פתרון מועד א תשעו

14 במרץ 2017

.1

(א) תת חבורה: מוגדרות: לכל $g_1, g_2 \in Z(G)$ צ"ל כי $g_1 g_2 \in Z(G)$. שזה שקול להראות שלכל $x \in G$ מתקיים $g_1 g_2 x = x g_1 g_2$. אכן כיוון ש g_1, g_2מתחלפות עם כל x מתקיים כי

$$g_1 g_2 x = g_1 x g_2 = x g_1 g_2$$

הופכי: יהא $g \in Z(G)$ אזי קיים $g^{-1} \in G$. נראה כי $g^{-1} \in Z(G)$. אכן לכל x מתקיים כי $gx = xg$ואם נכפיל ב g^{-1} משמאל ומימין נקבל כי $xg^{-1} = g^{-1}x$ כלומר $g^{-1} \in Z(G)$ כנדרש.
איבר יחידה: נראה שאיבר היחידה e של G שייך ל $Z(G)$ (ובפרט הוא יהיה יחידה ב $Z(G)$). אכן לכל $x \in G$ מתקיים $ex = x = xe$.
נוכיח כי היא תת חבורה נורמלית: יהא $g \in G, x \in Z(G)$ צריך להוכיח כי $gxg^{-1} \in Z(G)$ אכן מהגדרת המרכז נקבל כי $gxg^{-1} = xgg^{-1} = x \in G$

(ב) עבור $G = GL_n(\mathbb{R})$ חבורת המטריצות ההפיכות מעל הממשיים. מתקיים כי $Z(G) = \{\alpha I : 0 \neq \alpha \in \mathbb{R}\}$ המטריצות הסקלאריות ששונות מ־0.

.2

(א) הפרכה: למשל ניקח $G = S_3$ וניקח $\sigma = (1,2) \in S_3$ אזי $o(\sigma)o(\sigma) = 2 \cdot 2 = 4$ אך $\sigma^2 = id$ ולכן $o(\sigma^2) = 1$

(ב) הוכחה: אם הסדרים סופיים אז זה נכון כי: יהא $k = o(ab)$ אזי $(ab)^k = e$ נכפיל ב a^{-1} משמאל ו a מימין ונקבל $(ba)^k = e$ ולכן $o(ba) \leq k$ באותו אופן מראים ש $o(ab) \leq o(ba)$ ולכן שווים.
אם אחד מהם מסדר אינסופי למשל $o(ab) = \infty$ אז גם $o(ba) = \infty$ כי אם $o(ba) < \infty$ כמו במקרה הקודם נקבל גם ש $o(ab) < \infty$ סתירה.

.3

(א) יהא $\phi : G_1 \to G_2$ הומו'. אזי התמונה $H = Im(\phi) \leq G_2$ היא תת חבורה של G_2 ולכן $\frac{|G_2|}{|H|} \in \mathbb{Z}$ לפי משפט לגרנז'. מצד שני לפי משפט האיזו' מתקיים כי

$$G_1/\ker\phi \cong H = Im(\phi)$$

אזי

$$\frac{|G_1|}{|\ker\phi|} = |H|$$

ואז

$$\frac{|G_1|}{|H|} = |\ker\phi| \in \mathbb{Z}$$

כלומר $|H|$ מחלק גם את $|G_1|$וגם את $|G_2|$. כיוון שאלו מספרים זרים נקבל כי $|H| = 1$ ולכן $H = \{e_{G_2}\}$. אם התמונה של ההמור' זה רק האיבר הנטרלי של G_2אזי מדובר בהומו' הטריאלי (ששולח כל איבר ב G_1 לנטרלי של G_2).

(ב) יהא $e \neq g \in G$ אזי $o(g) = p^k$ עבור $1 \leq k \leq n$ לפי לגרנז ואז $o(g^{p^{k-1}}) = \frac{p^k}{\gcd(p^k, p^{k-1})} = p$ ולכן החבורה $\left\langle g^{p^{k-1}} \right\rangle$ היא בת p איברים ולכן איזומורפית ל $(\mathbb{Z}_p, +)$

.4

(א) כיוון ש a, p זרים נקבל כי $\gcd(a, p) = 1$ ולכן הוא צירוף לינארי שלהם. כלומר קיימים c, c' שלמים כך ש $ac + pc' = 1$ נפעיל מודולו p על השיוון ונקבל

$$ac = 1 \mod p$$

אם c אינו טבעי (אלא שלילי) נוסיף לו כפולות של pעד שנגיע למספר חיובי.

(ב) טענה: יהא x נתון אזי הוא פתרון ל (1) $18x = 24 \mod 120$ אמ"מ הוא פתרון ל (2) $3x = 4 \mod 20$
הוכחה: נניח $18x = 24 \mod 120$ אזי קיים k שלם כך ש $18x = 24 + 120k$ ואז $3x = 4 + 20k$ כלומר $3x = 20 \mod 60$. מצד שני אם $3x = 4 \mod 20$ אזי קיים kשלם כך ש $3x = 4 + 20k$ ואז $18x = 24 + 120k$ כלומר $18x = 24 \mod 120$.
מסקנה: נפתור $3x = 4 \mod 20$. כיוון ש $\gcd(3, 20) = 1$ ל -3 יש הופכי מודלו 20 שהוא 7. נכפול ב 7 את המשוואה ונקבל שהפתרון היחיד הוא

$$x = 7 \cdot 4 = 28 = 8 \mod 20$$

.5

(א) הפולינום $p(x) = x^2 + 1 \in \mathbb{Z}_3[x]$ הוא אי פריק כי ממעלה 2 ואין לו שורש ($p(0) = 1, p(1) = 2, p(2) = 2$) ולכן $\mathbb{F} = \mathbb{Z}_3[x]/\langle p \rangle$ הוא שדה ש $\mathbb{Z}_3$ תת שדה שלו ובנוסף, $[x] \in \mathbb{F}$ פתרון למשוואה $x^2 + 1 = 0$

(ב) לא קיים. הוכחה: נניח בשלילה כי קיים שדה $\mathbb{F}$ עם 4 איברים ו a איבר בו שמקיים $a^3 + a^2 + 1 = 0$. אם $a = 0$ נקבל $1 = 0$ סתירה לכן $a \neq 0$. כעת החבורה $\mathbb{F} \setminus \{0\}$ עם כפל בת שלושה איברים ו a שייך אליה ולכן לפי לגרנז' $a^3 = 1$ וולכן נקבל כי

$$a^3 + a^2 + 1 = 1 + a^2 + 1 = a^2$$

כאשר המעבר האחרון נכון בגלל שבשדה עם p^n איברים מתקיים שאם נחבר 1 לעצמו p איברים נקבל 0 (אצלנו $p = 2$) בצירוף ההנחה בשלילה נקבל כי $a^2 = 0$ ולכן $a = 0$ (כי בשדה אין מחלקי אפס). סתירה.