

# סיבוכיות

© ארזים

14 במרץ 2017

## 1 שדות סופיים

טענה 1.1 יהי  $p$  ראשוני. הקבוצה

$$\mathbb{Z}_p = \{0, 1, \dots, p-1\}$$

היא שדה ביחס לחיבור וכפל מודולו  $p$ .

**הוכחה:** ברור שהחיבור והכפל אסוציאטיביים, קומוטטיביים. דיסטריבוטיביות גם כן מתקיימת. 0 הוא אדיש לחיבור, 1 אדיש לכפל.

הנגדי של מספר  $a$  הוא  $p-a$ . נותר להוכיח כי לכל  $a \neq 0$  יש הופכי ביחס לכפל. יהי  $a \neq 0$ . נגדיר פונקציה  $f_a : \mathbb{Z}_p \rightarrow \mathbb{Z}_p$  באופן הבא:

$$f_a(x) = ax \pmod{p}$$

נרצה להוכיח כי  $1 \in \text{Im}(f_a)$ . נוכיח כי הפונקציה היא על  $\mathbb{Z}_p$ . לשם כך, מספיק להראות כי היא חד-חד-ערכית, שכן  $\mathbb{Z}_p$  קבוצה סופית. יהיו  $x, y \in \mathbb{Z}_p$  כך שמתקיים

$$f_a(x) = f_a(y)$$

נראה כי  $x = y$ .

$$ax = ay \pmod{p}$$

$$ax - ay = a(x - y) = 0 \pmod{p}$$

לכן  $p$  מחלק את  $ax - ay$  שמהלך. כעת,  $p$  ראשוני, ולכן מחלק את  $a$  או את  $x - y$ . לא יכול לחלק את  $a$ , שכן  $a \neq 0$  בתוך  $\mathbb{Z}_p$ . מכאן, נקבל כי  $p$  מחלק את  $x - y$ . כלומר

$$x - y = 0 \pmod{p}$$

$$x = y \pmod{p}$$

שניהם מתוך  $\mathbb{Z}_p$ , ולכן  $x = y$ . הראינו כי הפונקציה שלנו חד-חד-ערכית, ועל כן היא על - בפרט היא משיגה את 1, ולכן יש הופכי עבור  $a$ . ■

**הערה 1.2** נביט בבעיה החישובית הבאה: בהינתן זוג  $(a, p)$ , נרצה אלגוריתם שמוצא את  $a^{-1}$ . ההוכחה שלעיל נותנת אלגוריתם נאיבי שמבצע פעולות כפל (כופלים את  $a$  בכל איבר של  $\mathbb{Z}_p$  ומחפשים את ההופכי). זה זמן ריצה אקספוננציאלי באורך הקלט.

**הערה 1.3** אם  $n$  פריק, אזי  $\mathbb{Z}_n$  לא שדה. אפשר להראות כי אם  $a, n$  זרים, כלומר  $\gcd(a, n) = 1$ , אזי יש הופכי עבור  $a$  מודולו  $n$  (ההוכחה דומה להוכחת הטענה). מסמנים

$$\mathbb{Z}_n^* = \{a \in \mathbb{Z}_n \mid \gcd(a, n) = 1\}$$

**הגדרה 1.4** חבורה אבלית היא קבוצה  $G$  שעליה מוגדרת פעולה בשם כפל, שמסומנת  $\cdot$  (לאו דווקא כפל רגיל), שמקיימת את התכונות הבאות:

1.

$$\forall a, b, c \in G \quad a(bc) = (ab)c$$

2.

$$\exists e \in G \forall a \in G \quad ae = ea = a$$

3.

$$\forall a \in G \exists b \in G \quad ab = ba = e$$

4.

$$\forall a, b \in G \quad ab = ba$$

**דוגמאות**  $\mathbb{Z}_n$  חבורה אבלית ביחס לפעולת החיבור.  $\mathbb{Z}_n^*$  חבורה אבלית ביחס לכפל.

**הגדרה 1.5** חבורה  $G$  נקראת ציקלית אם יש  $g \in G$  המקיים

$$G = \{g^k \mid k \in \mathbb{Z}\}$$

**דוגמא**  $\mathbb{Z}_n$  ציקלית, וכן  $\mathbb{Z}$  - שתיהן נוצרות על ידי 1. גם  $\mathbb{Z}_p^*$  ציקלית, אבל זה מסובך יותר.

**הגדרה 1.6** יהי  $\mathbb{F}$  שדה. מרחב ווקטורי  $V$  מעל  $\mathbb{F}$  הוא חבורה אבלית (שנסמן את הפעולה שלה  $+$ , ונקרא לה חיבור) שעליו מוגדרת פונקציה

$$\lambda : \mathbb{F} \times V \rightarrow V$$

שנקראת כפל בסקלר. מסמנים

$$\lambda(a, v) = av$$

הכפל בסקלר צריך לקיים:

.1

$$\forall a, b \in \mathbb{F}, v \in V \quad (ab)v = a(bv)$$

.2

$$\forall v \in V \quad 1 \cdot v = v$$

.3

$$\forall a \in \mathbb{F}, u, v \in V \quad a(u + v) = au + av$$

.4

$$\forall a, b \in \mathbb{F}, v \in V \quad (a + b)v = av + bv$$

באלגברה ליניארית מוכיחים כי לכל מרחב ווקטורי  $V$  מעל  $\mathbb{F}$  יש בסיס (קבוצה פורשת ובלתי תלויה ליניארית) ומימד (הגודל של בסיס). מוכיחים גם שאם  $V$  מרחב ווקטורי מעל  $\mathbb{F}$  ממימד  $k$ ,  $V \cong \mathbb{F}^k$ .

**טענה 1.7** יהי  $V$  מרחב ווקטורי מעל  $\mathbb{Z}_p$  ממימד  $k$ . אזי  $|V| = p^k$ .

**הוכחה:** יהי  $B = \{v_1, \dots, v_k\}$  בסיס של  $V$  מעל  $\mathbb{Z}_p$ . אזי

$$V = \text{span} B = \left\{ \sum_{i=1}^k a_i v_i \mid a_i \in \mathbb{Z}_p \right\}$$

בנוסף, כל צירוף לינארי שכזה הוא שונה, כלומר לכל  $v \in V$  יש ייצוג יחיד שכזה. זאת משום שמתקיים

$$\begin{aligned} \sum a_i v_i &= \sum b_i v_i \\ \sum (a_i - b_i) v_i &= 0 \end{aligned}$$

ואז  $a_i = b_i$  לכל  $i$ , שכן  $B$  בסיס, ובפרט בלתי תלוי לינארית. יש אפשרויות עבור  $a_i$ , ולכן  $|V| = p^k$ . ■

**הגדרה 1.8** יהי  $\mathbb{F}$  שדה. המצייץ של  $\mathbb{F}$ , שמשומן  $\text{char}\mathbb{F}$ , הוא המספר המינימלי  $p$  עבורו

$$\underbrace{1 + 1 + \dots + 1}_p = 0$$

אם אין כזה אומרים שהמצייץ הוא 0.

**הערה 1.9** אם  $\text{char}\mathbb{F} = p > 0$  אזי  $\mathbb{Z}_p$  הוא תת שדה של  $\mathbb{F}$  (המצייץ תמיד ראשוני או 0).

**טענה 1.10** יהי  $\mathbb{F}$  שדה סופי. אזי קיימים מספר ראשוני  $p$  ושלים חיובי  $k$  עבורם  $|\mathbb{F}| = p^k$ .

**הוכחה:** יהי  $\text{char}\mathbb{F} = p$ . כיוון שלקחנו  $\mathbb{F}$  סופי, אזי  $p > 0$ , ואז  $\mathbb{Z}_p$  תת שדה. לכן נותר רק להראות כי  $\mathbb{F}$  הוא מרחב ווקטורי סוף מימדי מעל  $\mathbb{Z}_p$ . ברור כי  $\mathbb{F}$  חבורה אבלית. את הכפל בסקלר נגדיר לפי הכפל של השדה  $\mathbb{F}$ . פשוט לראות את האקסיומות של מרחב ווקטורי. המימד של  $\mathbb{F}$  מעל  $\mathbb{Z}_p$  סופי, שוב, כי  $\mathbb{F}$  סופי, ונסמנו  $k$ . מהטענה הקודמת,  $|\mathbb{F}| = p^k$ . ■