אלגברה מודרנית - 201015

מבחן מועד ב', תשע"ט, 24/3/2019

פתרונות

פתרון 1 (20 נק')

א. (5 נק') נאמר ש $a \equiv b \mod n$ אם n מחלק את $a-b$.

ב. (5 נק') נוכיח את הטענה לפי אינדוקציה על m. אם $m=1$ אז ברור שהטענה מתקיימת. נניח שהטענה מתקיימת עבור איזשהו $m \in \mathbb{N}$. אם p מחלק את a^{m+1}, נכתוב $a^{m+1} = a^m \cdot a$. מכיוון ש p ראשוני, נובע ש p מחלק את a^m או את a. לפי הנחת האינדוקציה, בכל מקרה נובע ש p מחלק את a. ניתן להסיק שהטענה נכונה לכל $m \in \mathbb{N}$.

ג. (10 נק') נגדיר קבוצה

$$S = \{x \in \mathbb{N} \mid x^4 = 5(y^4+z^4) \ : y,z \in \mathbb{N} \text{ קיימים}\}.$$

עלינו להראות ש S ריקה. נניח בשלילה ש S אינה ריקה. לפי עקרון הסדר הטוב קיים מספר מינימלי $x_0 \in S$. בהתאם קיימים $y_0, z_0 \in \mathbb{N}$ כך ש $x_0^4 = 5(y_0^4+z_0^4)$. נובע ש x_0^4 מתחלק ב 5. לפי סעיף ב' x_0 מתחלק ב 5 וניתן לכתוב $x_0 = 5x_1$ כאשר $x_1 \in \mathbb{N}$. נציב ונקבל $5^4 x_1^4 = 5(y_0^4+z_0^4)$ לכן $125x_1^4 = y_0^4+z_0^4$ ובפרט $y_0^4+z_0^4$ מתחלק ב 5. לפי המשפט הקטן של פרמה

$$y_0^4 + z_0^4 \equiv \begin{cases} 0+0 & 5|y_0, 5|z_0 \\ 0+1 & 5|y_0, 5 \nmid z_0 \\ 1+0 & 5 \nmid y_0, 5|z_0 \\ 1+1 & 5 \nmid y_0, 5 \nmid z_0 \end{cases}.$$

מכיוון ש $y_0^4+z_0^4$ מתחלק ב 5 נובע ש y_0, z_0 מתחלקים ב 5 וניתן לכתוב $y_0 = 5y_1, \ z_0 = 5z_1$ כאשר $y_1, z_1 \in \mathbb{N}$. נציב ונקבל $x_1^4 = 5(y_1^4+z_1^4)$ לכן $x_1 \in S$. אבל $x_1 = \frac{1}{5}x_0 < x_0$ בסתירה לכך ש x_0 האיבר המינימלי ב S. ניתן להסיק כי S ריקה.

פתרון 2 (20 נק')

א. (5 נק') הסדר של $x \in G$ הוא המספר הטבעי המינימלי $n \in \mathbb{N}$ (אם קיים) כך ש $x^n = e$ כאשר e האדיש ב G. אם לא קיים כזה מספר נאמר שהסדר של x אינסופי.

ב. (10 נק') נסמן ב $\langle g \rangle = \{g^t \mid t \in \mathbb{Z}\}$ תת החבורה של G הנוצרת על ידי g. ידוע לפי טענה כי $|\langle g \rangle| = \text{ord}(g)$. לפי משפט לגרנז' מתקיים ש $|\langle g \rangle|$ מחלק את $n = |G|$ לכן $\text{ord}(g)$ מחלק את n.

ג. (5 נק') ידוע כי $|S_3| = 6$. לפי הסעיף הקודם $2 = \text{ord}(\sigma)$ מחלק את $|H|$. כמו כן, $3 = \text{ord}(\rho)$ מחלק את $|H|$. נובע ש $2 \cdot 3 = 6$ מחלק את $|H|$ כי $2,3$ זרים אחד לשני. נובע ש $|H| \geq 6$ אבל $|H| \leq |S_3| = 6$. לכן $|H| = 6$ ונובע ש $H = S_3$.

פתרון 3 (20 נק')

א. (5 נק') לכל $s,t\in\mathbb{Z}$ מתקיים

$$\phi(s+t)=\begin{pmatrix}1 & s+t\\ 0 & 1\end{pmatrix}=\begin{pmatrix}1 & s\\ 0 & 1\end{pmatrix}\begin{pmatrix}1 & t\\ 0 & 1\end{pmatrix}=\phi(s)\phi(t)$$

לכן ϕ הומומורפיזם.

ב. (5 נק') אם $\phi(s)=\phi(t)$ אז $\begin{pmatrix}1 & s\\ 0 & 1\end{pmatrix}=\begin{pmatrix}1 & t\\ 0 & 1\end{pmatrix}$ לכן $s=t$. נובע ש ϕ חד־חד־ערכי.

ג. (10 נק') נקח $A=\phi(1)=\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}$. יהי $n\in\mathbb{N}$. נחשב

$$A^n=(\phi(1))^n=\phi(\underbrace{1+\cdots+1}_{n\text{ פעמים}})=\phi(n)=\begin{pmatrix}1 & n\\ 0 & 1\end{pmatrix}\neq\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}.$$

כאן השתמשנו בתכונה של הומומורפיזם לגבי חזקות. נובע שהסדר של A אינסופי.

פתרון 4 (20 נק')

א. (5 נק') יש כמה הגדרות שקולות. ניתן להגדיר נורמליות כך: תת חבורה H נורמלית ב G אם לכל $g\in G$ מתקיים $gHg^{-1}\subseteq H$.

ב. (5 נק') אם G אבלית ו H תת חבורה של G אזי לכל $g\in G$ מתקיים

$$gHg^{-1}=\{ghg^{-1}\mid h\in H\}=\{hgg^{-1}\mid h\in H\}=\{h\mid h\in H\}=H.$$

לפי ההגדרה, נובע ש H נורמלית.

ג. (10 נק') לפי משפט לגרנז' הגודל של המנה הוא

$$|G/H|=|\{gH\mid g\in G\}|=|G|/|H|=n/(n/p)=p.$$

יהי $aH\in G/H$ כך ש $aH\neq eH$ כאשר e האדיש ב G. אזי $\mathrm{ord}(aH)\neq 1$. לפי שאלה 2 סעיף ב' $\mathrm{ord}(aH)$ מחלק את $|G/H|=p$ ו p ראשוני. נובע ש $\mathrm{ord}(aH)=p$ לכן $|\langle aH\rangle|=\mathrm{ord}(aH)=p=|G/H|$. נובע ש $\langle aH\rangle=G/H$ ו G/H ציקלית, נוצרת על ידי aH.

פתרון 5 (20 נק')

א. (5 נק') יהי $R=\mathbb{Z}$ ויהי $u\in U$. לפי ההגדרה של U קיים $a\in\mathbb{Z}$ כל ש $ua=1$. יש רק שני מחלקים של 1 שהם $1,-1$. נובע ש $U\subseteq\{1,-1\}$. מצד שני, ברור ש $1,-1\in U$ כי $1\cdot 1=1$ ו $(-1)\cdot(-1)=1$. ניתן להסיק כי $U=\{1,-1\}$.

ב. (10 נק') אם $u\in U$. לפי ההגדרה של U קיים $a\in R$ כך ש $au=1$. כעת, יהי $r\in R$. מתקבל ש $r=r\cdot 1=r(au)=(ra)u\in\langle u\rangle$. נובע ש $R\subseteq\langle u\rangle$ אבל כמובן $\langle u\rangle\subseteq R$ ולכן $\langle u\rangle=R$.

ג. (5 נק') קודם נשים לב כי $1 \in G$ כי $1 \in U$ ו $1 - 1 = 0 \in I$ (האיבר 0 שייך ל I כי I תת חוג של R.) נוודא ש G סגורה ביחס לפעולת כפל. לשם כך יהיו $a, b \in G$. לפי ההגדרה של G מתקיים $a, b \in U$ לכן $ab \in U$ כי $(U, \cdot)$ חבורה. בנוסף, $a - 1, b - 1 \in I$. מכיוון ש I תת חוג של R מתקיים $(a - 1)(b - 1) \in I$. נכתוב

$$(a - 1)(b - 1) = ab - a - b + 1 = (ab - 1) - (a - 1) - (b - 1)$$

ונקבל $ab - 1 = (a - 1)(b - 1) + (a - 1) + (b - 1) \in I$. נובע ש $ab \in G$. כעת, נבדוק האם G מכילה את ההופכי של כל איבר שלה. לשם כך יהי $c \in G$, אז $c \in U$ ו $c - 1 \in I$. מכיוון ש $(U, \cdot)$ חבורה קיים $c^{-1} \in U$. נתבונן ב

$$c^{-1} - 1 = c^{-1}(1 - c) = -c^{-1}(c - 1) \in I$$

מכיוון ש $c - 1 \in I$ ו I אידאל. נובע ש $c^{-1} \in G$. הוכחנו ש G תת חבורה של U.