$* \; 0_R$

אם יש יחידה כפלית 1_R (שאז $(R,\cdot)$ מונואיד) נאמר שהחוג עם יחידה.

אם הכפל קומוטטיבי, נאמר שהחוג קומוטטיבי.

אם יש יחידה 1_R וגם הפכי (לכפל) לכל איבר $0_R \neq a \in R$ נאמר שזהו חוג חילוק.

$(R^*,\cdot)$ חבורה

$R^* = R \setminus \{0_R\}$

* אם $(R^*,\cdot)$ חבורה קומוטטיבית נאמר ש-R הוא שדה.

סדרי גודל: (O, Ω, Θ)

תהיינה $f,g:\mathbb{N}\to\mathbb{R}_+$ פונקציות.

$\left(\begin{array}{l} \mathbb{N}:=\{1,2,3,\dots\} \text{ מספרים טבעיים} \\ \mathbb{R}_+ := \{x\in\mathbb{R} \mid x>0\} \end{array}\right)$

* נרשום $f(n)=O(g(n))$ (כאשר $n\to\infty$) אם קיים קבוע ממשי $C>0$ ומספר טבעי n_0 כך ש:

$$n \geq n_0 \Rightarrow f(n) \leq C\cdot g(n)$$

בניסוח אחר: עבור n גדול מספיק $\frac{f(n)}{g(n)} \leq C$.

~~* נרשום~~

* נרשום $f(n)=\Omega(g(n))$ (כאשר $n\to\infty$) אם קיים קבוע $C>0$ ומספר טבעי n_0 כך ש-

$$n \geq n_0 \Rightarrow f(n) \geq C\cdot g(n)$$

* $\Theta = O + \Omega$, ז"א: נרשום $f(n)=\Theta(g(n))$ אם קיימים קבועים $0 < C_1 \leq C_2$ ומספר טבעי n_0

$$n \geq n_0 \Rightarrow C_1 g(n) \leq f(n) \leq C_2 \cdot g(n)$$

(ז"א: ל-n גדול מספיק $C_1 \leq \frac{f(n)}{g(n)} \leq C_2$)

הערה:

תנאי יותר חזק מ-Θ הוא כאשר

$$\lim_{n\to\infty} \frac{f(n)}{g(n)} = 1$$

זה מסומן בד"כ

$$f(n) = (1+\underset{\substack{\uparrow \\ \text{או קטן של } 1}}{o(1)})\cdot g(n)$$

(פירושו: פונקציה $\xrightarrow[n\to\infty]{} 0$)

שאלה:

כמה פעולות נדרשות כדי לחבר או להכפיל שני פולינומים?

נניח שהפעולות הבסיסיות הן:
חיבור / כפל של איברים בשדה $\mathbb{F}$.

חיבור פולינומים:

אם $a(x), b(x) \in \mathbb{F}_n[x]$ (ז"א: מעלות $a(x)$, $b(x)$ קטנה ממש מ-n) אז, במקרה הגרוע ביותר, נדרשות n פעולות בסיסיות (חיבור ב-$\mathbb{F}$) לחישוב $a(x)+b(x)$.

כפל פולינומים:

נניח: $a(x), b(x) \in \mathbb{F}_n[x]$,

$$\deg \begin{array}{l} a(x) \\ b(x) \end{array} \leq n-1$$

בגישה הישירה, לפי הגדרה:

$$c_k := \sum_{i+j=k} a_i b_j \qquad 0 \leq k \leq 2(n-1)$$

נדרשים: n^2 פעולות כפל ב-$\mathbb{F}$.

$(n-1)^2$ פעולות חיבור ב-$\mathbb{F}$.

פעולות חיבור

$0 \quad a_0b_0$

$1 \quad a_0b_1 + a_1b_0$

$\vdots$

$n-1 \quad a_0b_{n-1} + \dots + a_{n-1}b_0$

$\vdots \quad \vdots$

$0 \quad a_{n-1}b_{n-1}$

$$\left[\begin{array}{l} 0+1+\dots+(n-1)+(n-2)+\dots+0 = \\ = \frac{n(n-1)}{2} + \frac{(n-2)(n-1)}{2} \\ = \frac{(2n-2)(n-1)}{2} = (n-1)^2 \end{array}\right.$$