פיתרון לתרגיל 5:

תשובה 1:

א. נשים לב ש : $H = \langle 5 \rangle = \{0,5,10,15\}$. מאחר ש $(\mathbb{Z}_{20}, +)$ קומוטטיבית המחלקות הימניות והשמאליות זהות והן : H, 1+H, 2+H, 3+H, 4+H.

ב. נשים לב ש : $H = \langle 8 \rangle = \{8k : k \in \mathbb{Z}\}$. מאחר ש $(2\mathbb{Z}, +)$ קומוטטיבית המחלקות הימניות והשמאליות זהות והן : H, 2+H, 4+H, 6+H.

ג. $G = (U_{11}, \cdot)$, $H = \langle 10 \rangle = \{1,10\}$. מאחר ש G קומוטטיבית המחלקות הימניות והשמאליות זהות והן :

$$1 \cdot H = \{1,10\} = 10 \cdot H \,, 2 \cdot H = \{2,9\} = 9 \cdot H \,, 3 \cdot H = \{3,8\} = 8 \cdot H$$
$$4 \cdot H = \{4,7\} = 7 \cdot H \,, 5 \cdot H = \{5,6\} = 6 \cdot H$$

ד. $G = (\mathbb{R}^*, \cdot)$, $H = \mathbb{R}^+ = \{x \in \mathbb{R}^* : x > 0\}$. מאחר ש G קומוטטיבית המחלקות הימניות והשמאליות זהות והן :

אם $a \in \mathbb{R}^+$ דהיינו $a > 0$ אזי $aH = H$ ואם $a < 0$ אזי

$aH = \{ax : x > 0\} = \{y : y < 0\} = \mathbb{R}^-$ לכן סה"כ ישנן 2 מחלקות שמאליות (וימניות)

ה. $G = (\mathbb{R} \times \mathbb{R}, +)$, $H = \mathbb{Z} \times \mathbb{Z}$. מאחר ש G קומוטטיבית המחלקות הימניות והשמאליות זהות והן :

מחלקה שמאלית של $\mathbb{Z} \times \mathbb{Z}$ ב- $\mathbb{R} \times \mathbb{R}$ היא מהצורה $(a,b) + \mathbb{Z} \times \mathbb{Z}$ באשר $(a,b) \in \mathbb{R} \times \mathbb{R}$. שתי מחלקות $(a,b) + \mathbb{Z} \times \mathbb{Z}$ ו- $(c,d) + \mathbb{Z} \times \mathbb{Z}$ הן שוות אם ורק אם $(a,b) - (c,d) \in \mathbb{Z} \times \mathbb{Z}$ דהיינו $(a-c, b-d) \in \mathbb{Z} \times \mathbb{Z}$ ז"א $a - c, b - d \in \mathbb{Z}$. מכאן נסיק שהמחלקות השונות הן

$$\{(a,b) + \mathbb{Z} \times \mathbb{Z} : 0 \leq a, b < 1\}$$

תשובה 2:

א.

G חבורה ציקלית מסדר d , נניח שהיא נוצרת ע"י $a \in G$, כאשר $|a| = d$ דהיינו $G = \langle a \rangle$. יהי $b \in G$ אזי קיים $0 < k < d$ אז כך ש $b = a^k$ י. אם b יוצר או"א הוא יוצר את a וזאת או"א $a^{kr} = (a^k)^r = a$ עבור איזשהו r שלם. מכאן ש $kr = 1 \; mod \; d$ ומכאן נובע ש $\gcd(k,d) = 1$. סה"כ

$$\varphi(n) = |U_n| = |\{k : 0 < k < d, \gcd(k,d) = 1\}|.$$

ב. יהי $x \in \mathbb{Z}_n$ איבר מסדר d, אזי $\langle x \rangle \leq \mathbb{Z}_n$ ו- $|\langle x \rangle| = |x| = d$. מאחר ויש רק ת"יח אחת מסדר d, נובע שלכל $a \in \mathbb{Z}_n$ איבר מסדר d $\langle a \rangle = \langle x \rangle$.ובפרט $a \in \langle x \rangle$. לפי סעיף (א) ל- $\langle x \rangle$ יש בידיוק $\varphi(d)$ יוצרים. לכן קיימים $\varphi(d)$ איברים a כנ"ל, דהיינו איברים מסדר d.

ג.

נסתכל בחבורה Z_n, שהיא חבורה ציקלית מסדר n. לפי משפט שהוכחנו, לכל מספר טבעי $d \mid n$ קיימים ב- Z_n בדיוק $\varphi(d)$ איברים מסדר d. נסמן ב- A_d את קבוצת האיברים מסדר d ב- Z_n. אז $|A_d| = \varphi(d)$. ברור כי אם d_1 ו- d_2 הם מחלקים שונים של n, אזי $A_{d_1} \cap A_{d_2} = \phi$, וכי כל איבר של Z_n נמצא ב- A_d עבור איזשהו d שמחלק את n (כי הסדר של איבר בחבורה סופית מחלק את סדר החבורה). אז יש לנו: $Z_n = \bigcup_{d \mid n} A_d$, וזהו איחוד זר. מכאן:

$$\sum_{d \mid n} \varphi(d) = \sum_{d \mid n} |A_d| = \left| \bigcup_{d\ n} A_d \right| = |Z_n| = n .$$

תשובה 3:

נתון $|G| = p^2$, p ראשוני. נניח ש G אינה ציקלית. יהי $1 \neq a \in G$. לפי משפט לגרנז' $|a| \mid p^2$. מאחר ש p ראשוני, נקבל ש $|a| \in \{1, p, p^2\}$ אבל $a \neq 1$ לכן $|a| \neq 1$, כמו כן אם $|a| = p^2$ אז $|a| = |G|$ לכן $G = \langle a \rangle$ היא ציקלית בסתירה להנחה. לכן $|a| = p$ וסיימנו.

תשובה 4:

לפי משפט לגרנז' הסדר של האיברים ב – G יכול ליהיות $1, 2, p$ או $2p$. אם יש איבר $x \in G$ מסדר p סיימנו. אם יש איבר $a \in G$ מסדר $2p$ ניקח $x = a^2$ ואז $|x| = \frac{1}{2}|a| = p$ ושוב סיימנו. אחרת כל האיברים ב- G הם מסדר 1 או 2 . נראה שמצב זה בלתי אפשרי. אכן, האיבר היחיד מסדר 1 הוא איבר היחידה וכל שאר האיברים מסדר 2, עפ"י תרגיל מהכיתה אנו יודעים שבמקרה כזה G קומוטטיבית.. אם ב G יש רק איבר אחד a מסדר 2 אז היא ציקלית ונוצרת ע"י אותו איבר ואז $|G| = |a| = 2 \neq 2p$ בסתירה לנתון. לכן ב- G יש לפחות 2 איברים שונים מסדר 2, נסמנם $a, b \in G$. נתבונן בתת החבורה של G הנוצרת ע"י a ו- b, דהיינו $\langle a, b \rangle = \{1, a, b, ab\}$ (כי G קומוטטיבית $ab = ba$) תת-חבורה זו היא מסדר 4 , לכן שוב לפי לגרנז הסדר שלה מחלק את הסדר של G , דהיינו $4 \mid 2p$ לכן $2 \mid p$ בסתירה לטענה ש p ראשוני אי זוגי.

<u>תשובה 5:</u>

ראשית נוכיח כי φ_m הוא אכן הומומורפיזם של חבורות ולאחר מכן נוכיח שכל הומומורפיזם $\varphi: Z \to Z$ הוא מהצורה הנ"ל.

הוכחה: (i) לכל $x, y \in Z$: $\varphi_m(x+y) = m(x+y) \underset{\text{כללי חזקות}}{=} mx + my = \varphi_m(x) + \varphi_m(y)$.

זה מראה ש- φ_m הוא הומומורפיזם.

(ii) יהי $\varphi: Z \to Z$ הומומורפיזם (של חבורות). עלינו להראות כי קיים $m \in Z$ כך ש- $\varphi = \varphi_m$.
ואכן, ניקח $m = \varphi(1)$. אז לכל $x \in Z$:

$$\varphi(x) = \varphi(\underbrace{x \cdot 1}_{\text{חזקה של } 1}) = \underbrace{x \cdot \varphi(1)}_{\text{חזקה של } \varphi(1)} = \underbrace{x \cdot m}_{\text{חזקה של } m} = \underbrace{xm}_{\text{מכפלה}} = \underbrace{mx}_{\text{מכפלה}} = \underbrace{m \cdot x}_{\text{חזקה של } x} = \varphi_m(x)$$

מכאן ש- $\varphi = \varphi_m$, כנדרש.

<u>תשובה 6:</u>

א. יהי $g_1 \in G_1$, נסמן $|g_1| = n$ אזי $g_1^n = 1$ מכאן $1_{G2} = \varphi(1_{G1}) = \varphi(g_1^n) = \varphi(g_1)^n$ לכן $\varphi(g_1)^n = 1$ ומכאן $n \mid |\varphi(g_1)|$ כדרוש.

ב. אכן לפי הסעיף הקודם מקבלים גם ש $|\varphi(g_1)| \mid |g_1|$ כי $|g_1| = |\varphi^{-1}(\varphi(g_1))| \mid |\varphi(g_1)|$ הוא הומומורפיזם. לכן $|\varphi(g_1)| \mid |g_1|$ ו- $|g_1| \mid |\varphi(g_1)|$ ז"א $|\varphi(g_1)| = |g_1|$ כדרוש.

ג. יהי $y \in G_2$ כך ש $|y| = n$. φ אפימורפיזם, לכן קיים $x \in G_1$ כך ש $\varphi(x) = y$.
לפי סעיף (א) $|x| \mid |\varphi(x)| = |y|$. לכן $|x| = kn$ עבור איזשהו k טבעי. מכאן ניקח $z = x^k \in G_1$ ונקבל $|z| = |x^k| = \frac{|x|}{k} = n$.

ד. נניח ש $x \in G_1$ יוצר של G_1. מאחר ש $\varphi(x^k) = \varphi(x)^k$ נובע ש $\varphi(G_1) = \varphi(\langle x \rangle) = \langle \varphi(x) \rangle$, לכן אם $\varphi(x) = y \in G_2$ אינו יוצר של G_2 נובע ש $\varphi(G_1) = \langle \varphi(x) \rangle = \langle y \rangle \subsetneq G_2$ בסתירה להנחה ש φ על.

<u>תשובה 7:</u>

בשני הסעיפים אכן מדובר בהומומורפיזם שכן $f(x \cdot y) = (x \cdot y)^5 = x^5 \cdot y^5 = f(x) \cdot f(y)$.

ב- (א) הוא על שכן לכל $f\left(\sqrt[5]{a}\right) = a$, $a \in \mathbb{C}^*$. אבל לא חח"ע כי לכל a ממשי $\zeta_5 \cdot a \neq$ a באשר $\zeta_5 = cis(\frac{360}{5})$ שורש היחידה מסדר 5 מתקיים $f(\zeta_5 \cdot a) = f(\zeta_5)f(a) = 1 \cdot$ $a^5 = a^5 = f(a)$

ב- (ב) הוא חח"ע שכן עבור $a^5 = b^5$, $a, b \in \mathbb{Q}^*$ או"א $a = b$ זאת מאחר ושורש היחידה מסדר 5 הממשי היחיד הוא 1. אבל הוא לא על שכן $-1 \in \mathbb{Q}^*$ אינו בתמונה שכן $\sqrt[5]{-1}$ אינו רציונלי.