שדות

# הגדרה

שדה הוא קבוצה עם פעולות חיבור וכפל(לאו דווקא החיבור והכפל הרגילים) המקיימות את התכונות הבאות:

1. סגירות:
2. חילוף:
3. קיבוץ:
4. איברים ניטרליים: קיימים כך ש
5. איבר הופכי ונגדי: לכל קיים כך ש, קיים כך ש
6. פילוג:

# תרגיל 1.3

יהי שדה, הוכיחו את התכונות הבאות:

1. (פעולה זו נקראת צמצום)  
   הוכחה: נתון נכפיל ב ונקבל
2. הוכחה: נוסיף לשני האגפים את (קיים לפי התכונות):
3. הוכחה: יהי אזי קיים כך ש. נוסיף לאגפים . נקבל
4. הוכחה: הטענה שקולה ל
5. הוכחה: נראה ש. לפי סעיף ז .  
   נחזור להוכחת הטענה: ab

# תרגיל

הוכיחו כי האיבר הניטרלי ביחס לחיבור הינו יחיד

## הוכחה

נניח בשלילה שקיימים שונים. מתקיים – סתירה

# תרגיל 2.3

1. הוכיחו אי אינו שדה (ביחס לפעולה המושרית מ)  
   פתרון: יהי . לכן . קיים לa נגדי יחיד שהוא –a, אבל (ע"פ הגדרת )

# הגדרה

נסמן ב את קבוצת האיברים כאשר מוגדרת עליהם פעולת מודולו(modulo):

למשל :

# הגדרה

איבר (F אינו בהכרח שדה) נקרא "מחלק אפס" אם כך ש או

למשל בדוגמה הקודמת 2 הוא "מחלק אפס"

# תרגיל

הוכיחו שבשדה אין מחלקי אפס

## הוכחה

נניח בשדה קיים מחלק אפס. אזי שונים מ0 כך ש. נכפול את המשוואה ב(b הוא לא 0 לכן יש ). נקבל וזה בסתירה להנחה.

# תרגיל 2.3 סעיף ג'

הוכיחו ש אינו שדה עבור n פריק.

## הוכחה:

n פריק ולכן קיימים כך ש ואז נקבל ולכן עבור יש מחלקי אפס והוא לא שדה.

תת שדה

# קריטריון מקוצר לתת שדה

נאמר ש הואר תת שדה של אם וגם שדה בעצמו ביחס לפעולות מ.

מספיק להוכיח את התכונות הבאות:

1. עבור מתקיים

# תרגיל 2.6

הסביר מדוע (p ראשוני) אינו תת שדה של

## הסבר

למשל עבור נקבל , אבל , לכן לא מתקיימת סגירות

מורכבים

# הגדרה

# תרגיל

נשנה את פעולת הכפל ב ל . האם נשאר שדה?

תשובה: ממש לא! => אבל כלומר ל יש מחלקי אפס ולכן הוא כבר לא שדה

# הגדרה

המאפיין של שדה מסומן ב והוא מספר הקטן ביותר כך ש

אם אין מספר כזה אז נאמר שהמאפיין הוא 0.

המאפיין הוא או 0 או ראשוני

# תרגיל

בנו שדה בגודל 4 וחשבו את המאפיין שלו

# פתרון

נבנה טבלאות חיבור וכפל.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| \* | 0 | 1 | a | b |
| 0 | **0** | **0** | **0** | **0** |
| 1 | **0** | **1** | **a** | **b** |
| a | **0** | **a** | b | 1 |
| b | **0** | **b** | 1 | a |

פרט למכפלות 0 לא יתכן שמספר יחזור על עצמו. הסבר: אם למשל נקבל ע"פ צמצום

המודגשים הם לפי ההגדרות שכן אז אבל , לכן ואת שאר טבלת הכפל משלימים לפי האפשרויות שנשארו.

נראה ש: נניח בשלילה ש:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| + | 0 | 1 | a | b |
| 0 | **0** | **1** | **a** | **b** |
| 1 | **1** | a | b | 0 |
| a | **a** | b | 0 | 1 |
| b | **b** | 0 | 1 | a |

אבל אז . אותו דבר לגבי :

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| + | 0 | 1 | a | b |
| 0 | **0** | **1** | **a** | **b** |
| 1 | **1** | b | 0 | a |
| a | **a** | 0 | b | 1 |
| b | **b** | a | 1 | 0 |