תרגיל 2 מבוא לתורת החבורות

שאלה 2.1 הראו שבכל חבורה G עם מספר זוגי של איברים קיים איבר $x \neq e$ המקיים $x^2 = e$. (רמז: לכל איבר בחבורה יש הופכי יחיד).

פתרון: לכל איבר $g \in G$ קיים הופכי g^{-1}. להופכי הזה יש שתי אופציות בחיים. או ש $g = g^{-1}$ (ואז $g^2 = e$)או ש $g \neq g^{-1}$ ואז $g^2 \neq e$. יש לפחות איבר אחד בחבורה שההופכי שלו הוא עצמו וזה $g = e$. נניח שעבור כל שאר האיברים $g \neq g^{-1}$. אז אם נספור את האיברים בחבורה הם כולם באים בזוגות $\{g, g^{-1}\}$ למעט e שהוא לבד. אז מספר אברי החבורה הוא אי זוגי. בסתירה.

אפשר להסביר את ההוכחה הזאת קצת יותר פורמלית: אפשר להגדיר יחס שקילות שבו x שקול ל y אם $x = y$ או אם $x = y^{-1}$. מחלקות השקילות מכילות איבר וההופכי שלו. אם כל האיברים בחבורה שונים מההופכי (למעט e) אז כל מחלקות השקילות מכילות שני איברים למעט $\{e\}$ שמכילה רק איבר אחד. לכן ב G יש מספר אי זוגי של איברים. בסתירה. לכן חייב להיות איבר נוסף ששווה להופכי שלו.

שאלה 2.2 קבעו (והוכיחו את קביעתכם) האם התת קבוצות הבאות הן תת חבורות של החבורות הנתונות או לא:

1. $\mathbb{N} \subseteq (\mathbb{Z}, +)$.

פתרון: לא. אין הופכי. כלומר עבור $n \in \mathbb{N}$ לא קיים איבר $m \in \mathbb{N}$ כך ש $m + n = 0$.

2. $O_n(F) = \left\{A \in \mathrm{GL}_n(\mathbb{F}) \mid A^t = A^{-1}\right\} \subseteq \mathrm{GL}_n(\mathbb{F})$ המטריצות האורתוגונליות.

פתרון: כן. אפשר לוודא שכל הדרישות מתקיימות. הקבוצה הזאת לא ריקה כי I נמצאת בה. מכפלה של מטריצות אורתוגונליות היא גם אורתוגונלית כי אם A, B אורתוגונליות אז:

$$(AB)^t = B^t A^t = B^{-1} A^{-1} = (AB)^{-1}$$

ואם A אורתוגונלית גם ההופכית אורתוגונלית:

$$(A^{-1})^t = (A^t)^{-1} = (A^{-1})^{-1}$$

3. $\{A \in \mathrm{M}_n(\mathbb{F}) \mid \det A = 0\} \subseteq (\mathrm{M}_n(\mathbb{F}), +)$ (כאן $\mathrm{M}_n(\mathbb{F})$ הן כל המטריצות הריבועיות $n \times n$ עם פעולת החיבור)

פתרון: לא. אין בכלל סגירות. יכול להיות שסכום שתי מטריצות עם דטרמינטה 0 לא יהיה עם דטרמיננטה 0. למשל

$$A = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \quad B = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$$

שאלה 2.3 תהינה $H, K \leq G$ שתי תתי חבורות של חבורה G. הוכיחו או הפריכו את הטענות הבאות:

1. $H \cup K$ היא גם תת חבורה של G.

פתרון: לא. למשל $G = \mathbb{Z}$ ו $H = 2\mathbb{Z}$ ו $K = 3\mathbb{Z}$. נניח בשלילה ש $H \cup K$ היא חבורה. אז בפרט

$$1 = 3 - 2 \in H \cup K$$

בסתירה לכך ש $1 \notin H \cup K$.

הערה: אפשר להוכיח די בקלות את הוענה הבאה: $H \cup K$ חבורה אם ורק אם $H \subseteq K$ או $K \subseteq H$. כלומר בכל מקרה לא טריויאלי, איחוד תתי חבורות לא יוצא חבורה.

2. HK היא גם תת חבורה של G. (כאשר $HK = \{hk \mid h \in H \quad k \in K\}$)

פתרון: לא. למשל $G = S_3$. ניקח את $H = \{\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}\}$ ו $K = \{\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}\}$ אז אפשר לחשב ולבדוק ש

$$HK = \{\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}\}$$

אבל זאת לא תת חבורה. למשל בגלל ש

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \notin HK$$

שאלה 2.4 יהיו $m, n \in \mathbb{Z}$ שני מספרים שלמים. נסמן $d = \gcd(m,n)$ הוכיחו כי

$$\gcd(\frac{m}{d}, \frac{n}{d}) = 1$$

פתרון: יש צירוף לינארי

$$xm + yn = d$$

אז אם מחלקים ב d מקבלים

$$x\frac{m}{d} + y\frac{n}{d} = 1$$

ולכן

$$\gcd(\frac{m}{d}, \frac{n}{d}) = 1$$

יש כמובן עוד דרכים להראות את זה.

שאלה 2.5 הוכיחו כי בשביל שני מספרים שלמים $m, n \in \mathbb{Z}$ מתקיים כי $m \mid n$ אם ורק אם $\langle n \rangle \subseteq \langle m \rangle$. (כאשר $\langle n \rangle$ מסמן את התת חבורה הנוצרת על ידי n בתוך $(\mathbb{Z}, +)$. למעשה $\langle n \rangle = n\mathbb{Z}$)

פתרון: נניח $m \mid n$. אם $x \in \langle n \rangle$ זה אומר ש $n \mid x$ ולכן $m \mid x$ ולכן $x \in \langle m \rangle$. אז הוכחנו $\langle n \rangle \subseteq \langle m \rangle$. מצד שני, נניח $\langle n \rangle \subseteq \langle m \rangle$. אז בפרט $n \in \langle m \rangle$ ולכן $m \mid n$.

שאלה 2.6 חשבו את המחלק המשותף המקסימלי של זוגות המספרים הבאים. בנוסף, בטאו את ה $\gcd$ כצירוף של שני המספרים.

1. $24\ ,-11$
פתרון: נשתמש באלגוריתם אוקלידס.

$$24=-2\cdot(-11)+2$$

$$-11=-6\cdot 2+1$$

אז ה gcd הוא 1. נמצא את הצירוף הלינארי

$$\begin{aligned}1&=6\cdot 2-11=6\cdot(24+2\cdot(-11))-11\\&=6\cdot 24+13(-11)\end{aligned}$$

2. $117\ ,22$
פתרון: שוב, אלגוריתם אוקלידס.

$$117=5\cdot 22+7$$

$$22=3\cdot 7+1$$

ולכן ה gcd הוא 1. נמצא את הצירוף הלינארי

$$1=22-3\cdot 7=22-3(117-5\cdot 22)=-3\cdot 117+16\cdot 22$$

3. $785\ ,2780$
פתרון: די ברור ששני המספרים מתחלקים ב 5 אז בואו דבר ראשון נחלק אותם ב5.
קיבלנו

$$157,556$$

עכשיו נשתמש באלגוריתם אוקלידס

$$556=3\cdot 157+85$$

$$157=1\cdot 85+72$$

$$85=1\cdot 72+13$$

$$72=5\cdot 13+7$$

$$13=1\cdot 7+6$$

$$7 = 1 \cdot 6 + 1$$

אז ה gcd הוא 5. בחישוב לאחור זה יוצא

$$\begin{aligned} 1 &= 7 - 6 = 7 - (13 - 7) = 2 \cdot 7 - 13 = 2 \cdot (72 - 5 \cdot 13) - 13 \\ &= 2 \cdot 72 - 11 \cdot 13 = 2 \cdot 72 - 11 \cdot (85 - 72) = 13 \cdot 72 - 11 \cdot 85 \\ &= 13 \cdot (157 - 85) - 11 \cdot 85 = 13 \cdot 157 - 24 \cdot 85 \\ &= 13 \cdot 157 - 24 \cdot (556 - 3 \cdot 157) = -24 \cdot 556 + 85 \cdot 157 \end{aligned}$$

אז בסך הכל

$$5 = -120 \cdot 2780 + 420 \cdot 785$$