I

האוניברסיטה

מס' מחברת: 2

מס' מזהה

0	6	6	1	6	4	5	5	-	4

לפני הבחינה אנא מלא את הפרטים בכתב ברור ובדייקנות

שם הקורס מבנים אלגברי'ם I

מס' הקורס 80445

שם המורה פרופ שחר מוגס

תאריך בחינה 12/2/07

הוראות לתלמיד

1. הכן את התעודה המזהה לביקורת.
2. עליך למסור את המחברת בשלמותה לפני עזיבת האולם. עזיבת האולם ללא מסירת מחברת דינה ציון 0.
3. כתוב את התשובות בעט בכתב יד ברור ונקי על עמוד אחד של כל דף. אין לכתוב בשוליים.
4. כתוב טיוטה רק על צד אחד של הדף - וסמן "טיוטה". מחק את הטיוטה בצורה ברורה לפני מסירת המחברת. אין לתלוש דפים מהמחברת.

בהצלחה

לשימוש המורה

הציון (0-100): 99

המחברת נבדקה בתאריך _____

חתימת המורה _____

שאלה מספר:

1, 4, 5, 6.

25	1
25	4
24	5
25	6

④ יהי G חבורה סופית ויהי $p|n$, p ראשוני. אז, ישנו איבר מסדר p ב-G
(כלומר $e\neq a\in G$, כך ש- $a^p=e$, ולכל $t<p$, $a^t\neq e$).

הוכחה:

נגדיר קבוצה: $\Omega=\{(x_0,\dots,x_{p-1}):\prod_{j=0}^{p-1}x_j=e\}$, כאשר e איבר היחידה ב-G.

מובן כי $\Omega\neq\emptyset$, כי הווקטור $(e,\dots,e)\in\Omega$, כי $e\cdots e=e^p\underset{\uparrow}{=}e\cdot e^{p-1}\underset{\uparrow}{=}e^{p-1}\underset{\uparrow}{=}\dots=e$.

e ניטרלי לכפל   המשך באינדוקציה.

נאפיין את כל האיברים ב-Ω.

נשים לב כי ניתן לבחור את p-1 האיברים הראשונים ב-p-יה, בחירה כללית ותהליך הבחירה מגדיר את האיבר האחרון, כלומר, לכל בחירה של איברים מ-G, $y_0,\dots,y_{p-2}$, ישנו איבר יחיד ב-Ω, והוא $(y_0\cdots y_{p-2})^{-1}$.
לכן Ω היא אוסף כל הוקטורים מאיברי G, באורך p-1, לכן ניתן להסיק כי $|\Omega|=n^{p-1}$.

נגדיר יחס שקילות על איברי Ω: $x=(x_0,\dots,x_{p-1})$ שקול ל-$y=(y_0,\dots,y_{p-1})$, אם x מתקבל מ-y ע"י סיבוב, כלומר, ישנו $0\le r<p$, כך שלכל $0\le j\le p-1$, $x_j=y_{j+r\,(\mathrm{mod}\,p)}$. נראה בהמשך כי זה אכן יחס שקילות.

נציין טענה (ונוכיח בהמשך): עבור p ראשוני, ו-p-יה נתונה $x=(x_0,x_1,\dots,x_{p-1})$, אם איברי ה-p-יה לא כולם שווים זה לזה אז כל ההזזות הציקליות
$$(x_1,x_2,\dots,x_{p-2},x_{p-1},x_0),\dots,(x_{p-1},x_1,x_2,\dots,x_{p-2})$$
שונות זו מזו.

נשים לב כי $p|n^{p-1}$, שכן $p|n$, לכן [illegible].

נתבונן בפירוק Ω למחלקות שקילות. מהטענה נובע כי גודל כל מחלקת שקילות הוא 1 או p, כיוון שסכום גדלי מחלקות השקילות (שהוא גם הגודל של הקבוצה Ω) חייב להתחלק ב-p, וישנה מחלקת שקילות בגודל 1, היא $\{(e,\dots,e)\}$.

נקבל כי ישנן לפחות עוד p-1 מחלקות שקילות בגודל 1, כלומר ישנו $e\neq a\in G$ כך ש- $a^p=e$.

~~המשך מהדף הקודם~~

נניח כי הסדר של a הוא p, ונוכיח (בדרך השלילה) כי p הוא ראשוני.

נניח שקיימים $k<p$ כך ש $a^k=e$, ונראה כי $k=0$.

ידוע כי $a^0=e$ ולכן אם $k\neq 0$ אז $a^k\neq e$.

נחלק את p ב k ונקבל: $p=kq+r$ כאשר $r<k$. כלומר:

$$e=a^p=a^{kq+r}=a^{kq}\cdot a^r=(a^k)^q\cdot a^r=e^q\cdot a^r=e\cdot a^r=a^r$$

↑ מהנחת a

לכן, שכן $r<k$ קיבלנו $a^r=e$, בסתירה לבחירת k.

טענה: תהי G חבורה מסדר ראשוני p, אזי G חבורה ציקלית

וכל איבר שונה מ e הוא יוצר של G, כלומר $G=\langle x\rangle$.

הוכחה: נזכור כי $\mathbb{Z}_n^*=\{m\in\mathbb{Z}_n \mid \gcd(m,n)=1\}$. נניח כעת כי $x\in G$ כך ש $|x|\neq 1$ ו $|x|\neq p$. כיוון ש $|x|\mid p$, ומכיוון ש p ראשוני אז $|x|=1$ או $|x|=p$. מהשוויון $|x|=1$ נובע $x=e$, ומשפט לגראנז' מבטיח כי $|x|\mid |G|$, ולכן $|x|=p$ אזי $\langle x\rangle\subseteq G$ ו $|\langle x\rangle|=|G|$, ולכן $\langle x\rangle=G$, כלומר x יוצר את G, ובפרט G ציקלית.

טענה: אם p ראשוני, $x=(x_1,\dots,x_p)$ איבר כלשהו שאינו איבר היחידה או שכל הקואורדינטות שוות זו לזו, אזי x מסדר p.

הוכחה: נשים לב כי $\sigma(x)=(x_2,\dots,x_p,x_1)$, כלומר $\sigma(x)=y$, ו $x\neq y$ (כי $x_1\neq x_2$). כמו כן $\sigma^p(x)=x$. יתר על כן, לכל $0<k<p$ מתקיים $\sigma^k(x)\neq x$, שכן אחרת $x_1=x_{k+1}=x_{2k+1}=\dots=x_{pk+1}=x_p$, בסתירה לכך שכל הקואורדינטות שונות זו מזו.

טענה: תהי G חבורה ציקלית מסדר p ראשוני, אזי $G\cong\mathbb{Z}_p$ (באיזומורפיזם).

הוכחה: נגדיר $\varphi:\mathbb{Z}_p\to G$ כלומר $\varphi(k)=a^k$ כאשר a יוצר כלשהו של G. נשים לב כי φ חח"ע ועל, שכן $\ker\varphi=\{0\}$ ולכן φ חח"ע, ומכיוון ש $|\mathbb{Z}_p|=|G|=p$ אז φ גם על. נותר להראות כי φ הומומורפיזם, אך זה ברור מכך ש $\varphi(k+l)=a^{k+l}=a^k\cdot a^l=\varphi(k)\cdot\varphi(l)$.

טענה: יהי p ראשוני, $x\in\mathbb{Z}_p^n$ ו $\sigma=(1\,2\,\dots\,p)$. נגדיר $x\sim y$ אם קיים k כך ש $y=\sigma^k(x)$. אזי $\sim$ יחס שקילות.

הוכחה: נראה כי $\sim$ רפלקסיבי, סימטרי וטרנזיטיבי.

רפלקסיביות: $x=\sigma^0(x)$ ולכן $x\sim x$.

סימטריות: נניח כי $x\sim y$ אז קיים k כך ש $y=\sigma^k(x)$. אזי $x=\sigma^{p-k}(y)$ ולכן $y\sim x$.

טרנזיטיביות: נניח כי $x\sim y$ וגם $y\sim z$. אזי קיימים k,l כך ש $y=\sigma^k(x)$ ו $z=\sigma^l(y)$. אזי $z=\sigma^{k+l}(x)$ ולכן $x\sim z$.

אזי, $\sim$ מתקיים אם x הפעלה של σ (כלשהי).

5) הראו כי הטענה שלמטה סופי הוא שקר.

הוכחה: כיוון שתחום השלמים הוא קומוטטיבי (בכפל), נראה אחד אלפס, כי לשאלתנו איבר יחידה ("טריוויאלי לכפל"), והנסיון לבנות איבר שונה מאלפס, יעקב כי הקבוצה מכילה את הקומוטטיבי של שדה.

יהי R תחום שלמים סופי.

נראה תחילה קיום איבר יחידה.

יהי $a \in R \setminus \{0\}$. נגדיר הפונקציה $\varphi : R \to R$, ע"י $\varphi(x) = ax$

φ חח"ע, כי אם $ax = ay$, אזי $ax - ay = 0$, מדיסטריבוטיביות ב R, $a(x-y) = 0$, כיון ש R תחום שלמים, נקבל כי $a = 0$ או $x = y$. מהחיבור, $a \neq 0$, לכן $x = y$. לכן $x \neq y \Rightarrow \varphi(x) \neq \varphi(y)$ ~~מ~~ φ חח"ע.

~~נראה~~ נראה כי φ על, כי אם $z \in aR$ אזי z מהצורה $z = ax$ עבור $x \in R$ כלשהו $\Rightarrow \varphi(x) = z$ על.

כיון ש $a \in R$ ו φ חח"ע ועל, ישנו $u \in R$ כך ש $au = a$. נראה כי u הוא איבר יחידה לכפל.

~~יהי $x \in R$ אזי, $\exists b \in R$ כך ש $ab = x$~~

נשים לב ש $aR = R$, כי $aR \subseteq R$ (R סגור לכפל משמאל), ו $aR \supseteq R$ נובעת מקיומו של יחידה ומהתחום שלמים.

נניח כי $x \in R$. אזי, כיון ש $aR = R$, ישנו $b \in R$ כך ש $ab = x$.

נראה: $xu = (ab)u = a(bu) = a(ub) = (au)b = ab = x$

- $xu = (ab)u$: מהגדרת x
- $(ab)u = a(bu)$: אסוציאטיביות הכפל
- $a(bu) = a(ub)$: מהנחת השלילה שזהו קומוטטיבי
- $a(ub) = (au)b$: אסוציאטיביות הכפל
- $(au)b = ab$: מהגדרת u
- $ab = x$: הגדרת x

לכן u איבר יחידה.

יהי $b \in R \setminus \{0\}$ (אם $b = 0$ אזי u איבר יחידה שמתקיים). נתבונן בפונקציה $\psi : R \to R$, $\psi(x) = bx$. מהנתון $bR = R$ (מהגדרת b שמרנו על איבר היחידה), נשים לב כי $bu \in R$, לכן, $\exists a \in R$, כלומר, ישנו $a \in R$ כך ש $ba = u$ לכן b הפיך. לכן נקבל כי R הינו שדה, בסתירה.

(24/25)

$A, B \trianglelefteq G$

$\forall a \in A,\ b \in B \quad , \quad ab = ba$

$bab^{-1} \in B$ ולכן B נורמלי, $aba^{-1} \in B$. כלומר

$ab = b'a \iff aba^{-1} = b'$ כך

$aba^{-1} \in A$ ולכן A נורמלי, $bab^{-1} \in A$

$\begin{cases} ba = a'b \\ ab = b'a \end{cases} \iff bab^{-1} = a'$ כך

$ba = a'b \Rightarrow b = a'ba^{-1}$

$ab = b'a$

$\Rightarrow ab = a(a'ba^{-1})b = aa'ba^{-1}b$

$b' = a$

$hg_0 = g \Rightarrow h = gg_0^{-1}$

$$|O(x)| = \frac{|G|}{|Stab_a x|}$$

$\varphi : O(x)$

$\varphi\left(G/Stab_a(x)\right) \longrightarrow O(x)$

$\varphi(gH) = gx.$

$g_1x = g_2x \iff g_1H = g_2H \Rightarrow g_1 \in g_2H \Rightarrow g_1g_2^{-1} \in H \Rightarrow (g_1g_2^{-1})x = x$

$(g_2^{-1}g_1)(x) = x \Rightarrow g_1x = g_2x$

(1) צ"ל: הראו כי קיימת מספר p (p ראשוני) כך ש $O(x)$ הוא p-יעיל.

הוכחה: נתבונן בפעולת G על G, ע"י הצמדה, כלומר, הפעולה שלכל איבר $g\in G$ ו $x\in G$ היא $x\to gxg^{-1}$.

נתון שקיים $x,y\in G$ כך ש $O(x)\neq O(y)$. כיוון שלכל $x,y\in G$ מתקיים $O(x)=O(y)$ או $O(x)\cap O(y)=\emptyset$ (נכונה בגלל הסימטריה). הטענה נכונה לכל t, מהיות p^t, כלומר $t=1$ או $t=p$.

~~[illegible]~~

מאידך נראה כי קיים מסלול שמכיל את עצמו בלבד, נקבע כי קיים מסלול כזה (x). כיוון שיש מסלולים בגודל 1 - $\{e\}$ (כי לכל g, $gxg^{-1}=x$, כלומר $xg=gx$. (לכל g).

נראה בדיוק אותו דבר עבור A, מהיות A תת-חבורה של G, כי

$$\{gxg^{-1}=x,\ g\in G,\ \exists g\in A:\ xg=gx\}=O(x)$$

לכן, ישנם עוד איברים ב $O(x)$ שונים מ e, לכן $O(x)$ הוא לא טריוויאלי.

נניח אל שלילה שתי הטענות: (לכל חבורה G הפועלת על קבוצה X)

* לכל $x,y\in X$, אם $O(x)\neq O(y)$, אז $O(x)\cap O(y)=\emptyset$.

הוכחה: נניח כי $z\in O(x)\cap O(y)$. (כאשר z כלשהו). כלומר, קיים g כך ש $z=x^g$ (כאן סימון לפי gxg^{-1}).

$$\{h\in G:\ x^h=x\}=\{h\in G:\ z^{g^{-1}hg}=z\}=\{hg:\ h\in G,\ z^h=z\}=\{g^{-1}h:\ h\in G,\ z^h=z\}=O(z)$$

(כי לכל h יש h' יחיד כך ש $g^{-1}hg=h'$ (הפיכות הפעולה) ולכל h יש h' יחיד כך ש $hg=gh'$ (הפיכות הפעולה).

כלומר $O(x)=O(z)$. באופן דומה, $O(y)=O(z)$, לכן $O(x)=O(y)$.

$|Z(G)| = p$ ו- $Z(G) = \{e, \dots, x^{p-1}\}$ סדר של x הוא p ולכן $\langle x \rangle$ תת-חבורה של G. $G/Z(G)$ - מכפלה

$$G/Z(G) = \{xZ(G) : x \in G\}$$
$$= \{Z(G), x_1 Z(G), \dots, x_{p-1} Z(G)\}$$
$$= \{Z(G), \{x_1, x_1 \cdot x_1, \dots, x_1^{(p-1)}\}, \dots, \{x_{p-1}, \dots, x_{p-1}^{(p-1)}\}\}$$

$xy \neq yx$. נניח בשלילה שקיימים $x, y \in G/Z(G)$ שמתחלפים, כלומר

$$yxy^{-1}x^{-1} \neq e \Rightarrow x^{-1}y^{-1}xy \neq e$$

$G/Z(G)$ ציקלית $\Rightarrow$ $\exists$ x יוצר כך ש- $\varphi(y, xZ(G)) = yx$

$$|G/Z(G)| = p \Rightarrow |G| = p^2$$

$$\varphi(a^i, x^j) = \varphi(a^k, x^l) = a^k x^l$$

$\Leftrightarrow$

$i = k$! $j = l$ אחרת $x^{j-l} = a^{i-k}$

$$\varphi(a^{i_1} \cdot x^{j_1}, a^{i_2} \cdot x^{j_2}) = (a^{i_1} \cdot x^{j_1}) a^{i_2} \cdot x^{j_2} = a^{i_1+i_2} \cdot x^{j_1+j_2}$$

* שוב על מסלול שלנו את שוכן המחלקה.

הגדרה: יהי $x \in X$. נגדיר $Stab_G(x) = \{g \in G : xg = x\}$ תת-חבורה של G; $Stab_G(x) \neq \emptyset$, כי $x \overset{def}{=} xe$.

כלומר $g_1, g_2 \in Stab_G(x)$, אז $x = x g_1 = (x g_2) g_1 = x(g_2 g_1)$

(הצבה ב-g_1 אחרי g_2 ב-x — הצבה ב-x)

סגור לכפל.

ולכל $g \in Stab_G(x)$, אז $xg = x$

$xg = x(g^{-1})g = x(g^{-1}g) = xe = x$

(כפל) אף שני צדדי המשוואה את g^{-1}, ונקבל: $x = xe = x(g g^{-1}) = (xg)g^{-1} = xg^{-1}$

(הצבה ב-xg)

סגור ל$^{-1}$ ברור, לכן $Stab_G(x)$ תת-חבורה. (סימון: $Stab_G(x) = H$)

לצורך הקלקה כאן שהקבוצות של $Stab_G(x)$ כאן המסלול של x,

$O(x) \longleftrightarrow G/Stab_G(x)$ ניתן, $xg = (Hg)x$.

* מוצהר ה-G, כי אז $Hg_1 = Hg_2$, כפשוט $g_1 g_2^{-1} \in H$ (כי $H \ni e$ תת-חבורה)

ולכן $H \ni g_1 g_2^{-1}$, לפחות כלומר $g_1 g_2^{-1}$ איבר יחידה.

$$x g_2 = x g_1 \Leftrightarrow x = x g_1 g_2^{-1}$$

לכן * הינה מוצהרת.

* תחזק, כי אוף $x g_2 = x g_1$, g_2 אז $g_1 g_2^{-1}$ איבר יחידה (הפשוט בחוץ), לכן $Hg_2 = Hg_1$.

* עם, כי אוף $z \in O(x)$, אז $z = xg$ (מתקיים) $z = (Hg)x$

לכן שגיאה הקלקה תחת זאת כי G/H וכיוון ש-G סופית

$|G| = |G/H| \cdot |H|$, לכן צדדי המסלול שלנו איבר החבורה. ולכן סימון זה

טענת הקלקה והסימון כי G מרכז על ידי H

$A \cap B = \{e\}$ ~~$\subseteq A \cap B$~~ $B, A \trianglelefteq G$,

$a \cdot a \cdot b \cdot b \cdot a \cdot a \cdot b \cdot b$ $\quad aba^{-1} \in B$

$aba^{-1} = b_1$

$bab^{-1} = a_1$

$x \in G \setminus Z(G)$ מה $\neq 1$

$ab \neq ba \Rightarrow b \neq aba^{-1} \Rightarrow \exists b_1 \neq b$ s.t. $b_1 = aba^{-1}$ (כי $b \in B$)

$g_2 g_1 = h_2 g_2 h_1 g_1 = h_2 h_1 g_2 g_1 = h_1 h_2 g_2 g_1$

~~$h_1 h_2 g_1 g_2 = h_1 g_1$~~

$h_2 g_2 \quad h_1 h_2 g_1 g_2 = h_1 g_1 h_2 g_2 = g_1 h_1$

$= a\hat{a}b = eb = ab$ $\quad \Rightarrow b_1 b^{-1} = a\hat{a} = e$

$b_1 b^{-1} a = e \cdot a = a \in A \cap B$

$ab = abb^{-1}a = ab\hat{a}a = ba$

$(ak)ak = a^2k^2$ $\quad (a^1k)$

$aba^{-1} = b_1 \in B$, $bab^{-1} = a_1 \in A$ $\Rightarrow$ ~~$aba^{-1}b^{-1} = e \Rightarrow ab = b_1 a$~~

$B \ni b_1 = aba^{-1} = ab\hat{a}(\hat{b}b) = a(ba^{-1}b^{-1})b = a\hat{a}b$

$\Rightarrow b_1 b^{-1} = a\hat{a} \Rightarrow a\hat{a} = e \Rightarrow aba^{-1}b^{-1} = e \Rightarrow ab\hat{a} = b \Rightarrow ab = ba$.

$G/Z(G)$ $\quad n_q \mid n_q(G) \equiv 1 \bmod q \Rightarrow 1, 10, 19, 28, 37, 46$

$n_q(G) \mid |G| \quad \Rightarrow n_q(5) = 1$

$\Rightarrow n_q(G)$ אין מחלק יחיד מסדר q

$G/Z(G)$ ~~(h,g)~~

$(h,g) = (h,g)(h,g)(\hat{h},\hat{g}) \cdot g\hat{g} \in Q$?

$G/Z(G)$. $\quad \tilde{h} = hg \quad \tilde{h}\, g^{-1} h^{-1}$ $\quad a$ נקרא $Z(G)$

$x \in G$ לפי

$= a^{t+t_1} \cdot b^{s+s_1} = x \cdot y = a^t b^s \cdot a^{t_1} b^{s_1}$ כך $Z(G)$ ב, $x = a^t b^s$ אז

$t \in Z(G)$ כי $x = a^i \cdot t$ $\quad$ ~~$a^{-i} x$~~ $\Rightarrow$ לכן $\{a^i\}$ $\quad x \in G$ כך

$y = a^k \cdot l$ $\quad l \in Z(G)$

$xy = a^i t \cdot a^k l = a^i t \cdot a^i l = t a^k l a^i =$

$G/Z(G)$ ~~G~~ $\quad$ ו G כלל. הם מחזורי: