תרגיל 5 מבוא לתורת החבורות

שאלה 5.1

1. מצאו את שתי הספרות האחרונות של המספר 3333^{4444}.
פתרון: למצוא שתי ספרות אחרונות זה כמו לחשב ב $\mod 100$. המספר שלנו שווה בעצם ל

$$33^{4444}$$

33 אכן זר ל 100ולכן לפי משפט אוילר

$$33^{\varphi(100)} \equiv 1 \pmod{100}$$

קל לחשב ש

$$\varphi(100) = \varphi(5^2 2^2) = \varphi(5^2)\varphi(2^2) = (25-5)(4-2) = 40$$

ולכן

$$33^{40} \equiv 1 \pmod{100}$$

לכן

$$33^{4444} \equiv 33^{40\cdot 111} \cdot 33^4 \equiv (33^{40})^{111} \cdot 33^4 \equiv 33^4 \pmod{100}$$

את זה כבר קל לחשב

$$33^4 \equiv (33^2)^2 \equiv (1089)^2 \equiv (89)^2 \pmod{100}$$

$$89^2 = 7921$$

ולכן שתי הספרות האחרונות הן 21

2. הראו כי

$$29^{203} \equiv 9 \pmod{13}$$

פתרון: עובדים ב $\mod 13$ ולכן

$$29 = 3$$

שהוא אכן זר ל 13 ולכן אפשר להשתמש במשפט אוילר

$$\varphi(13) = 12$$

כי 13 ראשוני ולכן

$$3^{203} = 3^{12\cdot 17} 3^{-1} = (3^{12})^{17} 3^{-1} = 3^{-1}$$

קל לחשב שההופכי של 3 ב U_{13}הוא 9 ולכן קיבלנו את הדרוש.

שאלה 5.2

1. יהי $f:G\to H$ איזומורפיזם. הוכיחו כי f^{-1} הוא גם איזומורפיזם.
פתרון: קודם כל ברור ש f^{-1} חד חד ערכית ועל בתור הופכית לפונקציה חד חד ערכית ועל. נותר להוכיח שהיא הומומורפיזם. ניקח $x,y\in H$ צריך להוכיח ש

$$f^{-1}(xy)=f^{-1}(x)f^{-1}(y)$$

היות ש f היא על, יש $a,b\in G$ כך ש $x=f(a)$ ו $y=f(b)$ ולכן

$$f^{-1}(xy)=f^{-1}(f(a)f(b))$$

אבל בדלל ש f הומומורפיזם מתקיים

$$f^{-1}(f(a)f(b))=f^{-1}(f(ab)=ab=f^{-1}(x)f^{-1}(y)$$

כנדרש.

2. יהיו $f:G\to H$ ו $g:H\to K$ שני הומומורפיזמים. הוכיחו כי ההרכבה $g\circ f$ היא גם הומומורפיזם.
פתרון: די מיידי. ניקח $a,b\in G$ אז בגלל ש f,g הומומורפיזמים מתקיים.

$$gf(ab)=g(f(a)f(b))=g(f(a))g(f(b))$$

3. נאמר כי G איזומורפית ל H אם יש ביניהם איזומורפיזם. הוכיחו כי "איזומורפי ל" הוא יחס שקילות.
פתרון: רפלקסיביות: G איזומורפי לעצמו כי פונקציית הזהות היא איזומורפיזם.
סימטריות: אם $f:G\to H$ הוא איזומורפיזם אז ההופכי $f^{-1}:H\to G$ אי איזומורפיזם כמו שראינו כבר בסעיף קודם.
טרנזיטיביות: אם $f:G\to H$ ו $f':H\to K$ הם שני איזומורפיזמים אז ההרכבה $f'\circ f$ היא איזומורפיזם. ראינו בסעיף קודם שהיא הומומורפיזם. וידוע ממתמטיקה בדידיה שהרכבה של פונקציות על היא על והרכבה של חח"ע היא חח"ע.

שאלה 5.3 תהי G חבורה שלה יש בדיוק 4 איברים מסדר 5. תהי H חבורה איזומורפית ל G. הוכיחו כי גם ב H יש בדיוק 4 איברים מסדר 5.
פתרון: נניח $f:G\to H$ איזומורפיזם בין שתי החבורות. קודם כל נוכיח: אם $a\in G$ איבר מסדר m אז גם $f(a)$ מסדר m. הוכחה:
מצד אחד, אם $a^k=e$ אז

$$(f(a))^k=f(a^k)=f(e)=e$$

אבל מצד שני, אם איזשהוא k מקיים ש

$$(f(a))^k=e$$

אז למעשה

$$f(a^k)=f(e)$$

ולפי החח"ע

$$a^k = e$$

ולכן אותם ה k שעבורם $a^k = e$ מקיימים גם ש $(f(a))^k = e$ וממילא

$$\mathrm{o}(f(a)) = \mathrm{o}(a)$$

עכשיו, נסמן ב X את קבוצת האיברים מסדר 5. היות ש f חח"ע ועל אנחנו יודעים ש

$$|f(X)| = |X|$$

ולכן $f(X)$ היא גם קבוצה של 4 איברים מסדר 5. אם היה איבר $h \in H \backslash f(X)$ מסדר 5 אז גם $f^{-1}(h)$ מסדר 5 אבל $f^{-1}(h) \notin X$ בסתירה לכך ש X מכילה את כל האיברים מסדר 5.

ולכן גם ב H יש בדיוק 4 איברים מסדר 5. האיברים של הקבוצה $f(X)$.

שאלה 5.4 יהי $f : G \to H$ הומומורפיזם. נניח כי G אבלית, הוכיחו כי $\operatorname{Im} f$ גם חבורה אבלית.

פתרון: ניקח $x, y \in \operatorname{Im} f$. לפי הגדרה יש $a, b \in G$ כך ש

$$f(a) = x, \quad f(b) = y$$

ואז

$$xy = f(a)f(b) = f(ab)$$

ולפי אבליות של G מתקיים

$$f(ab) = f(ba) = f(b)f(a) = yx$$

כנדרש.

שאלה 5.5 עבור כל אחת מהפונקציות הבאות. קבעו אם היא הומומורפיזם/ מונומורפיזם/ אפימורפיזם/ איזומורפיזם.

1. עבור $G = (\mathbb{Q}, +)$ ו $H = (\mathbb{R} \backslash \{0\}, \cdot)$ הפונקציה $f : G \to H$ המוגדרת לפי $f(x) = e^x$.

   פתרון: זה הומומורפיזם כי

$$f(x+y) = e^{x+y} = e^x e^y = f(x)f(y)$$

   זאת כמובן לא פונקציה על אבל היא כן חח"ע ולכן בסך הכל זה מונומורפיזם.

2. $f : S_7 \to \mathbb{Z}$ המוגדרת לפי $f(\sigma) = \sigma(1)$.

   פתרון: זה בכלל לא הומומורפיזם אפילו אם לוקחים $\sigma = \mathrm{id}$ (תמורת הזהות) אז

$$f(\mathrm{id} \cdot \mathrm{id}) = f(\mathrm{id}) = \mathrm{id}(1) = 1$$

   אבל

$$f(\mathrm{id}) + f(\mathrm{id}) = 1 + 1 = 2$$

3. $f:\mathbb{Z}\to\mathbb{Z}_n$ המוגדרת לפי $f(k)=[k]$ (כלומר שולחת כל איבר k למחלקת השקילות שלו מודולו n)
פתרון: זה כן הומומורפיזם כי

$$f(k_1+k_2)=[k_1+k_2]=[k_1]+[k_2]=f(k_1)+f(k_2)$$

אני מדגיש כאן את ההבדל בין k שהוא איבר ב $\mathbb{Z}$ ל $[k]$ שהיא מחלקת שקליות ולכן איבר ב $\mathbb{Z}_n$. בדר"כ אנחנו מחפפים וכותבים k במקום $[k]$. הפונקציה הזאת היא כמובן על אבל לא חח"ע ולכן היא אפימורפיזם.

4. G חבורה ו $x\in G$. פונקציה $f:G\to G$ מוגדרת לפי $f(g)=xgx^{-1}$.
פתרון: זה הומומורפיזם

$$f(gh)=xghx^{-1}=xgx^{-1}xhx=f(g)f(h)$$

זאת פונקציה חח"ע ועל כי יש לה הופכית שהיא:

$$f^{-1}(g)=x^{-1}gx$$

ואכן קל לוודא ש

$$f^{-1}f=\mathrm{id}$$

$$ff^{-1}=\mathrm{id}$$

שאלה 5.6 בכל אחד מהסעיפים הבאים הפרך או תן דוגמא:

1. האם יש אפימורפיזם

$$f:\mathbb{Z}_4\to\mathbb{Z}_2\times\mathbb{Z}_2$$

פתרון: היות ששתי הקבוצות סופיות ובאותו גודל. אם יש ביניהן פונקציה על היא תהיה גם חח"ע. כלומר זה יהיה איזומורפיזם. אבל אין איזומורפיזם בין החבורות האלה כי אחת ציקלית והאחרת לא.

2. האם יש אפימורפיזם -

$$f:\mathbb{Z}_{20}\to\mathbb{Z}_5$$

פתרון: כן. אם נסמן ב $[k]_{20}$ איברים של $\mathbb{Z}_{20}$ וב $[k]_5$ איברים של $\mathbb{Z}_5$ אז האפימורפיזם פשוט שולח

$$f([k]_{20})=[k]_5$$

כלומר בוחרים נציג ממחלקת השקילות $[k]_{20}$ ומסתכלים על המחלקה שלו ב $\mod 5$.
שימו לב! דבר ראשון צריך להוכיח שהפונקציה הזאת בכלל מוגדרת היטב! כי הגדרנו אותה לפי נציגים. במקרה הזה זה קל. אם

$$[k]_{20} = [k']_{20}$$

זה אומר בעצם ש

$$20 \mid k - k'$$

ולכן וודאי

$$5 \mid k - k'$$

ולכן

$$[k]_5 = [k']_5$$

להוכיח שזה הומ' זה מיידי

$$f([k]_{20}+[k']_{20}) = f([k+k']_{20}) = [k+k']_5 = [k]_5+[k']_5 = f([k]_{20})+f([k']_{20})$$

קל לוודא שזו פונקציה על אבל לא חח"ע (למשל $[5]_{20} \neq [0]_{20}$ אבל שניהם נשלחים ל $[0]_5$) ולכן זה אפימורפיזם.

3. האם יש איזומורפיזם

$$f : (\mathbb{R}, +) \to (\mathbb{R}^+, \cdot)$$

רמז: התשובה כבר (כמעט) נמצאת בשאלה אחרת בתרגיל בית.
פתרון: קל לבדוק ש e^x הוא איזומורפיזם.

4. האם יש איזומורפיזם

$$f : (\mathbb{R}\backslash\{0\}, \cdot) \to (\mathbb{R}^+, \cdot)$$

פתרון: לא. ב $(\mathbb{R}^+, \cdot)$ אין אף איבר מסדר 2 ואילו ב $(\mathbb{R}\backslash\{0\}, \cdot)$ יש איבר מסדר 2 (הלא הוא -1)

5. האם יש מונומורפיזם

$$f : S_3 \to \mathbb{Z}_{100} \times \mathbb{Z}_{100} \times \mathbb{Z}_{50}$$

פתרון: לא. אינטואיטיבית. אם היה כזה אז S_3 היתה "שוכנת" בתוך החבורה האבלית מצד ימין בסתירה לכך ש S_3 לא אבלית. יותר פורמלית: נניח בשלילה שיש כזה מונומורפיזם. ניקח $a, b \in S_3$ כך ש

$$ab \neq ba$$

יש כאלה כי S_3 לא אבלית. היות ש f חח"ע נקבל ש

$$f(ab) \neq f(ba)$$

ולכן

$$f(a)f(b) \neq f(b)f(a)$$

בסתירה לכך ש $\mathbb{Z}_{100} \times \mathbb{Z}_{100} \times \mathbb{Z}_{50}$ אבלית.

שאלה 5.7 יהיו $f_1, f_2 : G \to H$ שני הומומורפיזמים. ניקח כמה איברים $g_1, \ldots, g_k \in G$ ונניח כי לכל $1 \leq i \leq k$ מתקיים

$$f_1(g_i) = f_2(g_i)$$

. הוכיחו כי לכל $x \in \langle g_1, \ldots, g_k \rangle \leq G$ מתקיים כי

$$f_1(x) = f_2(x)$$

לאמור: הומומורפיזמים שמסכימים על קבוצת איברים מסכימים על התת חבורה שהקבוצה הזאת יוצרת.
פתרון: נסמן ב X את קבוצת כל האיברים $x \in G$ שמקיימים $f_1(x) = f_2(x)$. קבוצה זו לא ריקה כי $g_1, \ldots, g_k \in X$. מעבר לכך, זו תת חבורה כי אם

$$x, y \in X$$

אז

$$f_1(xy) = f_1(x)f_1(y) = f_2(x)f_2(y) = f_2(xy)$$

ולכן $xy \in X$. ובדומה אם $x \in X$ אז

$$f_1(x^{-1}) = f_1(x)^{-1} = f_2(x)^{-1} = f_2(x^{-1})$$

ולכן $x^{-1} \in X$ קיבלנו ש X היא תת חבורה שמכילה את $g_1, \ldots, g_k$ ולכן

$$\langle g_1, \ldots, g_k \rangle \leq X$$

שזה בדיוק מה שרצינו להוכיח.