את אברי $F(X)$ החבורה החופשית הנוצרת ע"י X עם מילים מצומצמות.

פעולת הכפל היא שרשור ומעבר למילה מצומצמת.

(במקום $\bar{X}$ נרשום X^{-1})

תזכורת: חבורה חופשית נוצרת ע"י X היא חבורה G כך ש:

(א) $X\subset G$

(ב) לכל חבורה H והעתקה $f: X\to H$ ניתן להרחיב את f להומומורפיזם מ-G ל-H, באופן יחיד.

חבורה חופשית אבלית

(*) **הגדרה:** תהי X קבוצה. החבורה החופשית האבלית הנוצרת ע"י X היא החבורה G כך ש:

(1) G חבורה אבלית

(2) לכל חבורה אבלית H והעתקה $f: X\to H$ יש הומומורפיזם יחיד $\varphi: G\to H$

כך ש: $\varphi|_X = f$

טענה 1:

תהי X קבוצה. אם G_1, G_2 חבורות המקיימות את התנאים (*)

אזי G_1, G_2 איזומורפיות.

הערה (כתרגיל): לעבור על ההוכחה של הטענה המקבילה עבור חבורות חופשיות ולהבין שניתן להתאימה למקרה הנוכחי.

קיום?

נתבונן באוסף הבא: $\mathbb{Z}^X = \{\omega : X \longrightarrow \mathbb{Z}\}$ — אוסף כל הפונקציות מ-X ל-$\mathbb{Z}$

נגדיר עליה מבנה של חבורה. — באופן כללי אם A,B קבוצות $A^B = \{\omega : B \longrightarrow A\}$

נסמן את הפעולה ב +. $\omega, \omega' \in \mathbb{Z}^X$

אזי: $\omega + \omega' = v \in \mathbb{Z}^X$

וזה עובד כך: $v(x) = \omega(x) + \omega'(x)$

הערה: אם X סופית למשל מגודל n אזי ניתן לזהות את $\mathbb{Z}^X$ עם אוסף כל ה-n-יות של שלמים $\mathbb{Z}^n$ $\quad \mathbb{Z}^X \sim \{(k,l,m) \mid k,l,m \in \mathbb{Z}\} \quad X = \{a,b,c\}$

תרגיל: $(\mathbb{Z}^X, +)$ חבורה.

איבר היחידה הוא הפונקציה הקבועה 0. $0(x) = 0$.

(**) הגדרה: $A(X)$ תת-חבורה של $\mathbb{Z}^X$ $\{\omega \in \mathbb{Z}^X \mid$ התומך של ω סופי$\}$

תומך של ω = $\{x \in X \mid \omega(x) \neq 0\}$

משפט: $A(X)$ היא החבורה האבלית החופשית הנוצרת ע"י X, כאשר אנו מזהים כל איבר x_0 ב-X עם הפונקציה $\delta_{x_0} : X \longrightarrow \mathbb{Z}$

$$\delta_{x_0}(x) = \begin{cases} 1 & x = x_0 \\ 0 & x \neq x_0 \end{cases}$$ (הפונקציה המציינת של x_0)

הוכחה:

① $\mathbb{Z}^X$ אבלית והיא מכילה את X לאור הזיהוי $x_0 \longleftrightarrow \delta_{x_0}$.

② תהי H חבורה אבלית כל שהיא ותהי $f : X \longrightarrow H$ פונקציה כלשהי.

צריך להראות קיום הומומורפיזם יחיד $\varphi : \mathbb{Z}^X \longrightarrow H$ כך ש: $\varphi_X = f$.

נניח כי קיים הומומורפיזם φ $\varphi : \mathbb{Z}^X \longrightarrow H$ כך ש: $\varphi|_X = f$.

אזי יהי $\omega \in \mathbb{Z}^X$ איבר כלשהו (ω היא בעצם פונקציה כלשהי מ-X ל-$\mathbb{Z}$)

נחשב את $\varphi(\omega)$. נשים לב כי מתקיים:

נעשתה כרגע הפסקה מהוכחה, כי המרצה שכח להגדיר את $A(X)$.
אנחנו מסבירים מה זה $A(X)$ (**) וממשיכים להוכיח מעמ' הבא:

15-11-2006

דוגמאות:

1. אם X סופית אז: $A(X) = \mathbb{Z}^X$

2. אם $X = \mathbb{N}$

$$\mathbb{Z}^{\mathbb{N}} = \{ (a_1, a_2, a_3, \dots, a_n, \dots) \mid \begin{matrix} a_n \in \mathbb{Z} \\ \forall n \in \mathbb{N} \end{matrix} \}$$

$$A(\mathbb{N}) = \{ (a_1, a_2, \dots, a_n, a_{n+1}, \dots) \mid \text{קיים } M \ \forall n > M \ a_n = 0 \}$$ (החל ממקום מסוים כל האיברים הם 0)

3. $X = \mathbb{Z}$

$$\mathbb{Z}^{\mathbb{Z}} = \{ (\dots a_{-3}, a_{-2}, a_{-1}, a_0, \dots) \}$$

$$A(\mathbb{Z}) = \{ (\dots a_{-1}, a_0, a_1 \dots) \mid \text{כמעט כל } a_i \text{ הם } 0 \}$$

פרט למס' סופי של אינדקסים.

הערה: צריך להראות כי $A(X)$ היא תת-חבורה.

$A(X) \neq \emptyset$ כי פונקצית האפס $\in A(X)$.

אם $v, w \in A(X)$

נסמן $supp(v) = \{ x \in X \mid v(x) \neq 0 \}$ ($support$ = התומך)

$$supp(w) = \{ x \in X \mid w(x) \neq 0 \}$$

$$supp(v+w) \quad supp(v) + supp(w)$$

איחוד של קבוצות סופיות הוא סופי ולכן נובע כי אם $v + w \in A(X)$

כמו כן $supp(-v) = supp(v) \Longrightarrow -v \in A(X) \Longrightarrow A(X)$ תת חבורה.

$\boxed{//}$

המשך ההוכחה שהופסקה קודם:

נוכיח כעת את המשפט: $A(X)$ היא החבורה החופשית האבלית הנוצרת ע"י X.

תהי $f: X \longrightarrow H$ פונקציה כלשהי. H חבורה אבלית.

נוכיח כי קיים הומומורפיזם $\varphi: A(X) \longrightarrow H$ רק ש $\varphi|_X = f$.

יהי $w \in A(X)$. נסמן ב $Y = Y(w) \underset{\text{"}}{} supp(w)$ את התומך של w

נשים לב כי:

$$A(X) \ni w = \sum_{x \in supp(w)} w(x) \cdot \delta_x$$

המשך ←

נשים לב כי לכל $x \in X$ $\quad A(X) \ni \delta_x$

כאשר $w(x)\cdot\delta_x$ פירושו:

$$\varepsilon\,(\underbrace{\delta_x+\delta_x+\dots+\delta_x}_{|w(x)| \text{ פעמים}})$$

$$\varepsilon=\begin{cases}1 & w(x)\geq 0\\ -1 & w(x)<0\end{cases}$$

לכן φ מקיימת

$$\varphi(w)=\varphi\Big(\sum_{x\in Support(w)} w(x)\delta_x\Big)=$$

$$=\sum_{x\in Supp(x)} w(x)\varphi(\delta_x)=\sum_{x\in Y} w(x)f(x)\in\mathbb{Z}$$

$\Longleftarrow$ יחידות.

$\boxtimes$

נחזור על כל ההוכחה משום שהוא כי עשינו בלאגן גדול ☺

חבורה אבלית חופשית

X קבוצה, $\mathbb{Z}^X$ = אוסף כל הפונקציות מ-X ל-$\mathbb{Z}$

$A(X) \subset \mathbb{Z}^X$ = אוסף כל הפונקציות מ-X ל-$\mathbb{Z}$ עם תומך סופי

אם $\varphi : X \to \mathbb{Z}$

$\mathrm{supp}(\varphi) = \{x \in X \mid \varphi(x) \neq 0\}$

הפעולה ב-$A(X)$ מסומנת ע"י $+$.

משפט:

$A(X)$ היא החבורה החופשית האבלית הנוצרת ע"י X כאשר אנו מזהים כל איבר $x_0 \in X$ עם הפונקציה $A(X) \ni \delta_{x_0} : X \to \mathbb{Z}$

$$\delta_{x_0}(y) = \begin{cases} 1 & y = x_0 \\ 0 & y \neq x_0 \end{cases}$$

הוכחה: צריך להראות כי עבור כל חבורה אבלית H וכל פונקציה $f : X \to H$, קיים הומומורפיזם יחיד $\varphi : A(X) \to H$ כך ש: $\varphi|_X = f$

הוכחת יחידות: נניח כי יש φ כזו וננסה לחשב את $\varphi(w)$ עבור $w \in A(X)$.

נזכור כי w היא פונקציה מ-X ל-$\mathbb{Z}$ עם תומך סופי.

$$\boxed{w = \sum_{x \in \mathrm{supp}(w)} w(x)\delta_x} \quad (*)$$

כאשר בחבורה אבלית $(A, +)$ עבור $g \in A$ $n \in \mathbb{Z}$

$n > 0$ $\quad n \cdot g = \underbrace{g + g + \dots + g}_{n \text{ פעמים}}$

$n < 0$ $\quad n \cdot g = -\underbrace{(g + g \dots + g)}_{|n| \text{ פעמים}}$

$$\underset{\in A(X)}{(w(x) \cdot \delta_x)}(y) = \begin{cases} w(x) & y = x \\ 0 & y \neq x \end{cases}$$

ולכן ע"פ $(*)$ נקבל כי: $\varphi(w) = \varphi\left(\sum_{x \in \mathrm{supp}(w)} w(x)\delta_x\right) = \sum_{x \in \mathrm{supp}(w)} w(x)\varphi(\delta_x) = \quad (**)$

$$= \sum_{x \in \mathrm{supp}(w)} w(x) \cdot f(x) \implies \varphi \text{ יחידות}$$

כדי להראות קיום נשתמש ב-(**) בהגדרה.

נגדיר $\varphi(\omega)=\sum\limits_{x\in Supp\,\omega}\omega(x)f(x)$

וקיבלנו פונקציה $\varphi: A(X)\to H$

נשים לב כי $\varphi(\delta_{x_0})=\sum\limits_{x\in Supp(\delta_{x_0})}\delta_{x_0}(x)f(x)=$

$=\delta_{x_0}(x_0)f(x_0)=1\cdot f(x_0)$ (זהו הסבר מדוע החלפנו את $\varphi(\delta_x)$ ב- $f(x)$)

נראה כי φ הומומורפיזם.

יהיו $v,w\in A(X)$ נתבונן ב: $\varphi(v+w)$

סימון: $[w]=Supp(w)$

$$\varphi(v+w)=\sum_{x\in Supp(v+w)}(v+w)(x)f(x)=\sum_{x\in Supp(v)\cup Supp(w))}(v+w)(x)f(x)=$$

$$=\sum_{x\in[w]\cup[v]}(v(x)+w(x))f(x)=\sum_{x\in[v]\cup[w]}(v(x)f(x)+\sum_{x\in[v]\cup[w]}w(x)f(x)=$$

$$=\sum_{x\in Supp(v)}v(x)f(x)+\sum_{x\in Supp(w)}w(x)f(x)=\varphi(v)+\varphi(w)$$

כלומר φ הומומורפיזם. ∎

$$\Big(\sum_{x\in Supp(w)}\omega(x)\delta_x\Big)(y)=\sum(\omega(x)\delta_x)(y)=\sum_{x\in Supp(w)}\omega(x)\delta_x(y_0)=\begin{cases}0 & y_0\notin Supp(w)\\ \omega(y_0) & y_0\in Supp(w)\end{cases}$$

נקשר כעת פרשין לחבורות חופשיות.

יוצרים ויחסים

תהי X קבוצה ותהי $B\subset F(X)$:

כאשר $F(X)$ החבורה החופשית הנוצרת ע"י X

תהי N תת-החבורה הנורמלית של $F(X)$ הנוצרת ע"י B

כלומר תת-החבורה הנורמלית הקטנה ביותר ב-$F(X)$ אשר מכילה את B.

הסבר: אם G חבורה ו- $B\subset G$ תת-קבוצה

$\langle B^G\rangle$ היא תת-החבורה הנורמלית הנוצרת ע"י B = תת החבורה נורמלית

ב-G המינימלית המכילה את B.

20-11-2006 $\cap L \triangleleft G$ צו תת-החבורה ②

$R \subset L \triangleleft G$

נשים לב כי חיתוך תתי חבורות נורמליות הוא תת חבורה נורמלית.

כמו כן, גם נשים לב כי צו תת-חבורה הנוצרת על ידי כל האיברים ב-G הצמודים לאיברים ב-R.

$$\{grg^{-1} \mid g \in G,\ r \in R\} = R^G$$

r^g

__תרגיל:__ הוכח כי תת-החבורה הנוצרת על-ידי R^G נורמלית.

__הגדרה:__ תהי X קבוצה. $R \subset F(X)$ קבוצה. אז נסמן ב- $\langle X \mid R \rangle = F(X)/N$

כאשר N "$\langle R^{F(X)} \rangle$" תת-החבורה הנורמלית של $F(X)$ הנוצרת ע"י R.

X קבוצת יוצרים.

R קבוצת יחסים.

לביטוי $\langle X \mid R \rangle$ קוראים הצגה של חבורה (Group presentation)

נראה כמה דוגמאות:

__דוגמאות:__

(א) X כלשהי, $R = \emptyset$

$$\langle X \mid \emptyset \rangle = \langle X \rangle = F(X)$$

(ב) $X = \{a\}$

$R = \{a^5\}$

$\langle a \mid a^5 \rangle = \langle a \rangle /$ תת-החבורה הנורמלית הנוצרת ע"י a^5

$= \mathbb{Z}/5\mathbb{Z}$ (חבורה ציקלית מסדר 5)

(c) $X = \{a, b\}$

$R = aba^{-1}b^{-1}$

$$G = \langle ab \mid aba^{-1}b^{-1} \rangle = \mathbb{Z}^2$$

למה זה?

כי: $F(a,b)/$ תת-החבורה הנורמלית הנוצרת ע"י $aba^{-1}b^{-1}$

המשך

נסמן ב- a, b את תמונות a, b ב-G

$aba^{-1}b^{-1} = e$

אז: $ab = ba$

התמונה של איבר כמו $aabab^{-1}b^{-1}aba^{-1}b \in F(X)$

תמונתו ב-G היא: $aabab^{-1}b^{-1}aba^{-1}b$

אולם ב-G האיברים מתחלפים ולכן אפשר לסדר מחדש

$aaaaa^{-1}bb^{-1}b^{-1}bb = a^3b$

המשך ←

המשך דוגמא ③: טענה:

$G=\langle a,b \mid aba^{-1}b^{-1}\rangle = \{a^n b^m \mid n,m\in\mathbb{Z}\}$

עם כך קומוטטיבי: $(a^nb^m)(a^kb^l)=a^{n+k}b^{m+l}$

ננסה להבין מה זו החבורה הזו:

תת-החבורה הנורמלית של $F(X)$ הנוצרת $= N$

על ידי $aba^{-1}b^{-1}$

$$G = F(a,b)/N$$

איברי G הם מחלקות של N.

כלומר ביטויים מהצורה: $abaab^{-1}aba^{-1}N =$

$= abaab^{-1}aba^{-1}$

$a = aN$

$b = bN$

$ab = (aN)(bN) = abN$

$$aba^{-1}b^{-1} = (aN)(bN)(a^{-1}N)(b^{-1}N) = \underbrace{aba^{-1}b^{-1}}_{\in N} N = N = e$$

$ab=ba$

$aNbN = (ab)N = (ba)N = (ba)N = bNaN$

$abaab^{-1}aba^{-1}N = a^3bN$

מהשיוויון $aNbN=bNaN$ או $abN=baN$

נובע כי בכל מחלקה

$wN\in G=F(a,b)/N$ ניתן למצוא נציג מהצורה a^nb^m $n,m\in\mathbb{Z}$

לכן אוסף האיברים a^nb^mN ב-G הוא כל איברי G.

$$G=\{a^nb^mN \mid n,m\in\mathbb{Z}\}$$

נשים לב כי קיבלנו העתקה:

$$\varphi:\mathbb{Z}^2\longrightarrow G$$
$$(n,m)\longmapsto a^nb^mN$$

20-11-2006 ③

φ היא על.

φ היא הומומורפיזם:

$$\varphi((n,m)+(k,l)) = \varphi((n+k,\ m+l)) =$$

$$= a^{n+k}b^{m+l}N = (a^n b^m N)\cdot(a^k b^l N)$$

טענה: φ היא חח"ע.

הוכחה:

צריך להראות כי לכל $(k,l) \neq (m,n)$ ב $\mathbb{Z}^2$

$$a^k b^l N \neq a^n b^m N$$

זה יהיה $\Longleftrightarrow$ הגרעין טריוויאלי כלומר שאם $(n,m) \neq (0,0)$

אז $a^n b^m \neq N$

$a^n b^m \notin N$

N תת-החבורה הנורמלית הנוצרת ע"י $aba^{-1}b^{-1}$

$=$ תת-החבורה הנוצרת ע"י $\{gaba^{-1}b^{-1}g^{-1} \mid g \in F(a,b)\}$

היות וסך החזקות מעל a בכל אחד מהיוצרים הוא 0.

רק אם לכל איבר ב-N.

כנ"ל לגבי b ולכן נקבל כי אם $(n,m) \neq (0,0)$ $a^n b^m \notin N$

נראה עכשיו הוכחה אלטרנטיבית:

נתון מהומומורפיזם היחיד φ מ $F(a,b)$ ל-$\mathbb{Z}^2$ כך ש:

$$\varphi(a) = (1,0)$$

$$\varphi(b) = (0,1)$$

$$\varphi: F(a,b) \longrightarrow \mathbb{Z}^2$$

φ הוא הומומורפיזם $\boxed{\text{על}}$.

$$F(a,b)/K \cong \mathbb{Z}^2 \qquad K = Ker(\varphi)$$

$aba^{-1}b^{-1} \in K$ ולכן $N \subset K$

יהי $(m,n) \neq 0$ $a^m b^n \in F(X)$

מוסתק ל- $(m,n) \neq 0 \Longleftarrow a^m b^n \notin K \supset N$

נשים לב כי $\langle a,b \mid aba^{-1}b^{-1} \rangle \cong \mathbb{Z}^2 \cong A(a,b)$

(באופן כללי:) $\{\langle X \mid xyx^{-1}y^{-1} \rangle \ \forall x,y \in X\} \cong A(X)$

צורת סימון נוספת:

$\langle X \mid xy = yx \quad x,y \in X \rangle$

מהיותן תצוגה של חבורה $\langle X \mid R \rangle$

(אפילו עם X, R סופיות) בכלל קשה/בלתי אפשרי לענות על שאלות לגביה.

משפט קיילי

תהי G חבורה, אז ניתן לשכן את G בחבורת תמורות.

Y קבוצה. נסמן: $\{f: Y\to Y \mid f$ חח"ע ועל$\} = Per(Y)$

לכל חבורה G קיימת קב' Y והומומורפיזם חח"ע φ

$$\varphi: G \longrightarrow Per(Y)$$

הוכחה:

תהי $Y=G$. נגדיר העתקה $\varphi: G \longrightarrow Per(G)$

אז $\varphi(g)=\rho_g \in Per(G)$ עבור $\rho_g(x)=gx$ $\forall x\in G$

העובדה כי $\rho_g \in Per(G)$, כלומר חח"ע ועל, נובעת מכך כי G חבורה.

אם $\rho_g(x)=\rho_g(y)$ עבור x,y כלשהם $\Leftarrow gx=gy \Leftarrow x=y$

ע' כפל ב- g^{-1} משמאל ועל: לכל $y\in G$ $\rho_g(y^{-1}y)=g$

נבדוק כי φ הוא הומומורפיזם:

יהיו $g,h\in G$ אז:

$\varphi(gh)=\rho_{gh}$

$\varphi(g)\varphi(h)=\rho_g\rho_h$

עבור $x\in G$

$$\rho_{gh}(x)=ghx=\rho_g(hx)=\rho_g(\rho_h(x))=$$

$$=(\rho_g\cdot\rho_h)(x) \Longrightarrow \varphi(gh)=\varphi(g)\cdot\varphi(h)$$

כלומר זהו הומומורפיזם

נותר להראות כי $\varphi: G\longrightarrow Per(G)$ חח"ע:

נניח כי $g,h\in G$ ו- $\varphi(g)=\varphi(h)$ נתבונן ב

$$\varphi(g)(e)=\varphi(h)(e)$$

$$\varphi(g)(e)=\rho_g(e)=g\cdot e=g=h=h\cdot e=\rho_h(e)=\varphi(h)(e)$$

$\boxtimes$

G חבורה

$H<G$ תת-חבורה

$G/H = Y =$ אוסף כל המחלקות השמאליות של H

נגדיר העתקה, הומומורפיזם $\varphi: G \longrightarrow Per(Y)$

$$g \longmapsto \rho_g$$

$$\rho_g(xH) = gxH$$

קל לראות כי G הומומורפיזם:

$$\varphi(g_1g_2)(xH) = g_1g_2xH = \varphi(g_1)(g_2xH) =$$

$$= \varphi(g_1)(\varphi(g_2)(xH)) = (\varphi(g_1)\varphi(g_2))(xH)$$

(*) Ω קבוצה כלשהי לאו דווקא סופית

$Per(\Omega) =$ אוסף ההעתקות החח"ע ועל מ-Ω ל-Ω היא חבורה.

הפעולה: הרכבת פונקציות

$\varphi, \psi \in Per(\Omega)$

$$\varphi \circ \psi : \Omega \longrightarrow \Omega$$

אם $\varphi \circ \psi(x) = \varphi \circ \psi(y)$

$$\varphi(\psi(x)) = \varphi(\psi(y))$$

$$\Downarrow \text{ חח"ע } \varphi$$

$$\psi(x) = \psi(y)$$

$$\Downarrow \text{ חח"ע } \psi$$

$$x = y$$

היות ו-φ על ו-ψ על מהינתן $z \in \Omega$ קיים $y \in \Omega$ כך שמתקיים:

$\varphi(y) = z$ וקיים $x \in \Omega$ כך ש $\psi(x) = y$

$$(\varphi \circ \psi)(x) = \varphi(\psi(x)) = \varphi(y) = z$$

$\Leftarrow$ $\varphi \circ \psi$ חח"ע ועל.

העתקת הזהות שייכת ל-$Per(\Omega)$ והיא איבר היחידה.

ברור קיום הפכי.

משפט: תהי G חבורה , $H<G$ תת-חבורה

נתבונן בהומומורפיזם $\varphi: G \longrightarrow Per(G/H)$

$$\varphi(g)(xH)=gxH$$

אזי $Ker(\varphi)$ = תת החבורה הנורמלית הגדולה ביותר ב-G המוכלת ב-H.

כלומר, תת החבורה הנורמלית ב-G הגדולה ביותר המוכלת ב-H.

הוכחה: נניח $g\in Ker\varphi$. כלומר $\varphi(g)=id_{G/H}$

כלומר לכל $xH\in G/H$ קיים $gxH=\varphi(g)(xH)=xH$

וקיבלנו כי $g\in Ker\varphi \iff$ לכל $x\in G$ $gxH=xH$

$\iff x^{-1}gxH=H \quad \forall x\in G$

$\iff x^{-1}gx\in H \quad \forall x\in G$

$\iff g\in xHx^{-1} \quad \forall x\in G$

$\iff g\in \bigcap xHx^{-1}=N \quad (Ker\varphi=\bigcap_{x\in G}xHx^{-1} \Leftarrow)$

נשים לב כי $N=\bigcap_{x\in G}xHx^{-1}$ נורמלית כי:

נימוק 1: פירינו את N כגרעין של הומומורפיזם

נימוק 2: יהי $g\in G$. נתבונן ב gNg^{-1}:

$$gNg^{-1}=\cap g\Big(\bigcap_{x\in G}xHx^{-1}\Big)g^{-1}=\bigcap_{x\in G}gxHx^{-1}g^{-1}=$$

$$=\bigcap_{x\in G}gxH(gx)^{-1}=\bigcap_{y\in G}yHy^{-1}=N$$

$\Leftarrow$ N נורמלית.

נשים לב כי $N=\bigcap_{x\in G}xHx^{-1}$ נורמלי ב-G ו- $N\subset H$ כלומר $Ker\varphi$ היא אכן תת-חבורה נורמלית ב-G המוכלת ב-H.

צריך להראות כי אם $M\lhd G$ ו- $M\subset H$ אזי $M\subset N$.

$M\subset H \Leftarrow$ לכל $x\in G$ $M=xMx^{-1}\subset xHx^{-1}$ כי M נורמלית ב-G

ולכן $M\subset\bigcap_{x\in G}xHx^{-1}=N$ ולכן $M\subset N$

$\boxtimes$

שימוש במשפט:

טענה: תהי G חבורה סופית מסדר n.

יהי p ראשוני המחלק את n ונניח כי יש ב-G תת-חבורה H
מאינדקס $p > k > 1$

אזי G אינה חבורה פשוטה, כלומר יש ב-G תת-חבורה נורמלית N
כך ש: $\{e\} \neq N \neq G$

הוכחה: נתבונן בהומומורפיזם שהגדרנו $\varphi: G \longrightarrow$

אזי: $\ker\varphi = \bigcap_{x \in G} xHx^{-1} = N \subsetneq G$

$$\varphi: G \longrightarrow Per(G/H) \cong S_k$$

(חבורת התמורות על
k איברים)

תרגיל: ב-S_k אין איבר מסדר p עבור p ראשוני

$p > k$ כי $p \nmid k$ ולכן היות וב-G יש איבר מסדר p נסמנו g_0
(משפט קושי) נקבל כי $\varphi(g_0) = e \Leftarrow e \neq g_0 \in \ker\varphi \neq \{e\}$

▨

הגדרה: פעולה של חבורה G על קבוצה X היא הומומורפיזם מ- G ל- $Per(X)$

$$G \longmapsto Per(X)$$
$$g \longmapsto \rho_g$$

(*) ניתן לראות זאת גם כהעתקה $\varphi: G \times X \longrightarrow X$

כך שמתקיים: $\varphi(gh,x)=\varphi(g,\varphi(h,x))$ (2) ו- $\varphi(g,x)=\rho_g(x)$

מה-נתון הומומורפיזם $G \longrightarrow Per(X)$

$$g \longmapsto \rho_g$$

נגדיר ל- $g \in G$, $x \in X$ $\varphi(g,x)=\rho_g(x)$

מכיוון ש- $G \longrightarrow Per(X)$, $g \longmapsto \rho_g$ היא הומומורפיזם נקבל:

$$\varphi(gh,x)=\rho_{gh}(x)=\rho_g(\rho_h(x))=$$
$$=\rho_g(\varphi(h,x))=\varphi(g,\varphi(h,x))$$

(1) $G \longrightarrow Per(X)$ כך ש- $\rho_{gh}=\rho_g\rho_h$

$(1) \Rightarrow (2)$ $(2) \Rightarrow (1)$

מה-נתון פונקציה $\varphi: G \times X \longrightarrow X$ כך שמתקיים:

$$\forall g,h \in G,\ \forall x \in X: \varphi(gh,x)=\varphi(g,\varphi(h,x)),\ \varphi(e,x)=x$$

נגדיר פונקציה מ- G ל- $Per(X)$ ע"י $\rho_g(x)=\varphi(g,x)$.

טענה: ההעתקה המתקבלת היא הומומורפיזם מ-G ל-$Per(X)$

(כלומר לכל איבר $g \in G$ מגדירים $\rho_g : X \to X$

$$\rho_g(x) = \varphi(g,x)$$

(צריך להראות תחילה שכן תמורה ושזה הומומורפיזם)

הוכחה: ההגדרה $\rho_g(x) = \varphi(g,x)$ מגדירה עבור כל $g \in G$ העתקה ρ_g מ-X ל-X.

נחשב את ρ_{gh} עבור $g,h \in G$.

יהי $x \in X$:

$$\rho_{gh}(x) \overset{\text{הגדרת } \rho}{=} \varphi(gh,x) = \varphi(g, \varphi(h,x)) =$$

$$= \varphi(g, \rho_h(x)) = \rho_g(\rho_h(x)) = (\rho_g \rho_h)(x)$$

$\Leftarrow$ $\rho_{gh} = \rho_g \rho_h$ ולכן זהו הומומורפיזם.

נותר להראות כי זהו אכן תמורה:

נותר להראות כי לכל $g \in G$ $\rho_g \in Per(X)$, או במילים אחרות, כי

$\rho_g : X \to X$ חח"ע ועל.

מהחישוב לעיל לכל $g \in G$

$$id_X = \rho_e = \rho_{gg^{-1}} = \rho_g \rho_{g^{-1}}$$

$$id_X = \rho_e = \rho_{g^{-1}g} = \rho_{g^{-1}} \rho_g$$

התנאי $\rho(e,x) = x$ פירושו $\rho_e = id_X$

$$\begin{cases} \rho_g \rho_{g^{-1}} = \rho_{gg^{-1}} = \rho_e = id_X \\ \rho_{g^{-1}} \rho_g = \dots\dots = id_X \end{cases}$$

$\Longrightarrow$ $\rho_g \in Per(X)$

כלומר זוהי אכן תמורה.

א) תהי G חבורה כלשהי

X קבוצה כלשהי

נגדיר $\forall g\in G$ $\quad \varphi(g,x)=x$

$\forall x\in X$

זה שקול להומומורפיזם מ-G ל- $Per\,X$ אשר מעתיק כל איבר לזהות.

ב) תהי G חבורה ותהי $X=G$

נגדיר $\varphi: G\times G\longrightarrow G$

$\varphi(g,h)=gh$

זוהי ההעתקה המתאימה להומומורפיזם שהגדרנו בהוכחת משפט קיילי.

ג) תהי $G=SL_2(\mathbb{R})=$

$=\{A \mid A$ מטריצה 2×2 מעל $\mathbb{R}$ עם דטרמיננטה $1\}$ $\quad A=\begin{pmatrix}a&b\\c&d\end{pmatrix}$

$X=\mathbb{R}^2$ (אוסף כל הוקטורים)

$\varphi(A,v)=Av$

$A\in SL_2(\mathbb{R})$

$v\in\mathbb{R}^2$

נשים לב כי לכל $v\in\mathbb{R}^2$

$\begin{pmatrix}1&0\\0&1\end{pmatrix}v=v$

כלומר $\varphi(I,v)=v$

וגם $\varphi(AB,v)=AB\cdot v=$

$=A(Bv)=\varphi(A,\varphi(B,v))$

(כלומר זוהי פעולה)

באופן כללי אם: $G=GL_n(F)$ = חבורת המטריצות ההפיכות מסדר $n\times n$

מעל שדה F ! $X=F^n$ אז: $\varphi(A,v)=A\cdot v$ היא פעולה של G על F^n.

הערה: תהי G חבורה.

כאשר X הוא מרחב וקטורי, מתעניינים בהומומורפיזמים

$G \longrightarrow$ טרנספורמציות לינאריות הפיכות של X $= GL_F(X)$

הגדרה: תהי $\varphi: G\times X \longrightarrow X$ פעולה של חבורה G על X.

נוח בהרבה מקרים לרשום עבור $g\in G$ $x\in X$ $gx=\varphi(g,x)$

הגדרה: תהי G חבורה פועלת על קבוצה X כאשר מסמנים $gx=\varphi(g,x)=\rho_g x$

מה נתון $x\in X$ המסלול של x תחת G מסומן:

$$O(x)=\{gx \mid g\in G\}$$

המייצב של X: $stab_G(x)=\{g\in G \mid gx=x\}$

דוגמא:

$X=\{1,2,3,\dots,n\}$

$G=S_n$

נשים לב כי לכל $x\in X$

$O(x)=X$

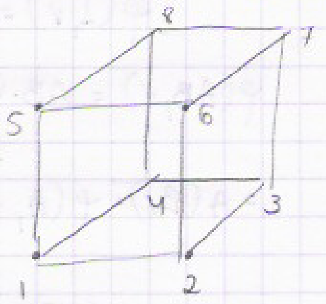
(G פועלת טרנזיטיבית)

$$stab=\{\pi\in S_n \mid \pi(n)=n\} \cong S_{n-1}$$

(זה איזומורפי)

דוגמא נוספת:

נתבונן בקוביה:



X = קדקדי הקוביה

G = איזומטריות מהקוביה לעצמה

הפעולה טרנזיטיבית כלומר $O(x)=X$ לכל $x\in X$

$$Stab(7) = Stab(1) = \{id, \underset{\substack{\| \\ \text{סיבוב ב-}120^\circ \text{ (התמונה אשר קודמת) סביב } [1,7] \\ \text{את } 1,2,7,8 \text{ ומחליף בין 4 ל-5 ובין 3 ל-6)}}}{\overset{\substack{\alpha \\ \| \\ \text{שיקוף במישור}}}{1,2,7,8}}, \underset{\|}{\sigma}, \alpha\cdot\alpha, \alpha^2, \alpha^2\alpha\}$$

כאשר $\alpha=(1)(2,5,4)(3,6,8)(7)$

G פועלת על X.

מסלולים:

לכל $x\in X$ $\quad O(x)=\{gx \mid g\in G\}\subset X$

מייצבים:

$$Stab_G(x)=\{g\in G \mid gx=x\}$$

טענה:

נניח כי G פועלת על X ו- $x,y\in X$ אזי מתקיים:

או $O(x)=O(y)$ או $O(x)\cap O(y)=\emptyset$

הוכחה: נשים לב כי אם $z\in O(x)$ אזי $O(z)=O(x)$

אם $z\in O(x)$ אזי קיים $g_0\in G$ כך ש: $z=g_0x$

לכן: (כי זו פעולה):

$$O(z)=\{g\cdot z \mid g\in G\}=\{gg_0x \mid g\in G\}=$$

$$=\{(gg_0)x \mid g\in G\}\subset O(x)$$

הראינו כי אם $z\in O(x)$ אזי $O(z)\subset O(x)$

אבל היות ואם $z\in O(x)$ $\quad \boxed{z=g_0x \Longleftarrow x=(g_0^{-1})z}$ (*) כי G פועלת על X

$\Longleftarrow x\in O(z) \Longleftarrow O(x)=O(z)$

לכן אם $x,y\in X$ $\quad O(x)\cap O(y)\neq\emptyset$ נובע כי קיים $z\in O(x)\cap O(y)$

ולכן $O(z)=O(x)$, $O(z)=O(y)$ $\Longleftarrow O(x)=O(y)$ ∎

הסבר מפורט את (*): נתון $z=g_0x$, נפעיל את g_0^{-1} על z

$$(g_0^{-1})(z)=(g_0^{-1})(g_0x)=(g_0^{-1}g_0)(x)=ex=x$$

משפט: תהי G חבורה הפועלת על הקבוצה X.
יהי $x_0 \in X$. נגדיר $H_0 = Stab_G(x_0)$
אזי יש התאמה חח"ע ועל בין איברי המסלול $O(x_0)$ של x_0 תחת G
ובין המחלקות השמאליות של H_0.

הערה: קל לבדוק כי $Stab_G(x)$ היא תת-חבורה

הוכחה: אם $x \in X$ אזי $e \in Stab_G(x)$ (כי e מקבע את הכל)

אם $g, h \in Stab_G(x)$ אזי $(gh)(x) = g(hx) = g(x) = x$

$\Leftarrow$ $Stab_G x \ni gh$

וכן מכך ש $gx = x$ נובע ש: $g^{-1}x = x \Rightarrow g^{-1} \in Stab_G x$

הוכחה: (של המשפט): נגדיר העתקה Ψ מ- G/H_0 ל- $O(x_0)$

$$\Psi(gH_0) = gx_0$$

צריך לבדוק שזה אכן מוגדר היטב; כלומר שאם $gH_0 = \tilde{g}H_0$

אזי $gx_0 = \tilde{g}x_0$ ואכן אם $gH = \tilde{g}H_0$

אזי קיים $h \in H_0$ $g = \tilde{g}h$

$\Leftarrow$ $gx_0 = (\tilde{g}h)x_0 = \tilde{g}(hx_0) = \tilde{g}x_0$

ברור כי ההעתקה $\Psi: G/H_0 \longrightarrow O(x_0)$

היא על כי אם $z \in O(x_0)$ קיים $g \in G$ כך ש: $z = g \cdot x_0$

ולכן $z = gx_0 = \Psi(gH_0)$

ההעתקה היא חח"ע כי:

נניח כי $\Psi(gH_0) = \Psi(\tilde{g}H_0)$

אזי פרוש הדבר כי $gx_0 = \tilde{g}x_0 \Rightarrow (g^{-1}\tilde{g})x_0 = x_0$

$$\Rightarrow g^{-1}\tilde{g} \in Stab_G(x_0) = H_0 \Rightarrow \tilde{g}H_0 = gH_0$$

(בעצם $gH_0 = \tilde{g}H_0 \xleftrightarrow{\text{שקול}} g^{-1}\tilde{g} \in H_0$)

27-11-2006

מסקנה:

אם G חבורה סופית ! G פועלת על X אזי מסלולי G הם קבוצות סופיות וגדליהן מחלקים את $|G|$.

הוכחה:

אם $x_0 \in X$ $\quad H_0 = Stab_G(x_0)$ אזי:

$$|O(x_0)| = |G/H_0| = [G:H_0] = \frac{|G|}{|H_0|}$$

∎

תהי G חבורה ותהיינה A,B תתי-חבורות סופיות של G.

קבוצה $\quad AB = \{ab \mid a\in A\ ,\ b\in B\}$

משפט: G חבורה

$A,B<G$ תתי-חבורות סופיות.

$$|AB| = \frac{|A||B|}{|A\cap B|}$$

הוכחה:

נתבונן בהעתקה $\quad \mu: A\times B \longrightarrow AB$

$$(a,b) \longmapsto a\cdot b$$

μ היא על

ננסה להבין מתי $\quad \mu(a_1,b_1) = \mu(a_2,b_2)$

$$a_1b_1 = a_2b_2$$

$$a_1h = a_2 \Leftarrow h = a_1^{-1}a_2 = b_1b_2^{-1} \Leftarrow\!\Rightarrow$$

$$\Rightarrow hb_2 = b_1\ ,\ b_2 = h^{-1}b_1$$

$$\begin{cases} a_1^{-1}a_2 \in H \\ b_1b_2^{-1} \in H \end{cases} \Longleftarrow h \in A\cap B = H$$

$$a_1H = a_2H \Longleftrightarrow a_1^{-1}a_2 \in H$$

$$Hb_1 = Hb_2 \Longleftrightarrow b_1b_2^{-1} \in H$$

בהינתן $(a,b) \in A\times B$

$$\{(a_2,b_2) \mid a_2b_2 = a_1b_1\} = \{(a_1h, h^{-1}b_1) \mid h\in H\}$$

נראה כי אם $a_2b_2 = a_1b_1$ אז קיים $h \in H$ כך ש: $a_2 = a_1h$

$b_2 = h^{-1}a_1$

ולהיפך אם $a_2 = a_1h$

$b_2 = h^{-1}b_1$

כאשר $h \in H = A\cap B$ אז:

$$a_2b_2 = (a_1h)(h_1^{-1}b_1) = a_1b_1$$

$a_1h \in A$

$h^{-1}b_1 \in B$

לכן ההעתקה $\mu : A\times B \longrightarrow AB$

היא $|H| = |A\cap B|$ ל-1 ולכן

$$|AB| = \frac{|A||B|}{|A\cap B|}$$

∎

משפטי סילו Sylow (ההוכחה לקוחה מהספר של Herstein)

תהי G חבורה סופית מסדר n ויהי p ראשוני

① אם $p^r \mid |G|$ אז יש ל-G תת-חבורה מסדר p^r.

② נניח כי $p^\alpha \mid |G|$ ו- $p^{\alpha+1} \nmid |G|$ אזי כל שתי תתי חבורות מסדר p^α של G הן צמודות. תתי-חבורות אלו נקראות תתי חבורות p-סילו של G $(v_p(|G|)=\alpha)$

③ מספר תתי חבורות p-סילו של G קונגרואנטי ל-1 מודולו p.

סימון/הגדרה (לוטה ב)

יהי p ראשוני ! $0 \neq x \in \mathbb{Z}$

$0 \leq v_p(x) = \alpha$ רק אם: $p^\alpha \mid x$ אבל $p^{\alpha+1} \nmid x$

הכי גדול

למה: נניח $n = p^r \cdot m$ (*) $m, r, p, n \in \mathbb{N}$, p ראשוני

$s = v_p(m)$ כלומר $p^s \mid m$ אבל p^{s+1} לא מחלק את m.

אזי $v_p\left(\binom{n}{p^r}\right) = s$

החזקה הגבוהה של p שמחלקת את n מעל p^r

הוכחה:

$$\binom{n}{p^r} = \frac{n!}{p^r!\,(n-p^r)!} = \frac{n(p-1)\cdot\ldots\cdot(n-(p^r-1))}{1\cdot2\cdot3\cdot\ldots\cdot p^r}$$

$$\binom{n}{p^r} \overset{(*)}{\underset{n=p^r\cdot m}{=}} \binom{p^r\cdot m}{p^r} = \frac{\cancel{p^r}\cdot m\,(p^r m-1)(p^r m-2)\cdot\ldots\cdot(p^r m(p^r-1))}{\cancel{p^r}\,(p^r-1)(p^r-2)\cdot\ldots\cdot(p^r-(p^r-1))} =$$

$$= m\prod_{i=1}^{p^r-1}\frac{p^r m-i}{p^r-i}$$

נשים לב כי לכל $1 \leq i \leq p^{r-1}$ מתקיים:

$$v_p\left(\frac{p^r m-i}{p^r-i}\right) = 0$$

$$\Longleftarrow\quad v_p\left(\binom{n}{p^r}\right) = v_p\left(m\cdot\prod\frac{p^r m-i}{p^r-i}\right) =$$

$$= v_p(m) + \sum_{i=1}^{p^r-1} v_p\left(\frac{p^r m-i}{p^r-i}\right) = v_p(m)+0 = v_p(m) = \underline{s}$$

מהמשפט לחלק ② של המשפט:
$V_p(161)=\alpha$ - נרחיב את ההגדרה
$\forall a,b \in \mathbb{Q}^*$
V_p ל- $\mathbb{Q}\setminus\{0\}$

$V_p\left(\frac{k}{l}\right)=V_p(k)-V_p(l)\in\mathbb{Z}$

דרך הוכחה:

א) $V_p(a\cdot b)=V_p(a)+V_p(b)$

ב) $V_p\left(\frac{p^r m-i}{p^r-i}\right)=0$ עבור $1\leq i\leq p^r-1$

דוגמה:

הסבר:

$V_3(162)=4$

$V_3\left(\frac{21}{18}\right)=1-2=-1$

כי:

$V_3\left(\frac{21}{18}\right)=V_3(21)-V_3(18)=V_3(3\cdot 7)-V_3(2\cdot 3^2)=1-2=-1$

הוכחת א':

נשים לב כי $V_p\left(\frac{m}{n}\right)=r$ פירושו כי ניתן לרשום

$\frac{m}{n}=p^t\frac{u}{v}$ $u,v\in\mathbb{Z}\setminus\{0\}$

$V_p\left(\frac{m}{n}\right)=p^t\frac{u}{v}$ u,v פרימריים ל- p:

(כי $V_p\left(\frac{m}{n}\right)=V_p(m)-V_p(n)=\alpha-\beta=t$ $\quad m=p^\alpha u$, $n=p^\beta v$)

לכן נסמן $V_p(a)=t$ $V_p(b)=r$

ואז עבור u_1,v_1,u_2,v_2 זרים ל- p כשהם מתקיים:

$a=p^t\frac{u_1}{v_1}$ $b=p^r\frac{u_2}{v_2}$ $\Rightarrow ab=p^{t+r}\frac{u_1u_2}{v_1v_2}$

ומכיוון ש- u_1,u_2,v_1,v_2 זרים ל- p

$V_p(ab)=t+r=V_p(a)+V_p(b)$

סוף הוכחת א.

הוכחת ב':

$V_p\left(\frac{p^r m-i}{p^r-i}\right)=V_p(p^r m-i)-V_p(p^r-i)=\ldots$

p^r-i אינו 0 מודולו p^r כי $1\leq i\leq p^r-1$ ולכן

$V_p(p^r-i)=V_p(-i)=V_p(i)$

ובאותו האופן גם $V_p(p^r m-i)=V_p(i)$

ולכן $V_p(i)-V_p(i)=0$

סוף הוכחת הלמה $\boxtimes$

הוכחת משפט סילו 1:

תהי G חבורה מסדר n ונניח כי p ראשוני ! $p^r \| |G|$

נתבונן באוסף כל תתי-הקבוצות של G בנות p^r איברים

$$\mathcal{M} = \{ X \subset G \mid |X| = p^r \}$$

נשים לב כי
$$|\mathcal{M}| = \binom{|G|}{p^r} = \binom{n}{p^r}$$

היות ו- G פועלת על עצמה, G פועלת גם על אוסף כל תתי-הקבוצות שלה $A \subset G$

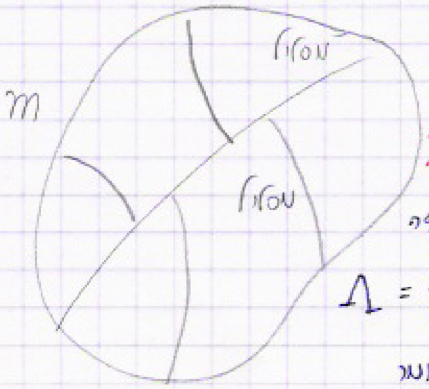
לכל $A \subset G$ נסמן $gA = \{ga \mid a \in A\}$ $(g \in G)$

נשים לב כי $|gA| = |A|$ ולכן G פועלת על $\mathcal{M}$

כלומר יש לנו הומומורפיזם

$$G \longrightarrow Per(\mathcal{M})$$
$$g \longmapsto f_g$$
$$f_g(A) = gA = \{ga \mid a \in A\}$$

לכן ניתן לפרק את $\mathcal{M}$ למסלולי G.



נמשיך את ההוכחה בעמוד הבא,

ונסביר כעת מדוע יש לנו פעולה על $\mathcal{M}$:

נניח כי G חבורה ו- G פועלת על קבוצה Ω

כשהי Ω נתבונן ב: $\Delta = \{ X \mid X \subset \Omega \}$

הפעולה על Ω משרה פעולה על Δ כלומר

מההומומורפיזם $G \longrightarrow Per(\Omega)$

כך ש: $g \longmapsto f_g$

נקבל הומומורפיזם $G \longrightarrow Per(\Delta)$

על ידי $g \longmapsto \tau_g$

$$\tau_{gh}(X) = \{ f_{gh}(x) \mid x \in X \} = \{ f_g f_h(x) \mid x \in X \} \in \Omega$$

(קל לבדוק כי T_g חח"ע ועל וכי היא הומומורפיזם)

נשים לב כי $|T_g(X)| = |X|$ ולכן משרה פעולה גם על $\{ X \subset \Omega : |X| = s \}$

עבור s נתון.

משפטי סילו

תהי G חבורה סופית מסדר n.

יהי p ראשוני המחלק את n.

1. אם $p^r \mid n$ אזי יש ל-G תת-חבורה מסדר p^r.

אם $p^\alpha \mid n$ ו- $p^{\alpha+1} \nmid n$: $\alpha = V_p(n)$ אז תת-חבורה מסדר p^α נקראת p-סילו.

2. כל שתי תתי-חבורות p-סילו של G הן צמודות.

3. מספר תתי-חבורות p-סילו של G הוא 1 מודולו p.

הערה: $2,1 \Longleftarrow n_p(G) \mid n$ (מס' חבורות p-סילו של G מחלק את $|G|$)

הוכחת הערה: מספר תתי-חבורות p-סילו ב-G מחלק את $|G|$

נתבונן ב- $\mathcal{L}$ - אוסף כל תתי-החבורות p-סילו של G

$$\mathcal{L} = \left\{ H<G \;\middle|\; \begin{matrix} H \text{ תת-חבורה} \\ |H| = p^\alpha \end{matrix} \right\}$$

$$\alpha = V_p(G)$$

1 אומר ש $\mathcal{L} \neq \emptyset$, G פועלת על $\mathcal{L}$ על ידי הצמדה

$$f_g : \mathcal{L} \longrightarrow \mathcal{L}$$
$$H \longmapsto gHg^{-1}$$

המשמעות של הטענה ב-2 כי כל שתי תת-חבורות p-סילו הן צמודות

היא כי פעולת G על $\mathcal{L}$ היא טרנזיטיבית

לכל $H_1, H_2 \in \mathcal{L}$ קיים $g \in G$ כך ש: $f_g(H_1) = gH_1g^{-1} = H_2$

נזכור כי בפעולה של G סופית על קבוצה Ω לכל $x \in \Omega$

$$\left| \text{מסלול } x \right| = [G : Stab_G\, x] = \frac{|G|}{|Stab_G\, x|}$$

עד כה הוכחת ההערה. ☒

נעבור עתה להוכחת המשפט:

(בעמוד הבא)

הוכחת חלק 1:

תהי G חבורה מסדר n. p^r מחלק של n $\quad n=p^r m$

צריך להראות כי קיימת תת-חבורה H מסדר p^r.

הגדרה:

$\mathcal{M}=\{X\subset G \mid |X|=p^r\}$ (אוסף של תת-קבוצות)

G פועלת על $\mathcal{M}$: כפולה: $\rho_g(X)=\{gx \mid x\in X\}$

ניתן לפרק את $\mathcal{M}$ למסלולים של G

זהו פירוק לאוסף של תת-קבוצות זרות ב-$\mathcal{M}$.

$$|\mathcal{M}|=\binom{n}{p^r}=\binom{p^r m}{p^r}$$

$U_p\left(\frac{k}{l}\right)=U_p(k)-U_p(l)$ = "חזקת p הגבוהה ביותר המחלקת את $\frac{k}{l}$"

הראינו, בשיעור הקודם, למה:

$$U_p(|\mathcal{M}|)=U_p\left|\binom{p^r m}{p^r}\right|=U_p(m)$$

$$\binom{p^r m}{} =$$

נסמן $s=U_p(m)$

$n=p^\alpha t \quad (t,p)=1$

$m=p^s t' \quad (t',p)=1$

$$p^\alpha t = n = p^r m \Longrightarrow s=\alpha-r$$

נתבונן בפירוק $\mathcal{M}$ למסלולי G.

היות ו- p^{s+1} אינו מחלק $\mathcal{M}$. יש מסלול של G ב- $\mathcal{M}$

אשר גודלו אינו מתחלק ב- p^{s+1}.

$n=p^r m \quad m=p^s\cdot t' \quad (t',p)=1$

תהי $X_0 \in \mathcal{M}$ תת קבוצה מגודל p^r כך שהמסלול שלה תחת G

גודלו אינו מתחלק ב- p^{s+1}

4-12-2006 המשך:

$$H = Stab\, x_0 = \{g \in G \mid g x_0 = x_0\}$$

נסמן $\mathcal{L}_0 = G x_0 =$ מסלול x_0 תחת G

$$= \{g x_0 \mid g \in G\}$$

$p^{s+1} \nmid |\mathcal{L}_0|$ הנחה מבחירת x_0

הסבר:

$$|\mathcal{L}_0| = \frac{|G|}{|H|} = \frac{p^\alpha t}{p^? *}$$

$$s \ge U_p(|\mathcal{L}_0|) = U_p\left(\frac{|G|}{|H|}\right) = U_p(|G|) - U_p(|H|) =$$

$$= \alpha - U_p(H) \Longrightarrow U_p(H) \ge \alpha - s = r \Longrightarrow$$

$$\Longrightarrow |H| \ge p^r$$

נותר להראות כי $|H| \le p^r$

נשים לב כי H הוא המייצב של x_0 $\quad H = \{g \in G \mid g x_0 = x_0\}$

זה אומר בפרט שלכל $h \in H$ $\quad h x_0 = x_0 \Longleftarrow$ נקבע $y_0 \in x_0$ אז:

לכן $h \in H$ $\quad h y_0 \in x_0 \Longleftarrow H y_0 = \{h y_0 \mid h \in H\} \subset x_0$

$$|\{h y_0 \mid h \in H\}| = |H|$$

$$\Longrightarrow |H| \le x_0 = p^r$$

$$\Downarrow$$

$|H| = p^r$ (הראינו אי-שוויונות משני הכיוונים)

ולכן H היא תת-חבורה של G מהסדר המבוקש.

הוכחת משפט סילו השני:

p ראשוני

תהי G חבורה סופית $\quad |G| = n = p^\alpha t$, $\quad t$ כך ש $p \nmid t$

$$\alpha = U_p(n)$$

1 $\Longleftarrow$ יש ל-G תת-חבורה מסדר p^α.

רוצים להראות כי כל שתי תת-חבורות מסדר p^α ב-G הן צמודות.

תהיינה $G > P, Q$ כך ש: $|P| = |Q| = p^\alpha$

רוצים להראות קיים $g\in G$ $Q=gPg^{-1}$ (קיים איבר אחד ב-G שמעתיק את P ל-Q ע"י הצמדה)

נתבונן במחלקות כפולות ב-G ביחס ל- P, Q:

אוסף כל תתי הקבוצות מהצורה $y\in G$ PyQ (איבר ב-G)

$$PyQ=\{ayb \mid a\in P,\ b\in Q\}$$

נשים לב כי כל שתי מחלקות כפולות הן או זרות או זהות.

כי: אם $z\in PyQ$ אז: $y\in PzQ$

כי אם $z\in PyQ$ אז קיימים $a\in P$, $b\in Q$ כך ש: $z=ayb$

$$\Downarrow$$

$$y\in a^{-1}zb^{-1}\in PzQ$$

$\Longleftarrow$ אם $z\in PyQ$ אז $PyQ=PzQ$ ומכאן כל שתי מחלקות כפולות הן או זהות או זרות.

אפשר להתבונן בחבורה $P\times Q$ מכפלה ישרה. (בנוי חבורה)

$$P\times Q=\{(a,b)\mid a\in P,\ b\in Q\}$$

$$(a,b)\cdot(a',b')=(aa',bb')$$

$H=P\times Q$ פועלת על G: נגדיר: $f_{(a,b)}(g)=agb^{-1}$

צריך לבדוק שזוהי פעולה.

מסלולי הפעולה הזו הן מחלקות כפולות של P ו-Q.

אם $Py_1Q\cap Py_2Q\neq\emptyset$

$\Longleftarrow$ יהי $z\in Py_1Q\cap Py_2Q$

$\Longleftarrow$ $y_1=a_1zb_1$

$$Py_1Q=Pa_1zb_1Q=PzQ$$

$$y_2=a_1zb_2 \quad //$$

$$Py_2Q=Pa_2zb_2Q=PzQ$$

קיבלנו חלוקה של G לקבוצות זרות מהצורה PyQ.

$$|P_yQ| = \frac{|P||Q|}{|P\cap_y Q_{y^{-1}}|}$$

נזכור כי $|P|=|Q|=p^{\alpha}$

אז: $|P_yQ| = \frac{p^{\alpha}\cdot p^{\alpha}}{|P\cap_y Q_{y^{-1}}|} = \frac{p^{2\alpha}}{|P\cap_y Q_{y^{-1}}|}$

אנו רוצים להראות קיים y_1 כך ש: $P=y_1Qy_1^{-1}$

טענה (שהוכחנו):

אם A,B תת-חבורות של G אז: $|A\cdot B| = \frac{|A||B|}{|A\cap B|}$

$\Longleftarrow$ עבור כל $g\in G$ $|AgBg^{-1}| = \frac{|A||gBg^{-1}|}{|A\cap gBg^{-1}|} = \frac{|A||B|}{|A\cap gBg^{-1}|}$

נחזור להמשך ההוכחה שלנו:

נשים לב כי אם $P\neq yQy^{-1}$ אז: $P\cap yQy^{-1} \subsetneq P$

זוהי תת-חבורה של P מסדר קטן מ-p^{α}

כלומר הסדר של $|P\cap_y Q_{y^{-1}}|=p^{\beta}$ כאשר $\beta<\alpha$

לכן, בכל מקרה בו $P\neq yQy^{-1}$

$$|P_yQ| = \frac{p^{2\alpha}}{|P\cap_y Q_{y^{-1}}|} = p^{2\alpha-\beta}$$

β תלוי ב-y אבל $\alpha >$

ולכן תמיד מתחלק ב- $p^{\alpha+1}$

לכן לא יתכן כי תמיד $P\neq yQy^{-1}$ כי אז היינו מקבלים פירוק של G לקבוצות זרות מגדלים המתחלקים ב-$p^{\alpha+1}$ ולכן גם $|G|$ מתחלק ב-$p^{\alpha+1}$ סתירה.

לכן נובע קיים $y_1\in G$ כך ש: $P=yQy^{-1}$

$\blacksquare$

הוכחת חלק 3 של משפט סילו

רוצים להראות כי מספר חבורות p-סילו ב-G הוא 1 מודולו p.

הוכחה: נסמן $\mathcal{L} = \{$ חבורות p-סילו של G $\}$

אז: G פועלת על $\mathcal{L}$ על-ידי הצמדה.

לפי 1: $\mathcal{L} \neq \emptyset$

לפי 2: הפעולה טרנזיטיבית

לכן $|\mathcal{L}| = \frac{|G|}{|stab_G(P)|}$

$P \in \mathcal{L}$ תת-חבורת p-סילו

המנרמל של P ב-G: $Stab_G(P) = \{g \in G \mid gPg^{-1} = P\} = N_G(P)$

נתבונן בחלוקה של G למחלקות כפולות ביחס ל- P:

$$PyP = \{ayb \mid a \in P,\ b \in P\}$$

$$|PyP| = \frac{|P||P|}{|P \cap yPy^{-1}|} = \frac{p^{2\alpha}}{|P \cap yPy^{-1}|}$$

אם $y \in Stab_G(P) = N_G(P)$ (מייצב תחת פעולת ההצמדה הוא מנרמל)

אז $P = yPy^{-1}$

$$P \cap yPy^{-1} = P$$

$$|PyP| = \frac{p^{2\alpha}}{p^{\alpha}} = p^{\alpha}$$

אם $y \notin N_G(P)$ אז: $|PyP| = \frac{p^{2\alpha}}{p^{\beta(y)}} = p^{2\alpha - \beta(y)}$

$\beta(y) < \alpha$ ומספר זה מתחלק ב- $p^{\alpha+1}$

נשים כי G היא האיחוד הבא:

$$G = \underset{y \in \Omega}{\bigcup} PyP = \underset{y \in N_G(P)}{\bigcup} PyP \uplus \underset{z \notin N_G(P)}{\bigcup} PzP$$

קבוצת נציגים

איחוד זר.

נזכור כי $P \subset N_G(P)$ ולכן $N_G(P) \cap \bigcup_{z \notin N_G(P)} PzP = \emptyset$ (החיתוך ריק)

ולכן $G \setminus N_G(P) = \bigcup_{z \notin N_G(P)} PzP$

אנו יודעים כי: $|G \setminus N_G(P)|$ מתחלק ב- $p^{\alpha+1}$

כי קבוצה זו היא איחוד של קבוצות מהצורה PzP $z \notin N_G(P)$

וכל אחת מהן גודלה מתחלק ב $p^{\alpha+1}$.

$$|\mathcal{L}| = \frac{|G|}{|N_G(P)|} = \frac{|N_G(P)| + |G \setminus N_G(P)|}{|N_G(P)|} = 1 + \frac{|G \setminus N_G(P)|}{|N_G(P)|}$$

כל הביטוי הזה מתחלק ב-p

כי המונה מתחלק ב- $p^{\alpha+1}$ והמכנה מחלק את $|G| = p^{\alpha} \cdot t$

ולכן קיבלנו כי $|\mathcal{L}|$ הוא 1 מודולו p.

6-12-2006 (1)

מבנים אלגבריים - שעור מס' 14

שימושים למשפטי סילו

תהי G חבורה מסדר $11^2\cdot 13$.

ממשפט סילו 1 $\Longleftarrow$ יש ל-G תת-חבורות מסדר 11^2 ו-13.

כמה תת-חבורות מסדר 11^2 יש ל-G?

$p=11$ מהו $a_{11}(G)$ (מס' חבורות 11-סילו של G)?

$$a_{11}(G)\equiv 1 \bmod 11$$

$$a_{11}(G) \mid 11^2\cdot 13$$

$\Longleftarrow$ $a_{11}(G) \mid 13$ $\Longleftarrow$ $a_{11}(G)=1$ (או 13 אבל $13\not\equiv 1 \bmod 11$).

נסמן ב-P את תת-החבורות מסדר 11^2 של G.

הערה:

נשים לב כי מכך ש-$a_{11}(G)=1$ נובע כי תת-חבורה 11-סילו של G היא נורמלית כי כל הצמדה שלה היא מאותו סדר.

$P<G$ $\quad 11^2=|P|=|gPg^{-1}|=11^2 \quad \forall g\in G$

$\Longleftarrow$ מיחידות תת-חבורה מסדר 11^2 נובע כי לכל $g\in G$ $gPg^{-1}=P$.

הוכחת ההערה: (ממשפט סילו)

$\alpha=\{A<G \mid |A|=p^\alpha\}$ אוסף כל תת-חבורות p-סילו של G.

G פועלת על α ע"י הצמדה והפעולה טרנזיטיבית (לפי 2)

$L\neq\emptyset$ לפי 1. כלומר L היא מסלול של G.

היה לנו משפט שאמר: בכל פעולה על חבורה סופית G

גודל מסלול שווה לגודל של G חלקי הגודל של המייצב

$$|\text{מסלול}| = \frac{|G|}{|\text{מייצב}|}$$

$$\Longleftarrow \quad |\text{מסלול}| \mid |G|$$

ראינו כי אם G פועלת על X $\quad H=Stab_G(x_0)=\{g\in G \mid gx_0=x_0\}$

אז יש התאמה חח"ע ועל בין G/H לבין Gx_0 - מסלול x_0 ☐

נחזור עתה לחבורה שלנו.

באופן דומה רואים כי ל- G שסדרה $11^2\cdot 13$

יש בדיוק תת-חבורה 13-סילו אחת. שנסמנה ב- Q.

$$a_{13}(G) \equiv 1 \bmod 13$$

$$a_{13}(G) \mid 11^2\cdot 13 \Rightarrow a_{13}(G) \mid 11^2$$

$\Leftarrow$ Q נורמלית ב- G.

G חבורה, $|G| = 11^2\cdot 13$

$P \lhd G$, מסדר 11^2

$Q \lhd G$, מסדר 13

$P\cap Q = \{e\}$ (כי הסדר של $P\cap Q$ צריך לחלק את 13 וגם את 11^2

אבל $(13, 11^2)=1$.

מתוך התרגילים הייתה טענה:

אם $A, B \lhd G$ תת-חבורות נורמליות ו- $A\cap B=\{e\}$ אז

הן מתחלפות (כלומר לכל $a\in A$, $b\in B$ $ab=ba$)

הוכחה: $a\in A$ $b\in B$

$$[a,b]= \text{(הקומוטטור)}$$

$$ab=ba \iff \underbrace{aba^{-1}}_{\in B \text{ כי } B \text{ נורמלית}}\ \underbrace{b^{-1}}_{\in B}=e$$

$$\left.\begin{array}{l}\Rightarrow [a,b]\in B \\ \Rightarrow [a,b]\in A\end{array}\right\} \Rightarrow \begin{array}{l}[a,b]\in A\cap B=\{e\} \\ [a,b]=e\end{array}$$

PQ תת-חבורה כי מכפלת שתי תתי-חבורות כאשר אחת מהן לפחות היא נורמלית היא תת-חבורה

$$|PQ| = \frac{|P|\cdot|Q|}{|P\cap Q|} = \frac{11^2\cdot 13}{1} = 11^2\cdot 13 = |G|$$

אז מצאנו תת-קבוצה של G מאותו הגודל של G

$\Leftarrow$ $PQ = G$

כלומר לכל איבר $g\in G$ קיימים $a\in P$ $b\in Q$

כך ש- $g=a\cdot b$

טענה: אם G חבורה, A,B תת-חבורות נורמליות של G

כך ש $A\cap B=\{e\}$ + $A\cdot B=G$ אז G איזומורפית ל- $A\times B$

$$G\cong A\times B$$

הוכחה: נגדיר העתקה $\mu: A\times B\longrightarrow G$

$$\mu(a,b)=ab$$

מההנחות נובע כי μ על והיא חח"ע כי אם

$\mu(a_1,b_1)=\mu(a_2,b_2)$, $a_1,a_2\in A,\ b_1,b_2\in B$

$$\Downarrow$$

$$a_1b_1=a_2b_2$$

$$\Downarrow$$

$$A\ni a_2^{-1}a_1=b_2b_1^{-1}\in B$$

$$\Downarrow$$

$$a_2^{-1}\cdot a_1=b_2b_1^{-1}\in A\cap B=\{e\}$$

$$\Downarrow$$

$$a_1=a_2\quad b_1=b_2$$

נראה כי μ הומומורפיזם:

$$\mu((a_1,b_1)(a_2,b_2))=\mu(a_1a_2,b_1b_2)=a_1a_2b_1b_2=$$

צ"ל: $a_1b_1a_2b_2=a_1a_2b_1b_2$

$$b_1a_2=a_2b_1$$

כלומר צריך להראות כי איברי A מתחלפים עם איברי B,

וזאת מהטענה שבתרגול שכן A,B נורמליות ו- $A\cap B=\{e\}$

$\blacksquare$

לכן $G\cong P\times Q$

Q היא מסדר ראשוני ולכן ציקלית $Q\cong\mathbb{Z}/13\mathbb{Z}$

P מסדר 11^2. אנו מכירים 2 כאלו $\mathbb{Z}/121\mathbb{Z}$

$\mathbb{Z}/11\mathbb{Z}\times\mathbb{Z}/11\mathbb{Z}$

משפט: חבורה מסדר p^2 היא אבלית והיא אחת מבין $\mathbb{Z}_p\times\mathbb{Z}_p$ או $\mathbb{Z}_{p^2}$

לכן חבורה G מסדר $11^2\cdot 13$ היא איזומורפית לאחת מבין $K=K_{13}\times K_{121}$

או $L=\mathbb{Z}_{13}\times(\mathbb{Z}_{11}\times\mathbb{Z}_{11})$

נשים לב כי: K,L אינן איזומורפיות.

אם K איזומורפית ל-L אזי לכל p חבורות p-סילו שלהן איזומורפיות. אבל עבור K הנתונה ו-$p=11$ חבורת 11-סילו שלה היא ציקלית מסדר 121 ואילו ל-L חבורת 11 סילו שלה אינה ציקלית.

טענה: יהיו m,n זרים.

אזי: $\mathbb{Z}_{mn}\cong\mathbb{Z}_m\times\mathbb{Z}_n$

הוכחה: נגדיר העתקה $\varphi:\mathbb{Z}_{mn}\to\mathbb{Z}_{m\cdot n}$

$$\varphi(k+mn\mathbb{Z})=(\alpha(k+mn\mathbb{Z}),\beta(k+mn\mathbb{Z}))$$

כאשר: $\alpha(k+mn\mathbb{Z})=k+m\cdot\mathbb{Z}$

$$\beta(k+mn\mathbb{Z})=k+n\cdot\mathbb{Z}$$

קל לבדוק כי φ הומו' חח"ע ועל $\Longleftarrow$ משפט השאריות הסיני.

משפט השאריות הסיני: בהינתן m,n זרים, לכל $a,b\in\mathbb{Z}$

יש $x\in\mathbb{Z}$ כך ש- $x\equiv a \bmod m$

$x\equiv b \bmod n$

x יחיד מודולו $m\cdot n$.

נמשיך בשיעור הבא.

11-12-2006

מבנים אלגבריים - שעור מס' 15

שעת קבלה של שחר עוזם:

יום ד' שעה 10-11

חדר 1 בבנין מתמטיקה.

התחלנו לראות בשעור קודם שימושים של משפטי סילו:

תהי G חבורה מסדר $11^2\cdot 13$

תהי P חבורה מסדר 11-סילו של G

תהי Q חבורה מסדר 13-סילו של G

ראינו כי P נורמלית ב-G

Q נורמלית ב-G

$P\cap Q=\{e\}$

$$\Longleftarrow \quad |PQ|=\frac{|P||Q|}{|P\cap Q|}=11^2\cdot 13=|G|$$

$$\Longleftarrow \quad PQ=G$$

$$\Longleftarrow \quad G=P\times Q$$

P היא חבורה ציקלית מסדר 13.

רק את חובות משעור קודם

טענה:

p ראשוני. חבורה מסדר p^2 היא אבלית.

הערנו במשפט הקודמת כי אם a,b זרים אז:

$$\mathbb{Z}/ab\mathbb{Z}\cong \mathbb{Z}/a\mathbb{Z}\times \mathbb{Z}/b\mathbb{Z}$$

הוכחה:

נגדיר העתקה:
$$\varphi: \mathbb{Z}/ab\mathbb{Z}\longrightarrow \mathbb{Z}/a\mathbb{Z}\times \mathbb{Z}/b\mathbb{Z}$$

$$\varphi(x)=(\varphi_1(x),\varphi_2(x))$$

כאשר:
$$\varphi_1: \mathbb{Z}/ab\mathbb{Z}\longrightarrow \mathbb{Z}/a\mathbb{Z}$$

$$\varphi_2: \mathbb{Z}/ab\mathbb{Z}\longrightarrow \mathbb{Z}/b\mathbb{Z}$$

$$x=n+ab\mathbb{Z}$$

$$\varphi_1(n+ab\mathbb{Z})=n+a\mathbb{Z}$$

$$\varphi_2(n+ab\mathbb{Z})=n+b\mathbb{Z}$$

ברור כי φ הומומורפיזם (כי φ_1 הומומורפיזם ו- φ_2 הומומורפיזם)

φ הוא חח"ע:

כי נניח $0\le m,n \le ab$

$$\varphi(n+ab\mathbb{Z})=\varphi(m+ab\mathbb{Z})$$

כלומר $\varphi_i(n+ab\mathbb{Z})=\varphi_i(m+ab\mathbb{Z})$ $i=1,2$

$\Longleftarrow$ a מחלק את $n-m$

b מחלק את $n-m$

$\Longleftarrow$ היות ו- a ו- b זרים ab מחלק את $n-m$

$\Longleftarrow$ $n=m$

$\Longleftarrow$ הראינו כי φ חח"ע $\Longleftarrow$ φ על משיקולי ספירה (משיקולי גודל)

משפט:

תהי G חבורה סופית מסדר חזקת ראשוני $|G|=p^r$

(p ראשוני, $r\in\mathbb{N}$)

אזי ל- G יש מרכז לא טריוויאלי:

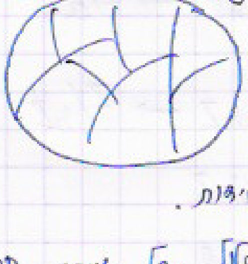
$$Z(G)=\{h\in G \mid hg=gh \quad \forall g\in G\} \underset{\text{לא טריוויאלי}}{\neq} \{e\}$$

הוכחה: לכל $h\in G$ נסמן ב- h^G או ב- $[h]$ את מחלקת הצמידות של h: $h^G=[h]=\{ghg^{-1}\mid g\in G\}$

נשים לב כי כל שתי מחלקות צמידות או זרות או שוות.

נשים לב כי $h\in Z(G)$ אם ורק אם $|[h]|=1$

G



נתבונן בפירוק של G למחלקות צמידות.

נשים לב כי מחלקת צמידות היא מסלול של איבר תחת פעולת G על G ע"י הצמדה.

לכן $|[h]|$ מחלק את $|G|$

11-12-2006 ②

היות ו $p^r=|G|$

נובע כי כל מחלקת צמידות, גודלה או 1 או כפולה (אפילו חזקה) של p

היות וסך כל גדלי מחלקות הצמידות הוא $p^r=|G|$ מתחלק ב-p

נובע כי $d=$ מספר מחלקות הצמידות ב-G שגודלן 1 חייב להתחלק ב-p

היות ו- $[e]=\{e\}$ גודלה 1, הרי ש: $d\geq 1$ ולכן $1\leq p\leq d$

ולכן יש מחלקות צמידות נוספות בגודל 1 ולכן $Z(G)\neq\{e\}$

▨

מסקנה:

אם G חבורה מסדר p^2 (p ראשוני) אזי G אבלית

הוכחה: נסמן $Z=Z(G)$

אם $Z=G$ סיימנו.

נניח בשלילה $Z\neq G$. אזי Z תת-חבורה לא טריויאלית של G מסדר $<|G|$

ולכן $|Z|=p$

נבחר $g_0\in G/Z$ ונתבונן בחבורה הציקלית הנוצרת ע"י g_0

מה הסדרים האפשריים:

$$\left.\begin{matrix}\cancel{1}\\ p\\ p^2\end{matrix}\right\} = |\langle g_0\rangle|$$

אם $|\langle g\rangle|=p^2$ אזי $G=\langle g_0\rangle$ ולכן G אבלית ובפרט $Z=G$

אבל הנחנו שזה לא מתקיים ולכן צריך להיות: $A=\langle g_0\rangle$ ציקלית מסדר p.

כמו כן: $A\cap Z=\{e\}$

כי אם $A\cap Z\neq\{e\}$ אזי $A=\langle x\rangle=Z$ וזו סתירה כי $Z\not\ni g_0\in A$

Z נורמלית לכן AZ תת-חבורה $|AZ|=\frac{|A||Z|}{|A\cap Z|}=p^2$

$\Leftarrow$ $AZ=G$

$\Leftarrow$ כל איבר ב-G הוא מהצורה $g_0^i z$

כאשר $0\leq i\leq p-1$, $z\in Z$

ולכן כל שני איברים ב-G מתחלפים
כלומר:

$$(g_0^{i_1}z_1)(g_0^{i_2}z_2)=$$
$$=g_0^{i_1}z_1g_0^{i_2}z_2=g_0^{i_1+i_2}z_1z_2=(g_0^{i_2}z_2)(g_0^{i_1}z_1)$$

ולכן $Z(G)=G$ בסתירה להנחה

$\blacksquare$

הערה: קיימות חבורות מסדר p^3 שאינן אבליות, למשל:

יהי p ראשוני

$$H=\left\{\begin{pmatrix}1&x&z\\0&1&y\\0&0&1\end{pmatrix}\;\middle|\;x,y,z\in\mathbb{F}_p\right\}$$ חבורת Heizenberg

$|H|=p^3$ (יש p אפשרויות לבחור x, p אפשרויות ל-y ו- p אפשרויות ל-z)

H חבורה ביחס לכפל מטריצות

$$\begin{pmatrix}1&x&z\\&1&y\\&&1\end{pmatrix}\begin{pmatrix}1&a&c\\&1&b\\&&1\end{pmatrix}=\begin{pmatrix}1&x+a&z+c+xb\\&1&y+b\\&&1\end{pmatrix}$$

H אינה אבלית:

$$\begin{pmatrix}1&1&0\\&1&0\\&&1\end{pmatrix}\begin{pmatrix}1&0&0\\&1&1\\&&1\end{pmatrix}=\begin{pmatrix}1&1&1\\&1&1\\&&1\end{pmatrix}$$

$$\neq$$

$$\begin{pmatrix}1&0&0\\&1&1\\&&1\end{pmatrix}\begin{pmatrix}1&1&0\\&1&0\\&&1\end{pmatrix}=\begin{pmatrix}1&1&0\\&1&1\\&&1\end{pmatrix}$$

עתה,

נתבונן בחבורה G מסדר $11^2\cdot 13$ אזי $G\cong P\times Q$

$|P|=11^2$

$|Q|=13$

חבורה אבלית מסדר 11^2 היא אחת משתי האפשרויות:

או $\mathbb{Z}/_{121}\mathbb{Z}$

או $\mathbb{Z}/_{11}\mathbb{Z}\times\mathbb{Z}/_{11}\mathbb{Z}$

הוכחה: תהי P חבורה מסדר 11^2 אזי היא אבלית. אם אינה ציקלית אזי

כל איבר $\neq e$ הוא מסדר 11 נבחר $e\neq a\in G$ $A=\langle a\rangle$

$|A|=11$

נבחר $b \in G \setminus A)$ אז $B = \langle b \rangle$

חבורה ציקלית מסדר 11 $A \cap B = \{e\}$

$AB = G$

והן מתחלפות ולכן $G \cong A \times B$

∎

משפט:

תהי G חבורה אבלית מסדר סופי n אזי יש חבורות ציקליות:

$$C_1, C_2, \dots, C_k$$

כאשר $|C_i| = n_i$

אזי: $G \cong C_1 \times C_2 \times \dots \times C_k$

$$n_1 \cdot n_2 \cdot \dots \cdot n_k = n$$

! $n_{i+1} \mid n_i$ לכל $1 \le i \le k-1$

$(n_1, \dots, n_k)$ נקבעים ע"י G ונקראים האינווריאנטות של G.

הוכחה:

טענת עזר:

נשים לב כי אם G אבלית מסדר n אזי היא מכפלה ישרה של חבורות סילו שלה.

הוכחה: (של טענת העזר)

יהיו $p_1, p_2, \dots, p_s$ הראשוניים השונים המחלקים את $n = |G|$

תהיינה $Q_1, \dots, Q_s$ תתי חבורות p_i-סילו של G כלומר $|Q_i| = p_i^{r_i}$

$Q_i < G$ כאשר $p^{r_i+1} \nmid |G|$.

נשים לב כי כל Q_i מוגדרת היטב -יחידה כי כל שתי תתי-חבורות p-סילו הן צמודות

ו-G אבלית ולכן פעולת ההצמדה היא הזהות.

לכל $1 \le j \le s$ $Q_1 Q_2 \dots Q_j \le G$ תת-חבורה !

$$|Q_1 Q_2 \dots Q_j| = p_1^{r_1} p_2^{r_2} \dots p_j^{r_j}$$

הוכחה באינדוקציה על j: עבור $j=1$ ברור.

נניח עבור $j-1$ ונסמן $L = Q_1 Q_2 \dots Q_{j-1}$

$$|L| = p_1^{r_1} p_2^{r_2} \dots p_{j-1}^{r_{j-1}}$$

L תת-חבורה

$$H = L \cap Q_j = \{e\}$$

H תת-חבורה

$$|H| \,\big|\, |Q_j| = p_j^{r_j}$$

כמו כן, $|H| \,\big|\, |L| = p_1^{r_1} \cdot \ldots \cdot p_{j-1}^{r_{j-1}}$

$\Longleftarrow$ $|H| = 1$

$\Longleftarrow$ $|LQ_j| = p_1^{r_1} \cdot \ldots \cdot p_j^{r_j}$

וברור LQ_j תת-חבורה.

$\Longleftarrow$ $G = Q_1 Q_2 \cdot \ldots \cdot Q_s$

וכן $G \cong Q_1 \times Q_2 \times \ldots \times Q_s$

הסבר: $G = \underbrace{Q_1 Q_2 \cdot \ldots \cdot Q_{s-1}}_{L_{s-1}} Q_s$

הערה: נשים לב כי:

$|G| = n$

$n = p_1^{r_1} p_2^{r_2} \ldots p_s^{r_s}$

Q_i תת-חבורה p_i-סילו

$|Q_i| = p_i^{r_i}$

ראינו $L_{s-1} \cap Q_s = \{e\}$

לכן $G \cong L_{s-1} \times Q_s$

$$L_{s-1} = \underbrace{Q_1 Q_2 \ldots Q_{s-2}}_{L_{s-2}} Q_{s-1}$$

$$L_{s-1} \cong L_{s-2} \times Q_{s-1}$$

וכן הלאה...

הראינו כי חבורה אבלית סופית היא מכפלה ישרה של חבורות סילו שלה.

עתה, נקבע ראשוני p וננסה להבין את מבנה חבורות סופיות אבליות מסדר p^r

משפט (8):

אם G אבלית סופית $|G| = p^r$ p ראשוני אזי קיימות חבורות ציקליות $C_1, \ldots, C_k$ כך ש: $G = C_1 \times C_2 \times \ldots \times C_k$

הערה: (כמו למשל בספר של Rotman)

הגדרה: מעריך של חבורה G (ההגדרה סופית) הוא d מינימלי רק שלכל $g\in G$ $g^d=e$

קיים d כזה כי לכל $d\in G$ $n=|G|$ $g^n=e$

נעבור, לשם נוחות, לכתיב חיבורי: $(G,+,0)$

אזי מעריך של G הוא d מינימלי כך ש $dg=0$ לכל $g\in G$

נשים לב כי אם G חבורה מסדר חזקות p אזי המעריך שלה חייב להיות חזקה של p.

נוכיח את משפט (*) באינדוקציה על המעריך של החבורה.

תהי G חבורה אבלית מסדר p^r ממעריך p.

G היא מרחב וקטורי מעל $\mathbb{F}_p=\mathbb{Z}/p\mathbb{Z}$

הוכחה: על G מוגדרת פעולת חיבור המקיימת את כל הדרישות מחיבור במרחב וקטורי.

צריך להגדיר כפל בסקלר מהשדה המקיים רשימה של דרישות:

עבור $g\in G$ $\alpha\in\mathbb{Z}/p\mathbb{Z}$

נבחר $a\in\mathbb{Z}$ כך ש a מועתק ל-α בהעתקה הקנונית $\mathbb{Z}\to\mathbb{Z}/p\mathbb{Z}$

נגדיר:

$$\alpha\cdot g=ag=\underbrace{g+g+\dots+g}_{a\text{ פעמים}}$$

למשל $p=3$

$$\mathbb{Z}/p\mathbb{Z}=\{0+3\mathbb{Z},1+3\mathbb{Z},2+3\mathbb{Z}\}$$

היות ולכל $g\in G$

$pg=0$

$a=$ 2 או 5

או 29

(כלומר הנבחר מודולו הוא מוצדק)

$$\alpha\cdot g=ag=\underbrace{g+g+\dots+g}_{a\text{ פעמים}}$$

מוגדר היטב כלומר תלוי ב-α וב-g ולא בבחירת a.

צריך לבדוק: $\forall\alpha,\beta\in\mathbb{Z}/p\mathbb{Z}$

$\forall g_1,g_2\in G$

$\alpha(g_1+g_2)=\alpha g_1+\alpha g_2$

$(\alpha+\beta)g_1=\alpha g_1+\beta g_1$

תרגיל קל

נזכור להוכחת משפט (א)

תהי G חבורה אבלית מסדר p^r מעריך p. אזי G היא מרחב וקטורי

מעל $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ ולכן יש לה בסיס: $g_1 g_2 \dots g_r$

ומקבלים ש:

$G \cong \langle g_1 \rangle \times \langle g_2 \rangle \times \dots \times \langle g_n \rangle$ מכפלה ישרה.

זהו בדיוק הפירוש של הטענה ש $g_1 \dots g_r$ בסיס: כל איבר ב- g

ניתן להציג באופן יחיד כ:

$\alpha_i \in \mathbb{Z}/p\mathbb{Z}$ $\quad g = g_1\alpha_1 + g_2\alpha_2 + \dots + g_r\alpha_r$.

עתה, נניח כי הוכחנו את טענת המשפט עבור חבורות

אבליות מסדר p^* ומעריך p^{s-1} (* הוא חזקה כלשהי כי לא משתמשים בזה)

תהי G חבורה אבלית מסדר p^r ומעריך p^s

נתבונן בתת-החבורה $H = pG$:

$H = \{pg \mid g \in G\}$

צריך לבדוק שאכן הקבוצה H היא תת-חבורה.

ואכן $0 \in H$ כי $0 = p \cdot 0$

סגירות: אם $h_1, h_2 \in H$ אזי קיימים $g_1, g_2 \in G$ כך ש: $g_1 = ph_1$, $g_2 = ph_2$

ולכן $h_1 + h_2 = pg_1 + pg_2 =$

$= p(g_1 + g_2) = \underbrace{(g_1+g_2)+(g_1+g_2) \dots +(g_1+g_2)}_{p \text{ פעמים}}$

הפכי: $h \in H$

$h = pg$

$-h = p(-g)$

כל $h \in H$ הסדר שלו הוא $\frac{1}{p} \cdot$ הסדר של $g \in G$ כך ש: $h = p \cdot g$

$h \in H \Longleftarrow$ קיים $g \in G$ $\quad h = p \cdot g$

$\Longleftarrow$ המעריך של H הוא המעריך של G חלקי p.

המשך בעמוד הבא

13-12-2006

מבנים אלגבריים - שעור מס' טז

משפט: חבורה G אבלית סופית היא סכום ישר של חבורות ציקליות. ראינו כי די לטפל במקרה בו $p^r=|G|$ עבור איזשהו ראשוני p.

במקרה זה סכום ישר = מכפלה ישרה.

Ω ולכל $\alpha\in\Omega$ G_α חבורה

$$f_1,f_2\in\prod_{\alpha\in\Omega}G_\alpha=\{f:\Omega\to\cup G_\alpha \mid f(\alpha)\in G_\alpha\}$$

$$(f_1,f_2)(\alpha)=f_1(\alpha)f_2(\alpha)$$

סכום ישר:
$$\bigoplus_{\alpha\in\Omega}G_\alpha=\left\{f\in\prod_{\alpha\in\Omega}G_\alpha \;\middle|\; f:\Omega\to\bigcup_{\alpha\in\Omega}G_\alpha \quad \forall_\alpha\in\Omega\ f(\alpha)\in G_\alpha \quad \text{לכמעט כל } \alpha\in\Omega\ f(\alpha)= \right\}$$

פרט למספר סופי של מקומות

דוגמא: $\Omega=\mathbb{N}$ $G_i=\mathbb{Z}/2\mathbb{Z}$

$$\prod_{n\in\mathbb{N}}\mathbb{Z}/2\mathbb{Z}=\{(x_1,x_2,\dots)\mid x_i\in\mathbb{Z}_2/\mathbb{Z}\ \forall i\}$$

$\geq$ בתור תת-חבורה

$$\bigoplus_{n\in\mathbb{N}}\mathbb{Z}/2\mathbb{Z}=\{(x_1,x_2,\dots)\mid x_i\in\mathbb{Z}_2/\mathbb{Z}\ \forall i \quad x_j=0 \text{ לכמעט כל } j\}$$

משפט: תהי G חבורה אבלית כך ש $p^r=|G|$ p ראשוני $r\in\mathbb{N}$ אזי $G\cong C_1\times C_2\dots\times C_m$ כאשר C_i ציקלית מסדר p^{r_i}.

הגדרה: (שנשתמש בה בהוכחה)

מעריך של חבורה $e(G)=\min\{k\mid kg=0\}$

הוכחת המשפט: באינדוקציה על המעריך של G.

אם $e(G)=1 \iff G=\{0\}$

אם $e(G)=p$ אזי G מרחב וקטורי מעל $\mathbb{Z}/p\mathbb{Z}$

לכן יש ל-G בסיס כמרחב וקטורי מעל $\mathbb{Z}/p\mathbb{Z}$ $z_1,\dots\dots,z_r$

ומתקיים כי G חבורה אבלית סופית ממעריך p^s $(s<r)$ ונניח כי המשפט מתקיים עבור חבורות אבליות ממעריך $<p^s$. נוכיח את המשפט עבור G.

נגדיר $H=pG=\{pg\mid g\in G\}$ תת-חבורה של G

טענה: $e(H) = e(G)/p$

הוכחה: יהי $h\in H$ אזי קיים $g\in G$ $h=pg$

$\Longleftarrow$ הסדר של h הוא $\frac{1}{p}$ הסדר של g

$p^{t}h=0 \Longleftrightarrow p^{t+1}g=0$

נחזור להוכחת המשפט:
(אנו יודעו חבורה ממעריך יותר קטן)

לכן לפי הנחת האינדוקציה קיימים $z_1,\dots,z_m \in H$

כך ש: $H=\langle z_1\rangle\times\langle z_2\rangle\times\dots\times\langle z_m\rangle$

לכל z_i $1\le i\le m$ קיים $y_i\in G$ כך ש: $z_i=py_i$

נתבונן באיברים $y_1,\dots,y_m \in G$.

נאמר כי איברים $x_1,\dots,x_n \in G$ הם בלתי

תלויים אם לכל $a_i\in\mathbb{Z}$ $1\le i\le n$

אם $0=a_1x_1+a_2x_2+\dots+a_nx_n$

אז $a_ix_i=0$ לכל i כלומר $\forall i\ \operatorname{order}(x_i)|a_i$

וזה גם שקול לכך
$\Longleftrightarrow$ $\langle x_1,\dots,x_n\rangle=\langle x_1\rangle\times\langle x_2\rangle\times\dots\times\langle x_n\rangle$

הערה כללית: M חבורה אבלית
$K,L<M$ תת-חבורות
ומתקיים: $K\cap L=\{0\}$
$K+L=M$
אז מתקיים
$K\times L\cong M$

אז יש לנו חבורה G
$\langle z_1\rangle\times\langle z_2\rangle\times\dots\times\langle z_m\rangle = H = pG$

מתקיים $y_i\in G$ $z_i=py_i$

טענה: $y_1,\dots,y_m$ בלתי תלויים

הוכחה: נניח כי $a_i\in\mathbb{Z}$ $\sum_{i=1}^{m}a_iy_i=0$

$\Longleftarrow$ $0=p(\sum_{i=1}^{m}a_iy_i)=\sum_{i=1}^{m}a_ipy_i=$

$=\sum_{i=1}^{m}a_iz_i=0$

$\Longleftarrow$ $\forall i\ a_iz_i=0$ $\Longleftarrow$ הסדר של $p^{d_i}=z_i$ מחלק את a_i

מכאן לכל $1\le i\le n$ $a_i=a_i'p$ $a_i'\in P$

$\Longleftarrow$ $0=\sum_{i=1}^{m}a_iy_i=\sum_{i=1}^{m}a_i'py_i=$

$=\sum_{i=1}^{m}a_i'z_i$

מאי תלות ה-z_i-ים $\Longleftarrow$ $a_i'z_i=0$ $\Longleftarrow$ $a_iy_i=a_i'py_i=0$

אז מה קיבלנו בינתיים?

קיבלנו $y_1, \dots, y_m \in G$ כך ש-G מכילה את הסכום הישר של החבורות הציקליות $\langle y_i \rangle$ $1 \le i \le m$.

אם מתמצעים למשפט

$$G = \underbrace{C_1 \times C_2 \times \dots \times C_m}_{} \times \underbrace{C_{m+1} \times \dots \times C_n}_{}$$!

אז: כל אחת מסדר p — מסדרים $\ge p^2$

נסמן $G = [p] = \{g \in G \mid pg = 0\}$

נשים לב כי $G[p]$ תת-חבורה של G.

$G[p]$ היא מרחב וקטורי מעל $\mathbb{Z}/p\mathbb{Z}$

כמו כן:

$$p^{r_1} = |\langle y_1 \rangle|$$

$$py_1' = p^{r_1} y_1 = 0 \qquad 0 \ne y_1' = p^{r_1 - 1} y_1 \in G$$

$y_i' = p^{r_i - 1} y_i$ כאשר $p^{r_i} = |\langle y_i \rangle|$

$$y_1', y_2', \dots, y_m' \in G[p]$$

$\square$ נחזור על כך בשיעור הבא.

<u>משפט:</u> תהי G חבורה אבלית מסדר p^n כאשר p ראשוני.

אזי קיימות תת-חבורות ציקליות $C_1,\dots,C_m$ רק ש $G=C_1\times C_2\times\dots\times C_m$

<u>הערה:</u> כאשר $C_1,\dots,C_m$ תת-חבורות של G אזי הפרוש של $G=C_1\times C_2\times\dots\times C_m$ הוא שלכל i C_i נורמלית. כלומר לכל $x\in C_i$, $y\in C_j$ $(i\neq j)$ מתקיים $yx=xy$ כלומר לכל $g\in G$ קיימים $h_1\in C_1\dots h_m\in C_m$ רק ש $g=h_1\dots h_m$ והם יחידים.

<u>הוכחה:</u> התחלנו את ההוכחה באינדוקציה על המעריך של G.

בשיעור הקודם ראינו שאם $H=pG$ אזי קיימים $\xi_1,\dots,\xi_m\in H$ רק ש $H=\langle\xi_1\rangle\times\dots\times\langle\xi_m\rangle$. בחרנו לכל $1\le i\le m$ $y_i\in G$ רק ש: $\xi_i=py_i$ וראינו ש $\{y_i\}$ בלתי-תלויים, כלומר, ראינו שאם נסמן $L_i=\langle y_i\rangle$ אז המכפלה הישרה $L_1\times\dots\times L_m$ היא תת-חבורה של G ואם $l_1+\dots+l_m=l_1'+\dots+l_m'$ אזי לכל $1\le i\le m$ $l_i=l_i'$. ראינו גם ש $G[p]$, אוסף כל האיברים מסדר p ב-G, היא תת-חבורה של G. מכיוון שכל האיברים בה הם מסדר p או 1 ניתן לראותה כמרחב-וקטורי מעל $\mathbb{Z}/p\mathbb{Z}$. המשכנו גם וראינו שאם נסמן $d_i=ord(\xi_i)$ ונתבונן ב $\bar{y}_i=d_iy_i\in G$ אזי:

$$p\bar{y}_i=pd_iy_i=d_ipy_i=d_i\cdot 0=0$$

ולכן $\bar{y}_i\in G[p]$ והם איברים בלתי-תלויים מעל $\mathbb{Z}/p\mathbb{Z}$ (זה כי אם נניח ש $\Sigma\bar{a}_i\bar{y}_i=0$ נוכל לבחור $a_i=\bar{a}_i \bmod p$ רק ש $\Sigma a_i\bar{y}_i=0$ ומכאן לקבל $a_id_i=0$, כלומר ש a_id_i מחלק את pd_i שהוא הסדר של y_i ומכאן לקבל ש $\bar{a}_i=0$ לכל i).

נשלים את $\{\bar{y}_i\}$ לבסיס $\bar{y}_1,\dots,\bar{y}_m,w_1,\dots,w_k$ של $G[p]$.

נראה כעת להראות ש $G=\langle y_1\rangle\times\langle y_2\rangle\times\dots\times\langle y_m\rangle\times\langle w_1\rangle\times\dots\times\langle w_k\rangle$

ומכאן לסיים את ההוכחה.

כלומר, צריך להראות שכל $g\in G$ הוא מהצורה $g=\sum_1^m h_i+\sum_1^k f_j$

כאשר $h_i\in\langle y_i\rangle$! $f_j\in\langle w_j\rangle$ והצגה זו היא יחידה.

נתחיל מכך שקיימת הצגה: יהי $g\in G$. $pg\in H$ ולכן קיימים $a_1,\dots,a_m$ כך ש:

$$pg=\sum_1^m a_i\xi_i=\sum_1^m a_i p y_i=p\sum_1^m a_i y_i$$

ולכן

$$\Longrightarrow\quad 0=p\Big(g-\sum_1^m a_i y_i\Big)$$

כלומר $\Big(g-\sum_1^m a_i y_i\Big)\in G[p]$

לכן קיימים $a'_1,\dots,a'_m,b_1,\dots,b_k\in\mathbb{Z}$ כך ש

$$g-\sum_1^m a_i y_i=\sum_1^m a'_i\bar{y}_i+\sum_1^k b_j w_j$$

$$\Longleftrightarrow\quad g=\sum_1^m (a_i y_i+a'_i\bar{y}_i)+\sum_1^k b_j w_j=\sum_1^m (a_i+d_i a'_i)y_i+\sum_1^k b_j w_j\,.$$

כלומר ההצגה אכן קיימת.

נעבור לכך שקיימת הצגה יחידה: כלומר נראה שאם $\sum_1^m a_i y_i+\sum_1^k b_j w_j=0$
אזי לכל $1\le i\le m$ $a_i y_i=0$ ולכל $1\le j\le k$ $b_j w_j=0$. אכן, אם מתקיים השוויון אזי

$$0=p\cdot 0=p\Big(\sum_1^m a_i y_i+\sum_1^k b_j w_j\Big)=\sum_1^m a_i p y_i+\sum_1^k b_j p w_j=$$

$$=\sum_1^m a_i\xi_i$$

לכן, לכל $1\le i\le m$ $a_i\xi_i=0$! a_i מתחלק ב d_i.

אם נרשום $a_i=a'_i d_i$ נקבל ש $0=\sum_1^m a'_i d_i y_i+\sum b_j w_j=\sum_1^m a'_i\bar{y}_i+\sum b_j w_j$

ומכיוון ש $\bar{y}_1,\dots,\bar{y}_m,w_1,\dots,w_k$ בסיס מעל $\mathbb{Z}/p\mathbb{Z}$ נקבל ש: $p|b_j$ $\quad p|a'_i$

ולכן $b_j w_j=0$ $\quad a'_i=\tilde{a}_i p$ מכאן ש:

$$a_i y_i=a'_i d_i y_i=\tilde{a}_i p d_i y_i=\tilde{a}_i 0=0$$

$$b_j w_j=0$$

כלומר הראינו יחידות.

18-12-2006 ②

הערה: הראינו שאם G אבלית ו- $|G|=p^r$ אזי $G=C_1\times C_2\times\dots\times C_m$

כאשר $|C_i|=p^{r_i}$ ו- $\sum_1^m r_i=r$ בה"כ ניתן להניח $r_1\ge r_2\ge\dots\ge r_m$.

טענה: $r_n,\dots,r_1$ יחידים.

כלומר, אם $C_1\times C_2\times\dots\times C_n\cong D_1\times\dots\times D_k$ ו- $|C_i|=p^{r_i}$ $|D_j|=p^{s_j}$

אזי $k=n$ ו- $r_i=s_i$ $\forall 1\le i\le n$

הוכחה: נסמן $G=C_1\times\dots\times C_n$. $G[p]$ הינו מרחב וקטורי מעל $\mathbb{Z}/p\mathbb{Z}$

ומתקיים (מספר המחברים מסדר p ב- C_i) $L_i=C_i[p]$: $G[p]=L_1\times\dots\times L_n$

מכיוון שמימד של מרחב וקטורי הוא יחיד נקבל ש $n=k$ ($|G[p]|=p^n=p^k$).

נשאר להראות $r_i=s_i$ $\forall 1\le i\le n$

נשים לב שאם נרצה לחשב כמה C_i-ים הם מסדר p אזי מספיק יהיה לחשב

כמה C_i-ים יש שסדרם גדול מ p. נשים לב שאם נגדיר $H=pG$

אזי $H=pC_1\times\dots\times pC_n=\prod_1^n pC_i$ אך מכיוון שאם $p=|C_i|$ אזי $\{pC_i\}=0$

ואם $|C_i|>p$ אזי $|pC_i|=|C_i|/p$ קיים $m<n$ רק ש $H=\prod_1^m pC_i$

ו- m ניתן ע"י $m=\max\{i: p^{r_i}>p\}$. נשים לב כי m נקבע ע"י

H, והאינדוקציה על סדר החבורה אך סדר כל אחד מבין pC_i נקבע ביחידות

על ידי H. לכן אך סדר כל אחד מבין $C_1,\dots,C_m$ נקבע ע"י H ולכן ע"י G.

יש $n-m$ גורמים, $C_{m+1},\dots,C_n$ מסדר p.

נניח האינדוקציה על סדר החבורות כי עבור חבורה מסדר קטן מ p^r הפירוק למכפלות

ציקליות אזי החבורות הציקליות נקבע ביחידות.

תהי G מסדר p^r. נתבונן ב $H=pG$. $|H|<|G|$ ולכן עפ"י הנחת

האינדוקציה, מספר הגורמים בפירוק של H למכפלת חבורות ציקליות נקבע באופן

יחיד ע"י H (ולכן ע"י G) וכן, אפילו הם נקבעים (הסדרים) של pC_i נקבעים

ומתקיים $(|C_i|=|pC_i|\cdot p)$.

משפט-

תהי G חבורה אבלית סופית מסדר n.

קיימות חבורות ציקליות $C_1,\dots,C_k$ כך ש $G=C_1\times\dots\times C_k$

ואם נסמן $|C_i|=n_i$ אזי לכל $1\le i\le k$ $|C_{i+1}|\,\big|\,|C_i|$

הוכחה:

נתבונן בפירוק של n למכפלת ראשוניים $n=p_1^{s_1}\cdots p_m^{s_m}$.

אזי $G=Q_1\times\dots\times Q_m$ כאשר Q_i חבורת p_i-סילו של G ו $|Q_i|=p_i^{s_i}$

לכל Q_i ניתן לפרק למכפלה $Q_i=C_{i,1}\times\dots\times C_{i,k_i}$ של חבורות ציקליות.

נסמן, לכל $1\le i\le r$ (כאשר $r=\max\{n_i\}$), $L_i=C_{1,i}\times\dots\times C_{m,i}$

ואז ברור ש $G=L_1\times\dots\times L_r$ וכן ש $|L_{i+1}|$ מחלקת את $|L_i|$.

נשאר רק להראות ש L_i ציקלית אך זה ברור מכך ש $C_{j,i}$ ציקליות

מסדרים זרים מבוססת (רמז: מה שאם C,D ציקליות כך ש $|C|=a$ ו $|D|=b$ ו a,b זרים אזי $C\times D$ ציקלית מסדר $a\cdot b$)

משפט:

תהי G חבורה אבלית סופית.

אזי קיימות תת-חבורות ציקליות $C_1,\dots,C_m$ כך ש $G \cong C_1\times C_2\times\dots\times C_m$

($G=C_1\times C_2\times\dots\times C_m$ $\quad C_i<G$

$G=C_1+C_2+\dots+C_m$ (והסכום יחיד. כלומר לכל $g\in G$ יש $x_1=c_1,\dots,x_m=c_m$ יחידים כך ש: $g=x_1+x_2+\dots+x_m$)

לפני שנוכיח את המשפט נוכיח למה:

למה: תהי G חבורה אבלית ויהיו $x_1\dots x_n\in G$ יוצרים של G.

אזי עבור כל $a_1,\dots,a_n\in\mathbb{Z}$ כך שהמחלק המשותף המירבי שלהם הוא 1

קיימת קבוצת יוצרים $y_1\dots y_n\in G$ של G כך ש $y_1=a_1x_1+\dots+a_nx_n$

(כלומר ניתן להשלים את $a_1x_1+\dots+a_nx_n$ לקבוצת יוצרים בגודל n)

(נוכיח בהמשך...)

הוכחת המשפט:

יהי n הגודל המינימלי של קבוצת יוצרים של G. נבחר קבוצת יוצרים מגודל מינימלי זה.

$\{x_1,\dots,x_n\}$ כך שהסדר של x_1, שנסמנו ב-k, הוא הקטן ביותר מבין כל הסדרים

של איברים המשתתפים בקבוצות בנות n יוצרים של G.

נסמן $H=\langle x_2,\dots,x_n\rangle$ ונשים לב ש $H<G$ תת-חבורה ממש.

לכן ניתן להוכיח באינדוקציה כי H היא סכום ישר של חבורות ציקליות וכדי להראות

ש $G=\langle x_1\rangle\times H$ אם כך, צריך להראות שמתקיים:

(א) כל איבר ב-G הוא סכום של איבר מ-$\langle x_1\rangle$ ו-H

(ב) $\langle x_1\rangle\cap H=\{0\}$

(א) מתקיים כי $x_1,\dots,x_n\in\langle x_1\rangle+H$ ולכן $G=\langle x_1,\dots,x_n\rangle\subseteq\langle x_1\rangle+H$

וההכלה ההפוכה ברורה $G\supseteq\langle x_1\rangle+H$

כדי להראות את ב', נניח כי $\langle x_1\rangle\cap H\neq\{0\}$ ונבחר $0\neq g\in\langle x_1\rangle\cap H$

אזי קיימים $b_1,\dots,b_n\in\mathbb{Z}$ כך ש $b_1x_1=g=b_2x_2+b_3x_3+\dots+b_nx_n$

$\Longleftrightarrow 0=-b_1x_1+b_2x_2+\dots+b_nx_n$

יהי d המחלק המשותף המירבי של $b_1 \dots b_n$ ונגדיר $a_1 = \frac{-b_1}{d}$

! $a_i = \frac{b_i}{d}$ לכל $1 \le i \le n$

$a_1, \dots, a_n$ זרים ולכן אם נסמן $y_1 = a_1x_1 + \dots + a_nx_n$ אזי לפי הלמה

קיימים $y_2, \dots, y_n \in G$ כך ש $\{y_1 \dots y_n\}$ יוצרים את G.

נתבונן ב-y_1 ונשים לב כי $dy_1 = d(a_1x_1 + \dots + a_nx_n) =$

$= -b_1x_1 + b_2x_2 + \dots + b_nx_n$

לכן, הסדר של $y_1 \ge d \ge b_1 \ge b_1 >$ סדר של $x_1 = k$ וזוהי סתירה למינימליות בחירת $\{x_1, \dots, x_n\}$

כקבוצה המכילה את האיבר עם הסדר הקטן ביותר מבין כל הסדרים של איברים

המשתתפים בקבוצות בנות n יוצרים של G.

טענה:

יהיו $a_1 \dots a_n \in \mathbb{Z}$ זרים. אזי קיימת מטריצה $A \in SL_n(\mathbb{Z}) = \{A \in M_n(\mathbb{Z}) : |A| = 1\}$

כך שהשורה הראשונה שלה היא $(a_1 \dots a_n)$

הערה: נשים לב כי הטענה גוררת את הלמה מהמשפט הקודם כי אם נתון $a_1 \dots a_n$

זרים קיימת מטריצה כמו בטענה ואז ניתן להגדיר $y_i = \sum a_{ij}x_j$ ואז

מספיק להראות ש $y_1 \dots y_n$ יוצרים את G.

לשם כך די להראות כי לכל $1 \le k \le n$ $x_k \in \langle y_1, \dots, y_n \rangle$

היות ! $A \in SL_n(\mathbb{Z})$ יש לה הופכית $(b_{ij}) = B = A^{-1} \in SL_n(\mathbb{Z})$

ומתקיים $\sum_{k=1}^{n} b_{ik}a_{kj} = \delta_{ij}$

נתבונן ב $\xi_i = \sum_{k=1}^{n} b_{ik}y_k \in \langle y_1 \dots y_n \rangle$

ואז $\xi_i = \sum_{k=1}^{n} b_{ik}y_k = \sum_{k=1}^{n} b_{ik} \sum_{j=1}^{n} a_{kj}x_j =$

$= \sum_{k=1}^{n}\sum_{j=1}^{n} b_{ik}a_{kj}x_j = \sum_{j=1}^{n}\left(\sum_{k=1}^{n} b_{ik}a_{kj}\right)x_j = \sum_{j=1}^{n} \delta_{ij}x_j = x_i$

ולכן לכל $1 \le i \le n$ $x_i = \xi_i \in \langle y_1, \dots, y_n \rangle$

הערה נוספת: עבור המקרה של $n=2$ ראינו כבר שאם $\gcd(a_1, a_2) = 1$ אזי קיימים

$k, l \in \mathbb{Z}$ כך ש $ka_1 + la_2 = 1$ ולכן $\det\begin{pmatrix} a_1 & a_2 \\ -l & k \end{pmatrix} = a_1k + a_2l = 1$

כלומר ראינו כבר את הטענה עבור מקרה זה

הוכחת הטענה בשיעור הבא

25-12-2006

מבנים אלגבריים - שיעור מס' 19

נותרה לנו טענה משיעור קודם שעלינו להוכיח

טענה: אם $a_1,\dots,a_n \in \mathbb{Z}$ כך שהמחלק המשותף המרבי שלהם הוא 1

אזי קיימת מטריצה

$(a_{ij}) = A \in SL_n(\mathbb{Z})$ $\quad a_{ij}\in\mathbb{Z}$

$1\le i,j\le n$ $\quad \det A=1$

כך שהשורה הראשונה היא $a_1,\dots,a_n$

כלומר $a_{1j}=a_j$ $\quad 1\le j\le n$

הוכחה (רעיון ההוכחה):

נתחיל מהוקטור $v_0=(a_1,\dots,a_n)$

וניצור סדרות וקטורים $v_1,v_2,\dots$

כאשר כל v_{i+1} מתקבל מ- v_i על ידי אחת מהפעולות הבאות:

(א) שינוי סדר

$v_i=(x_1,\dots,x_n)$

$v_{i+1}=(x_{\pi(1)},\dots,x_{\pi(n)})$ $\quad \pi\in S_n$

תאור שלב א':

$v_{i+1}=v_i\cdot B_\pi$

מטריצת התמורה $\pi(i)=\begin{pmatrix}0&1&0&0&0\\ \vdots\\ 0&0&0&1&\dots\end{pmatrix}$

(ב) הפחתת כפולה שלמה של מקום k ממקום l $\quad k\neq l$

$v_i=(x_1\dots x_k\ x_l\dots x_n)$

$v_{i+1}=(x_1\dots x_k\ x_l-mx_k\dots x_n)$ $\quad m\in\mathbb{Z}$

תאור שלב ב':

$$v_{i+1}=v_i\begin{array}{cc}\begin{pmatrix}1 & \cdots & -m & \cdots\\ & \ddots & \vdots & \\ 0 & & \vdots & 1\end{pmatrix} & k\\ \quad\quad\ l & \end{array}$$

כלומר מטריצה C כך ש: $C_{ii}=1$, 0 בכל מקום אחר פרט ל- C_{kl}

קל לראות כי ניתן לבחור צעדים כאלו כך שלאחר מספר סופי של צעדים נקבל

$v_N=(1,0,\dots,0)$

(ג) נרשה גם צעד שלישי (מסוג ג):

כפל של x_1 ב- -1 $\quad v_{i+1}=(-x_1,x_2,\dots,x_n)$

v_0

$v_1=v_0A_1$ $\quad$ A_j מטריצה מאחד משלושת הסוגים לעיל

$v_2=v_1A_2$

$\vdots$

$v_N=v_{N-1}A_N$

$\Leftarrow$ $v_N=v_0(A_1A_2\dots A_N)$

קיבלנו כי $(1\,0\,0\,0\ldots0)=(a_1\ldots\ldots a_n)Y$

כאשר $Y=A_1A_2\ldots A_N$

$\det Y=(\pm1)$

$Y\in M_n(\mathbb{Z})$

אם $\det Y=-1$ אזי נוסיף צעד:

אנחנו נמצאים ב: $(1\;0\ldots\ldots0)$

ונעבור ל $(1,-0,\ldots\ldots0)$ ("הופכים" את הסימן של אפס אין צעד רק מבחינת הוקטור)

וכעת הדטרמיננטה היא 1.

$$(1\,0\ldots\ldots0)=(1\,0\ldots0)\begin{pmatrix}1&&&&\\&-1&&&\\&&1&&\\&&&\ddots&\\&&&&1\end{pmatrix}$$

ב· הגבלת הכלליות הדטרמיננטה היא 1.

דוגמה: אם יש לנו $(6\;10\;15)$

1. $$(6\;4\;15)=(6\;10\;15)\begin{pmatrix}1&-1&0\\&1&0\\&&1\end{pmatrix}$$

2. $$(6\;4\;3)=(6\;4\;15)\begin{pmatrix}1&0&0\\&1&-3\\&&1\end{pmatrix}$$

$$(6\;1\;3)=(6\;4\;3)\begin{pmatrix}1&&\\&1&\\&-1&1\end{pmatrix}$$

$$(0\;1\;3)=(6\;1\;3)\begin{pmatrix}1&&\\-6&1&\\0&&1\end{pmatrix}$$

$$(1\;0\;3)=(0\;1\;3)\begin{pmatrix}0&1&\\1&0&\\&&1\end{pmatrix}$$

$(1\;0\;0)$

25-12-2006

②

<u>קיבלנו כי:</u>

$$(1\ 0\ 0 \dots 0) = (a_1 \dots a_n) Y$$

$$Y \in SL_n(\mathbb{Z})$$

ולכן קיימת מטריצה $Z = Y^{-1} \in SL_n(\mathbb{Z})$

$$(1\ 0\ 0 \dots 0) Z = (a_1 \dots a_n) \underbrace{YZ}_{I} = (a_1 \dots a_n)$$

ולכן למטריצה $Z \in SL_n(\mathbb{Z})$ יש שורה $(a_1 \dots a_n)$ כמבוקש.

נשים לב כי, כל עוד לא הגענו למצב בו כל המקומות פרט לאחד (לכל היותר) הם 0 ניתן בכל שלב להקטין את סכום הערכים המוחלטים של המספרים בוקטור $(x_1 \dots x_n)$.

<u>אפשרות א':</u> יש רק מקום אחד יחיד שונה מ-0.

<u>אפשרות ב':</u> יש שני מקומות $x_k, x_l \neq 0$ אזי ע"י צעד מסוג ב, כלומר הפחתת כפולת האחד מהשני, ניתן להקטין את סכום הערכים המוחלטים.

כי נניח $0 < x_k < x_l$

$$(\dots x_k\ x_l \dots) \to (\dots x_k,\ x_l - x_k \dots)$$

$$|x_k| + |x_l - x_k| < |x_k| + |x_l|$$

אם $x_k < 0 < x_l$

$$|x_k| < |x_l|$$

אזי:

$$(\dots x_k\ x_l \dots) \to (0 \dots x_k \dots x_l + x_k \dots)$$

ושוב

$$|x_k| + |x_k + x_l| < |x_k| + |x_l|$$

וכן הלאה...

התהליך חייב להעצר כלומר ניתן להמשיך ולהקטין את סכום הערכים המוחלטים

רק מספר סופי של פעמים

כלומר לאחר מספר סופי של צעדים נגיע לצעד בו: $V_k = (x_1 \ldots x_n)$

הוא וקטור בו יש רק מקום אחד שונה מ-0 (לכל היותר)

כלומר $V_k = (0 \ldots 0\ d \ldots 0)$

d הוא מחלק של $(a_1 \ldots a_n)$ והיות והם זרים $d = \pm 1$ וסיימנו

כי בכל אחד מהצעדים אנו שומרים על המחלק המשותף המירבי

של n-ית המספרים.

אם $V_j = (x_1 \ldots x_n)$

$V_{j+1} = (y_1 \ldots y_n)$

אז $g.c.d(x_1 \ldots x_n) = g.c.d(y_1 \ldots y_n)$ (*)

(*) ברור עבור שינוי סדר.

(*) ברור עבור כפל של אחד מה איברים ב-(-1)

את (*) צריך להוכיח עבור מקרה בו

יש $1 \le k \ne l \le n$

$$y_j = \begin{cases} x_j & j \ne l \\ x_l + m x_k & j = l \end{cases}$$

אם $\forall i \quad d \mid x_i$

אז $\forall j \quad d \mid y_j$

ולהיפך אם $\forall j \quad d \mid y_j$

$\forall i \quad d \mid x_i$

25-12-2006

$y_l = x_l + m x_k$

כי $y_j = x_j$ $\forall j \neq l$

$x_l = y_l - m y_k$

מפרט $y_k = x_k$

זהו תהליך דומה לאלגוריתם של
אוקלידס רק שפועל על יותר
משני מספרים

נתחיל נושא חדש:

הגדרה: תהי G חבורה. סדרה נורמלית ב-G היא סדרת תת-חבורות.

כך ש: $G = G_0 \triangleright G_1 \triangleright \dots \triangleright G_k = 1$

G_i $\quad 0 \le i \le k$

$G_k = 1$ $\quad G_0 = G$ וכל i $\quad G_i \triangleright G_{i+1}$

הערות: * G_5 נורמלית ב-G_4 אבל לא בהכרח נורמלית ב: G_0, G_1, G_2, G_3.

* לכל חבורה יש סדרות נורמליות: $G = G_0 \triangleright G_1 = \{e\}$

* מרשים חזרות: $G_i = G_{i+1}$

הגדרה: סדרת הרכב עבור G היא סדרה נורמלית כך ש לכל $0 \le i \le k-1$
חבורת המנה G_i/G_{i+1} פשוטה.

הגדרה: עידון של סדרות נורמליות:

סדרה נורמלית $G = H_0 \triangleright H_1 \triangleright \dots \triangleright H_m = \{e\}$

תקרא עידון (refinment) של סדרה נורמלית $G = G_0 \triangleright G_1 \triangleright \dots \triangleright G_k = \{e\}$

אם קיימת פונקציה חח"ע

$$\varphi : \{0, 1, \dots, k\} \to \{0, 1, \dots, m\}$$

$$\varphi(0) = 0$$

$$\varphi(k) = m$$

ולכל $0 \le i \le k$ $\quad G_i = H_{\varphi(i)}$

תהי G סופית

משפט: ותהי $G=G_0 \rhd G_1 \rhd \dots \rhd G_n=\{e\}$ סדרה נורמלית

אזי יש לה עידון $G=H_0 \rhd H_1 \rhd \dots \rhd H_m=\{e\}$

כך ש H_i/H_{i+1} פשוטה $0\leq i\leq m-1$

כלומר לכל סדרה נורמלית יש עידון שהוא סדרת הרכב (אנחנו מרשים חזרות)

למה: אם $G=G_0 \rhd G_1 \dots \rhd G_k=1$ ו- G סופית

אזי $|G|=\prod_{i=0}^{k-1} |G_i/G_{i+1}|$ (סדר החבורה הוא מכפלת הסדרים של הגורמים)

הגדרה: בהינתן סדרה נורמלית $G=G_0 \rhd G_1 \rhd \dots \rhd G_k=\{e\}$

המנות G_i/G_{i+1} נקראים הגורמים של הסדרה.

הוכחת הלמה: אם G חבורה סופית ו- N תת-חבורה נורמלית אזי:

$$|G|=|G/N|\cdot|N|$$

הוכחת המשפט:

תהי $G=G_0 \rhd G_1 \rhd \dots \rhd G_k=1$ סדרה נורמלית.

אם כל G_i/G_{i+1} פשוטה אז סיימנו.

אחרת יהי $0\leq i\leq k-1$ כך ש $L=G_i/G_{i+1}$ אינה פשוטה

אזי ב- L יש תת-חבורה נורמלית $N \lhd L$ $N\neq L$

$N\neq\{e\}$

כי נתבונן בהומומורפיזם $\varphi: G_i \longrightarrow L=G_i/G_{i+1}$

ונגדיר $\tilde{G}$ להיות $\varphi^{-1}(N)$ אזי $\tilde{G} \rhd G_{i+1}$ ו- $G_i \rhd \tilde{G}$

אם $h\in\tilde{G}$ (כלומר $\varphi(h)\in N$) ! $g\in G_i$

אזי:

$$\underbrace{\varphi(ghg^{-1})=\varphi(g)\underbrace{\varphi(h)}_{\in N}\varphi(g^{-1})}_{\in N}$$

$$\Longleftarrow \quad ghg^{-1}\in\varphi^{-1}(N)=\tilde{G}$$

כלומר $G_i \rhd \tilde{G}$

נעבור את $G_0 \triangleright G_1 \triangleright \dots \triangleright G_i \triangleright G_{i+1} \triangleright \dots G_k$

על ידי הוספת $\tilde{G}$ בין G_i ל- G_{i+1} ונבדוק אם כל המנות פשוטות

וסיימנו אם יש לחזור על התהליך וברור שאחרי מספר סופי של צעדים

התהליך חייב להעצר.

$\boxed{\diagup\diagup}$

הערה: אם G אינסופית יתכן והתהליך לא נעצר למשל $\mathbb{Z} \triangleright 1$

$\mathbb{Z} \triangleright 10\mathbb{Z} \triangleright 1$

$\mathbb{Z}_5 \triangleright 5\mathbb{Z} \triangleright 10\mathbb{Z} \triangleright 1$

יש דוגמאות אינסופיות בהן התהליך נעצר;

למשל $G = SL_2(\mathbb{R})$

$$G = SL_2(\mathbb{R}) \triangleright \{I\}$$

$$SL_2(\mathbb{R}) \triangleright Z = \{I, -I\} \triangleright \{I\}$$

$$\begin{pmatrix} 1 & 0 \\ c & 1 \end{pmatrix} \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$$

$$SL_2(\mathbb{R}) / \{I, -I\} = PSL_2(\mathbb{R})$$ פשוטה.

אך אם למשל $H = \left\{ \begin{pmatrix} 1 & a & b \\ & 1 & c \\ & & 1 \end{pmatrix} \middle| a,b,c \in \mathbb{Z} \right\}$ התהליך לא נעצר.

הגדרה: שתי סדרות נורמליות של G

$$G = G_0 \triangleright G_1 \triangleright \dots \triangleright G_m = 1$$

$$G = H_0 \triangleright H_1 \triangleright \dots \triangleright H_n = 1$$

יקראו שקולות אם: $m = n$ ויש תמורה π על $\{0,1,\dots,n-1\}$

כך ש: $$G_i / G_{i+1} \cong H_{\pi(i)} / H_{\pi(i)+1}$$

ננסח משפט שנצריך במשפט הבא:

משפט העידון של שרייר:

תהי G חבורה סופית אזי לכל שתי סדרות נורמליות יש עידונים שקולים.

מסקנה: (מהמשפט) (משפט ז'ורדן-הולדר)

תהי G חבורה סופית ותהיינה $G=G_0 \triangleright G_1 \triangleright \dots \triangleright G_m=1$

$G=H_0 \triangleright H_1 \triangleright \dots \triangleright H_n=1$

סדרות הרכב ללא חזרות אזי הן שקולות ובפרט $n=m$.

נסתכל לדוגמא על: G חבורה נורמלית ציקלית מסדר 60

המנות הן $C_2 \quad C_2 \quad C_3 \quad C_5$

$$C_{60} \triangleright C_{30} \triangleright C_{15} \triangleright C_5 \triangleright 1$$

ואפשר למשל:

$$C_{60} \triangleright C_{20} \triangleright C_4 \triangleright C_2 \triangleright 1$$

$C_3 \quad C_5 \quad C_2 \quad C_2$ המנות הן

(דוגמה: הכללה של המשפט היסודי של האריתמטיקה שכן מס' ניתן לפרק יחיד לראשוניים עד כדי שינוי סדר)

הגדרה: (עבור התרגיל)

חבורה G תקרא פתירה אם יש לה סדרה נורמלית עם גורמים ציקליים (כל הגורמים)

מבנים אלגבריים - שיעור מס' 20

הגדרה: חבורה G סופית, תקרא פתירה אם יש לה סדרה נורמלית
עם גורמים ציקליים (גורמים = מנות).

דוגמא שימושית: בהינתן פולינום, שואלים האם ניתן להציג את כל השורשים
כביטויים במקדמים תוך שימוש בפעולות ($\sqrt{\ }, \cdot, -, +$) (המשך הדוגמא לא ממש ברור
אבל אפשר להמשיך בלי זה)

המטרה שלנו היא להגיע למשפט ג'ורדן הולדר:

משפט ג'ורדן הולדר:

תהי G חבורה סופית, אז כל שתי סדרות הרכב ללא חזרות הן שקולות.

הלמה של צסנהאוס:

תהי G חבורה ויהיו A, A^*, B, B^* תתי חבורות כך ש $A \triangleleft A^*$ $B \triangleleft B^*$

אז $A(A^*\cap B) \triangleleft A(A^*\cap B^*)$

$B(A\cap B^*) \triangleleft B(A^*\cap B^*)$

ומתקיים $B(A^*\cap B^*)/B(A\cap B^*) \cong A(A^*\cap B^*)/A(A^*\cap B)$

[מסקנה מלמה זו: משפט העידון של שרייר (שיוכח בהמשך)

תהי G חבורה אזי לכל שתי סדרות נורמליות של G יש עידונים שקולים]

הוכחת הלמה: $A(A^*\cap B^*)$ היא תת-חבורה כי $A \triangleleft A^*$ $A^*\cap B^* \le A^* \Rightarrow A(A^*\cap B^*)$

היא תת-חבורה. נגדיר: $D = (A^*\cap B)(A\cap B^*)$ ושוב נבדוק שזוהי תת-חבורה

$A^*\cap B \le A^*\cap B^*$ כי $B \triangleleft B^*$, $A \triangleleft A^*$ אם $x \in A^*\cap B$ $y \in A^*\cap B^*$

$yxy^{-1} \in B$ $(y\in B^*, x\in B, B\triangleleft B^* \Rightarrow yxy^{-1}\in B)$.

$yxy^{-1} \in A^*$ $(y\in A^*, x\in A^*)$

$\Rightarrow A^*\cap B \triangleleft A^*\cap B^*$

באותה הדרך $A\cap B^* \triangleleft A^*\cap B^*$

$\Rightarrow$ D תת חבורה (מכפלה של שתי תת-חבורות נורמליות) ! $D \triangleleft A^*\cap B^*$

נראה כי $A(A^*\cap B^*)/A(A^*\cap B) \cong A^*\cap B^*/D$ ← נסמן את השוויון הרצוי ב- $\boxtimes$

נשים לב כי אם נחליף בה $\boxtimes$ את B ב- A (נקבל) הוכחה של

המשך בעמ' הבא ←

$$B(A^*\cap B^*)/B(B^*\cap A) \cong B^*\cap A^*/(B^*\cap A)(B\cap A^*)$$

נשים לב כי $A^*\cap B^* = B^*\cap A^*$ וגם $(B^*\cap A)(B\cap A^*) = (A^*\cap B)(A\cap B^*)$

$(B^*\cap A)(B\cap A^*) = (A\cap B^*)(A^*\cap B) \Longleftarrow B\cap A^* = A^*\cap B\ ,\ B^*\cap A = A\cap B^*$

ואנו יודעים שאם H חבורה $K,L \triangleleft H$ אזי $KL=LK$

ולכן $= (A^*\cap B)(A\cap B^*)$

הוכחה $\boxed{/}$:

$$A(A^*\cap B^*)/A(A^*\cap B) \cong A^*\cap B^*/\underbrace{(A^*\cap B)(A\cap B^*)}_{D}$$

נמצא הומומורפיזם $\varphi: A(A^*\cap B^*) \longrightarrow A^*\cap B^*/D$

כך ש- φ על ! $\ker\varphi = A(A^*\cap B)$

אם $x\in A(A^*\cap B^*)$ אז $x=ac$ כך ש $a\in A$! $c\in A^*\cap B^*$

נגדיר $\varphi(x)=\varphi(ac)=cD\in A^*\cap B^*/D$

ac לא מההכרח מוגדרים ביחידות לכן צריך להוכיח ש-φ מוגדרת היטב.

φ מוגדרת היטב: $a'c'=x=ac$ $\quad a,a'\in A$ $\quad c,c'\in A^*\cap B^*$

$$A\ni a^{-1}a' = c(c')^{-1}\in A^*\cap B^* \Longleftarrow a'c'=ac$$

לכן $c(c')^{-1}\in(A^*\cap B^*)\cap A = A\cap B^* \subseteq D$ $\ (A\subseteq A^*)$

$$cD=c'D \Longleftarrow \underbrace{cD=Dc}_{\text{נורמלית}} = \underbrace{Dc'=c'D}_{\text{נורמלית}} \Longleftarrow c(c')^{-1}\in D \Longleftarrow$$

$\Longleftarrow$ φ מוגדרת היטב.

φ על: $\varphi: A(A^*\cap B^*)\longrightarrow A^*\cap B^*/D$ $\quad A^*\cap B^*\subseteq A(A^*\cap B^*)$ $\quad \varphi|_{A^*\cap B^*}$ היא ההומומורפיזם הטבעי מ- $A^*\cap B^*$ על $A^*\cap B^*/D$

φ הומומורפיזם: לבדוק לבד.

$\ker\varphi = A(A^*\cap B)$

$$x\in\ker\varphi \Longleftrightarrow x=ac\ ,\ c\in D \Longleftarrow cD=D$$

[בעצם $\ker\varphi = A\cdot D\cap A(A^*\cap B^*)$] $\quad \ker\varphi = A(D) = A(A^*\cap B)(\ \cap B^*) =$

$$= A(A\cap B^*)(A^*\cap B) = A(A^*\cap B)$$

27-12-2006

$$A(A^*\cap B) = \ker\varphi \triangleleft A(A^*\cap B^*)$$

מאותה הגדרה $B(B^*\cap A) \triangleleft B(B^*\cap A^*)$

האיזומורפיזם נובע מהסימטריה של $\boxtimes$

כי:

$$B(B^*\cap A^*)/B(B^*\cap A) \cong A^*\cap B^*/D \cong A(A^*\cap B^*)/A(A^*\cap B)$$

$$\cong$$

והלמה של צסנהאוז הוכחה.

בשבוע הבא שחר לא יהיה, עמנואל סרצון יחליף אותו
ויתחיל איתנו את תורת החוגים וכשחר יחזור נמשיך מנושא זה.

תורת החוגים (עמנואל פרג'ון מחליף את שחר מוזס)

עד כה למדנו:

שדות: הכללה של $\mathbb{C}, \mathbb{R}, \mathbb{Q}$ $\{F, +, \cdot, 0 \neq 1\}$

מרחבים וקטורים: $\mathbb{R}^n, \mathbb{C}^n$ (F, V), $\begin{matrix} F \times V \longrightarrow F \\ (a, v) \longmapsto av \end{matrix}$ V חבורה אבלית

חבורות: $G \times G \to G$, $(G, \cdot)$ כמו הכללה של פרמוטציות של $(0, 1, \dots, n-1)$

$$\Sigma_n = \{ \{0, 1, \dots, n-1\} \xrightarrow{\cong} \{0, 1, \dots, n-1\} \}$$

כאשר למדנו על מרחבים וקטורים הגענו לטרנספורמציות לינאריות ממרחב וקטורי אחד לשני: $V \to W$

בחירת בסיס ל-V, W הביא אותנו למטריצה ריבועית. נתמקד במטריצות ריבועיות (מעל שדה F) $n \times n$ $A = (a_{ij})$ ונסמן את אוסף כל המטריצות הללו ב-$M_n(\mathbb{F})$

מטריצות אלו מתארות טרנספורמציות לינאריות (אחרי בחירת בסיס) מ-V ל-V כאשר $\dim V = n$

אילו פעולות אנחנו מכירים על מטריצות?

$$C, B, A \in M_{n \times n}(\mathbb{F})$$

(1) $B + A = A + B$

(2) $A \cdot B \neq B \cdot A$ בדרך

(3) $A + 0 = A$

(4) $A \cdot I = I \cdot A = A$

בדרך כלל אין עבור A אין מטריצה הופכית אלא אם כן הדטרמיננטה שלה שונה מאפס.

בהשוואה לעומת זאת לכל $x \neq 0$ $\Leftarrow$ קיים y כך ש: $yx = 1$ וזה לא נכון במטריצות. למטריצות למשל $\nexists A$ (לא קיים A) כך ש:

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} A = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

והביטוי $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}^{-1}$ חסר משמעות.

(5) $A \cdot (B + C) = AB + AC$

הגדרה:

חוג R הוא קבוצה עם שתי פעולות "חשבון" כפל + חיבור $\{R,+,\cdot\}$

כך שמתקיים:

① R כקבוצה הוא חבורה חילופית לגבי החיבור. (ה-$+$ הוא חילופי)

② הכפל אסוציאטיבי, כלומר $(a\cdot b)\cdot c = a\cdot(b\cdot c)$

③ $a\cdot(b+c) = ab + ac$ (דיסטריביוטיביות)

$(b+c)a = ba+ca$ (כיוון שהכפל לא קומוטטיבי צריך לכתוב את שני הצדדים)

הנה דוגמא טריויאלית:

ניקח חבורה חיבורית $(A,+,0)$ ונגדיר פעולת כפל בין אבריה $a\cdot b=0$

(0 קיים כי הוא איבר היחידה של החבורה החיבורית).

קל לראות כי ① ו-② מתקיימים.

ב-③ משתמשים ב-0. זוהי דוגמא שאינה מעניינת.

דוגמא מעניינת: אוסף המטריצות $M_{n\times n}(F)$ שהדטרמיננטה שלהן שונה מאפס.

זוהי חבורה אך 0 לא נמצאית שם ולכן זוהי חבורה ולא חוג.

דוגמא נוספת (חשובה): כל שדה הוא חוג.

כל שדה $(F,+,\cdot)$ הוא חוג המקיים שאוסף $F\setminus\{0\}$ הוא חבורה חילופית ביחס לכפל.

אך לא כל חוג הוא שדה. למשל חוג המטריצות אינו שדה כי לא לכל מטריצה יש הפכי.

הדוגמא הראשית לחוג: חוג השלמים: $(\mathbb{Z},+,\cdot,1,0)$ זהו חוג עם יחידה

לגבי הכפל. כלומר לכל איבר $a\cdot 1=a\cdot 1=a$. $(-1)^{-1}=(-1)$

דוגמא: $2\mathbb{Z}$ = המספרים הזוגיים.

כחבורה חיבורית $2\mathbb{Z}\cong\mathbb{Z}$

$1 \to 2$

$0 \to 0$

אך האם הם איזומורפיים כחוג? לא כי ל-$2\mathbb{Z}$ אין יחידה.

כלומר $2\mathbb{Z}$ לא איזומורפי ל-$\mathbb{Z}$ כחוג.

$3\mathbb{Z}$ הוא גם חוג.

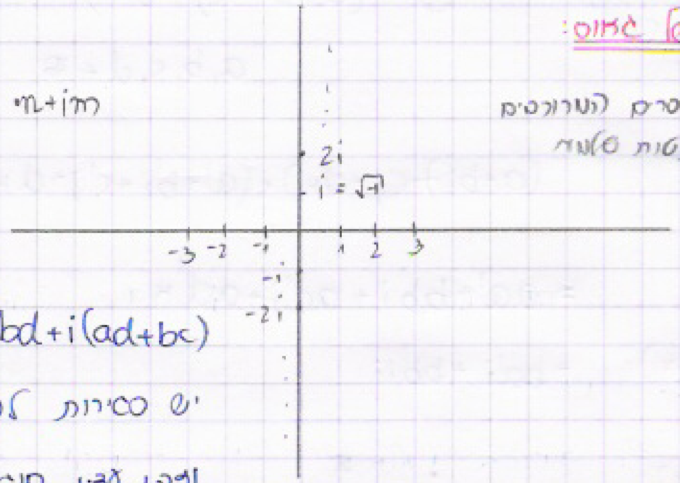
וכן $n\mathbb{Z}$ נראה חוג. לא ברור עדיין אם ל-n-ים שונים אלו חוגים איזומורפים.

חוג של גאוס:

אוסף המספרים המרוכבים
עם קואורדינטות שלמות

$\mathbb{Z}[i]$

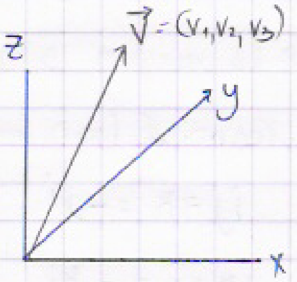
$\mathbb{C} \subseteq$ ($\mathbb{Z}$ שלמים ו' את i)



$$(a+ib)(c+id) = ac - bd + i(ad+bc)$$

יש סגירות לחיבור וגם לכפל

וזהו עדיין חוג.



האם אפשר להגדיר מבנה חוג על $\mathbb{R}^3$?

תשובה: ננסה מכפלה וקטורית: $\vec{V} \times \vec{W}$

$$\det \begin{pmatrix} e_1 & e_2 & e_3 \\ v_1 & v_2 & v_3 \\ w_1 & w_2 & w_3 \end{pmatrix} = V \times W$$

$\vec{V} = \sum e_i v_i$

$\vec{W} = \sum e_i w_i$

קל לראות שזה מקיים את הכללים

זה לא קומוטטיבי: $V \times W = -W \times V$ (בפיסיקה, שדה מגנטי לשמאל תלוי המכפלה הזו).

$V \times V = 0$ (כי אם שתי שורות שוות אז הדטרמיננטה היא 0)

נבדוק אסוציאטיביות: $U \times (V+W) = U \times V + U \times W$

$$(V \times W) \times U \neq V \times (W \times U)$$

האם אפשר להגדיר חוג על $\mathbb{R}^4$?

חשב על זה Hamilton :

ולא כמו במרוכבים

(המספרים הקווטרניונים) $Q = \{a+bi+cj+dk\}$ (הוא חשב על האיברים בצורה הזו)

$a,b,c,d \in \mathbb{R}$

$$(a+bi+cj+dk)\cdot(a'+b'i+c'j+d'k) =$$

איך מחשבים באמת? הוא רצה לשמור על הכלל הבסיסי, איך נגדיר את כללי הכפל.

$$= aa' + ab'i + ac'j + ad'k$$

$$+ ba'i + bb'ii$$

מסתמכים על רק ש:

$bi = ib$

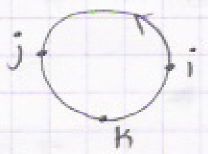
j

k

הוחלט כי: $i^2 = j^2 = k^2 = -1 \overset{?}{=} ijk$ (**)

$ij = (-j\cdot i) = -ji$ (*)

המספרים האלה אינם מתחלפים בינירם כמו מכפלה וקטורית.



הוא רשם את 3 הנקודות על המעגל

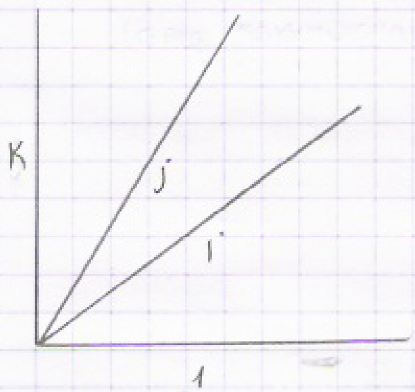
וקבע את הכפל לפי המעגל:

$$\left.\begin{aligned} ij &= k = -ji \\ jk &= i = -kj \\ k\cdot i &= j = -ik \end{aligned}\right\} \quad (***)$$

כאשר הוא קבע את הכפל לפי הכללים הנ"ל: הוא קיבל חוג (לא קומוטטיבי) בו הכפל משרה מבנה חבורה על ה $(Q-\{0\})$

קווטרניונים בלי האפס

מספר $\{\pm i, \pm j, \pm k, \pm 1\}$ זוהי חבורה לא קומוטטיבית עם 8 איברים



1-1-2007

דוגמא נוספת:

נסתכל על אוסף כל הפונקציות $C^n(\mathbb{R}^k) = \{f: \mathbb{R}^k \to \mathbb{R} \mid f$ רציפה / גזירה n פעמים$\}$

האם ניתן לחבר אותן? כן!

" " להכפיל אותן כן!

הופכי? לא קיים לגבי הכפל.

כלומר זהו חוג לגבי הכפל הרגיל כאשר:

[illegible] $\begin{cases} (f\cdot g)(x) = f(x)\cdot g(x) \\ (f+g)(x) = f(x)+g(x) \end{cases}$

ומתקיים $-(f)(x) = -(f(x))$

עבור כל תת-קבוצה X של $\mathbb{R}^n$ ($X \subseteq \mathbb{R}^n$ עבור כל מרחב טופולוגי)

$$C(X,\mathbb{R}) = \{f: X \to \mathbb{R} \mid f \text{ רציפה}\}$$

נדבר עכשיו על כמה תכונות של חוגים:

R = Ring (לפעמים מסומן גם A כמו בצרפתית Anneau)

כמה תכונות יסודיות של חוגים:

כמו בשדות, מתוך האקסיומות, ניתן להראות:

① $a\cdot 0 = 0\cdot a = 0$ לכל $a \in R$

כי: $a\cdot 0 = a(0+0) = a\cdot 0 + a\cdot 0 = 0$

② $(-a)\cdot b = a\cdot(-b) = -(ab)$

הגדרה: יחידה בחוג R הוא איבר e כך שלכל איבר אחר $e\cdot a = a$, $a\cdot e = a$

חוג עם איבר יחידה, נקרא חוג עם יחידה

הגדרה: מחלקי אפס: איבר $a \neq 0$ נקרא מחלק אפס אם קיים איבר $b \neq 0$ כך שמתקיים $ba = 0$ או מתקיים $ab = 0$

שימו לב: אם $ab = 0$ וקיים a^{-1} אז $0 = a^{-1}(ab) = (a^{-1}a)b = 1b = b$

דוגמא מסוג הפכי

דוגמא: מתוך $M_{2\times 2}(\mathbb{R})$

$$\underbrace{\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}}_{\text{שני איברים } \neq 0 \text{ שמכפלתם אפס.}} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

הגדרה: תחום שלמות (Integral Domain)

הוא חוג ללא מחלקי אפס, וכן חילופי לגבי הכפל.
(קומוטטיבי)

(הדוגמא הראשית לזה היא $\mathbb{Z}[i]$, המספרים השלמים של גאוס, $\mathbb{Z}$)

משפט: (לא נוכיח באופן מלא)

יהי R תחום שלמות סופי, (כלומר) עם מספר סופי של איברים.

אזי R הוא שדה, (כלומר קיים הפכי לכל וקיימת יחידה)

דוגמאות של המשפט:

תחילה דוגמא נגדית: $\mathbb{Z}/6\mathbb{Z}$

$\mathbb{Z}/n\mathbb{Z}$ הוא חוג ביחס לכפל והחיבור הרגילים, עם היחידה הרגילה

יש בו מחלקי אפס כי $2\cdot 3=0$ ולכן אכן לא שדה.

אך אם ניקח $\mathbb{Z}/11\mathbb{Z}$ הוא סופי, קומוטטיבי ולכן הוא שדה. דוגמא חיובית

מתווה של ההוכחה: (ניתן למצוא את ההוכחה בעמ' 167 ב- Herstein)

עלינו למצוא: ① איבר יחידה

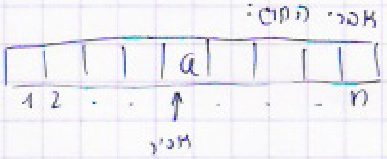
② איבר הפכי.

ניקח איבר a ונכפול בכל שאר האיברים x_i:

$$(ax_1, ax_2, \dots, ax_n)$$

שאלה: האם אחד מהמכפלות אלו הוא a כי אז ה-x_i שכפלנו בו הוא מועמד ליחידה.

טענה: אחת המכפלות $ax_j = a$: נניח בשלילה שלא קיים:



~~אז~~ אם לא קיימים $i \neq j$ כך ש: $ax_i = ax_j$

$\Longleftarrow$ $a(x_i - x_j) = 0$ אבל $i \neq j$ ולכן $x_i \neq x_j$

ואין מחלקי אפס $x_i = x_j$ וזו סתירה כי הנחנו שהם שונים

ולכן $ax_i = a$ ורק נותר להראות כי x_i הוא היחידה.

מאותו האופן נחפש את ההכ'.

העתקות של חוג'ים $A \longrightarrow B$

דוגמא: $\mathbb{Z} \xrightarrow{x2} \mathbb{Z}$

איך נגדיר את ההעתקה?

הגדרה: העתקה בין חוגים, הומומורפיזם של חוגים:

היא פונקציה $f: A \longrightarrow B$

$$\forall a \in A \quad a \longmapsto f(a) \in B$$

והיא צריכה לקיים את שני הכללים הבאים:

$$f(a \overset{A}{+} b) = f(a) \overset{B}{+} f(b)$$

$$f(a \underset{A}{\cdot} b) = f(a) \underset{B}{\cdot} f(b)$$

דוגמא נגדית: $f(x) = 2x$ $\quad f: \mathbb{Z} \longrightarrow \mathbb{Z}$

נבדוק אם מתקיים:

$2(x+y) \overset{?}{=} 2x+2y$ כן!

$2(x \cdot y) \overset{?}{=} 2x \cdot 2y$ לא!

ולכן זוהי אינה העתקה של חוג'ים.

שאלה לסיום:

תזכורת: אם $G \xrightarrow{f} H$ העתקה של חבורות אזי:

$$K = \mathrm{Ker} f = \{g \mid f(g) = e_H\}$$

$K \lhd G$ נורמלית.

שאלה: מה מתאים לחבורה נורמלית עבור חוג'ים?

$$K = \mathrm{Ker} f \subseteq A \xrightarrow{f} B$$

(ענה ע) רק בשעור הבא.

מבנים אלגבריים 1 - שיעור מס' 22

נשלים את מה שחסר לנו על חבורות ואז נעבור לחוגים:

משפט (שרייר): תהי G חבורה סופית. לכל שתי סדרות נורמליות יש עידונים שקולים.

מסקנה: (משפט ז'ורדן הולדר) אם G חבורה סופית אזי כל שתי סדרות ההרכב ללא חזרות הן שקולות.

הלמה של זסנהאוז: G חבורה

$A \triangleleft A^*$ $\quad B \triangleleft B^*$ תת-חבורות של G אזי:

$$A(B\cap A^*) \triangleleft A(B^*\cap A^*)$$

$$B(A\cap B^*) \triangleleft B(A^*\cap B^*)$$

ו-:

$$A(B^*\cap A^*)/A(A^*\cap B) \cong B(A^*\cap B^*)/B(A\cap B^*)$$

הוכחת משפט העידון של שרייר:

תהי G חבורה ו-:

$$G=G_0 \triangleright G_1 \triangleright \dots \triangleright G_n=\{e\}$$

$$G=H_0 \triangleright H_1 \triangleright \dots \triangleright H_m=\{e\}$$ שתי סדרות נורמליות.

נגדיר: $G_{ij}=G_{i+1}(G_i\cap H_j)$ $\quad (0\le i\le n-1\ ,\ 0\le j\le m)$

ועבור $(0\le i\le n\ ,\ 0\le j\le m-1)$ $\quad H_{ij}=H_{j+1}(H_j\cap G_i)$

נשים לב כי:

$$(*)\quad G_{ij}=G_{i+1}(G_i\cap H_j) \triangleright G_{i+1}(G_i\cap H_{j+1})=G_{i,j+1}$$

[כי $A=G_{i+1}\triangleleft G_i=A^*$ $\quad B=H_{i+1}\triangleleft H_i=B^*$
ומהלמה של זסנהאוז מתקבל $(*)$]

נשים לב כי אם

$$G_{i0}=G_{i+1}(G_i\cap \overset{G}{\overset{\shortparallel}{H_0}})=G_{i+1}\cdot G_i=G_i$$

$$G_{im}=G_{i+1}(G_i\cap \overset{\{e\}}{\overset{\shortparallel}{H_m}})=G_{i+1}$$

ונקבל כי $G_{im}=G_{i+1,0}$

המשך בעמוד הבא ←

נתבונן בסדרה: $G=G_{0,0} \triangleright G_{0,1} \triangleright G_{0,2} \triangleright \dots \triangleright G_{0m}=G_{1,0} \triangleright \dots \triangleright G_{1,1} \dots$

$\dots \triangleright \dots \triangleright G_{1m}=G_{2,0} \triangleright G_{2,1} \triangleright \dots \triangleright G_{n-1,m}=G_{n,0}=\{e\}$

ובסדרה $G=H_{0,0} \triangleright H_{1,0} \triangleright H_{2,0} \triangleright \dots \triangleright H_{n,0}=H_{0,1} \triangleright \dots \triangleright H_{1,1} \triangleright H_{2,1} \dots$

$\triangleright \dots \triangleright H_{n,1}=H_{0,2} \triangleright H_{1,2} \triangleright H_{2,2} \triangleright \dots \triangleright H_{n,m-1}=H_{0,m}=\{e\}$

והמעברים בסדרה המתחנה הם מהלמה של זסנהאוז עבור

$B^*=H_j \quad B=H_{j+1}$

$A^*=G_i \quad A=G_{i+1}$ ונקבל:

$$H_{ij}=H_{j+1}(H_j\cap G_i) \triangleright H_{j+1}(H_j \cap G_{i+1})=H_{i+1,j}$$

$$H_{0j}=H_{j+1}(H_j\cap \underset{\overset{\shortparallel}{G}}{G_0}) \triangleright H_{j+1}H_j=H_j$$

$$H_{nj}=H_{j+1}(H_j\cap \underset{\overset{\shortparallel}{\{e\}}}{G_n})=H_{j+1}$$

נתבונן בשתי הסדרות הנורמליות שקיבלנו, ונשים לב כי אורך כל אחת מהסדרות שקיבלנו הוא $n\cdot m+1$ ומהלמה של זסנהאוז נובע כי:

$$G_{ij}/G_{ij+1} \cong H_{ij}/H_{i+1j} \qquad 0\le j\le m-1 \quad 0\le i\le n-1$$

$\boxed{/}$

הוכחת משפט ז'ורדן הולדר:

נתבונן בשתי סדרות הרכב: (ללא חזרות)

$$(*) \quad G=G_0 \triangleright G_1 \triangleright \dots \triangleright G_n=\{e\}$$

$$(**) \quad G=H_0 \triangleright H_1 \triangleright \dots \triangleright H_m=\{e\}$$

לפי משפט העידון של שרייר יש להם עידונים שקולים:

$$G=\tilde{G}_0 \triangleright \tilde{G}_1 \triangleright \dots \triangleright \tilde{G}_k=\{e\} \quad ((*) \text{ עידון})$$

$$G=\tilde{H}_0 \triangleright \tilde{H}_1 \triangleright \dots \triangleright \tilde{H}_k=\{e\} \quad ((**) \text{ עידון})$$

וקיימת תמורה π על $\{0,1,\dots,k-1\}$ כך ש-

$$\tilde{G}_i/\tilde{G}_{i+1} \cong \tilde{H}_{\pi(i)}/\tilde{H}_{\pi(i)+1}$$

נשים לב כי בסדרה הנורמלית $G=\tilde{G}_0 \triangleright \tilde{G}_1 \triangleright \dots \triangleright \tilde{G}_k=\{e\}$

המנות המוספות הן בדיוק המנות שהופיעו בסדרת ההרכב $(*)$ וכן שאר $k-n$ המנות הן טריוויאליות.

מאותו הגיון בסדרה $G=\tilde{H}_0 \triangleright \tilde{H}_1 \triangleright \dots \triangleright \tilde{H}_k=\{e\}$ יש בדיוק $k-m$ מנות שאינן טריוויאליות

והן המנות, החבורות הפשוטות, המופיעות במנות מסדרה (**).

לכן היות והסדרות $G=\tilde{G}_0 \triangleright \dots \triangleright \tilde{G}_k=\{e\}$

ו- $G=\tilde{H}_0 \triangleright \dots \triangleright \tilde{H}_k=\{e\}$

שקולות נובע כי מס' הופעות הסדרה הטריוויאלית בכ"א הוא שווה

כלומר $k-n=k-m=r$

$$\Longrightarrow n=m$$

לכן ברור כי יש תמורה η של $\{0,1,\dots,n-1\}$

כך ש: $G_i/G_{i+1} \cong H_{\eta(i)}/H_{\eta(i)+1}$

$\boxed{}$

דוגמאות:

(א) נתבונן בחבורה ציקלית מסדר $2^2\cdot 3\cdot 5$

$$C_{60} \overset{C_2}{\triangleright} C_{30} \overset{C_2}{\triangleright} C_{15} \overset{C_3}{\triangleright} C_5 \overset{C_5}{\triangleright} \{e\}$$

$$C_{60} \overset{C_3}{\triangleright} C_{20} \overset{C_2}{\triangleright} C_{10} \overset{C_5}{\triangleright} C_2 \overset{C_2}{\triangleright} \{e\}$$

(ב) תרגיל: מצאו סדרות הרכב ל- S_4.

ונחזור לחומר של חוגים - המשך:

נזכור כי בחוגים לא דרשנו קיום איבר יחידה.

במקרים רבים מדברים על חוגים עם איבר יחידה.

"מסקנה": מתי מס' טבעי הוא סכום של שני ריבועים (טבעיים)?

נראה כי ראשוני $p\neq 2$ הוא סכום של שני ריבועים אם ורק אם $p\equiv 1 \mod 4$

הומומורפיזם של חוגים:

R,S חוגים. העתקה $\varphi:R\to S$ היא הומומורפיזם אם מתקיים:

לכל $a,b\in R$ $\quad \varphi(a+b)=\varphi(a)+\varphi(b)$

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

כאשר מדובר על חוגים עם איבר יחידה אזי דורשים גם כי $\varphi(1)=1_S$

דוגמא: $R=\mathbb{Z}$ $\quad S=\mathbb{Z}/n\mathbb{Z}$

$$\varphi:\mathbb{Z}\to\mathbb{Z}/n\mathbb{Z}$$

$$\varphi(k)=k+n\mathbb{Z}$$

דוגמא: $R=\mathbb{Z}$ $S=\mathbb{Z}$ חוגים ללא איבר יחידה.

$\varphi:\mathbb{Z}\to\mathbb{Z}$ $\varphi(x)=0$

דוגמא: $\{f:$ פונקציות רציפות מ-$[0,1]$ ל-$\mathbb{R}\}$ $C=[0,1]=\mathbb{R}$ חוג

ההומומורפיזם $\varphi(f)=f(\frac{1}{3})$

הגדרה: יהיו R,S חוגים $\varphi:R\to S$ הומומורפיזם

אזי: $I=\ker\varphi=\{a\in R|\varphi(a)=0\}$

אם $b,a\in I$ אזי $a+b\in I$

ואם $a\in I$! $x\in R$ אז $ax\in I$ וגם $xa\in I$

(מהגדרת הכפל בהומומורפיזם)

הגדרה: אידיאל בחוג R הוא תת-קבוצה I כך ש-I תת-חבורה ביחס לחיבור

ולכל $a\in I$ $x\in R$ $ax,xa\in I$ ומסמנים $I\lhd R$

דוגמאות: $R=\mathbb{Z}$

אידיאלים: $\{0\}$ בכל חוג ה-0 הוא אידיאל

$m\mathbb{Z}$ $m\in\mathbb{Z}$

$1\mathbb{Z}=\mathbb{Z}$

ואלו הן כל האפשרויות.

הגדרה: יהי R חוג ו- $I\lhd R$ אידיאל.

נתבונן ב- $R/I=\{a+I|a\in R\}$ ונגדיר עליה מבנה של חוג.

היא חבורה חיבורית כחבורת מנה של $(R,+,0)$ אז:

$(a+I)+(b+I)=(a+b)+I$

ונגדיר כפל: עבור $a,b\in R$ נגדיר

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

חוג זה נקרא חוג מנה

צריך להראות:

(א) מוגדר היטב

(ב) מקיים חוג

כלומר אם $a+I=a'+I$ ו- $b+I=b'+I$

אז צריך להוכיח כי: $ab+I=a'b'+I$.

8-1-2007

③

$a = a' + u \qquad u \in I$!

$b = b' + v \qquad v \in I$

$$ab + I = (a'+u)(b'+v) + I = a'b' + \underset{I}{\underset{\Uparrow}{a'v}} + \underset{I}{\underset{\Uparrow}{ub'}} + \underset{I}{\underset{\Uparrow}{uv}} + I = a'b' + I$$

[דוגמא: $R = \mathbb{Z}$ ו- $I = 2\mathbb{Z}$ $\qquad I \cdot I = I$

$(2\mathbb{Z})(2\mathbb{Z}) = (4\mathbb{Z}) < 2\mathbb{Z}$]

צריך לבדוק כי זה אכן חוג.

כלומר צריך לבדוק כי הכפל אסוציאטיבי ואת חוקי הפילוג. אבל זה נובע מיד מההגדרה ומכך כי R הוא חוג.

משפט: (תרגיל)

יהיו R,S חוגים ו- $\varphi: R \to S$ הומומורפיזם על (כלומר לכל $s \in S$ יש $a \in R$ כך ש $\varphi(a) = s$)

אזי S איזומורפי ל- R/I כאשר $I = \ker\varphi$

נאמר כי שני חוגים K,L הם איזומורפים אם יש הומומורפיזם חח"ע ועל $\varphi: K \to L$ כך שמתקיים $\varphi^{-1}: L \to K$ הומומורפיזם.

דוגמאות: חוג פולינומים:

$$\mathbb{Z}[x] = \{a_0 + a_1x + \dots + a_nx^n \mid n \geq 0 \quad a_i \in \mathbb{Z}\}$$

$$\mathbb{R}[x] = \{a_0 + a_1x + \dots + a_nx^n \mid n \geq 0 \quad a_i \in \mathbb{R}\}$$

חוגי מטריצות:

יהי $\mathbb{F}$ שדה אז אפשר להסתכל על $M_n(\mathbb{F}) = \{$מטריצות עם מקדמים ב-$\mathbb{F}\}$

הגדרה: יהי R חוג. איבר $0 \neq a \in R$ יקרא מחלק אפס אם קיים $0 \neq b \in R$ כך ש $ab = 0$ או $ba = 0$

דוגמא: בחוג $\mathbb{Z}$ אין מחלקי אפס.

בחוג מטריצות $M_2(\mathbb{Z})$ יש מחלקי אפס

בחוג $\mathbb{Z}[x]$ אין מחלקי אפס.

הגדרה: חוג קומוטטיבי ללא מחלקי אפס ייקרא **תחום שלמות**.

הגדרה: חוג בו כל האיברים השונים מאפס מהווים חבורה ביחס לכפל (ובפרט יש יחידה) ייקרא **חוג חילוק**.

משפט: תחום שלמות סופי הוא שדה

הוכחה: יהי $0\neq a\in R$ נתבונן ב-

$$aR=\{ax \mid x\in R\}$$

נגדיר העתקה $\varphi: R\longrightarrow aR$ והיא חח"ע

$$(x\longmapsto ax)$$

כי אם $ay=\varphi(y)=\varphi(x)=ax$

$$\Longrightarrow \underbrace{a(y-x)}_{\text{אין מחלקי אפס}} \Longrightarrow y=x$$

ו- $a\neq 0$

ולכן φ היא על $\Longleftarrow$ קיים $u_0\in R$ כך ש: $au_0=a$

יהי $b\in R$ אזי קיים $x\in R$ כך ש- $ax=b$ ואז u_0 הוא איבר היחידה

$$bu_0=axu_0=au_0x=ax=b$$

הערה! $|R|=|aR|$ נובע כי $u_0\in aR$ ולכן קיים הנ"ל.

הגדרה:
חוג

הומומורפיזם

R,S חוגים $\varphi: R \to S$ הוא הומומורפיזם
אם: $\varphi(ab)=\varphi(a)\varphi(b)$ $\forall a,b\in R$
$\varphi(a+b)=\varphi(a)+\varphi(b)$

$\ker\varphi = \{x\in R \mid \varphi(x)=0\}$

גרעין הומומורפיזם הוא אידיאל.
כלומר תת-קבוצה I רק ש:
- I תת-חבורה חיבורית של $(R,+,0)$
- לכל $x\in I$ ולכל $a\in R$ $ax\in I$

חוג R יקרא תחום שלמות אם הוא:
- קומוטטיבי
- אין מחלקי אפס כלומר אם $a,b\in R$ שונים מאפס אז $ab\neq 0$

משפט
אם R הוא תחום שלמות עם איבר יחידה אז:
R שדה $\iff$ האידיאלים היחידים ב-R הם $\{0\}$ ו-R

הוכחה:
$\Leftarrow$ נניח R שדה.
אם $I \lhd R$ אידיאל ו- $I\neq(0)$ אז יהי $0\neq a\in I$
היות ו-R שדה לכל $b\in R$ קיים $x\in R$ כך ש $ax=b$ (ניקח $x=a^{-1}b$)
ולכן גם $b\in I$ ו- $I=R$
$\Rightarrow$ צריך להראות קיום הפכי. יהי $0\neq a\in R$
נתבונן ב $aR=\{ax \mid x\in R\}$; נשים לב כי aR הוא אידיאל
ו- $0\neq a=a\cdot 1\in aR$ לכן $(0)\neq aR$ ולכן $aR=R$
ובפרט קיים $y\in R$ כך ש: $ay=1$ והראינו קיום איבר נגדי

∎

חוג מנה

אם R חוג. $I \triangleleft R$ אידיאל.

הגדרנו חוג מנה $R/I=\{a+I \mid a\in R\}$

$$\varphi : R \longrightarrow R/I$$ ההומומורפיזם הטבעי

$$a \longmapsto a+I$$

הערה:

יש התאמה חח"ע ועל בין קבוצת האידיאלים של R/I וקבוצת האידיאלים ב- R המכילים את I.

נסמן

$$A=\{J\triangleleft R/I \mid J \text{ אידיאל ב-} R/I\}$$

$$B=\{K\triangleleft R \mid K \text{ אידיאל ב-}R,\ I\subset K\}$$

נגדיר: $\alpha: A\longrightarrow B$ ע"י $\alpha(J)=\varphi^{-1}(J)$

ונגדיר $\beta: B\longrightarrow A$ ע"י $\beta(K)=\{a+I \mid a\in K\}=\varphi(K)$

נשים לב כי לכל אידיאל J ב- R/I $\alpha(J)$ מכיל את I

כי $0+I\in J$ איבר האפס ב R/I $\varphi^{-1}(0+I)=I$

$\alpha(J)$ הוא אידיאל כי:

אם $a,b\in\alpha(J)$ כלומר $\varphi(a)\in J$

$\varphi(b)\in J$

אזי $\varphi(a+b)=\underset{J}{\underset{\cap}{\varphi(a)}}+\underset{J}{\underset{\cap}{\varphi(b)}}\in J$

$\Longleftarrow$ $a+b\in\underset{\alpha(J)}{\underset{\shortparallel}{\varphi^{-1}(J)}}$

אם $a\in\alpha(J)$ ו $x\in R$ אזי:

$$\underset{J}{\varphi(a)}\,\varphi(x)\in J,\qquad \varphi(ax)=\varphi(a)\varphi(x)\in J$$

J אידיאל

ולכן $ax\in\varphi^{-1}(J)=\alpha(J)$

ולכן α העתקה מ- A ל- B

כעת נראה כי גם β העתקה מ- B ל- A.

נניח כי $I\subset K\lhd R$

נניח כי $u,v\in\varphi(K)$

אזי יש $a,b\in K$ כך ש $\varphi(a)=u$

$\varphi(b)=v$

לכן $u+v=\varphi(a)+\varphi(b)=\varphi(\underset{K}{a+b})\in\varphi(K)$

ואם $a\in\varphi(K)$

$y\in R/I$

אזי קיים $u\in K$ כך ש $a=\varphi(u)$

קיים $x\in R$ כך ש $y=\varphi(x)$

$$ya=\varphi(u)\varphi(x)=\varphi(\underset{K}{ux})\in\varphi(K)$$

ולכן $\beta: B\longrightarrow A$

נראה כעת כי $\alpha\circ\beta=Id_B$

$\beta\circ\alpha=Id_A$

נבדוק תכונות הוכחת ההערה:

יהי $J\lhd R/I$ נחשב את:

$$\beta(\alpha(J))=\beta(\{a\in R|\varphi(a)\in J\})=$$

$$=\varphi(\{a\in R|\varphi(a)\in J\})=\{\varphi(a)\,|\,{}^{a\in R}_{\varphi(a)\in J}\}\subset J$$

מאידך לכל $y\in J\subseteq R/I$ קיים $a\in R$ כך ש: $\varphi(a)=y$ ולכן

$$\beta(\alpha(J))\supseteq J$$

ולכן קיבלנו כי $\beta\circ\alpha = id_A$

עתה נתבונן ב: $\alpha\circ\beta$:

יהי $I \subset K \triangleleft R$

$$\alpha(\beta(K)) = \alpha(\varphi(K)) =$$

$$= \alpha(\{\varphi(x) \mid x\in K\}) = \varphi^{-1}(\{\varphi(x) \mid x\in K\}) =$$

$$= \{y\in R \mid \varphi(y) \in \{\varphi(x) \mid x\in K\}\} = L$$

נשים לב כי $K \subset L$

נניח כי $b\in L$ אזי קיים $x\in K$ רק ש: $\varphi(b)=\varphi(x)$

לכן קיים

$$0 = \varphi(b)-\varphi(x) = \varphi(b-x)$$

$$\Longleftarrow \quad b-x\in I$$

כלומר $b\in x+I$

כלומר קיים $a\in I$ רק ש $b = x+a \in K$

כי $x\in K$ $a\in I\subset K$

ולכן $L\subset K$ וקיבלנו $\alpha(\beta(K))=K$ כלומר $\alpha\circ\beta = Id_B$

$\boxtimes$

מסקנה:

אם R חוג קומוטטיבי עם איבר יחידה ! $M\triangleleft R$ אידאל אזי R/M שדה

אם ורק אם M אידאל מקסימלי

הגדרה: אידאל M בחוג R יקרא אידאל מקסימלי אם:

(א) $M\neq R$

(ב) כל אידאל $I\triangleleft R$ המכיל את M הוא או M או R.

10-1-2007

③

ננסח מחדש את המשפט שהוכחנו קודם כי פרשנו קודם יותר מדי:

R חוג קומוטטיבי עם יחידה. ונניח כי ב-R יש רק שני אידיאלים (0) ו-R

אזי R שדה.

הוכחה:

$0\neq a\in R$

aR אידיאל (נובע מקומוטטיביות)

$a\in aR$ כי $1\in R$ $\qquad a=a\cdot 1$

אז aR אידיאל $\neq 0$ ולכן $1\in aR$ ולכן קיים הפכי.

בניסוח הקודם פרשנו תחום שלמות ובמקום זה השתמשנו בתכונה זו.

הסבר: במשפט שהוכחנו בתחילת השיעור צ"ל להניח כי R חוג קומוטטיבי עם איבר יחידה.

המשפט אומר: אם R חוג קומוטטיבי עם איבר יחידה אזי:

R שדה $\Longleftrightarrow$ יש ב-R בדיוק שני אידיאלים (0) ו-R

משפט:

יהי R חוג קומוטטיבי עם איבר יחידה.

אזי יש ב-R אידיאל מקסימלי

הוכחה:

נתבונן באוסף $\mathcal{M}$ של כל האידיאלים ב-R השונים מ-R.

$\mathcal{M}$ קבוצה סדורה חלקית ביחס להכלה.

צריך להראות כי יש ב-$\mathcal{M}$ איבר מקסימלי.

הלמה של צורן אומרת שמספיק להראות כי לכל שרשרת C ב-$\mathcal{M}$ יש איבר $I\in\mathcal{M}$ (חסם מל') מעל C.

תהי $C\subseteq\mathcal{M}$ (מוכלת ב-$\mathcal{M}$) שרשרת כלומר קבוצה כלשהי של אידיאלים כך שלכל $K,L\in C$

או $K\subseteq L$ או $L\subseteq K$

בהינתן שרשרת C נגדיר $I=\bigcup_{K\in C}K$ (איחוד כל האידיאלים)

ברור כי $I\supseteq K$ לכל $K\in C$.

נותר לבדוק ① I אידיאל (ההוכחה בתרגול)

② $I\neq R$ (כי $1\notin I$ כי אם $1\in I$ אזי קיים $K\in C$ כך ש: $1\in K$

$\Longleftarrow K=R$ וסתירה.)

I אידיאל כי אם $a\in I$, $x\in R$ אז קיים $K\in C$ כך ש:

$a\in K \Leftarrow$ $xa\in K$ (כי K אידיאל) ולכן $xa\in I$ (אם שמאליות לצד)

אם $a,b\in I \Leftarrow$ קיים $K\in C$, $a\in K$

$L\in C$, $b\in L$

בה"כ $K\subset L$ ולכן $a\in K\subset L$, $a+b\in L$

$\Leftarrow a+b\in I$

15-1-2007

מבנים אלגבריים - שעור מס' 24

נוכיח שוב משפט שניסחנו בפעם שעברה:

משפט: יהי R חוג קומוטטיבי עם יחידה, אזי R שדה אם ורק אם (האידיאלים) היחידים של R הם R ו-(0) (אין צורך בתחום שלמות כי בהוכחה רק מספיק קומוט)

מסקנה: יהי R חוג קומוטטיבי עם יחידה אזי אידיאל $M \triangleleft R$ הוא מקסימלי אם ורק אם R/M שדה.

יהי F שדה, אזי כל תת חוג של F אינו מכיל מחלקי אפס (השדה כמובן אין מחלקי אפס)

משפט: יהי R תחום שלמות, (חוג קומוטטיבי ללא מחלקי אפס) אז ניתן לשכנו בשדה. (לא דרשנו חוג עם יחידה)

(הרעיון: לחקות את בניית $\mathbb{Q}$ מ $\mathbb{Z}$)

הוכחה:

נתבונן בקבוצה $\Omega = R\times R^* = \left\{(a,b) \,\middle|\, \begin{matrix} a,b\in R \\ b\neq 0\end{matrix}\right\}$

נגדיר יחס שקילות על Ω. נאמר $(a,b)\sim(a',b')$ (כאשר $a,b,a',b'\in R$, $b,b'\neq 0$)

אם $ab'=a'b$ $\left(\frac{a}{b}=\frac{a'}{b'}\right)$

נבדוק שזהו אכן יחס שקילות:

רפלקסיביות: $(a,b)\sim(a,b)$ - זה מיידי.

סימטריות: $(a,b)\sim(a',b') \Longrightarrow (a',b')\sim(a,b)$ זה גם מיידי כי החוג קומוטטיבי.

טרנזיטיביות: $(a,b)\sim(a',b')$

$(a',b')\sim(a'',b'')$

אזי $(a,b)\sim(a'',b'')$ (פשוט צריך להוכיח)

כי: $ab'=a'b$ ①

$a'b''=a''b'$ ②

$①,② \Longrightarrow ab'a'b''=a'ba''b'$

$\Leftarrow$

$$ab''=a''b$$

כי: $0=ab''a'b'-a''ba'b'=$

$=(ab''-a''b)a'b'$

מכיוון ש $b'\neq 0$ נקבל

$$0=(ab''-a''b)a'$$

אם $a'\neq 0$

אזי נקבל כי $a=a''=0$ ושוב $ab''=a''b=0$

כי $a=0 \underset{b'\neq 0}{\Leftarrow} ab'=a'b=0b=0$

$a''=0 \underset{b'\neq 0}{\Leftarrow} a''b'=a'b''=0b'=0$

נסמן ב F את אוסף מחלקות השקילות ב Ω ביחס ל $\sim$

$$F=\Omega/\sim=\{\underset{\frac{a}{b}}{[a,b]} \mid {a,b\in R \atop b\neq 0}\}$$

$$[a,b]=\{(x,y)\mid ay=xb,\ x,y\in R,\ y\neq 0\}$$

נראה כעת כי ניתן להגדיר על F מבנה של שדה וכן כי ניתן לשכן את R ב-F.

כי זה כמו: $\frac{a}{b}+\frac{c}{d}=\frac{ad+bc}{bd}$

כדי שזה יהיה שדה, נדרש להגדיר:

חיבור: $[a,b]+[c,d]=[ad+bc,bd]$

כפל: $\underset{\frac{a}{b}\cdot\frac{c}{d}=\frac{ac}{bd}}{[a,b]\cdot[c,d]}=[ac,bd]$

איבר אפס: $[0,b]$ $\quad 0\neq b\in R$ כלשהו

איבר יחידה: $[b,b]$ $\quad 0\neq b\in R$ כלשהו

צריך לבדוק שכל ההגדרות הללו תקינות:

-אבל יעין בהגדרת חיבור וכפל הוא איבר ב-F

כלומר $bd\neq 0$ ומתקיים כי R תחום שלמות $b,d\neq 0$

צריך לבדוק, אי-תלות בנציגים כלומר אם:

לגבי חיבור אם $[a',b']=[a,b]$ ו

$[c',d']=[c,d]$

אזי צריך להראות:

$[a'd'+b'c',\ b'd']=[ad+bc,\ bd]$

(ואת אותו הדבר לעשות לגבי כפל)

<u>נבדוק:</u>

נתון: $0\neq b,b',d,d'$

$a'b=ab'$

$c'd=cd'$

צריך להראות:

$$(a'd'+b'c')bd=(ad+bc)b'd'$$

$$a'd'bd+b'c'bd\stackrel{?}{=}adb'd'+bcb'd'$$

$$\|$$

$$a'bdd'=ab'dd'$$

וכן לגבי שני המחוברים הנוספים.

ולכן מתקיים שוויון.

באופן דומה בודקים לגבי הגדרת הכפל.

נשים לב כי לכל $[c,d]\in F$

$$[0,b]+[c,d]=[0d+bc,\ bd]=[bc,\ bd]=[c,d]$$

כי $(bc,bd)\sim(c,d)$

$$(bc)d=(bd)c$$

ובבדיקה פורמאלית: $[b,b'][c,d]=$

$=[bc][bd]=[c,d]$

כלומר $[b,b]\in F$ איבר היחידה

כעת צריך לבדוק שאכן: - $(F,+,0)$ חבורה חיבורית קומוטטיבית,

- אסוציאטיביות (הכל)

- חוק פילוג

- הפכי לכל.

נבדוק, לשם דוגמא, קיום הופכי לכל:

נניח $\underline{0} \neq [a,b] \in F$ $\Longleftarrow$ $a \neq 0$ ונתבונן ב- $[b,a] \in F$

ולכן $[b,a][a,b] = [ba, ab] = \underline{1}$

(שאר הדברים תרגיל)

נותר להראות שיכון של R ב F. נבחר $0 \neq b_0 \in R$

ונגדיר $\varphi: R \longrightarrow F$ באופן הבא: $\varphi(a) = [ab_0, b_0]$

צריך לבדוק כי φ היא הומומורפיזם של חוגים ו- φ חח"ע

אז נבדוק הומו' כלומר: $\forall a,b \in R \ \varphi(a+b) = \varphi(a) + \varphi(b)$

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

ואכן:

$$\varphi(a) + \varphi(b) = [ab_0, b_0] + [bb_0, b_0] =$$

$$= [ab_0b_0 + bb_0b_0, b_0b_0] = [(a+b)b_0, b_0]$$

כי: $(ab_0b_0 + bb_0b_0)b_0 = (a+b)b_0(b_0b_0)$

(והכל באופן דומה)

<u>חח"ע</u>: נניח כי $a, a' \in R$ ו- $\varphi(a) = \varphi(a')$

אזי: $[ab_0, b_0] = [a'b_0, b_0]$

כלומר: $ab_0b_0 = a'b_0b_0$

היות ו- $b_0 \neq 0$ אז $b_0b_0 \neq 0$

ולכן היות ו- R תחום שלמות נקבל כי $a = a'$ כנדרש

$\square$

הערה: השדה F שבנינו, נקרא שדה השברים של R.

דוגמא:

$\mathbb{R}$ שדה הממשיים.

$\mathbb{R}[x]$ חוג הפולינומים עם מקדמים ממשיים.

זהו חוג קומוטטיבי ללא מחלק אפס וניתן לבנות השדה השברים שלו

שסימון: $\mathbb{R}(x)=\left\{\frac{p(x)}{q(x)} \;\middle|\; \begin{matrix} p(x),q(x)\in\mathbb{R}[x] \\ q(x)\neq 0\end{matrix}\right\}$

הגדרה: חוג אוקלידי: R הוא חוג אוקלידי אם הוא

תחום שלמות עם פונקציה: $d:R\longrightarrow \mathbb{Z}^+=\{n\in\mathbb{Z}\mid n\geq 0\}$

כך שמתקיים:

(א) לכל $a,b\in R$ $\quad d(ab)\geq d(a)$

(ב) לכל $a,b\in R,\ b\neq 0$ קיימים $t,r\in R$ כך ש:

$a=tb+r$

או $r=0$ או $d(r)<d(b)$

דוגמאות:

(1) $\mathbb{Z}$

ונגדיר: $d(n)=|n|$

כי נשים לב ש: (א) $|m\cdot n| = |m||n|\geq |m|$ $\quad \mathbb{Z}\ni m,n\neq 0$

$n\neq 0 \Longrightarrow |n|\geq 1$

(2) חלוקה עם שארית

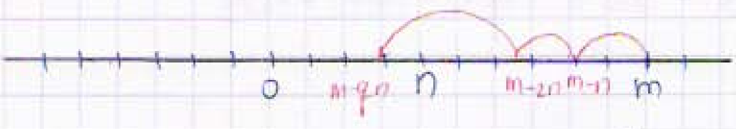
נראה באמת בעזרה גאומטרית:

הערה (לבית): ניתן להוכיח

במקרה זה אפילו: או $r=0$

או $|r|\leq \frac{|n|}{2}$

$\mathbb{Z}$



$\mathbb{Z}\ni m,n\neq 0$

$m=qn+r$

או $r=0$ $\quad |r|<|n|$

דוגמא ב:

יהי F שדה

$R=F[x]$ חוג הפולינומים מעל F

$$F[x]=\{a_0+a_1x+\dots+a_nx^n \mid \mathbb{Z}\ni n\geq 0,\ a_i\in F,\ 0\le i\le n\}$$

החזקה הגבוהה ביותר שמופיעה עם מקדם $\neq$ מאפס.

$$d(a_0+a_1x+\dots+a_nx^n)=\max\{0\le m\le n \mid a_m\neq 0\}$$

פה: הקבוצה שמימינה ריקה

כי מניחים $0\neq a_0+a_1x+\dots+a_nx^n$

צריך לבדוק כי זהו חוג אוקלידי:

ראשית: $F[x]$ הוא תחום שלמות.

דבר שני: לכל $F[x]\ni p(x)\neq 0$

$$0\le d(p(x))\in\mathbb{Z}$$

כמו כן: יהיו $p(x),q(x)\in F[x]$ ונניח כי $q(x)\neq 0$

אז טענה:

קיימים $q(x),r(x)\in F[x]$

כך ש: $p(x)=f(x)q(x)+r(x)$

או $r(x)=0$ או $d(r(x))<d(q(x))$

הוכחה: חילוק פולינומים.

אם $0=p(x) \Longrightarrow 0=0\cdot q(x)+0$ וסיימנו.

אם $d(q(x))>d(p(x))$ אז: $p(x)=0\cdot q(x)+p(x)$ וסיימנו

אחרת: $q(x)=a_nx^n+\dots+a_0$

$p(x)=b_mx^m+\dots+b_0$

כאשר $a_n,b_m\neq 0$ $m\ge n$

$$p(x)-\frac{b_m}{a_n}x^{m-n}q(x)=h(x)\in F[x]$$

אז $h(x)=0$ ואז סיימנו.

כי $p(x)=\frac{b_m}{a_n}x^{m-n}q(x)+0$

אז $p(x)=\frac{b_m}{b_n}x^{m-n}q(x)+h(x)$

כאשר $d(p(x))>d(h(x))$

ולאפשר להנחת האינדוקציה, כי קיימים פולינומים $g_1(x),g_2(x)\in F[x]$

כך ש:

$$h(x)=g_1(x)q(x)+g_2(x)$$

$$0=g_2(x) \quad \text{או} \quad d(g_2(x))<d(x)$$

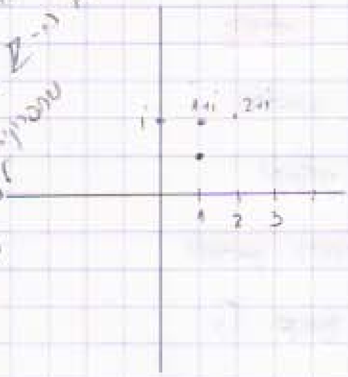
ונקבל

$$p(x)=\left(\frac{b_m}{a_n}x^{m-n}+g_1(x)\right)q(x)+g_2(x)$$

כנדרש

$\Longleftarrow$ $F[x]$ חוג אוקלידי.

חוגים אוקלידיים מתנהגים כמו $\mathbb{Z}$ (בשל ה- $\mathbb{Z}$ מוכללים ... של ראשוני)



דוגמא 3: $\{m+ni \mid m,n\in\mathbb{Z}\}=\mathbb{Z}[i]$ חוג השלמים של גאוס

טענה: $\mathbb{Z}[i]$ הוא חוג אוקלידי: (לחשוב כתרגיל)

דוגמא 4: $\mathbb{Z}[\sqrt{-5}]=\{m+n\sqrt{-5} \mid m,n\in\mathbb{Z}\}$ זהו גם חוג

שאינו אוקלידי (הוכחת תרגום שלמות)

מתקיים כאן: $6=2\cdot3=(1+\sqrt{-5})(1-\sqrt{-5})$

משפט:

יהי R חוג אוקלידי אזי כל אידיאל ב- R הוא ראשי כלומר הוא

מהצורה aR כאשר $a\in R$

הגדרה: R חוג קומוטטיבי. אידיאל ראשי הוא אידיאל מהצורה aR.

הוכחה: יהי R חוג אוקלידי

יהי $I\lhd R$ אידיאל

אם $I=(0)$ סיימנו כי $0=0\cdot R$.

אחרת, יהי $a\in I$ איבר כך ש: $d(a)\le d(b)$ $\forall b\in I$, $b\neq0$

נתבונן ב: $\{d(x) \mid 0\neq x\in I\}\subseteq\mathbb{Z}^+$

יש לה איבר מינימלי k ויהי $0\neq a\in I$ כך ש: $d(a)=k$

(נותר לנו להראות שכל איבר ב-I היא מהצורה aR)

יהי $x\in I$ אז קיימים $r,q\in R$ כך ש: $x=qa+r$

ואז $r=0$ או $d(x)>d(r)$

היות ו-I אידיאל נובע $r=\underset{I}{x}-\underset{I}{\underbrace{q\,a}}\in I$

ולכן לא יתכן $r\neq 0$ כי

$d(b)\geq d(a)$ לכל $b\in I$ ונובע $r=0$.

כלומר $x=q\cdot a\in aR$ אז קיבלנו $I\subset aR$

מאידך היות $a\in R$! $aR\subset I$

$\Downarrow$

$I=aR$

■

מסקנה: בחוג אוקלידי יש יחידה.

הוכחה:

נתבונן ב R כאידיאל ב-R ולכן $a\in R=aR$

וקיבלנו קיום $u\in R$ כך ש: $a=au$

ומכאן נובע כי u איבר היחידה.

כל $b\in R$ היא מהצורה $b=ax$ $x\in R$

$bu=axu=aux=ax=b$

■

הגדרה: תחום שלמות עם יחידה בו כל אידיאל הוא מהצורה aR נקרא חוג ראשי. כל חוג אוקלידי הוא חוג ראשי.

17-1-2007

מבנים אלגבריים - שמור עמ' 25

תזכורת:

חוג אוקלידי:

B תחום שלמות $d: R\setminus\{0\} \longrightarrow \mathbb{Z}^+$

- לכל $a,b \in R\setminus\{0\}$ $d(ab) \geq d(a)$

- לכל $a,b \in B$ $b \neq 0$

קיימים $t,r \in B$ כך ש: $a=bt+r$

או $r=0$ או $d(r)<d(b)$

הגדרה:

B חוג קומוטטיבי (עם יחידה).

אידיאל ראשי הוא אידיאל מהצורה aR

- בתחום אוקלידי כל אידיאל הוא מהצורה aR

- בתחום אוקלידי יש יחידה

חוג ראשי:

חוג קומוטטיבי עם יחידה, תחום שלמות בו כל אידיאל הוא ראשי.

הגדרה: B חוג קומוטטיבי.

$a,b \in B$ נאמר כי a מחלק את b $a|b$ אם קיים $c \in B$ כך ש: $ac=b$

הגדרה: מחלק משותף מירבי:

$a,b \in R$ איבר d יקרא מחלק משותף מירבי שלהם. $d=(a,b)$

אם: - $d|a$ וגם $d|b$

- אם $c \in R$: $c|a$: $c|b$ אזי $c|d$

טענה: יהי R חוג אוקלידי, אזי לכל שני איברים $a,b \in R$ יש מחלק משותף מירבי
יתר על כן קיימים $\lambda,\mu \in R$ כך ש: $d=\lambda a+\mu b$

הוכחה: נתבונן באידיאל $aR+bR = \{ax+by \mid x,y\in R\}$
היות ו-R חוג אוקלידי, R הוא גם חוג ראשי ולכן קיים $d\in R$
כך ש: $dR+bR=dR$.
היות ו- $1\in R$ נקבל $b,a\in aR+bR=dR$
$\Leftarrow$ d מחלק את a וגם את b וקיים $d=a\lambda+b\mu$.
נניח כי $c|a$ ו- $c|b$ אזי $c|a\lambda+b\mu=d$.

$\boxtimes$

נשים לב כי כבר עבור $\mathbb{Z}$ מחלק משותף מירבי אינו יחיד:
2 ו- -2 הם מחלקים משותפים מירביים של $4,6$.

הגדרה: יהי R חוג קומוטטיבי עם איבר יחידה.
איבר $a\in R$ יקרא יחידה (unit) אם קיים $b\in R$ כך ש $ab=1$.

למה: יהי R תחום שלמות עם יחידה, $a,b\in R$ $a|b$ וגם $b|a$
$\Leftarrow$ קיימת יחידה $u\in R$ כך ש: $a=bu$

הוכחה: $b|a \Leftarrow$ קיים $u\in R$ כך ש: $a=bu$
$a|b \Leftarrow$ קיים $v\in R$ כך ש: $b=av$
$\Leftarrow$ $a=bu=a(vu) \Leftarrow vu=1$ אם $a\neq 0$

כי:
אם $a\neq 0$ $a=a(vu)$
$\Longleftrightarrow a-a(vu)=0$
$a(1-vu)=0$
$\Longrightarrow 1-vu=0$ כי $a\neq 0$
$\Longrightarrow vu=1 \Longrightarrow$ u יחידה.

אם $a=0$ אזי גם $b=0$ (כי R תחום שלמות) וניקח $u=1$

$\boxtimes$

למה: יהי R חוג אוקלידי ויהי $b\in R\setminus\{0\}$ איבר שאינו יחידה

אזי לכל $a\in R\setminus\{0\}$ $d(ab)>d(a)$

הוכחה: נתבונן ב- $R\triangleright aR$.

$ab\in aR$.

נשים לב כי לכל $x\in aR$ $d(x)\geq d(a)$ ובפרט $d(ab)\geq d(a)$

נזכור כי הוכחנו שאם I אידיאל בחוג אוקלידי $I\neq(0)$!

אז $I=cR$ לכל איבר $c\in I$ כך ש $d(x)\geq d(c)$ לכל $x\in I$

לכן אם $d(ab)$ אינו גדול ממש מ $d(a)$ אזי בהכרח $d(ab)=d(a)$

ולכן $d(x)\geq d(ab)$ לכל $x\in aR$ ולכן $aR=abR$

$\Leftarrow$ קיים $y\in R$ כך ש $a\in aR$

מקיים $a=aby$

$a\neq 0 \Rightarrow by=1 \Rightarrow b$ יחידה. ∎

הגדרה: יהי R חוג אוקלידי.

איבר $a\in R$ יקרא אי-פריק אם לא ניתן להציג את a כמכפלת שני איברים שאינם הפיכים. כלומר אם $a=bc \Rightarrow$ אז b או c הפיכים, כלומר יחידות.

הגדרה: יהי R חוג קומוטטיבי עם יחידה.

אזי $a\in R$ יקרא ראשוני אם האידיאל aR הוא אידיאל ראשוני.

אידיאל $I\triangleleft R$ בחוג קומוטטיבי עם יחידה יקרא ראשוני אם לכל $b,c\in R$ אם $b\cdot c\in I$ אזי $b\in I$ או $c\in I$.

דוגמאות:

- $R=\mathbb{Z}$, $I=3\mathbb{Z}$. אידיאל ראשוני.
- $R=\mathbb{Z}$, $I=6\mathbb{Z}$ אז $2\cdot 3\in 6\mathbb{Z}$ אבל $2,3\notin 6\mathbb{Z}$
- נתבונן בחוג עם מחלקי אפס אזי אידיאל האפס (0) אינו ראשוני.

יהי $a\in R$ ראשוני אז נניח $a|bc$ $\Longleftrightarrow$ $bc\in aR$

$\Downarrow$

$b\in aR$ או $c\in aR$

$\Downarrow$ (מראשוניות האידאל aR)

$a|b$ או $a|c$

הערה:

$\mathbb{Z}[x]$ אינו חוג אוקלידי. ויותר מזה $\mathbb{Z}[x]$ אינו חוג ראשי.

טענה: יהי R חוג אוקלידי! $0\neq a\in R$ אזי a ראשוני $\Longleftrightarrow$ a אי-פריק

טענה: יהי R תחום שלמות עם יחידה. $0\neq a\in R$ אזי a ראשוני $\Longrightarrow$ a אי-פריק.

נוכיח את הטענות בשעור הבא

22-1-2007 ①

מבנים אלגבריים - שעור מס' 26

נראה היום שניתן להראות מה טבעי כסכום של שני ריבועים

אמרנו בשיעור הקודם כי R חוג קומוטטיבי, $a\in R$ ראשוני

אם לכל $b,c\in R$ אם $a|bc$ אזי $a|b$ או $a|c$

כלומר אם האידיאל $I=aR$ הוא אידיאל ראשוני.

$I\triangleleft R$ ראשוני $\Longleftrightarrow$ $bc\in I \Rightarrow b\in I$ או $c\in I$.

כמו כן אמרנו כי:

R חוג אוקלידי $0\neq a\in R$ לא הפיך יקרא אי-פריק אם לא ניתן לרשום כמכפלה

$a=bc$ כאשר אף אחד מבין b ו c אינו הפיך.

למה שניסחנו פעם קודמת

למה: יהי R חוג אוקלידי עם יחידה $a\neq 0$ אזי a ראשוני $\Rightarrow$ a אי-פריק.

הוכחה:

נניח a ראשוני ונניח כי $a=bc$ $\Rightarrow$ $a|bc$ $\Rightarrow$ היות ו a ראשוני

$a|b$ או $a|c$ נניח למשל $a|b$ כלומר קיים $x\in R$ כך ש: $b=ax$

ולכן $a=bc=axc$ ובמילים אחרות $0=a-axc=a(1-xc)$

$\Rightarrow$ $1-xc=0$ (כי הנחנו $a\neq 0$)

$\Rightarrow$ $xc=1$

$\Rightarrow$ כלומר c הפיך (מטרתנו בעצם היא להראות שאחד מ b ו c הפיכים)

∎

משפט: יהי R חוג אוקלידי ויהי $0\neq a\in R$

אזי או a הפיך או a ניתן להצגה כמכפלה סופית של איברים אי-פריקים.

$$a=\pi_1\pi_2\cdots\pi_m$$

כאשר $0\neq\pi_i\in R$ אי-פריק $\forall\, 1\leq i\leq m$

הוכחה: יהי $0\neq a\in R$.

אזי אם a הפיך סיימנו. אם a אי פריק גם סיימנו.

נניח באינדוקציה כי הטענה נכונה ומתקיימת עבור כל איבר $0\neq x\in R$ לא הפיך

כך ש: $d(x)<d(a)$

היות ! $a\neq0$ אינו הפיך ואינו אי-פריק נובע כי קיימים $b,c\in R$

לא הפיכים כך ש: $a=b\cdot c$.

נזכור כי הראינו אם $0\neq x\in R$ לא הפיך ! $0\neq y\in R$ אזי $d(xy)>d(y)$

$\Leftarrow$ b לא הפיך (לא יחידה) $\Leftarrow$ $d(c)<d(a)$

c לא הפיך $\Leftarrow$ $d(b)<d(a)$

מהנחת האינדוקציה ניתן להציג את b ! c כמכפלות סופיות של אי-פריקים.

כלומר קיימים $n\in\mathbb{N}$ $\beta_1,\dots,\beta_n\in R$ אי-פריקים $b=\beta_1\cdot\ldots\cdot\beta_n$

! $\gamma_1,\dots,\gamma_k\in R$ אי-פריקים $c=\gamma_1\cdot\ldots\cdot\gamma_k$

ולכן $a=b\cdot c=\beta_1\cdot\ldots\cdot\beta_n\gamma_1\cdot\ldots\cdot\gamma_k$ מכפלה של אי-פריקים.

$\blacksquare$

או $d(a)=\min\{d(x)|x\in R\}$

נשים לב כי אם $0\neq a\in R$! $d(a)=0$ אז או a הפיך או a אי-פריק

אחרת $a=b\cdot c$ כאשר b,c אינם הפיכים

וזה אומר $0=d(a)=d(b\cdot c)>\underbrace{d(c)}_{\in\mathbb{N}}$ וזו סתירה.

כי b לא הפיך

(לא יתכן טבעי קטן מ-0)

תזכורת למה זה חוג אוקלידי:

הגדרנו:

R חוג אוקלידי אם קיימת פונקציה $d:R\setminus\{0\}\longrightarrow\mathbb{N}$ כך ש: ① $d(ab)>d(a)$

② לכל $a,b\in R\setminus\{0\}$

קיימים $t,r\in R$ כך ש: $a=bt+r$

או $r=0$ או $d(r)<d(b)$

נשלים עכשיו את הכיוון השני של השקילות בין אי-פריקות לראשוניות:

משפט: יהי R חוג אוקלידי. $R\ni a\neq0$ a ראשוני $\Longleftrightarrow$ a אי-פריק

הוכחה: $\Leftarrow$ ראינו בתרגול השבוע.

עבור הכיוון השני נוכיח למה:

למה: יהי R חוג אוקלידי ונניח $a|bc$ ($a,b,c\in R\setminus\{0\}$)

נניח $a|bc$ ונניח a זר ל b כלומר $aR+bR=R$ $(a,b)=1$

אזי $a|c$

22-1-2007 ②

הוכחה: נתון $aR+bR=R$

$\Leftarrow$ קיימים $\lambda,\mu\in R$

כך ש: $\lambda a+\mu b=1$

נכפול ב- c ונקבל $\lambda ac+\mu bc=c$

$$a\,|\,\lambda ac+\mu bc=c \quad \Leftarrow \quad \begin{matrix} a\,|\,\lambda ac \\ a\,|\,\mu bc \end{matrix}$$

הוכחת המשפט:

נניח $0\neq a\in R$ אי-פריק ונניח כי $b,c\in R$ $\neq 0$ כך ש: $a|bc$

צריך להראות $a|b$ או $a|c$.

הערה: ניתן להניח כי $b,c\neq 0$

נניח $a\nmid b$

נתבונן באידאל $aR+bR=J$

היות ו- R תחום אוקלידי קיים $\gamma\in R$ כך ש: $aR+bR=\gamma R$

כלומר $\gamma|a$ ו- $\gamma|b$.

אם γ הפיך אז $\gamma R=R$ כלומר a ו- b זרים ולכן לפי הטענה

נובע כי $a|c$ וסיימנו.

נניח בשלילה כי γ אינו-הפיך. נתון כי $\gamma|a$ כלומר קיים $x_0\in R$

כך ש: $a=\gamma x_0$ והנחנו כי a אי-פריק.

$\Leftarrow$ x_0 הפיך. (נשים לב כי $a=\gamma x_0$ $\Leftarrow$ $\gamma=ax_0^{-1}$

ולכן היות ו- γ מחלק את b נובע כי גם a מחלק את b

כי

$\exists y\in R$ ו- $b=\gamma y=a(x_0^{-1}y)$ וסיימנו.

משפט: יהי R חוג אוקלידי.

כל איבר $0\neq a\in R$ שאינו הפיך, ניתן לפרק כמכפלת ראשוניים

ופירוק זה הוא יחיד עד כדי סדר והפיכים כלומר אם $a=\pi_1\cdot\ldots\cdot\pi_n$

$n\in\mathbb{N}$ π_i ראשוניים

דוגמה. $15=3\cdot5=-3\cdot-5=(-5)(-3)$

$$a=\pi'_1\cdot\ldots\cdot\pi'_m \quad m\in\mathbb{N}$$

π'_j ראשוניים

אזי $n=m$ וקיימת תמורה $\alpha\in S_n$ כך שלכל $1\leq i\leq n$ $\pi_i=\pi'_{\alpha(i)}u_i$

כאשר $u_i\in R$ הפיך.

הוכחה: קיום פירוק כבר ראינו.

נניח $\pi'_1\cdot\ldots\cdot\pi'_m=\pi_1\cdot\ldots\cdot\pi_n=a$

אזי $\pi_1|a$, כלומר π_1 מחלק את a לכן קיים $1\leq j_1\leq m$

כך ש: $\pi_1|\pi'_{j_1}$

$$\pi'_{j_1}=\pi_1u_1$$

! u_1 הפיך כי π'_{j_1} אי-פריק.

סמן "כובע" כי מוריד אותו

$$\Leftarrow \pi_2\cdot\ldots\cdot\pi_n=\pi'_1\cdot\ldots\cdot\hat{\pi}'_{j_1}\cdot\ldots\cdot\pi'_m u_1$$

ועכשיו חוזרים על התהליך: π_2 מחלק את אגף שמאל ולכן מאגף ימין

$\Leftarrow$ קיים $1\leq j_2\leq m$

$$\pi_2|\pi'_{j_2}$$

$\pi_{j_2}=\pi_2u_2$ וכו'....

∎

22-1-2007 ③

נתבונן על התהליך של ההוכחה הקודמת:

$$\pi_1\cdots\pi_n = \pi_1'\cdots\pi_m'$$

$\Leftarrow$ קיים $1\le j_1\le m$

כך ש: $\pi_1 \mid \pi_{j_1}'$

$\Leftarrow$ $\pi_{j_1}' = \pi_1 u_1$

u_1 הפיך !

$$\pi_1\pi_2\cdots\pi_n = \pi_1'\cdots\pi_{j_1-1}'\pi_j'\pi_{j+1}'\cdots\pi_m'$$

$$\pi_1(\pi_2\cdots\pi_n) = \pi_1'\cdots(\pi_1u_1)\cdots\pi_m'$$

נטען כי ניתן לחלק ב- π_1

$\Leftarrow$ $\pi_2\cdots\pi_n = \pi_1'\cdots\pi_{j_1-1}'\pi_{j_1+1}'\cdots\pi_m'u_1$

כלומר: $\pi_1\alpha = \beta\pi_1u_1$

$$\Rightarrow \pi_1(\alpha-\beta u_1) = 0$$

$$\pi_1\ne 0 \Rightarrow \alpha-\beta u_1 = 0 \Rightarrow \alpha=\beta u_1$$

וחוזרים על התהליך הזה פעם אחר פעם.

π_2 מחלק את $\pi_1'\cdots\hat{\pi}_j'\cdots\pi_m'u_1$

מסמנים בכובע כי הועקר

ו- π_2 (ראשוני) אינו מחלק את u_1

כי u_1 הפיך לכן קיים $1\le j_2\le m$, $j_2\ne j_1$

כך ש: $\pi_2 \mid \pi_{j_2}'$

$$\pi_{j_2}' = \pi_2u_2$$

u_2 הפיך ונקבל:

$$\pi_3\cdots\pi_n = \pi_1'\cdots\hat{\pi}_{j_2}'\cdots\hat{\pi}_{j_1}'\cdots\pi_1'u_1u_2$$

נחזור על התהליך עבור π_3. נמצא $1\le j_3\le m$

$j_3\ne j_1, j_2$ $\pi_{j_3}' = \pi_3u_3$

התהליך לא יכול להיעצר עבור $i\le n$ כי אחרת היינו מקבלים

$$\underset{\text{לא הפיך}}{\pi_i}\cdots\pi_n = \underbrace{u_1\cdots u_{i-1}}_{\text{הפיך}}$$

וזו סתירה.

לכן $n \le m$ וקיבלנו

$1 = \underbrace{\text{מכפלה של יחידים}}_{m-n}, u_1 u_2 \dots u_n$

(משיקולי סימטריה באותו אופן $m \le n$ ולכן $m=n$)

$\alpha(i) = j_i$

(זה דומה מאוד להוכחה שעשינו על מספרים שלמים)

נושא) מתי מספר טבעי הוא סכום של שני ריבועים?

נתחיל ראשית מהשאלה מתי מספר ראשוני הוא סכום ריבועים.

משפט: $p \in \mathbb{N}$ ראשוני הוא סכום של שני ריבועים

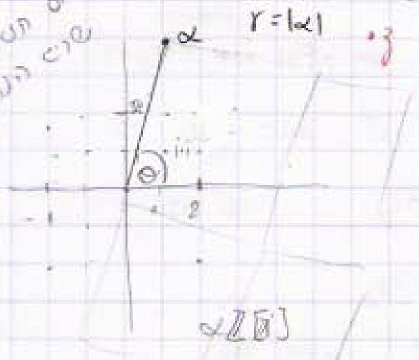
$p = a^2 + b^2$ כאשר $a, b \in \mathbb{Z}$

(פרמה) $\Longleftrightarrow$ $p = 2$ או $p \equiv 1 \pmod 4$

משפט: $\mathbb{Z}[i] = \{a+bi \mid a, b \in \mathbb{Z}\}$ הוא חוג אוקלידי.

נגדיר את d: $d(a+bi) = |a+bi|^2$

נבדוק כי מתקיימים התנאים של d: $d(\alpha\beta) = |\alpha\beta|^2 = |\alpha|^2 \cdot |\beta|^2 \ge |\alpha|^2$ $0 \ne \alpha, \beta \in \mathbb{Z}[i]$



נותר לבדוק "חלוקה עם שארית":

יהי $\alpha \in \mathbb{Z}[i]$ כך ש: $\alpha = a+bi$

יהי $z \in \mathbb{Z}[i]$ $z = u + iv$

אנו רוצים לחלק עם שארית את z ב- α.

רוצים להסתכל על $z - \beta\alpha$ כאשר $\beta \in \mathbb{Z}[i]$

לכל $z \in \mathbb{C}$ קיים $\beta \in \mathbb{Z}[i]$ כך $z - \beta\alpha$

שייך לריבוע באורך צלע באורך של α ($|\alpha|$) שמרכזו בראשית.

22-1-2007

נשים לב כי לכל $x \in \diamond$ כלומר x בריבוע שאורך
צלעו $|\alpha|$ ומרכזו בראשית מתקיים:

$$|x|^2 \leq \left(\frac{|\alpha|}{2}\right)^2 + \left(\frac{|\alpha|}{2}\right)^2 = \frac{|\alpha|^2}{2} < |\alpha|^2$$

כלומר $\mathbb{Z}[i]$ הוא תחום אוקלידי.

נחזור להוכחת המשפט על סכום ריבועים:

טענה: יהי p ראשוני אז: $p \equiv 1 \bmod 4$ אז -1 ב-$\mathbb{Z}/p\mathbb{Z}$ הוא שארית ריבועית

כלומר קיים $x \in \mathbb{Z}/p\mathbb{Z}$ כך ש: $x^2 = -1$ ב $\mathbb{Z}/p\mathbb{Z}$

נניח את הטענה אז: יהי $x_0 \in \mathbb{Z}$

כך ש: $x_0^2 \equiv -1$ מודולו p. זה אומר ש:

$x_0^2 + 1$ מתחלק ב-p כלומר

$$p \mid x_0^2 + 1 = (x_0+i)(x_0-i)$$

נשים לב כי p לא מחלק את (x_0+i) וגם p לא מחלק את (x_0-i)

$\Leftarrow$ p אינו ראשוני ב-$\mathbb{Z}[i]$
(כי זהו תחום אוקלידי)

$\Leftarrow$ p אינו אי-פריק, כלומר קיימים $\alpha, \beta \in \mathbb{Z}[i]$ לא הפיכים כך ש:

$$p = \alpha\beta$$

$$\Leftarrow \quad d(p) = p^2 = \underbrace{|\alpha|^2 |\beta|^2}_{d(\alpha)\, d(\beta)}$$

$$\Leftarrow \quad |\alpha|^2 = \begin{cases} \cancel{1} \\ p \\ \cancel{p^2} \end{cases}$$

לא 1 כי α אינו הפיך

כי β אינו הפיך

לכן $\underbrace{|\alpha|^2}_{a^2+b^2} = p$ אם $\alpha = a+bi$

וקיבלנו את המשפט.

מס׳ זוגי של גורמים

הוכחת הטענה: נגדיר $X = 1 \cdot 2 \cdot 3 \cdot \ldots \cdot \frac{p-1}{2}$ $(p \equiv 1 \bmod 4)$

טענה: $X^2 = -1$

$$X = (-1)(-2)(-3) \cdot \ldots \cdot \left(-\frac{p-1}{2}\right) =$$

נהפוך את הסדר

$$= \left(\frac{p+1}{2}\right)\left(\frac{p+3}{2}\right) \cdot \ldots \cdot (p-3)(p-2)(p-1)$$

$$X^2 = 1 \cdot 2 \cdot 3 \cdot \ldots \cdot \left(\frac{p-1}{2}\right)\left(\frac{p+1}{2}\right) \ldots (p-1) = (p-1)! = -1$$

נימוק שני:

נניח $0 \neq a = X^2$

נתבונן ב: $(a)^{\frac{p-1}{2}} = (X^2)^{\frac{p-1}{2}} = X^{p-1} = 1$

זהו גם תנאי מספיק

מספר ה a-ים ב- $\mathbb{Z}/p\mathbb{Z}^*$ כך שהם ריבוע הוא בדיוק $\frac{p-1}{2}$

במקרה שלנו: $(-1)^{\frac{p-1}{2}} = 1$

כי $\frac{p-1}{2}$ הוא זוגי.

24-1-2007

חוגים אלגבריים - שיעור אחרון

נחזור על משהו משיעור קודם:

משפט (הכנה):

ראשוני p ניתן להצגה כסכום של שני ריבועים (שלמים) אם ורק אם $p\equiv 1 (mod 4)$

טענה: כאשר $p\equiv 1$ מודולו 4 -1 הוא שארית ריבועית כלומר קיים x ב $\mathbb{Z}/p\mathbb{Z}$ כך ש- $x^2\equiv -1$ (ב $\mathbb{Z}/p\mathbb{Z}$).

הוכחת הטענה:

(א) נרשום x כמה:

$$x = 1\cdot 2\cdot 3\cdots\underbrace{\frac{p-1}{2}}_{\text{זוגי}} = (-1)(-2)(-3)\cdots\left(-\frac{p-1}{2}\right) =$$

$$= (p-1)(p-2)\cdots\left(\frac{p+1}{2}\right) = \frac{p+1}{2}\cdot\frac{p+1}{3}\cdots(p-1)$$

(היות וזה מס' זוגי ניתן לשנות את הסדר לכפל וזה לא ישתנה.)

$$x^2 = 1\cdot 2\cdots\left(\frac{p-1}{2}\right)\left(\frac{p+1}{2}\right)\cdots(p-1) = (p-1)!$$

ראינו כי $(p-1)! = -1$ ב $\mathbb{Z}/p\mathbb{Z}$

אם נסביר זאת שוב: נתבונן ב- $G = (\mathbb{Z}/p\mathbb{Z})^*$

$(p-1)!$ היא מכפלת כל האיברים ב $(\mathbb{Z}/p\mathbb{Z})^* = G$

לכל $a\in(\mathbb{Z}/p\mathbb{Z})^*$ פרט ל-1 ול- -1 $a^{-1}\neq a$

כי משוואה לפולינום x^2-1 יש לכל היותר שני שורשים $1, -1$.

אז נסתכל במכפלה: $1\cdot 2\cdot 3\cdots\frac{1}{2}\cdot\frac{1}{3}\cdots(p-1) = 1\cdot(-1) = -1$

טענה: יהי $p(x)\in F[x]$ פולינום ממעלה n אזי ל- $p(x)$ יש לכל היותר n שורשים

למה: אם $\alpha\in F$ שורש של $p(x)\in F[x]$ אזי $x-\alpha$ מחלק את $p(x)$

הוכחת הלמה: α שורש פירושו $p(\alpha)=0$.

נחלק את $p(x)$ ב- $x-\alpha$.

$F[x]$ תחום אוקלידי $p(x) = q(x)(x-\alpha) + r(x)$

כאשר $1 = d(x-\alpha) > d(r(x))$ — כי תחום אוקלידי, d של פולינום הינו המעלה שלו

$\Leftarrow$ $d(r(x)) = 0$ כלומר $r(x) = b\in F$

מאידך $0 = p(\alpha) = \underset{0}{q(\alpha)(\cancel{x}-\alpha)} + \underset{b}{r(\alpha)} \Leftarrow r(x) = b = 0$

קיבלנו $p(\alpha) = 0 \Leftarrow p(x) = q(x)(x-\alpha)$ למשהו α.

לכן אם $\alpha_1, \dots, \alpha_m$ שורשים של $p(x)$

$\alpha_i \neq \alpha_j$ לכל $1 \leq i, j \leq m$

$(x-\alpha_1) | p(x)$

$(x-\alpha_2) | p(x) = (x-\alpha_1)q_1(x)$

נשים לב כי פולינומים מהצורה $x-\beta$ הם אי-פריקים ולכן ראשוניים

לכן $x-\alpha_2$ מחלק את $x-\alpha_1$ או את $q_1(x)$

הנחנו: $\alpha_1 \neq \alpha_2$ $(x-\alpha_2)$ לא מחלק את $(x-\alpha_1)$

לכן $(x-\alpha_2)$ מחלק את $q_1(x)$.

אז: $q_1(x) = (x-\alpha_2)q_2(x)$

אם עתה $p(x) = (x-\alpha_1)(x-\alpha_2)q_2(x)$ עכשיו ממשיכים באותה הצורה

$(x-\alpha_3) | (x-\alpha_1)(x-\alpha_2)q_2(x)$ ושוב מאותם שיקולים הוא מחלק את $q_2(x)$

$\Leftarrow q_2(x) = (x-\alpha_3)q_3(x)$

⋮

וכן הלאה

וקיבלנו כי: $p(x) = (x-\alpha_1)(x-\alpha_2)(x-\alpha_3)\dots(x-\alpha_m)q_m(x)$

$q_m(x) \in F[x]$ איזשהו פולינום $q_m(x) \neq 0$ (כי $p(x)$ אינו פולינום האפס)

$d((x-\alpha_1)\dots(x-\alpha_m)) = m$

$\Downarrow$

$n = d(p(x)) = d\left(\prod_{i=1}^{m}(x-\alpha_i) \cdot q_m(x)\right) \geq \underset{m}{d\left(\prod_{i=1}^{m}(x-\alpha_i)\right)}$

כלומר לפולינום מדרגה m יש לכל היותר m שורשים. $\boxtimes$ (סיום הוכחת המשפט)

24-1-2007

② הנימוק השני ②

נתבונן ב $(\mathbb{Z}/p\mathbb{Z})^*$

(זוהי חבורה ציקלית) (חצי מהאיברים בחבורה ציקלית מסדר זוגי (הם ריבוע)

ב- $(\mathbb{Z}/p\mathbb{Z})^*$ נשים כי:

איבר מהצורה x^2 ב- $(\mathbb{Z}/p\mathbb{Z})^*$ מקיים כי $a^{\frac{p-1}{2}}=1$

$$a^{\frac{p-1}{2}}=(x^2)^{\frac{p-1}{2}}=x^{p-1}=1$$

כל שארית ריבועית ב- $(\mathbb{Z}/p\mathbb{Z})^*$ היא שורש של הפולינום

$$y^{\frac{p-1}{2}}=1$$

והיפך, כל שורש של פולינום זה הוא שארית ריבועית.

נובע מכך ש: $(\mathbb{Z}/p\mathbb{Z})^*$ חבורה ציקלית.

לכן נשים לב כי -1 הוא שורש של הפולינום $y^{\frac{p-1}{2}}-1$ כי $\frac{p-1}{2}$ זוגי

אם נעשה נסתכל במודולו 13

0	1	2	3	4	5	6	7	8	9	10	11	12
ריבוע	1	4	9	3	12	10	10	12	3	9	4	1

$$\varphi: (\mathbb{Z}/p\mathbb{Z})^* \longrightarrow (\mathbb{Z}/p\mathbb{Z})^* \qquad 2<p$$

$$\omega \longmapsto \omega^2$$

φ היא העתקה 2 ל-1

$$(\omega_0)^2=(-\omega_0)^2$$

ולכן $|\varphi((\mathbb{Z}/p\mathbb{Z})^*)|=\frac{p-1}{2}$

$\boxtimes$

למה: תהי $(G,\cdot,1)$ חבורה אבלית סופית.

אזי G ציקלית אם ורק אם לכל $k<|G|$ מספר האיברים $g\in G$ כך ש: $g^k=1$ לכל היותר k.

הוכחה:

נזכור כי חבורה אבלית סופית היא מהצורה: $C_{n_1}\times C_{n_2}\times\dots\times C_{n_r}$

כאשר C_{n_i} היא ציקלית מסדר n_i ולכל $1\le i\le r-1$

$n_{i+1}|n_i \Longrightarrow$ כי $g\in G$ מקיים $g^{n_1}=1$

$$g(x_1,x_2,\dots,x_r)$$

$$g^{n_1}=(x_1^{n_1},x_2^{n_1},\dots,x_r^{n_1})=(1,\dots,1)=1$$

לכן אילו אם G ציקלית קיבלנו כי $n_1<|G|$ שורשים ל- $g^{n_1}=1$ וסתירה

☒

משפט: יהי R חוג אוקלידי. אזי אידיאל aR, $a\in R$ הוא מקסימלי אם ורק אם a ראשוני.

הוכחה:

נניח a אינו ראשוני, אזי a אינו אי-פריק כלומר $a=bc$, b,c לא הפיכים ולכן $d(b)<d(a)$

לכן האידיאל $aR\subsetneq bR$ מכיל ממש את aR

מצד שני, היות ו-b אינו הפיך אזי האידיאל $bR\neq R$

קיבלנו כי aR אינו אידיאל מקסימלי.

הכיוון השני:

נניח להפך כי a ראשוני ונניח כי $aR\subset U\triangleleft R$ אידיאל אזי היות וחוג אוקלידי הוא חוג ראשי קיים $u\in U$ כך ש: $U=uR$ ולכן $a\in uR \Longleftarrow a=uv$, $v\in R$

a ראשוני $\Longleftarrow$ a אי-פריק ולכן או u הפיך או v הפיך $\Longleftarrow$

אם u הפיך $\Longleftarrow$ $uR=U=R$

אם v הפיך $\Longleftarrow$ $U=uR=av^{-1}R=aR$ ($a=uv$, $u=av^{-1}$)

וקיבלנו או $U=R$ או $U=aR$ ו- aR מקסימלי ☒