אביב 2005
ליאור

אלגברה מודרנית - 104134 קבוצת תרגול 12
סמסטר אביב 2005 - שיעורי בית מס' 1#

1. צ"ל $(na,nb)=n(a,b)$.

נגדיר $L:=(a,b)$. עפ"י הגדרת ה-ממג"ב אנו יודעים שמתקיים$L>0$, $L|a$, $L|b$, ושכל מספר טבעי d שמחלק את a ואת b, מחלק גם את L. עלינו להוכיח ש-$(na,nb)=n(a,b)=\mathbf{nL}$.

נעבוד לפי הגדרת ה-ממג"ב, ובעזרת האמור לעיל:

- **$nL|na$** → $L|a$ (משום שאם $L|a$ קיים q כך ש-$Lq=a$, ואז $nLq=na$ כלומר $nL|na$.
- **$nL|nb$** → $L|b$ (באותו אופן).
- יהי d מספר טבעי שמחלק את na ואת nb, כלומר קיימים u,v כך ש: $du=na$, $dv=nb$. מכיוון ש-$L=(a,b)$ אזי לפי המשפט היסודי קיימים 2 מספרים טבעיים e,f כך ש-$L=ae+bf$. נכפול פי n ונקבל $nL=(na)e+(nb)f$. נציב את הביטויים של na ו-nb ונקבל $\underline{\mathbf{nL}}=(du)e+(dv)f=\underline{\mathbf{d}(ue+vf)}$, משמע **לכל d שמחלק את na ו-nb, d מחלק גם את nL.**
- מאחר שמתקיימות 3 הטענות שלעיל, הרי שלפי ההגדרה - $(na,nb)=nL$.

<u>משל</u>

4.

א. נתון $(a,m)=1$, $(b,m)=1$, צ"ל $(ab,m)=1$.

- קיימים u_1,v_1 כך ש- $au_1+mv_1=1$.
- קיימים u_2,v_2 כך ש- $bu_2+mv_2=1$.
- נכפול את שתי המשוואות -

$(au_1+mv_1)(bu_2+mv_2)=abu_1u_2+au_1mv_2+bu_2mv_1+mv_1mv_2=$

$\mathbf{ab}(u_1u_2)+\mathbf{m}(au_1v_2+bu_2v_1+mv_1\,v_2)=1$ → יש u_0,v_0 טבעיים כך ש: $abu_0+mv_0=1$

→ $(ab,m)|1$ → $(ab,m)=1$ ולכן לפי משפט שהוכחנו בכיתה* (הוכחה בהמשך):

* ההוכחה המלאה - נגדיר $L:=(ab,m)$. מתקיים $L|ab$, $L|m$, כלומר יש s,t כך ש-$Ls=ab$, $Lt=m$. קיבלנו קודם ש-$abu_0+mv_0=1$, נציב ונקבל - $Lsu_0+Ltv_0=1$, ולכן

$L(su_0+tv_0)=1$ כלומר $L|1$. מאחר ש-L הוא ממג"ב מתקיים $L>0$, ולכן $(ab,m)=L=1$.

ב. צ"ל את הכיוון ההפוך:

- נתון ש- $(ab,m)=1$. מכאן שלפי הגדרת ה-ממ"גב: כל d שמחלק את ab ואת m מקיים בהכרח $d|1$.
- ננית בשלילה ש-$(a,m)=e\neq 1$. e הוא מספר טבעי, והוא ממג"ב ולכן $e>0$, ומכאן ש-$e>1$.
- e מקיים elm ו-ela, ולכן גם $elab$ (כי אם ela אז קיים q כך ש-$eq=a$ ולכן $e(qb)=ab$). מאחר ש-e מחלק את m ואת ab הוא חייב כאמור לעיל לקיים $e|1$ אבל אמרנו ש- $e>1$ ולכן מתקבלת סתירה - לא יתכן ש=$(a,m)\neq 1$ כלומר בהכרח $(a,m)=1$.
- באותו אופן ניתן להוכיח ש- $(b,m)=1$.

ג. צ"ל $(a,b)=1$ <==> $(a^2,b^2)=1$.

- בכיוון אחד ←: נתון ש-$(a,b)=1$. לפי סעיף א' מתקיים $(a*a,b)=1$, כלומר $(a^2,b)=1$. מכיוון שבפעולת (x,y) אין חשיבות לסדר, נוכל להחליף את הסדר ל-$(b,a^2)=1$ ואז להפעיל את סעיף א' שוב (למעשה אין בכך צורך כי סעיף א' פועל באותו אופן גם אם המכפלה בצד ימין). מכאן:
$(a^2,b^2) = 1$
- בכיוון השני →: נתון ש-$(a^2,b^2)=1$, כלומר $(a*a,b*b)=1$. לפי סעיף ב' עולה מכך ש=$(a,b*b)=1$, ואם נפעיל שוב את סעיף ב' (גם כאן אין משמעות לסדר האיברים בסוגריים) נקבל ש-$(a,b)=1$. משל.

5.

א. חשב $(315,483)$: נשתמש באלגוריתם אוקלידס כמובן:

$(315,483)=(315,483 \bmod 315)=(315,168)=(168,315 \bmod 168)=(168,147)$
$=(147,168 \bmod 147)=(147,21)=21$

כעת נעבור על התהליך בכיוון השני ונמצא זוג מספרים שלמים שמקיימים $315x+483y=21$:

$21=168-147=168-(315-1*168)=2*168-315=2*(483-1*315)-315$

$=2*483-3*315$ ➔ $x=-3;\ y=2.$

ב. חשב $(259,91)$:

$(259,91)=(91,259 \bmod 91)=(91,77)=(77,91 \bmod 77)=(77,14)$

$=(14,77 \bmod 14)=(14,7)=7$

ולמציאת x,y:

$7=14-7=14-(77-5*14)=6*14-77=6*(91-77)-77=6*91-7*77$

$=6*91-7*(259-2*91)=20*91-7*259$ ➔ $x=-7;\ y=20$

6. a,b שלמים נתונים כמכפלת חזקות של מספרים ראשוניים.

א. ניתן להניח שהפירוק עושה שימוש באותם מספרים ראשוניים מכיוון שביכולתנו ליצור קבוצה סופית של מספרים ראשוניים שבה מופיעים **כל** האלמנטים המרכיבים את a **וכל** האלמנטים המרכיבים את b (מספרים סופיים). קבוצה זו תשמש לתיאור a ו-b כאשר לכל אחד מהם תתאים סדרה יחידה של מעריכים עבור המספרים הראשוניים בקבוצה בהתאמה (במידה שמספר ראשוני אינו מופיע במספר מסויים ניתן לשייך לו את המעריך 0 עבור אותו מספר).

בניסוח מתמטי: לכל מספר ראשוני p ולכל מספר שלם a, קיים מספר שלם אי שלילי $i\geq 0$ כך שמתקיים $p^i|a$ (במקרה ש-p כלל לא מחלק את a, $i=0$), ועל כן $a=q*p^i$, ומכיוון ש-q אף הוא מספר שלם ניתן להמשיך את תהליך הפירוק עליו עד לקבלת $q=1$, ולקבל בסוף את הפירוק למספרים ראשוניים של a.

$a=p_1^{i1}p_2^{i2}p_3^{i3}...p_n^{in}$ (ובאותו אופן $b=p_1^{j1}p_2^{j2}p_3^{j3}...p_n^{jn}$).

ב. ביטוי הממג"ב באמצעות המרכיבים הראשוניים:

בהנתן a,b המבוטאים ע"י מכפלת מספרים ראשוניים $p_1..p_n$

$a=p_1^{i1}p_2^{i2}p_3^{i3}...p_n^{in}$; $b=p_1^{j1}p_2^{j2}p_3^{j3}...p_n^{jn}$

$(a,b) := p_1^{\min\{i1,j1\}}p_2^{\min\{i2,j2\}}p_3^{\min\{i3,j3\}}...p_n^{\min\{in,jn\}}$

מתקיים $(a,b)|a$, משום שחזקת כל אחד מהמספרים הראשוניים קטנה או שווה לחזקה של אותו מספר ראשוני ב-a, וניתן ע"י כפל בלבד באותם מספרים ראשוניים להגיע ל-a), ובאותו אופן $(a,b)|b$. כמו כן, כל מספר שמחלק את a ואת b, ניתן לפירוק לאותם מספרים ראשוניים כאשר החזקות של כל אחד מהם

קטנות או שוות לחזקות של המספרים הראשוניים המרכיבים את (a,b) בהתאמה.

ג. ביטוי כמק"ב - באותו אופן שביטאנו את הממג"ב: בהנתן זוג מספרים טבעיים a,b הנתונים ע"י פירוק למספרים ראשוניים באופן הבא:

$a=p_1^{i1}p_2^{i2}p_3^{i3}...p_n^{in}$; $b=p_1^{j1}p_2^{j2}p_3^{j3}...p_n^{jn}$

$[a,b] := p_1^{\max\{i1,j1\}}p_2^{\max\{i2,j2\}}p_3^{\max\{i3,j3\}}...p_n^{\max\{in,jn\}}$

מתקיים $a|[a,b]$ כיוון שחזקתו של כל מספר ראשוני ב-[a,b] גדולה או שווה לחזקת אותו מספר ב-a, ובאותו אופן מתקיים גם $b|[a,b]$. כמו כן, אם קיים e טבעי כך ש-$a|e$ ו-$b|e$, אזי e ניתן לפירוק למספרים ראשוניים הכוללים לפחות את כל המספרים הראשוניים $p_1..p_n$ (למרות שיתכן שירכיבו אותו גם מספרים נוספים), ולכל אחד מהם חזקה גדולה או שווה לחזקת אותו מספר ב-[a,b].

ד. לפי הסעיפים הקודמים:

$(a,b) := p_1^{\min\{i1,j1\}}p_2^{\min\{i2,j2\}}p_3^{\min\{i3,j3\}}...p_n^{\min\{in,jn\}}$

$[a,b] := p_1^{\max\{i1,j1\}}p_2^{\max\{i2,j2\}}p_3^{\max\{i3,j3\}}...p_n^{\max\{in,jn\}}$

$(a,b)*[a,b]=p_1^{\min\{i1,j1\}+\max\{i1,j1\}}p_2^{\min\{i2,j2\}+\max\{i2,j2\}}p_3^{\min\{i3,j3\}+\max\{i3,j3\}}...p_n^{\min\{in,jn\}+\max\{in,jn\}}$

$=p_1^{i1+j1}p_2^{i2+j2}p_3^{i3+j3}...p_n^{in+jn} = (p_1^{i1}p_2^{i2}p_3^{i3}...p_n^{in})*(p_1^{j1}p_2^{j2}p_3^{j3}...p_n^{jn})$

$=a*b$ ➔ משל $[a,b]=ab / (a,b)$

8. צ"ל שלמשוואה $ax+by=c$ יש פתרונות x,y שלמים אמ"ם $(a,b)|c$.

א. בכיוון אחד ➔: נגדיר $d:=(a,b)$. נתון ש-$(a,b)|c$, כלומר $d|c$ ולכן קיים q שלם כך ש-$dq=c$. מכיוון ש-d הוא (a,b), הרי שלפי המשפט הבסיסי קיימים u,v שלמים כך ש-$au+bv=d$, ואם נכפול ב-q נקבל $auq+bvq=dq=c$. נגדיר $x=uq$, $y=vq$ (x,y שלמים) ומתקיים $ax+by=c$ כלומר יש פתרונות שלמים למשוואה.

ב. בכיוון השני ➔ נתון שקיימים x,y שלמים כך ש-$ax+by=c$. נגדיר שוב $d:=(a,b)$. משתמע ש-$d|a$ ו-$d|b$, כלומר קיימים u,v שלמים כך ש-$du=a$ ו-$dv=b$. נציב בנתון ונקבל $dux+dvy=c$, כלומר $d(ux+vy)=c$ ולכן $d|c$. נציב חזרה את הערך של d ונקבל $(a,b)|c$. משל.

אביב 2005
ליאור

אלגברה מודרנית - 104134 קבוצת תרגול 12
סמסטר אביב 2005 - שיעורי בית מס' 2#

14. n,m שלמים אי זוגיים, צ"ל $8|n^2-m^2$.

קיימים q_1,r_1 כך ש-$n=2q_1+r_1$. מאחר ש-n איזוגי, הרי שבהכרח $r_1=1$, כלומר $n=2q_1+1$. באותו אופן קיים q_2 כך ש-$m=2q_2+1$.

$$n^2-m^2=(2q_1+1)^2-(2q_2+1)^2=(4q_1^2+4q_1+1)-(4q_2^2+4q_2+1)$$
$$=4q_1^2-4q_2^2+4q_1-q_2=4[(q_1^2-q_1)+(q_2^2-q_2)]$$

בהנתן מספר שלם x, קיימים v,u כך ש-$x=2u+v$, כאשר v שווה 0 או 1 אם x הוא זוגי או איזוגי בהתאמה, כלומר בחלוקה ל-2 נקבל שארית v.

$x^2=4u^2+2uv+v=2(2u^2+uv)+v$, כלומר בחלוקה ל-2 תוותר אותה שארית v, ולכן $x^2-x=[2(2u^2+uv)+v]-[2u+v]=2(2u^2+uv-u)$, כלומר 2 מחלק אותו.

נחזור למשוואה שקיבלנו קודם - 2 מחלק את $(q_1^2-q_1)$ ואת $(q_2^2-q_2)$, כלומר קיימים s,t כך ש= $(q_1^2-q_1)=2s$, $(q_2^2-q_2)=2t$, ולכן

$$n^2-m^2=4[(q_1^2-q_1)+(q_2^2-q_2)]=4(2s+2t)=8(s+t)$$

והמסקנה היא ש-$8|n^2-m^2$, משל.

פרק ב' - יחסי שקילות

3.

א. כן, יחס שקילות וקבוצת מחלקות השקילות היא $\mathbb{R}^+$ (כל הממשיים האי-שליליים, כולל אפס המצוי במחלקה לבדו): $[x]=\{x,-x \mid \forall x \in R^+\}$

ב. כן, יש אינסוף מחלקות שקילות שניתן לייצג כ-...[100],[10],[1]. ניתן גם לכתוב $[10^n]$ לכל n שלם ואי שלילי. הייצוג המלא (לכל מחלקת שקילות ערך n אחר): $[x]=\{10^{n-1} \le a < 10^n \mid n \in N, a \in Z^+\}$

ג. כן, יש 10 מחלקות שקילות והן [9]...,[1],[0]. ניתן לומר שזהו שוויון מודולו 10 ולכן מתקיימות התכונות הדרושות של שוויון רגיל.

$$[x]=\{a \equiv x(\mathrm{mod}\,10) \mid a \in Z^+\}$$

ד. כן, כל מחלקת שקילות מייצגת מעגל ברדיוס קבוע שמרכזו בראשית (על כן יש אינסוף מחלקות):

$$[(x,y)]=\{(a,b) \mid a,b \in R, a^2+b^2=x^2+y^2\}$$

ה. לא, זה אינו יחס שקילות. למשל לא מתקיימת רפלקסיביות **לכל** נקודה (a,b) כאשר a≠b כי אז a-b ≠ b-a.

ו. כן, ואוסף כל מחלקות השקילות הוא קבוצת כל הישרים העוברים בראשית (כי כל ישר שמקביל הוא למעשה הזזה של אחד מהם). זה ניתן לייצוג כ-[y=ax] כאשר a שייך ל-$\mathbb{R}$. (בתוספת מחלקת השקילות של הישר [x=0]).

$$[y=ax]=\{y=mx+n \mid m,n\in R, a=m\}$$
$$[x=0]=\{x=a \mid a\in R\}$$

ז. לא, זה אינו יחס שקילות משום שאם נקח שני ישרים מקבילים l_1,l_2, נוכל לקחת ישר l_3 האנכי לשניהם, ובכך נסתר עקרון האסוציאטיביות:

$l_1 \parallel l_2$ אבל $l_1 \perp l_3$, $l_3 \perp l_2$

5. א. נבדוק עפ"י הגדרת השקילות:

- a~a כי f(a)=f(a) כי הפונקציה היא העתקה ועפ"י ההגדרה ח"ע.
- אם a~b אז לפי הנתון f(a)=f(b) ומכיוון שאלו ערכים שווים ניתן להפוך את סדר השווין - f(b)=f(a) כלומר גם b~a.
- אם a~b וגם b~c אזי f(a)=f(b)=f(c) כלומר f(a)=f(c) ולכן a~c.

מאחר ש-3 התנאים מתקיימים זהו יחס שקילות.

ב. על מנת שכל מחלקת שקילות תהיה בעלת איבר יחיד f צריכה להיות ח"ע: כיוון שלכל a~b מתקיים f(a)=f(b), ואם f ח"ע אזי בהכרח נובע שגם a=b, כלומר לכל a~b ← a=b ולכן כל מספר a מצוי לבדו במחלקת השקילות של עצמו.

ג. מאחר שהוכחנו שניתן לבסס יחס שקילות על העתקה ח"ע בין 2 קבוצות כמו בסעיף א', ניישם זאת ע"י הפונקציה המוגדרת בסעיף זה - היחס "a~b אמ"ם f(a)=a(b)" הוא יחס שקילות. נגדיר n:=a-b (n הוא מספר שלם לפי הנתון):

$$f(a)=f((a-b)+b)=f(n+b)=\cos(2\pi\cdot(n+b))+i\cdot\sin(2\pi\cdot(n+b))$$

בפונקציות ה-sin וה-cos כל היסט בכפולות שלמות של 2π מתבטל:

$$=\cos(2\pi\cdot n+2\pi\cdot b)+i\cdot\sin(2\pi\cdot n+2\pi\cdot b)=\cos(2\pi\cdot b)+i\cdot\sin(2\pi\cdot b)=f(b)$$

מכאן ש-f(a)=f(b) אמ"ם ההפרש a-b הוא שלם (כלומר a~b לפי ההגדרה), ומכך משתמע לפי סעיף א' שזה יחס שקילות.

ד. הפונקציה f גג מעתיקה כל אחת ממחלקות השקילות ב-S1 לאיבר ב-S2.
מאחר שהוכחנו בסעיף א' שלכל a~b מתקיים f(a)=f(b), אזי f גג הינה ח"ע - מעתיקה כל איבר מהתחום (מחלקת שקילות) לאיבר אחד בתמונה (S2) ואין כל משמעות לשאלה לפי איזה מאברי מחלקת השקילות יקבע ערכה של f גג, כי f מעתיקה את כל האברים באותה מחלקת שקילות לאותו איבר ב-S2. במילים אחרות - לכל שני איברים ב-S1/~ : אם [a]=[b] אז כל האיברים בהם שקולים (ניקח איבר אחד מכל קבוצה - a~b) ואז f^([a])=f(a)=f(b)=f^([b]).
כמו כן, ניתן לראות ש-f גג מוגדרת היטב על כל S1 משום שעל פי ההגדרה, מחלקות השקילות ב-S1 מכסות את הקבוצה כולה (כלומר איחוד מחלקות השקילות שווה ל-S1), וכל איבר ב-S1 שייך בדיוק לאחת ממחלקות השקילות הללו.
נוכיח ש-f גג חח"ע בכיוון ההפוך - אם f^([a])=f^([b]) לכל זוג איברים b,a ב-S1 השייכים למחלקות השקילות [a] ו-[b] בהתאמה מתקיים f(a)=f(b). לפי סעיף א' מכך נובע a~b ולכן עפ"י ההגדרה [a]=[b] - כלומר f גג היא חח"ע.

פרק ג' - קונגרואנציה מודולו n

2. u=4n+3, צריך להוכיח שלא ניתן לרושמו ע"י a^2+b^2. בדומה לשאלה 14 בפרק א' - נכתוב את a,b,u במודולו 4:

$$a\equiv s \quad b\equiv t \quad u\equiv 3 \pmod 4$$

הערכים של s,t הם בין 0 ל-3. נעלה אותם בריבוע:

$$s^2\equiv \begin{cases} 0 & s=0,2 \\ 1 & s=1,3 \end{cases}$$

וכנ"ל לגבי t^2

האפשרויות לתוצאת השיוון במודולו 4 הן: $s^2+t^2=0,1,2 \pmod 4$, אבל כאמור $u\equiv 3 \pmod 4$, ולכן לא יתכן שוויון. משל

3.

אביב 2005
ליאור

א. צ"ל $a\equiv b \pmod n$ ← $ak\equiv bk \pmod n$. לפי הנתון קיים u שלם כך ש-$a=b+un$ (כי $a-b=un \equiv 0 \pmod n$). כעת אפשר לכפול ב-k (לכל k) ולקבל $ak=bk+unk$, ואם נפעיל מודולו n יתאפס unk כי הוא כפולה שלמה של n-$unk\equiv 0 \pmod n$ ולכן $ak\equiv bk+0 \pmod n$. משל

ב. נתון $a\equiv b \pmod n$, $c\equiv d \pmod n$, כלומר קיימים u,v שלמים כך ש-$a=b+un$, $c=d+vn$. נחבר את המשוואות: $a+c=b+d+(u+v)n$, ונפעיל מודולו n כך שהאיבר האחרון יתאפס. נקבל $a+c=b+d+0 \pmod n$ - משל.

ג. נוכיח באינדוקציה: בסיס- $m=0$, $a_0\equiv b_0 \pmod n$ לפי הנתון, ולפי סעיף א' לכל k_0 מתקיים $k_0a_0\equiv k_0b_0$.

צעד האינדוקציה: בהנחה שהטענה מתקיימת עבור m מסויים - נוכיח שהיא מתקיימת גם עבור m+1. נתון - $\sum_{i=0}^{m} k_i a_i \equiv \sum_{i=0}^{m} k_i b_i \pmod n$

כמו כן לפי הנתון גם $a_{m+1}\equiv b_{m+1}$ ולכן לפי סעיף א' עבור כל k_{m+1} מתקיים

$$k_{m+1}a_{m+1}\equiv k_{m+1}b_{m+1} \pmod n$$

לכן, לפי סעיף ב' ניתן לחבר את המשוואות ולקבל

$$\sum_{i=0}^{m} k_i a_i + k_{m+1}a_{m+1} \equiv \sum_{i=0}^{m} k_i b_i + k_{m+1}b_{m+1} \pmod n$$

$$\sum_{i=0}^{m+1} k_i a_i \equiv \sum_{i=0}^{m+1} k_i b_i$$

ד. נקח מקרה פרטי של סעיף ג' בו נבחר את k כסדרה $k_i=10^i$, את המספר a=0 (כלומר $a_i=0$ זהותית) ו-b מהסעיף הקודם הוא x. לפי סעיף ג':

$$x = \sum_{i=0}^{m} 10^i \cdot x_i = \sum_{i=0}^{m} k_i \cdot x_i = \sum_{i=0}^{m} k_i \cdot x_i \equiv \sum_{i=0}^{m} k_i \cdot a_i \equiv \sum_{i=0}^{m} k_i \cdot 0 = 0$$

כלומר $x \equiv 0 \pmod n$

אביב 2005
ליאור

אלגברה מודרנית - 104134 קבוצת תרגול 12

סמסטר אביב 2005 - שיעורי בית מס' 3# - חבורות

פרק א' - חבורות

1.

א. לא, זו אינה חבורה משום שלא מתקיים תנאי האסוציאטיביות:
$(a-b)-c=a-b-c \neq a-(b-c)=a-b+c$.
כפועל יוצא גם כי האיבר הנייטראלי ($e=0$) אינו מקיים $x-e=x \neq e-x$.

ב. לא, זו אינה חבורה. התנאי הנדרש מחבורת מטריצות ביחס לכפל הוא שכל המטריצות תהיינה הפיכות. התנאי ab-cd אינו מספיק כפי שניתן לראות למשל במטריצה $\begin{pmatrix} 1 & 2 \\ 2 & 4 \end{pmatrix}$ בה $ab \neq cd$ אבל למטריצה אין הופכית.

ג. כן, זו חבורה. לפי התנאי $ad \neq 0$ גם a וגם d שונים מ-0, ולכן דרגת המטריצה היא 2 (בלי קשר ל-b - היא כבר מדורגת) והיא הפיכה, כלומר לכל איבר בחבורה יש הופכי. איבר נייטראלי: $e=I_{2x2}$. להוכחת סגירות נבדוק:

ומאחר שנתון $ad,eg \neq 0$ הרי ש-$aedg \neq 0$ $\begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \cdot \begin{pmatrix} e & f \\ 0 & g \end{pmatrix} = \begin{pmatrix} ae & af+dg \\ 0 & dg \end{pmatrix}$

(האסוציאטיביות נובעת מכפל מטריצות)

*(*הערה לשני הסעיפים הבאים- הנחתי שהחבורה מוגבלת למטריצות בגודל קבוע, אחרת הפעולה לא מוגדרת על כל זוג איברים בחבורה).*

ד. זו חבורה: עפ"י חוקי הדטרמיננטים $|AB|=|A|*|B|=1$ ולכן יש סגירות. כמו כן, עפ"י חוקי כפל מטריצות מתקיימת אסוציאטיביות $(AB)C=A(BC)$. האיבר הנייטראלי לפי חוקי כפל מטריצות: $e=I$ (מאותו סדר של שאר המטריצות בחבורה) - $IA=AI=A$, ו-I שייך לחבורה כי $|I|=1$. לבסוף - לכל איבר A בחבורה יש איבר הופכי, כיוון שמטריצות שהדטרמיננטה שלהן היא 1 הן הפיכות, ודטרמיננטת ההופכית שלהן היא $1/1=1$. (ניתן גם לומר ש-$A*A^{-1}=I$, ולכן $|A|*|A^{-1}|=|I|=1$ ולכן גם $|A^{-1}|=1$).

ה. לא, זו אינה חבורה - משום שלמשל אין סגירות בכפל: $|AB|=|A|*|B|=2*2=4$. כמו כן, האיבר הנייטראלי בכפל מטריצות, $I=e$, לא שייך לחבורה כי הדטרמיננטה שלו היא אחד, ולכן גם אין למטריצות בחבורה איברים הופכיים בתוך החבורה (גם אם נניח שהיו הופכיים ושהיה איבר נייטראלי - $|e|=|A|*|A^{-1}|=2*2=4$ וקיבלנו סתירה.)

9. חבורה G מכילה מספר זוגי של איברים. יש להוכיח שקיים איבר שריבועו הוא e, מלבד e עצמו: $a^2=e$, אבל גם $a*a^{-1}=e$, כלומר $a^2=a*a=a*a^{-1}$, וכיוון שמותר לצמצם בחבורה - $a=a^{-1}$. משמע - צריך להוכיח שקיים איבר מלבד e ששווה להופכי של עצמו.

כיוון שלכל איבר בחבורה חייב להיות הופכי, וכיוון שמתקיים $a=(a^{-1})^{-1}$ הרי שההתאמה של כל זוג איברים היא חח"ע, כלומר ניתן היה לחלק את כל האיברים בחבורה לזוגות של איברים הופכיים זה לזה, אלא שהאיבר e הוא ההופכי של עצמו ולכן אין לו זוג. מכיוון שנתון שבחבורה יש מספר זוגי של איברים נובע מכך שקיים עוד איבר אחד - נסמנו a - שגם לו אין בן זוג, אבל מכיוון שחייב להיות לו הופכי הרי שעליו להיות ההופכי של עצמו $a=a^{-1}$, ומכאן נובע ש-$a^2=e$ כאמור לעיל.

24. $a \circ b = ab - a - b + 2$

א. נגדיר $a=x+1$, $b=y+1$. כאשר $x,y>0$ (וממשיים) לפי הנתון ולכן $xy>0$. נציב:

$a \circ b = (1+x)(1+y)-(1+x)-(1+y)+2 = 1+x+y+xy-1-x-1-y+2 = 1+xy > 1$

ולכן מתקיימת סגירות.

ב. אסוציאטיביות -

I) $(a \circ b) \circ c=(ab-a-b+2) \circ c=(ab-a-b+2)*c-(ab-a-b+2)-c+2$

$=abc-ac-bc+2c-ab+a+b-2-c+2=\underline{abc-ac-bc-ab+a+b+c}$

II) $a \circ (b \circ c)=a \circ (bc-b-c+2)=a*(bc-b-c+2)-a-(bc-b-c+2)+2$

$=abc-ab-ac+2a-a-bc+b+c-2+2=\underline{abc-ab-ac-bc+a+b+c}$

התוצאות זהות (עד כדי סדר האיברים..) ולכן מתקיימת אסוציאטיביות.

ג. נדרש $a\circ e=a$ (מאחר שהפעולה סימטרית על שני האופרנדים, היא קומוטטיבית ולכן מובטח $a\circ e=e\circ a$):

$a\circ e=e\circ a=ae-a-e+2=a \rightarrow ae-e=2a-2 \rightarrow e(a-1)=2a-2 \rightarrow e=(2a-2)/(a-1)=2$

כלומר $e=2$ (ו-e שייך ל-G). החילוק אפשרי כי $a>1$.

ד. נראה שלכל a ב-G קיים b כך ש- $a\circ b=e=2$:

$a\circ b=ab-a-b+2=2 \rightarrow ab-a-b=0 \rightarrow ab-b=b(a-1)=a \rightarrow b=\underline{a^{-1}=a/(a-1)}$

וניתן גם לראות שההופכי של e הוא עצמו ($2/(2-1)=2$).

התנאי ההכרחי הוא שכל ההופכיים יהיו גם הם ב-G, ואכן לכל $a>1$, מתקיים $a-1>0$, כך ש-$a^{-1}=a/(a-1)$ הוא מוגדר תמיד וחיובי, וכיוון שלכל $a>1$ מתקיים $a>a-1$ (המונה גדול מהמכנה), הרי ש-a^{-1} יהיה תמיד ממשי גדול מ-1, ולכן בהכרח שייך ל-G.

פרק ב' - תת חבורות.

3.

א. לא, Q^+ לא כוללת הופכיים (חיבוריים) עבור איבריה, ובמידה שהכוונה אכן לכל הרציונאליים החיוביים (כלומר ללא 0) היא גם אינה כוללת את האיבר האדיש לפעולת החיבור.

ב. לא, כיוון שלא מתקיימת סגירות לפעולת החיבור, למשל $\pi^1+\pi^1=2\pi$ אבל $\log_\pi 2\pi=\log_\pi\pi+\log_\pi 2=1+\log_\pi 2$ - לא שייך לשלמים

ג. כן, זוהי תת חבורה והיא זהה למעשה לחבורת כל הממשיים מלבד שכל איבר בה מוכפל במקדם קבוע i. R עצמה היא תת חבורה של C, כיוון שהיא מוכלת כולה ב-C ומקיימת את כל התנאים לחבורה ביחס לחיבור (כפי שהוכח בכיתה). אם נכפול כל איבר ב-R במקדם i נוכל להוציא את i כגורם משותף בכל פעולה (כי מדובר בפעולת החיבור) ולכן אותן הוכחות תקפות.

5.

- לכל a,b,c ב-Z(G): $(ab)c=a(bc)$, כי Z(G) מוכלת ב-G ולכן מקיימת את האסוציאטיביות שלה.

- האיבר האדיש של G מקיים ex=xe=x לכל x ב-G ולכן הוא שייך גם ל-Z(G). מכיוון שהשוויון הזה מתקיים לכל x ב-G ובפרט לכל x ב-Z(G), e הוא גם האיבר האדיש של Z(G).

- סגירות - לכל a,b ב-Z(G) מתקיים ax=xa וכן bx=xb לכל x ב-G. לכן, ולפי האסוציאטיביות (שמתקיימת בכל G), מתקיים

(ab)x=a(bx)=a(xb)=(ax)b=(xa)b=x(ab)

כלומר גם ab מתחלף בכפל עם כל x השייך ל-G

- קיום הופכיים - לכל a ב-Z(G) קיים איבר הופכי a^{-1} ב-G כיוון ש-G היא חבורה, כלומר $a*a^{-1}=e$, כאשר e הוא האיבר הנייטראלי של G (ולמעשה גם של Z(G)). לכן, לכל x ב-G מתקיים ax=xa, ואם נכפול ב-a^{-1} מימין ומשמאל:

$ax=xa \rightarrow a^{-1}*ax=ex=x=a^{-1}*xa \rightarrow \underline{\mathbf{xa^{-1}}}=a^{-1}*xa*a^{-1}=a^{-1}*x*e=\underline{\mathbf{a^{-1}x}}$

כלומר גם ההופכי של a ב-G מתחלף עם כל איבר בכפל, ולכן גם הוא במרכז.

9. נגדיר את n בתור האיבר החיובי הקטן ביותר של תת החבורה G. כיוון שזו חבורה מתקיימת סגירות בחיבור, ולכן n+n+…+n=an שייך ל-G לכל a טבעי, וכיוון שגם ההופכי של n, n- שייך ל-G, a יכול להיות גם שלילי או אפס, כלומר an שייך ל-G לכל a שלם (ב-Z) - או במילים אחרות היות שהחבורה מקיימת סגירות לחיבור, היא מקיימת גם סגירות לכפל בשלמים.
- נשאר להוכיח רק שתת החבורה כוללת **רק** איברים מהצורה an: נניח בשלילה שקיים איבר m בחבורה שאינו מתחלק ב-n, כלומר ה-ממג"ב שלו עם n - 0<L:=(m,n) הוא קטן מ-n (כי לפי ההגדרה L|n, כלומר L≤n, אבל אם היה מתקיים השוויון אז היה מתקבל ש-n|m בסתירה להנחה). מכיוון ש-n מוגדר כאיבר הקטן ביותר בחבורה, אזי בהכרח L אינו ב-G, ואולם עפ"י משפט ה-ממג"ב, בהכרח קיימים מספרים שלמים a,b כך ש-L=an+bm, וכיוון שכאמור החבורה מקיימת סגירות לחיבור ולכפל בשלמים הרי ש-L שייך ל-G, וקיבלנו סתירה. מכאן, שלא יתכן שקיים m בחבורה שאינו מתחלק ב-n.

- לסיכום - הוכחנו שכל a ב-Z מקיים na שייך ל-G, ושלא קיימים עוד איברים ב-G, ומכאן ש-G היא תת החבורה nZ כנדרש.

חבורות דיהדרליות:

לצורך פישוט החישובים, נתייחס ל-α,β לא כזוויות אלא כמספרי הקודקודים התואמים להן (כל זוית $2\pi k/n$ שבין 0 ל-2π מתאימה באופן חח"ע לקודקוד מסויים ולכן ניתן להחליף בהגדרות. טכנית, ניתן להחליף את ההעתקות S ו-R בהעתקות S' ו-R' הפועלות באופן שקול לחלוטין על מספרי קודקודים. לחלופין אפשר היה להגדיר את i כזווית, אבל קל יותר לראות את הפרמטרים כמספרים שלמים כי כך קל לראות שמדובר בחבורה.

את מספרי הקודקודים נחשב ביחס לציר x ועם כיוון השעון.

א'. פונקציית הסיבוב R - ניתן מיד לראות שזוהי העתקה אדטיבית, כלומר סיבוב ב-α ואחריו סיבוב ב-β שקול לגמרי לסיבוב ב-α+β. ניתן גם לומר ש-R היא טרנספורמציה לינארית של הקודקודים (מקבוצת הקודקודים לעצמה) ועל כן מתקיימת הדרישה - $R_{\alpha+\beta}=R_\alpha+R_\beta$.

שיקוף S - לכל קודקוד i (בין 0 ל-n) "מחליפים צדדים" ביחס לקודקוד α - נסמן לכל קודקוד שמספרו i את ...→i כערכו החדש של i עפ"י ההעתקה.

S_α: $i\rightarrow\alpha-(i-\alpha)=2\alpha-i$

הרכבת העתקות S (סדר ההעתקות הוא מימין לשמאל):

$S_\alpha S_\beta$: $i\rightarrow\alpha-((2\beta-i)-\alpha)=i+2(\alpha-\beta)$ ➔ $S_\alpha S_\beta = R_{2(\alpha-\beta)}$

(אפשר לראות שמתקבלת צורה של סיבוב i→i+..., ולכן ניתן להחליף בהעתקת R שהפרמטר שלה הוא התוספת שקיבלנו $2(\alpha-\beta)$..

ב.

נשתמש באותן הגדרות -

$S_\beta R_\alpha$: $i\rightarrow2\beta-(i+\alpha) = 2(\beta-\alpha/2)-i$ ➔ $S_\beta R_\alpha = S_{\beta-\alpha/2}$

וזו בדיוק הצורה של העתקה S (i→2x-i) ולכן ניתן להחליף בהעתקה $S_{\beta-\alpha/2}$ באותו אופן:

$R_\alpha S_\beta$: $i\rightarrow(2\beta-i)+\alpha = 2(\beta+\alpha/2)-i$ ➔ $R_\alpha S_\beta = S_{\beta+\alpha/2}$

לחלופין ניתן לפתור סעיף זה בדרך שונה בעזרת סעיף א׳:

ניתן לראות גרפית ש-S_α היא ההופכית של עצמה ולכן ביכולתנו לכפול מימין ב-S_β בשני האגפים. כמו כן ניתן לראות גרפית שסיבוב לאחר היפוך שקול לסיבוב זהה אך בכיוון ההפוך לפני אותו היפוך, כלומר $S_\alpha R_\beta = R_{(-\beta)} S_\alpha$ מכאן:

$S_\gamma S_\beta = R_{2(\gamma-\beta)}$ לפי א׳ → $S_\gamma = R_{2(\gamma-\beta)} S_\beta = S_\beta R_{2(\beta-\gamma)}$

כעת אם נסמן $\alpha=2(\beta-\gamma)$ ונבודד את γ נקבל - $2\gamma=2\beta-\alpha$ או $\gamma=\beta-\alpha/2$, כלומר

$S_\beta R_\alpha = S_{\beta-\alpha/2}$

ג.

$S_\alpha R_\beta S_\alpha$: $i \rightarrow 2\alpha - [(2\alpha-i)+\beta] = 2\alpha-2\alpha+i-\beta = i+(-\beta)$ ➔ $S_\alpha R_\beta S_\alpha = R_{-\beta}$

לחלופין, בדרך השניה ניתן להחליף את הסדר

$S_\alpha R_\beta S_\alpha = S_\alpha S_\alpha R_{(-\beta)} = R_{(-\beta)}$

אלגברה מודרנית - 104134 קבוצת תרגול 12

סמסטר אביב 2005 - שיעורי בית מס' 4# - סדר של איבר וחבורות ציקליות

2. צ"ל - $o(ab)=o(ba)$

נגדיר $k:=o(ab)$,$m:=o(ba)$ אזי $(ab)^{o(ab)}=abab...ab=e$.

אם נכפול את שני האגפים משמאל ב-a^{-1}, ומימין ב-a, נקבל

$a^{-1}*abab...ab*a=a^{-1}*e*a=(a^{-1}a)baba...ba = a^{-1}a = e$

$baba....ba=(ba)^{o(ab)}=e$

ומכיוון שבאגף שמאל הורדנו a אחד משמאל והוספנו אחד מימין שמרנו על אותו מספר של $o(ab)$ זוגות, רק שכעת סדרם שונה. מכאן נובע שכאשר נעלה את ba בחזקת $o(ab)$ נקבל את e, כלומר $o(ba)$ (מספר הזוגות המינימלי בסדר החדש) מחלק את $o(ab)$ - אבל לא נוכל להבטיח שהוא בהכרח שווה לו. כדי להוכיח שוויון נפעל בכיוון הפוך, נקח את $baba…ba=e$ (כאשר יש $o(ba)$ זוגות), ונפעיל את אותן פעולות רק עם כפל ב-b וב-b^{-1} משני האגפים, ואז נקבל ש-$o(ab)$ מחלק את $o(ba)$, כלומר $o(ab)|o(ba)$ אבל קודם ראינו ש-$o(ba)|o(ab)$ ולכן הם שווים, משל.

ב. $n:=o(a)$, $m:=o(b)$, $k:=o(ab)$. נתון $(n,m)=1$ וכן $ab=ba$. צריך להוכיח $k=mn$.

לפי הנתונים $a^n=b^m=e$ ← ולכן $(a^n)^m(b^m)^n=e=a^{nm}b^{nm}=ab^{mn}$ ולכן עפ"י משפט **k|mn** (כי k לפי ההגדרה הוא החזקה המינימלית שתתן את e).

כמו כן ידוע ש-$e=(ab)^k$ כלומר אם נכפול בהופכי של b^m נקבל ת

כמו כן, $(ab)^k=e=a^kb^k$ - ניתן להפריד כך כיוון ש-$ab=ba$. מכאן שאם נכפול בהופכי של b^k נקבל ש-$a^k=b^{(-k)}$:

נעלה את שני האגפים בחזקת m :

$(a^k)^m = a^{km} = (b^{(-k)})^m = (b^m)^{-k} = e^{-k} = e$ → $n \mid km$, $(m,n)=1$ אבל → **$n \mid k$**

כלומר מצאנו שיש חזקה של a שנותנת e, ולכן $n=o(a)$ מחלק אותה.

באותו אופן נעלה המשווה מקודם בחזקת n :

$(a^k)^n=(a^n)^k=e^k=e=(b^{(-k)})^n=b^{-kn}$ → $b^{kn}=e$ → $m \mid kn$, $(m,n)=1$ אבל → **$m \mid k$**

(ניתן להוריד את המינוס מהחזקה משום שאם מספר שווה ל-e אז גם ההופכי שלו הוא e).

מאחר שגם n|k וגם m|k, ה-כמק"ב שלהם מחלק אותו גם הוא: [m,n] | k, כיוון ש-k ניתן לפירוק לגורמים ראשוניים שחזקותיהם גדולות או שוות לחזקותיהם בפירוק של n,m, הן גם גדולות מהחזקות של הכמק"ב - כפי שהוכחנו בתרגיל בית מספר 1..). מאחר ש-(m,n)=1 הרי ש-mn=[m,n] (לפי המשפט מתקיים [m,n]=(mn/(m,n) ולכן **mn|k.**

לסיכום - הראנו ש-k|mn, וכן mn|k, ולכן המסקנה הבלתי נמנעת היא ש-k=mn, או במילים אחרות o(ab)=o(a)*o(b) ומש"ל.

3. נתון $aba^{-1}=b^2$, וכן $a^5=e$. (כל פעולות הצמצום וההופכיים בתרגיל זה נובעים מכך ש-G היא חבורה). נעלה את המשוואה הראשונה בריבוע:

$(aba^{-1})^2=(aba^{-1})(aba^{-1})= ab(a^{-1}a)ba^{-1}=ab^2a^{-1} = b^4$

נציב את b^2 מהמשוואה המקורית ונקבל

$b^4 =a(aba^{-1})a^{-1}=a^2ba^{-2}$

נעלה את המשוואה שקיבלנו שוב בריבוע (ונציב בסופה שוב את b^2 שלנו)

$b^8=(a^2ba^{-2})^2=(a^2ba^{-2})(a^2ba^{-2})= a^2b(a^{-2}a^2)ba^{-2}=a^2b^2a^{-2} = a^2(aba^{-1})a^{-2}=a^3ba^{-3}$

באותו אופן:

$b^{16}=(a^3ba^{-3})^2=(a^3ba^{-3})(a^3ba^{-3})= a^3b(a^{-3}a^3)ba^{-3}=a^3b^2a^{-3} = a^3(aba^{-1})a^{-3}=a^4ba^{-4}$

$b^{32}=(a^4ba^{-4})^2=(a^4ba^{-4})(a^4ba^{-4})= a^4b(a^{-4}a^4)ba^{-4}=a^4b^2a^{-4} = a^4(aba^{-1})a^{-4}=a^5ba^{-5}$

אבל בביטוי האחרון נציב $a^5=e$ ונצמצם, כך שנקבל לבסוף $b^{32}=ebe=b$, ונצמצם:

$b^{31}=e$, כלומר **o(b)=31.**

5.

א. בחבורה מסדר סופי קיים איבר מסדר סופי (פרט ל-e): **נכון**

להוכחה נקח a כלשהו בחבורה: מאחר וזו חבורה מתקיימת סגירות ולכן החזקה a^n שייך אף הוא לחבורה לכל n טבעי (למעשה לכל n שלם, אבל נסתפק בטבעיים). אולם מאחר ש-n אינו מוגבל אך החבורה היא סופית קיים מספר סופי של חזקות שונות, או במילים אחרות קיימים u,v טבעיים כך ש-$a^u=a^v$ (נבחר אותם כך ש-u>v). מאחר שזו חבורה נוכל לצמצם ע"י כפל ב- a^{-v} ונקבל

$a^u a^{-v}=a^{u-v}=e$, (u-v הוא חיובי), ומכאן נובע שהסדר של a הוא $o(a)=u-v$ וזהו בהחלט מספר סופי.
הערה - מאחר שלא משנה איזה איבר לקחנו ניתן לטעון טענה חזקה יותר והיא שכל האיברים הם בעלי סדר סופי בחבורה שכזו.

ב. בחבורה מסדר אינסופי קיים איבר מסדר אינסופי: **לא תמיד -**
דוגמה לקיום - $(Z,+)$ - כל האיברים מלבד $e=0$ הם מסדר אינסופי (כלומר לפחות קיים אחד כזה).
אי קיום - נקח את חבורת המספרים המרוכבים שהם שורשי יחידה, כלומר מהצורה - (כלומר $G=\{z \in C \mid z^n=1,\ n\in N\}$), ביחס לכפל. כל המספרים הללו הם בעלי נורמה 1, ואם נמיר לייצוג פולארי נראה שנקבל את הצורה הכללית $z=1*cis(\pi p/q)$ כאשר p/q רציונלי. זוהי חבורה (מקיימת סגירות עפ"י חוקי המרוכבים, ולכל איבר מתקבל ההופכי ע"י הפיכת סימן הארגומנט שלו), והסדר שלה הוא כמספר הרציונלים. עפ"י חוקי החזקות במרוכבים - כל איבר בחבורה אשר נעלה אותו בחזקת q יתן איבר מהצורה $1*cis(qp\pi/q)=cis(p\pi)$, ואם נעלה אותו בריבוע פעם נוספת נקבל $cis(2\pi p)$, כלומר מספר מרוכב בעל ארגומנט שהוא כפולה שלמה של 2π, ולכן זהו 1 (שהוא גם e בחבורה זו). מכאן שלכל איבר a ב-G, $a=cis(p\pi/q)$: $o(a)=2q$, ולכן הוא סופי תמיד.

ג. בחבורה מסדר סופי קיים איבר מסדר אינסופי: **לא נכון**.
כפי שהוכחנו בסעיף א', לכל איבר שנבחר בחבורה סופית נוכל למצוא 2 חזקות זהות (כלומר אם נכפול אותו בעצמו מספיק פעמים נתחיל לחזור על עצמנו), ולכן קיים לו סדר סופי.

ד. בחבורה מסדר אינסופי קיים איבר מסדר סופי (פרט ל-e): **לא תמיד**
דוגמה לקיום - חבורת כל שורשי היחידה (מסדר כלשהו) במרוכבים, ביחס לכפל (ראה סעיף ב').
דוגמה לאי-קיום - $(Z,+)$ - חבורה מסדר אינסופי, וכל מספר שאינו $e=0$, כאשר נחבר אותו לעצמו, ילך ויתרחק מהאפס (יגדל בערכו המוחלט).

ה. מצא חבורה מסדר אינסופי שכל איבר בה הוא מסדר סופי:
חבורת כל שורשי היחידה (מסדר כלשהו) במרוכבים, ביחס לכפל (ראה סעיף ב').

אביב 2005
ליאור

חבורות ציקליות

1. א. תת החבורה הנוצרת ע"י האיבר הנתון היא מאותו סדר של האיבר עצמו (נגדיר n), כיוון שלאחר כפל בעצמו n פעמים נגיע עפ"י הגדרת סדר איבר חזרה ל-e, ובכך סיימנו לבנות את החבורה הציקלית כיוון שהאיברים המתקבלים ע"י חזקות גבוהות יותר או שוות ל-n שקולים למעשה ל-n האיברים הראשונים שקיבלנו.

נבדוק עבור המספר $a=(1+i)/\sqrt{2}$ ע"י העברה לייצוג פולרי ומציאת חזקה שתניב את האיבר הנייטראלי (1 כי מדובר בכפל רגיל).

$$a=\sqrt{2}*cis(\pi/4)/\sqrt{2} = cis(\pi/4) \rightarrow a^8=1^8*cis(8*\pi/4)=cis(2\pi)=1$$

זוהי החזקה הראשונה שנותנת את התוצאה 1 (ניתן לראות גרפית שכל חזקה מסובבת את המספר $\pi/4$ על מעגל היחידה).

ב. נפעיל תהליך דומה על האיבר $1+i$: $b=\sqrt{2}*cis(\pi/4)$. ניתן לראות שככל שנעלה את b בחזקות גבוהות יותר, הנורמה שלו תלך ותגדל (בעוד שהארגומנט יבצע כמו בסעיף הקודם קפיצות במחזוריות של 8), ולכן לעולם לא נוכל להגיע חזרה לאיבר הנייטראלי 1. מכאן נובע שסדר האיבר $1+i$ הוא אינסוף, ולכן שסדר תת החבורה שהוא יוצר הוא אינסוף (כי כאמור לכל חזקה שנקח ל-b נקבל מספר חדש, בלא חזרות.

5. U_n היא חבורת המחלקות הזרות ל-n ביחס לכפל:

א. $U_8=\{ [1], [3], [5], [7] \}$, כיוון שהמספרים 1,3,5,7 מייצגים כל אחד מחלקה שאיבריה שקולים זה לזה (מודולו 8), וכולם זרים ל-8. בכדי שחבורה זו תהיה ציקלית יש להראות שניתן ליצור אותה מאחד האיברים שבה (באמצעות פעולת הכפל, כאמור). 1 הוא האיבר הנייטראלי ולכן מחלקת השקילות שלו לא מסוגלת ליצור אף מספר מלבד 1 עצמו - $1^n=1 \pmod 8$ לכל n.

באותו אופן $3^2=9\equiv 1 \pmod 8$, $3^3=27\equiv 3$. ניתן לראות שמחלקת השקילות [3] לא יכולה לחרוג מתת החבורה $\{1,3\}$ וליצור את U_8 כולה.

$5^2=25\equiv 1 \pmod 8$, $5^3=125\equiv 5$ ולכן מחלקת השקילות [5] יכולה ליצור רק את תת החבורה $\{1,5\}$.

$7^2=49\equiv 1 \pmod 8$, $7^3=343\equiv 7$ ולכן מחלקת השקילות [7] יכולה ליצור רק את תת החבורה $\{1,7\}$.

המסקנה - ב-U_8 אין אף איבר שיוצר אותה, ולכן היא אינה ציקלית.

ב. החבורה U_9 כוללת את { [1],[2].[4].[5].[7].[8] } (רק 3,6 אינם זרים ל-9). נחפש ביניהם יוצרים (נתייחס למחלקות כאל נציגיהן בין 0 ל-9). סדר החבורה הוא $|U_9|=6$

האיבר [1] אינה יוצרת מאותה סיבה שנאמרה בסעיף הקודם - מאחר ש-1 הוא הנייטראלי, כל החזקות שלו שוות אליו ולא מסוגלות ליצור את החבורה כולה.

האיבר [2] מסוגל ליצור את שאר החבורה (אם נבחר כל נציג של המחלקה):

$2^0=\mathbf{1}, 2^1=\mathbf{2}, 2^2=\mathbf{4}, 2^3=\mathbf{8}, 2^4=16\equiv\mathbf{7}, 2^5=32\equiv\mathbf{5} \pmod 9$

החל מהחזקה השישית אנו חוזרים לאיבר הנייטראלי $2^6=64\equiv\mathbf{1} \pmod 9$

$o([2])=6$, $\mathbf{<[2]>=\{[1],[2],[4],[5],[7],[8]\}=U_9}$

גם האיבר [5] מסוגל ליצור את שאר החבורה:

$5^0=\mathbf{1}, 5^1=\mathbf{5}, 5^2=25\equiv\mathbf{7}, 5^3=125\equiv\mathbf{8}, 5^4=625\equiv\mathbf{4}, 5^5=3125\equiv\mathbf{2} \pmod 9$

החל מהחזקה השישית אנו חוזרים לאיבר הנייטראלי $5^6=15625\equiv\mathbf{1} \pmod 9$

$\mathbf{o([5])=6}$, $\mathbf{<[5]>=\{[1],[2],[4],[5],[7],[8]\}=U_9}$

ניתן לראות שהאיברים שהם בעלי סדר זהה לסדר החבורה $\{2,5\}$ הם יוצרים שלה, משום שאם $n:=o(a)$ אז לאיבר a בהכרח קיימות בדיוק n חזקות שונות $\pmod 9$ שכולן בחבורה (בגלל הסגירות) ולכן מהווים את החבורה כולה (כיוון שיש בה n איברים). כך, אם סדר האיבר שונה מסדר החבורה, כלומר יש לו פחות מ-n חזקות שונות הוא יוכל ליצור לכל היותר תת חבורה ציקלית בתוך אותה חבורה (אם הוא עצמו מסדר סופי, כלומר אחת החזקות השונות שלו היא האיברה נייטראלי).

מכאן שעלינו למצוא מהו הסדר של שאר האיברים בחבורה U_9:

ולכן כאמור הוא לא יכול ליצור את החבורה כולה, אלא תת חבורה $o([1])=1$

$<[1]>=\{[1]\}$

$4^2=16\equiv 7$ $4^3=64\equiv 1$ → $o([4])=3$; $7^2=49\equiv 4$ $7^3=343\equiv 1$ → $o([7])=3$;

כלומר 4 ו-7 יוצרים כל אחד רק את תת החבורה - $<[4]>=<[7]>=\{[1],[4],[7]\}$

$8^2=64\equiv 1 \rightarrow o([8])=2 \rightarrow <[8]>=\{[1],[8]\}$

מצאנו כבר שהם יוצרים את כל החבורה **$o([2])=6, o([5])=6$**

תרגילי סיכום

4. נתון ש-2,7 נמצאים בחבורה H. מכיוון שהפעולה היא חיבור, ההופכיים 7-,2- מצויים גם הם ב-H. מכיוון שמתקיימת סגירות בחבורה, אם נחבר את איבר a (השייך ל-H) לעצמו n פעמים, נקבל תוצאה an שאף היא בחבורה - לכל a בחבורה ולכל n טבעי, ומכיוון שיש לנו גם את ההופכי a-, הדבר נכון גם ל-n שלילי (ואם n=0 אז na=0=e וגם תוצאה זו היא בחבורה), כלומר מתקיימת סגירות לכפל איבר בכל מספר שלם.

נמצא את ה-ממג"ב - $(2,7)=1$ (שני המספרים הם ראשוניים ולכן ברור שהם זרים). עפ"י המשפט קיימים מספרים שלמים a,b כך ש- $(2,7)=2*a+7*b=1$, אבל הוכחנו ש-2a וש-7b גם הם בחבורה, ולכן לפי הסגירות לחיבור גם $2a+7b=1$ בחבורה.

מאחר ש-1 שייך לחבורה, לפי מה שהוכחנו גם כל כפולה שלו במספר שלם היא בחבורה, כלומר לכל $n\epsilon Z \leftarrow 1*n=n\epsilon H$ ומכאן ש-Z מוכלת בתוך H, אבל נתון ש-H היא תת חבורה של השלמים ולכן H מוכלת בתוך Z, ומשני התנאים הללו נובע משל $Z=H$.

אביב 2005
ליאור

אלגברה מודרנית - 104134 קבוצת תרגול 12
סמסטר אביב 2005 - שיעורי בית מס' 5# - לגראנז' וחברים

.6

א. מאחר ש-p ראשוני, Up היא מהצורה $Up=\{[1],[2],\ldots[p-1]\}$ כלומר $\{[1],[2],[3]\ldots[2^n]\}$ (משום שכל האיברים זרים ל-p), ולכן גודלה - $|Up|=2^n$.
ידוע ש-$p=2^n+1$, כלומר $2^n=p-1$. נכפול את שני האגפים ב-2^n, ונקבל

$$(2^n)^2=2^n(p-1)=p\cdot 2^n - 2^n \equiv -2^n \equiv 1(\text{mod } p)$$

ומכאן ש-$[2]^{2n}\equiv 1=e$ (כי 2 מייצג את המחלקה [2]), כלומר הסדר של [2] יהא אשר יהא מחלק את 2n. נבדוק האם יתכן שהסדר של [2] קטן מ-2n -נגדיר ש-$a:=o([2])$, ונניח $2n=a*q$ בהתאם למה שקיבלנו קודם (q מספר שלם חיובי) - אם $q\geq 2$ אז $a\leq n$, אבל $2^a\leq p-1<p$ ולכן לא שקול ל-1 מודולו p. על כן נדרש ש- $a>n$, ומכאן שבהכרח $q<2$ כלומר $q=1$ ולכן $a=2n$ - הסדר של [2] הוא 2n.

ב.

נגדיר את H בתור תת החבורה הציקלית הנוצרת ע"י [2], כלומר $H=\langle[2]\rangle$. הסדר של האיבר [2] הוא כמו סדר תת החבורה הזו : $|H|=o([2])$., ולכן לפי משפט לגראנז' מחלק את סדר החבורה כולה כלומר $2n \mid 2^n \leftarrow o([2]) \mid 2^n$, ואם נצמצם ב-2 נקבל $n \mid 2^{n-1}$, ומכאן שקיים q שלם כך ש-$q*n=2^{n-1}$ $\leftarrow$ $q=2^{n-1}/n$. ומכאן ש-n חייב להיות גם הוא חזקה של 2 (קטנה שווה ל-2^{n-1}) כדי ש-q אכן יהיה שלם.

14. יהי איבר a בחבורה G. מאחר שהסדר של חבורה G הוא זוגי (10) אנו יודעים בוודאות שיש לה לפחות איבר אחד מסדר 2, כיוון שאם נחלק את G לזוגות של איברים יחד עם ההופכיים שלהם e יעמוד בפני עצמו כי הוא שווה להופכי שלו, ונשאר עם 9 איברים נוספים שיש לחלק לזוגות (לא תתכן חפיפה בין זוגות כיוון ש-$(a^{-1})^{-1}=a$), כך שבהכרח לפחות עבור אחד מהם מתקיים שהוא שווה להופכי של עצמו - $b=b^{-1}$. לכן, אם נכפול את שני האגפים ב-b נקבל $b^2=e$, ומצאנו איבר מסדר 2. מאחר שיש איבר מסדר 2, תת החבורה הציקלית שהוא יוצר $\langle b\rangle$ היא מסדר 2 (מאחר שהיא כוללת את $\{e,b\}$, וכל כפל נוסף ב-b יחזיר אותנו לשני איברים אלה).
כעת אנו רוצים לבדוק האם קיימים איברים מסדרים אחרים. מאחר שלפי המשפט לכל a בחבורה מתקיים $a^{|G|}=a^{10}=e$, הסדר של כל איבר חייב לחלק את 10. אם

נבחר a שאינו e, הסדר שלו יכול להיות 2,5 או 10 (הוא אינו 1 כיוון שאז a=e בסתירה לאיבר שבחרנו). מאחר שכבר מצאנו איבר מסדר 2, נראה האם יתכן מצב בו אין אף איבר מסדר 5:

נניח בשלילה שכל האיברים בסדרה הם מסדר 2 (מלבד e כאמור לעיל): ננסה למצוא תת חבורה - נקח a ו-b שונים (שאינם הופכיים זה לזה), וכדי לקיים את תנאי תת החבורה גם את e. כדי לקיים סגירות גם ab יהיה בתת החבורה (נבדוק את ba בהמשך). מאחר שכל אלה הם איברים מסדר 2, כל איבר יהיה ההופכי של עצמו, למשל $aa^{-1}=a^2=e \leftarrow a=a^{-1}$ (ניתן לצמצם כי אלה איברים ב-G שהיא חבורה). ולכן כל ההופכיים גם הם בחבורה. לבסוף - נראה שהאיבר ba מצוי גם הוא בתת החבורה - נניח שהוא מצוי בה, ונכפול אותו ב-ab: $ab*ba=a(b^2)a=aea=a^2=e$, ולכן ba הוא ההופכי של ab, אבל מצאנו כבר ש-ab הוא מסדר 2 ולכן ההופכי של עצמו, כך שנובע ab=ba וזו היא תת חבורה אבלית.

אם כן, החבורה שמצאנו היא {e,a,b,ab}, והוכחנו שהיא תת חבורה חוקית, אולם היא מסדר 4 ולכן מתקיימת סתירה למשפט לגראנז', כיוון ש-4 אינו מחלק את |G|=10. מכאן שהנחת השלילה שגויה, ולא כל האיברים (פרט ל-e) הם מסדר 2. מאחר שלא כל האיברים הם מסדר 2 (מלבד e), קיים לפחות איבר אחד שסדרו הוא אחת האפשרויות שנותרו - יתכן שהוא מסדר 5 (ולכן קיימת חבורה מסדר 5 - ראה בהמשך). לחלופין, יתכן שקיים איבר מסדר 10 (נקרא לו c). במקרה זה G היא חבורה ציקלית, כיוון שיש בה איבר שסדרו זהה לסדר החבורה, ולכן G=<c> (הוא יוצר שלה). כעת ניתן לקחת את c^2: $(c^2)^5=c^{10}=e$ כלומר הסדר של c^2 הוא 5. (באותו אופן ניתן לומר ש c^5 הוא מסדר 2, למרות שכבר הוכחנו שקיים כזה איבר). מכאן שאם יש איבר שהסדר שלו הוא 10, חייב להיות איבר (ריבועו) שהסדר שלו הוא 5.
הוכחנו שבכל מקרה קיים איבר מסדר 5, ולכן (בדומה לאיבר מסדר 2) - הוא יוצר תת חבורה ציקלית מסדר 5. בשורה התחתונה - בכל מקרה קיימות לפחות תת חבורה אחת מסדר 2 ואחת מסדר 5.

16. G היא חבורה מסדר 33. נראה שיש בה איבר מסדר 3.

בדומה לשאלה הקודמת, יהי a איבר בחבורה G (שאינו e). לפי משפט שהוכחנו $a^{|G|}=a^{33}=e$, לכן הסדר של a מחלק את 33 (o(a)|33). נחלק למקרים: לא יתכן שהסדר של a הוא 1 כי a שונה מ-e. אם הסדר של a הוא 3, מצאנו את האיבר המבוקש ולכן סיימנו. אם הסדר הוא 33, נקח את $b=a^{11}$ ועפ"י חוקי החזקות $b^3=a^{33}=e$ ולכן מצאנו איבר מסדר 3.

האפשרות השלישית והאחרונה היא שהסדר של a הוא 11, כלומר $a^{11}=e$. במקרה זה נביט על החבורה <a> - זו תת חבורה ציקלית מסדר 11, כלומר יש בה 11 איברים - כל אחד מהם הוא מסדר 11 (מלבד e שהוא מסדר 1), כיוון שלפי לגראנז' הסדר של כל איבר בתת החבורה <a> צריך לחלק את הסדר של <a> כלומר את 11, וזהו מספר ראשוני (ואף איבר מלבד e לא יכול להיות מסדר 1).

כעת נמשיך "למפות" את סדרי האיברים ב-G ע"י חלוקה לעוד תתי חבורות. כיוון שתתי חבורות שונות מסדרים ראשוניים (ובפרט 11 במקרה זה) לא יכולות להחתך אחת עם השניה מלבד ב-e (הוכחנו בכיתה שכל חיתוך חבורות הוא תת חבורה, ולכל חבורה מסדר p ראשוני יכולה להיות תת חבורה רק מסדר p או 1, כלומר אם תתי החבורות אינן זהות, אזי החיתוך הוא e בלבד). מכך נובע שכל איבר שנשייך לתת חבורה מסויימת ימצא אך ורק בה (מלבד e כמובן) ולכן נוכל לחלק את G לתתי חבורות ללא חפיפה.

נניח שקיים b נוסף מסדר 11, שאינו ב-<a>. b הוא יוצר לתת חבורה ציקלית נוספת מסדר 11, ולכן הורדנו 10 איברים נוספים מסך האיברים ב-G (ללא e), כך שכעת נותרו לנו 13 איברים (כולל e). אילו לא היה קיים b כזה, משמעות הדבר היא ששאר האיברים שנותרו ב-G (כלומר כל אלה שאינם ב-<a>) הם מסדר 3 או 33, ובמקרים אלה הוכחנו שבהכרח שקיים לפחות איבר אחד מסדר 3.

נבחר באותו אופן איבר נוסף - c - מסדר 11 שאינו ב-<a> או ב-<b> (גם כאן - אם לא קיים c כזה אזי בהכרח נותרנו עם איברים שסדרם 3 או 33 וסיימנו). בחבורה הציקלית הנוצרת ע"י c יהיו 11 איברים - 10 מהם מסדר 11 והאיבר הנוסף הוא e, כלומר הורדנו 10 נוספים מ-G (ללא e) ולכן נותרנו ב-G עם 3 איברים שאינם מסדר 11 - בהם e (כאמור, לא יתכן שהם חלק מתת חבורה נוספת החופפת לאחת מתתי החבורות הקיימות כיוון שהוכחנו שאין חפיפות. שני האיברים האחרים הם מסדר 3

או 33, ולכן, לפי האמור לעיל - בכל מקרה קיים לפחות איבר אחד מסדר 3 (למעשה 3 האיברים שנותרו - הכוללים את e - יהוו תת חבורה מסדר 3).

.18

א. צ"ל שבחבורה מסדר 8 יש תת חבורה מסדר 2.בדומה לשאלה א', נקח את החבורה ונחלק אותה לזוגות - מספר יחד עם ההופכי שלו. e הוא ההופכי של עצמו ולכן ימצא לבדו, ומכאן שנותר מספר אי זוגי (שבעה במקרה זה) איברים שיש לסדר בזוגות. כמו כן לא יתכן חיתוך/חפיפה בין זוגות כאלה כיוון ש-$a=(a^{-1})^{-1}$, כלומר ההופכי של ההופכי הוא תמיד המספר המקורי עצמו (במילים אחרות ההעתקה להופכיים היא חח"ע). מכאן שלפחות איבר אחד בהכרח יוותר ללא בן זוג מבין האחרים, ומכיוון שחייב להיות לו הופכי הוא יאלץ להיות ההופכי של עצמו - נסמן $b=b^{-1}$. מכאן שאם נכפול ב-b את שני האגפים נקבל $b^2=e$ ולכן מצאנו איבר מסדר 2 - תת החבורה הציקלית שהוא יוצר $<b>=\{e,b\}$ היא תת חבורה מסדר 2 (יש לה את e, שני האיברים בה הם ההופכיים של עצמם, ומתקיימת כאמור סגירות eb=b (b*b=e*e=e).

ב. G היא מסדר 15 ויש לה תת חבורה יחידה מסדר 3 (נכנה H) ותת חבורה יחידה מסדר 5 (נכנה I). לפי משפט לגראנז' כל תת חבורה חייבת להיות מסדר שיחלק את סדר G כלומר את 15.

נראה שהחיתוך בין החבורות הוא $\{e\}$ - כל חיתוך של חבורות הוא תת חבורה, אולם כל תת חבורה של 3 או של 5 חייבת להיות מסדר שיחלק גם את 3 וגם את 5, ולכן חייבת להיות מסדר 1 כלומר להיות בדיוק $H\cap I=\{e\}$ (e אכן מצוי בשניהם לפי ההגדרה כי הן תתי חבורות של G). לכן, סך האיברים המצוי בשתי תתי החבורות הוא $|H\ U\ I|=3+5-1=7$ (e מצוי בשתיהן, ויש לספור אותו רק פעם אחת), כלומר נותרו 8 איברים שאינם באף תת חבורה.

נקח איבר a ב-G שאינו מצוי באף אחת מהחבורות (אחד מאותם 8) - הוא אינו מסדר 3 ואינו מסדר 5, כיוון שאז החבורה הציקלית שהיה יוצר - <a> - היתה מאותו סדר ולכן שווה ל-H או ל-I (בהתאמה) כי נתון שהן החבורות היחידות מסדרים אלה, אולם אז גם a היה שייך לאחת מהן בסתירה להנחה. a גם שונה מ-e ולכן אינו מסדר 1.

לפי המשפט הסדר של a מחלק את הסדר של G, כלומר o(a)|15, אולם ראינו שהסדר אינו 1,3,5, ולכן נותרה רק האפשרות שהסדר של a יהיה 15. כלומר מצאנו איבר שהסדר שלו שווה לסדר של החבורה G כולה, כלומר G=<a> (כי החבורה <a> מסדר 15 מוכלת ב-G מאותו סדר), כלומר a יוצר את G ולכן G היא חבורה ציקלית, ומשל.

משפט השאריות הסיני

יש למצוא x שמקיים :

$x=2+7a \leftarrow x\equiv 2 \pmod 7$

$x=3+4b \leftarrow x\equiv 3 \pmod 4$

$x=4+9c \leftarrow x\equiv 4 \pmod 9$

ניתן לראות ש-x כזה אינו יחיד בכל Z, אלא רק בתחום שקטן מ-M=7*4*9=252, (רמז לכך ניתן ע"י המשפט עצמו המגביל את התחום של x ל-M), כיוון שכל הגדלים המגדירים את החבורות שלעיל מחלקים אותו, ולכן כל החבורות חוזרות על עצמן אחריו. מאחר שגדלים אלה הם זרים בזוגות (1=(4,9)=(7,4)=(7,9)), הרי ש-M הוא המספר הקטן ביותר המאפשר זאת.

- כשלב ביניים נמצא x שיקיים (x mod 7)=2, וגם (x mod 9)=(x mod 4)=0.
מספר כזה צריך להיות כפולה של 36=9*4, ולכן נעבור על הכפולות של 36 :
(36 mod 7)=1, (72 mod 7)=2. לכן x=72.

- כעת נמצא y שיקיים (y mod 4)=3 אבל (y mod 9)=(y mod 7)=0, כלומר הוא כפולה של 63=9*7 : (63 mod 4)=3, לכן y=63.

- לבסוף - z שיקיים (z mod 9)=4, ובמקביל (z mod 4)=(z mod 7)=0, כלומר z הוא כפולה של 28=4*7 : (28 mod 9)=1 כדי למצוא שארית גדולה פי 4 נכפול את 28 פי 4 : (112 mod 9)=(28*4 mod 9)=4, לכן z הוא 112.

כעת, המספר המבוקש, לפי משפט השאריות הסיני, הוא

(2x+3y+4z mod 252)=(144+189+448 mod 252)=(751 mod 252)=247

ואכן (247 mod 7)=2, (247 mod 9)=4, (247 mod 4)=3.

אביב 2005
ליאור

נוסחת אוילר

א. המספר n הוא למעשה מספר המספרים בתחום 0…n-1. עפ"י ההגדרה $\varphi(n)$ הוא מספר המספרים הזרים ל-n באותו תחום, ולכן ההפרש בין השניים שבאגף שמאל, צריך להיות **מספר המספרים <u>שאינם</u> זרים ל-n בתחום זה,** כלומר בפירוק למספרים ראשוניים יש להם לפחות גורם משותף אחד עם n - $H=|\{x \mid (x,n)>1,\ 0\le x\le n-1\}|$.

עפ"י הגדרת החבורה A_i, היא כוללת את כל המספרים שהמספר הראשוני p_i מחלק אותם, כלומר את כל הכפולות של p_i בתחום - משמע זוהי חבורה ציקלית: $A_i=<p_i>$. מאחר ש-n מורכב ממכפלת כל הראשוניים הללו- $\prod p_i$ כאשר $1\le i\le k$, הרי שאיחוד כל הקבוצות A_i בתחום זה נותן את כל הכפולות הכוללות לפחות אחד מהמספרים הראשוניים המרכיבים את n, כלומר את כל המספרים שמתחלקים ב-p_i כלשהו ולכן יש להם מחלק משותף עם n. מכאן שגם באגף ימין קיבלנו בדיוק את מספר המספרים שאינם זרים ל-n בתחום 0…n-1 (אותו |H| ממקודם)

ב.

נגדיר $M=p_1\cdot p_2\cdot p_3\cdots p_k$

$$M=\prod_{i\in I} p_i$$

$$\left|\bigcap_{i\in I} A_i\right| = \left|\{x \mid 0\le x<n,\ M \mid x\}\right|$$

באגף שמאל - חיתוך כל הקבוצות A_i עבור i בתחום I - מתקבלת קבוצת המספרים בתחום {1...n} **שכל** המספרים הראשוניים p_i (i בתחום I) מחלקים אותם - כלומר M מחלק אותם. מכאן שאגף שמאל הוא מספר המספרים בתחום {1…n} המתחלקים ב-M, כלומר כל המספרים מהצורה qM (כאשר q שלם) בתחום. מכאן ש-A_i היא חבורה ציקלית והיוצר שלה הוא M, ולפי לגראנז', סדר חיתוך החבורות הוא n/M (ואכן M|n כי הוא מורכב מכל האיברים הראשוניים שהיו ב-n, שחזקותיהן מסדר 1). אם נציב חזרה את M מלמעלה זהו בדיוק אגף ימין.

ג. קודם נפתור את השוויון הימני, בנפרד עבור כל מספר ראשוני המרכיב את n. נעשה שימוש בסעיף א' כשהוא "מנוון" כלומר רק עבור מקרה פרטי בו ניתנת חבורת A_i בודדת כל פעם (כך שאין צורך באיחוד באגף ימין).

$$p_i^{\alpha_i} - \varphi_{(p_i^{\alpha_i})} = \left|A_i\right| = p_i^{\alpha_i} \Big/ p_i = p_i^{\alpha_i - 1}$$

$$\varphi_{(p_i^{\alpha_i})} = p_i^{\alpha_i} - p_i^{\alpha_i - 1}$$

כעת נותר להוכיח שהפונקציה φ מקיימת φ(ab)=φ(a)*φ(b) (לכל a,b זרים כמו במקרה שלנו, אין צורך לבדוק עבור מקרה אחר אך ניתן לנחש שזה לא יעבוד), ולכן ניתן להפריד את n למכפלת מרכיביו הראשוניים, ולהפעיל את φ על כל אחד מהם בנפרד (ורק אח״כ לכפול את כולם יחד):

נציב את הנוסחה שמצאנו ב-א׳ עבור φ, נחליף את האיחוד עפ״י משפט ההכלה וההדחה הנתון (עבור 2 קבוצות), ובסוף נחליף את סדר החיתוך לפי סעיף ב׳.

$$\tilde{n} := p_i^{\alpha_i} \cdot p_j^{\alpha_j}$$

$$\varphi_{(\tilde{n})} = \tilde{n} - \left|A_i \bigcup A_j\right| = \tilde{n} - \left|A_i\right| - \left|A_j\right| + \left|A_i \bigcap A_j\right| = \tilde{n} - \frac{\tilde{n}}{p_i} - \frac{\tilde{n}}{p_j} + \frac{\tilde{n}}{p_i p_j}$$

$$= \tilde{n} \cdot \left(1 - \frac{1}{p_i} - \frac{1}{p_j} + \frac{1}{p_i p_j}\right) = p_i^{\alpha_i} \cdot p_j^{\alpha_j} \left(1 - \frac{1}{p_i} - \frac{1}{p_j} + \frac{1}{p_i p_j}\right)$$

$$\varphi_{(p_i^{\alpha_i})} = p_i^{\alpha_i} - \left|A_i\right| = p_i^{\alpha_i} - \frac{p_i^{\alpha_i}}{p_i} = p_i^{\alpha_i}\left(1 - \frac{1}{p_i}\right)$$

$$\varphi_{(p_j^{\alpha_j})} = p_j^{\alpha_j} - \left|A_j\right| = p_j^{\alpha_j} - \frac{p_j^{\alpha_j}}{p_j} = p_j^{\alpha_j}\left(1 - \frac{1}{p_j}\right)$$

$$\varphi_{(p_i^{\alpha_i})} \cdot \varphi_{(p_j^{\alpha_j})} = p_i^{\alpha_i} p_j^{\alpha_j} \cdot \left(1 - \frac{1}{p_i}\right)\left(1 - \frac{1}{p_j}\right) = p_i^{\alpha_i} p_j^{\alpha_j} \left(1 - \frac{1}{p_i} - \frac{1}{p_j} + \frac{1}{p_i p_j}\right)$$

ולכן ניתן לראות שעבור כל שני אלמנטים ראשוניים בחזקות מסויימות $\varphi_{(p_i^{\alpha_i})} \cdot \varphi_{(p_j^{\alpha_j})} = \varphi_{\left(p_i^{\alpha_i} p_j^{\alpha_j}\right)}$. מכאן, ניתן לכפול באיברים ראשוניים נוספים (ניתן להוכיח באינדוקציה) ולקבל לבסוף את מכפלת כל האלמנטים הראשוניים המרכיבים את n:

$$\varphi_{(n)} = \varphi_{\left(\prod_{i=1}^{k} p_i^{\alpha_i}\right)} = \varphi_{(p_1^{\alpha_1})} \cdot \varphi_{(p_2^{\alpha_2})} \cdots \varphi_{(p_k^{\alpha_k})} = \prod_{i=1}^{k} \varphi_{(p_i^{\alpha_i})}$$

וזהו השוויון השמאלי ולכן מש״ל

אביב 2005
ליאור

אלגברה מודרנית - 104134 קבוצת תרגול 12
סמסטר אביב 2005 - שיעורי בית מס' 6# - תמורות

4. הצמדת תמורות:

$\tau=(5\ 6)(1\ 3)$, $\sigma=(1\ 2)(3\ 4)$

א. נדרש $a^{-1}\sigma a=\tau$ כלומר $\sigma a=a\tau$. לכן, לכל n,m המקיימים $\tau_{(n)}=m$ מתקיים (אם נפעיל את שתי ההעתקות על איבר n): $a\tau_{(n)}=a_{(m)}=\sigma a_{(n)}=\sigma(a_{(n)})$, כלומר ההעתקה σ צריכה להעתיק את $a_{(n)}$ ל-$a_{(m)}$. מכאן ניתן לבנות את ההעתקה:

$\sigma(a_{(1)})=a_{(3)}$ ← $\tau_{(1)}=3$

$\sigma(a_{(3)})=a_{(1)}$ ← $\tau_{(3)}=1$ ומכיוון שיצרנו פה מעגל מסדר 2 נוכל לבחור למשל את המעגל $(1\ 2)$ המרכיב את σ, כך ש-$a_{(1)}=2\ a_{(3)}=2$.

$\sigma(a_{(5)})=a_{(6)}$ ← $\tau_{(5)}=6$ באותו אופן

$\sigma(a_{(6)})=a_{(5)}$ ← $\tau_{(6)}=5$ ונקח את המעגל השני ב-σ כך שנקבל $a_{(5)}=3\ a_{(6)}=4$

את האיברים שנותרו ב-a נבחר שרירותית ממה שנשאר - $a_{(4)}=6\ a_{(2)}=5$, ולסיכום:

$a=\begin{pmatrix}1&2&3&4&5&6\\1&5&2&6&3&4\end{pmatrix}$ או במעגל - $a=(2\ 5\ 3)(4\ 6)$, ולכן ההעתקה ההפוכה היא:

$a^{-1}=\begin{pmatrix}1&2&3&4&5&6\\1&3&5&6&2&4\end{pmatrix}$ או במעגל $a^{-1}=(2\ 3\ 5)(4\ 6)$.

ניתן לראות ש-$a^{-1}\sigma a(1)=a^{-1}\sigma(1)=a^{-1}(2)=3=\tau(1)$

$a^{-1}\sigma a(2)=a^{-1}\sigma(5)=a^{-1}(5)=2=\tau(2)$

$a^{-1}\sigma a(3)=a^{-1}\sigma(2)=a^{-1}(1)=1=\tau(3)$

$a^{-1}\sigma a(4)=a^{-1}\sigma(6)=a^{-1}(6)=4=\tau(4)$

$a^{-1}\sigma a(5)=a^{-1}\sigma(3)=a^{-1}(4)=6=\tau(5)$

$a^{-1}\sigma a(6)=a^{-1}\sigma(4)=a^{-1}(3)=5=\tau(6)$

*תשומת לב לכך שיש מספר תשובות אפשריות.

ב. רעיון כללי - אם ננסה לפעול באותה שיטה כמו בסעיף הקודם נגלה שעבור כל מעגל ב-τ (ההעתקה באגף ימין) נזדקק למעגל באותו גודל ב-σ (ההעתקה ההנתונה באגף שמאל לפני ההרכבה).

נניח בשלילה שניתן למצוא העתקה מצמידה a -

הסדר של איבר n כלשהו תחת ההעתקה τ הוא בדיוק גודל המעגל בו הוא מופיע (כיוון שהפעלה חוזרת של τ עליו תביא אותו למקום המקורי לאחר מספר פעמים השווה לגודל המעגל שלו. אם האיבר אינו מופיע באף מעגל הסדר שלו הוא 1). לכן, מאחר שנדרש שהרכבת ההעתקות באגף שמאל תתן העתקה זהה ל-τ, הרי שגם באגף ימין נדרש שהסדר של n תחת ההעתקה המורכבת יהיה זהה, ואולם לפי משפט סדר של איבר תחת הרכבת העתקות הוא ה-כמק"ב של סדריו תחת כל אחת מההעתקות בנפרד (σ, a, ו-a^{-1} שהסדר שלו תחתיה זהה לסדרו תחת a כי היא מורכבת ממעגלים זהים בכיוון הפוך). נקח למשל את האיבר 1 - תחת τ הסדר שלו הוא בדיוק 2, ואילו תחת ההעתקה המורכבת הסדר שלו יהיה כפולה של 3, ולכן קיבלנו סתירה.

6.

א. $\begin{pmatrix}12345\\31245\end{pmatrix}=\begin{pmatrix}12345\\21345\end{pmatrix}\begin{pmatrix}12345\\32145\end{pmatrix}$ ההעתקה שקולה למעגל (2 3 1) ולכן הסדר הוא 3

ב. $\begin{pmatrix}12345\\14325\end{pmatrix}=\begin{pmatrix}12345\\42315\end{pmatrix}\begin{pmatrix}12345\\41325\end{pmatrix}^{-1}=\begin{pmatrix}12345\\21345\end{pmatrix}\begin{pmatrix}12345\\41325\end{pmatrix}\begin{pmatrix}12345\\41325\end{pmatrix}^{-1}$

הסדר הוא 2 כיוון שרק 2 ו-4 מחליפים מקומות כל פעם (המעגל הוא (4 2)).

ג. נתרגם למעגל - (6 5 4 3 2 1) וכעת קל יותר לראות שכל איבר עובר לבא אחריו ולכן הסדר הוא 6.

10. נשים לב שהתמורה $\begin{pmatrix}123456789\\312ab7896\end{pmatrix}$ כוללת למעשה את שתי המעגלים (9 8 7 6)(2 3 1), ואילו האיברים 4,5 הם זרים לשני המעגלים הללו. קיימות שתי a=4, b=5, ואז התמורה שווה לשני המעגלים הללו בלבד, או a=5, b=4, ואז התמורה שווה ל-(5 4)(9 8 7 6)(2 3 1). נפרק לטרנספוזיציות:

אי זוגי → (6 7)(6 8)(6 9)(1 3)(1 2) = (6 7 8 9)(1 3 2)

זוגי→ (4 5)(6 7)(6 8)(6 9)(1 3)(1 2)=(4 5)(6 7 8 9)(1 3 2)

ולכן נבחר a=5, b=4 ונקבל את התמורה השניה שהיא הזוגית.

13. a=(1 2 3)

$C_{s3}(a)=\{a^2,a,1\}$, כיוון שכפל בתמורת הזהות (1) קומוטטיבי עפ"י הגדרת החבורה, כפל a בעצמו קומוטטיבי גם הוא, וכפל ב-a^2=(1 3 2) (שיתן את תמורת הזהות כי הסדר של a הוא 3) גם הוא קומוטטיבי כי (a*a)*a=a*(a*a).

ניתן לומר אם כן ש- $C_{s3}(a)=<a>$, ויש בכך הגיון כיוון שלא ניתן למצוא תמורה מסדר 3 שזרה ל-a ולכן מתחלפת איתה בכפל.

דרך ב' - נשתמש בכללי הצמידות: התחלפות בכפל מחייבת שכל איבר ברכז של a יצמיד את a לעצמו: $xa=ax \Leftrightarrow xax^{-1}=a$. כעת, מתקיים כלל הצמידות הקובע $xax^{-1}=(x_{(a1)}, x_{(a2)},\dots x_{(an)})$, ולכן גם $a=(x_{(a1)}, x_{(a2)},\dots x_{(an)})$, ובמקרה של S3 - $a= (x_{(1)},x_{(2)},x_{(3)})$. אם נכתוב את a כמעגל יש לבדוק את כל ה"הסטים" שלו (השקולים זה לזה) - (1 2 3), (2 3 1), (3 1 2):

$a=(1\ 2\ 3)$: $x_{(1)}=1, x_{(2)}=2, x_{(3)}=3 \rightarrow x=1$

$a=(2\ 3\ 1)$: $x_{(1)}=2, x_{(2)}=3, x_{(3)}=1 \rightarrow x=a$

$a=(3\ 1\ 2)$: $x_{(1)}=3, x_{(2)}=1, x_{(3)}=2 \rightarrow x=(3\ 1\ 2)=(1\ 2\ 3)(1\ 2\ 3)=a^2$

עבור S4:

באותו אופן כמו עבור S3 - לפי המשפט לא יתכנו תמורות צמודות ל-a שהן בעלות מבנה מעגלי שונה (כלומר שאינן מעגל מסדר 3). מכיוון שאיננו רוצים את 4 במעגלי התמורות המצויות ברכז של a, נקבע $x_{(4)}=4$, ולכן מעגלי התמורות של האיברים ברכז של a יראו בדיוק אותו דבר (ויהיו על כן $C_{s4}(a)=\{1, a, a^2\}$).

עבור A4: A4 כוללת את כל התמורות ב-S4 שהן זוגיות. מאחר שבכך לא התווספו לנו תמורות חדשות לחבורה, גם לא יתווספו לרכז (כיוון שפעולת ההרכבה לא השתנתה). מאחר שכל החבורות שהצבנו ברכז קודם הן זוגיות - תמורת הזהות שייכת ל-A4, וכן (1 2)(1 3)=(1 2 3); (1 3)(1 2)=(1 3 2) הרי שגם לא ירדו איברים מהרכז, ולכן הוא נותר $C_{A4}(a)=\{1, a, a^2\}$.

14. א. מיון האיברים ב-S6 עפ"י סדר:

(a,b,c,d,e,f הם 6 מספרים שונים בתחום 1...6)

סדר 1: אך ורק תמורת הזהות.

סדר 2: צירוף כל התמורות המורכבות מ-1, 2 או 3 מעגלים זרים זה לזה באורך 2.

אלו תמורות בעלות אחת הצורות (a,b) ; (a b)(c d) ; (a b)(c d)(e f)

סדר 3: צירוף כל התמורות המורכבות מ-1 או 2 מעגלים זרים באורך 3

(a b c) ; (a b c)(d e f). תשומת לב שגם תמורות המורכבות ממעגלים באורך 2 שאינם זרים עשויות להיות מסדר 3, אך אלו יהיו שקולות לאחד מסוגי האיברים שכבר פורטו(למשל (1 3 2)=(1 3)(1 2)).

סדר 4: כל התמורות השקולות למעגל בעל 4 איברים, וכן כל התמורות הבנויות ממעגל באורך 4 ומעגל זר לו באורך 2: (a b c d) ; (a b c d)(e f)

סדר 5: כל התמורות הבנויות ממעגלים בעלי 5 איברים - (a b c d e).

סדר 6: כל התמורות הבנויות ממעגלים בעלי כל ששת האיברים, או ממכפלת תמורות זרות מסדרי 2 ו-3: (a b)(c d e) ; (a b c d e f).

ב.כפי שראינו בסעיף הקודם, ב-S6 יש מספר איבר מסדר 6. ב-S7 קיימות תמורות מהצורה (a b c d e f g), ולמעשה בכל Sn קיימים לפחות כל האיברים השקולים למעגל מהצורה $(a_1, a_2,\ldots a_n)$, (אם n אינו ראשוני ניתן למצוא צורות נוספות).

20. $\sigma=\begin{pmatrix}1234567\\3456172\end{pmatrix}$ נתרגם למעגל: ← (1 3 5)(2 4 6 7), וזו תמורה אי-זוגית (למשל (2 4)(2 6)(2 7)(1 3)(1 5)=σ). נניח שמספר הטרנספוזיציות המרכיבות את τ הוא m, והוא זוגי או איזוגי. מספר הטרנספוזיציות המרכיבות את τ^4 הוא 4m, ולכן הוא בהכרח זוגי, כלומר ההעתקה τ^4 היא זוגית, ולכן לעולם לא תוכל להיות שווה ל-σ. המסקנה - לא קיימת τ המקיימת את התנאי הדרוש.

23. כן, מאחר שהתמורה σ ניתנת לבניה גם ממעגל אחד שאורכו 5, נוכל לשמור על מספיק איברים קבועים בה. כל הדרוש הוא שלפחות אחד האיברים הללו יהיו בין 1 ל-5. נהיה נדיבים ונקח למשל את התמורה (12 11 10 9 8)=σ. זוהי תמורה מסדר 5 כך ש**כל** האיברים מ-1 עד 5 (עד 7 למעשה) נותרים בה קבועים.

בכתיבה אחרת: $\sigma=\begin{pmatrix}1&2&3&4&5&6&7&8&9&10&11&12\\1&2&3&4&5&6&7&9&10&11&12&8\end{pmatrix}$

אביב 2005
ליאור

אלגברה מודרנית - 104134 קבוצת תרגול 12

סמסטר אביב 2005 - שיעורי בית מס' 7# - ת"ח נורמליות והומומורפיזם

3. G היא חבורה ציקלית, כלומר יש לה יוצר - $G=<g>$, וניתן לייצג כל איבר בה כחזקה של g. נבנה את ההעתקה φ באופן כללי: יהיה a איבר כלשהו ב-G (לא בהכרח שונה מ-g). נקבע שההעתקה תקיים $\varphi(g)=a$. מאחר שב-G יש n איברים, הרי שיש לנו n אפשרויות שונות להגדרה זו (לרבות g עצמו והאיבר הנייטראלי e). כעת, בכדי לקיים את תנאי הגדרת ההומומורפיזם היסודי $\varphi(a)\varphi(b)=\varphi(ab)$ נביט בפעולה $\varphi(g)*\varphi(g)$ (כאשר * היא באופן גנרי הפעולה המוגדרת על G ואין לנו צורך להכיר אותה). לפי ההגדרה, כדי שההעתקה תהיה הומומורפיזם נדרש $\varphi(g)*\varphi(g)=\varphi(g*g)$ (כאשר $\varphi(g)=a$), ועל מנת שנוכל לאן מועתק g אולם מאחר שכבר קבענו ש-$\varphi(g)=a$, וערכו של $g*g=g^2$ נקבע עפ"י החבורה G והפעולה המוגדרת בה, הרי שנותר רק נעלם אחד במשוואה, כך שנכפית עלינו ההגדרה $\varphi(g*g)=a*a=a^2$, ומאחר ש-a עצמו הוא בחבורה אז גם a*a יהיה בה בשל הסגירות.

באותו אופן נבנה את $\varphi(g^3)=\varphi(g*g*g)=\varphi(g*g)*\varphi(g)=(a*a)*a=a^3$, וכן הלאה. קיבלנו אם כן שכדי שההעתקה תקיים את התנאי להומומורפיזם מספיק לקבוע את a בהתחלה מתוך n האיברים ב-g, ונקבל $\varphi(g^i)=a^i$ לכל $1\le i\le n$ - (מאחר ש-g הוא היוצר של G הרי שהוא מסדר n, ולכן $g^n=e$ כך שניתן לומר גם ש-i בתחום $0\le i\le n-1$ - לאחר n פעמים שנכפול ב-g נסיים לעבור על כל האיברים ב-G). תשומת לב שכמקרים פרטיים נקבל את ההומומורפיזמים הטריוויאליים - אם בחרנו a=e (האיבר הנייטראלי של G) אזי נקבל את ההעתקה $\varphi(g^i)=e$, ואם a=g נקבל את העתקת הזהות.

13. הרעיון - נוכיח שמכל איבר g ב-G שנבחר, נוכל להגיע חזרה לאותו g באמצעות חזקה שהיא כפולה שלמה של m. כך נוכל להראות שלכל g בחבורה יש איבר מקור מסויים (h) שמשתווה לו כאשר הוא מועלה בחזקת m.

נתון $(n,m)=1$ כלומר קיימים שלמים a,b כך ש-$na+mb=1$.

$$g=g^{na+mb}=g^{na}g^{mb}=(g^n)^a(g^m)^b=e(g^m)^b=(g^b)^m$$

נגדיר $h=g^b$ ו-מש"ל, כלומר לכל g קיים h כזה.

16. א. לא בהכרח - נקח למשל את $Z_4=\{0, 1, 2, 3\}$ ואת $U_8=\{1, 3, 5, 7\}$. נדרש למצוא העתקה φ, למשל $\varphi:U_8\to Z_4$, המקיימת בין השאר

$$\varphi(3)+\varphi(3)=\varphi(3*3)=\varphi(1)$$

$$\varphi(5)+\varphi(5)=\varphi(5*5)=\varphi(1)$$

$$\varphi(7)+\varphi(7)=\varphi(7*7)=\varphi(1)$$

ואפשר לראות שזה יהיה בלתי אפשרי בחבורה Z_4, כיוון שסדר כל אחר מהאיברים ב-U_8 הוא 2 (מלבד e), בעוד שב- Z_4 הם מסדרים שונים.

ב. חבורות מסדר 5 (מספר ראשוני) הן ציקליות כפי שהוכחנו בעבר - (כל איבר שנבחר יוצר תת חבורה ולכן הסדר שלו חייב לחלק את 5). לכן, בדומה לשאלה 3, נוכל לבחור יוצר של כל אחת מהחבורות ולהגדיר את ההעתקה כך שתעביר את היוצר של חבורת המקור (נקרא לו g) ליוצר של חבורת היעד (נקרא לו a) כלומר $\varphi(g)=a$. עפ"י חוקי ההומומורפיזם אנו נקבע בכך למעשה גם את ההעתקה לשאר האיברים כיוון ש- $\varphi(g^2)=\varphi(g*g)=\varphi(g)*\varphi(g)=a*a=a^2$ ובדומה גם לשאר האיברים, כך שיתקיים $\varphi(g^i)=a^i$ לכל i בתחום (לרבות i=5 כך שהאיבר הנייטראלי של חבורת המקור יועתק לאיבר הנייטראלי של חבורת היעד). מאחר שבשתי החבורות יש בדיוק 5 איברים ואנו נעבור עליהם בדרך זו באופן שיטתי, ההעתקה תהיה על, ומאחר שבמקרה זה גם קל למצוא את ההעתקה ההופכית $\varphi'(a^i)=g^i$ ברור שהיא גם חח"ע, ולכן מצאנו איזומורפיזם.

פרק ח' - תת חבורות נורמליות.

2. א. נתון ש-N ו-H הן תת חבורות של G, כאשר N היא תת חבורה נורמלית. נבדוק עפ"י ההגדרה - עבור n_1h_1 ו-n_2h_2 ב-NH, נבדוק סגירות לחיבור בעזרת ההגדרה של N כתת חבורה נורמלית - כל איבר מ-G (ובפרט מ-H) המוכפל בה משמאל יכול לעבור לימין - האיבר מ-N עשוי להשתנות אולם הוא עדיין ישאר איבר כלשהו ב-N-

$n_1h_1*n_2h_2=n_1(h_1n_2)h_2=n_1(n_3h_1)h_2=(n_1n_3)(h_1h_2)$ → שייך ל-NH

$(n_1h_1)^{-1}=h_1^{-1}n_1^{-1}=n_2h_1^{-1}$ → שייך ל-NH

ומובן שקיימים ב-NH איברים, למשל e השייך גם ל-N וגם ל-H כתת חבורות (ולכן $e*e=e$ שייך אף הוא ל-NH).

ב. כבר הראינו ש-NH היא תת חבורה, נותר לבדוק האם לכל איבר g ב-G מתקיים התנאי $NH=NHg^{-1}$, כלומר כל g מצמיד כל אחד מאיברי NH לאיבר אחר ב-NH. יהיו n_1,h_1 ב-N,H ו-n_1h_1 ב-NH. נבחר g שרירותי מחבורה G ונחשב:

$g^{-1}(n_1h_1)g=(g^{-1}n_1)(h_1g)=(n_2g^{-1})(gh_2)=n_2(g^{-1}g)h_2=n_2h_1$ → שייך ל-NH

ביצענו שתי החלפות במקביל - משמאל החלפנו את סדר המכפלה של g^{-1} באיבר מ-N (לא משנה מה האיבר החדש שנקבל במקום n_1, אלא העובדה שהוא מ-N), ובאותו אופן החלפנו את g עם האיבר מ-H. מהשוויון הנ"ל נובע ש-NH היא תת חבורה נורמלית.

5. א'.

N(H) מוגדרת כקבוצת כל האיברים ב-G המצמידים כל איבר ב-H חזרה לאיבר כלשהו ב-H. יהיו a,b ב-N(H), כלומר מקיימים $a^{-1}Ha=H$ וכנ"ל לגבי b, ויהיה h ב-H. עפ"י חוקי תת חבורה נורמלית (aH=Ha)

$(ab)^{-1}h(ab)=b^{-1}a^{-1}hab=b^{-1}a^{-1}(ha)b=b^{-1}a^{-1}(a\hat{h})b=b^{-1}(a^{-1}a)\hat{h}b=b^{-1}\hat{h}b=b^{-1}bh=h$

תשומת לב שבכל החלפה של h שמרנו עליו כאיבר ב-H, כלומר התוצאה שייכת ל-H גם היא.

ב'. נראה לפי ההגדרה של ת"ח נורמלית: יהיה n איבר ב-N(H). בשביל להוכיח נורמליות, צריך להראות ש-$n^{-1}Hn$ שייך ל-H (עבור כל איבר שבחרנו מ-H). אבל, לפי הנתון בתחילת השאלה - מאחר ש-n שייך לחבורה N(H), הרי שהוא מצמיד את תת החבורה H לעצמה (כלומר לכל n ב-N(H) מתקיים $n^{-1}Hn=H$ כי כך מוגדרת החבורה N(H)) ולכן מש"ל.

ג. בכיוון אחד - נניח ש-H נורמלית ב-G. המשמעות היא שלכל איבר g ב-G מתקיים $g^{-1}Hg$ שייך ל-H, אבל לפי ההגדרה בתחילת השאלה כל איבר המקיים זאת שייך ל-N(H), ולכן כל g ב-G שייך ל-N(H), כלומר G מוכלת ב-N(H), אבל מאחר ש-N(H) היא תת חבורה של G (לפי סעיף א') הרי שהיא מוכלת בה, ומההכלה ההדדית נובע שהן שוות.

בכיוון השני - נניח ש-N(H)=G, כלומר כל איבר g ב-G שייך גם ל-N(H), ולכן מקיים $g^{-1}Hg=H$. מכך, לפי הגדרת תת החבורה הנורמלית, נובע ש-H נורמלית ל-G, מש"ל.

אביב 2005
ליאור

8. יהיו a,b איברים ב-G. נביט על <a> (תת החבורה שיוצר a) - לפי הנתון היא נורמלית ב-G, ולכן מתקיים עבורה ש**כל** b ב-G מצמיד אותה לעצמה: $bAb^{-1}=A$ (כאשר $A=<a>$), ובפרט bab^{-1} שייך ל-<a> ולכן שווה לחזקה כלשהי של a (מאחר ש-<a> היא ציקלית), כלומר קיים j שלם כך ש-$bab^{-1}=a^j$. כעת נעביר אגפים ע"י כפל מימין ב-b, וסיימנו -קיים j שלם כך ש: $ba=a^jb$ (וניתן לחזור על התהליך עבור **כל** a, ובכל פעם כאמור הוא נכון לכל b).

11. תהי $H=\{h_1,h_2,\ldots,h_k\}$. בהנתן איבר כלשהו g ב-G, נבנה עבור H את הרשימה הבאה

$$gh_1g^{-1}=q_1 \; ; \quad gh_2g^{-1}=q_2 \; ; \quad gh_3g^{-1}=q_3 \ldots gh_kg^{-1}=q_k$$

מתקבלת הקבוצה $Q=\{q_1,q_2,\ldots,q_k\}$ - נראה שהיא אכן בעלת k איברים שונים:

$$q_1=q_2 \rightarrow gh_2g^{-1}=gh_1g^{-1} \rightarrow h_2=h_1$$

נראה שהיא תת חבורה:

Q אינה ריקה מאחר שבנינו אותה מאברי H (שאינה ריקה אף היא). ניתן גם לראות שמאחר ש-e שייך ל-H, $geg^{-1}=e$ ולכן האיבר הנייטראלי (אותו איבר של G ושל H) מצוי ב-Q.

$$q_iq_j= gh_ig^{-1}gh_jg^{-1}=gh_ih_jg^{-1}$$

ומאחר ש-h_ih_j שייך לתת החבורה H כי היא מקיימת סגירות, אזי q_iq_j שייך ל-Q

$$q_i^{-1}= (gh_ig^{-1})^{-1}=(g^{-1})^{-1}(gh_i)^{-1}=(g^{-1})^{-1}(h_i)^{-1}(g)^{-1}=gh_i^{-1}g^{-1}$$

ומאחר ש-h_i^{-1} שייך גם הוא לתת החבורה H, אזי q_i^{-1} שייך ל-Q.

הראינו אם כך ש-Q היא תת חבורה של G (אין תלות ב-g שבחרנו ולכן זה נכון לכל g ב-G), והוכחנו שהיא מסדר k, אולם עפ"י הנתון יש רק חבורה אחת מסדר כזה ולכן בהכרח $Q=H$, ועל כן לכל $1\le i\le k$ מתקיים ש- gh_ig^{-1} שייך ל-H, כלומר $gHg^{-1}=H$ ולכן H היא ת"ח נורמלית. מש"ל.

אביב 2005
ליאור

אלגברה מודרנית - 104134 קבוצת תרגול 12

סמסטר אביב 2005 - שיעורי בית מס' 8# - חבורות מנה ומשפט הומומורפיזם I

3. הסדר של איבר בחבורה המנה - $o(aN)=m$ אם m הוא המספר המינימלי המקיים $(aN)^m=e_{aN}=eN$.

נביט על הגדרת הפעולה בחבורת המנה:

$(aN)(bN)=abN \rightarrow (aN)(aN)=aaN=a^2N \rightarrow ... (aN)^m=a^mN=eN$

הערה - תשומת לב שמהשורה האחרונה **לא** נובע ש- $a^m=e$ מאחר שבחבורה G זהו שוויון קוסטים רגיל (זהו שוויון איברים רק ב-G/N), אלא ש-a^m שייך ל-N.

כעת - אנו יודעים ש-$a^k=e$ - אם נציב: $(aN)^k=a^kN=eN$, ולכן הסדר של aN מחלק את k.

5. א. נבחר g מטריצה כללית ב-G, ו-Λ כלשהו ב-P.

$$gPg^{-1}=\begin{pmatrix}a&0\\c&d\end{pmatrix}\begin{pmatrix}e&0\\f&g\end{pmatrix}\left(\frac{1}{ad}\begin{pmatrix}d&0\\-c&a\end{pmatrix}\right) \qquad |\Lambda|=eg-0f=eg>0$$

$$=\frac{1}{ad}\begin{pmatrix}ae&0\\ce+df&dg\end{pmatrix}\begin{pmatrix}d&0\\-c&a\end{pmatrix}=\frac{1}{ad}\begin{pmatrix}aed&0\\...&dga\end{pmatrix} \qquad ad\neq 0 \qquad \text{נחלק}$$

$$=\begin{pmatrix}e&0\\...&g\end{pmatrix} \qquad \Rightarrow |gPg^{-1}|=eg>0$$

או לחילופין (קצר יותר): $|gPg^{-1}|=|g||P||g^{-1}|=|g||g^{-1}||P|=|gg^{-1}||P|=|P|$

(בשיטה השניה - מותר להחליף את סדר האיברים כיוון שמדובר במספרים ממשיים)

כלומר בכל מקרה קיבלנו $|gPg^{-1}|>0$, ולכן gPg^{-1} שייך ל-P, כלומר P היא ת"ח נורמלית.

ב. ניתן מייד לראות שהסדר של P הוא מחצית מהסדר של G, כיוון שהיא מכסה בדיוק חצי מהמטריצות בה (כל אלו עם הדטרמיננטה החיובית). לכן, הקוסט השני יהיה אוסף כל המטריצות בעלות הדטרמיננטה השלילית ב-G. נשיג זאת למשל ע"י כפל במטריצת היחידה שבה יש סימן מינוס באחת האחדות:

$$q=\begin{pmatrix}-1&0\\0&1\end{pmatrix} \qquad |q|=-1 \qquad \forall \Lambda\in P \Rightarrow |q\Lambda|=|q||\Lambda|=-|\Lambda|<0$$

$$|g(qP)g^{-1}|=|g||(qP)||g^{-1}|=|g||g^{-1}||(qP)|=|gg^{-1}||(qP)|=|(qP)|<0$$

ולכן G/P={P,qP}, כלומר $G/P=\left\{P,\begin{pmatrix}-1&0\\0&1\end{pmatrix}P\right\}$ והיא מסדר 2.

9. ראשית כל - מאחר ש-M תת חבורה, לפי לגראנז' יתקיים תמיד m|n, ולכן n/m הוא מספר שלם והפעולה ניתנת לחישוב לכל g ב-G. יתר על כן אם נביט על M כקוסט ב-G, עפ"י לגראנז', היחס בין גודל החבורה G לגודל כל אחד מהקוסטים aM הוא האינדקס : [G:M] = |G| / |M| = n/m, שהוא מספר הקוסטים של M ב-G ועל כן גם מספר האיברים בחבורת המנה G/M - כלומר הסדר של G/M (o(G/M)=n/m).

מכאן, שאם נבחר את האיבר בחבורת המנה $g^{(n/m)}M$, ששווה לפי הגדרת הכפל בחבורת המנה (ראה שאלה 3 לעיל) ל-$(gM)^{(n/m)}$ ניתן לראות שזהו איבר בחבורה המועלה בחזקת סדר החבורה שלו, ולכן $g^{(n/m)}M=(gM)^{(n/m)}=(gM)^{o(G/M)}=eM$, ומכיוון שבאגף ימין יש לנו איבר מתת החבורה M, ובאגף שמאל איבר נוסף מאותה תת חבורה וכן את $g^{(n/m)}$, הרי שמתוך הסגירות של תת החבורה M נובע ש-$g^{(n/m)}$ שייך אף הוא ל-M.

13. א. צריך להוכיח שכל האיברים ב-G שהם מסדר m הם תת חבורה של G :

- e שייך ל-M (M אינה ריקה).

- אם a שייך ל-M, אזי $e=e^{-1}=(a^m)^{-1}=(a^{-1})^m$ כלומר גם a^{-1} שייך ל-M וכל ההופכיים בתת החבורה.

- יהיו a,b ב-M. הואיל ו-G אבלית, מתקיים $(ab)^m=a^mb^m=e*e=e$, כלומר יש סגירות. המסקנה - M היא תת חבורה.

ב. יהי x איבר ב-G/M שמקיים את התנאי, איבר זה הוא מהצורה x=aM, כאשר a הוא איבר ב-G. לפי חוקי כפל קוסטים : $x^m=(aM)^m=(aM)(aM)\dots(aM)=a^mM$

נכפה את התנאי הנתון $x^m=e$ (הנייטראלי של חבורת המנה הוא למעשה eM=M) ← $a^mM=eM$. כדי ששווין הקוסטים הזה יתקיים, a^m חייב להיות שייך גם הוא ל-M - לפי ההגדרה - a^m יהיה שייך ל-M אמ"מ $(a^m)^m=a^{m*m}=e$ (הפעם זהו האיבר הנייטראלי ב-G). כלומר הסדר של האיבר a ב-G מחלק את m^2. כמו כן, מאחר שהסדר של G עצמה הוא nm, ו-a איבר ב-G, ידוע שהסדר של a מחלק גם את nm. מאחר ש-(n,m)=1 קיימים s,t כך ש-sn+tm=1 נכפול את המשוואה הזו ב-m ונקבל

$m=snm+tm^2$, ואם נעלה את a בחזקת כל אגף זה נקבל $a^m=(a^s)^{mn}(a^t)^{mm}$, אבל הראינו קודם שהסדר של a מחלק את שני המעריכים באגף שמאל ולכן $e=e*e=a^m$, וזו בדיוק הגדרת השייכות ל-M. מסקנה - a עצמו חייב להיות שייך ל-M כדי לקיים את התנאי, ולכן, לפי ההגדרה שנתנו (x=aM) מתקבל x=M, כלומר x הוא האיבר האדיש של חבורת המנה G/M. מש"ל.

פרק י' - משפט הומומורפיזם ראשון

1. נייצג כל z ב-N באופן פולארי: $z=R\text{cis}\theta$ (כאשר R>0 ו-$0<\theta<2\pi$) מוגדר כך באופן חח"ע). אם כך: $N=\{z \text{ in } C \mid R=1\}$ כלומר זהו מעגל היחידה במישור המרוכב. N היא תת חבורה כיוון שהיא כוללת את האיבר הנייטראלי 1 (=1+0i), לכל z ב-N קיים ההופכי $z^{-1}=1/z$ (גם ב-N לא קיים 0), וכל שני איברים a,b ב-N מקיימים $a*b=(1*\text{cis}\theta_a)*(1*\text{cis}\theta_b)=1*\text{cis}(\theta_a+\theta_b)$ כלומר המכפלה מצויה גם היא ב-N. מאחר שכל החבורות שאנו עוסקים בהם כאן מוגדרות לגבי פעולת כפל רגיל (ממשיים או מרוכבים) הרי שהן קומוטטיביות, ולכן כל תת חבורה ב-C^* - לרבות N - היא נורמלית, וחבורת המנה C/N תהיה מוגדרת היטב.
נגדיר את הפעולה φ להיות $\varphi:C^*\to R+$, $\varphi(R\text{cis}\theta)=R$ (או במונחים קרטזיים - $\varphi(z)=(a^2+b^2)^{½}$). שתי החבורות מוגדרות לגבי הכפל, ומאחר שהרדיוס מוגדר להיות חיובי תמיד ו-G אינה כוללת את 0, הרי שאין חריגה מהתחום, וההעתקה היא על (כל מספר ממשי יכול להיות הרדיוס של המספר מרוכב).
האיבר הנייטראלי בתמונה הוא בדיוק 1, ולכן $\ker(\varphi)=N$, ולפי משפט ההומומורפיזם הראשון: $\mathbb{C}^*/\ker(\varphi) = G/N \cong \text{Im}(\varphi) = (\mathbb{R}^+,\cdot)$

8. א'. נוכיח תחילה ש-N היא ת"ח של G:
- N אינה ריקה - e_G (הנייטראלי ב-G) שייך ל-N כיוון ש-$\varphi(e_G)=e_{G'}$ לפי הגדרת הומומורפיזם, וכיוון שנתון כי N' היא תת חבורה של G', בהכרח האיבר הנייטראלי של G', $e_{G'}$, שייך לה.

אביב 2005
ליאור

- הופכיים - אם a שייך ל-N אזי $\varphi(a)$ שייך ל-N' ומאחר שהיא חבורה אז גם ההופכי לאיבר זה - $(\varphi(a))^{-1}$ שייך ל-N'. לפי הגדרת הומומורפיזם מתקיים במקרה זה - $(\varphi(a))^{-1}=\varphi(a^{-1})$, כלומר גם $\varphi(a^{-1})$ שייך ל-N', ולכן לפי ההגדרה הנתונה - a^{-1} שייך ל-N (משמע - יש ב-N את כל ההופכיים).

- יהיו a,b שייכים ל-N - $\varphi(a), \varphi(b)$ שייכים ל-N', וכיוון שהיא חבורה מתקיים $\varphi(a)\varphi(b)$ שייך אף הוא ל-N', וכיוון ש-φ הוא הומומורפיזם, גם $\varphi(a)\varphi(b)=\varphi(ab)$ שייך ל-N', ולכן ab שייך ל-N ומתקיימת סגירות.

אם כן, N היא תת חבורה של G. נבדוק נורמליות - צ"ל שלכל a ב-G מתקיים aNa^{-1} שייך ל-N - נפעיל את ההומומורפיזם φ:

$$\varphi(aNa^{-1})=\varphi(a)\cdot\varphi(N)\cdot\varphi(a^{-1})=\varphi(a)\cdot N'\cdot(\varphi(a))^{-1}$$

הכוונה ב-$\varphi(N)$ היא התמונה אליה מעתיקה φ את N, כלומר N'. הפעולות הללו התבצעו בתוך החבורה G', ומכיוון ש-N' נורמלית ב-G', הרי שהיא מתחלפת (בפעולה המוגדרת ב-G') עם כל איבר ב-G', ובפרט עם $\varphi(a)^{-1}$:

$$\varphi(a)\cdot N'\cdot\varphi(a)^{-1}=(\varphi(a)\cdot\varphi(a)^{-1})\cdot N'=e'N'$$

ומכאן שהפעלת ההעתקה על aNa^{-1} נותנת איבר ב-N', כלומר aNa^{-1} שייך ל-N, ולכן N היא נורמלית ב-G.

ב'.. נביט על חבורת המנה G'/N', ונגדיר את הפעולה $\psi: G \rightarrow G'/N'$; $\psi(a)=\varphi(a)N'$. נראה שהיא מוגדרת היטב ומהווה הומומורפיזם בעצמה: התחום הוא G כולה, וההומומורפיזם הנתון מוגדר עליה היטב. התוצאה (אגף ימין) היא מכפלת איבר ב-G' בתת החבורה N', כלומר זהו קוסט בחבורת המנה G'/N'. הפעולה חד-ערכית כיוון ש-φ היא חד ערכית כך שלכל a מוגדר $\varphi(a)$ בודד, כלומר אם a,b שניהם ב-G ומתקיים a=b, אזי $\varphi(a)=\varphi(b)$ ולכן

$$\psi(a)=\varphi(a)N'=\varphi(b)N'=\psi(b)$$

מאחר שההעתקה שלנו מוגדרת היטב, נביט בתכונות שלה: $\ker(\psi)$ כולל את כל האיברים ב-G המועתקים לאיבר הנייטראלי ב-G'/N', שהוא e'N'=N'. מכאן שאם נכפה את התנאי $\psi(a)=\varphi(a)N'=e'N'$, אז לפי תכונת הקוסט $\varphi(a)*(e')^{-1}$ = $\varphi(a)e'$ שייך ל-N', ומאחר ש-e' שייך ל-N' (כי היא תת חבורה) הרי ש-$\varphi(a)$ חייב

גם הוא להיות שייך ל-N', ומכאן לפי ההגדרה הנתונה ש-a עצמו שייך ל-N, ולכן:
$N=\ker(\psi)$. מכאן, לפי משפט ההומומורפיזם הראשון - סיימנו:

$$G/\ker(\psi) = G/N \cong \mathrm{Im}(\psi) = G'/N',$$

שאלות מסכמות (סעיף כ')

23.

א. לא יתכן, כי הסדר של U_8 הוא 4, ואילו Z_2 היא מסדר 2, כך שכל העתקה תהיה חייבת להעתיק לפחות לאיבר אחד ב-Z_2 יותר מאיבר אחד ב-U_8. לכן ההעתקה לא יכולה להיות חח"ע.

ב. הסדר של Z_7 הוא 7, בעוד ש-Z כלל אינה חבורה סופית. לא ניתן למצוא העתקה שהיא **על** Z פשוט כיוון שאין מספיק איברים.

ג. הגדרת העתקה שכזו אינה אפשרית מכיוון שהיא צריכה ליצור תת חבורה בתוך Z_{10}, ולא תתכן אף תת חבורה מסדר 4 (כמו הסדר של U_8) כיוון שסדרה לא יחלק את הסדר של Z_{10}. זה רק אחד הנימוקים, אבל את השני נשמור לסעיף הבא..

ד. לא יתכן הומומורפיזם כזה - ניתן היה לכאורה להגדיר פעולה שיוצרת תת חבורה מסדר 4 בתוך Z_{64}, כיון ש- 4|64, אבל הבעיה היא לשמור על הסדר של החבורה המקורית - ב-U_8 כל איבר הוא מסדר 2 (מלבד 1 הנייטראלי), וההומומורפיזם חייב לשמור על תנאי זה כיוון שאם לכל x מתקיים $x^2=e$, הרי שעבור התמונה מתקיים:
$e_{image}=\varphi(e_{source})=\varphi(x^2)=\varphi(x)\varphi(x)=[\varphi(x)]^2$ כלומר כל איבר בתמונה הוא גם מסדר 2 לכל היותר (האיבר הנייטראלי ישאר כמובן מסדר 1). מאחר שב-Z_{64} (ולמעשה בכל Z_n) האיבר היחיד מסדר 2 הוא n/2 (32 במקרה הנוכחי), ומאחר שנדרש גם שההעתקה תהיה חח"ע, לא ניתן להעתיק אליו את כל האיברים ב-U8 מלבד e.

ה.לא יתכן. אמנם גודלן של שתי החבורות שווה $U_{18}=\{1,5,7,11,13,17\}$, וגם ב-$S_3$ קיימים $3!=6$ איברים, אבל יש כמה תכונות בסיסיות ששונות בין החבורות ובכלל זאת ש-U_{18} הינה חבורה אבלית (כי פעולת הכפל מודולו 18 המוגדרת בה היא קומוטטיבית) בעוד ש-S_3 אינה אבלית (בפעולת ההרכבה יש חשיבות לסדר) ולכן אם נדרוש הומומורפיזם, לכל σ_1,σ_2 ב-S_3 נדרש

$$\varphi(\sigma_1\sigma_2)=\varphi(\sigma_1)\varphi(\sigma_2)=\varphi(\sigma_2)\varphi(\sigma_1)=\varphi(\sigma_2\sigma_1)$$

ואז בהכרח $\sigma_1\sigma_2=\sigma_2\sigma_1$ (וזה כאמור חייב להתקיים לכל σ_1,σ_2) - בסתירה למוכר ב-S_3, ולכן לא יתכן שקיים הומומורפיזם כזה. (אגב, גם כאן יש

תרגיל "העשרה" -

א. נפעיל את למת ההצמדה:

$$\sigma=(1\ 3\ 5)(2\ 4\ 6)(7\ 8\ 9)=\pi^{-1}\tau\pi=\pi^{-1}((1\ 2\ 4)(3\ 5\ 9)(6\ 8\ 7))\pi$$

$$=((\pi^{-1}(1)\ \pi^{-1}(2)\ \pi^{-1}(4))\ \ ((\pi^{-1}(3)\ \pi^{-1}(5)\ \pi^{-1}(9))\ \ ((\pi^{-1}(6)\ \pi^{-1}(8)\ \pi^{-1}(7))=$$

נתאים את האיברים לבניית ההעתקה π^{-1}:

$$\pi^{-1}=\begin{pmatrix}1&2&3&4&5&6&7&8&9\\1&3&2&5&4&7&9&8&6\end{pmatrix}\rightarrow\pi=\begin{pmatrix}1&2&3&4&5&6&7&8&9\\1&3&2&5&4&9&6&8&7\end{pmatrix}=(2\ 3)(4\ 5)(6\ 9\ 7)$$

ב. קודם כל - מספר האפשרויות לסידור n איברים שונים הוא $n!$. מתוך כך נתחיל לצמצם חזרות - נייצג את ההעתקה כמבנה של מעגלים זרים - ידוע שיש רק ייצוג אחד כזה. נניח גם שמקומות הסוגריים קבועים (למשל לפי סדר גדלי המעגלים, מ-1 ועד ל-n) ורק סדר האיברים יכול להשתנות.

כל מעגל ניתן "לסובב" כל עוד נשמר הסדר הפנימי שלו - ניתן לקבוע זאת למעשה ע"י בחירת האיבר במקום הראשון (או במקום שרירותי אחר) וסידור שאר האיברים לפי הסדר הקבוע לאותו מעגל (למשל $(3,2)=(2,3)$). לכן, לכל i בין 1 ל-n: לבחירת האיבר הראשון של המעגל ה-i יש i אפשרויות, ויש a_i מעגלים כאלה. ולכן עבור כל i כזה עלינו לחלק את מספר הסידורים הכולל ב- i^{a_i} אפשרויות סידור פנימיות בכלל המעגלים מסדר i שהן שקולות.

בנוסף, מאחר שאנחנו משנים את סדר האיברים, תהיה לנו עדיין כפילות כאשר נחליף יחד את כל האיברים בין מעגלים מאותו סדר (למשל $(4,5)(2,3)$ ו-$(2,3)(4,5)$). מאחר שזה שקול להחלפה בין מקומות המעגלים, הרי שכדי לצמצם את החזרות הללו עלינו לחלק עבור כל i גם במספר האפשרויות השונות לסידור a_i המעגלים מסדר זה, כלומר $(a_i)!$.

אם כן, אנו צריכים לקחת את מספר הסידורים הכולל של n איברים, ולכל i בין 1 ל-n לחלק אותו ב- $i^{a_i}\cdot a_i!$,

לכן, מספר האיברים במחלקת הצמידות של σ הנתונה יהיה $\dfrac{n!}{\left(\prod_{i=1}^{n}(i^{a_i}\cdot a_i!)\right)}$

ג. נקרא לתמורה הנתונה $\sigma=(1...r)(r+1...n)$ אנו נדרשים למצוא את $C_{Sn}(\sigma)$ כלומר את כל האיברים ב- Sn שמתחלפים עם σ בכפל (כפי שהוא מוגדר על תמורות):

$$C_{Sn}(\sigma)=\{\ \tau \text{ in } S_n \mid \tau\sigma=\sigma\tau\ \} = \{\ \tau \text{ in } S_n \mid \tau\sigma\tau^{-1}=\sigma\ \}$$

ניתן לראות שלפי ההגדרה לעיל כל τ יהיה במחלקת הצמידות של σ.

נשתמש בלמת ההצמדה כדי לראות כמה אפשרויות יש להגדרה של τ.

$$\tau((1...r)(r+1...n))\tau^{-1} \Longrightarrow (\tau(1)...\ \tau(r))(\tau(r+1)...\ \tau(n)) = \tau$$

השוויון האחרון נובע מהצורך להצמיד את ההעתקה לעצמה. כעת נראה כמה אפשרויות יש לבצע העתקות כאלו - כל מעגל חייב להיות מועתק לעצמו, דהיינו לשמור על הסדר הפנימי שלו - אולם ההעתקה יכולה "לסובב" אותו בלי לשנותו. לכן, כמו בסעיף הקודם יש לנו עבור המעגל הראשון בדיוק r אפשרויות לבחור מי יהיה האיבר הראשון שיופיע במעגל (כלומר מהו $\tau(1)$), ולאחר מכן נהיה חייבים לקבוע את ההעתקה עבור שאר האיברים בהתאם לסדר המעגל המקורי. באותו אופן עבור המעגל השני יש לנו n-r איברים ולכן n-r אפשרויות לקביעת תוצאת ההעתקה $\tau(r+1)$. לכן בסך הכל עבור מקרה כללי ($r\neq n/2$) יש לנו $r(n-r)$ אפשרויות - כלומר $r(n-r)$ העתקות τ שונות, ולכן זהו גודל הרכז של σ:

$$\mathbf{|C_{Sn}(\sigma)|_{r\neq n/2}=r(n-r)}.$$

עבור המקרה הפרטי של $r=n/2$, ניתן לראות ש-$r=n-r$, ולכן מספר ההעתקות יהיה לכאורה r^2, אולם עלינו לזכור שבמצב זה יכולה העתקה τ להביא גם להחלפה בסדר המעגלים (כלומר לכל העתקה τ כמו קודם, נוספת העתקה τ' שיוצרת את אותם שני מעגלים (עם אותו סדר פנימי) אולם מחליפה את הסדר ביניהם). לכן במקרה כזה סך ההעתקות τ השייכות לרכז יהיה $\mathbf{|C_{Sn}(\sigma)|_{r=n/2}=2r^2}$

ד. יהי a שייך ל-G. נביט ברכז של a: ידוע שהוא מהווה תת חבורה (הוכחנו בכיתה) וכאמור - $C_G(a)=\{\ b \text{ in } G \mid ba=ab\ \} = \{\ b \text{ in } G \mid bab^{-1}=a\ \}$

כלומר לפי ההגדרה $C_G(a)$ הוא למעשה תת חבורה נורמלית.

אם כך, נביט על חבורת המנה $G/C_G(a)$, ונבדוק מהו גודלה (כלומר כמה קוסטים שונים יש לרכז של a ב-G - יהיו u,v שני איברים שונים ב-G - נדרוש $uC_G(a)\neq vC_G(a)$ ונקבל את הדרישה ש- uv^{-1} לא יהיה שייך ל-$C_G(a)$. לכן $uv^{-1}a \neq auv^{-1}$, ואם נכפול את שני האגפים ב-v מימין וב-u^{-1} משמאל נקבל

אביב 2005
ליאור

$v^{-1}av \neq u^{-1}au$, כלומר אלה הם 2 איברים שונים במחלקת הצמידות a^G. הדרישה הזו פועלת לשני הכיוונים, כלומר עבור כל זוג איברים שונים במחלקת הצמידות של a, נקבל 2 קוסטים שונים של הרכז של a ב-G, כלומר גודל חבורת הצמידות הוא מספר הקוסטים של $C_G(a)$, או האינדקס שלו: $|a^G|=[G : C_G(a)]$, ולכן לפי משפט לגראנז' מתקיים

$$|G|=|C_G(a)|*[G : C_G(a)]= |C_G(a)|*|a^G|$$

ה. לפי הסעיף הקודם $|G|=|C_G(a)|*|a^G| \leftarrow |C_{Sn}(a)|= |S_n| / |a^{Sn}|$. ידוע ש- $|S_n|$ (מספר התמורות על n מספרים) הוא $n!$, ולכן אם נציב את התוצאה מסעיף ב' נקבל:

$$\left|C_{S_n}(\sigma)\right| = \frac{n!}{\frac{n!}{\left(\prod_{i=1}^{n}(i^{a_i}\cdot a_i!)\right)}} = \left(\prod_{i=1}^{n}(i^{a_i}\cdot a_i!)\right)$$

אביב 2005
ליאור

אלגברה מודרנית - 104134 קבוצת תרגול 12

סמסטר אביב 2005 - שיעורי בית מס' 9# - חוגים

4. שלב ראשון - נוכיח שזו חבורה חיבורית - R מוכל ב-C (המרוכבים) ו-C הינו שדה ולכן גם חבורה חיבורית. לכן מספיק להוכיח ש-R הוא תת חוג ב-C, כלומר תת חבורה עם סגירות גם לכפל.

e=0+0i=0 שייך ל-R ← R אינו ריק.

לכל x,y ב-R, (x1+iy1)+(x2+iy2)=(x1+x2)+i(y1+y2) והתוצאה היא ב-R, כיוון שחיבור שלמים שומר על סגירות ונשאר שלם (Z חבורה)

לכל x=a+bi ב-R, ההופכי החיבורי יסומן ב- x=-a-bi- איבר זה הוא בחבורה (כיוון שלכל מספר שלם יש הופכי חיבורי ב-Z), ומתקיים x+(-x)=a+bi-a-bi=0

- כעת נראה סגירות לכפל -

יהיו x,y ב-R, x=a1+ib1, y=a2+ib2.

xy=(a1+ib1)(a2+ib2)=(a1a2-b1b2)+i(a1b2+a2b1), והתוצאה היא בחבורה מאחר שגם כפל שלמים הוא מספר שלם. מאחר שאלו פעולות הכפל והחיבור הרגילות, הן גם קומוטטיביות ומתקיים xy=yx.

את תכונות האסוציאטיביות והדיסטריביוטיביות אנו יכולים "לרשת" מן השדה C, כיוון ש-R מוכל בתוכו (והתכונות הללו מתקיימות לכל האיברים ב-C).

לבסוף מאחר שזו היא פעולת הכפל הרגילה - נבחר את 1+0i=1 בתור היחידה - לכל x ב-R מתקיים x*1=1*x=(a+bi)*1=a+bi. ניתן גם לומר שמאחר שהאיבר האדיש הכפלי של C מצוי ב-R הוא היחידה של R ולכן R הוא חוג עם יחידה (הוכח בכיתה).

ב. יהי x=a+bi איבר (שונה מאפס) ב-R - אנו מחפשים איבר y=c+di ב-R, כך ש-xy=1:

$$x=(a+bi) \qquad y=(c+di) \qquad xy=(a+bi)(c+di)=(ac-bd)+i(ad+bc)=1$$

$$\begin{cases} (*)\ ac-bd=1 \\ (**)\ ad+bc=0 \end{cases}$$

נחלק לאפשרויות ונכפה את התנאי שהמקדמים יהיו שלמים:

$$1)\ b=0 \underset{(x\neq 0)}{\rightarrow} a\neq 0 \underset{**}{\rightarrow} d=0 \underset{*}{\rightarrow} ac=1 \Rightarrow c=\tfrac{1}{a}\left(\in\mathbb{Z}\right)\Rightarrow a=\pm 1$$

$$2)\ a=0 \underset{(x\neq 0)}{\rightarrow} b\neq 0 \underset{**}{\rightarrow} c=0 \rightarrow bd=-1 \Rightarrow d=\tfrac{-1}{b}\left(\in\mathbb{Z}\right)\Rightarrow b=\pm 1 \Rightarrow x=\pm i$$

$$3)\ a,b\neq 0 \underset{*}{\rightarrow} c=\frac{1+bd}{a} \underset{**}{\rightarrow} ad+\frac{b+b^2d}{a}=0 \rightarrow d(a+\tfrac{b^2}{a})+\tfrac{b}{a}=0 \rightarrow$$

$$d=\frac{-b/a}{b^2/a+a}=\frac{-b}{b^2+a^2}\rightarrow\left(\in\mathbb{Z}\right)\Rightarrow b^2+a^2\leq 1,\ \ a,b\in\mathbb{Z}\Rightarrow b^2+a^2=1$$

וניתן לראות שהאפשרות השלישית היא סתירה מאחר שאם a,b שונים מאפס ושלמים, הם יכולים להיות לכל הפחות שווים ל-1 בערכם המוחלט (לגבי כל אחד מהם), ואז סכום הריבועים שלהם גדול מ-1.

לכן האיברים ההפיכים הם $\pm 1,\ \pm i$

5. א. הקבוצה {2a+1 | a in Z} היא למעשה קבוצת כל המספרים האי זוגיים, ולכן 0 אינו נמצא בה ואין אדיש חיבורי כך שזו אינה חבורה ביחס לחיבור הרגיל ולא יכולה להיות חוג בכלל. נראה שאכן אין אדיש חיבורי: נדרוש (2a+1)+(2b+1)=(2a+1) ← 2b+1=0 ← b=-1/2 וזה לא ב-Z.

ב. הקבוצה אינה מקיימת סגירות לכפל: $(a\sqrt{3})(b\sqrt{3}) = 3ab = (\sqrt{3}ab)\sqrt{3} \rightarrow (\sqrt{3}ab) \notin \mathbb{Z}$ ולכן אינה חוג.

ג. נראה שזו חבורה חיבורית

$$(a+b\sqrt{3})+(c+d\sqrt{3}) = (a+c)+(b+d)\sqrt{3}$$

$$\forall a,b \in \mathbb{Q},\ -a,-b \in \mathbb{Q} \rightarrow (a+b\sqrt{3})+(-a-b\sqrt{3}) = 0$$

ומאחר שזו תת קבוצה של הממשיים, זה מספיק להוכחה שזו תת חבורה.

$$(a+b\sqrt{3})*(c+d\sqrt{3}) = (ac+3bd)+(ad+bc)\sqrt{3}$$

ומכאן שמתקיימת סגירות לכפל. כמו כן, בפעולות החיבור והכפל הרגילות נשמרת האסוציאטיביות והדיסטריביוטיביות (וניתן לומר גם שהקבוצה מוכלת בחבורת הממשיים ולכן שומרת על תכונות אלו) ולכן זהו חוג. מחלקי אפס - גם כאן ניתן לראות שאין מחלקי אפס מאחר שהקבוצה מוכלת בממשיים עם הפעולות הרגילות. נבדוק זאת :

$$(a+b\sqrt{3})*(c+d\sqrt{3}) = 0$$

$$(ac+3bd)+(ad+bc)\sqrt{3} = 0 \rightarrow ac+3bd = 0,\ ad+bc = 0$$

$$a = -\tfrac{bc}{d} \rightarrow \tfrac{-bc^2}{d} = -3bd \rightarrow c^2 = 3d^2 \rightarrow c = \pm\sqrt{3}d$$

הנחנו ש-d שונה מאפס כיוון שאם d=0 אזי כדי לאפס את 2 המשוואות נדרש b או c שווים לאפס, וגם a או c שווים לאפס, כלומר c=0 ולכן זה יהיה למעשה כפל באפס ולכן לא רלוונטי)

קיבלנו סתירה לכך שכל המקדמים רציונאליים (את הפעולות על המקדמים אנו מבצעים בשדה Q), ומכאן שאין מחלקי אפס בחוג, ולכן זהו תחום שלמות.

.11

א. שלב ראשון - נוכיח שזו חבורה חיבורית. מאחר שהיא מוכלת בממשיים מספיק להוכיח שזו תת חבורה

e=0 שייך ל-$\mathbb{Q}\left[\sqrt{2}\right]$, ולכן הוא אינו ריק.

לכל x,y ב-$\mathbb{Q}\left[\sqrt{2}\right]$, $(x_1+y_1\sqrt{2})+(x_2+y_2\sqrt{2})=(x_1+x_2)+\sqrt{2}(y_1+y_2)$ והתוצאה היא ב-$\mathbb{Q}\left[\sqrt{2}\right]$,

כיוון שחיבור המקדמים הרציונאלים שומר על סגירות (Q היא שדה)

לכל $x = a+b\sqrt{2}$ ב-$\mathbb{Q}\left[\sqrt{2}\right]$, ההופכי החיבורי יסומן ב- $-x = -a-b\sqrt{2}$ איבר זה הוא בחבורה

(כיוון שלכל מספר רציונאלי יש הופכי חיבורי ב-Q), ומתקיים x+(-x)=0

- כעת נראה סגירות לכפל -

אביב 2005
ליאור

יהיו x,y ב-R, $x=a+b\sqrt{2}$, $y=c+d\sqrt{2}$.

$xy=(a_1+b_1\sqrt{2})(a_2+b_2\sqrt{2})=(a_1a_2+2b_1b_2)+\sqrt{2}(a_1b_2+a_2b_1)$, והתוצאה היא בחבורה מאחר שגם כפל רציונאלים הוא ב-Q. מאחר שזוהי פעולת הכפל הרגילה, היא גם קומוטטיבית ומתקיים xy=yx.

את תכונות האסוציאטיביות והדיסטריביוטיביות אנו יכולים "לרשת" משדה הממשים, כיוון ש-$\mathbb{Q}\left[\sqrt{2}\right]$ מוכל בתוכו והפעולות עליו הן הרגילות. מכאן שזהו חוג קומוטטיבי.

לבסוף מאחר שהוגדרה פעולת הכפל הרגילה - נבחר את היחידה של הממשיים (אשר מתאימה לתבנית ושייכת אף היא לקבוצה) בתור היחידה שלנו - לכל x ב-R מתקיים x*1=1*x=x ולכן זה נכון גם לכל x ב-$\mathbb{Q}\left[\sqrt{2}\right]$.

ב. יהי $x(\neq 0)$ איבר ב-$\mathbb{Q}\left[\sqrt{2}\right]$ - נחפש איבר y כך ש- xy=0:

$$xy=(a+b\sqrt{2})(c+d\sqrt{2})=(ac+2bd)+\sqrt{2}(ad+bc)=0$$

$$\begin{cases} ac+2bd=0 \\ ad+bc=0 \end{cases} \begin{matrix} \cdot d \\ \cdot c \end{matrix} \rightarrow \begin{cases} acd+2bd^2=0 \\ acd+bc^2=0 \end{cases} \rightarrow b(2d^2-c^2)=0$$

והאפשרויות להתאפסות הן:

$$1)\ b=0 \rightarrow \begin{cases} (a=0)\ or\ (c=0) \\ (a=0)\ or\ (d=0) \end{cases} a=0 \rightarrow x=(a+b\sqrt{2})=0$$

$$2)2d^2=c^2 \rightarrow c=\pm d\sqrt{2}$$

ניתן לראות שהאפשרות השניה עומדת בסתירה לכך שהמקדמים רציונאליים, ואילו האפשרות ש-b=0 מחייבת a=0 ולכן x=0 וזו גם סתירה. על כן, $\mathbb{Q}\left[\sqrt{2}\right]$ הוא תחום שלמות.

ג. עפ"י ההגדרה לשדה - עלינו לדרוש שהחוג הקומוטטיבי שלנו (שהוא עם יחידה) יהיה גם עם חילוק, כלומר שלכל איבר השונה מאפס יהיה הופכי. יהי x ב-$\mathbb{Q}\left[\sqrt{2}\right]$ - צריך להוכיח שקיים y ב-$\mathbb{Q}\left[\sqrt{2}\right]$ כדלקמן:

$x=(a+b\sqrt{2})$ $y=(c+d\sqrt{2})$ $xy=(a+b\sqrt{2})(c+d\sqrt{2})=(ac+2bd)+\sqrt{2}(ad+bc)=1$

$\begin{cases} (*)\ ac+2bd=1 \\ (**)\ ad+bc=0 \end{cases}$ נבדוק אפשרויות (נדרוש שהמקדמים יהיו רציונליים):

$$1)b=0 \underset{(x\neq 0)}{\rightarrow} a\neq 0 \rightarrow d=0 \rightarrow ac=1 \Rightarrow c=1/a \left(\in \mathbb{Q}\right)$$

$$2)a=0 \underset{(x\neq 0)}{\rightarrow} b\neq 0 \underset{**}{\rightarrow} c=0, d\neq 0 \rightarrow 2bd=1 \Rightarrow d=1/2b \left(\in \mathbb{Q}\right)$$

$$3)a,b\neq 0 \underset{*}{\rightarrow} c=\frac{1-2bd}{a} \underset{**}{\rightarrow} ad+\frac{b-2b^2d}{a}=0 \rightarrow d(a-2b^2/a)+b/a=0 \rightarrow$$

$$d=\frac{b/a}{2b^2/a-a}= \underbrace{\frac{b}{2b^2-a^2}\left(\in \mathbb{Q}\right)}_{\left(2b^2-a^2\neq 0 \leftarrow 2b^2\neq a^2 \leftarrow \sqrt{2}b\neq \pm a \leftarrow a,b\in\mathbb{Q}\right)} \qquad c\underset{**}{=}\frac{-a}{b}d=\frac{-a}{2b^2-a^2}\left(\in \mathbb{Q}\right)$$

כלומר יש הופכי לכל איבר (למעט עבור x=0)

$$\Rightarrow c,d\in\mathbb{Q} \qquad \Rightarrow \qquad y=\frac{b\sqrt{2}-a}{2b^2-a^2}\in\mathbb{Q}\left[\sqrt{2}\right]$$

והוא בחוג.

13.א. נכון - לכל a הפיך ב-R יש b ב-R כך ש-ab=1, כמו כן -a(-1)=- ו- b(-1)=-b

-a=(-1)a → (-a)(-b)=(-1)a*(-1)b=(-1)(-1)ab=(-1)(-1)1=1 ולכן -b הוא ההופכי של -a

ב. לא נכון - ניתן להגיע עם פעולת החיבור לאפס שאינו הפיך. למשל ב-(Z,+, ·) 1 ו- 1- הם הפיכים (כל אחד מהם הוא ההופכי של עצמו) אבל סכומם הוא 0 ואינו הפיך.

ג. לא נכון - נקח למשל את (Z,+,·) - כל מספר השונה מ-0 ומ-1-/+ אינו הפיך, אבל אין מחלקי אפס.

ד. לא נכון - אם קיים a הפיך (0≠), עבורו יש b מסויים (0≠) כך ש-ab=0, הרי שעבור b מתקיים $b=a^{-1}ab=a^{-1}*0=0$, וזו סתירה כיוון ש-b≠0.

סעיף ז' - חוגי פולינומים

1. מאחר שחוגי פולינומים הם אוקלידיים ניתן להפעיל את אלגוריתם אוקלידס:

א.

$$\begin{bmatrix} x^4+1 & x^3+1 \\ -x^4+x & x \\ \hline 1-x & \end{bmatrix} \Rightarrow \begin{bmatrix} x^3+1 & -x^2-x-1 \\ -x^3-x^2 & 1-x \\ \hline 1+x^2 & \\ -x^2-x & \\ \hline x+1 & \\ -x-1 & \\ \hline 2\equiv 0 \pmod 2 & \end{bmatrix}$$

ולכן השארית האחרונה (1-x) היא ה-ממג"ב. נמצא את פונקציות הדרושות לקבלתו:

$(x^4+1)\mathbf{*1} + (x^3+1)\mathbf{*(-x)} = (x^4+1) - (x^4+x) = 1-x$

ב.

$$\begin{array}{l} x^6+x^3+x+1 \;\big|\; x^4-x^2+x+1 \\ -x^6+x^4 \\ \hline -x^4+x^3+x+1 \\ -(-x^4-x^2) \\ \hline x^3+x^2+x+1 \\ -x^3+x \\ \hline x^2+1 \\ -x^2+1 \\ \hline 0 \end{array}$$

ומכאן עולה ש-f(x) | g(x) ולכן $f(x)=x^2+1=(f(x),g(x))$

והפונקציות הדרושות הן פשוטות - $(x^6+x^3+x+1)\mathbf{*0} + (x^2+1)\mathbf{*1} = x^2+1$

ג.

$$\left[\begin{array}{l} x^2+2x+1 \\ \overline{x^5+x^4+x^3+2x^2+3x+2\,\big|\,x^3-x^2+2x+1} \\ {}^{-}x^5-x^4+2x^3+x^2 \\ \hline 2x^4-x^3+x^2+3x+2 \\ {}^{-}2x^4-2x^3-x^2+2x \pmod 5 \\ \hline x^3+2x^2+x+2 \\ {}^{-}x^3-x^2+2x+1 \\ \hline 3x^2-x+1 \end{array}\right] \underset{4=-1(\mathrm{mod}5)}{\Rightarrow} \left[\begin{array}{l} 2x+2 \\ \overline{x^3-x^2+2x+1\,\big|\,3x^2-x+1} \\ {}^{-}x^3-2x^2+2x \pmod 5 \\ \hline x^2+1 \\ {}^{-}x^2-2x+2 \pmod 5 \\ \hline 2x-1 \end{array}\right] \Rightarrow \left[\begin{array}{l} -x-1 \\ \overline{3x^2-x+1\,\big|\,2x-1} \\ {}^{-}3x^2+x \pmod 5 \\ \hline -2x+1 \\ {}^{-}-2x+1 \\ \hline 0 \end{array}\right]$$

ולכן השארית האחרונה 2x-1 היא הממג"ב. נמצא את a(x),b(x) עפ"י השלבים של האלגוריתם (ב-Z5):

$$\left(x^3\text{-}x^2\text{+}2x\text{+}1\right)\text{-}\underbrace{\left[\left(x^5\text{+}x^4\text{+}x^3\text{+}2x^2\text{+}3x\text{+}2\right)\text{ - }\underbrace{\left(\left(x^3\text{-}x^2\text{+}2x\text{+}1\right)*\left(x^2\text{+}2x\text{+}1\right)\right)}_{\left(x^5+x^4+x^3-x^2+4x+1\right)}\right]}_{3x^2-x+1}*\left(2x\text{+}2\right)=$$

$$\left(x^3\text{-}x^2\text{+}2x\text{+}1\right)\text{-}\underbrace{\left(3x^2\text{-}x\text{+}1\right)*\left(2x\text{+}2\right)}_{x^3-x^2+2}=\boxed{2x\text{-}1}$$

כעת נפתח את הסוגריים בביטוי הראשון:

$$=\left(x^5\text{+}x^4\text{+}x^3\text{+}2x^2\text{+}3x\text{+}2\right)\left(\text{-}(2x\text{+}2)\right)+\left(x^3\text{-}x^2\text{+}2x\text{+}1\right)\left(1\text{+}(x^2\text{+}2x\text{+}1)*(2x\text{+}2)\right)$$

$$=\left(x^5\text{+}x^4\text{+}x^3\text{+}2x^2\text{+}3x\text{+}2\right)\left(\text{-}2x\text{-}2\right)+\left(x^3\text{-}x^2\text{+}2x\text{+}1\right)\left(2x^3\text{+}x^2\text{+}x\text{+}3\right)=2x-1$$

וקיבלנו את הפונקציות הרצויות.

.3

$$\left[\begin{array}{l} x \\ \overline{x^4+1\,\big|\,x^3+1} \\ x^4+x \\ \hline 1-x \end{array}\right] \Rightarrow \left[\begin{array}{l} -x^2-x-1 \\ \overline{x^3+1\quad\big|\,-x+1} \\ {}^{-}x^3-x^2 \\ \hline x^2+1 \\ {}^{-}x^2-x \\ \hline x+1 \\ {}^{-}x-1 \\ \hline 2 \end{array}\right] \Rightarrow \frac{-x+1}{2} \equiv \frac{6x+8}{2} \equiv 3x+4 \pmod 7$$

כלומר בשלב האחרון - בחלוקה ב-2 קיבלנו שהשארית היא אפס, ולכן 2 מתפקד כ-ממג"ב. עם זאת, ניתן לראות שע"י כפל בסקלרים מ-Z7 ניתן לקבל גם מספרים אחרים, ובכלל זאת את 1:

$$\left(x^3\text{+}1\right)\text{ - }\underbrace{\left[\left(x^4\text{+}1\right)\text{ - }\left(x^3\text{+}1\right)*x\right]}_{1-x}*\left(-x^2-x-1\right)=2$$

$$=-\left(x^4\text{+}1\right)\left(-x^2-x-1\right)+\left(x^3\text{+}1\right)\left(1\text{+}x*(\text{-}x^2\text{-}x\text{-}1)\right)$$

$$=\left(x^4\text{+}1\right)\left(x^2+x+1\right)\ +\ \left(x^3\text{+}1\right)\left(\text{-}x^3\text{-}x^2\text{-}x\text{+}1\right)=2$$

וע"י כפל פי 4 ניתן לראות שהממג"ב 1 והפולינומים זרים.

$$=\left(x^4\text{+}1\right)\left(4x^2+4x+4\right)\ +\ \left(x^3\text{+}1\right)\left(\text{-}4x^3\text{-}4x^2\text{-}4x\text{+}4\right)=8\equiv 1 \pmod 7$$

אביב 2005
ליאור

אלגברה מודרנית - 104134 קבוצת תרגול 12

סמסטר אביב 2005 - שיעורי בית מס' 10# - אידאלים והומומורפיזם של חוגים

1. א. נראה קודם ש-Ia מקיים סגירות לחיבור ולהופכיים -

$$\forall x_1, x_2 \in I_a \;\; a(x_1 - x_2) = ax_1 - ax_2 = 0 - 0 = 0 \to x_1 - x_2 \in I_a$$

מאחר ש-Ia מוכל כולו בחוג R זהו תנאי מספיק להוכחה שהוא חבורה חיבורית. כעת עלינו להראות שהוא מקיים סגירות לכפל במטרה להוכיח שהוא תת חוג (תכונות האסוצ' והדיסט' נובעות ישירות מכך שהוא מוכל בחוג R).

$$\forall x_1, x_2 \in I_a \;\; a(x_1 x_2) = (ax_1)x_2 = 0x_2 = 0 \to x_1 x_2 \in I_a$$

כעת יש להראות שמתקיימת גם סגירות לכפל מימין בכל איבר מ-R (עקרונית, ניתן היה להסתפק רק בכך מאחר ש-R מכיל ממילא את כל האיברים ב-Ia ולכן הוכחה זו מראה גם את הסגירות של Ia לכפל בהוכחה שהוא חוג)

$$\forall x \in I_a, r \in R \;\; a(xr) = (ax)r = 0r = 0 \to xr \in I_a \to I_a \underset{right}{\lhd} R$$

ב. באותו אופן כמו בסעיף הקודם - נראה תחילה שזה תת חבורה חיבורית

$$\forall ax_1, ax_2 \in I_a \;\; ax_1 - ax_2 = a(\underbrace{x_1 - x_2}_{\in R}) \in I_a$$

ונראה סגירות לכפל מימין עבור **כל איבר** ב-R, (ובפרט סגירות לכפל שני איברים מתוך Ia) -

$$\forall ax \in I_a, r \in R \;\; (ax)r = a\underbrace{(xr)}_{\in R} \in I_a \to I_a \underset{right}{\lhd} R$$

4. נכנה את קבוצת כל הנילפוטנטים בשם M.

ראשית נראה שזהו תת חוג. היותו תת חבורה חיבורית נובע מכך :

$$\forall x, y \in M \;\; \exists n, m \in \mathbb{N} : \; x^n = y^m = 0$$

$$(x-y)^{n+m} = x^{n+m} - x^{n+m-1}y + x^{n+m-2}y^2 - \ldots + x^n y^m - x^{n-1}y^{m+1} + \ldots - xy^{n+m-1} + y^{n+m}$$

$$= \cancel{x^n x^m} + \cancel{x^n x^{m-1} y} + \cancel{x^n x^{m-2} y^2} + \ldots + \cancel{x^n y^m} + \cancel{x^{n-1} y^m y} + \ldots \cancel{xy^{n-1} y^m} + \cancel{y^n y^m}$$

$$= 0x^m + 0x^{m-1}y + 0x^{m-2}y^2 + \ldots + 0*0 + x^{n-1}0y + \ldots xy^{n-1}0 + y^n 0 = 0$$

(אין חשיבות לסימנים של איברי הבינום מאחר שכולם מתאפסים ממילא). אם כן, מצאנו חזקה (n+m) שמאפסת את האיבר x-y כלומר גם הוא נילפוטנט. סגירות לכפל היא קצת יותר פשוטה - $\forall \underset{x^n = y^m = 0}{x, y \in M} \;\; (xy)^{nm} = x^{nm} y^{nm} = (x^n)^m (y^m)^n = 0*0 = 0$ (נעזרנו בקומוטטיביות).

אם כן, זהו תת חוג כעת, לפי הגדרת האידאל - צריך להוכיח. $\forall a \in M, r \in R \overset{?}{\to} ar \in R.$ (הואיל והחוג קומוטטיבי מספיק להוכיח אידאל מכיוון אחד) : נעזר בקומוטטיביות -

$$a \in M \to \exists n \in \mathbb{N}, \;\; a^n = 0 \to (ar)^n = a^n r^n = 0r^n = 0 \Rightarrow ar \in R$$

5. נראה שחיתוך האידאלים השמאליים הוא אידאל שמאלי עפ"י ההגדרה.

$$I,J \underset{left}{\lhd} R \to \forall i \in I,\ j \in J, r \in R:\ ri \in I,\ rj \in J$$

$$\forall x \in I \bigcap J,\ r \in R \quad \to \quad \underbrace{rx \in I}_{I \bigcap J \subseteq I \to x \in I} \ , \ \underbrace{rx \in J}_{I \bigcap J \subseteq J \to x \in J} \to rx \in I \bigcap J$$

באשר לחיתוך של אידאלים שמאלי וימני:

$$I \underset{right}{\lhd} R, J \underset{left}{\lhd} R \to \forall i \in I,\ j \in J, r \in R:\ ir \in I,\ rj \in J$$

$$\forall x, y \in I \bigcap J:$$

$$\left.\begin{array}{l} x, y \in I \to (x-y) \in I,\ xy \in I \\ x, y \in J \to (x-y) \in J,\ xy \in J \end{array}\right\} (x-y), xy \in I \bigcap J$$

כלומר החיתוך מקיים סגירות לחיבור ולכפל ולכן הוא **תת חוג.** כמו כן:

$$\forall k \in I \bigcap J,\ r \in R \to kr \in I,\ rk \in J$$

ומכך ניתן לראות שאם החוג קומוטטיבי אז מתקיים kr=rk ואז המכפלה שייכת גם ל-I וכם ל-J כלומר לחיתוך, דהיינו עבור חוג קומוטטיבי חיתוך האידאל השמאלי והימני יהיה אידאל (למעשה ניתן היה לומר זאת מייד מאחר שבחוג קומוטטיבי אין חשיבות לכיוון האידאל

פרק ד'

3.

א. נבנה העתקה כללית - כדי שההעתקה תשמר את פעולת החיבור עליה להיות בראש ובראשונה הומומורפיזם בין חבורות - נזכר בצורה הכללית להעתקה מעין זו עבור פעולת החיבור, ונכפה עליה לקיים את התנאי הדומה גם עבור הכפל:

$\varphi: \mathbb{Z} \to \mathbb{Z}_{10}$, $\varphi(x)=nx \pmod{10}$

$x,y \in \mathbb{Z} \to \varphi(x+y)=n(x+y)=nx+ny=\varphi(x)+\varphi(y) \pmod{10}$

$\varphi(xy)=n(xy) \quad \varphi(x)\varphi(y)=nxny=n^2xy \pmod{10}$

$n=n^2 \pmod{10}$

תשומת לב ששתי הפעולות בחוגים Z ו-Z_{10} קומוטטיביות ולכן היה ביכולתנו לבודד את n. אם כן התנאי שקיבלנו הוא ש-n יהיה אידמפוטנט ב-Z_{10} - המספרים המקיימים זאת הם $0^2=0$, $1^2=1$, $5^2=25\equiv 5 \pmod{10}$, ו-$6^2=36\equiv 6 \pmod{10}$. לכן ההומומורפיזמים הם

$\varphi(x)\equiv 0$ (ההומומורפיזם האפס); $\varphi(x)=x$ או $5x$, $6x \pmod{10}$

ב. בסעיף זה דרך הפעולה היא זהה, למעט הדרישה שהתקבלה בסעיף האחרון - הדרישה לאדימפוטנטיות, שצריכה להתקיים בתמונת ההעתקה, כלומר הפעם ב-Z עצמה, ולכן נדרשים מספרים שלמים המקיימים $n^2=n$ - $n(n-1)=0$ (ניתן להעביר אגף כי יש הופכיים לחיבור, ולהוציא n לפי חוק הפילוג בחוג). המספרים היחידים המקיימים זאת ב-Z הם 0 ו-1 (כי אין מחלקי אפס), ולכן יתכנו רק הומומורפיזם האפס $\varphi(x)\equiv 0$ והומומורפיזם הזהות $\varphi(x)=x$.

5.נראה שזו תת חבורה חיבורית (של חבורת המטריצות 2x2 - החיבור הוא קומוטטיבי זה), ונוסיף את הדרישה לסגירות לכפל.

$$\begin{pmatrix} a & -b \\ b & a \end{pmatrix} - \begin{pmatrix} c & -d \\ d & c \end{pmatrix} = \begin{pmatrix} a-c & -b+d \\ b-d & a-c \end{pmatrix} \in R$$

$$\begin{pmatrix} a & -b \\ b & a \end{pmatrix}\begin{pmatrix} c & -d \\ d & c \end{pmatrix} = \begin{pmatrix} ac-bd & -ad-bc \\ bc+ad & -bd+ac \end{pmatrix} \in R$$

מתקיימת סגירות וזהו תת חוג

כעת נבדוק גם את הכפל בכיוון השני:

$$\Updownarrow =$$

$$\begin{pmatrix} c & -d \\ d & c \end{pmatrix}\begin{pmatrix} a & -b \\ b & a \end{pmatrix} = \begin{pmatrix} ca-db & -cb-da \\ da+cb & -db+ca \end{pmatrix}$$

כלומר גם פעולת הכפל היא קומוטטיבית. מאחר שהחוג מוכל בכל המטריצות 2x2 איבר היחידה שלו יהיה מטריצת I בגודל 2x2, ואכן מטריצה זו שייכת ל-R עפ"י התנאים (a=1,b=-b=0).

ב. נגדיר העתקה ונראה שהיא מוגדרת היטב והומומורפיזם.

$$\varphi: \mathbb{R}^{2\times 2} \to \mathbb{C}\ ,\ \varphi_{\left(\begin{smallmatrix} a & -b \\ b & a \end{smallmatrix}\right)} = a+bi$$

$$\begin{pmatrix} a & -b \\ b & a \end{pmatrix} = \begin{pmatrix} c & -d \\ d & c \end{pmatrix} \Rightarrow a+bi = c+di$$

$$\varphi_{\left(\begin{smallmatrix} a & -b \\ b & a \end{smallmatrix}\right)} + \varphi_{\left(\begin{smallmatrix} c & -d \\ d & c \end{smallmatrix}\right)} = a+bi+c+di = (a+c)+i(b+d) = \varphi_{\left(\begin{smallmatrix} a+c & -b-d \\ b+d & a+c \end{smallmatrix}\right)}$$

$$\varphi_{\left(\begin{smallmatrix} a & -b \\ b & a \end{smallmatrix}\right)}\varphi_{\left(\begin{smallmatrix} c & -d \\ d & c \end{smallmatrix}\right)} = (a+bi)(c+di) = (ac-bd)+i(ad+bc) = \varphi_{\left(\begin{smallmatrix} ac-bd & -ad-bc \\ bc+ad & -bd+ac \end{smallmatrix}\right)} = \varphi_{\left(\left(\begin{smallmatrix} a & -b \\ b & a \end{smallmatrix}\right)\left(\begin{smallmatrix} c & -d \\ d & c \end{smallmatrix}\right)\right)}$$

כעת נמצא את הגרעין שלה ונפעיל את משפט ההומומורפיזם הראשון (לחוגים)

$$\ker(\varphi) = \left\{ \begin{pmatrix} a & -b \\ b & a \end{pmatrix} : a+bi = 0 \right\} = \left\{ \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \right\}$$

$$\mathbb{R}^{2\times 2} = \mathbb{R}^{2\times 2} \Big/ \{0\} = \mathbb{R}^{2\times 2} \Big/ \ker(\varphi) \cong \mathrm{Im}(\varphi) = \mathbb{C}$$

8. א. נביא בקצרה את מהלך ההוכחה משאלה 11 בפרק א, תוך החלפת ה-2 בשורש במספר שלם n: בשלב ראשון נוכיח ש-$\mathbb{Q}\left[\sqrt{n}\right]$ חבורה חיבורית. מאחר שהיא מוכלת בממשיים מספיק להוכיח שזו תת חבורה. 0 שייך ל-$\mathbb{Q}\left[\sqrt{n}\right]$, ולכן היא אינה ריקה. כמו כן, לכל x,y ב-$\mathbb{Q}\left[\sqrt{n}\right]$, מתקיים $(x_1-y_1\sqrt{n})+(x_2-y_2\sqrt{n})=(x_1-x_2)+\sqrt{n}(-y_1-y_2) \in \mathbb{Q}\left[\sqrt{n}\right]$ (החבורה אבלית כי חיבור ממשיים קומוטטיבי). כעת נראה סגירות לכפל - יהיו x,y ב-$\mathbb{Q}\left[\sqrt{n}\right]$, $x=a+b\sqrt{n}$, $y=c+d\sqrt{n}$: $xy=(a_1+b_1\sqrt{n})(a_2+b_2\sqrt{n})=(a_1a_2+nb_1b_2)+\sqrt{n}(a_1b_2+a_2b_1)$, והתוצאה היא

אביב 2005
ליאור

בחבורה מאחר שגם כפל רציונאלים הוא ב-Q. מאחר שזוהי פעולת הכפל הרגילה, היא גם קומוטטיבית ומתקיים xy=yx.

את תכונות האסוציאטיביות והדיסטריביוטיביות אנו מקבלים משדה הממשים, כיוון ש- $\mathbb{Q}\left[\sqrt{n}\right]$ מוכל בתוכו והפעולות עליו הן הרגילות. מכאן שזהו חוג קומוטטיבי.

היחידה היא אותה יחידה של הממשיים כיוון ש-1 שייך ל- $\mathbb{Q}\left[\sqrt{n}\right]$.

כעת נראה שזהו תחום שלמות - יהי x(≠0) איבר ב- $\mathbb{Q}\left[\sqrt{n}\right]$ - נחפש איבר y(≠0) כך ש- xy=0:

$$xy=(a+b\sqrt{n})(c+d\sqrt{n})=(ac+nbd)+\sqrt{n}(ad+bc)=0$$

$$\left.\begin{matrix}ac+nbd=0\\ad+bc=0\end{matrix}\right\}\begin{matrix}\cdot d\\ \cdot c\end{matrix}\rightarrow\left\{\begin{matrix}acd+nbd^2=0\\acd+bc^2=0\end{matrix}\right\}\rightarrow b(nd^2-c^2)=0$$

והאפשרויות להתאפסות הן:

$$1)\ b=0\rightarrow\left\{\begin{matrix}(a=0)\ or\ (c=0)\\(a=0)\ or\ (d=0)\end{matrix}\right\}a=0\rightarrow x=(a+b\sqrt{n})=0$$

$$2)nd^2=c^2\rightarrow c=\pm d\sqrt{n}$$

ניתן לראות שהאפשרות השניה עומדת בסתירה לכך שהמקדמים רציונאליים, ואילו האפשרות ש-b=0 מחייבת a=0 ולכן x=0 וזו גם סתירה. על כן, $\mathbb{Q}\left[\sqrt{n}\right]$ הוא תחום שלמות.

לבסוף - נראה שזהו שדה - עפ"י ההגדרה לשדה - נותר לנו רק לדרוש שהחוג הקומוטטיבי שלנו (שהוא עם יחידה) יהיה גם עם חילוק, כלומר שלכל איבר השונה מאפס יהיה הופכי. יהי x ב- $\mathbb{Q}\left[\sqrt{n}\right]$ - צריך להוכיח שקיים y ב- $\mathbb{Q}\left[\sqrt{n}\right]$ כדלקמן:

$$x=(a+b\sqrt{n})\qquad y=(c+d\sqrt{n})\qquad xy=(a+b\sqrt{n})(c+d\sqrt{n})=(ac+nbd)+\sqrt{n}(ad+bc)=1$$

נבדוק אפשרויות (נדרוש שהמקדמים יהיו רציונליים):

$$\left\{\begin{matrix}(*)\ ac+nbd=1\\(**)\ ad+bc=0\end{matrix}\right\}$$

$$1)b=0\underset{(x\neq 0)}{\rightarrow}a\neq 0\rightarrow d=0\rightarrow ac=1\Rightarrow c=1/a\left(\in\mathbb{Q}\right)$$

$$2)a=0\underset{(x\neq 0)}{\rightarrow}b\neq 0\underset{**}{\rightarrow}c=0,d\neq 0\rightarrow nbd=1\Rightarrow d=1/nb\left(\in\mathbb{Q}\right)$$

$$3)a,b\neq 0\underset{*}{\rightarrow}c=\frac{1-nbd}{a}\underset{**}{\rightarrow}ad+\frac{b-nb^2d}{a}=0\rightarrow d(a-nb^2/a)+b/a=0\rightarrow$$

$$d=\frac{b/a}{nb^2/a-a}=\underbrace{\frac{b}{nb^2-a^2}\left(\in\mathbb{Q}\right)}_{\left(nb^2-a^2\neq 0\ \leftarrow nb^2\neq a^2\ \leftarrow\sqrt{n}b\neq\pm a\ \leftarrow a,b\in\mathbb{Q}\right)}\qquad c\underset{**}{=}\frac{-a}{b}d=\frac{-a}{nb^2-a^2}\left(\in\mathbb{Q}\right)$$

$$\Rightarrow c,d\in\mathbb{Q}\qquad\Rightarrow\qquad y=\frac{b\sqrt{n}-a}{nb^2-a^2}\in\mathbb{Q}\left[\sqrt{n}\right]$$

כלומר יש הופכי לכל איבר (למעט עבור x=0), והוא בחוג.

המסקנה היא שלכל n - $\mathbb{Q}\left[\sqrt{n}\right]$ הוא שדה, ולכן בפרט עבור n=3,5.

ב. ננסה לבדוק באמצעות העתקה טריוויאלית האם ניתן לעבור ישירות -

אביב 2005
ליאור

$$\varphi:\mathbb{Q}\left[\sqrt{3}\right]\to\mathbb{Q}\left[\sqrt{5}\right]$$
$$\varphi(a+\sqrt{3}b)=a+\sqrt{5}b$$

העתקה זו מוגדרת היטב ועל מאחר שאנחנו שומרים על וקטורי המקדמים. נבדוק האם היא הומומורפיזם:

$$\varphi_{\left((a+\sqrt{3}b)+(c+\sqrt{3}d)\right)}=\varphi_{\left((a+c)+\sqrt{3}(b+d)\right)}=(a+c)+\sqrt{5}(b+d)=(a+\sqrt{5}b)+(c+\sqrt{5}d)=\varphi_{\left(a+\sqrt{3}b\right)}+\varphi_{\left(c+\sqrt{3}d\right)}$$

$$\varphi_{\left((a+\sqrt{3}b)*(c+\sqrt{3}d)\right)}=\varphi_{\left((ac+3bd)+\sqrt{3}(ad+bc)\right)}=(ac+3bd)+\sqrt{5}(ad+bc)$$

$$\not\Updownarrow$$

$$\varphi_{\left(a+\sqrt{3}b\right)}\varphi_{\left(c+\sqrt{3}d\right)}=(a+\sqrt{5}b)(c+\sqrt{5}d)=(ac+5bd)+\sqrt{5}(ad+bc)$$

כלומר זה אינו הומומורפיזם ביחס לכפל.
נראה שלא קיים אף הומומורפיזם שעונה על הדרישות - נניח שקיים איזומורפיזם כזה -

$$\varphi:\mathbb{Q}\left[\sqrt{5}\right]\to\mathbb{Q}\left[\sqrt{3}\right]$$

שני התחומים הם שדות כך שיש בהם יחידה. מתקיים $\varphi(1)=1$ - מאחר שזה אמור להיות הומומורפיזם, הוא חייב להעתיק את איבר היחידה מהתחום ליחידה של התמונה $\varphi(x)=\varphi(x*1_{\mathbb{Q}[\sqrt{5}]})=\varphi(x)\varphi(1_{\mathbb{Q}[\sqrt{5}]})=\varphi(x)*1_{\mathbb{Q}[\sqrt{3}]}$. לכן מתקיים גם $\varphi(n)=n$:

$$\varphi(3)=3=\varphi(\sqrt{3}\sqrt{3})=\varphi(\sqrt{3})\varphi(\sqrt{3})=(a+\sqrt{5}b)(a+\sqrt{5}b)=a^2+5b^2+2\sqrt{5}ab$$

$$ab=0\underset{a,b\in\mathbb{Q}}{\Rightarrow}a=0\ \ or\ \ b=0$$

כעת מהשוואת מקדמים נראה $a^2+5b^2=3\ \Rightarrow\begin{cases}a^2=3\to a=\sqrt{3}\\5b^2=3\to b\ \sqrt{3/5}\end{cases}$

ההנחה הראשונה נובעת מכך שברציונאליים אין מחלקי אפס (שדה), ובשורה השניה מתקבלת סתירה לכך ש-a,b הם רציונאליים כלומר סתירה לכך שקיים הומומורפיזם כזה.

אביב 2005
ליאור

אלגברה מודרנית - 104134 קבוצת תרגול 12

סמסטר אביב 2005 - שיעורי בית מס' 11# - אידאלים מקסימליים

פרק ו'

2. א. נראה שזו חבורה (2+1) וחוג (3):

$$M+Ra=\{m+ra \mid m\in M, r\in R\}$$

1) $0\in M, R \to 0+0\cdot a\in M+Ra\neq\phi$

2) $\forall m_1,m_2\in M,\ r_1,r_2\in R:\ \ (m_1+r_1a)-(m_2+r_2a)\underset{*}{=}(m1-m2)+(r_1-r_2)a\in M+Ra$

3) $\forall m_1,m_2\in M,\ r_1,r_2\in R:\ \ (m_1+r_1a)(m_2+r_2a)=(m_1m_2)+(m_1r_2+r_1m_2)a+(r_1a)(r_2a)$

$$\underset{**}{=}(m_1m_2)+(\underbrace{m_1r_2+r_1m_2}_{=m_3+m_4\in M})a+(r_1r_2aa)=m_5+\underbrace{m_6}_{\in M}a+\underbrace{(ra)}_{\in R}a\in M+Ra$$

שוויון * ב-2 נובע מקומוטטיביות החיבור, והיכולת להוציא את a מחוץ לסוגריים בשדה (פילוג)

שוויון ** ב-3 נובע מהקומוטטיביות בכפל בחוג R, ומכך ש-M אידאל ולכן בולע את r או את a.

ב. נראה שזה אידאל בכיוון אחד

$$M+Ra=\{m+ra \mid m\in M, r\in R\}$$

$$\forall m\in M,\ r,x\in R:\ \ (m+ra)x\underset{*}{=}(mx+rax)\underset{**}{=}\tilde{m}+(rx)a\underset{***}{=}\tilde{m}+\tilde{r}a\in M+Ra$$

* - M הוא אידאל, ** - R קומוטטיבי, *** - R חוג ולכן סגור לכפל.

מאחר שהחוג קומוטטיבי אין צורך להוכיח שזהו גם אידאל בכיוון השני.

ג. נראה שכל איבר ב-M שייך גם ב-M+Ra, אבל יש איברים ב-M+Ra שאינם ב-M

$$\left.\begin{array}{l}1)\ \forall m\in M,\ m=m+0\cdot a\in M+Ra\to M\subseteq M+Ra\\ 2)\ a\notin M,\quad a=0_M+1\cdot a\in M+Ra\to M\neq M+Ra\end{array}\right\}M\subset M+Ra$$

ד.

$$\left.\begin{array}{l}\ldots\to M\underset{\neq}{\subset}M+Ra\\ (M+Ra)\lhd R\\ M\underset{\max}{\lhd}R\end{array}\right\}M+Ra=R$$

הראינו כבר ש-M+Ra הוא אידאל ב-R ושהוא מכיל ממש את M, אבל מאחר שנתון ש-M אידאל מקסימלי, הרי ש-M+Ra חייב להיות R כולו.

ה. הראינו שעבור המקרה ש-a לא שייך ל-M, כל איבר ב-R ניתן לייצוג כאיבר ב-M+Ra, נקח איבר כללי ב-R ונכפול ב-b:

$$a\notin M\to\ldots\to M+Ra=R$$

$$Rb=(m+ra)b=mb+rab=\tilde{m}+r\tilde{\tilde{m}}\in M\to Rb\in M$$

$$M=\{x\in R \mid Rx\in M\}\to b\in M$$

מאחר שהתוצאה היא תמיד ב-M, קיבלנו ש-b מקיים את הגדרת האידאל של M.

5. א'. נראה ש-8Z הוא אידאל. קל לראות שזהו חוג הודות לכך ש-Z הוא חוג -

$$8\mathbb{Z}=\{8x \mid x\in\mathbb{Z}\}$$

$$0\in 8\mathbb{Z}\neq\phi\ ;\ \forall \underbrace{8a,8b\in 8\mathbb{Z}}_{(a,b\in\mathbb{Z})},\ 8a-8b=8\underbrace{(a-b)}_{\in\mathbb{Z}}\in 8\mathbb{Z}\ ;\ \forall 8a,8b\in 8\mathbb{Z},\ 8a\cdot 8b=8\underbrace{(8ab)}_{\in\mathbb{Z}}\in 8\mathbb{Z}$$

ושהוא אידאל ב-4Z (ולמעשה בכל nZ) -

$$8\mathbb{Z}\subset 4\mathbb{Z}$$

$$\forall 8a\in 8\mathbb{Z},\ 4b\in 4\mathbb{Z}\ \rightarrow\ 8a\cdot 4b=8\underbrace{(4ab)}_{\in\mathbb{Z}}\in 8\mathbb{Z}\rightarrow 8\mathbb{Z}\lhd 4\mathbb{Z}$$

$$\left(\forall n\mathbb{Z}\subset 4\mathbb{Z}\rightarrow\forall na\in n\mathbb{Z},4b\in 4\mathbb{Z},\ \ na\cdot 4b=n(4ab)\in n\mathbb{Z}\rightarrow n\mathbb{Z}\lhd 4\mathbb{Z}\right)$$

כדי לקבל את התנאי ש-nZ מוכל ב-4Z, נדרש כמובן 4|n (4 מחלק את n). קל לראות שהאידאלים ב-4Z יהיו 4Z עצמו, 8Z, וכן הלאה. המקסימלי מביניהם שאינו 4Z עצמו, הוא לפיכך 8Z.

לחלופין ניתן להניח כי קיים אידאל I בין החוג 4Z לאידאל 8Z, שמקיים:

$$\exists I\lhd 4\mathbb{Z},\quad 8\mathbb{Z}\underset{\neq}{\subset} I\subset 4\mathbb{Z}$$

$$\exists x\in I\subset 4\mathbb{Z},\ \ x=4n,\quad x\notin 8\mathbb{Z}\rightarrow 2\nmid n\rightarrow 2\mid(n+1)$$

$$4(n+1)\in 8\mathbb{Z}\underset{8\mathbb{Z}\subset I}{\rightarrow}4(n+1)\in I\rightarrow 4n+4\in I\underset{4n\in I}{\rightarrow}4\in I\rightarrow\forall k\in\mathbb{Z},\ \ 4k\in I\rightarrow I=4\mathbb{Z}$$

ולכן I שווה 4Z כלומר 8Z הוא מקסימלי.

ב. ניתן לראות שהקוסטים בחוג המנה הם 8Z ו-8Z+4 (כיוון ש-8Z+4n שווה לקוסט 8Z כאשר n זוגי, ולקוסט 8Z+4 כאשר n אי-זוגי). נדרוש ש-8Z יהיה איבר האפס בחוג המנה.

(כפל קוסטים) *	**8Z**	**8Z+4**
8Z	8Z	8Z
8Z+4	8Z	8Z+16=8Z

קיבלנו ש-8Z=(8Z+4)*(8Z+4), כלומר 8Z+4 הוא מחלק אפס ולכן חוג המנה אינו תחום שלמות ולא יכול להיות שדה. (ניתן גם לומר שהמכפלה אינה שווה לאף אחד מהנכפלים ולכן זהו אינו איבר היחידה כלומר לא קיים איבר יחידה ולכן זה אינו שדה).

ג. חוג מנה אמור היה להיות שדה כאשר האידאל בו מחלקים הוא מכסימלי, אולם ניתן לראות במקרה זה שהחוג המקורי - 4Z אינו חוג עם יחידה, ולכן תנאי המשפט לא מתקיימים (מאחר שכדי לקבל בלוח הכפל איבר יחידה בחוג המנה - nZ+1 - אנו צריכים מכפלה של איברים ב-nZ שתתן לנו אחד (מעל nZ) ולכן נדרש n=1.

אביב 2005
ליאור

פרק ז'

2. משפט פרמה הקטן - אם a שונה מ-0 וזר ל-p

$$p \mid a^p - a \to a^p = qp + a \to a^p = a \pmod p \to a^{p-1} = 1 \pmod p$$

$$\mathbb{Z}_5 : p = 5 \to a^4 = 1$$

$$3x^{44} + 2x^{57} + 3x^{74} + 2x^{219} = 3\underbrace{(x^{\overbrace{4}^{44}})^{11}}_{1} + 2x\underbrace{(x^{\overbrace{4}^{56}})^{14}}_{1} + 3x^2\underbrace{(x^{\overbrace{4}^{72}})^{18}}_{1} + 2x^3\underbrace{(x^{\overbrace{4}^{216}})^{54}}_{1}$$

$$= 3 + 2x + 3x^2 + 2x^3 = \underbrace{(3+2x)}_{\substack{\equiv 3-3x \\ x=1}}\underbrace{(1+x^2)}_{x^2=-1}$$

$$(3+2x)(1+x^2)\begin{cases} x^2 = -1 \equiv 4 \pmod 5 \to x = \pm 2 \equiv 2,3 \\ 3 = -2x = 3x \pmod 5 \to x = 1 \end{cases}$$

מאחר ש-p שבחרנו הוא 5, כל המספרים ב-Z5 זרים לו ולכן תנאי המשפט מתקיימים. נוסיף רק את התוצאה שנשמטה עבור a=0 מאחר שגם x=0 מאפס את המשוואה, ונקבל 0,1,2,3

4. I הוא למעשה חוג הפולינומים עם מקדמים בחוג 2Z, ולכן יתנהג כמוהו - בחיבור פולינומים המקדמים ישמרו על סגירות ב-2Z וקיימים להם ההופכיים החיבוריים, כלומר I הוא חבורה חיבורית. גם כפל פולינומים מ-I ישמור על סגירות מאחר שעבור כל המקדמים כפל מספרים זוגיים יהיה זוגי, ולכן I היא חוג (האסוציאטיביות והדיסטריביוטיביות נובעות מהכלה בחוג כלל הפולינומים עם מקדמים שלמים). העובדה שזהו אידאל נובעת מכך שגם אם אחד הפולינומים אינו מ-I, עדיין בכל אחת ממכפלות המקדמים של חזקות x ישתתף גורם מהפולינום ב-I, ומכפלת מספר זוגי באיזוגי גם היא זוגית.
נראה בקצרה באופן סימבולי:

$$654 + 738x^5 - 132x^{16} \in I \neq \phi$$

$$\forall f, g \in I : \ f = \sum (2a_i)x^i, \ g = \sum (2b_i)x^i, \ a_i, b_i \in \mathbb{Z} \to \ f - g = \sum (2a_i - 2b_i)x^i = \sum 2(a_i - b_i)x^i \in I$$

$$\forall f \in I, \ g \in \mathbb{Z}_{[x]} : \ f = \sum (2a_i)x^i, \ g = \sum b_i x^i, \ \ a_i, b_i \in \mathbb{Z} \ \to fg = \sum_{i,j} (2a_i \cdot b_j)x^{i+j} = \sum_{i,j} 2(a_i b_j)x^{i+j} \in I$$

הוכחת האידאל מכילה את הסגירות לכפל. מספיק להוכיח בכיוון אחד מאחר שהכפל והחיבור קומוטטיביים.

ב. נראה ש-I אינו מקסימלי:

נניח בשלילה ש-I מקסימלי ונביט על חוג המנה Z[x] / I. איבר האפס בחוג זה הינו I, ואיבר היחידה יהיה I+1 (מאחר שהנייטראלי בפעולת כפל פולינומים מעל Z הוא 1).
כעת נביט על האידאל M:

אביב 2005
ליאור

$$M := \{i + ra \mid i \in I, r \in \mathbb{Z}_{[x]},\ a \notin I\} \quad I \subseteq M$$

1) $M \neq \phi$

2) $\forall i_1, i_2 \in I,\ r_1, r_2 \in \mathbb{Z}_{[x]} \quad (i_1 + r_1 a) - (i_2 + r_2 a) = (i_1 - i_2) + (r_1 - r_2)a \in M$

3) $\forall i \in I, r, f \in \mathbb{Z}_{[x]},\ \ (i + ra)f = if + fra = \tilde{i} + \tilde{r}a \in M \ \Rightarrow\ M \lhd Z_{[x]}$

$a \notin I,\ 0 \in I,\ 1 \in \mathbb{Z}_{[x]} \rightarrow 0 + 1 \cdot a = a \in M \rightarrow I \underset{\neq}{\subset} M,\ \ I \underset{\max}{\lhd} \mathbb{Z}_{[x]} \Rightarrow M = Z_{[x]}$

$1 \in \mathbb{Z}_{[x]} \rightarrow 1 \in M \rightarrow \exists i_0 \in I, r_0 \in \mathbb{Z}_{[x]} :\ 1 = i_0 + r_0 a$

$$in\ \ {}^{\mathbb{Z}_{[x]}}\!/_{I} : I + 1 = I + (i_0 + r_0 a) = \underbrace{(I + i_0)}_{0} + (I + r_0 a) = (I + r_0)(I + a)$$

כלומר מצאנו הופכי לכל איבר מהצורה I+a שהוא איבר בחוג המנה שאינו ה-0 של חוג זה (כלומר אינו I), ולכן אם הנחנו ש-U מקסימלי אזי חוג המנה צריך להיות שדה (זהו משפט שהוזכר בכיתה)

כעת, I+1 הוא איבר היחידה בשדה זה. נבחר את האיבר x+I שהוא איבר נוסף בחוג המנה, ונחפש את ההופכי שלו (שחייב להתקיים אם זהו שדה):

$$(I + x)(I + P_{(x)}) = I + 1 \rightarrow I + xP_{(x)} = I + 1 \rightarrow xP_{(x)} - 1 \in I$$

וזו סתירה כי ב-I לא קיימים פולינומים עם מקדמים אי זוגיים (והמקדם החופשי כאן הוא 1).

מכאן שלא יתכן ש-I מקסימלי.

פרק ח'.

א. הפולינום x^2+x+1 אינו פריק מעל Z_2 מאחר שאין לו שורשים שם והוא ממעלה 2

ב. גם x^2+1 אינו פריק מעל Z_7 מאותה סיבה (אי קיום שורשים בפולינום ממעלה 2).

ג. נבחר p=3 ונראה שהוא מחלק את מקדמי הפולינום מלבד המקדם של האיבר הראשון, ואילו $3^2=9$ אינו מחלק את המקדם החופשי 3, ולכן לפי קריטריון איזנשטיין (בהנחה שנלמד בהרצאות) זהו פולינום שאינו פריק.

ד. x^2-12 אינו פריק כי אין לושורש ברציונאליים - $\sqrt{12} \notin \mathbb{Q}$

ה. ניתן לראות שהמספר 3 מחלק את כל מקדמי הפולינום מלבד המקדם של האיבר הראשון בו (8), וש-$3^2=9$ אינו מחלק את האיבר החופשי (24) ולכן עפ"י קריטריון איזנשטיין פולינום זה אינו פריק.

ו. קל לראות שהפולינום פריק מאחר ש- $\pm\sqrt[4]{2}$ הם שורשים שלו מעל הממשיים, ולכן הוא ניתן לפירוק - $x^4 - 2 = (x^2 - \sqrt{2})(x^2 + \sqrt{2}) = (x - \sqrt[4]{2})(x + \sqrt[4]{2})(x^2 + \sqrt{2})$ (למעשה מספיק להראות את השלב הראשון)

ז. ניתן לראות שלפולינום אין שורשים שפותרים אותו ב-Z_2, ומאחר שמעלתו היא 3 די בכך להראות שהוא אינו פריק.

ח. ניתן לראות ש-5 מחלק את כל המקדמים מלבד הראשון, ומאחר ש-$5^2=25$ אינו מחלק את 30 הרי שהפולינום אינו פריק לפי אייזנשטיין.

4. מאחר שאנו יודעים שורש אחד של הפולינום, נוכל לפרק אותו מעל Q לגורם (x-r/s) כפול פונקציה נוספת, אבל בכדי שנוכל לפרק אותו מעל Z נרצה להשתמש דווקא בפונקציה עם מקדמים שלמים בתור המחלק שלו, ולכן נבחר את (sx-r) כגורם שמאפס את המשוואה, כלומר הפונקציה הנתונה היא בהכרח פריקה מעל Z[x] למכפלה מהצורה (sx-r) כפול פונקציה נוספת - f(x).

פונקציה f(x) זו תהיה בהכרח ממעלה m-1 מאחר שכפל שלה באיבר (sx-r) ממעלה 1 נותן את הפונקציה הנתונה ממעלה m. לכן נפתח את המכפלה ונקבץ חזקות דומות של x, ולאחר מכן פשוט נשווה את מקדמי החזקות הרצויות של x (יהיה רק איבר אחד עם x^m ורק איבר אחד חופשי).

$$a_0 + a_1 x + a_2 x^2 + \ldots + a_m x^m = \sum_{i=0}^{m} a_i x^i = (sx - r) f_{(x)}$$

$$f_{(x)} = \sum_{i=0}^{m-1} b_i x^i, \quad \deg(f_{(x)}) = m-1$$

$$\sum_{i=0}^{m} a_i x^i = s \cdot x f_{(x)} - r \cdot f_{(x)} = sx \sum_{i=0}^{m-1} b_i x^i - r \sum_{i=0}^{m-1} b_i x^i$$

$$= \underbrace{\left(sx \cdot b_{m-1} x^{m-1} \right)}_{sb_{m-1}x^m} + \left(sb_{m-2} x^{m-1} + rb_{m-1} x^{m-1} \right) + \ldots\ldots + \left(sxb_0 x^0 + rb_1 x \right) + rb_0$$

$$a_m x^m = s \cdot b_{m-1} x^m \rightarrow a_m = sb_{m-1} \rightarrow \boxed{s \mid a_m}$$

$$a_0 = rb_0 \rightarrow \boxed{r \mid a_0}$$

אביב 2005
ליאור

אלגברה מודרנית - 104134 קבוצת תרגול 12

סמסטר אביב 2005 - שיעורי בית מס' 12#

פרק ט

1. נביט ב- $f(x)=2x^3+x^2+2x+2\in\mathbb{Z}_5[x]$ ונבדוק פריקות. מאחר שמדובר בפולינום ממעלה 3 מספיק לבדוק האם יש לו שורשים בשדה Z_5 -

$f(0)=2,\ f(1)=2,\ f(2)=26=1,\ f(3)=71=1,\ f(4)=154=4 \pmod 5$

אין שורשים ולכן הפולינום אינו פריק מעל Z_5 , ומכאן שהאידאל <f(x)> ב-$Z_5[x]$ הינו אידאל מקסימלי (כפי שהוכח בכיתה - כל אידאל אחר המכיל אותו ואינו שווה לו יהיה בהכרח כל $Z_5[x]$) נראה זאת בקצרה - נניח שקיים אידאל I כך ש- $\exists I:\ \langle f(x)\rangle\subset_{\neq} I\subset\mathbb{Z}_5[x]$. כל אידאל בחוג הפולינומים הוא ראשי, ועל כן $I=\langle h(x)\rangle$ ומאחר ש-f(x) עצמו שייך גם הוא ל-I הרי הוא כפולה של היוצר שלו, כלומר נובע ש- $f(x)=h(x)\cdot g(x)$. אולם אמרנו ש-f הוא אי פריק, ועל כן מתחייב ש-g הוא למעשה סקלר פשוט ב-Z_5. אם כך, הרי שגם 1 שייך ל-I (כי בחוג פולינומים אין חשיבות לכפל בסקלר), ועל כן I= $Z_5[x]$, ומכך עולה שהאידאל <f(x)> הוא מקסימלי. מכאן, עפ"י משפט שהוכח בכיתה, נובע שחוג המנה - $\mathbb{Z}_5[x]/\langle f(x)\rangle$ הוא שדה.

כעת משנוכחנו שחוג המנה הוא שדה, נמצא בו הופכי לאיבר $\overline{2x-1}=2x-1+\langle f(x)\rangle$. ראשית נייצג את כל הקוסטים בשדה זה ע"י פולינומים ממעלה קטנה מ-3, ונתייחס להופכי כאיבר כללי בחוג המנה. נכפול את האיברים ונשווה לאיבר היחידה בחוג זה, שהוא הקוסט 1+<f(x)>

$$\overline{(2x-1)}\cdot\overline{(ax^2+bx+c)}=\left(2x-1+\langle f(x)\rangle\right)\cdot\left(ax^2+bx+c+\langle f(x)\rangle\right)=$$
$$(2x-1)(ax^2+bx+c)+\langle f(x)\rangle=2ax^3+(2b-a)x^2+(2c-b)x-c+\langle f(x)\rangle=1+\langle f(x)\rangle$$
$$\left(2ax^3+(2b-a)x^2+(2c-b)x-c\right)-1\in\langle f(x)\rangle$$
$$\overline{2x^3}=\overline{-x^2-2x-2}$$
$$\overline{a(-x^2-2x-2)+(2b-a)x^2+(2c-b)x-c}=\bar{1}$$
$$\overline{(2b-2a)x^2+(2c-b-2a)x-c-2a}=\bar{1}$$
$$a=b,\quad 2c-2a-b=0\ \rightarrow\ 2c=3b$$
$$-c-2a=1\ \rightarrow\ c=-1-2a\ \rightarrow\ 2c=-2-4b=3b\rightarrow 7b=-2=2b$$
$$b=-1,\ a=-1,\ c=1$$
$$\left(\overline{2x-1}\right)^{-1}=\overline{-x^2-x+1}$$

ואכן -

$$(\overline{2x-1})(\overline{-x^2-x+1})=\overline{-2x^3-2x^2+2x+x^2+x-1}=\overline{-2x^3-x^2+3x-1}$$
$$\overline{\left(-2x^3-x^2+3x-1\right)+f(x)}=\overline{0+0+\cancel{5x}+1}=\bar{1}=1+\langle f(x)\rangle$$

3. נתחיל בדומה לתרגיל הקודם - ע"י נסיון לפרק את הפולינום. הוא ממעלה 3 ולכן מחפש שורשים ב-Z_3 :

$$f(0)=2,\quad f(1)=5=2,\quad f(2)=18=0 \pmod 3$$

הפעם ראינו שיש שורש ולכן הפולינום פריק. נמצא אותו ע"י חילוק ב-Z_3 :

כלומר הפירוק הוא

$$x^3+2x^2+2=(x-2)f(x)$$

$$x^3+2x^2+2=(x-2)(x^2+x+2)$$

$$\begin{array}{r|l} x^3+2x^2+2 & x-2 \\ \hline -\underline{x^3-2x^2} & x^2+x+2 \\ x^2+2 & \\ -\underline{x^2-2x} & \\ 2x+2 & \\ -\underline{2x-1} & \\ 3=0 & \end{array}$$

ב. נביט בקוסט $I+2x^2+1$ בחוג המנה $Z_3[x]\ /\ I$ נדרוש שיהיה לו הופכי בחבורת המנה (כלומר ממעלה קטנה ממש מהמעלה של I שהיא 3)

$$(2x^2+1+I)(ax^2+bx+c+I)=(2ax^4+2bx^3+(2c+a)x^2+bx+c)+I=1+I$$
$$a=0,\ b=0$$
$$ax^2+bx+c \Rightarrow c$$

מהדרישה נובע שהמקדמים a,b=0, ולכן **לא** קיים פולינום הופכי לפולינום הנתון בחוג המנה (סקלר לא יכול להיות ההופכי)

ג. מאחר שראינו ש- $x^3+2x^2+2=(x-2)(x^2+x+2)$, אנו יכולים לראות שמתקיים :

$$\overline{x^3+2x^2+2}=\bar{0} \quad \Leftrightarrow \quad (x^3+2x^2+2)+I=0+I$$
$$\left.\begin{array}{l} x-2+I=\overline{x-2}\neq\bar{0} \\ x^2+x+2+I=\overline{x^2+x+2}\neq\bar{0} \end{array}\right\} \overline{(x-2)}\cdot\overline{(x^2+x+2)}=\overline{x^3+2x^2+2}=\bar{0}$$

כלומר מצאנו שני איברים בחוג המנה ששונים מ-0 אך מכפלתם היא 0 (איבר האפס של חוג המנה).

4.א. לפי ההגדרה, האידאל הראשי הוא קבוצת כל המכפלות של x. מכפלת x בכל פולינום שהוא תתן פולינום שבו אין מקדם חופשי :

$$\langle x\rangle=\{x\cdot f_{(x)}\}\rightarrow\left\{x\cdot(a_0+a_1x+a_2x^2+\ldots+a_nx^n)\right\}=\left\{xa_0+a_1x^2+a_2x^3+\ldots+a_nx^{n+1}\right\}$$

ב. נביט על האידאל <x> וננסה להרחיב אותו לאידאל גדול יותר, I שאינו שווה לו. לפי סעיף א', האידאל כולל כבר את כל האידאלים בעלי מקדם חופשי 0, ולכן ההרחבה תהיה באמצעות סקלר x : $I=\langle x,t\rangle=\{\langle x\rangle+f\cdot t\}\quad t\in F,\quad f\in F[x]$. אולם, מאחר ש-F הוא שדה יש בו הופכיים, ולכן ניתן לכפול את t שבחרנו ב-t^{-1} ולקבל שאיבר היחידה של השדה F שייך ל-I, ועל כן האידאל I יהיה קבוצת כל הפולינומים F[x] :

$$t^{-1} \in F \rightarrow \tilde{f} = t^{-1} f \rightarrow \tilde{f} \cdot t = f t^{-1} t = f \rightarrow \{\tilde{f} \cdot t\} = \{f \mid f \in F[x]\} = F[x]$$

מכאן, שכל אידאל שגדול מ-<x> ב-F[x] יהיה חוג הפולינומים F[x] עצמו, ולכן האידאל <x> מקסימלי.

ג. נביט בסעיף הקודם ונראה שאם ננסה להוכיח באותו אופן, נתקע בשלב מציאת t^{-1} מאחר ש-Z אינו שדה ואין בו הופכיים לכל האיבר מלבד 1-/+. לכן נוכל למצוא אידאל המכיל את <x> ואינו שווה לכל Z[x].

ד. נקח בדומה לסעיף ב' את האידאל הבא:

$$I = \langle x, 2 \rangle = \{xg_{(x)} + 2f_{(x)} \mid \ f_{(x)}, g_{(x)} \in Z[x]\}$$
$$a,b \in I \rightarrow a - b = (xg_1 + 2f_1) - (xg_2 + 2f_2) = x(g_1 - g_2) + 2(f_1 - f_2) \in I$$
$$a,b \in I \rightarrow ab = (xg_1 + 2f_1)(xg_2 + 2f_2) = x(xg_1g_2 + 2f_1g_2 + 2g_1f_2) + 2(2f_1f_2) \in I$$
$$\langle x \rangle \subset_{\neq} I \subset_{\neq} \mathbb{Z}[x]$$

מאחר ש-אנו מוגבלים בבחירת הפונקציות f,g לכאלו שמקדמיהן שלמים, לא נוכל למצוא את ההופכי הכפלי של 2, ולכן נשאר עם פונקציות שהאיבר החופשי שבהן זוגי (זהו למעשה I - קבוצת כל הפונקציות עם מקדם חופשי זוגי). קל לראות ש-I מכיל ממש את <x> (אם נבחר f(x)=0), ומוכל ממש ב-Z[x] מאחר שאינו כולל למשל את איבר היחידה שלו (כי הוא בעל מקדם חופשי איזוגי).

6. מאחר שאנו מעל שדה סופי מספיק לבדוק את האפשרויות עבור n השייכות לו, וכל ערך אחר יהיה שקול לאחת מהן. עבור כל אחת מהאפשרויות נבדוק האם קיימים שורשים בשדה (כיוון שהפולינום ממעלה 3 זה מספיק):

$$n = 0: x^3 + \cancel{0x} + 2 \rightarrow \ f(0) = 2, \ f(1) = 0, \ f(2) = 10 = 1 \pmod 3$$
$$n = 1: x^3 + x + 2 \rightarrow \ f(0) = 2, \ f(1) = 1, \ f(2) = 12 = 0 \pmod 3$$
$$n = 2: x^3 + 2x + 2 \rightarrow \ f(0) = 2, \ f(1) = 2, \ f(2) = 14 = 2 \pmod 3$$

ניתן לראות שרק עבור n=2 קיבלנו שלפולינום אין שורשים ולכן רק אז הוא אי פריק. עפ"י משפט שהוכחנו בכיתה - חוג המנה הנתון הוא שדה אמ"מ הפולינום היוצר את האידאל במכנה הוא אי פריק, כלומר חוג המנה הנתון יהיה שדה עבור כל n=2+3k.

אביב 2005
ליאור

פרק י

2. א. בכיוון אחד, נניח שמתקיימת הכלה:

$$m\mathbb{Z} \subseteq n\mathbb{Z} \to \forall m \in \mathbb{N},\ m \in n\mathbb{Z} \to \exists z \in \mathbb{Z}, m = nz \to n \mid m$$

בכיוון השני נניח ש- n|m

$$n \mid m \to \exists z \in \mathbb{Z},\ nz = m \to m\mathbb{Z} = (nz)\mathbb{Z} \subseteq n\mathbb{Z}$$

ב. נתון ש-kZ מכיל את mZ ואת nZ, ולכן לפי סעיף א' מתקיים k|m ו-k|n. מאחר ש-kZ הוא האידאל המינימלי שמקיים זאת, k הוא האיבר המקסימלי שמחלק את שניהם (נניח שגם d|n ו-d|m אבל אם גם k מחלק אותם מתקיים m=kv, ולכן d|kv וגם m=ku, ולכן מתקיים d|k כמו כן נתון ש-kZ הוא האידאל המינימלי ולכן k>d לכל d כזה שנבחר). ניתן לראות שזוהי בדיוק הגדרת ה-ממג"ב ולכן k=(m,n).

ג. בכיוון אחד:

$$I = m\mathbb{Z} + n\mathbb{Z} \subseteq \mathbb{Z}$$
$$(m,n) = 1 \to \exists a,b \in \mathbb{Z},\ am + bn = 1 \in I \to 1 \cdot \mathbb{Z} \subseteq I \to I = \mathbb{Z}$$

בכיוון שני $I = \mathbb{Z} \to 1 \in I \to \exists a,b \in \mathbb{Z},\ am + bn = 1 \to (m,n) = 1$ (מתוך משפט שהוכחנו בכיתה בתחילת השנה - אם ניתן להגיע באמצעות צירוף לינארי של שני מספרים ל-1, הם זרים.

ד. נבחין שכדי שאיבר a יהיה בחיתוך האידאלים mZ ו-nZ צריך להתקיים m|a וגם n|a. לכן נבחר את הכמק"ב [m,n]: $I = \{a \in \mathbb{Z} : n \mid a, m \mid a\} = [m,n] \cdot \mathbb{Z}$ כיוון שכל איבר בו מחולק ע"י m,n, והוא עצמו מחלק איבר אחר שמחולק ע"י m ו-n (כך שלא נאבד איברים שנמצאים בחיתוך).

8. א.

$$\left\langle f_{(x)}, g_{(x)} \right\rangle = \{ f_{(x)}a_{(x)} + g_{(x)}b_{(x)} \mid a,b \in F[x] \}$$

1) $f_{(x)}, g_{(x)} \in \left\langle f_{(x)}, g_{(x)} \right\rangle \neq \phi$

2) $\forall a_{1(x)}b_{1(x)}, a_{2(x)}b_{2(x)} \in F[x] \to \quad (f_{(x)}a_{1(x)} + g_{(x)}b_{1(x)}) - (f_{(x)}a_{2(x)} + g_{(x)}b_{2(x)})$

$$= f_{(x)} \overbrace{(a_{1(x)} - a_{2(x)})}^{\in F[x]} + g_{(x)} \overbrace{(b_{1(x)} - b_{2(x)})}^{\in F[x]} \in \left\langle f, g \right\rangle$$

3) $\forall f_{(x)}a_{(x)} + g_{(x)}b_{(x)} \in \left\langle f_{(x)}, g_{(x)} \right\rangle,\ c_{(x)}, d_{(x)} \in F[x] \to \quad (f_{(x)}a_{(x)} + g_{(x)}b_{(x)})(c_{(x)} + d_{(x)})$

$$= f \underbrace{(ac + ad)}_{\in F[x]} + g \underbrace{(bc - bd)}_{\in F[x]} \in \left\langle f, g \right\rangle$$

ב.

1) $d_{(x)} \mid f_{(x)} \to f_{(x)} = d_{(x)}u_{(x)};\quad d_{(x)} \mid g_{(x)} \to g_{(x)} = d_{(x)}v_{(x)}$

$\forall q \in \left\langle f_{(x)}, g_{(x)} \right\rangle, \exists a_{(x)}, b_{(x)} \in F[x] \to q = f_{(x)}a_{(x)} + g_{(x)}b_{(x)}$

$$= d_{(x)}u_{(x)}a_{(x)} + d_{(x)}v_{(x)}b_{(x)} + d_{(x)}\left(u_{(x)}a_{(x)} + v_{(x)}b_{(x)}\right) \to d_{(x)} \mid q_{(x)} \to \left\langle f_{(x)}, g_{(x)} \right\rangle \subseteq \left\langle d_{(x)} \right\rangle$$

2) $d_{(x)} = (f_{(x)}, g_{(x)}) \to \exists a_{(x)}, b_{(x)} \in F[x] \to d_{(x)} = f_{(x)}a_{(x)} + g_{(x)}b_{(x)}$

$$\forall q \in \left\langle d_{(x)} \right\rangle \to q \in \left\langle f_{(x)}, g_{(x)} \right\rangle \to \left\langle d_{(x)} \right\rangle \subseteq \left\langle f_{(x)}, g_{(x)} \right\rangle \quad \Rightarrow \left\langle d_{(x)} \right\rangle = \left\langle f_{(x)}, g_{(x)} \right\rangle$$