שיעור 3

חלוקה של פולינומים עם שארית-

משפט- יהיו $f,g\in F[x]$, $g\neq 0$. אזי קיימים $q,r\in F[x]$

$$f=q\cdot g+r$$

(q – מנה, r – שארית.)

$\deg r<\deg q$ או $r=0$

$f,g\in\mathbb{Z}$, $g\neq0$ $\quad f=q\cdot g+r \quad 0\le r<|g| \quad q,r\in\mathbb{Z}$

הוכחה-

(יחידות): $f=q_1g+r_1=q_2g+r_2$

$$(q_1-q_2)g=r_2-r_1$$

אם $r_2-r_1\neq0$, אזי גם $q_1-q_2\neq0$.

$$\deg(g)\le\underbrace{\deg(q_1-q_2)}_{\ge0}+\deg(g)=\deg(r_2-r_1)\le\max\{\deg r_1,\deg r_2\}<\deg(g)$$

סתירה. לכן, $r_2=r_1 \Rightarrow q_2=q_1$.

(קיום): $f=a_nx^n+\dots+a_1x+a_0$

$g=g_mx^m+\dots+g_1x+g_0 \quad g_m\neq0$

נוכיח עם אינדוקציה ב-n.

$n=0$ - f קבוע. אם $m=0$, $f=\overbrace{(f\cdot g^{-1})}^{q}g$, $r=0$

אם $m>0$ $\quad f=0\cdot g+f$, $0=\deg(f)<\deg(g)$

$n>0$, אם $n>m$, $f=0\cdot g+f$

נניח ש $n\ge m$ $\quad \bar f=f-x^{n-m}a_nb_m^{-1}g$, $\deg\bar f\le n-1$

$\bar f=q_1\cdot g+r \quad \deg(r)<\deg(g)$ (הנחת האינדוקציה.)

$$f=\bar f+(a_nb_n^{-1}x^{n-m})g=q_1g+r+(a_nb_m^{-1}x^{n-m})g$$

$$=\underbrace{(q_1+a_nb_m^{-1}x^{n-m})}_{q}g+r=q\cdot g+r$$

מ.ש.ל.

הגדרה- יהי $f,g \in F[x]$, $g\neq 0$. אומרים ש-f מתחלק ב-g (או g מחלק את f) אם קיים $h\in F[x]$, כך ש- $f=g\cdot h$. (סימונים- $g|f$, $f:g$)

טענה- (1) אם $b|c$, $a|b$ $\Leftarrow$ $a|c$.

(2) אם $a|c$, $a|b$ $\Leftarrow$ $a|(b\pm c)$

(3) אם $a|b$ $\Leftarrow$ $a|b\cdot c$

(4) אם a מחלק את $b_1,\dots,b_m$, אזי a מחלק את $c_1b_1+\dots+c_mb_m$, לכל $c_i\in F[x]$.

הוכחה- (1)

$$b=a\cdot f$$
$$\downarrow$$
$$c=b\cdot g = a\cdot(f\cdot g)$$
$$\downarrow$$

לכן, $a|c$.

(2)

$$\begin{cases} b=a\cdot f_1 \\ c=a\cdot f_2 \end{cases} \Rightarrow b\pm c = a\cdot f_1 \pm a\cdot f_2$$
$$\downarrow$$
$$a|(b\pm c)$$

(3)

$$b=a\cdot f \Rightarrow bc = a(f\cdot c)$$
$$\downarrow$$
$$a|(bc)$$

(4)

$$b_i = a\cdot f_i$$
$$c_1b_1+\dots+c_mb_m = c_1af_1+\dots+c_ma\cdot f_m = a(c_1f_1+\dots+c_mf_m)$$

מ.ש.ל.

משפט- אם $f,g\in F[x]$ וגם $f\cdot g=1$, אזי f,g פולינומים קבועים. (שונים מ-0).

הוכחה-

$$0=\deg(f\cdot g)=\deg(1)$$
$$\underbrace{\deg(f)}_{\geq 0}\underbrace{\deg(g)}_{\geq 0}=0 \longleftrightarrow \deg(f)=\deg(g)=0$$

מ.ש.ל.

טענה - יהיו $f,g \neq 0$. אם $f|g$ וגם $g|f$, אזי קיים
פולינום קבוע $c\neq 0$ כך ש- $f=c\cdot g$.

הוכחה - $f=g\cdot h_1$

$$g=f\cdot h_2$$

$$f=f\cdot h_1\cdot h_2$$

$$0\neq f(1-h_1h_2)=0$$

$\Downarrow$

$h_1h_2=1 \longrightarrow h_2,h_1$ מעלתם, קבועים

$\downarrow$

$c=h$ מש"ל.

הגדרה - $a,b\in F[x](\mathbb{Z})$ כך שלפחות אחד מהם $\neq 0$. אומרים ש
$d\in F[x]$ מתוקן משותף גדול ביותר של a,b, (סימון: $gcd(a,b)$)
אם (1) $d|a, d|b$
(2) אם $c|a, b|a$ $\Longleftarrow$ $c|d$.

טענה - $a,b\in F[x](\mathbb{Z})$ כך שלפחות אחד מהם $\neq 0$. נניח $d=gcd(a,b)$ קיים.
אזי לכל איבר הפיך c, $c\cdot d$ הוא $gcd(a,b)$.
אם d' - הוא $gcd(a,b)$, אזי $d'=c'\cdot d$, כאשר c' הפיך.

הוכחה - נתחיל מחלק השני, נניח d, d' שני $gcd(a,b)$

נניח ש-d הוא $gcd(a,b)$, c איבר הפיך
נוכיח ש- $c\cdot d$ - הוא $gcd(a,b)$. $\leftarrow$ $a=d\cdot h=(cd)(c^{-1}h)$

$\downarrow$

$(cd)|a$ $\rightarrow$ באופן דומה, $(cd)|b$

נניח ש- $x|b$, $x|a$ $\Longleftarrow$ $x|d$, $d=x\cdot y$

$$cd=x\cdot(cy)$$

$\downarrow$

$x|(cd)$

מש"ל

טענה - (1) $a|b \longleftrightarrow a=\gcd(a,b)$

(2) $a=\gcd(a,0)$ כאשר $a\neq 0$.

(3) $\gcd(t\cdot a, t\cdot b) = t\cdot \gcd(a,b)$

(4) $\gcd(a,\gcd(b,c)) = \gcd(\gcd(a,b),c)$

הוכחה - (1) $\Leftarrow$: נניח $a=\gcd(a,b) \xleftarrow{\text{הגדרה}} a|b$.

$\Rightarrow$: נניח $a|b$. $a|a \to a|d (=\gcd(a,b))$

לכן $d|a$, $\leftarrow a=c\cdot d$ (c טבעי) $\leftarrow$ a הוא $\gcd(a,b)$.

(2) $a|0$, $a|a$, נניח $(c|a\ ,\ c|0) \to c|a \to$

a הוא $\gcd(a,)$.

(3) $d=\gcd(a,b)$, $D=\gcd(a,b)$

צ"ל: $D \stackrel{?}{=} c\cdot td$ (c טבעי)

$$\begin{cases} ta = t\cdot d\cdot x \\ tb = t\cdot d\cdot y \end{cases}$$

$$\begin{cases} a = d\cdot x \\ b = d\cdot y \end{cases}$$

$$\begin{cases} td|ta \\ td|tb \end{cases} \Rightarrow (td)|D$$

$$D = td\cdot c$$

$$\begin{cases} ta = D\cdot u \\ tb = D\cdot v \end{cases}$$

$$\to \begin{cases} ta = td\cdot cu \\ tb = t\cdot d\cdot c\cdot v \end{cases}$$

$$\to \begin{cases} a = (dc)\cdot u \\ b = (dc)\cdot v \end{cases} \to (dc)|a,\ (dc)|b \to (dc)|d.$$

$d=dc\cdot c' \to cc'=1.$

$\downarrow$

c טבעי.

(4) $d_1 | \gcd(a,b) \Leftarrow$

$d_1 | a \rightarrow d_1 | d_2$

$d_1=\gcd(b,c) \leftarrow \begin{cases} d_1 | b \\ d_1 | c \end{cases} \rightarrow d_1 | d_2$

$\downarrow$

באופן סמטרי, $d_2 | d_1$.

$\downarrow$

$d_2 = d_1 \cdot c'$

$\uparrow$ קבוע

מש"ל.

משפט- יהיו $f,g \in F[X](\mathbb{Z})$ שלפחות אחד מהם $\neq 0$.

אזי $d=\gcd(f,g)$ קיים וניתן להציג אותו $d=uf+v\cdot g$

כאשר $u,v \in F[X](\mathbb{Z})$