תרגול 3

## פולינומים:

יהי $F$ שדה.

$F[X]$ - אוסף כל הפולינומים הפורמליים עם מקדמים מ-$F$

פולינום פורמלי - $a_0, a_1, \ldots$ , $\{a_n\}_{n=0}^{\infty}$ , רק שעבור $N\in\mathbb{N}$

כלשהו, לכל $n>N$ $a_n=0$

כותבים פולינום פורמלי בצורה $a_0+a_1x+\ldots+a_nx^n$

**פעולת הכפל על פולינומים:**

$$\left(\sum_{i=0}^{n} a_i x^i\right)\left(\sum_{j=0}^{m} a_j x^j\right) = \sum_{k=0}^{m+n}\left(\sum_{i+j=k}(a_i b_j)\right)x^k$$

כל פולינום מגדיר פונקציה מ-$F$ ל-$F$, אם $P=\sum_{i=0}^{n} a_i x^i$,

אז הפונקציה המתאימה $T_P: F\to F$, מוגדרת ע"י: $T_P(\alpha)=\sum_{i=0}^{n} a_i \alpha^i$

**תרגיל:** נתון פולינום $\mathbb{Z}[x]\ni f(x)=x^n+a_{n-1}x^{n-1}+\ldots+a_0$,

ונתון שיש לו שורש שלם $b\neq 0$, הוכיחו ש $b|a_0$.

**פתרון:** $b$ שורש של $f$, כלומר, $\underset{\overset{\|}{0}}{f(b)}=b^n+a_{n-1}b^{n-1}+\ldots+a_1b+a_0$

$$\Longleftarrow \quad -(b^n+a_{n-1}b^{n-1}+\ldots+a_1b)=a_0$$

$$-b(b^{n-1}+a_{n-1}b^{n-2}+\ldots+a_1)=a_0$$

$$\Downarrow$$

$$b|a_0$$

**תרגיל:** נתון פולינום $f(x)\in\mathbb{R}[x]$, ונתון שיש לו שורש מרוכב, $z_0$

הראו ש $\bar{z}_0$ הוא גם שורש של הפולינום.

**פתרון:** $f(x)=a_nx^n+a_{n-1}x^{n-1}+\ldots+a_1x+a_0$.

כיוון ש-$z_0$ שורש של $f$, מתקיים ש:

$$0=f(z_0)=a_nz_0^n+a_{n-1}z_0^{n-1}+\ldots+a_1z_0+a_0$$

ניקח צמוד לשני האגפים, $\bar{0}=\overline{a_nz_0^n+\ldots+a_0} =$

$$= \overline{a_nz_0^n}+\overline{a_{n-1}z_0^{n-1}}+\ldots+\overline{a_0}$$

תכונה של צמוד

$$= \overline{a_n}\,\overline{z_0}^{\,n} + \overline{a_{n-1}}\,\overline{z_0}^{\,n-1} + \dots + \overline{a_0} = a_n\overline{z_0}^{\,n} + a_{n-1}\overline{z_0}^{\,n-1} + \dots + a_0 = f(\overline{z_0})$$

שמירה על כפל בצמוד

$a_0,\dots,a_n\in\mathbb{Z}$

**הערה:** באופן כללי, אם $f\in\mathbb{Z}[x]$, ו $z\in\mathbb{C}$ כלשהו,
$$f(\bar z)=\overline{f(z)}$$

**חלוקה עם שארית:**

**משפט:** יהיו $f,g\in F[x]$, ונניח $g\neq 0$. אז קיימים ויחידים $q,r\in F[x]$ כך ש- $f=q\cdot g+r$, $\deg(r)<\deg(q)$ ←
מתקיים תמיד.

**תרגיל:** נבצע חלוקה עם שארית של $f=x^4-x^3-18x+17x+1$
ב $g=x+4$

$$\begin{array}{l}
\quad x^3-5x^2+2x+9 \\
\hline
x^4-x^3-18x^2+17x+1 \;\big|\; x+4 \\
-\;x^4+4x^3 \\
\hline
\quad 0-5x^3 \\
\quad -\;-5x^3-20x^2 \\
\hline
\qquad 0+2x^2 \\
\qquad -\;2x^2+8x \\
\hline
\qquad\quad 0+9x \\
\qquad\quad -\;9x+36 \\
\hline
\qquad\qquad 0-35
\end{array}$$

$$\longrightarrow x^3-5x^2+2x+9-\frac{35}{x+4}$$

**הגדרה-** יהיו $f,g\in F[x]$. נאמר ש $g$ מחלק את $f$. אם קיים $q\in F[x]$ כך ש $f=q\cdot g$ (כלומר, $r=0$), $g|f$.

**הגדרה-** פולינום $f$ נקרא מתוקן אם המקדם העליון בו הוא 1

**דוגמאות-** $x^3+2013$ , $x+17$ ← $2x$ - לא מתוקן.

**תרגיל-** יהיו $f,g\in F[x]$, פולינומים מתוקנים, כך ש- $f|g$ ו- $g|f$.
הראו ש $f=g$.

**פתרון-** מהנתון ש- $g|f$, קיים $q\in F[x]$ כך ש $f=q\cdot g$.
מהנתון ש- $f|g$, קיים $q'\in F[x]$. כך ש $qq'f=f$ $\deg f+\deg qq'=\deg f$

סה"כ: $g = q'\cdot f$

$$\deg(qq')=0 \Downarrow \deg(q)+\deg(q')=0 \Downarrow \deg(q)=\deg(q')=0$$

$\longrightarrow$ $f = q'\cdot f\cdot q = f(q\cdot q')$

אכן $f = q\cdot q'\cdot f$

נטען ש-$qq'=1$.

יש לנו $f-qq'f=0$

$f(1-qq')=0$

f מתוקן ולכן $\neq 0$: מכאן $qq'=1$.

ונראה ש $q=q'=1$ $\quad qq' = f$ $\leftarrow$ המקדם העליון של f = $\Leftarrow$ 1

$\Longleftarrow$ = מקדם עליון של $g\cdot 1 = q\cdot g$

$q=1$ $\longleftarrow$ $f=g$.

## מחלק משותף מקסימאלי (gcd):

יהיו $f,g\in F[X]$. פולינום $d\in F[X]$ נקרא <u>מחלק משותף</u> של f ו-g אם $d|f$ ו- $d|g$.

d נקרא מחלק משותף מקסימאלי אם d מחלק משותף של f ו-g וגם לכל מחלק משותף $d'$ של f ו-g מתקיים $d'|d$

* מהתרגיל הקודם: לכל זוג פולינומים f ו-g שונים מ-0, יש gcd מתוקן יחיד. (כי כל שני gcd מחלקים זה את זה).

דוגמא: ניקח $\left.\begin{array}{l} f=(x-3)(x-1) \\ g=(x-1)(x-7)\end{array}\right\}$ $(x-1)$ הוא gcd של f ו-g, כל gcd של f ו-g הוא מהצורה $\alpha(x-1)$ כאשר $\alpha\in F$

**אלגוריתם אוקלידס:**

נתונים $f,g\in F[x]$. רוצים למצוא $\gcd$ שלהם. אלגוריתם אוקלידס עושה זאת באמצעות חלוקה עם שארית: נניח בה"כ $\deg f\geq \deg g$

**שלב ראשון-** נכתוב $f=q_1 g+r_1$ $\deg r<\deg g$

טענה- $\gcd(g,f)=\gcd(g,r)$

**הסבר-** קבוצת המחלקים המשותפים של $f,g$ = קבוצת המחלקים המשותפים של $g$ ו- $r$.

**שלב שני-** נחלק את $g$ ב- $r_1$ עם שארית: $g=q_2 r_1+r_2$

$\deg r_2<\deg r_1$. כעת, $\gcd(g,r_1)=\gcd(r_1,r_2)$

אותו טיעון כמו קודם.

**שלב שלישי-** $r_1=q_3 r_2+r_3$

**השלב ה-k -** $r_{k-2}=q_k r_{k-1}+r_k$

מתישהו נקבל $r_{k-1}=q_{k+1}+r_k$

ואז, $\gcd(f,g)=\dots=\gcd(r_{k-1},r_k)=\underline{r_k}$

הגדרה- פולינום $0\neq f\in F[x]$ ולא קבוע נקרא אי-פריק אם אי-אפשר לכתוב אותו כמכפלה $f=g\cdot h$.

כלומר, $\deg g>0$ , $\deg h>0$

טענה- יהי $p\in F[x]$ ממעלה 2 או 3, אזי $p$ אי פריק אם אין שורש ב- $F$.

תזכורת- אם $\alpha$ שורש של $p$, $x-\alpha \mid p$