גירסה 1.02 – 24.3.2010
גירסה 1.01 – 19.2.2010
גירסה 1.00 – 7.10.2002

שאלות באלגברה מודרנית– חלק ראשון

מסמך זה הורד מהאתר http://www.underwar.co.il/.
אין להפיץ מסמך זה במדיה כלשהי, ללא אישור מפורש מאת המחבר.
מחבר המסמך איננו אחראי לכל נזק, ישיר או עקיף, שיגרם עקב השימוש במידע המופיע במסמך, וכן לנכונות התוכן של הנושאים המופיעים במסמך. עם זאת, המחבר עשה את מירב המאמצים כדי לספק את המידע המדויק והמלא ביותר.

כל הזכויות שמורות ל**ניר אדר**

Nir Adar
Email: nir@underwar.co.il
Home Page: http://www.underwar.co.il/

מסמך זה הוא הראשון בסדרת מסמכים הבאים להציג לקורא שאלות ופתרונות בנושאים באלגברה מודרנית. רוב התיאוריה איננה נמצאת בדפים אלו. ניתן להוריד את המשפטים אליהם מסתמכים התרגילים באתר http://www.underwar.co.il/.
נושאים המכוסים במסמך זה: מספרים שלמים, קונגרואנציה מודולו n, חבורות ותת חבורות.

אנא שלחו תיקונים והערות אל המחבר.

מספרים שלמים

תרגיל

נתון: $(a,b)=1,\ a\mid bc$.
צ"ל: $a\mid c$

הוכחה

$(a,b)=1 \Leftarrow$ על פי משפט קיימים n,m כך ש ma+nb=1.
יהי c מספר שלם. נכפול ב-c את הביטוי: c=mac+nbc.
$a\mid bc \Leftarrow$ קיים q כך ש $bc=aq$.
$a\mid c \Leftarrow mac+naq=a(mc+nq)$
מ.ש.ל

קונגרואנציה מודולו n

הוכח את הטענה הבאה:

$a\equiv b(\mathrm{mod}\,n)$ אמ"מ ל-a ול-b אותה שארית בחלוקה בn.

פתרון

כיוון 1: נניח כי לa ולb אותה שארית בחלוקה בn.

$$\exists x\in R: a=xn+r \quad 0\le r<|n|$$
$$\exists y\in R: b=yn+r \quad 0\le r<|n|$$
$$\Downarrow$$
$$a-b=xn+r-(yn+r)=(x-y)n$$
$$\Downarrow$$
$$n\mid a-b$$
$$\Downarrow$$
$$a\equiv b(\mathrm{mod}\,n)$$

כיוון 2: נניח כי $a\equiv b(\mathrm{mod}\,n)$.
נסמן: $a=xn+r_1, 0\le r_1<|n|, \quad b=yn+r_2, 0\le r_2<|n|$
נשתמש בנתון: $a\equiv b(\mathrm{mod}\,n) \Leftarrow n\mid a-b \Leftarrow n\mid (x-y)n+r_1-r_2$.
מכאן: $n\mid r_1-r_2$ וגם $n\mid (x-y)n$.
לכל n, מתקיים כי $-|n|<r_1-r_2<|n| \Leftarrow r_1=r_2=0$.

חבורות

תרגיל

תהי G חבורה בה לכל $a \in G$ מתקיים $a^2 = e$. הוכח כי G חבורה אבלית.

פתרון

נראה כי $ab=ba$ לכל $a.b$.
לכל איבר $g \in G$ מתקיים $g^2 = e$.

$$g \cdot g = e \Rightarrow g(g \cdot g^{-1}) = e \cdot g^{-1} \Rightarrow$$
$$g = g^{-1}, \forall g \in G$$

ניקח $a,b \in G$, בפרט מתקיים $(ba)^{-1} = ba$. נכפול בab משמאל:

$$ab(ba)^{-1} = ab \cdot (ba)$$
$$ab(ba)^{-1} = a(bb)a = a \cdot e \cdot a = a \cdot a$$

נכפול בba מימין:

$$ab((ba)^{-1} \cdot ba) = e \cdot ba$$

ומכאן ba=ab.

תרגיל

צ"ל: אם G חבורה כך ש $(ab)^2 = a^2b^2$ לכל $a,b \in G$ אזי G חבורה אבלית.

פתרון

G חבורה ומתקיים $(ab)(ab) = a^2b^2$.
צריך להוכיח אבליות, כלומר לכל $a,b \in G$, $ab = ba$
נביט בביטוי $(ab)(ab) = a^2b^2$.

$$(ab)(ab) = a^2b^2$$
$$abab = a^2b^2$$
$$a^{-1}abab = a^{-1}a^2b^2$$
$$bab = ab^2$$
$$babb^{-1} = ab^2b^{-1}$$
$$ba = ab$$

לכל $a,b \in G$ $ab=ba$, מכאן לפי ההגדרה נובע כי החבורה אבלית.

תרגיל

הוכח: אם G מכילה מספר זוגי של איברים, קיים $a \neq e$ כך ש $a^2 = e$.

פתרון

נסמן את אברי החבורה ב $e, a, a_1, a_1^{-1}, a_2, a_2^{-1} ..., a_n, a_n^{-1}$.
(זוהי חבורה סופית).
נסדר זוגות של מספר וההופכי שלו. נשאר עם e ועוד איבר a.
מכיוון שזו חבורה, לכל איבר צריך להיות הופכי יחיד. ההופכי של e הוא e, ולכן מתחייב שההופכי של a הוא a עצמו.
מכאן קיים $a \neq e$ כך ש $a^2 = e$.

תת חבורות

תרגיל

תהיינה H_1, H_2 תת חבורות של G. הוכח כי $H_1 \cup H_2$ ת"ח של G אמ"מ $H_1 \subseteq H_2$ או $H_1 \supseteq H_2$.

הוכחה

כיוון אחד:
נניח ש $H_1 \subseteq H_2$ או $H_1 \supseteq H_2$ ונראה כי $H_1 \cup H_2$ ת"ח של G.
נניח בלי הגבלת כלליות כי $H_1 \subseteq H_2$. $\Leftarrow H_1 \cup H_2 = H_2$. ידוע כי H_2 תת חבורה ולכן $H_1 \cup H_2$ ת"ח של G.

כיוון שני:
נניח $H_1 \cup H_2$ ת"ח של G.
צ"ל: $H_1 \subseteq H_2$ או $H_1 \supseteq H_2$
נניח בשלילה שלא, כלומר $H_1 \not\subset H_2$ וגם $H_2 \not\subset H_1$.
$H_1 \not\subset H_2$: קיים a ב H_1 כך ש $a \notin H_2$.
$H_2 \not\subset H_1$: קיים b ב H_2 כך ש $b \notin H_1$.
$a, b \in H_1 \cup H_2$. $H_1 \cup H_2$ היא תת חבורה ולכן יש סגירות.
$a \bullet b \in H_1 \cup H_2 \Leftarrow ab \in H_1$ or $ab \in H_2$
אם $ab \in H_1 \Leftarrow a^{-1}ab \in H_1 \Leftarrow b \in H_1$ סתירה.
אם $ab \in H_2 \Leftarrow abb^{-1} \in H_2 \Leftarrow a \in H_2$ סתירה.
לכן $H_1 \subseteq H_2$ או $H_1 \supseteq H_2$.

תרגיל

הראה כי קבוצת המספרים המרוכבים $\{z \in \mathbb{C} \mid |z| = 1\}$ היא תת חבורה של החבורה הכפלית $\mathbb{C}^*$.

פתרון

נראה את קיום התכונות:

- סגירות:

$a+bi, c+di$

$a^2+b^2=1, c^2+d^2=1$

$(a+bi)\cdot(c+di)=(ac-bd)+(ad+bc)i=m+ki$

$ac-bd=m$

$ad+bc=k$

$|m+ki|=m^2+k^2=(ac-bd)^2+(ad+bc)^2=a^2c^2-2abdc+b^2d^2+a^2d^2+2abcd+b^2c^2=$

$=a^2c^2+b^2d^2+a^2d^2+b^2c^2=(a^2+b^2)(c^2+d^2)=1$

מכפלת שני איברים שייכת לקבוצה.

- אסוציאטיביות: אם גודלה של כל מכפלת שני איברים השייכים לקבוצה היא 1, ברור כי גם מכפלת שלושה איברים בסדר כלשהו תהיה 1.
- קיום איבר יחידה: האיבר 1 שייך לקבוצה.
- קיום הופכי: ידוע כי עבור כל שורש יחידה, קיים מספר a כך שמכפלתו בשורש היחידה תהיה 1.