מתמטיקה דיסקרטית - תרגול 2

סמסטר קיץ תשפ"ד

נושאים: מבוא להוכחות, מבוא לתורת הקבוצות.

מבוא להוכחות

תרגיל 1. הוכיחו את הטענות הבאות:

1. לכל מספר שלם n, אם n זוגי אז n^2 זוגי.
2. לכל מספר שלם n, אם n^2 זוגי אז n זוגי.
3. סכום של מספר רציונלי ומספר אי-רציונלי הוא אי-רציונלי.
4. לכל מספר טבעי n, אם n הוא ריבוע ואי-זוגי אז קיים מספר שלם k כך ש-$n = 4k+1$.
5. לכל מספר שלם n, אם n זוגי אז **לא** קיים מספר k כך ש-$n^2 = 4k+2$.

פתרון 1. 1. יהי $n \in \mathbb{Z}$ כך ש-n זוגי.

- אזי, קיים $m \in \mathbb{Z}$ כך ש-$n = 2m$, ולכן $n^2 = 4m^2$.
- מכאן, עבור $k = 2m^2 \in \mathbb{Z}$ מתקיים $n^2 = 2k$.
- לכן קיים $k \in \mathbb{Z}$ כך ש-$n^2 = 2k$, וכך n^2 זוגי.

2. יהי $n \in \mathbb{Z}$. נוכיח את הקונטרפויזטיב של הטענה: אם n אי-זוגי אז n^2 אי-זוגי.

- נניח ש-n אי-זוגי, כלומר קיים $m \in \mathbb{Z}$ כך ש-$n = 2m+1$, ולכן

$$n^2 = (2m+1)^2 = 4m^2 + 4m + 1 = 2\left(2m^2 + 2m\right) + 1.$$

- מכאן, עבור $k = 2m^2 + 2m \in \mathbb{Z}$ מתקיים $n^2 = 2k+1$.

- לכן קיים $k \in \mathbb{Z}$ כך ש-$n^2 = 2k+1$, וכך n^2 אי-זוגי.

3. יהי $q \in \mathbb{Q}$ רציונלי ו-$r \in \mathbb{R} \setminus \mathbb{Q}$ אי-רציונלי. נניח בשלילה ש-$r+q \in \mathbb{Q}$.

- קיימים $n_1, m_1 \in \mathbb{Z}$ כך ש-$n_1 \neq 0$ ו-$q = {}^{m_1}/_{n_1}$, וקיימים $n_2, m_2 \in \mathbb{Z}$ כך ש-$n_2 \neq 0$ ו-$(r+q) = {}^{m_2}/_{n_2}$. אזי,

$$r = (r+q) - q = \frac{m_2}{n_2} - \frac{m_1}{n_1} = \frac{m_2 \cdot n_1 - m_1 \cdot n_2}{n_1 \cdot n_2} \in \mathbb{Q},$$

וזאת בסתירה לכך ש-r אינו רציונלי.

- הגענו לסתירה ולכן הטענה נכונה.

4. יהי $n \in \mathbb{N}$ ריבוע אי-זוגי.

- מכיוון ש-n ריבוע, קיים $m \in \mathbb{N}$ כך ש-$n = m^2$.
- בנוסף, ראינו שאם m^2 אי-זוגי אז m אי-זוגי (הקונטרפוזיטיב של טענה 1), ולכן קיים $k \in \mathbb{Z}$ כך ש-$m = 2k+1$. לכן,

$$n = m^2 = (2k+1)^2 = 4k^2 + 4k + 1 = 4\left(k^2 + k\right) + 1,$$

ולכן עבור $z = k^2 + k \in \mathbb{Z}$ מתקיים $n = 4z + 1$, וקיים מספר שלם $z \in \mathbb{Z}$ כך ש-$n = 4z + 1$.

5. יהי $n \in \mathbb{Z}$ זוגי, ונניח **בשלילה** כי קיים מספר k כך ש-$n^2 = 4k + 2$.

- מכיוון ש-n זוגי, קיים $m \in \mathbb{Z}$ כך ש-$n = 2m$. לכן,

$$4k + 2 = n^2 = (2m)^2 = 4m^2$$

$$\begin{aligned} 4k + 2 &= 4m^2 \\ 4k - 4m^2 &= 2 \\ 4\left(k - m^2\right) &= 2 \\ k - m^2 &= \frac{1}{2} \end{aligned}$$

- נשים לב ש-$k - m^2 \in \mathbb{Z}$, בסתירה לכך ש-$k - m^2 = 1/2$.
- הגענו לסתירה, ולכן לא קיים שלם k כך ש-$n^2 = 4k + 2$.

תרגיל 2. הוכיחו או הפריכו את הטענות הבאות:

1. לכל שני מספרים ממשיים a, b, אם $a^2 > b^2$ אז $a > b$.
2. המכפלה של שני ריבועים היא ריבוע.
3. לכל מספר ראשוני p מתקיים $(-1)^p = -1$.

פתרון 2. **1.** הפרכה: נבחר $a = -1, b = 0$ ונקבל $(-1)^2 > 0^2$ אבל $-1 < 0$.

2. יהיו $a, b \in \mathbb{N}$ כך ש-a, b ריבועים, נוכיח ש-$a \cdot b$ הוא ריבוע:

הוכחה. ידוע ש-a הוא ריבוע, ולכן קיים $x \in \mathbb{N}$ כך ש-$a = x^2$. באופן דומה, מכיוון ש-b הוא ריבוע קיים $y \in \mathbb{N}$ כך ש-$b = y^2$. נבחר $z = x \cdot y \in \mathbb{N}$ ונקבל

$$a \cdot b = x^2 \cdot y^2 = (x \cdot y)^2 = z^2,$$

ולכן קיים $n \in \mathbb{N}$ כך ש-$a \cdot b = n^2$, כלומר $a \cdot b$ הוא ריבוע. $\square$

3. הפרכה: נבחר $p = 2$ ונקבל $(-1)^2 = 1$.

טענה 1. $\sqrt{2} \notin \mathbb{Q}$ ($\sqrt{2}$ הוא אי-רציונלי).

הוכחה. נניח בשלילה כי $\sqrt{2}$ הוא רציונלי. אזי קיימים $m, n \in \mathbb{N}$ כך ש-$n \neq 0$, $\sqrt{2} = \frac{m}{n}$ ו-m/n לא ניתן לצמצום. מכאן,

$$\frac{m^2}{n^2} = 2 \implies m^2 = 2n^2.$$

לכן מהגדרה מתקיים ש-m^2 הוא זוגי, ומטענה שהראנו גם m זוגי: קיים $k \in \mathbb{Z}$ כך ש-$m = 2k$. אזי,

$$2n^2 = m^2 = (2k)^2 = 4k^2 \implies n^2 = 2k^2.$$

לכן n^2 הוא זוגי, וכך גם n זוגי. מכאן, הראנו כי m וגם n זוגיים, בסתירה לכך ש-m/n לא ניתן לצמצום (ניתן לצמצם ב-2). הגענו לסתירה ולכן $\sqrt{2}$ הוא אי-רציונלי. $\square$

<u>שאלה מתרגיל הבית:</u> אסוציאטיביות של XOR - לכל p, q, r מתקיים

$$(p \oplus q) \oplus r \equiv p \oplus (q \oplus r)\,.$$

הוכחה. ניתן להראות באמצעות טבלת אמת. בנוסף, ניתן לפתח כל אחד מהאגפים לקבלת שוויון:

$$\begin{aligned}(p \oplus q) \oplus r &\equiv ((p \wedge \neg q) \vee (\neg p \wedge q)) \oplus r \\ &\equiv (((p \wedge \neg q) \vee (\neg p \wedge q)) \wedge \neg r) \vee (\neg ((p \wedge \neg q) \vee (\neg p \wedge q)) \wedge r) \\ &\equiv ((p \wedge \neg q) \wedge \neg r) \vee ((\neg p \wedge q) \wedge \neg r) \vee ((\neg (p \wedge \neg q) \wedge \neg (\neg p \wedge q)) \wedge r) \\ &\equiv ((p \wedge \neg q) \wedge \neg r) \vee ((\neg p \wedge q) \wedge \neg r) \vee (((\neg p \vee q) \wedge (p \vee \neg q)) \wedge r) \\ &\equiv ((p \wedge \neg q) \wedge \neg r) \vee ((\neg p \wedge q) \wedge \neg r) \vee (((\neg p \vee q) \wedge (p \vee \neg q)) \wedge r) \\ &\equiv ((p \wedge \neg q) \wedge \neg r) \vee ((\neg p \wedge q) \wedge \neg r) \vee (((p \wedge q) \vee (\neg p \wedge \neg q)) \wedge r) \\ &\equiv (p \wedge \neg q \wedge \neg r) \vee (\neg p \wedge q \wedge \neg r) \vee (p \wedge q \wedge \neg r) \vee (\neg p \wedge \neg q \wedge r)\,.\end{aligned}$$

$$\begin{aligned}p \oplus (q \oplus r) &\equiv p \oplus ((q \wedge \neg r) \vee (\neg q \wedge r)) \\ &\equiv (p \wedge \neg ((q \wedge \neg r) \vee (\neg q \wedge r))) \vee (\neg p \wedge ((q \wedge \neg r) \vee (\neg q \wedge r))) \\ &\equiv (p \wedge (\neg (q \wedge \neg r) \wedge \neg (\neg q \wedge r))) \vee (\neg p \wedge q \wedge \neg r) \vee (\neg p \wedge \neg q \wedge r) \\ &\equiv (p \wedge ((\neg q \vee r) \wedge (q \vee \neg r))) \vee (\neg p \wedge q \wedge \neg r) \vee (\neg p \wedge \neg q \wedge r) \\ &\equiv (p \wedge ((\neg q \wedge \neg r) \vee (q \wedge r))) \vee (\neg p \wedge q \wedge \neg r) \vee (\neg p \wedge \neg q \wedge r) \\ &\equiv (p \wedge \neg q \wedge \neg r) \vee (\neg p \wedge q \wedge \neg r) \vee (\neg p \wedge \neg q \wedge r) \vee (p \wedge q \wedge \neg r)\,.\end{aligned}$$

שני הביטויים שקולים לאותו הביטוי, ולכן שקולים בעצמם. $\square$

מבוא לתורת הקבוצות

תזכורת:

1. הקטע הסגור $[a,b]$ מוגדר להיות

$$[a,b] = \{x \in \mathbb{R} \mid a \leq x \leq b\}\,.$$

2. הקטע הפתוח (a,b) מוגדר להיות

$$(a,b) = \{x \in \mathbb{R} \mid a < x < b\}\,.$$

3. הקטע החצי-פתוח חצי-סגור $(a,b]$ מוגדר להיות

$$(a,b] = \{x \in \mathbb{R} \mid a < x \leq b\}\,.$$

4. הקטע החצי-סגור חצי-פתוח $[a,b)$ מוגדר להיות

$$[a,b) = \{x \in \mathbb{R} \mid a \leq x < b\}\,.$$

תרגיל 3. חשבו את $A\cup B, A\cap B, A\setminus B, A\triangle B$ עבור:

1. $A=[0,3]\,, B=(2,7]$
2. $A=\{2k\mid k\in\mathbb{N}\}\,, B=\{2k+1\mid k\in\mathbb{N}\}$

פתרון 3. 1.

$$A\cup B=[0,7]\,,\quad A\cap B=(2,3]\,,\quad A\setminus B=[0,2]\,,\quad A\triangle B=[0,2]\cup(3,7]$$

2.

$$A\cup B=\mathbb{N},\quad A\cap B=\emptyset,\quad A\setminus B=A,\quad A\triangle B=\mathbb{N}$$

הגדרה 1. תהי A קבוצה. קבוצת החזקה של A, $P\left(A\right)$, היא קבוצה שאיבריה הם כל תתי-הקבוצות של A:

$$P\left(A\right)=\{S\mid S\subseteq A\}$$

הערה 1. עבור קבוצה A בת n איברים, ב-$P\left(A\right)$ יש 2^n איברים:

- עבור תת-קבוצה כלשהי, לכל אחד מ-n האיברים יש שתי אפשרויות: להיכנס לקבוצה, או לא להיכנס.
- לכן, יש בסך הכל $2\cdot 2\cdot\dots\cdot 2=2^n$ תתי-קבוצות.

תרגיל 4. 1. חשב את $P\left(P\left(P\left(\emptyset\right)\right)\right)$.

2. כמה איברים יש ב-$P\left(P\left(P\left(P\left(P\left(P\left(\emptyset\right)\right)\right)\right)\right)\right)$?

פתרון 4. 1.

$$P\left(\emptyset\right)=\{\emptyset\}$$
$$P\left(P\left(\emptyset\right)\right)=\{\emptyset,\{\emptyset\}\}$$
$$P\left(P\left(P\left(\emptyset\right)\right)\right)=\{\emptyset,\{\emptyset\}\,,\{\{\emptyset\}\}\,,\{\emptyset,\{\emptyset\}\}\}$$

2. נשים לב כי ב-$\emptyset$ יש 0 איברים. לאחר כל הפעלה של P על קבוצה בת n איברים, נקבל קבוצה בת 2^n איברים. לכן, מספר האיברים ב-$P\left(P\left(P\left(P\left(P\left(P\left(\emptyset\right)\right)\right)\right)\right)\right)$ הוא

$$2^{2^{2^{2^{2^{2^{0}}}}}}=2^{65536}.$$

תרגיל 5. הוכח/הפרך את הטענות הבאות, עבור קבוצות A, B, C.

1. $P(A \cup B) \subseteq P(A) \cup P(B)$
2. $P(A) \cup P(B) \subseteq P(A \cup B)$
3. $P(A \cap B) \subseteq P(A) \cap P(B)$
4. $P(A) \cap P(B) \subseteq P(A \cap B)$

פתרון 5.

1. הפרכה: עבור $A = \{1\}, B = \{2\}$:

$$P(A \cup B) = \{\emptyset, \{1\}, \{2\}, \{1,2\}\}$$

$$P(A) \cup P(B) = \{\emptyset, \{1\}\} \cup \{\emptyset, \{2\}\}$$

נשים לב כי $\{1,2\} \in P(A \cup B)$ אך $\{1,2\} \notin P(A) \cup P(B)$.

2. הוכחה: נראה שאם $S \in P(A) \cup P(B)$, אז $S \in P(A \cup B)$.

$$\begin{aligned} S \in P(A) \cup P(B) &\iff (S \in P(A)) \vee (S \in P(B)) \\ &\iff (S \subseteq A) \vee (S \subseteq B) \\ &\implies S \subseteq A \cup B \\ &\iff S \in P(A \cup B). \end{aligned}$$

3. הוכחה:

$$\begin{aligned} S \in P(A \cap B) &\iff S \subseteq A \cap B \\ &\iff (S \subseteq A) \wedge (S \subseteq B) \\ &\iff (S \in P(A)) \wedge (S \in P(B)) \\ &\iff S \in P(A) \cap P(B). \end{aligned}$$

4. מכיוון שכל צעדי הוכחת הסעיף הקודם הם דו-כיווניים, גם כיוון זה מתקיים מאותה ההוכחה.