גירסה 1.00 – 7.10.2002

שאלות באלגברה מודרנית – חלק שני

מסמך זה הורד מהאתר http://underwar.livedns.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: underwar@hotmail.com
Home Page: http://underwar.livedns.co.il

מסמך זה הוא השני 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://underwar.livedns.co.il.
נושאים המכוסים במסמך זה: מספרים שלמים, סדר של חבורה, קוסטים, חבורות ציקליות, משפט לגרנג'.

אנא שלחו תיקונים והערות אל המחבר.

מספרים שלמים

תרגיל

צ"ל: $3/a$ אם סכום הספרות של a מתחלק ב3.

פתרון

נתון: a מתחלק ב3.

$$a \equiv a_k a_{k-1} ... a_0 = a_0 + 10 \cdot a_1 + ... + 10^k a_k$$

נתון כי:

$$a_0 + 10 \cdot a_1 + ... + 10^k a_k = 0 (\mathrm{mod}\, 3)$$

$$a_0 + 10 \cdot a_1 + ... + 10^k a_k = \underbrace{a_0 + a_1 + ... + a_k}_{A} + \underbrace{9 \cdot a_1 + ... + (10^k - 1) a_k}_{B}$$

$3 \mid B$

we know that $3 \mid a$, so we can state that: $3 \mid A \Rightarrow$

$$a_0 + a_1 + ... + a_k = 0 (\mathrm{mod}\, 3)$$

סדר של איבר

הגדרה - תזכורת

יהי $a \in G$. הסדר של האיבר a מסומן $o(a)$ הוא המספר הטבעי הקטן ביותר n כך ש $a^n = e$.

תרגיל

G חבורה, $g \in G$ המקיים o(g)=n.
יהי k המקיים $g^k = e$.
צ"ל: n|k.

פתרון

בכל מקרה $n \le k$ (כי n הוא הסדר של g). נניח בשלילה ש $n \nmid k$. נחלק את k בn עם שארית.

$$k = qn + r, 0 < r < n$$

$$e = g^k = g^{qn+r} = g^{gn} \cdot g^r = (g^n)^q \cdot g^r = e^q \cdot g^r = g^r$$

קיבלנו סתירה. מצאנו $0 < r < n$ המקיים $e = g^r$. קיבלנו סתירה למינימליות של n.
מכאן r בהכרח שווה 0, כלומר n|k.

תרגיל

נתון: $o(g)=n$

צ"ל: $o(g^k)=\frac{n}{(n,k)}$

פתרון

הגדרה – תזכורת:

הכפולה המשותפת הקטנה ביותר (כמק"ב) של a וb היא מספר d המקיים:
1. $a|d$,$b|d$.
2. אם $a|f$, $b|f$ אזי גם $d|f$.

כלומר d הוא המספר הקטן ביותר שa,b מחלקים.
הסימון של הכמק"ב: d=[a,b]
טענת עזר (ללא הוכחה): $(a,b)\cdot[a,b]=a\cdot b$

וכעת להוכחה:
נסמן: $o(g^k)=x$.
נוכיח כי:

א. $x\left|\frac{n}{(n,k)}\right.$

ב. $\frac{n}{(n,k)}\left|x\right.$

א.
נסתכל על:

$$(g^k)^{\frac{n}{(n,k)}}=g^{\frac{nk}{(n,k)}}=(g^n)^{\frac{k}{(n,k)}}=e^{\frac{k}{(n,k)}}=e$$

רואים כי אכן g^k המופעל $\frac{n}{(n,k)}$ פעמים שווה לe.

מכאן, לפי הגדרת הסדר, $x\left|\frac{n}{(n,k)}\right.$

ב.

$$e=(g^k)^x=g^{kx}\Rightarrow n\,|\,kx\Rightarrow$$
$$\exists a\in\mathbb{N}:kx=na\Rightarrow n\,|\,na,k\,|\,na\Rightarrow[n,k]\,|\,na\Rightarrow[n,k]\,|\,kx$$
$$\Downarrow\left((n,k)\cdot[n,k]=nk\right)$$
$$\frac{nk}{(n,k)}\left|kx\Rightarrow\frac{n}{(n,k)}\right|x$$

תרגיל

נתונה חבורה G, $a,b \in G$.
צ"ל : $o(ab)=o(ba)$.

פתרון

נסמן : $o(ab) \equiv k$. ומכאן :

$$(ab)^k = e$$

$$a^k b^k = e$$

נכפיל כעת k פעמים משמאל ב b ונכפיל k פעמים בימין ב b^{-1} .

$$\underbrace{b \cdot b \cdot \ldots \cdot b}_{\text{k times}} \cdot a^k \cdot e = \underbrace{b \cdot b \cdot \ldots \cdot b}_{\text{k times}} \cdot \underbrace{b^{-1} \cdot b^{-1} \cdot \ldots \cdot b^{-1}}_{\text{k times}} = e$$

$$\Downarrow$$

$$b^k a^k = e$$

$$(ba)^k = e$$

מכאן שאם נכפיל את k ba פעמים אזי נקבל e.
כעת נרצה לראות שk הוא אכן מספר הפעמים המינימלי הדרוש, כלומר k הוא גם הסדר של ba.
יהי t הסדר של ba. נוכיח $t=k$.

$$b^t a^t = e$$

$$\Downarrow \text{ in the same way as above}$$

$$(ab)^t = e$$

t גדול או שווה מk, כי k זוהי לפי הגדרה חזקה מינימלית שבעזרתה נגיע לe.
ראינו גם קודם שk גדול או שווה t. מכאן בהכרח $k=t$ והרי $o(ab) \equiv k$ וגם $o(ba) \equiv t$,
לכן מ.ש.ל.

תרגיל

נתון: $o(a)=n, o(b)=m, ab=ba$ וגם $(n,m)=1$.
צ"ל: $o(ab)=o(a)o(b)$

פתרון

$o(ab)\equiv k \Rightarrow (ab)^k = e$
$a^k b^k = e$

נראה כי $k=[o(a),o(b)]$. על מנת שהפעלת ab k פעמים תביא ל1, צריך להתקיים:
$a^k=1$ וגם $b^k=1$. מכאן $n\mid k, m\mid k$. ולכן צריך להתקיים $k=[o(a),o(b)]$.
ידוע כי $(n,m)=1$. נשתמש בטענה: $(a,b)\cdot[a,b]=a\cdot b$.
ניתן לראות מהטענה כי הכפולה המשותפת הקטנה ביותר של מספרים זרים שווה למכפלה ביניהם.
ולכן $k=[o(a),o(b)]=o(a)\cdot o(b)$.
מ.ש.ל

תרגיל

הוכח כי בחבורה מסדר סופי קיים איבר (פרט לאיבר האדיש) מסדר סופי.

פתרון

תהי חבורה G כך ש $|G|=n$. יהי $a\neq e, a\in G$. נראה כי $o(a)\le n$. (n סופי ולכן הסדר של a סופי).
מטעמי סגירות מתקיים כי: $a\cdot a\in G$.
נרשום את חזקות a:

$$a, a^2, a^3, ..., a^k, ..., a^l, ...$$

כיוון שכל החזקות הן בG, וG סופית, מספר החזקות השונות של a הוא סופי.
כלומר, קיימים k,l, כך ש $k\neq l$ ומתקיים $a^k=a^l$.
נניח בלי הגבלת כלליות: $l>k$.
מכאן: $\underbrace{a\cdot a\cdot ...\cdot a}_{\text{k times}}=\underbrace{a\cdot a\cdot ...\cdot a}_{\text{l times}}$. נכפיל ב a^{-1} k פעמים ונקבל $e=a^{l-k}$.
בגלל שהנחנו $l>k$ אזי $l-k>0$ טבעי.
על פי משפט, $o(a)\mid l-k$ ומכאן $o(a)$ סופי.

תרגיל

מצא דוגמא לחבורה מסדר אינסופי, אשר כל איבר בה הוא מסדר סופי.

פתרון אפשרי

נתבונן בקבוצה H - קבוצת הוקטורים הבינריים האינסופיים, ביחס לחיבור מודולו 2. זוהי חבורה. מתקיימת סגירות עקב תכונות חיבור מודולו 2. קיים איבר אדיש (ווקטור ה0). לכל איבר בקבוצה קיים הופכי. עבור איבר a ההופכי הוא a עצמו. סדר החבורה הוא אינסופי (ישנם אינסוף ווקטורים באורך אינסופי).
אולם סדר כל איבר הוא סופי, והוא 2, מכיוון ש $\forall a \in H, a^2 = e$.
חבורה זו עומדת בתנאים המתבקשים מהשאלה.

תרגיל

תהי G חבורה סופית מסדר 10. הוכח כי קיימים ב-G איבר מסדר 2 ואיבר מסדר 5.

פתרון

לפי מסקנה ממשפט לגרנג', הסדר של איברי החבורה יהיה 1,2,5 או 10 בלבד.
האיבר שהסדר שלו 1 הוא איבר היחידה.
נניח תחילה שלא קיים איבר מסדר 10, כלומר החבורה איננה ציקלית.
סדר כל איבר יכול להיות 2 או 5. כל איבר בחבורה הוא יוצר של תת חבורה מסדר 2 או 5. עבור כל שני איברים a,b השייכים לחבורה, כל תת חבורה שאחד מהם יוצר היא או זרה, או שזו אותה תת חבורה.
כלומר אנו מחלקים את כל איברי החבורה פרט לאדיש, לקבוצות של זוגות ושל חמישיות.
אולם, ישנם בחבורה 9 איברים אותם נרצה לחלק לתת חבורות שונות. לא ניתן לחלקם רק לזוגות ללא שארית, וגם לא רק לחמישיות בלא שארית, אולם ידוע כי אלו החלוקות האפשריות היחידות. לכן בהכרח ישנן גם תתי חבורות מסדר 2 וגם תתי חבורות מסדר 5.

כעת נניח שקיים איבר מסדר 10, כלומר החבורה ציקלית.
נשתמש במשפט שהוכח בכיתה: תהי G חבורה ציקלית מסדר n, ויהי m מספר שמחלק את n, אז קיימת ב-G תת חבורה מסדר m.
ידוע כי 2 ו-5 מחלקים את 10, לכן בהכרח ישנה תת חבורה מסדר 2 ותת חבורה מסדר 5, כלומר יש איבר (היוצר) שהוא מסדר 2 ויש יוצר מסדר 5.

חבורות ציקליות

תרגיל

צ"ל: U_8 לא ציקלית.

פתרון

נביט בתת החבורות שכל אחד מאברי U_8 יוצר:

$U_8 = \{1,3,5,7\}$
$<1>=\{1\}$
$<3>=\{1,3\}$
$<5>=\{1,5\}$
$<7>=\{1,7\}$

אף אחד מאיברי הקבוצה אינו יוצר אותה ולכן U_8 לא ציקלית.

תרגיל

צ"ל: U_9 ציקלית.

פתרון

$U_9 = \{1,2,4,5,7,8\}$
$<1>=\{1\}$
$<2>=\{2,4,8,16 \equiv 7,32 \equiv 5,64 \equiv 1\}$
$<4>=\{4,16 \equiv 7,64 \equiv 1\}$
$<5>=\{5,5^2 \equiv 7,5^3 = 8,5^4 = 4,5^5 = 2,5^6 = 1\}$
$<7>=\{7,49 \equiv 4\}$
$<8>=\{8,1\}$

U_9 ציקלית. היוצרים שלה הם 2 ו5.

<u>תרגיל</u>

ידוע כי כל תת החבורות של $\mathbb{Z}$ הן מהצורה $n\mathbb{Z}$.
צ"ל: למצוא את היוצר של $n\mathbb{Z}\cap m\mathbb{Z}$.

<u>פתרון</u>

נביט תחילה בחיתוך $n\mathbb{Z}\cap m\mathbb{Z}$. האיברים הנמצאים בחיתוך הם האיברים מהצורה $x\cdot[n,m]$ כאשר [n,m] זהו הכמק"ב, ו-x הוא מספר טבעי כלשהו.
לפיכך, $<[n,m]>$ זהו היוצר של $n\mathbb{Z}\cap m\mathbb{Z}$.

<u>תרגיל</u>

תהי G חבורה אבלית מסדר pq, כאשר p,q>1 ראשוניים שונים.
צ"ל: G חבורה ציקלית.

<u>פתרון</u>

נראה כי קיים איבר $a\in G$ מסדר pq אמ"מ G ציקלית.
$p\neq q$ ולכן |G|>1. יהי $e\neq a\in G$.
על פי מסקנה ממשפט לגרנג' סדר האיבר מחלק את סדר החבורה. $o(a)\mid pq$ ובנוסף $o(a)\neq 1$.
ישנן שתי אפשרויות.
אפשרות ראשונה: $o(a)=pq$ ואז G ציקלית.
אפשרות שניה: בלי הגבלת כלליות: $o(a)=p$.
נניח כי יש איבר b כך שמתקיים $o(b)=q$.
לפי תרגיל שהוצג קודם לכן במסמך זה, מתקיים $o(ab)=o(a)\cdot o(b)=pq$ ומכאן G ציקלית.
לפיכך נניח כי לא קיים b כזה כך ש $o(b)=q$.
מכאן כל האיברים ב-G פרט לאדיש הם מסדר p.
כלומר מספר האיברים בחבורה הוא מהצורה $p\cdot n+1$
אולם ידוע כי $p>1$ ולכן $p\nmid p\cdot n+1$. סתירה לכך שG חבורה אבלית מסדר pq ולכן בהכרח קיים איבר מסדר pq. ולכן החבורה ציקלית.

קוסטים

תרגיל

עבור כל אחד מהמקרים הבאים חשב את הקוסטים הימניים.

1. G - אוסף כל המטריצות ההפיכות עם פעולת כפל מטריצות.

$$H=\left\{A\in G\,\middle|\,|A|=1\right\}$$

פתרון

נשתמש בכך ש $Ha=Hb\Leftrightarrow b\cdot a^{-1}\in H$.
יהיו $A,B\in G$.

$$HA=HB\Leftrightarrow BA^{-1}\in H$$

$$\left|BA^{-1}\right|=1\Leftrightarrow|B|\left|A^{-1}\right|=1\Leftrightarrow|B|\cdot\frac{1}{|A|}=1\Leftrightarrow|A|=|B|$$

כלומר שתי מטריצות נמצאות באותו קוסט, אם יש להם אותה הדטרמיננטה.
כלומר, אוסף כל הקוסטים הוא:

$$\left\{HA\,\middle|\,|A|=r,r\in\mathbb{R}^*\right\}$$

$$\mathbb{R}^*=R/\{0\}$$

הערה: מספר הקוסטים הימנים שווה למספר הקוסטים השמאליים.

2.

G - אוסף כל המטריצות הממשיות $f:R\to R$ עם פעולת חיבור פונקציות,
כלומר: $(f\cdot g)(x)\equiv f(x)+g(x)$.

פתרון

סכום שתי פונקציות בנקודה יחושב כאחת בנקודה ועוד השניה בנקודה.
G היא חבורה.
איבר האפס: $\forall x\in R,f_0(x)=0$
איבר הופכי: $f^{-1}(x)=-f(x)$

ניקח H תת חבורה: $H=\left\{f\in G\,|\,f(1)=0\right\}$. $Ha=Hb$ אמ"מ $b\cdot a^{-1}\in H$

$$H+f_1=H+f_2\Leftrightarrow f_2+\left(f_1^{-1}\right)\in H$$

$$\Leftrightarrow f_2+(-f_1)\in H$$

$$\left(f_2+\left(-f_1\right)\right)(1)=0\Leftrightarrow f_2(1)-f_1(1)=0$$

$f_1(1)=f_2(1)$ כלומר שתי פונקציות נמצאות באותו קוסט אם התמונה של 1 כל ידי הפונקציות זהה.

אוסף הקוסטים הוא: $\{H+f \mid f(1)=r, r\in\mathbb{R}\}$.
בכל קוסט נמצאים כל הפונקציות שמקבלים עבור 1 את אותו הערך מבין הערכים האפשריים ב $\mathbb{R}$. כלומר: $[G:H]=|\mathbb{R}|$.

.3

$$G=3\mathbb{Z}, H=6\mathbb{Z}$$

$$H+a=H+b \Leftrightarrow n+(-a)\in H$$
$$\Leftrightarrow b-a\in H$$
$$\Leftrightarrow 6\mid b-a$$
now we state that $a=3Z_a, b=3Z_b, Z_a, Z_b\in\mathbb{R}$
$$\Leftrightarrow 6\mid 3\cdot(Z_b-Z_a)$$
$$\Leftrightarrow 2\mid (Z_b-Z_a)$$
$$\Leftrightarrow Z_a=Z_b \pmod 2$$

כלומר ל Z_a ול Z_b אותה שארית בחלוקה ב2.
שאריות אפשריות הן 0 או 1.
מכאן a,b באותו קוסט אמ"מ $Z_a=Z_b \pmod 2$

מכאן שיש שני קוסטים:
$$I=\{a=3Z_a \mid Z_a\equiv 0 \pmod 2, Z_a\in\mathbb{R}\}=\{3Z_a \mid Z_a=2k, k\in\mathbb{Z}\}=\{6k \mid k\in\mathbb{Z}\}=H$$
$$II=\{a=3Z_a \mid Z_a\equiv 1 \pmod 2, Z_a\in\mathbb{R}\}=\{3Z_a \mid Z_a=2k+1, k\in\mathbb{Z}\}=\{6k+3 \mid k\in\mathbb{Z}\}=H+3$$

הקוסטים ביחד משלימים לG.

משפט לגרנג'

תרגיל

הוכח: G חבורה מסדר p^2 , p ראשוני, אזי בG יש תת חבורה מסדר p.

פתרון

נמצא איבר $a \in G$ מסדר p, כי אם קיים איבר כזה אזי הוא יוצר של תת חבורה מהסדר המבוקש.
יהי $e \neq a \in G$ יתכן כי $O(a)$ הוא $1, p, p^2$.
האפשרות שסדר האיבר הוא 1 נפסלת בגלל הגדרת התרגיל.
אם מצאנו איבר מסדר p הרי הוכחנו את שרצינו.
לכן נניח כי $o(a) = p^2$, היות ו $G =< a >\Leftarrow |G| = p^2 \Leftarrow p^2 = o(a) = |< A >|$, כלומר G ציקלית. מכאן כל איבר בG הוא מהצורה a^k.
נחפש איבר כנ"ל מהצורה הזו, שהסדר שלו הוא p.
נשתמש בטענה הבאה: $o(g) = n \Rightarrow o(g^k) = \frac{n}{(n,k)}$.
בעזרת הטענה נאמר כי:

$$O(a) = p^2 \Rightarrow o(a^k) = \frac{p^2}{(p^2, k)} = p$$

$$\Rightarrow (p^2, k) = p \Rightarrow k = p$$

קיבלנו כי האיבר $a^k = a^p$ הוא מסדר p והוא היוצר של תת חבורה מסדר p.

מ.ש.ל