מבוא למתמטיקה אקדמית
אופיר שנבל

1 מבוא

מטרת חוברת זו היא לתת לסטודנטים מתחילים את הידע המתמטי הבסיסי אותו יפגשו במהלך התואר. כמובן שרוב החומר הנלמד בתואר לא מופיע בחוברת זו. כמו כן, ישנם נושאים שמוזכרים בחוברת שלא בהכרח ילמדו במהלך התואר (גם כתלות במחלקה) אך הכרה שלהם תוכל לעזור להבין מושגים אחרים.

1.1 תורת הקבוצות , לוגיקה והוכחות מתמטיות

1.1.1 לוגיקה

פסוק הוא טענה מתמטית שלגביה ניתן לקבוע אם היא טענת שקר או טענת אמת, כלומר פסוק הוא תמיד אמיתי או שקרי. למשל: בשבוע יש שבעה ימים, לדג יש רגליים, $2 < 3$.

הגדרה 1.1 בהנתן שני פסוקים α, β. נאמר ש

1. הפסוק α וגם β אמת רק אם שני הפסוקים הם אמת. סימון $\alpha \wedge \beta$.
2. הפסוק α או β אמת רק אם לפחות אחד מהפסוקים הוא אמת. סימון $\alpha \vee \beta$.
3. נאמר שהפסוק α גורר את הפסוק β אם כאשר α הוא אמת אז בהכרח גם β הוא אמת. מסמנים $\alpha \Rightarrow \beta$ ואומרים כי הטענה α חזקה יותר מהטענה β. אם $\alpha \Rightarrow \beta$ וגם $\beta \Rightarrow \alpha$ אז מסמנים $\alpha \Leftrightarrow \beta$ ואומרים כי הטענות שקולות זו לזו או שטענה α נכונה אם ורק אם β נכונה.

למשל, הפסוק "יורד גשם" גורר את הפסוק "יש עננים בשמיים" אבל ההיפך לא נכון כי ייתכן שיש עננים אבל לא יורד גשם. לשם פשטות וקיצור אנחנו נשתמש לעיתים באותיות כדי לסמן פסוקים או טענות מתמטיות.

דוגמא 1.2 יהיו α_1 הטענה x מספר זוגי. α_2 הטענה x מתחלק ב3. α_3 הטענה x מתחלק ב6. אזי מתקיים

1. $\alpha_3 \Rightarrow \alpha_1$.
2. $\alpha_3 \Rightarrow \alpha_2$.
3. α_1 לא גורר את α_3
4. α_2 לא גורר את α_3.
5. $\alpha_3 \Leftrightarrow (\alpha_1 \wedge \alpha_2)$.

חוץ מקשרים לוגים כמו "גרירה", "או" ו"וגם" אנו נוהגים להשתמש בבניית טענות מתמטיות גם בכמתים, בעיקר קיים המסומן ב $\exists$ ולכל המסומן ב $\forall$. למשל ניתן לטעון כי לכל מספר ממשי x קיים מספר ממשי אחר y כך ש $x-y$ הוא מספר שלם. בהמשך נדון באיך מוכיחים טענות מסוג זה, אך לפני כן עלינו ללמוד עוד מספר מושגים.

1.1.2 קבוצות

קבוצה היא אוסף כלשהו של עצמים. עצמים אלו נקראים איברי הקבוצה. נסמן קבוצה לרוב באותיות גדולות ואת איבריהם באותיות קטנות.
סימון: תהיי A קבוצה, נסמן כי האיבר x שייך לקבוצה A ע"י $x \in A$.
יש מספר דרכים לתאר איברים בקבוצה

1. כתיבה מפורשת- למשל קבוצה שאיבריה הם x, y, z תסומן ב $A = \{x, y, z\}$.

הערה 1.3 אין משמעות לחזרות או לסדר איברי הקבוצה, כלומר

$$\{x, y, z\} = \{z, x, y\} = \{x, x, y, z, z\}.$$

לעיתים ניתן לקצר בכתיבה אם ברורה הכוונה, למשל $B = \{1, 2, 3, \ldots, 20\}$. בצורה זו ניתן להגדיר גם קבוצות אינסופיות, למשל את קבוצת המספרים הטבעיים

$$\mathbb{N} = \{1, 2, 3, \ldots\},$$

או את קבוצת המספרים השלמים

$$\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}.$$

2. תיאור קבוצה על פי תכונות איבריה. למשל הקבוצה B לעיל ניתנת לכתיבה גם על ידי $B = \{x \in \mathbb{N} : 1 \leq x \leq 20\}$. פה הסימן : נקרא כ"כך ש". כלומר בקבוצה B יש את כל המספרים הטבעיים כך שמספרים אלו בין 1 ל20. בצורה זו אפשר להגדיר את קבוצת המספרים הרציונלים

$$\mathbb{Q} = \left\{ \frac{n}{m} : n \in \mathbb{Z}, m \in \mathbb{N} \right\}.$$

סימון: בהנתן קבוצה A בעלת מספר סופי של איברים, נסמן ב$|A|$ את מספר האיברים בקבוצה ונאמר ש$|A|$ הוא גודל הקבוצה. נעיר שמשתמשים באותו סימון גם לקבוצות עם אינסוף איברים.

למעלה השתמשנו במושג שוויון של קבוצות מבלי להגדיר את זה פורמלית, נרצה לעשות זאת עכשיו באמצעות מושג ההכלה.

הגדרה 1.4 תהיינה A, B קבוצות. נאמר כי הקבוצה B מכילה את הקבוצה A אם כל (הסימון הלוגי הוא $\forall$) איבר השייך לA גם שייך לB. בכתיב מתמטי ניתן לכתוב

$$\forall x \in A \Rightarrow x \in B.$$

אם A מוכלת בB נכתוב $A \subseteq B$. ניתן גם לומר במקרה זה כי A היא תת קבוצה של A.

דוגמא 1.5 1. $\{x, y\} \subseteq \{x, y, z\}$.

2. קבוצת הזוגיים המוגדרת ע"י $\{2t : t \in \mathbb{Z}\}$ מוכלת בקבוצת המספרים השלמים.

3.

$$\mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q}.$$

הגדרה 1.6 תהיינה A, B קבוצות. נאמר כי הן קבוצות שוות ונסמן $A = B$ אם יש להן בדיוק אותם איברים. במילים אחרות $A = B$ אם A מוכלת בB וגם B מוכלת בA.

הגדרה 1.7 קבוצה בה אין אף איבר נקראת הקבוצה הריקה ותסומן ב $\{\}$ או ב $\emptyset$.

דוגמא 1.8

$$\{x \in \mathbb{Q} : x^2 = -1\} = \emptyset.$$

כעת, נרצה להגדיר את פעולות החיתוך והאיחוד בין שתי קבוצות.

הגדרה 1.9 תהיינה A, B קבוצות. החיתוך בין קבוצות אלו שיסומן ב $A \cap B$ הוא קבוצת כל האיברים ששייכים גם לA וגם לB. בכתיב מתמטי ניתן לרשום

$$A \cap B = \{x : x \in A \text{ וגם } x \in B\}.$$

דוגמא 1.10 החיתוך בין קבוצת המספרים הזוגיים וקבוצת כל המספרים המתחלקים ב3 הוא קבוצת כל המספרים המתחלקים ב6. כלומר

$$\{2t : t \in \mathbb{Z}\} \cap \{3t : t \in \mathbb{Z}\} = \{6t : t \in \mathbb{Z}\}$$

הערה 1.11 אם $A \cap B = \emptyset$ נאמר כי הקבוצות A, B הן זרות.

בצורה דומה מגדירים איחוד בין קבוצות

הגדרה 1.12 תהיינה A, B קבוצות. האיחוד ביניהן מוגדר להיות קבוצת כל האיברים השייכים לA או לB (זכרו שזה כולל את האיברים שנמצאים בשתי הקבוצות). בכתיב מתמטי ניתן לכתוב

$$A \cap B = \{x : x \in A \text{ או } x \in B\}.$$

הערה 1.13 בהינתן קבוצות A, B מתקיים

1. $A \cap B \subseteq A, \quad A \cap B \subseteq B$.

2. $A \subseteq A \cup B, \quad B \subseteq A \cup B$.

כמובן שניתן גם לדבר על איחוד או חיתוך של מספר גדול יותר של קבוצות, או אפילו אינסוף קבוצות. מושג נוסף שיהיה שימושי

הגדרה 1.14 תהיינה A, B קבוצות. אזי

$$A \setminus B = \{a \in A : a \notin B\}.$$

דוגמא 1.15 תהיינה $A = \{a, b, c\}, \quad B = \{c, d, e\}$. אזי $A \setminus B = \{a, b\}$.

מכפלה קרטזית: ראינו כי בהנתן שני איברים a, b הקבוצות $\{a, b\} = \{b, a\}$ כלומר אין חשיבות לסדר. עם זאת במקרים רבים יש חשיבות לסדר, כמו בסדרה או בווקטור יש חשיבות למיקום של כל איבר. נתאר מושג הנותן חשיבות לסדר האיברים.
סימון: אם a, b איברים אזי (a, b) ייקרא זוג סדור, כאשר מתקיים שוויון $(a, b) = (c, d)$ רק אם $a = c$ וגם $b = d$.

הגדרה 1.16 תהיינה A, B קבוצות. המכפלה הקרטזית $A \times B$ של A עם B היא אוסף כל הזוגות הסדורים (a, b) כך ש $a \in A, b \in B$. כלומר

$$A \times B = \{(a, b) : a \in A \text{ וגם } b \in B\}.$$

דוגמא 1.17 $A = \{1, 2, 3\}$, $B = \{a, b\}$. אזי

$$A \times B = \{(1, a), (2, a), (3, a), (1, b), (2, b), (3, b)\}.$$

בדומה להגדרת זוג סדור ניתן להגדיר שלישיה סדורה רביעיה סדורה ובאופן כללי עבור מספר טבעי n מגדירים את הn-יה הסדורה $(a_1, a_2, \ldots, a_n)$.

הגדרה 1.18 עבור $A_1, A_2, \ldots, A_n$ קבוצות,

$$A_1 \times A_2 \times \ldots \times A_n = \{(a_1, a_2, \ldots, a_n) : a_i \in A_i, \forall 1 \leq i \leq n\}.$$

סימון: המכפלה הקרטזית של קבוצה A עם עצמה n פעמים תסומן בA^n.

1.1.3 הוכחות מתמטיות

הוכחה מתמטית היא סדרה סופית של טענות הנובעות זו מזו בעזרת כללי הלוגיקה, תוך שימוש בהגדרות, באקסיומות, ובידע קודם שהוכח קודם לכן, המראה שטענה מסוימת היא נכונה. הוכחה לכך שטענה מסוימת איננה נכונה נקראת הפרכה של הטענה.

בפרק זה נדון בכמה כללים הקשורים להוכחות מתמטיות מסוגים מסוימים ובנוסף נתאר שתי דרכי הוכחה נפוצות, הוכחה על דרך השלילה והוכחה באינדוקציה.

למרות שיש סוגים רבים של טענות מתמטיות, חלק גדול מאוד מהן ניתן לחלק לשני סוגיים מרכזיים.

1. טענות מהצורה לכל x מתקיים " ".

2. קיים x כך ש" ".

נדון קודם בגישה להוכחה או להפרכה של הסוג הראשון.

1. תהיי α טענה מהצורה לכל x מתקיים " ". על מנת להוכיח את α יש להשתמש בטיעון כללי ולא לתת דוגמה. למשל אם α היא הטענה: לכל $x \in \mathbb{R}$ קיים $y \in \mathbb{R}$ כך ש $x - y \in \mathbb{Z}$ ניתן להוכיח את α על ידי כך שלכל x ממשי אפשר לבחור את y להיות שווה ל $x - 1$ ואז החיסור $y - x = 1 \in \mathbb{Z}$. חשוב לשים לב כי לא עשינו שום הגבלה על x ולכן אכן הוכחנו את הטענה לכל $x \in \mathbb{R}$.

   כדי להפריך טענה מסוג לכל x מתקיים " " מספיקה דוגמה אחת עבורה הטענה לא מתקיימת, דוגמה כזו תקרא דוגמה נגדית. למשל כדי להפריך את הטענה לכל $x \in \mathbb{Z}$ קיים $y \in \mathbb{Z}$ כך ש $y^2 = x$ מספיק להראות כי עבור $x = 2$ זה לא מתקיים. אכן ישנם רק שני מספרים ממשים $y = \pm\sqrt{2}$ שמקיימים $y^2 = x$. מכיוון שאף אחד מהם לא שלם זה מפריך את הטענה.

2. תהיי β טענה מהסוג קיים x כך ש" ". על מנת להוכיח את β מספיק להציג x שמקיים את התכונה המוצגת ב"כך ש" ואז להוכיח כי אכן הוא מקיים את התכונה. למעשה במקרה זה ההוכחה היא ע"י דוגמה. למשל אם β היא הטענה: קיימים $x, y \in \mathbb{Z}$ כך ש $x^y = y^x$ ניתן להוכיח על ידי הבחירה $x = 2, y = 4$ ואז אכן מתקיים כי $2^4 = 4^2$.

לעומת זאת, על מנת להפריך טענה מסוג זה יש לתת טיעון כללי שמראה כי דוגמה כז אינה קיימת.

למשל נרצה להפריך את הטענה: קיימים ממשיים חיובים כך ש

$$\sqrt{xy} > \frac{x+y}{2}.$$

נפריך את הטענה ע"י שנראה כי לכל ממשיים חיוביים מתקיים

$$x + y \geq 2\sqrt{xy}.$$

יהיו x, y ממשיים חיובים, אזי מתקיים כי

$$(x-y)^2 = x^2 + y^2 - 2xy \geq 0 \Rightarrow x^2 + y^2 + 2xy = (x+y)^2 \geq 4xy \Rightarrow x + y \geq 2\sqrt{xy}.$$

קיבלנו בצד ימין את האי שוויון המבוקש ולכן הפרכנו את הטענה.

לכל פסוק ניתן להתאים את פסוק השלילה שלו, למשל שלילת הפסוק "יורד גשם" היא "לא יורד גשם", שלילת הפסוק "יש אינסוף מספרים שלמים" היא "יש מספר סופי של מספרים שלמים". כמובן שאם פסוק α הוא אמת, אז שלילתו היא שקר וגם ההיפך נכון, כלומר אם השלילה היא אמת אז הפסוק α הוא שקר. ניתן להשתמש בלוגיקה זו כדי להוכיח טענות מתמטיות, לדוגמה במקום להוכיח כי טענה כלשהי תמיד נכונה אפשר להוכיח כי שלילתה בהכרח איננה נכונה. או במקום להוכיח כי טענה α גוררת את הטענה β ניתן להוכיח את הטענה השקולה כי שלילת β גוררת את שלילת α. לצורת הוכחה זו קוראים הוכחה על דרך השלילה. הדוגמה הידועה הראשונה בהיסטוריה להוכחה על דרך השלילה היא ההוכחה של אוקלידס לכך שיש אינסוף מספרים ראשונים. הנה מתווה ההוכחה, כאשר נשתמש בהוכחה בכך שכל מספר טבעי הגדול מ1 מתחלק בהכרח במספר ראשוני.

טענה 1.19 קיימים אינסוף מספרים ראשוניים.

הוכחה: נניח בשלילה כי קיים מספר סופי m של מספרים ראשונים. נסמנם ב $p_1, p_2, \ldots, p_m$. כעת נגדיר מספר חדש k המתקבל על ידי מכפלת כל המספרים הראשוניים ואז הוספת 1, כלומר

$$k = (p_1 \cdot p_2 \cdot p_3 \cdot \ldots \cdot p_m) + 1.$$

כעת, k לא מתחלק באף אחד מהראשוניים $p_1, p_2, \ldots, p_m$ כי החלוקה של k בכל אחד מהם תיתן שארית 1 אבל מכיוון ש k הוא מספר טבעי גדול מ1 הוא חייב להתחלק בראשוני כלשהו ולכן הגענו למסקנה כי קיים מספר ראשוני חוץ מהראשוניים $p_1, p_2, \ldots, p_m$ וזוהי סתירה לוגית להנחה שלנו כי יש מספר סופי של ראשוניים. מכאן אנו מסיקים שיש אינסוף ראשוניים. □

דוגמה נוספת להוכחה על דרך השלילה היא הוכחה קלאסית בסדרות, שמראים כי כל סדרה מתכנסת היא בהכרח חסומה על ידי כך שמראים שאם סדרה איננה חסומה אז היא בהכרח איננה מתכנסת.

סוג ההוכחה האחרון שנגע בו בפרק זה היא הוכחה באינדוקציה. טכניקת ההוכחה באינדוקציה מסתמכת על אקסיומת הסדר הטוב שטוענת שבכל תת קבוצה של המספרים הטבעיים קיים איבר הכי קטן.

כעת נניח כי אנו רוצים להוכיח כי טענה מסוימת P מתקיימת לכל טבעי n (אולי החל ממקום כלשהו).

דוגמא 1.20 נרצה להוכיח כי לכל טבעי n מתקיים

$$1 + 2 + \ldots + n = \frac{n(n+1)}{2}.$$

למעשה יש כאן אינסוף טענות מתמטיות

$$1 = \frac{1 \cdot (1+1)}{1}, \quad \frac{2(2+1)}{2}, \ldots$$

נסתכל בקבוצת כל הטבעיים עבורם P לא נכונה. ע"פ אקסימות הסדר הטוב קיים בקבוצה זו איבר מינימלי.

על כן, אם הטענה P נכונה עבור איזשהו $k \in \mathbb{N}$ (נסמן זאת ב $P(k)$) ומתקיים לכל $r \geq k$ כי $P(r) \Rightarrow P(r+1)$ אזי הטענה P נכונה לכל $r \geq k$. למעשה יש כאן שלושה שלבים. שלב הבדיקה (מציאת k עבורו P מתקיימת), שלב ההנחה (בו מניחים כי $P(r)$ נכונה) ושלב הצעד בו מראים כי $P(r) \Rightarrow P(r+1)$.

נחזור לדוגמה. נרצה להוכיח כי לכל טבעי n מתקיים

$$1+2+\ldots+n=\frac{n(n+1)}{2}.$$

בדיקה: הטענה מתקיימת עבור $n=1$.

הנחה: נניח כי הטענה מתקיימת ל $r\in\mathbb{N}$, כלומר

$$1+2+\ldots+r=\frac{r(r+1)}{2}.$$

צעד: נוכיח כי הטענה מתקיימת עבור $r+1$ על ידי שימוש בהנחה.

$$1+\ldots+r+(r+1)=\frac{r(r+1)}{2}+(r+1)=\frac{r(r+1)+2(r+1)}{2}=\frac{(r+1)(r+2)}{2}.$$

קיבלנו כי הטענה מתקיימת עבור $n=r+1$ ולכן הטענה מתקיימת לכל מספר טבעי.

הערה 1.21 את ההנחה כי הטענה נכונה עבור טבעי r ניתן להחליף בהנחה כי ההטענה נכונה לכל טבעי הקטן או שווה לr.

דוגמא 1.22 נוכיח באינדוקציה כי כל טבעי הגדול מ1 ניתן לכתיבה כמכפלה של מספרים ראשוניים. עבור המספרים $2,3$ הטענה ברורה כי הם ראשוניים. נניח כי הטענה נכונה לכל טבעי הקטן או שווה לr, כלומר כל מספר טבעי הקטן או שווה לr וגדול מ1 ניתן לכתיבה כמכפלה של ראשוניים. נוכיח כי הטענה נכונה גם עבור $r+1$. ישנן שתי אפשרויות. או ש $r+1$ הוא מספר ראשוני ואז הטענה ברורה. או ש $r+1$ הוא לא ראשוני. אבל אז קיימים שני טבעים $1<a,b<r+1$ כך ש $r+1=ab$. על פי ההנחה ניתן לכתוב את a,b כמכפלה של ראשוניים ולכן מהצבה ב $r+1=ab$ גם את $r+1$ ניתן לכתוב כמכפלה של ראשוניים. הוכחנו כי כך טבעי הגדול מ1 ניתן לכתיבה כמכפלה של ראשוניים.

1.2 יחסי שקילות ופונקציות

יחסי שקילות ופונקציות הם מושגים המופיעים כמעט בכל תחומי המתמטיקה. שני מושגים אלו הם מקרים פרטיים של מושג היחס מקבוצה A לקבוצה B.

1.2.1 יחסי שקילות

הגדרה 1.23 בהנתן שתי קבוצות A, B, לתת קבוצה R של המכפלה הקרטזית ביניהן $R \subseteq A \times B$ קוראים יחס מA לB.

נעסוק תחילה ביחסים דו־מקומיים, כלומר בתתי קבוצות של $A \times A$.

דוגמא 1.24 תהיי A קבוצת כל התלמידים בכיתה. נגדיר יחס, $R \subseteq A \times A$ על ידי הכלל, עבור $x, y \in A$ שני תלמידים $(x, y) \in R$ אם x, y יושבים באותה שורה.

נשים לב כי בדוגמה לעיל מתקיימות התכונות הבאות:

1. לכל $x \in A$ מתקיים $(x, x) \in R$ כי כל תלמיד יושב באותה שורה שהוא עצמו יושב בה.
2. אם $(x, y) \in R$ אז גם $(y, x) \in R$.
3. אם עבור x, y, z שלושה תלמידים מתקיים כי $(x, y) \in R$ וגם $(y, z) \in R$ אזי $(x, z) \in R$.

ליחסים דו מקומיים המקיימים תכונות אלו יש שמות מיוחדים

הגדרה 1.25 תהיי A קבוצה ויהי R יחס על A. אזי

1. אם לכל $x \in A$ מתקיים כי $(x, x) \in R$ אזי R ייקרא יחס רפלקסיבי.
2. אם לכל $x, y \in A$ מתקיים כי $(x, y) \in R$ גורר כי גם $(y, x) \in R$ אזי R ייקרא יחס סימטרי.
3. אם לכל $x, y, z \in A$ כך ש $(x, y) \in R$ וגם $(y, z) \in R$ נובע כי גם $(x, z) \in R$ נאמר כי R הוא יחס טרנזיטיבי.

דוגמא 1.26 תהיי $A = \mathbb{Z}$ קבוצת השלמים. נגדיר יחס, $R \subseteq A \times A$ על ידי הכלל $(x, y) \in R$ אם $x - y$ הוא מספר זוגי. קל לבדוק כי R הוא יחס רפלקסיבי סימטרי וטרנזיטיבי.

נשים לב כי בדוגמה לעיל היחס R מחלק למעשה את קבוצת השלמים לשתי קבוצות־ הזוגיים והאי זוגיים. תכונה זו היא תכונה המאפיינת יחס שקילות.

הגדרה 1.27 יחס דו מקומי ייקרא יחס שקילות אם הוא רפלקסיבי, סימטרי וטרנזיטיבי.

כאשר נתון יחס שקילות על קבוצה X מקובל לסמנו ב $\sim$ ובמקום לסמן $(x, y) \in \sim$ מקובל לכתוב $x \sim y$. הדוגמה הבאה מכלילה את דוגמה 1.26.

דוגמא 1.28 תהיי $A = \mathbb{Z}$ קבוצת השלמים ויהי n מספר טבעי. נגדיר יחס על A על ידי הכלל $x \sim y$ אם $x - y$ מתחלק ללא שארית בn. קל לבדוק כי $\sim$ הוא אכן יחס שקילות. הפעם היחס מחלק את השלמים לn מחלקות שונות.

נרצה להגדיר פורמלית מהן מחלקות אלו

הגדרה 1.29 תהיי X קבוצה, יהי $x \in X$ ויהי $\sim$ יחס על X. מחלקת השקילות של x מוגדרת להיות

$$[x]_\sim = [x] = \{y \in X : x \sim y\}. \tag{1}$$

למשל בדוגמה 1.28 מחלקת השקילות של 2 הם כל המספרים השלמים שנותנים שארית 2 בחלוקה בn. נטען ללא להוכיח כי יחס שקילות על קבוצה למעשה מחלק את הקבוצה כך שכל איבר בקבוצה שייך בדיוק למחלקת שקילות אחת. כלומר הקבוצה היא למעשה איחוד זר של מחלקות השקילות.

1.2.2 פונקציות

מקרה פרטי מאוד מוכר של יחסים הוא פונקציה.

הגדרה 1.30 יחס f מקבוצה A לקבוצה B ייקרא פונקציה אם לכל $x \in A$ קיים ויחיד $y \in B$ כך ש $(x, y) \in f$. במילים אחרות, פונקציה היא התאמה מA לB הלוקחת כל איבר בA לאיבר יחיד בB.

דוגמא 1.31 תהיי $A = \{a, b\}$ ותהיי $B = \{1, 2, 3\}$ אזי

1. $R_1 = \{(a, 1)(a, 2), (b, 3)\}$ הוא לא פונקציה מA לB כי ישנם שני איברים בB המתאימים לa.
2. $R_2 = \{(a, 1)\}$ הוא לא פונקציה מA לB כי לא קיים איבר בB המתאים לb.
3. $R_3 = \{(a, 1), (b, 3)\}$ כן פונקציה מA לB.

חשוב לשים לב כי A, B ממלאים תפקידים שונים בהגדרת הפונקציה.

הגדרה 1.32 בהנתן פונקציה מקבוצה A לקבוצה B, A נקרא תחום הפונקציה ו B נקרא טווח הפונקציה.

סימון: בהנתן פונקציה $f \in A \times B$ מקובל לסמן $f : A \to B$. בנוסף אם $(x, y) \in f$ מקובל לסמן $f(x) = y$. חשוב לציין כי סימון זה מוגדר היטב מכיוון שקיים y יחיד המתאים לx.

הערה 1.33 שתי פונקציות f, g הן שוות אם יש להן את אותו תחום, אותו טווח ולכל x ששייך לתחום מתקיים $f(x) = g(x)$.

הגדרה 1.34 בהנתן פונקציה $f \in A \times B$, אם $f(x) = y$ נאמר כי x הוא מקור של y, וy היא תמונה של x.

הערה 1.35 בהנתן פונקציה $f : A \to B$ לכל $x \in A$ קיים $y \in B$ יחיד כך ש $f(x) = y$, אבל ייתכן שישנו איבר נוסף $z \in X$ (או הרבה איברים נוספים) כך ש $f(z) = y$. בנוסף ייתכן כי ישנם איברים $w \in B$ כך שלכל $x \in A$ $f(x) \neq w$. במילים אחרות, ייתכן שיש איברים בB שהם תמונות של איברים שונים בA ומאידך ייתכן שישנם איברים בB שאינם תמונה של אף איבר בA.

בהינתן פונקציה $f : A \to B$ נרצה לתת שם לקבוצת כל האיברים ב$y \in B$ שעבורם קיים $x \in A$ כך ש $f(x) = y$.

הגדרה 1.36 תהיי $f : A \to B$ פונקציה. התמונה של f מוגדרת להיות

$$Im(f) = \{f(x) : x \in A\} = \{y \in B : y = f(x) \text{ כך ש } x \in A \text{ קיים}\}$$

נרצה כעת להגדיר שני סוגים מיוחדים של פונקציות, המתקשרות לשני המקרים המתוארים בהערה 1.35.

הגדרה 1.37 תהיי $f : A \to B$ פונקציה.

1. אם עבור $x_1, x_2 \in A$ נובע כי

$$x_1 \neq x_2 \Rightarrow f(x_1) \neq f(x_2).$$

נאמר כי הפונקציה f היא חד חד ערכית, או בקיצור חח"ע. במילים אחרות, עבור פונקציה חח"ע, למקורות שונים יש תמונות שונות.

2. נאמר כי f היא פונקציה על אם $Im(f) = B$. במילים אחרות, פונקציה היא על אם לכל איבר בטווח יש מקור.

הערה 1.38 בדרך כלל כדי להראות כי פונקציה $f : A \to B$ היא חח"ע אנחנו נניח כי עבור איברים כלשהם $x_1, x_2 \in A$ מתקיים $f(x_1) = f(x_2)$ ונוכיח כי בהכרח $x_1 = x_2$.

דוגמא 1.39 נסמן ב $\mathbb{R}$ את קבוצת המספרים הממשיים וב $\mathbb{R}^+$ את קבוצת הממשיים האי שליליים, כלומר גדולים או שווים לאפס, ונסתכל על הפונקציה המוגדרת ע"י $f(x) = x^2$ במקרים הבאים.

1. $f : \mathbb{R} \to \mathbb{R}$ זוהי פונקציה שאינה חח"ע (כי למשל $f(-2) = f(2) = 4$)וגם אינה על, כי למספרים השליליים אין מקורות.

2. $f : \mathbb{R}^+ \to \mathbb{R}$ זוהי פונקציה חח"ע אבל לא על.

3. $f : \mathbb{R} \to \mathbb{R}^+$ זוהי פונקציה שאינה חח"ע, אבל היא כן על.

4. $f : \mathbb{R}^+ \to \mathbb{R}^+$ זוהי פונקציה חח"ע ועל.

אנחנו לומדים מהדוגמה לעיל כי מה שקובע האם פונקציה תהיה חח"ע או על, זה לא רק הכלל שמגדיר את הפונקציה אלא גם מי הם התחום והטווח.

הגדרה 1.40 תהיי A קבוצה. פונקציה $f : A \to A$ המקיימת $f(x) = x$ לכל $x \in A$ נקראת פונקצית הזהות על A ותסומן ב Id_A.

לעיתים נרצה להפעיל מספר פונקציות אחת לאחר השניה.

הגדרה 1.41 תהיינה $f : X \to Y, \quad g : Y \to Z$ פונקציות. נגדיר את הרכבת הפונקציות להיות $g \circ f : X \to Z$ על ידי הכלל $g \circ f(x) = g(f(x))$ לכל $x \in X$.

נשים לב שכדי שהרכבת הפונקציות $g \circ f$ תהיה מוגדרת צריך להתקיים כי התמונה של f מוכלת בתחום של g.

הערה 1.42 לכל פונקציה $f : A \to B$ מתקיים

$$f \circ Id_A = f = Id_B \circ f.$$

כלומר פונקצית הזהות היא "איבר אדיש" ביחס להרכבה.

נחזור לרגע לסעיף 4 של דוגמה 1.39 לפונקציה $f : \mathbb{R}^+ \to \mathbb{R}^+$ המוגדרת על ידי הכלל $f(x) = x^2$. נשים לב כי אם נבצע הרכבה של f עם הפונקציה $g : \mathbb{R}^+ \to \mathbb{R}^+$ המוגדרת על ידי $g(x) = \sqrt{x}$ נקבל את פונקצית הזהות, כלומר $f \circ g = g \circ f = Id_{\mathbb{R}}$. זה מוביל אותנו להגדרה של פונקציה הפיכה.

הגדרה 1.43 פונקציה $f : A \to B$ תקרא הפיכה אם קיימת פונקציה $g : B \to A$ כך ש

$$g \circ f = Id_A, \quad f \circ g = Id_B.$$

הפונקציה g תקרא הופכית לf.

נרצה להראות כי אם לפונקציה f קיימת פונקציה הופכית, אזי היא יחידה. לשם כך נטען מבלי להוכיח כי הרכבת פונקציות היא אסוציטיבית. כלומר

טענה 1.44 תהיינה $f_3 : X_3 \to X_4 \;\; f_2 : X_2 \to X_3 \;\; f_1 : X_1 \to X_2$ פונקציות. אזי מתקיים

$$(f_3 \circ f_2) \circ f_1 = f_3 \circ (f_2 \circ f_1).$$

טענה 1.45 תהי $f : A \to B$ פונקציה הפיכה. אזי קיימת לה פונקציה הופכית יחידה.

הוכחה: נניח הפונקציות $g_1, g_2 : B \to A$ הופכיות לf. נראה כי בהכרח $g_1 = g_2$. על פי הערה 1.42 וטענה 1.44 מתקיים לכל $x \in B$. כי

$$g_1(x) = (g_1 \circ Id_B)(x) = (g_1 \circ (f \circ g_2))(x) = ((g_1 \circ f) \circ g_2)(x) = (Id_A \circ g_2)(x) = g_2(x).$$

לכן קיבלנו כי לכל $x \in B$ מתקיים $g_1(x) = g_2(x)$, כלומר $g_1 = g_2$. □

מכיוון שפונקציה הופכית לפונקציה f היא יחידה ניתן לתת לה סימון מיוחד.

סימון: בהנתן פונקציה הפיכה f נסמן את ההופכית לה ב f^{-1}.

נחזור שוב לדוגמה 1.39. ראינו כי לפונקציה בסעיף הרביעי יש פונקציה הפכית. אפשר לבדוק כי כל הפונקציות האחרות בדוגמה זו אינן הפיכות. כמו כן הפונקציה בסעיף 4 היא היחידה מבין הפונקציות בדוגמה זו שהיא גם חח"ע וגם על. מסתבר שזה אינו מקרה.

משפט 1.46 פונקציה $f : A \to B$ היא הפיכה אם ורק אם היא גם חח"ע וגם על.

הוכחה: כיוון ראשון: נניח כי f הפיכה. נוכיח קודם כל כי היא חח"ע. יהיו $x_1, x_2 \in A$ כך ש $f(x_1) = f(x_2)$ אזי

$$x_1 = f^{-1} \circ f(x_1) = f^{-1} \circ f(x_2) = x_2.$$

ולכן f חח"ע. כעת נראה כי f היא על. יהי $y \in B$. נסמן $x = f^{-1}(y)$. אזי מתקיים

$$f(x) = f(f^{-1}(y)) = f \circ f^{-1}(y) = y.$$

כלומר לכל $y \in B$ קיים מקור בA ולכן f היא על.

כיוון שני: נניח כי f היא חח"ע ועל ונוכיח כי היא הפיכה על ידי מציאת פונקציה $g : B \to A$ הופכית לA. נגדיר את g באופן הבא:

יהי $y \in B$. מכיוון שf היא על, קיים $x \in A$ כך ש $f(x) = y$. מחח"ע של f כי x זה הוא מקור יחיד לy ולכן ניתן להגדיר לכל $y \in B$ את $g(y) = x$. זוהי פונקציה כי כל איבר בB נשלח לאיבר יחיד בA. וכעת רק נותר לראות כי אכן לכל $x \in A$ ולכל $y \in B$ מתקיים

$$f \circ g(y) = f(x) = y, \quad g \circ f(x) = g(y) = x.$$

לכן g פונקציה הופכית לf.

□

נסיים את הדיון בפונקציות עם טענה פשוטה יחסית ומספר מסקנות מידיות ממנה ללא הוכחה.

טענה 1.47 תהי A קבוצה סופית ותהי $f : A \to B$ פונקציה. אזי $|Im(f)| \leq |A|$ ושוויון מתקיים אם ורק אם f חח"ע.

מוכיחים זאת באינדוקציה על הגודל של הקבוצה A.

מסקנה 1.48 תהיי A קבוצה סופית ותהיי $f : A \to B$ פונקציה חח"ע. אזי $|A| \leq |B|$.

מסקנה 1.49 תהיי B קבוצה סופית ותהיי $f : A \to B$ פונקציה על. אזי $|A| \geq |B|$.

מסקנה 1.50 תהיינה A, B קבוצות סופיות. אם קיימת פונקציה חח"ע ועל מA לB אזי $|A| = |B|$.

הערה 1.51 עבור קבוצות אינסופיות ככה מגדירים קבוצות בעלות אותו גודל, אם קיימת פונקציה חח"ע ועל ומאחת לשניה.

מסקנה 1.52 תהיינה A וB קבוצות סופיות בעלות אותו גודל ותהיי $f : A \to B$ פונקציה. אזי f היא חח"ע אם ורק אם היא על.

לעיתים בהנתן קבוצות, יש אפשרות לבצע פעולות בין איברי הקבוצות, למשל חיבור של מספרים שלמים, או כפל של מספר רציונלי במספר שלם. נרצה לתת הגדרה פורמלית.

הגדרה 1.53 בהנתן שתי קבוצות A, B, לפונקציה $f : B \times A \to A$ קוראים פעולה על A. לפונקציה $* : A \times A \to A$ קוראים פעולה בינארית על A.

בהנתן פעולה $*$ על קבוצה A, במקום $*(a_1, a_2)$ נסמן $a_1 * a_2$.

1.3 חבורות

אמנם אפשר ללמוד אלגברה ליניארית גם בלי להכיר את המושג חבורה, אבל בהחלט היכרות עם המושג יכולה לעזור להבין טוב יותר חלק מהתיאוריה שנדון בה בפרקים בהמשך.

הגדרה 1.54 תהיי G קבוצה עם פעולה בינארית $*$ עליה. נאמר כי G היא חבורה (ביחס לפעולה $*$) אם מתקיימות התכונות הבאות:

1. מתקיימת אסוציטיביות, כלומר לכל $g_1, g_2, g_3 \in G$ מתקיים $(g_1 * g_2) * g_3 = g_1 * (g_2 * g_3)$.
2. קיים איבר $e \in G$ כך שמתקיים $e * g = g = g * e$ לכל $g \in G$. e נקרא האיבר האדיש או האיבר הניטרלי של החבורה G.

3. לכל איבר $g \in G$ קיים איבר $h \in G$ כך ש $g * h = e = h * g$. האיברים g, h ייקראו הופכים זה לזה.

דוגמא 1.55 קבוצת השלמים ביחס לפעולת החיבור היא חבורה אותה נסמן ב $(\mathbb{Z}, +)$. אכן

1. חיבור של שני מספרים שלמים נותן מספר שלם לכן חיבור היא פעולה בינארית על השלמים.
2. חיבור מספרים שלמים היא פעולה אסוציטיבית.
3. המספר אפס הוא האיבר האדיש ביחס לחיבור.
4. ההופכי של $a \in \mathbb{Z}$ הוא $-a \in \mathbb{Z}$.

הערה 1.56 תהיי G חבורה. אם הפעולה ביחס אליה G חבורה היא ברורה אז לכל שני איברים $g, h \in G$ נסמן gh במקום $g * h$.

דוגמא 1.57 קבוצת הרציונלים ללא האפס $\mathbb{Q} \setminus \{0\}$ ביחס לפעולת הכפל היא חבורה שתסומן ב $(\mathbb{Q} \setminus \{0\}, \cdot)$. אכן

1. כפל של שני מספרים רציונלים נותן מספר רציונלי ולכן כפל היא פעולה בינארית על המספרים הרציונלים.
2. המספר 1 הוא האיבר האדיש ביחס לכפל.
3. כפל מספרים היא פעולה אסוציטיבית.
4. ההופכי של $0 \neq \frac{n}{m} \in \mathbb{Q}$ הוא $\frac{m}{n} \in \mathbb{Q}$.

ההערה הבאה קלה מאוד להוכחה ונשארת כתרגיל לקורא

הערה 1.58 בהנתן חבורה, האיבר האדיש הוא יחיד ולכל איבר קיים הופכי יחיד.

הגדרה 1.59 חבורה G תקרא אבלית או חילופית אם לכל $g, h \in G$ מתקיים כי $gh = hg$.

כל הדוגמאות שראינו עד עכשיו היו של חבורות אבליות, אך קיימות חבורות שאינן אבליות.

דוגמא 1.60 נסמן בG את חבורת הפונקציות ההפיכות $f : \mathbb{R} \to \mathbb{R}$ ביחס לפעולת ההרכבה. זוהי אכן חבורה כי הרכבת פונקציות הפיכות נותנת פונקציה הפיכה, האיבר האדיש הוא פונקצית הזהות על $\mathbb{R}$, הרכבת פונקציות היא פעולה אסוציטיבית וכמובן שלכל פונקציה הפיכה יש הופכית. אבל זוהי לא חבורה אבלית. ניתח למשל את $f_1(x) = x + 1$ ואת $f_2(x) = x^3$ (בדקו שהן אכן הפיכות). אזי

$$f_2 \circ f_1(x) = (x + 1)^3 \neq x^3 + 1 = f_1 \circ f_2(x).$$

נחזור כעת ליחס שקילות שהגדרנו קודם לכן על קבוצת השלמים. יהי $n \in \mathbb{N}$. נגדיר על השלמים יחס שקילות, $x \sim y$ אם ורק אם $x - y$ מתחלק בלי שארית ב n. אזי קיימות בדיוק n מחלקות שקילות, אותן נסמן ב

$$\{[0], [1], \ldots, [n-1]\}.$$

נרצה להראות כי למעשה יש על קבוצה זאת מבנה טבעי של חבורה אבלית.

הגדרה 1.61 יהיו $a, b \in \mathbb{Z}$ כך ש $a \sim b$. אזי נאמר כי a, b קונגרואנטיים זה לזה ונסמן

$$a \equiv b \pmod{n}.$$

נשים לב כי לכל $a \in \mathbb{Z}$ קיים ויחיד $0 \leq r \leq n - 1$ כך ש $a \equiv r \pmod{n}$. פה, r הוא השארית של a בחלוקה ב n. כלומר $a \in [r]$.

נרצה להגדיר פעולות חיבור וכפל על מחלקות השקילות לעיל. באופן כללי כדי להגדיר פונקציות או פעולות על מחלקות שקילות יש לבדוק כי הגדרת הפעולה לא תלויה באיבר אותו בוחרים מתוך מחלקת השקילות. לשם כך נזדקק למשפט הבא:

משפט 1.62 יהיו $a_1, a_2, b_1, b_2 \in \mathbb{Z}$ כך ש

$$a_1 \equiv a_2 \pmod{n}, \quad b_1 \equiv b_2 \pmod{n}.$$

אזי

1. $a_1 + b_1 \equiv a_2 + b_2 \pmod{n}$.
2. $a_1 \cdot b_1 \equiv a_2 \cdot b_2 \pmod{n}$.

הוכחה: מכיוון ש $a_1 \equiv a_2 (\mathrm{mod}\ n)$ ו $b_1 \equiv b_2 (\mathrm{mod}\ n)$ נובע כי n מחלק את $a_1 - a_2$ וגם את $b_1 - b_2$.

1. לפי ההערה בתחילת ההוכחה, n מחלק את הסכום

$$a_1 - a_2 + b_1 - b_2 = (a_1 + b_1) - (a_2 + b_2).$$

לפי ההגדרה, נובע כי $a_1 + b_1 \equiv a_2 + b_2 (\mathrm{mod}\ n)$.

2. לפי ההערה בתחילת ההוכחה קיימים מספרים שלמים $r, s \in \mathbb{Z}$ כך ש $a_1 - a_2 = rn$ ו $b_1 - b_2 = sn$. נובע ש

$$\begin{aligned} a_1 b_1 &= (a_2 + rn)(b_2 + sn) \\ &= a_2 b_2 + n(rb_2 + a_2 s + rsn) \end{aligned}$$

לכן $a_1 b_1 - a_2 b_2$ כפולה של n, כלומר $a_1 b_1 \equiv a_2 b_2 \pmod{n}$.

□

כעת אנחנו יכולים להגדיר פעולות חיבור וכפל על מחלקות השקילות

$$\{[0], [1], \ldots, [n-1]\}.$$

על ידי $[r_1] + [r_2] = [r_3]$ כאשר r_3 הוא השארית של החלוקה של $r_1 + r_2$ ב n. ובאופן דומה $[r_1] \cdot [r_2] = [r_4]$ כאשר r_4 הוא השארית של החלוקה של $r_1 r_2$ בחלוקה ב n. על פי המשפט לעיל הפעולות הללו לא תלויות בנציגים שנבחר מתוך מחלקות השקילות השונות.

הגדרה 1.63 הקבוצה

$$\{[0], [1], \ldots, [n-1]\}.$$

ביחס לפעולת החיבור והכפל שהוגדרו לעיל תסומן ב $\mathbb{Z}_n$.

טענה 1.64 הקבוצה $\mathbb{Z}_n$ היא חבורה ביחס לפעולת החיבור המוגדרת עליה.

הוכחה: על פי משפט 1.62 פעולת החיבור (והכפל) על $\mathbb{Z}_n$ מוגדרת היטב וברור כי פעולה זו היא בינארית כי תוצאת החיבור נותנת איבר ב $\mathbb{Z}_n$.

האיבר $[0]$ אדיש ביחס לחיבור. אסוציטיביות הפעולה נרכשת מאסוציטיביות החיבור בשלמים ולבסוף, לכל איבר $[r] \in \mathbb{Z}_n$ יש איבר הופכי חיבורי (נגדי) $[n-r] \in \mathbb{Z}_n$.

□

קל לבדוק כי גם פעולת הכפל ב $\mathbb{Z}_n$ היא בינארית, אסוציטיבית ויש איבר אדיש ביחס לכפל $[1]$. אבל, ברור כי $\mathbb{Z}_n$ אינה חבורה ביחס לכפל כי ל $[0]$ אין הופכי.

שאלה 1.65 יהי n מספר טבעי. האם $(\mathbb{Z}_n \setminus \{[0]\}, \cdot)$ היא חבורה. בפרט האם לכל איבר ב $\mathbb{Z}_n \setminus \{[0]\}$ קיים הופכי.

נענה על שאלה זו בהמשך ונראה שהתשובה תלויה בn, כרגע נסתפק בדוגמה.

דוגמא 1.66 ב $\mathbb{Z}_3$ לכל איבר שונה מאפס יש הופכי כי $[2] \cdot [2] = [1] = [1] \cdot [1]$. אבל ב $\mathbb{Z}_4$ לאיבר $[2]$ אין הופכי.

נסיים את הפרק עם דוגמה חשובה אותה נכליל במספר אופנים בהמשך. נסתכל בקבוצה $\mathbb{R}^2$. זוהי קבוצת הזוגות הסדורים עם קורדינטות ממשיות, אבל אפשר לזהות אותה באותה מידה באופן הבא

$$\mathbb{R}^2 = \left\{ \begin{pmatrix} a \\ b \end{pmatrix} : a, b \in \mathbb{R} \right\}.$$

על קבוצה זו ניתן לחשוב כקבוצת הנקודות "במישור ה xy " כאשר a היא קורדינטת ה x ו b היא קורדינטת ה y. כל נקודה $\begin{pmatrix} a \\ b \end{pmatrix}$ ניתן גם לזהות עם ווקטור או חץ בעל נקודת התחלה בראשית הצירים $\begin{pmatrix} 0 \\ 0 \end{pmatrix}$ ונקודת סוף $\begin{pmatrix} a \\ b \end{pmatrix}$. בעזרת זיהוי זה ניתן גם להגדיר פעולת חיבור על $\mathbb{R}^2$ על ידי

$$\begin{pmatrix} a_1 \\ b_1 \end{pmatrix} + \begin{pmatrix} a_2 \\ b_2 \end{pmatrix} = \begin{pmatrix} a_1 + a_2 \\ b_1 + b_2 \end{pmatrix}.$$

קל לבדוק כי $\mathbb{R}^2$ ביחס לפעולת חיבור זו היא חבורה אבלית עם איבר אדיש $\begin{pmatrix} 0 \\ 0 \end{pmatrix}$.

נעיר, ונרחיב על כך בהמשך, שניתן להגדיר פעולה (לא בינארית) טבעית נוספת על $\mathbb{R}^2$ על ידי כפל בסקלר מ $\mathbb{R}$ באופן הבא:
עבור סקלר $\alpha \in \mathbb{R}$ ווקטור $\begin{pmatrix} a \\ b \end{pmatrix} \in \mathbb{R}^2$ נגדיר

$$\alpha \begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} \alpha a \\ \alpha b \end{pmatrix}.$$

2 שדות ופולינומים

2.1 שדות

הגדרנו את קבוצות המספרים $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$. על קבוצות אלו מוגדרות שתי פעולות בינאריות, חיבור שנסמן ב$+$ וכפל שנסמן ב $\cdot$. נרצה לבדוק את התכונות של קבוצות אלו ביחס לפעולות החיבור והכפל. נשים לב כי $(\mathbb{N}, +)$ איננה חבורה כי אין איבר אדיש וגם אין הופכי. לעומת זאת $(\mathbb{Z}, +), (\mathbb{Q}, +), (\mathbb{R}, +)$ חבורות אבליות. נשאל מה לגבי הכפל. ברור כי ל0 אין הופכי באף אחת מהקבוצות, אבל האם לשאר האיברים יש הופכי? קודם כל $(\mathbb{Z} \setminus \{0\}, \cdot)$ איננה חבורה כי רק ל ± 1 יש הופכי. לעומת זאת $(\mathbb{Q}\setminus\{0\}, \cdot), (\mathbb{R}\setminus\{0\}, \cdot)$ הן חבורות אבליות. בנוסף לתכונות החיבור והכפל ישנו בקבוצות אלו גם חוק הפילוג המקשר בין פעולות החיבור והכפל. $\mathbb{Q}, \mathbb{R}$ הם דוגמאות למושג שדה שנגדיר עכשיו פורמלית.

הגדרה 2.1 תהיי F קבוצה עליה מוגדרות פעולות בינאריות $+$ ו $\cdot$. נאמר כי F הוא שדה אם לכל $x, y, z \in F$ מתקיים

- קומוטטיביות של חיבור: $x + y = y + x$
- קיבוציות של חיבור: $(x + y) + z = x + (y + z)$
- קיום אדיש חיבורי: $x + 0 = 0 + x = x$
- קיום הופכי חיבורי: $x + (-x) = (-x) + x = 0$
- קומוטטיביות של כפל: $xy = yx$
- קיבוציות של כפל: $(xy)z = x(yz)$

- קיום אדיש כפלי: $0 \neq 1 \in F$ כך ש $1x = x = x1$
- קיום הופכי כפלי של כל $x \neq 0$: $xx^{-1} = 1 = x^{-1}x$
- פילוג: $x(y+z) = xy + xz$

כלומר, $(F,+)$ ו $(F \setminus \{0\}, \cdot)$ הן חבורות אבליות ומתקיים חוק הפילוג.

הראינו, לא פורמלית כי $\mathbb{R}$ ו $\mathbb{Q}$ הם שדות אבל $\mathbb{Z}, \mathbb{N}$ אינם שדות. בהמשך הקורס נכיר עוד שדה חשוב: קבוצת המספרים המרוכבים $\mathbb{C}$.

סימון: יהי F שדה. אזי נסמן $F \setminus \{0\} = F^*$.

הערה 2.2 יהי F שדה, אזי מכך ש $(F,+)$ ו $(F^*,\cdot)$ הן חבורות נובע כי האדיש החיבורי והאדיש הכפלי בשדה הם יחידים, לכל איבר קיים נגדי (הופכי חיבורי) יחיד ולכל איבר שונה מאפס בשדה קיים הופכי כפלי יחיד.

אנחנו מכירים את התכונה שתוצאת המכפלה של מספר ממשי באפס (האדיש החיבורי) היא אפס. נראה שזה נכון לכל שדה. תכונה נוספת חשובה שיש לשדה היא שאם מכפלת שני איברים היא אפס אזי אחד מהם הוא בהכרח אפס. נדגיש שמאוחר יותר נראה דוגמאות למבנים אחרים שם תכונה זאת לא מתקיימת.

טענה 2.3 יהי F שדה ויהיו $x, y \in F$. אזי מתקיים

1. $x \cdot 0 = 0$.
2. $x \cdot y = 0 \Rightarrow (x = 0 \vee y = 0)$.

הוכחה:

1.
$$x \cdot 0 = x(0+0) = x \cdot 0 + x \cdot 0.$$
כעת, ע"י חיבור הנגדי של $x \cdot 0$ משני הצדדים נקבל כי $x \cdot 0 = 0$.

2. אם $x \neq 0$ קיים לו הופכי $x^{-1} \in F$. לכן, אם $x \cdot y = 0$, על ידי כפל שני הצדדים של המשוואה ב x^{-1} נקבל
$$x^{-1} \cdot x \cdot y = x^{-1} \cdot 0 \Rightarrow 1 \cdot y = 0 \Rightarrow y = 0.$$
קיבלנו כי אם $x \cdot y = 0$ אזי בהכרח $x = 0$ או $y = 0$.

□

ישנן תכונות נוספות שאפשר להסיק מתכונות השדה, נחזור אל חלקן מאוחר יותר. כרגע נרצה להתמקד בשדה מאוד חשוב, שדה המספרים המרוכבים.

2.2 המספרים המרוכבים

נשים לב שבמעבר מהקבוצה $\mathbb{N}$ לקבוצה $\mathbb{Z}$ אנחנו מקבלים פתרונות למשוואות שלפני כן לא יכלנו לפתור, למשל $2x+4=0$. דבר דומה קורה במעבר מ $\mathbb{Z}$ ל $\mathbb{Q}$ ובמעבר מ $\mathbb{Q}$ ל $\mathbb{R}$.

האם יש פתרון למשוואה $x^2+1=0$?

ידוע שאין פתרון ממשי. נרצה לבנות מערכת מספרים חדשה (בעצם שדה) שבה יש פתרון למשוואה הזאת - וגם להרבה משוואות אחרות.

הגדרה 2.4 יהי i סימן פורמלי (בינתיים ללא משמעות מיוחדת). נגדיר קבוצה

$$\mathbb{C} = \{a+ib \mid a,b \in \mathbb{R}\}$$

הנקראת "קבוצת המספרים המרוכבים". בשלב זה נתייחס ל $a+ib$ כביטוי פורמלי. רק אחרי שנגדיר על $\mathbb{C}$ פעולות ונכיר את התכונות שלהן, נתחיל לדבר על ביטויים כמו $a+ib$ כ"מספרים".

אנו נגדיר על $\mathbb{C}$ שתי פעולות: חיבור וכפל. בהמשך, נראה שיש לקבוצה זו כמה תכונות נחמדות מאוד:

- ניתן לשכן את $\mathbb{R}$ כתת קבוצה של $\mathbb{C}$ במובן מסויים.
- נראה ש $\mathbb{C}$ מהווה שדה.
- נראה שיש פירוש גאומטרי לכל אחד מהפעולות $+,\cdot$ על $\mathbb{C}$.
- נראה שלכל פולינום ממשי (יוגדר בהמשך) יש שורש ב $\mathbb{C}$.

הגדרה 2.5 נגדיר פעולות חיבור וכפל על ידי

$$(a+ib)+(c+id) = (a+c)+i(b+d)$$

$$(a+ib)\cdot(c+id) = (ac-bd)+i(ad+bc).$$

מאוחר יותר ניתן פירוש גיאומטרי לפעולות הנ"ל, אך לעת עתה נסביר כי אנחנו רוצים כי שהסימן i יקיים את התכונה $i^2=-1$. על ידי הזיהוי $i=0+i1$ נקבל

$$i^2 = (0+i1)(0+i1) = (0-1)+i0 = -1+i0.$$

נרצה להראות כי $\mathbb{C}$, ביחד עם הפעולות שהגדרנו עליו הוא שדה. נסמן $0=0+i0$ ו $1=1+i0$. קל לבדוק כי 0 אדיש ביחס לחיבור שהגדרנו ב $\mathbb{C}$ ו 1 אדיש ביחס לכפל ב $\mathbb{C}\setminus\{0\}$. בדיקה פשוטה מוכיחה את המשפט הבא

משפט 2.6 קבוצת המספרים המרוכבים עם הפעולות הבינאריות המוגדרות לעיל היא שדה.

כעת, אנו מעוניינים "לזהות" את $\mathbb{R}$ כתת קבוצה של $\mathbb{C}$ במובן מסויים. לשם כך, נאפשר לעצמינו לכתוב מספר ממשי a גם בצורה של $a+i0$. למעשה, כבר עשינו את זה עבור המספרים $0,1$.

הגדרה 2.7 מספר $z=a+ib$ נקרא "ממשי" אם $b=0$ ו"מדומה טהור" אם $a=0$. לכל מספר מרוכב $z=a+ib$ נסמן $\mathrm{Re}(z)=a$ (זה נקרא החלק הממשי של z) ו $\mathrm{Im}(z)=b$ (זה נקרא החלק המדומה של z).

כדי להבין קצת יותר טוב מאיפה באות ההגדרות האלה, ואת הגדרות החיבור והכפל של המרוכבים, נגדיר את "מישור המרוכבים" ע"י התאמה בין כל ביטוי $a+ib$ לבין הנקודה (ווקטור) $\begin{pmatrix} a \\ b \end{pmatrix}$ במישור $\mathbb{R}^2$ (הוגדר במבוא).

באמצעות התאמה זו, ניתן לחשוב על החלק הממשי של z כקואורדינטה של z בכיוון ציר ה x והחלק המדומה של z הוא הקואורדינטה של z בכיוון ציר ה y. בנוסף, לפי ההתאמה הזאת, ניתן לראות שחיבור שני מספרים מרוכבים משקף את הסכום של שני וקטורים:

$$(a+ib)+(c+id) = (a+c)+i(b+d) \longleftrightarrow \begin{pmatrix} a \\ b \end{pmatrix} + \begin{pmatrix} c \\ d \end{pmatrix} = \begin{pmatrix} a+c \\ b+d \end{pmatrix}.$$

גם לכפל של מספרים מרוכבים ניתן לתת משמעותי גיאומטרית, נעשה זאת בהמשך.
יש עוד מושג גאומטרי בקשר למספרים מרוכבים.

הגדרה 2.8 יהי $z = a + ib \in \mathbb{C}$. הערך המוחלט של z, מסומן ב $|z|$, נתון על ידי $|z| = \sqrt{a^2 + b^2}$.

לפי ההתאמה

$$a + ib \longleftrightarrow \begin{pmatrix} a \\ b \end{pmatrix}$$

ניתן לראות שהערך המוחלט של z הוא בדיוק האורך של הווקטור $\begin{pmatrix} a \\ b \end{pmatrix}$:

הגדרה 2.9 עבור כל $z = a + ib \in \mathbb{C}$, נגדיר את הצמוד $\overline{z}$ של z ע"י $\overline{z} = a - ib$.

טענה 2.10
- לכל $z = a + ib \in \mathbb{C}$ מתקיים $z\overline{z} = |z|^2$
- אם $z \neq 0$ אזי ל z יש הופכי שהוא $z^{-1} = \frac{\overline{z}}{|z|^2}$.

יש אינטראקציה בין הפעולות שהגדרנו (חיבור, כפל, חלק ממשי, חלק מדומה, ערך מוחלט, צמוד) שחשוב להכיר.

טענה 2.11 לכל $z, w \in \mathbb{C}$, $\alpha \in \mathbb{R}$ ו $n \in \mathbb{N}$ מתקיימים:

1. $|z| = 1 \iff z^{-1} = \overline{z}$.
2. $\overline{\overline{z}} = z$.
3. $\mathrm{Re}(\overline{z}) = \mathrm{Re}(z)$.
4. $\mathrm{Im}(\overline{z}) = -\mathrm{Im}(z)$.
5. $z \in \mathbb{R} \iff z = \overline{z}$
6. z מדומה טהור $\iff \overline{z} = -z$.
7. $|\overline{z}| = |z|$.
8. $\overline{z + w} = \overline{z} + \overline{w}$.

9. $\overline{\alpha z} = \alpha \cdot \overline{z}$

10. $|z + w| \leq |z| + |w|$

11. $\overline{zw} = \overline{z} \cdot \overline{w}$

12. $\overline{z^n} = \overline{z}^n$

13. $|zw| = |z| \cdot |w|$.

14. $|z^n| = |z|^n$.

צורה קוטבית למספר מרוכב

על מנת להבין יותר לעומק את המשמעות הגאומטרית של כפל מספרים מרוכבים, נעזר שוב במישור המרוכבים. מסתבר שיש קשר בין כפל מספרים לבין סיבובים של וקטורים סביב הראשית. כדי לדייק, אנו נצטרך צורה חדשה עבור מספר מרוכב.

הגדרה 2.12 יהי $z \in \mathbb{C}$ כאשר $z \neq 0$ ונסמן $z = a + ib$. הארגומנט של z הוא מספר $0 \leq \theta \leq 2\pi$ כך ש $\cos(\theta) = a/|z|$. נסמן את הארגומנט על ידי $\arg(z) = \theta$.

נשים לב שלכל $z \in \mathbb{C}$, $z \neq 0$, נוכל לכתוב $r = |z|$ ו $\theta = \arg(z)$. אז $\cos\theta = a/|z| = a/r$ ו $\sin\theta = b/|z| = b/r$ לכן $z = a + ib = r(\cos\theta + i\sin\theta)$.

הגדרה 2.13 (צורה קוטבית של מספר מרוכב). יהי $z \in \mathbb{C}, z \neq 0$. צורה קוטבית של z היא צורה של $z = r(\cos\theta + i\sin\theta)$. נסמן $e^{i\theta} = \text{cis}(\theta) = \cos\theta + i\sin\theta$ ואז $z = r\,\text{cis}(\theta) = re^{i\theta}$.

נשאלת השאלה: בהינתן מספר מרוכב $z = a + ib$, האם יש אפשרות אחת לכתוב אותו בצורה קוטבית? התשובה היא שלא: אם $a + ib = r(\cos\theta + i\sin\theta)$ אז בהכרח $r = |z| = \sqrt{a^2 + b^2}$ אבל יש גמישות לגבי הזווית θ: ניתן לקחת כל זווית $\theta = \arg(z) + 2\pi k$ כאשר $k \in \mathbb{Z}$ (נציין שאין הבדילים בין האופציות הנ"ל ל θ מבחינה גאומטרית - ההבדלים הוא רק בערך של θ בתור מספר ממשי.)

משפט 2.14 לכל $z, w \in \mathbb{C}$ כאשר $z, w \neq 0$, אם נכתוב אותם בצורה קוטבית $z = r_1\text{cis}(\theta_1), w = r_2\text{cis}(\theta_2)$ אזי מתקיים $zw = r_1 r_2 \text{cis}(\theta_1 + \theta_2)$.

בסימנים אחרים המשפט נותן $r_1 e^{i\theta_1} r_2 e^{i\theta_2} = r_1 r_2 e^{i(\theta_1 + \theta_2)}$.

הוכחה:

$$\begin{aligned} zw &= r_1(\cos\theta_1 + i\sin\theta_1)r_2(\cos\theta_2 + i\sin\theta_2) \\ &= r_1r_2((\cos\theta_1\cos\theta_2 - \sin\theta_1\sin\theta_2) + i(\sin\theta_1\cos\theta_2 + \cos\theta_1\sin\theta_2)) \\ &= r_1r_2(\cos(\theta_1+\theta_2) + i\sin(\theta_1+\theta_2)) = r_1r_2e^{i(\theta_1+\theta_2)} \end{aligned}$$

□

יש כמה תכונות יפות שנובעות מהמשפט:

- ניתן לפרש כפל מספרים מרוכבים בצורה גאומטרית: כשמכפילים z ב w, מכפילים את האורך של כל אחד ומחברים את הזוויות.
- משפט דה־מואבר: לכל $n \in \mathbb{Z}$ ו $\theta \in \mathbb{R}$ מתקיים

$$(\cos\theta + i\sin\theta)^n = \cos(n\theta) + i\sin(n\theta) \iff (\mathrm{cis}(\theta))^n = \mathrm{cis}(n\theta) \iff (e^{i\theta})^n = e^{in\theta}.$$

- ניתן לפרש את הנוסחה להופכי כפלי: אם נכתוב $z = r\mathrm{cis}(\theta)$ אז

$$z^{-1} = \frac{\overline{z}}{|z|^2} = \frac{1}{r^2}\overline{r\cos\theta + ir\sin\theta} = \frac{1}{r^2}(r\cos\theta - ir\sin\theta) = \frac{1}{r}(\cos(-\theta) + i\sin(-\theta))$$

שזהו מספר בעל ערך מוחלט ההופכי של $r = |z|$ ובעל זווית מינוס הזווית של z. בפרט, עם $r = |z| = 1$ אז $z^{-1} = \overline{z}$ שזהו מספר שמתקבל מ z על ידי שיקוף ביחס לציר הממשיים במישור המרוכבים.

שורשים מסדר n של 1.

אנו רוצים שיטה למצוא שורשים מסדר כלשהו n של 1, כלומר לפתור את המשוואה $z^n = 1$. באמצעות משפט דה מואבר מיד אנו רואים ששורש אחד הוא $\mathrm{cis}(2\pi/n)$ מכיוון ש $(\mathrm{cis}(2\pi/n))^n = \mathrm{cis}(2\pi) = 1$. מסתבר שבעצם כל כפולה שלמה של המספר הזה גם שורש מסדר n של 1: יהי $k \in \mathbb{Z}, k \geq 0$. אזי $(\mathrm{cis}(2\pi k/n))^n = \mathrm{cis}(2\pi k) = 1$. אז קיבלנו n שורשים שונים מסדר n של 1:

$$1, \mathrm{cis}(2\pi/n), \mathrm{cis}(2(2\pi/n)), \ldots, \mathrm{cis}((n-1)(2\pi/n)).$$

2.3 השדה $\mathbb{Z}_p$

למעשה בסעיף זה נוכיח משפט יחיד הקובע לאילו ערכי n הקבוצה $\mathbb{Z}_n$ היא שדה. למעשה כמעט כל תכונות השדה מתקיימות לכל ערכי n כפי שראינו במבוא, אך ראינו שם שיש מקרים שבהם לכל איבר ב $\mathbb{Z}_n$ יש הופכי ומקרים שבהם לא לכל איבר יש הופכי.

משפט 2.15 הקבוצה $\mathbb{Z}_n$ היא שדה אם ורק אם n מספר ראשוני.

הוכחה: נניח תחילה כי $\mathbb{Z}_n$ שדה ונוכיח כי n בהכרח ראשוני. נעשה זאת בהוכחה על דרך השלילה, כלומר נראה שאם n לא ראשוני אזי $\mathbb{Z}_n$ איננו שדה. אכן, אם n לא ראשוני, אזי $n = ab$ עבור טבעיים כלשהם $1 < a, b < n$. לכן $[a], [b] \in \mathbb{Z}_n \setminus \{[0]\}$ ומתקיים $[a] \cdot [b] = [0]$. לכן על פי טענה 2.3 $\mathbb{Z}_n$ איננו שדה וזה מסיים את הוכחת הכיוון הראשון.

נניח כעת כי n הוא ראשוני ונוכיח כי $\mathbb{Z}_n$ הוא שדה. למעשה התכונה היחידה שנותרה להוכיח היא כי לכל $[a] \in \mathbb{Z}_n \setminus \{[0]\}$ יש הופכי. יהי $[a] \in \mathbb{Z}_n \setminus \{[0]\}$. נסתכל בקבוצה

$$S = \{[a] \cdot [0], [a] \cdot [1], \ldots, [a] \cdot [n-1]\}$$

ונטען שכל איברי S שונים זה מזה ואז בהכרח קיים $[x] \in \mathbb{Z}_n$ כך ש $[a] \cdot [x] = [1]$, כלומר $[x]$ הופכי ל $[a]$. נניח בשלילה כי קיימים $[x_1] \neq [x_2] \in \mathbb{Z}_n$ כך ש $[a] \cdot [x_1] = [a] \cdot [x_2]$ ונניח כי $x_2 > x_1$. לכן $[a][x_2 - x_1] = [0]$ ולכן $a \cdot (x_2 - x_1)$ הוא מספר שלם המתחלק בn. אך מכיוון שn ראשוני, מכך שהוא מחלק את $a \cdot (x_2 - x_1)$ נובע שהוא מחלק או את a או את $x_2 - x_1$, אך מכיוון ששני מספרים אלו קטנים ממש מn זה לא ייתכן וקיבלנו סתירה להנחת השלילה שלנו, ולכן כל איברי S שונים זה מזה ול $[a]$ יש הופכי. □

הערה 2.16 ראינו כי $\mathbb{Z}_n$ הוא שדה אם ורק אם n הוא ראשוני. לרוב נסמן ב $\mathbb{Z}_p$ עבור מספר ראשוני p. נוסיף שעבור מספר טבעי כלשהו $m \geq 2$ קיים שדה עם m איברים אם ורק אם m הוא חזקה טבעית של מספר ראשוני. ההוכחה משתמשת בכלים החורגים מתוכן ספר זה. למשל, $\mathbb{Z}_4$ הוא לא שדה, אבל קיים שדה עם 4 איברים.

בהמשך, כאשר נעבוד עם השדה $\mathbb{Z}_p$ נוותר על הסימון המסורבל $[a] \in \mathbb{Z}_n$ ונרשום פשוט $a \in \mathbb{Z}_n$.

2.4 פולינומים

פולינומים הם אוביקטיבים שמופיעים בהקשרים רבים במתמטיקה, ובפרט באלגברה ליניארית. למעשה אנו נפגשים בפולינומים עוד בלימודי התיכון ואפילו אף לפני כן. למשל במשוואה ריבועית, $ax^2 + bx + c = 0$, צד שמאל של המשוואה הוא פולינומים ממעלה שניה.

הגדרה 2.17 יהי F שדה. פולינום ממעלה $n \in \mathbb{N}$ מעל השדה F הוא ביטוי הפורמלי

$$p(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots a_2 x^2 + a_1 x + a_0$$

כאשר $a_n, a_{n-1}, \ldots, a_0 \in F$ נקראים מקדמי הפולינום. $a_n \neq 0$ נקרא המקדם המוביל של הפולינום. בדרך כלל מעלת הפולינום תסומן ב $deg(p(x))$.

דוגמא 2.18

1. $p(x) = 2x^3 - 4x^2 + 7$ הוא פולינום ממעלה 3 מעל הממשיים.
2. $g(z) = -5z^2 + (1+i)z - 3i$ הוא פולינום ממעלה 2 מעל המרוכבים.
3. $p(x) = 7$ הוא פולינום ממעלה אפס.
4. לפונקצית האפס קוראים גם פולינום האפס $p(x) = 0$ ולא מייחסים לו דרגה.

הערה 2.19 למעשה פולינום עם מקדמים בשדה F הוא פונקציה $p(x) : F \to F$ המוגדרת ע"י $p(x)(t) = p(t)$ לכל $t \in F$.

נאמר כי שני פולינומים $p(x), g(x)$ שווים זה לזה אם הם מאותה מעלה וכל מקדמיהם שווים בהתאמה, כלומר המקדם של x^j בפולינום $p(x)$ שווה למקדם של x^j בפולינום $g(x)$ לכל j שלם אי שלילי.

במקום לתת הגדרה פורמלית מסורבלת של חיבור וכפל פולינומים, ניתן דוגמה שממחישה כיצד עושים זאת. לא פורמלית נאמר כי חיבור עושים על ידי חיבור של המקדמים של אותן חזקות וכפל עושים על ידי חוק פתיחת סוגריים ועם החוק כי $x^i x^j = x^{i+j}$.

דוגמא 2.20 יהיו $p(x) = 4x^3 + 2x - 1$ ו $g(x) = x^2 - 4x$. אזי

1. $p(x) + g(x) = 4x^3 + x^2 - 2x - 1$.

2. $p(x)g(x) = (4x^3 + 2x - 1)(x^2 - 4x) = 4x^5 - 16x^4 + 2x^3 - 9x^2 + 4x$.

סימון: קבוצת כל הפולינומים במשתנה x עם מקדמים בשדה F תסומן ב $F[x]$.

בדומה למספרים טבעיים, גם בפולינומים אנחנו רוצים לפרק פולינום כמכפלה של גורמים "ראשוניים", כלומר גורמים שאין דרך לרשום אותם כמכפלה לא טרוויאלית של פולינומים אחרים. ניתן הגדרה פורמלית.

הגדרה 2.21 יהי $p(x) \in F[x]$. נאמר כי $p(x)$ הוא פריק אם קיימים פולינומים $g_1(x), g_2(x) \in F[x]$ ממעלה לפחות 1 כך ש $p(x) = g_1(x)g_2(x)$. אם פולינום הוא לא פריק נאמר כי הוא אי־פריק.

פריקות פולינומים מתקשרת למושג השורש של פולינום.

הגדרה 2.22 יהי F שדה ויהי $p(x) \in F[x]$. איבר $x_1 \in F$ ייקרא שורש של $p(x)$ אם מתקיים $p(x_1) = 0$.

דוגמא 2.23

1. 2 הוא שורש של הפולינום $p(x) = 2x^2 - 5x + 2$.
2. $(1 + i)$ הוא שורש של הפולינום $p(z) = z^2 - 2i$ מעל $\mathbb{C}$.
3. 3 הוא שורש של הפולינום $p(x) = x^2 + 1$ מעל $\mathbb{Z}_5$.

על מנת לקשר בין מושג הפריקות ומושג השורש נזכר בתכונת החלוקה עם שארית של פולינומים.

משפט 2.24 יהי F שדה ויהיו $p(x), g(x) \in F[x]$ אזי קיימים שני פולינומים $q(x), r(x) \in F[x]$ כאשר $deg(r(x)) < deg(g(x))$ כך שמתקיים

$$p(x) = q(x)g(x) + r(x).$$

מסקנה 2.25 יהי F שדה ויהי $p(x) \in F[x]$ פולינום שונה מפלינום האפס. אזי אם $x_1 \in F$ שורש של $p(x)$ אזי $p(x) = (x - x_1)g(x)$ עבור $p(x) \in F[x]$ כלשהו. כלומר $p(x)$ מתחלק ללא שארית ב $(x - x_1)$.

הוכחה: נחלק עם שארית את $p(x)$ ב $(x-x_1)$. על פי משפט 2.24

$$p(x) = q(x)(x-x_1) + r(x)$$

כאשר $r(x)$ הוא איבר בשדה. נציב x_1. אז מכיוון ש x_1 הוא שורש של $p(x)$ נקבל

$$p(x_1) = q(x_1)(x_1-x_1) + r(x_1) \Rightarrow 0 = g(x_1)\cdot 0 + r(x_1).$$

לכן $r(x_1) = 0$, ומכיוון ש $r(x)$ הוא איבר בשדה, מקבלים כי הוא פשוט איבר האפס של השדה.

□

כמה מסקנות מהמשפט לעיל ומהגדרות של פריקות ושורש

מסקנה 2.26

1. כל פולינום ממעלה אפס או אחת הוא אי פריק.
2. אם לפולינום ממעלה לפחות 2 יש שורש אז הוא פריק.
3. אם פולינום ממעלה $2,3$ הוא פריק אז יש לו שורש.
4. נעיר שההיפך מהסעיף השני לא נכון באופן כללי, כלומר יש פולינומים פריקים שאין להם שורשים. למשל, עבור השדה $\mathbb{R}$ הפולינום $x^4+2x^2+1 = (x^2+1)^2$ הוא פולינום פריק אבל אין לו שורשים ממשיים.

נרצה לדעת כיצד ניתן לפרק פולינום לגורמים אי פריקים ובפרט איך מוצאים שורשים של פולינום. נעיר כי באופן כללי זו בעיה קשה ולעיתים אף אי פתירה, עם זאת נציג מספר דרכים שיכולות לעזור לעשות זאת. דוגמה פשוטה שאנו מכירים מבית הספר היא המקרה של פולינום ממעלה שניה. בהנתן פולינום ממעלה שניה $p(x) = ax^2+bx+c$ על מנת למצוא את שורשיו עלינו לפתור את המשוואה $ax^2+bx+c=0$. זה ניתן לעשות על ידי הנוסחה הידועה

$$x_{1,2} = \frac{-b \pm \sqrt{b^2-4ac}}{2a}.$$

ואז מתקיים $p(x) = a(x-x_1)(x-x_2)$. לשם שלמות נוכיח את נוסחת השורשים.

הוכחה: תהיי $ax^2+bx+c=0$ משוואה ריבועית, כלומר $a \neq 0$. על ידי הכפלת שני האגפים ב $4a \neq 0$ נקבל

$$4a^2x^2+4abx+4ac = 0 \Rightarrow 4a^2x^2+4abx = -4ac.$$

כעת על ידי הוספה של b^2 לשני האגפים נקבל

$$4a^2x^2 + 4abx + b^2 = b^2 - 4ac \Rightarrow (2ax + b)^2 = b^2 - 4ac.$$

נוציא שורש ונקבל

$$2ax + b = \pm\sqrt{b^2 - 4ac} \Rightarrow x^2 = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}.$$

□

הגדרה 2.27 יהי F שדה ויהי $\alpha \in F$ שורש של פולינום $p(x) \in F[x]$. נאמר כי הריבוי של α כשורש הוא $k \in \mathbb{N}$ אם $(x-\alpha)^k$ מחלק את $p(x)$ אבל $(x-\alpha)^{k+1}$ לא מחלק את $p(x)$.

נזכור כי לעיתים לפולינום אין שורשים מעל השדה בו אנחנו עובדים. למשל ל $p(x) = x^2 + 1$ אין שורשים ממשיים ואילו ל $q(x) = x^2 + x + 1$ אין שורשים מעל $\mathbb{Z}_2$. מסתבר שמעל המרוכבים דבר זה לא יכול לקרות. המשפט הבא כל כך חשוב שהוא קיבל את השם "המשפט היסודי של האלגברה".

משפט 2.28 יהי $p(z)$ פולינום מעל המרוכבים ממעלה n. אזי יש לו בדיוק n שורשים (כאן הכוונה היא לספירת שורשים עם ריבוי). במילים אחרות, אם ל $p(z)$ מקדם מוביל a, אזי קיימים $z_1, z_2, \ldots, z_n \in \mathbb{C}$ לאו דווקא שונים, כך ש

$$p(z) = a(z - z_1) \cdot (z - z_2) \cdot \ldots \cdot (z - z_n).$$

ראינו איך מוצאים שורשים לפולינום ממעלה שניה, וראינו שמעל המרוכבים תמיד יש שורשים, אבל עדיין נשאלת השאלה, איך ניתן למצוא אותם? אחד הכלים היעילים במציאת שורשים ובכלל בפירוק פולינום הוא חלוקת פולינומים. הרעיון מתבסס על כך שראינו כי אם x_1 הוא שורש של פולינום $p(x) \in F[x]$ אזי קיים פולינום $q(x) \in F[x]$ ממעלה קטנה ב1 מ $p(x)$ כך ש $p(x) = q(x)(x - x_1)$. נראה איך מוצאים את $q(x)$ על ידי דוגמה.

דוגמא 2.29 יהי $p(x) = x^3 - 6x^2 + 11x - 6$. קל לראות כי 1 הוא שורש של $p(x)$ (אחר כך נפתח כלים "לנחש באופן מושכל" שורש). לכן $x^3 - 6x^2 + 11x - 6 = (x-1)q(x)$.

עכשיו מתחילה חלוקת הפולינום. מתחילים מחלוקת הגורם x^3 של $p(x)$ בגורם x של $x-1$ ונקבל x^2. מחשבים

$$(x^3-6x^2+11x-6)-x^2(x-1)=-5x^2+11x-6. \tag{2}$$

מחלקים את הגורם $-5x^2$ של $-5x^2+11x-6$ בגורם x של $x-1$ ונקבל $-5x$. מחשבים

$$(-5x^2+11x-6)-(-5x)(x-1)=6x-6. \tag{3}$$

מחלקים את הגורם $6x$ של $6x-6$ בגורם x של $x-1$ ונקבל 6. מחשבים

$$(6x-6)-6(x-1)=0.$$

נציב את זה ב (3) ונקבל

$$(-5x^2+11x-6)-(-5x)(x-1)=6(x-1)\Rightarrow -5x^2+11x-6=(-5x+6)(x-1).$$

נציב זאת ב (2) ונקבל

$$(x^3-6x^2+11x-6)-x^2(x-1)=(-5x+6)(x-1)\Rightarrow x^3-6x^2+11x-6=(x^2-5x+6)(x-1).$$

כלומר מצאנו פירוק לפולינום $p(x)$ וכעת ניתן להמשיך על ידי נוסחת שורשים ולמצוא

$$p(x)=(x-3)(x-2)(x-1).$$

אז איך ניתן "לנחש באופן מושכל" שורש של פולינום? אין שיטה שעובדת בכל מקרה, אבל עבור פולינום ממעלה שלישית, אם קיים לו שורש רציונלי אז קל לנחש אותו.

טענה 2.30 יהי p מספר שלם שונה מאפס ויהי

$$g(x)=px^3+bx^2+cx+q$$

פולינום שכל מקדמיו שלמים. אזי אם x_1 הוא שורש רציונלי של $g(x)$ אז קיימים a_1 מחלק של q ו a_2 מחלק של p כך ש $x_1=\frac{a_1}{a_2}$.

אנחנו רואים שבדוגמה לעיל $q=6$ ולכן מחלקיו הם $\{\pm1,\pm2,\pm3,\pm6\}$ ואילו $p=1$ ולכן מחלקיו הם $\{\pm1\}$. אכן כל שורשי הפולינום מתקבלים מחלוקה של מחלק של q במחלק של p.

ראינו מוקדם יותר כי ייתכן כי לפולינום $p(x)\in\mathbb{R}[x]$ אין בהכרח שורשים ממשיים והדוגמה הראשונה שראינו היא $p(x)=x^2+1$. נרצה להראות כי לפולינום מעל הממשיים ממעלה אי זוגית בהכרח יש שורש ממשי. זה ינבע ישירות מהמשפט הבא.

משפט 2.31 יהי $p(z)$ פולינום בעל מקדמים ממשיים. אם z_1 הוא שורש של הפולינום אזי גם $\overline{z_1}$ הוא שורש של $p(z)$.

הוכחה: יהיו $a_0, a_1, \ldots, a_n \in \mathbb{R}$ ויהי

$$p(z) = a_n z^n + \ldots + a_1 z + a_0.$$

נניח כי $p(z_1) = 0$ אזי גם $\overline{p(z_1)} = \overline{0} = 0$.

נשתמש בתכונות $(8), (11)$ מטענה 2.11 ובכך ש $\overline{a_i} = a_i$ לכל $0 \leq i \leq n$.

$$\begin{aligned} 0 = \overline{p(z_1)} = \overline{a_n z_1^n + \ldots + a_1 z_1 + a_0} = \overline{a_n z_1^n} + \ldots + \overline{a_1 z_1} + \overline{a_0} = \\ \overline{a_n}\bar{z_1}^n + \ldots + \overline{a_1}\bar{z_1} + \overline{a_0} = a_n \bar{z_1}^n + \ldots + a_1 \bar{z_1} + a_0 = \\ a_n \bar{z_1}^n + \ldots + a_1 \bar{z_1} + a_0 = p(\overline{z_1}). \end{aligned}$$

ולכן $\overline{z_1}$ הוא שורש של $p(z)$. □

מסקנה 2.32 יהי $p(z)$ פולינום בעל מקדמים ממשיים ממעלה אי זוגית, אזי קיים לו שורש ממשי.

דוגמא 2.33 נרצה למצוא פירוק מעל הממשיים של הפולינום $p(x) = x^3 - 7x^2 + x - 7$ ונניח כי ידוע לנו כי i הוא שורש של הפולינום. דרך אחת לחפש את הפירוק זה לחלק את $p(x)$ ב $(x - i)$, אך דרך זו יחסית מסורבלת. נוכל להמנע מכך ע"י שימוש במשפט שמבטיח לנו כי גם $-i$ הוא שורש ולכן $x^2 + 1 = (x - i)(x + i)$ מחלק את $p(x)$. על ידי חלוקה מקבלים

$$p(x) = (x^2 + 1)(x - 7).$$