תרגול 2 – 88-112 אלגברה לינארית 1
סמסטר א' תשע"ו

29 באוקטובר 2015

1 מספרים מרוכבים – המשך

מסקנה 1.1. נניח שרוצים לפתור את המשוואה $z^n = r\text{cis}\theta$. אזי הפתרונות הם

$$z_k = \sqrt[n]{r}\text{cis}\left(\frac{\theta + 2\pi k}{n}\right)$$

כאשר k הוא אינדקס שערכיו הם $0, 1, \ldots, n-1$.
(שימו לב ש-$\sqrt[n]{r}$ הוא מספר ממשי חיובי)

תרגיל 1.2. פתרו את המשוואה $z^4 + 16i = 0$.

פתרון. נעביר אגפים, ונקבל שצריך לפתור את $z^4 = -16i$. נעביר את $-16i$ לצורה הפולרית שלו:

$$r = \sqrt{0^2 + (-16)^2} = \sqrt{16^2} = 16$$

פה המספר מדומה טהור, ולכן הזווית היא $90°$ או $270°$. $-16i$ על ציר y מלמטה, ולכן הזווית היא $270° = \frac{3\pi}{2}$. לכן, הצורה הפולרית היא $-16i = 16\text{cis}\frac{3\pi}{2}$. לפי הנוסחה שלנו, הפתרונות הם

$$z_k = \sqrt[4]{16}\text{cis}\left(\frac{\frac{3\pi}{2} + 2\pi k}{4}\right) = 2\text{cis}\left(\frac{3\pi}{8} + \frac{\pi k}{2}\right)$$

עבור $k = 0, 1, 2, 3$. במפורש,

$$z_0 = 2\text{cis}\left(\frac{3\pi}{8}\right), \quad z_1 = 2\text{cis}\left(\frac{7\pi}{8}\right), \quad z_2 = 2\text{cis}\left(\frac{11\pi}{8}\right), \quad z_3 = 2\text{cis}\left(\frac{15\pi}{8}\right)$$

2 שדות

נסמן כמה קבוצות של מספרים:

- $\mathbb{N} = \{1, 2, 3, \ldots\}$ – קבוצת המספרים הטבעיים.
- $\mathbb{Z} = \{0, \pm1, \pm2, \pm3, \ldots\}$ – קבוצת המספרים השלמים.

- $\mathbb{Q}=\left\{\frac{p}{q}\middle|p,q\in\mathbb{Z},q\neq 0\right\}$ – קבוצת המספרים הרציונליים.
- $\mathbb{R}$ – קבוצת המספרים הממשיים.
- $\mathbb{C}=\{a+bi|a,b\in\mathbb{R}\}$ – קבוצת המספרים המרוכבים (שהגדרנו בתרגול הקודם).

הגדרה 2.1. שדה הוא קבוצה $\mathbb{F}$ יחד עם שתי פעולות, $+$ ("חיבור") ו-$\cdot$ ("כפל"), כך שמתקיימות האקסיומות הבאות:

1. סגירות: לכל $a,b\in\mathbb{F}$, $a+b\in\mathbb{F}$ וגם $a\cdot b\in\mathbb{F}$.
2. אסוציאטיביות (קיבוציות): לכל $a,b,c\in\mathbb{F}$, לחיבור מתקיים $(a+b)+c=a+(b+c)$ ולכפל מתקיים $(a\cdot b)\cdot c=a\cdot(b\cdot c)$.
3. קומוטטיביות (חילופיות): לכל $a,b\in\mathbb{F}$, $a+b=b+a$ וגם $a\cdot b=b\cdot a$.
4. קיום איברים ניטרליים: קיימים איברים $0_{\mathbb{F}},1_{\mathbb{F}}\in\mathbb{F}$ כך שלכל $a\in\mathbb{F}$, $a+0_{\mathbb{F}}=0_{\mathbb{F}}+a=a$ וגם $a\cdot 1_{\mathbb{F}}=1_{\mathbb{F}}\cdot a=a$.
(בנוסף, $0_{\mathbb{F}}\neq 1_{\mathbb{F}}$)
5. קיום איברים הופכיים:
   (א) לכל $a\in\mathbb{F}$ קיים **איבר נגדי**, שיסומן $-a\in\mathbb{F}$, כך ש-$a+(-a)=(-a)+a=0_{\mathbb{F}}$.
   (ב) לכל $0_{\mathbb{F}}\neq a\in\mathbb{F}$ קיים **איבר הופכי**, שיסומן $a^{-1}\in\mathbb{F}$, כך ש-$a\cdot a^{-1}=a^{-1}\cdot a=1_{\mathbb{F}}$.
6. דיסטריביוטיביות (פילוג): לכל $a,b,c\in\mathbb{F}$ מתקיים $(a+b)\cdot c=a\cdot c+b\cdot c$.

הערה 2.2. כדי להקל בכתיבה, כאשר השדה $\mathbb{F}$ נתון, במקום לכתוב $0_{\mathbb{F}}$ נכתוב 0, ובמקום לכתוב $1_{\mathbb{F}}$ נכתוב 1.

דוגמה 2.3. נסתכל על הקבוצות שהזכרנו, ונבדוק מי מהן היא שדה:

1. $\mathbb{N}$ אינה שדה – כי אין איבר ניטרלי לחיבור (ואין נגדיים והופכיים).
2. $\mathbb{Z}$ אינה שדה – כי אין איברים הופכיים.
3. $\mathbb{Q}$, $\mathbb{R}$ ו-$\mathbb{C}$ הם כן שדות.

לשדות יש תכונות רבות המוכרות לנו מ-$\mathbb{R}$. נציג כמה מהן בתרגול, וחלקן יופיעו בשיעורי הבית. דף מלא עם התכונות – באתר הקורס (ולעצלנים, ממש כאן).

תרגיל 2.4. יהי $\mathbb{F}$ שדה. הוכיחו שלכל $a,b,c\in\mathbb{F}$, אם $a\cdot c=b\cdot c$ וגם $c\neq 0$, אזי $a=b$ (לתכונה זו קוראים **כלל הצמצום**. שימו לב שהיא אינה מתקיימת כאשר $c=0$. למשל, אנחנו יודעים ש-$0\cdot 1=0\cdot 2$, אבל $1\neq 2$).

הוכחה. כיוון ש-$c\neq 0$, קיים $c^{-1}\in\mathbb{F}$. נכפול בו את שני האגפים מימין, ונקבל:

$$(a\cdot c)\cdot c^{-1}=(b\cdot c)\cdot c^{-1}\Longrightarrow a\cdot\left(c\cdot c^{-1}\right)=b\cdot\left(c\cdot c^{-1}\right)\Longrightarrow a\cdot 1=b\cdot 1\Longrightarrow a=b$$

$\square$

תרגיל 2.5. יהי $\mathbb{F}$ שדה. הוכיחו שלכל $a \in \mathbb{F}$, $a \cdot 0 = 0 \cdot a = 0$. (הוכחתם בהרצאה)

תרגיל 2.6. יהי $\mathbb{F}$ שדה. הוכיחו שלכל $a \in \mathbb{F}$, $-a = (-1) \cdot a$.

הוכחה. יהי $a \in \mathbb{F}$. צריך להוכיח $(-1) \cdot a + a = 0_{\mathbb{F}}$. מתקיים:

$$(-1) \cdot a + a = (-1) \cdot a + 1 \cdot a \overset{\text{distributivity}}{=} (-1+1) \cdot a = 0 \cdot a = 0$$

כפי שרצינו. $\square$

תרגיל 2.7. יהי $\mathbb{F}$ שדה. הוכיחו שהאיבר הניטרלי לחיבור הוא יחיד.

הוכחה. נניח שיש שני איברים ניטרליים לחיבור, $0_1, 0_2 \in \mathbb{F}$, ונוכיח שהם שווים. נסתכל על $0_1 + 0_2$:

$$0_1 \overset{0_2 \text{ is neutral}}{=} 0_1 + 0_2 \overset{0_1 \text{ is neutral}}{=} 0_2$$

כדרוש. $\square$

קבוצת המספרים השלמים מודולו n

הגדרה 2.8. לאורך הדיון להלן, $n \geq 2$ יהיה מספר טבעי. **קבוצת המספרים השלמים מודולו n** היא הקבוצה

$$\mathbb{Z}_n = \left\{\overline{0}, \overline{1}, \ldots, \overline{n-1}\right\}$$

לכל $m \in \mathbb{Z}$, נגדיר את $\overline{m}$ כך: אם r היא שארית החלוקה של m ב-n, אזי $\overline{m} = \overline{r}$.
מגדירים פעולות על $\mathbb{Z}_n$ מגדירים באופן הכי טבעי שאפשר: לכל $\overline{m}, \overline{k} \in \mathbb{Z}_n$ נגדיר

$$\begin{aligned} \overline{m} + \overline{k} &= \overline{m+k} \\ \overline{m} \cdot \overline{k} &= \overline{m \cdot k} \end{aligned}$$

דוגמה 2.9. נציג דוגמאות לחישובים ב-$\mathbb{Z}_n$:

1. עבור $n = 9$,

$$\begin{aligned} \overline{3} + \overline{4} &= \overline{7} \\ \overline{3} \cdot \overline{2} &= \overline{6} \\ \overline{3} \cdot \overline{4} &= \overline{12} = \overline{3} \end{aligned}$$

2. עבור $n = 11$,

$$\begin{aligned} \overline{3} \cdot \overline{4} &= \overline{12} = \overline{1} \\ \overline{7} + \overline{9} &= \overline{16} = \overline{5} \end{aligned}$$

לאחר עבודה מתישה, מקבלים את המשפט הבא:

משפט 2.10. $(\mathbb{Z}_n, +, \cdot)$ שדה אם ורק אם n ראשוני.

הגדרה 2.11. תהי R קבוצה. איבר $0 \neq a \in R$ נקרא **מחלק אפס**, אם קיים איבר $0 \neq b \in R$ שעבורו $a \cdot b = 0$.

טענה 2.12 (מההרצאה). בשדה אין מחלקי אפס.

דוגמה 2.13. ב-$\mathbb{Z}_{200}$, אנחנו יודעים ש-$\overline{2}\cdot\overline{100}=\overline{200}=\overline{0}$, וברור $\overline{2},\overline{100}\neq 0$. קיבלנו שיש מחלקי אפס, ולכן $\mathbb{Z}_{200}$ הוא לא שדה. באופן דומה מוכיחים שלכל n פריק, $\mathbb{Z}_n$ אינו שדה.

הערה 2.14. יהי p ראשוני. נסתכל על $\mathbb{Z}_p$ כשדה:

1. איבר היחידה החיבורי הוא $\overline{0}$.
2. איבר היחידה הכפלי הוא $\overline{1}$.
3. הנגדי של איבר $\overline{m}\in\mathbb{Z}_p$ הוא $\overline{-m}=\overline{p-m}$.
4. אם $a,k\in\mathbb{Z}$ מקיימים $a\cdot m+k\cdot p=1$, אזי $\overline{m}^{-1}=\overline{k}$ ב-$\mathbb{Z}_p$.
באופן כללי, יש שיטה למציאת k; בקורס הזה מספיק ניסוי וטעייה.

תרגיל 2.15.

1. מצאו את ההופכי של $\overline{5}$ ב-$\mathbb{Z}_7$.
2. מצאו את ההופכי של $\overline{5}$ ב-$\mathbb{Z}_{11}$.
3. מצאו את ההופכי של $\overline{3}$ ב-$\mathbb{Z}_{11}$.

פתרון.

1. ב-$\mathbb{Z}_7$, $\overline{5}^{-1}=\overline{3}$.
2. ב-$\mathbb{Z}_{11}$, $\overline{5}^{-1}=\overline{9}$.
3. ב-$\mathbb{Z}_{11}$, $\overline{3}^{-1}=\overline{4}$.

תרגיל 2.16. פתרו את המשוואה $\overline{3}\cdot x+\overline{6}=\overline{5}$ מעל $\mathbb{Z}_{11}$ ומעל $\mathbb{Z}_3$.

פתרון.

1. מעל $\mathbb{Z}_{11}$: קודם מעבירים את $\overline{6}$ אגף, ומקבלים

$$\overline{3}\cdot x=\overline{5}-\overline{6}=\overline{5-6}=\overline{-1}=\overline{10}$$

כעת, רוצים לכפול בהופכי של $\overline{3}$, כדי שבאגף ימין נקבל x $\overline{1}\cdot x=x$. לפי התרגיל הקודם, ההופכי הוא $\overline{4}$, ולכן

$$x=\overline{1}\cdot x=\overline{12}\cdot x=\overline{4}\cdot\overline{3}\cdot x=\overline{4}\cdot\overline{10}=\overline{40}=\overline{7}$$

כלומר הפתרון הוא $x=\overline{7}$.

2. מעל $\mathbb{Z}_3$: כאן $\overline{0}=\overline{6}=\overline{3}$ ו-$\overline{2}=\overline{5}$, ולכן המשוואה היא

$$\overline{0}=\overline{0}\cdot x+\overline{0}=\overline{2}$$

קיבלנו סתירה, ולכן אין פתרון.

תת-שדה

הגדרה 2.17. יהי $\mathbb{F}$ שדה. תת-קבוצה $\mathbb{H} \subseteq \mathbb{F}$ נקראת **תת-שדה** של $\mathbb{F}$, אם $\mathbb{H}$ שדה ביחס לאותן פעולות כמו של $\mathbb{F}$.

דוגמה 2.18. $\mathbb{Q}$ תת-שדה של $\mathbb{R}$, שהוא תת-שדה של $\mathbb{C}$.
אבל $\mathbb{Z}_p$ אינו תת-שדה של $\mathbb{R}$, כי ב-$\mathbb{R}$, $1 + (p-1) = p$, אבל ב-$\mathbb{Z}_p$, $\bar{1} + \overline{p-1} = \bar{0}$.

טענה 2.19 (קריטריון מקוצר לתת-שדה). תהי $\mathbb{H} \subseteq \mathbb{F}$ תת-קבוצה. אזי $\mathbb{H}$ תת-שדה של $\mathbb{F}$ אם ורק אם התנאים הבאים מתקיימים:

1. $1_{\mathbb{F}} \in \mathbb{H}$.
2. לכל $a, b \in \mathbb{H}$ מתקיים $a -_{\mathbb{F}} b \in \mathbb{H}$.
3. לכל $a, b \in \mathbb{H}$ כך ש-$b \neq 0_{\mathbb{F}}$, מתקיים $a \cdot b^{-1} \in \mathbb{H}$.

תרגיל 2.20. נגדיר את הקבוצה $\mathbb{Q}\left[\sqrt{2}\right] = \left\{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\right\}$. הוכיחו ש-$\mathbb{Q}\left[\sqrt{2}\right]$ תת-שדה של $\mathbb{R}$.

הוכחה. ניעזר בקריטריון המקוצר.

1. ראשית, $1 = 1 + 0 \cdot \sqrt{2}$, ולכן $1 \in \mathbb{Q}\left[\sqrt{2}\right]$.
2. אם $a + b\sqrt{2}, c + d\sqrt{2} \in \mathbb{Q}\left[\sqrt{2}\right]$, אז בבירור

$$\left(a + b\sqrt{2}\right) - \left(c + d\sqrt{2}\right) = (a-c) + (b-d)\sqrt{2} \in \mathbb{Q}\left[\sqrt{2}\right]$$

3. כעת, נניח $a + b\sqrt{2}, c + d\sqrt{2} \in \mathbb{Q}\left[\sqrt{2}\right]$, ונניח $c + d\sqrt{2} \neq 0$.
ניעזר בטריק דומה למרוכבים – ולכן נקרא לו "כפל בצמוד":

$$\begin{aligned}\frac{a + b\sqrt{2}}{c + d\sqrt{2}} &= \frac{a + b\sqrt{2}}{c + d\sqrt{2}} \cdot \frac{c - d\sqrt{2}}{c - d\sqrt{2}} = \frac{ac - ad\sqrt{2} + bc\sqrt{2} - 2bd}{c^2 - 2d^2} = \\ &= \frac{ac - 2bd}{c^2 - 2d^2} + \frac{bc - ad}{c^2 - 2d^2}\sqrt{2} \in \mathbb{Q}\left[\sqrt{2}\right]\end{aligned}$$

כדי להצדיק את העובדה שכפלנו וחילקנו ב-$c - d\sqrt{2}$, צריך להוכיח כי לא יכול להיות ש-$c - d\sqrt{2} = 0$. נניח בשלילה שאכן $c - d\sqrt{2} = 0$. אם $d \neq 0$, אז $\sqrt{2} = \frac{c}{d} \in \mathbb{Q}$, בסתירה (הרי $\sqrt{2} \notin \mathbb{Q}$). לכן $d = 0$, ומכאן שגם $c = 0$. אז $c + d\sqrt{2} = 0$, בסתירה להנחה מתחילת הסעיף.

לפי הקריטריון המקוצר לתת-שדה, $\mathbb{Q}\left[\sqrt{2}\right]$ הוא תת-שדה של $\mathbb{R}$.

$\square$

המאפיין של שדה

הגדרה 2.21. יהי $\mathbb{F}$ שדה. **המאפיין** של $\mathbb{F}$, מסומן $\operatorname{char}\left(\mathbb{F}\right)$, הינו מספר הפעמים הקטן ביותר שצריך להוסיף את $1_{\mathbb{F}}$ לעצמו עד שמקבלים $0_{\mathbb{F}}$. אם אין מספר כזה, מגדירים $\operatorname{char}\left(\mathbb{F}\right)=0$.

דוגמה 2.22.

1. $\operatorname{char}\left(\mathbb{Q}\right)=\operatorname{char}\left(\mathbb{R}\right)=\operatorname{char}\left(\mathbb{C}\right)=0$.
2. $\operatorname{char}\left(\mathbb{Z}_{p}\right)=p$.

משפט 2.23. יהי $\mathbb{F}$ שדה. אזי $\operatorname{char}\left(\mathbb{F}\right)=0$ או ש-$\operatorname{char}\left(\mathbb{F}\right)$ ראשוני.