שדה - הגדרה:

שדה הוא קבוצה F עם שתי פעולות שתסומנה ע"י $+$ (חיבור) ו $\square$ (כפל) שמקיימות:

1. סגירות לחיבור: $a+b\in F \Leftarrow \square a,b \square F$.
2. קומוטטיביות (חילוף בחיבור): $a+b=b+a \Leftarrow \square a,b \square F$
3. אסוציאטיביות (קיבוץ בחיבור): $(a+b)+c=a+(b+c) \Leftarrow \square a,b,c \square F$.
4. קיום איבר נייטרלי לחיבור: קיים $0 \square F$ כך שלכל $a\in F$ מתקיים: $a+0=a$
5. קיום איבר נגדי: לכל $a\in F$ קיים איבר נגדי שיסומן ע"י $-a$ וגם $-a\in F$, כך שמתקיים $a+(-a)=0$.
6. סגירות לכפל: $a\cdot b\in F \Leftarrow : \square a,b \square F$.
7. אסוציאטיביות (קיבוץ בכפל): $(a\cdot b)\cdot c=a\cdot(b\cdot c) \Leftarrow \square a,b,c \square F$.
8. קומוטטיביות (חילוף בכפל): $a\cdot b=b\cdot a \Leftarrow \square a,b \square F$.
9. קיום איבר יחידה ב- F שיסומן ע"י 1 והמקיים: $a\cdot 1=a$ לכל $a\in F$.
10. לכל $a\in F$ קיים איבר הופכי ב- F שיסומן ב- a^{-1} ומקיים: $a\cdot a^{-1}=1$ $(a\neq 0)$.
11. דיסטריבוטיביות: $a\cdot(b+c)=a\cdot b+a\cdot c \Leftarrow a,b,c\in F$.

<u>משפט- תכונות של שדה (חלק קטן):</u>

אם F שדה, אז:

1. איבר האפס הוא יחיד.
2. איבר היחידה הוא יחיד
3. הנגדי יחיד
4. ההופכי יחיד
5. $a\cdot 0=0 \Leftarrow a\in F$.
6. $-1\cdot a=-a$
7. $-(-a)=a$
8. $-(ab)=(-a)b=a(-b)$
9. $(a^{-1})^{-1}=a$
10. $-(a+b)=-a+-b$
11. $(ab)^{-1}=a^{-1}b^{-1}$
12. $a,b\in F$ ו- $ab=0 \Leftarrow a=0 \ or \ b=0$.

חשבון מודולו n

שני כללים חשובים:

1. $(a+b)(\bmod n)=\left[a(\bmod n)+b(\bmod n)\right](\bmod n)$.
2. $(a\cdot b)(\bmod n)=\left[a(\bmod n)\cdot b(\bmod n)\right](\bmod n)$.

כיצד לבדוק ש- Z_n הוא שדה?

מספיק לבדוק קיום a^{-1}, זאת כי כל שאר הסעיפים בהכרח מתקיימים.

<u>משפט:</u>

$a\in Z_n$ $(a\neq 0)$ אז a הפיך לגבי כפל מודולו n אמ"מ a זר ל-n (ל-a ול-n אין גורמים משותפים).

<u>מסקנה:</u>

Z_n הוא שדה אמ"מ המספר n הוא ראשוני.