אלגברה לינארית II שיעור II

הגדרה: יהי R חוג קומוטטיבי. איבר $0\neq a\in R$ נקרא מחלק 0 אם קיים $0\neq b\in R$ כך ש- $ab=0$

⚠ כידוע בשדות אין מחלקי 0. גם ב- $\mathbb{Z}$ אין מחלקי 0.

טענה: ב- $F[X]$ גם אין מחלקי 0.

הוכחה: $f=f_0+f_1X+\dots+f_nX^n$ $\quad f_n\neq 0$

$g=g_0+g_1X+\dots+g_mX^m$ $\quad g_m\neq 0$

$$f\cdot g=\Big(\sum_{i=0}^{n} f_iX^i\Big)\Big(\sum_{j=0}^{m} g_jX^j\Big)=\underbrace{f_ng_m}_{\neq 0 \text{ ולא מצטמצם}}X^{n+m}+\text{חזקות נמוכות של } x \Rightarrow f\cdot g\neq 0 \quad \blacksquare$$

הגדרה: יהי $0\neq f\in F[X]$. $\deg f=\max\{n \mid f_n\neq 0\}$

⚠ $0\le \deg f\in\mathbb{Z}$; $\deg f=0 \Leftrightarrow f$ פולינום קבוע ; $\deg 0:=-\infty$

טענה: אם $f,g\neq 0$ אזי (1) $\deg(f\cdot g)=\deg f+\deg g$

(2) $\deg(f+g)\le \cancel{\deg f+\deg g}$ $\max\{\deg f,\deg g\}$

הוכחה: (1) בסימונים הקודמים $\deg f=n$, $\deg g=m$, $\deg(fg)=n+m$ ✓

(2) $f=f_nX^n+\dots$

$g=g_mX^m+\dots$

$\Rightarrow f+g=?X^{\max\{n,m\}}+$ חזקות נמוכות $\Rightarrow \deg(f+g)\le\max\{n,m\}$ $\blacksquare$

חלוקה של פולינומים עם שארית:

משפט: יהיו $f,g\in F[X]$, $g\neq 0$. אזי קיימים ויחידים $q,r\in F[X]$

$f=q\cdot g+r$ וגם או $r=0$ או $\deg r<\deg g$.

⚠ q נקראת מנה של חלוקה של f ב- g, r נקראת שארית.

תזכורת: אם $f,g\in\mathbb{Z}$, $g\neq 0$ אזי קיימים ויחידים $q,r\in\mathbb{Z}$ כך ש $f=q\cdot g+r$

וגם $0\le r<|g|$.

הוכחה: $f=f_nX^n+$ חזקות נמוכות, $g=g_mX^m+$ חזקות נמוכות, $g_m\neq 0 \Leftarrow \deg g=0$.

$\deg f\le m$

נוכיח באינדוקציה על n: $\xleftarrow{\text{שאומר}}$

• $n=0$: $f=f_0$ - פולינום קבוע. אם $m>0$ נקח $r=f$, $q=0$

ונקבל $f=0\cdot g+f$, $\deg r<\deg g=m$.

אם $m=0$: אזי $g=g_0\neq 0$: $f=f_0=\underbrace{(f_0\cdot g_0^{-1})}_{q}g_0+\underbrace{0}_{r}$

• $n>0$. נ.ה שהטענה נכונה לכל $\tilde f$ עם $\deg\tilde f<n$.

אם $n<m$ אזי: $f=0\cdot g+\underbrace{f}_{r}$

נ.ה $n\geq m$.

$$f=f_nx^n+O(x^{n-1})$$
$$g=g_mx^m+O(x^{m-1})$$

נתבונן ב-

$$f_1=f-f_ng_m^{-1}\underbrace{x^{n-m}\cdot g}_{\deg=n}$$

$f_n\cdot g_m^{-1}\cdot g_m=f_n$ לכן $\deg f_1<n$.

לפי הנ"ל $f_1=q_1g+r$ ($r=0$ או $\deg r<\deg g$).

$$f=f_ng_m^{-1}x^{n-m}\cdot g+(q_1g+r)=\underbrace{(f_ng_m^{-1}x^{n-m}+q_1)}_{q}g+r$$

מקיים דרוש ■

<u>יחידות</u>: $f=qg+r=\tilde qg+\tilde r$ ($\deg r<\deg g$, $\deg\tilde r<\deg g$).

$$(q-\tilde q)g=\tilde r-r$$

נ.ה $\tilde r-r\neq 0$ $\deg(\tilde r-r)<\deg g$

$$\deg g>\deg(\tilde r-r)=\deg(\tilde q-q)g=\deg(q-\tilde q)+\deg g\geq\deg g$$

סתירה!

$$\Leftarrow r=\tilde r\Leftarrow(q-\tilde q)g=0\xLeftarrow{g\neq0}q=\tilde q\quad\blacksquare$$

<u>הגדרה</u>: יהי R חוג קומוט' ללא מחלקי 0. אומרים שאיבר $a\in R$ <u>מחלק את</u> איבר b אם קיים $c\in R$ כך ש- $b=ac$. סימון: $a|b$, $b\vdots a$

⚠ אם $a\neq 0$ אזי c יחיד.

<u>טענה</u>:

(i) אם $a\|b$, $b\|c$ $\Leftarrow$ $a\|c$
(ii) אם $a\|b$, $a\|c$ $\Leftarrow$ $a\|(b\pm c)$
(iii) אם $a\|b$ $\Leftarrow$ $a\|b\cdot c$ $\forall c$
(iv) אם $a\|b_1,\dots,b_n$ $\Leftarrow$ $a\|b_1c_1+\dots+b_nc_n$ $\forall c_i$

<u>טענה</u>: יהי R חוג קומוטטיבי ללא מחלקי 0. יהיו $0\neq a,b\in R$ אזי $a|b$ וגם $b|a$

$\Leftarrow$ $\boxed{a=bc}$ כאשר c איבר הפיך (קיים c' כך ש- $c\cdot c'=1$)

המשך לינארית II שיעור II

⚠ קבוצת ההפיכים חבורה עם כפלית: ⊛ $\{1,-1\} = \mathbb{Z}^*$

⊛ $F\setminus\{0\} = F^* = F[x]^*$

<u>הוכחה:</u> $b=ac$, $a=bc'$ ⇐ $\underset{\neq 0}{b} = \underset{\neq 0}{b}c'\cdot c$ ⇐ $c'c=1$

<u>הגדרה:</u> יהי R חוג קומוטטיבי עם יחידה ללא מחלקי 0. יהיו $a,b\in R$ כך שלפחות אחד מהם אינו 0. <u>המחלק המשותף הגדול ביותר</u> של a,b זה כל איבר $d\in R$ שמקיים:

① $d|a$, $d|b$

② אם $x|a$, $x|b$ ⇐ $x|d$

<u>טענה:</u> יהיו $a,b\in R$ לפחות אחד מהם אינו 0. נניח $d=\gcd(a,b)$, $\tilde{d}=\gcd(a,b)$.

אזי $\tilde{d}=d\cdot c$ כאשר $c\in R^*$

(כי $\tilde{d}|d$ וגם $d|\tilde{d}$)

מתקיים גם להפך: אם $c\in R^*$, $d=\gcd(a,b)$ אזי $d\cdot c=\tilde{d}=\gcd(a,b)$

⇐ <u>מסקנה:</u> <u>בפולינומים</u> $\gcd(a,b)$ מוגדר עד כדי כפל בקבוע

<u>בשלמים</u> - עד כדי סימן.

<u>משפט:</u> <u>קיים $\gcd(a,b)$</u> עבור $a,b\in F[x]$ או $a,b\in\mathbb{Z}$

<u>הוכחה:</u> נגדיר קבוצה $X=\{h=au+bv \mid u,v\in F[x],\ h\neq 0\}$.

$a,b\neq 0$ ⇐ $a,b\in X$, $X\neq\emptyset$ (כאם אחד מהם מתאפס אין מה להוכיח).

יהי $D\in X$ איבר מדרגה מינימלית ב-X. נוכיח $D=\gcd(a,b)$

נחלק את a ב-D עם שארית: $a=qD+r$ $\qquad D=au_0+bv_0$

$$r=a-qD=a-q(au_0+bv_0)=a(1-qu_0)-qbv_0$$

אם $r\neq 0$ אזי $r\in X$ סתירה! כי $\deg r<\deg D$

לכן $r=0$ ו-D מחלק את a מסימטריה גם את b.

יהי $x\in R$, $x|a$, $x|b$ צ"ל $x|D$

אבל $D=au_0+bv_0$ לכן $x|D$ כנדרש! ∎