אלגברה מודרנית - 201015
מבחן מועד ב', תשע"ח, 13.3.2018
פתרון

פתרון 1 (25 נק')

א. (15 נק') מכיוון ש $b|n$ ניתן לכתוב $n = bk$. כעת, a, b זרים זה לזה. לפי הלמה של בזו קיימים $s, t \in \mathbb{Z}$ כך ש $sa + tb = 1$. נכפיל ב k ונקבל $sak + tbk = k$. נשים לב ש $a|n$ אבל $n = bk$ לכן $a|tbk$. נובע ש $a|(sak + tbk)$, כלומר $a|k$ ולכן $ab|bk$ $ab|n \iff$.

ב. (10 נק') לא. דוגמא נגדית: $n = a = b = 2$. אז $a|n, b|n$ אבל $ab \not| n$.

פתרון 2 (25 נק')

א. (15 נק') יהי $t \in \mathbb{N}$. לפי הלמה של אוקלידס ניתן נכתוב $t = kq + r$ כאשר $k, r \in \mathbb{Z}$ ו $0 \le r \le q - 1$. כעת,

$$\begin{aligned} g^t = 1 &\iff g^{kq+r} = 1 \\ &\iff (g^q)^k g^r = 1 \\ &\iff 1^k g^r = 1 \\ &\iff g^r = 1 \\ &\iff r = 0 \end{aligned}$$

כי (לפי ההגדרה של סדר) $g^i \neq 1$ לכל $i = 1, \ldots, q - 1$. קיבלנו ש

$$g^t = 1 \iff t = qk \iff q|t.$$

ב. (10 נק') ראשית נשים לב כי $e^{i\theta} = 1 \iff \frac{\theta}{2\pi} \in \mathbb{Z}$. נובע ש

$$\begin{aligned} g^t = 1 &\iff e^{i2t\pi/1000} = 1 \\ &\iff \frac{2t\pi}{1000 \cdot 2\pi} \in \mathbb{Z} \iff t \in 1000\mathbb{Z}. \end{aligned}$$

נובע ש $\mathrm{ord}(g) = 1000$. באופן דומה,

$$\begin{aligned} (g^3)^t = 1 &\iff e^{i6t\pi/1000} = 1 \\ &\iff \frac{6t\pi}{1000 \cdot 2\pi} \in \mathbb{Z} \\ &\iff 3t \in 1000\mathbb{Z} \\ &\iff 3t \equiv 0 \mod 1000 \\ &\iff t \equiv 0 \mod 1000 \\ &\quad (\text{כי } (3, 1000) = 1) \\ &\iff t \in 1000\mathbb{Z} \end{aligned}$$

ונובע ש $\mathrm{ord}(g^3) = 1000$.

פתרון 3 (25 נק')

א. (5 נק')

$$\begin{aligned}\ker\varphi &= \{\sigma \in S_n \mid \varphi(\sigma) = 1\} \\ &= \{\sigma \in S_n \mid \operatorname{sgn}(\sigma) = 1\} \\ &= A_n.\end{aligned}$$

ב. (10 נק') באופן כללי, הגרעין של הומומורפיזם הוא תת חבורה נורמלית. לפי הסעיף הקודם, $A_n = \ker(\varphi)$ לכן A_n תת חבורה נורמלית של S_n.

ג. (10 נק') אם $n = 1$ אז $S_1 = A_1$ לכן האינדקס של A_1 ב S_1 הוא $|S_1|/|A_1| = 1$. בהמשך נניח ש $n \geq 2$. לפי משפט ההומומורפיזם, $S_n/\ker\varphi \cong \mathrm{Im}\varphi$. לכן, לפי סעיף א', $S_n/A_n \cong \mathrm{Im}\varphi$. ברור ש $\mathrm{Im}\varphi = \{1,-1\}$ כי $n \geq 2$ לכן יש תמורות זוגיות ותמורות אי־זוגיות. לכן $S_n/A_n \cong \{1,-1\}$. נובע שהאינדקס של A_n ב S_n הוא

$$|S_n/A_n| = |\{1,-1\}| = 2.$$

פתרון 4 (20 נק')

א. (15 נק') נשים לב ש $a \in \mathbb{F}_p$ הופכי לעצמו אם ורק אם

$$a^2 = 1 \iff a^2 - 1 = 0 \iff (a+1)(a-1) = 0.$$

ברור ש $a = 1$ פתרון למשוואה זו. אם $a \neq 1$, אז $a - 1 \neq 0$ וניתן להכפיל ב $(a-1)^{-1}$ (ההופכי קיים כי $\mathbb{F}_p$ שדה). מתקבל $a + 1 = 0$ לכן $a = -1$. בסיכום, יש בדיוק שני איברים שהם הופכיים לעצמם: 1 ו -1.

ב. (10 נק') נשים לב ש $a + 8\mathbb{Z}$ הופכי לעצמו אם ורק אם

$$\begin{aligned}&(a+8\mathbb{Z})(a+8\mathbb{Z}) = 1 + 8\mathbb{Z} \\ \iff &a^2 + 8\mathbb{Z} = 1 + 8\mathbb{Z} \\ \iff &a^2 - 1 \in 8\mathbb{Z}.\end{aligned}$$

אם a זוגי אז $a^2 - 1$ אי־זוגי ולכן $a^2 - 1 \notin 8\mathbb{Z}$. נותר לבדוק את האפשרויות $a \in \{1,3,5,7\}$.

a	$a^2 - 1 \mod 8$
1	0
3	$8 \equiv 0$
5	$24 \equiv 0$
7	$48 \equiv 0.$

לכן כל אחד מ $1 + 8\mathbb{Z}, 3 + 8\mathbb{Z}, 5 + 8\mathbb{Z}, 7 + 8\mathbb{Z}$ הופכי לעצמו.