

שיטות הוכחה:

נעשה קצת סדר – איך לגשת לשאלות במתמטיקה ולנסות להוכיח טענות מתמטיות.

ראשית, נבחין בעובדה הסטטיסטית הבאה: רוב מוחלט של הטענות שאנחנו צריכים להוכיח הן טענות של "לכל". למשל:

"יהי (=נתון) משולש $\triangle ABC$ שווה שוקיים, עם זווית: $B = 60^\circ$. הוכיחו שהמשולש הוא שווה צלעות". זו, בפועל, טענה של "לכל": "כל משולש שווה שוקיים עם זווית שווה ל-60 הוא שווה צלעות".

מצד שני, טענת "לכל" אפשר בפועל לתאר עם קשר הגרירה. למשל, בדוגמה שלנו: "אם משולש הוא שווה-שוקיים וגם אחת מהזוויות שלו היא 60, אז המשולש הוא שווה צלעות".

אי לכך ובהתאם לזאת, נמקד את עיקר מאמצינו בשיטות הוכחה של טענת גרירה – איך מראים שהפסוק $p \rightarrow q$ הוא T ? נציג כמה שיטות לעשות זאת.

1. נכונות באופן ריק:

אם $p = F$, הפסוק $p \rightarrow q$ הוא "אוטומטית" T . אי-אפשר "באמת" להוכיח טענות עם נכונות באופן ריק (אם נתון משולש שווה-שוקיים, אנחנו אף פעם לא ננסה להראות שהוא לא כזה...), אבל זה מופיע לעיתים בתוך הוכחות "גדולות יותר".

2. "הוכחה ישירה":

זו דרך המלך – אנחנו מניחים ש: $p = T$ (שהנתונים נכונים), ובאמצעות הנתונים+הגדרות+משפטים+ידע מתמטי קודם וכו' מראים שגם $q = T$. כך הוכחנו את כל השאלות בגיאומטריה בבית הספר, כך גם עשינו באינדוקציה (הנחנו $P(n) = T$ והראנו ש: $P(n+1) = T$, וכך הוכחנו שאכן: $P(n) \rightarrow P(n+1) = T$).

כדי להוכיח ישירות, אנחנו צריכים לשלוט בהגדרות, במשפטים וכן הלאה. למשל, נוכיח את הטענה הבאה: "יהי $n \in \mathbb{Z}$. הוכיחו שאם n אי-זוגי אז n^2 אי-זוגי". כדי להוכיח זאת כמו שצריך, אנחנו צריכים להגדיר את המושג של "אי-זוגי". נגדיר:

מספר שלם $n \in \mathbb{Z}$ נקרא אי-זוגי אם קיים $k \in \mathbb{Z}$ כך ש: $n = 2k + 1$.

נקרא זוגי אם קיים $k \in \mathbb{Z}$ כך ש: $n = 2k$.
 כעת, נוכיח את הטענה. יהי $n \in \mathbb{Z}$. נניח ש- n אי-זוגי ונוכיח ש- n^2 אי-זוגי.
 אם כן, n אי-זוגי ולכן - לפי ההגדרה - קיים $k \in \mathbb{Z}$ כך ש: $n = 2k + 1$.
 נעלה בריבוע ונקבל:

$$n^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$$

מכיוון ש- k שלם, גם $2k^2 + 2k$ שלם, ולכן - לפי ההגדרה - n^2 אי-זוגי, כנדרש.

3. *Contrapositive* - "ללכת הפוך":

הפסוק $p \rightarrow q$ שקול לפסוק $\neg q \rightarrow \neg p$ (תוכיחו בטבלת אמת!). למשל, הפסוק "אם הגובה שלי הוא מעל 1.80 אז הגובה שלי הוא מעל 1.70" שקול לפסוק: "אם הגובה שלי לא מעל 1.70, אז הגובה שלי לא מעל 1.80"; כאן, p הוא "מעל 1.80" ו- q הוא "מעל 1.70".
 מכיוון שהפסוקים שקולים, במקום להוכיח את $p \rightarrow q$ ישירות, נוכיח את $\neg q \rightarrow \neg p$ ישירות.

למשל, נוכיח את הטענה: יהי $n \in \mathbb{Z}$. הוכיחו שאם n^2 אי-זוגי אז n אי-זוגי. מה יקרה אם ננסה להוכיח ישירות? נתון ש: $n^2 = 2k + 1$, וצ"ל שגם n אי-זוגי. אנחנו רוצים להגיע מהנתון על n^2 למסקנה על n , וכדי להגיע מ- n^2 ל- n אנחנו צריכים להוציא שורש: $n = \sqrt{2k + 1}$, ואיך נתקדם מפה...?
 אצלנו, p הוא " n^2 אי-זוגי" ו- q הוא " n אי-זוגי". הקונטרה-פוזיטיב היא: "אם n הוא לא אי-זוגי, אז n^2 הוא לא אי-זוגי". כלומר, הטענה היא: אם n זוגי אז n^2 זוגי. את הטענה הזו נוכיח ישירות - נניח ש- n זוגי, צ"ל: n^2 זוגי.
 אם כן, n זוגי ולכן - לפי ההגדרה - קיים $k \in \mathbb{Z}$ עבורו: $n = 2k$. נעלה בריבוע ונקבל:

$$n^2 = 4k^2 = 2 \cdot 2k^2$$

מכיוון ש- k שלם, גם $2k^2$ שלם ולכן - לפי ההגדרה - n^2 זוגי.

4. חלוקה למקרים:

נחלק את הנתונים p לכמה מקרים שונים, ובכל מקרה נוכיח שהמסקנה q היא נכונה (ישירות בדרך כלל).

למשל, נוכיח את הטענה הבאה: יהי $n \in \mathbb{Z}$. אם n לא מתחלק ב-3 אז שארית החלוקה של n^2 ב-3 היא 1. במילים אחרות, אם $n \not\equiv 0 \pmod{3}$ אז $n^2 \equiv 1 \pmod{3}$.

אם כן, את הנתון " n לא מתחלק ב-3" אפשר לחלק לשני מקרים - קיים k שלם כך ש: $n = 3k + 1$, קיים k שלם כך ש: $n = 3k + 2$. אנחנו נראה שבכל מקרה המסקנה אכן מתקיימת. מקרה ראשון: נניח ש: $n = 3k + 1$. נעלה בריבוע:

$$n^2 = (3k + 1)^2 = 9k^2 + 6k + 1 = 3(3k^2 + 2k) + 1$$

ואכן, שארית החלוקה של n^2 ב-3 היא 1.

מקרה שני: נניח ש: $n = 3k + 2$. נעלה בריבוע:

$$n^2 = (3k + 2)^2 = 9k^2 + 12k + 4 = 9k^2 + 12k + 3 + 1 = 3(3k^2 + 4k + 1) + 1$$

ואכן, שארית החלוקה של n^2 ב-3 היא 1.

סה"כ, הראנו שבכל מקרה שבו n לא מתחלק ב-3, שארית החלוקה של n^2 ב-3 היא 1 והטענה אכן נכונה.

5. הוכחה בשלילה:

לפי כלל הגרירה: $p \rightarrow q \equiv \neg p \vee q$. לכן, אפשר להראות: $\neg(p \rightarrow q) \equiv p \wedge \neg q$. בהוכחה בשלילה, במקום להראות ש: $p \rightarrow q = T$, נראה ש: $\neg(p \rightarrow q) = F$, ולפי מה שהסברנו אפשר להראות במקום: $p \wedge \neg q = F$. בפועל, נניח שהנתונים הם T , ובנוסף נניח שגם השלילה של המסקנה $\neg q$ היא T (הנחה כזו נקראת "הנחה בשלילה"), וננסה להגיע לסתירה. ברגע שהגענו לסתירה, הוכחנו שהטענה המקורית אכן נכונה.

נעשה שתי דוגמאות - נוכיח שיש אינסוף מספרים ראשוניים, ונוכיח ש- $\sqrt{2}$ אי-רציונלי.

רק נזכיר - מספר $p > 1$ טבעי הוא ראשוני, אם p מתחלק רק בעצמו וב-1. למשל: 2, 3, 5, 7, 11, 13, 17, 19, ...

משפט:

קיימים אינסוף מספרים ראשוניים.

הוכחה:

נניח בשלילה שהטענה לא נכונה. כלומר, יש מספר סופי של ראשוניים. אם

כן, אפשר להציג את כולם ברשימה: p_1, p_2, \dots, p_n . (איך נגיע לסתירה? נראה שבהכרח יש עוד ראשוני, שלא נמצא ברשימה – וזו סתירה לכך שברשימה נמצאים כולם). נתבונן במספר הבא:

$$S = p_1 \cdot \dots \cdot p_n + 1 = \prod_{i=1}^n p_i + 1$$

האם S ראשוני? אם כן, S הוא ראשוני שלא ברשימה (הוא "הרבה" יותר גדול מכולם) וזו סתירה. אם לא, אז S מתחלק בראשוני, אבל הראשוני הזה לא נמצא ברשימה כי בכל הראשוניים שברשימה S לא מתחלק (בגלל ה-1). בכל מקרה, יש ראשוני שלא נמצא ברשימה, וסתירה. לכן, הטענה נכונה – יש אינסוף ראשוניים.

משפט:

$\sqrt{2}$ אי-רציונלי.

הוכחה:

נניח בשלילה שהטענה לא נכונה, כלומר $\sqrt{2}$ רציונלי. לכן, קיימים $n \in \mathbb{N}, m \in \mathbb{Z}$ כך ש: $\sqrt{2} = \frac{m}{n}$, כך שהשבר הוא מצומצם (איך נגיע לסתירה? נראה שהשבר לא מצומצם). נעלה את שני האגפים בריבוע:

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

לכן, m^2 זוגי ולכן גם m זוגי – אפשר לרשום: $m = 2k$. נציב זאת בשוויון ונקבל:

$$(2k)^2 = 2n^2 \implies n^2 = 2k^2$$

לכן, n^2 זוגי ולכן גם n זוגי. אם כן, m, n שניהם זוגיים ולכן השבר $\frac{m}{n}$ לא מצומצם (אפשר לצמצם אותו ב-2 לפחות), וסתירה. לכן הטענה נכונה: $\sqrt{2}$ אי-רציונלי.

*הערה: אם n הוא לא ריבוע (כלומר, לא $1, 4, 9, 16, \dots$), אז \sqrt{n} הוא אי-רציונלי.

הפרכת טענות:

אנחנו רוצים להראות שטענה איננה נכונה. אם אנחנו רוצים להראות

שטענט "לכל" אינה נכונה, מספיקה לנו דוגמה נגדית - דוגמה אחת ספציפית מפורשת שבה הטענה לא נכונה. למשל, אם אנחנו רוצים להראות ש: $\exists x (P(x) \wedge Q(x)) \equiv (\exists x P(x)) \wedge (\exists x Q(x))$ דוגמה אחת ספציפית לשני פרדיקטים P, Q שעבורם הטענה לא נכונה. למשל, מעל השלמים: $P(x) : x > 0$ ו- $Q(x) : x \leq 0$.

הוכחת טענות קיום:

למשל: לכל x ממשי חיובי, קיים y ממשי חיובי שקטן מ- x . מספיק להצביע על y ספציפי שמקיים את הדרוש. במקרה שלנו - יהי $x > 0$. המספר: $y = \frac{x}{2}$ מקיים את הדרוש - חיובי וקטן מ- x .

*הוכחת יחידות:

כשנרצה להראות שיצור מסוים הוא היחיד שמקיים תנאי מסוים (למשל, להראות שבשדה יש איבר יחיד שהוא נייטרלי לחיבור), אפשר להניח בשלילה שיש עוד מישהו אחר שמקיים את התנאי ולהגיע לסתירה; לחלופין, להניח שיש עוד מישהו שמקיים את התנאי ולהראות שהם אותו אחד. נוכיח בשדה הנייטרלי לחיבור הוא יחיד. \mathbb{F} שדה, $0_{\mathbb{F}}$ הנייטרלי. נניח בשלילה שקיים $b \in \mathbb{F}$ ששונה מ- $0_{\mathbb{F}}$ המקיים: $a + b = b + a = a$ לכל $a \in \mathbb{F}$. כעת, אפשר לומר (למשל):

$$b + 0_{\mathbb{F}} = 0_{\mathbb{F}} + b$$

מחילופיות החיבור. בצד שמאל לא נרשום את $0_{\mathbb{F}}$ ובצד ימין לא נרשום את b (שניהם נייטרליים...) ואז נקבל:

$$b = 0_{\mathbb{F}}$$

בסתירה לכך שהם שונים זה מזה.

הוכחת שוויון בין קבוצות:

אמרנו כבר ש: $A = B$ פירושו: $x \in A \iff x \in B$. לכן, כשנרצה להוכיח ש: $A = B$ נוכיח ש: $x \in A \iff x \in B$. יש לנו שתי דרכים לעשות זאת - או להוכיח את ה"אם ורק אם" בבת אחת (כלומר, להשתמש

אך ורק בהגדרות או שקילויות לוגיות), או להוכיח שתי גרירות לצד אחד:
 $x \in A \rightarrow x \in B$ וגם $x \in B \rightarrow x \in A$. שיטה זו נקראת הכלה דו־כיוונית.
 למשל, נוכיח שלכל שלוש קבוצות A, B, C מתקיים:

$$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$$

אם כן: (תזכורת: $x \in A \cap B \iff x \in A \wedge x \in B$;
 $x \in A \cup B \iff x \in A \vee x \in B$)

$$x \in A \cup (B \cap C) \iff x \in A \vee x \in (B \cap C) \iff x \in A \vee (x \in B \wedge x \in C)$$

המעבר הראשון - לפי הגדרת איחוד. המעבר השני - לפי הגדרת חיתוך.
 שקילות לוגית: $p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$; אצלנו:

$$p : x \in A, q : x \in B, r : x \in C$$

ונקבל:

$$x \in A \vee (x \in B \wedge x \in C) \iff (x \in A \vee x \in B) \wedge (x \in A \vee x \in C)$$

נמשיך:

$$(x \in A \vee x \in B) \wedge (x \in A \vee x \in C) \iff (x \in A \cup B) \wedge (x \in A \cup C) \iff x \in (A \cup B) \cap (A \cup C)$$

המעבר הראשון - לפי הגדרת איחוד. המעבר השני - לפי הגדרת חיתוך.
 סה"כ:

$$x \in A \cup (B \cap C) \iff x \in (A \cup B) \cap (A \cup C)$$

לפי הגדרת השוויון בין קבוצות, נקבל שאכן: $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$.

הפרש סימטרי:

ההפרש הסימטרי של שתי קבוצות A, B מסומן: $A \Delta B$, זו קבוצת כל
 האיברים שנמצאים ב- A או ב- B אבל לא בשניהם. כלומר:

$$A \Delta B = (A \cup B) \setminus (A \cap B) = (A \setminus B) \cup (B \setminus A)$$

למשל:

$$A = \{1, 2, 3\}, B = \{1, 3, 5, 7, 8\} \implies A \Delta B = \{2, 5, 7, 8\}$$

תכונות:

א. $A \Delta B = B \Delta A$.

ב. $A \Delta \emptyset = A, A \Delta A = \emptyset$.

משלים:

המשלים של A מתאר את קבוצת כל האיברים שלא נמצאים ב- A : $x \in A^c \iff x \notin A$. כדי לומר מהו המשלים, אנחנו צריכים להגיד איפה האיברים כן נמצאים. לכן, כשאנחנו מדברים על משלים אנחנו מניחים שיש קבוצה גדולה U שנמצאת מאחורי הקלעים וכל האיברים נלקחים ממנה.
למשל:

$$U = \{1, 2, 3, 4, 5\}, A = \{1, 4\} \implies A^c = \{2, 3, 5\}$$

U נקראת "קבוצה אוניברסלית". בעצם: $A^c = U \setminus A$.

$$x \notin A \cap B \iff \neg(x \in A \cap B) \iff \neg(x \in A \wedge x \in B)$$

דה־מורגן:

$$\iff \neg(x \in A) \vee \neg(x \in B) \iff x \notin A \vee x \notin B$$

תכונות:

1. $(A^c)^c = A$.

2. חוק המשלים: $A \setminus B = A \cap B^c$.

איחוד וחיתוך של יותר משתי קבוצות:

מבחינת הגדרה, איבר נמצא בחיתוך אם ורק אם הוא נמצא בכל אחת מהקבוצות המשתתפות בחיתוך; איבר נמצא באיחוד אם ורק אם הוא נמצא בלפחות אחת מהקבוצות המשתתפות באיחוד (קיימת קבוצה שהאיבר שייך

אליה). למשל:

$$\{1, 2, 3, 4\} \cap \{1, 2, 4, 8\} \cap \{2, 4, 6, 8\} = \{2, 4\}$$

$$\{1, 2, 3, 4\} \cup \{1, 2, 4, 8\} \cup \{2, 4, 6, 8\} = \{1, 2, 3, 4, 6, 8\}$$

הבעיה היא איך נסמן את האיחוד/חיתוך האלו.

אם יש לנו מספר סופי של קבוצות: A_1, \dots, A_n , אפשר לרשום:

$$A_1 \cup \dots \cup A_n = \bigcup_{i=1}^n A_i, \quad A_1 \cap \dots \cap A_n = \bigcap_{i=1}^n A_i$$

איך נטפל במקרה הכללי (אינסוף קבוצות)? נשים לב, במקרה הסופי, אפשר לרשום את קבוצת האינדקסים: $I = \{1, 2, \dots, n\}$. את החיתוך/איחוד אפשר לתאר באמצעות קבוצת האינדקסים באופן הבא:

$$\bigcup_{i=1}^n A_i = \bigcup_{i \in I} A_i$$

כלומר, במקום לומר "מפורשות" מאיפה לאיפה האינדקס רץ, נאמר שהוא שייך לקבוצת אינדקסים.

למשל: $A_i = \{1, 2, 3, \dots, i\}$, כאשר: $i \in I = \{1, \dots, 20\}$. לכן:

$$\bigcap_{i \in I} A_i = \bigcap_{i=1}^{20} A_i = A_1 \cap \dots \cap A_{20} = \{1\} \cap \{1, 2\} \cap \dots \cap \{1, 2, \dots, 20\} = \{1\}$$

כך, נוכל לסמן גם חיתוך/איחוד עם כל קבוצת אינדקסים - החיתוך והאיחוד של הקבוצות A_i כאשר $i \in I$ הוא:

$$\bigcup_{i \in I} A_i, \quad \bigcap_{i \in I} A_i$$

למשל: $A_i = \{i, i + \frac{1}{2}\}$ כאשר $i \in I = \mathbb{R}$. למשל: $A_{\sqrt{2}} = \{\sqrt{2}, \sqrt{2} + \frac{1}{2}\}$.
כעת:

$$\bigcap_{i \in \mathbb{R}} A_i = \emptyset, \quad \bigcup_{i \in I} A_i = \mathbb{R}$$

כל מספר ממשי נמצא באחת הקבוצות לפחות, ולכן האיחוד הוא כל הממשיים;
 אין מספר שנמצא בכל הקבוצות ולכן החיתוך ריק).
 *אפשר לסמן:

$$\bigcap_{i \in \mathbb{N}} = \bigcap_{i=1}^{\infty}$$

כלומר, אפשר לסמן את הטבעיים כאינדקס שרץ מ-1 ועד "אינסוף".
 דרך נוספת לתאר חיתוך/איחוד כאלו – אחרי שהגדרנו את קבוצת האינדקסים,
 לסמן ב- \mathcal{F} (או כל אות אחרת שבא לכם, כמובן) את קבוצת כל הקבוצות
 שלנו, למשל בדוגמה האחרונה:

$$\mathcal{F} = \{A_i \mid i \in \mathbb{R}\}$$

ואז:

$$\bigcap_{i \in \mathbb{R}} A_i = \cap \mathcal{F}, \quad \bigcup_{i \in \mathbb{R}} A_i = \cup \mathcal{F}$$

למשל:

$$\mathcal{F} = \{\{1, 2, 3, 4\}, \{1, 2, 4, 8\}, \{2, 4, 6, 8\}\}$$

אז:

$$\cap \mathcal{F} = \{1, 2, 3, 4\} \cap \{1, 2, 4, 8\} \cap \{2, 4, 6, 8\} = \{2, 4\}$$