

תרגול מס' 11 במבנים אלגבריים 1

יישומים בקריפטוגרפיה למשפט לגרנז'.

טענה: לכל מספר ראשוני p החוג: $\mathbb{F}_p = (\mathbb{Z}_p, +(\text{mod } p), \cdot(\text{mod } p))$ הוא שדה סופי מסדר p .

הרחבה של \mathbb{F}_p ממימד $n \in \mathbb{N}$ מתבצעת ע"י הוספת שורש $\alpha \notin \mathbb{F}_p$ של פולינום אי-פריק מעל \mathbb{F}_p (כלומר שהמקדמים הם מהשדה הזה) ממעלה $n \in \mathbb{N}$. התוצאה $k = \mathbb{F}_p(\alpha)$ היא שדה סופי מסדר $q = p^n$ שניתן לסמן אותו ע"י \mathbb{F}_q (כל ההרחבות מאותו מימד איזומורפיות ולכן α לא חשוב עד כדי איזומורפיזם).

המספר p (לכל שדה $\mathbb{F}_{q=p^n}$) נקרא **המאפיין** $\text{char}(\mathbb{F}_q)$ של השדה, כלומר המספר המינימלי המקיים:

$$\underbrace{1+1+\dots+1}_{p \text{ times}} \equiv 0 \quad \text{עבור } \mathbb{Q}, \mathbb{R} \text{ אומרים שהמאפיין הוא אפס.}$$

טענה: החבורה הכפולית $\mathbb{F}_q^\times = \mathbb{F}_q - \{0\}$ היא ציקלית.

דוגמאות:

1. $\mathbb{F}_{13}^\times = \{1, 2, \dots, 12\} = \langle 2 \rangle$ ציקלית מסדר 12.

2. השדה $k = \mathbb{F}_3(i) = \mathbb{F}_9$ כאשר i הוא שורש הפולינום $x^2 + 1$ היא הרחבה ממימד 2:

$$k = \{a + ib : a, b \in \mathbb{F}_3\} \quad \text{מסדר: } 3^2 = 9.$$

זו לא תהיה הרחבה מעל \mathbb{F}_5 שכן הפולינום הזה מתפצל מעל \mathbb{F}_5 : $x^2 + 1 = (x-2)(x+2)$.

כלומר שני השורשים 2,3 שייכים כבר ממילא ל- \mathbb{F}_5 .

גם כאן החבורה הכפולית היא ציקלית: $k^\times = \langle i-1 \rangle$, והיא מסדר 8.

תשע"ד מועד א': אילו מן השדות הסופיים הבאים מכילים איבר x כך ש: $x^4 + 1 = 0$:

א. \mathbb{F}_2 ב. \mathbb{F}_9 ג. \mathbb{F}_7 ד. \mathbb{F}_2 וגם \mathbb{F}_9 ה. \mathbb{F}_2 וגם \mathbb{F}_7 ו. כל שלושת השדות האלה.

פתרון: תשובה ד.

בעיית הלוג הדיסקרטי: Discrete Log Problem (DLP)

בהינתן מספרים טבעיים: $1 < g < n$ ו- $g^x \pmod n$, קשה (=סיבוכיות זמן ריצה תת-אקספוננציאלית) למצוא את x .

אלגוריתם הצפנה Diffie-Hellman (1976)

ניעזר בחבורת מספרים טבעיים ציקלית כיפולית $G = \langle g \rangle$ בה $n = |G|$, מספרים טבעיים ידועים לכולם. השימוש הנפוץ הוא בחבורה הציקלית $G = U_p = \mathbb{F}_p^\times = \{1, 2, 3, \dots, p-1\}$ עבור מספר ראשוני p מספיק גדול (לפחות 100 ספרות בינאריות).

לכל משתמש ברשת יש מפתח פרטי סודי: מספר טבעי $a \in [2, n-1]$ ומפתח ציבורי $g^a \pmod n$. כך יכולים שני משתמשים ברשת פומבית, לתאם ביניהם מפתח הצפנה שיהיה ידוע רק להם.

אלגוריתם:

- אליס שולחת לבוב את המפתח הפומבי שלה.
 - בוב מחשב את מפתח ההצפנה $(g^a)^b = g^{ab}$ ואת מפתח הפענוח: $(g^a)^{-b} = g^{-ab}$ לשחזור.
 - אותו התהליך מתרחש בכיוון ההפוך אצל אליס.
- קעת שניהם יציפו הודעות ע"י מכפלה ב- g^{ab} ויפענחו ע"י מכפלה ב- g^{-ab} .

הערות:

1. סודיות המפתח הפרטי של שניהם לא נפגמה.
2. רק אליס יכלה מתוך המפתח הציבורי של בוב לחשב את המפתח המשותף ולהיפך.
3. שיטה זו היא **סימטרית**: אם ניתן לחשב את מפתח ההצפנה, אז ניתן לחשב את מפתח הפענוח.
4. חסרון: כל אחד יכול להתחזות להיות אליס או בוב או אפילו לעבוד מול שניהם בהתחזות כפולה (Man in the middle attack).

חבורות מעל שדות סופיים

תרגיל: הראה כי $\text{GL}_2(\mathbb{Z}_2) \cong D_3 = S_3$.

פתרון: מראים ש: $\text{GL}_2(\mathbb{Z}_2) = \langle a, b : a^3 = b^2 = 1, ab = ba^2 \rangle$.

תרגיל: הראה כי: $G = \left\{ \begin{pmatrix} x & y \\ 0 & 1 \end{pmatrix} : x, y \in \mathbb{F}_q, x \neq 0 \right\}$ יחד עם פעולת מכפלת מטריצות היא חבורה

וחשב את גודלה ואת מרכזה.

פתרון:

האסוציאטיביות נורשת ממכפלת מטריצות. כמו כן היחידה שייכת, את הסגירות קל לבדוק וההופכי של

הוא $\begin{pmatrix} x & y \\ 0 & 1 \end{pmatrix}$, כלומר שייך לחבורה. $\begin{pmatrix} x^{-1} & -\frac{y}{x} \\ 0 & 1 \end{pmatrix}$

גודל החבורה הוא $q(q-1)$. קל לבדוק שהמרכז כאן הוא טריוויאלי.