

עוד מעט על השדות: שדה השאריות

1. חיבור וכפל של שאריות. תכונה מיוחדת של מספרם שלמים: קיום חילוק עם שארית. נקבע מספר שלם $n > 0$. אזי

את כל מספר שלם x ניתן לרשום בצורה $x = qn + r$ כאשר השארית r הוא ב- $\{0, 1, \dots, n-1\}$.

נסמן שארית של מספר שלם x בחילוק ב- n (אומרים גם: מודולו n) ע"י $res_n(x)$ או פשוט $res(x)$.

נגדור פעולות עם שאריות ע"י הנוסחאות

$$a \oplus b = res(a + b)$$

$$a \otimes b = res(a \cdot b)$$

2. למה. לכל מספרים שלמים x, y מתקיים

$$res(x + y) = res(x) \oplus res(y)$$

$$res(x \cdot y) = res(x) \otimes res(y)$$

הוכחה. יהיו $a = res(x)$, $b = res(y)$. זה אומר כי $x = qn + a$, $y = pn + b$. אזי $x + y = (q + p)n + (a + b)$ וזה גורר כי $res(x + y) = res(a + b) = a \oplus b$. יתר על כן, $xy = (qb + pa + qpn)n + ab$, וזה גורר כי $res(xy) = res(ab) = a \otimes b$. סוף ההוכחה.

3. אוסף שאריות מודולו n , יחד עם פעולות חיבור וכפל המוגדרים דלעיל, מסמנים Z_n . זה לא תמיד שדה. למשל, האיבר $2 \in Z_4$ לא הפיך (בדקו זאת). נזכיר

הגדרה. מספר שלם p נקרא ראשוני (prime) אם התכונה הבאה מתקיימת. אם a, b שלמים ו- $a \cdot b$ מתחלקת ב- p אז אחד מ- a, b מתחלק ב- p . דוגמאות. $2, 3, 5, -7$ ראשוניים. 4 לא ראשוני.

4. למה. אם F שדה, $a, b \in F$, $ab = 0$, $a \neq 0$, אז בהכרח $b = 0$. הוכחה. ואמנם, נכפיל את שני האגפכם של $ab = 0$ ב- a^{-1} . נקבל $0 = a^{-1}(ab) = (a^{-1}a)b = b$.

5. טענה. אם מספר n לא ראשוני, אז Z_n לא שדה. ואמנם, אם n לא ראשוני, קיימים a, b כך ש- ab מתחלק ב- n אך a, b לא מתחלקים ב- n . זה אומר כי $res(a)res(b) = 0$ למרות ש- $res(a) \neq 0$, $res(b) \neq 0$.

6. נוכיח עתה כי Z_p שדה כאשר p ראשוני.

קודם כל, עבור כל מספר שלם n פעולות חיבור וכפל ב- Z_n מקיימות כל תכונות של שדה פרט לקיום הופכי.

לכן, עלינו לוודא כי כל איבר השונה מאפס ב- Z_p (p ראשוני) הפיך.

יהי $x \in Z_p, x \neq 0$.

נתבונן ב- $(p-1)$ כפולות של x : $x, 2x, \dots, (p-1)x$. אילו שניים מהם היו זהים, זה היה אומר כי $i \cdot x = j \cdot x$ עבור $i < j$. אזי היינו מקבלים $(j-i)x = 0$ וזה דבר בלתי-אפשרי.

לכן, הכפולות $x, 2x, \dots, (p-1)x$ מקבלים $p-1$ ערכים שונים שהם כל השאריות השונות מאפס. זה גורר כי אחד הערכים האלה הוא 1. המשפט הוכח.

יש משורת לסמן את שדה השאריות מודולו p ב- F_p .

7. אופיין של שדה.

יהי F שדה.

אם $x \in F$, מתקיים

$$\underbrace{x + \dots + x}_n = \underbrace{(1 + \dots + 1)}_n x$$

לכן, עבור מספר טבעי n כדאי להגדיר איבר שדה F הנקרא n ע"י הנוסחה

$$n = \underbrace{1 + \dots + 1}_n$$

האיברים החדשים שהגדרנו מקיימים את התכונה הנעימה $n \cdot m = nm$ – הם מוכפלים כמו מספרים טבעיים רגילים.

אפשר גם להמשיך ולהגדיר את איברי השדה המתאימים למספרים שלמים שליליים:

$$-n = \underbrace{(-1) + \dots + (-1)}_n$$

איברי השדה $0, 1, 2, \dots$ לא חייבים להיות כולם שונים ב- F . למשל, עבור $F = F_2$

$$0 = 2 = 4 = \dots, \quad 1 = 3 = 5 = \dots$$

הגדרה. אם כל איברי השדה $0, 1, 2, 3, \dots$ שונים, אומרים כי השדה בעל אופיין 0 (וכותבים

$char F = 0$). אחרת אופיין של שדה הוא המספר הטבעי n הקטן ביותר כך ש- $n = 0$ ב- F .

למה. אופיין של שדה הוא 0 או מספר ראשוני.

ואמנם, אם $char F = pq$ אז $p, q \neq 0$, כאיברי שדה, אך מכפלתם שווה לאפס.

אם השדה F בעל אופיין p אז האיברים $0, 1, \dots, p-1$ של שדה מהווים שדה ביחס לפעולות

חיבור וכפל של השדה. שדה זה איזומורפי ל- F_p .

8. המשפט הבא הוכח ע"י גלואה (Evariste Galois, 1811-1832):

משפט.

1. יהי F שדה סופי בעל אופיין p . אזי מספר איברים בו חיזקה של p .

2. יהי $q = p^n$. קיים ויחיד עד כדי איזומורפיזם שדה סופי בן q איברים.

החלק הראשון של המשפט פשוט מאוד – נוכל להוכיח אותו בעוד שני שיעורים.

החלק השני יותר עמוק.

מקובל לסמן ב- F_q את השדה היחיד בן q איברים.