

4.11.18

4 ורע 5 תרצ"ה

פולינומים

הערה: $f \in K[x]$ ו- $g \in K[x]$ הם פולינומים
 אם $f = g + h$ אז $h = f - g$ ו- $h \in K[x]$
 $\mathbb{Z} \subseteq \mathbb{Z} = \{x^p\} \subseteq K[x]$

$$R = K[x_p \mid 0 \neq f \in K[x]]$$

הערה

\otimes $I = \langle x_p, 0 \neq f \in K[x] \rangle \neq R$
 $I \in M$ מיוצגת על ידי $R \rightarrow \Omega$ ו- $\Omega = R/M$

הערה: $K \subseteq \Omega$ (המלבד), $K \rightarrow R \rightarrow \Omega$
 והוא Ω - \mathbb{Z} על ידי $f \in K[x]$
 $\Omega \ni \alpha_p = x_p + M$

Ω - \mathbb{Z} על ידי $f \in K[x]$
 (1) $K \subseteq \Omega$ ו- $f \in K[x]$ על ידי Ω
 (2) Ω - \mathbb{Z} על ידי $f \in K[x]$

Ω - \mathbb{Z} על ידי $f \in K[x]$
 אם $f \in K[x]$ אז $f(\alpha) = 0$ ו- $\alpha \in \Omega$
 $K(\alpha) = K[x]/(f)$

$f \in K[x]$ ו- $\alpha \in \Omega$ אז $f(\alpha) = 0$
 $\alpha \in \bar{K} \iff \alpha \in \Omega \iff f(\alpha) = 0$

* הנהיגו את הפולינום

1.6 עליו המורה
 (עליו המורה המורה המורה)
 (PID) עליו המורה המורה
 $K[x], \mathbb{Z}$ עליו המורה המורה

עליו המורה המורה המורה $R \neq 0$ עליו המורה המורה
 $f: R \setminus \{0\} \rightarrow \mathbb{Z}_{\geq 0}$
 $f(r) = |m|$ עליו המורה המורה
 $f(p) = \deg p$ עליו המורה המורה
 $K[x]$ עליו המורה המורה

עליו המורה המורה המורה $I \triangleq R$ עליו המורה המורה
 $f(a) \neq 0$ עליו המורה המורה
 $b \in \langle a \rangle \iff b \in I$ עליו המורה המורה
 $r = 0 \iff f(r) < f(a)$ עליו המורה המורה
 $r = b - aq \in I$ עליו המורה המורה
 $b = aq + r$ עליו המורה המורה

$b \in \langle a \rangle$

$\mathbb{Z}[\alpha] = \{a + b\alpha : a, b \in \mathbb{Z}\}$ עליו המורה המורה
 $\alpha = \frac{1 + \sqrt{-19}}{2}$ עליו המורה המורה
עליו המורה המורה המורה המורה

$PID \iff \dots$ עליו המורה המורה

$a = bu$ פ"ק, a ל"ק $u \in R$ 1 הכרחי
 $a \neq 0$ $u \in R^*$ $u \in R^*$ $u \in R^*$
 $\Leftrightarrow a = bu$ פ"ק $u \in R^*$ $a \neq 0$ 2
 $a \mid b$ $\Leftrightarrow a \mid bc$ פ"ק $a \neq 0$ 3

$0 \neq p \in R$ 1
 $a \neq 0$ $a \mid a$ 2
 $a \mid a$ 3
 3 4

5 R a, b $a \mid b$ $a \mid b$
 $a \mid b$ $a \mid b$ $a \mid b$
 $a \mid b$ $a \mid b$ $a \mid b$
 $a \mid b$ $a \mid b$ $a \mid b$

הכנה 6-8

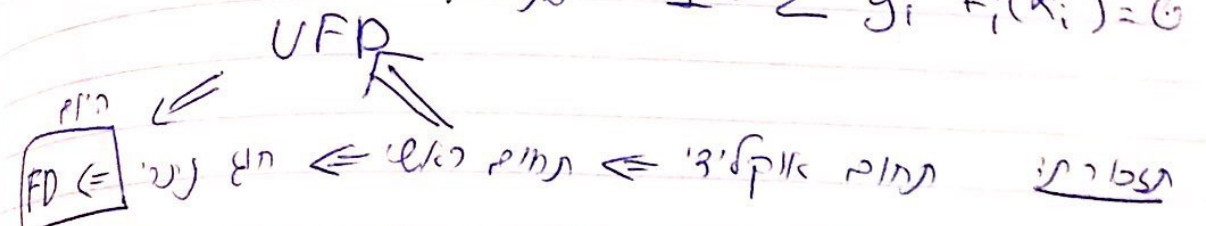
המקום המקומי: $R = K[x_1, \dots, x_n]$ (אנחנו נניח ש- K הוא שדה) \rightarrow $M = \langle f(x) \rangle$ \rightarrow R/M \rightarrow R/M \rightarrow R/M

$f \in R$ \rightarrow $\langle f(x) \rangle$ \rightarrow R/M \rightarrow R/M \rightarrow R/M

$1 = \sum_{i=1}^n g_i(x) f_i(x)$ \rightarrow $f_i(\alpha_i) = 0$ \rightarrow $R \rightarrow L[x_1, \dots, x_n]$ \rightarrow L/K

$$R \rightarrow L[x_1, \dots, x_n] \quad x_i \mapsto \alpha_i$$

\otimes L/K \rightarrow $1 = \sum \bar{g}_i f_i(\alpha_i) = 0$



$a=bc \Leftrightarrow$ (לא הפיך) $0 \neq a \in R$

$a|b \Leftrightarrow a|bc$ \Leftrightarrow $0 \neq a \in R$

$\Leftrightarrow a=bu$ \rightarrow $a \sim b$ $\Leftrightarrow a \sim b$

אזכר תלמידי < א. פירוק

(FD) תחום R נקרא תחום פריקות אם
 $a \neq 0$ אז $a = p_1 \cdots p_r$ ו- $r=0$ או $r=1$ ו- p_i אי-פריקים
 (אם a הוא אי-פריק) (אם a הוא פריק)

כלומר: $\mathbb{Z} = \{\sqrt{2}, \sqrt{2}, \sqrt{2}, \dots\}$ הוא FD

$$2 = \sqrt{2} \cdot \sqrt{2} = (\sqrt{2} \sqrt{2}) (\sqrt{2} \sqrt{2}) \dots$$

טענה: תחום שלמות R הוא FD

אם R הוא תחום שלמות ו- $a \in R$ אז a הוא פריק או אי-פריק.
 אם a אי-פריק אז a אי-פריק גם ב- R .
 אם a פריק אז $a = bc$ ו- b, c אי-פריקים.

עקביות: $(\sqrt{5}+1)(\sqrt{5}-1) = 4$

טענה: מקיים $FD \Leftrightarrow$ כל אי-פריקים ראשוניים.
 הוכחה: כיוון \Rightarrow תבנית היחידה והיחידה \Leftrightarrow לכל
 קבוצה של אי-פריקים ראשוניים יש אי-פריק מקסימלי.
 הפוך: קבוצה

$$I = \{a - b \mid a, b \text{ פריקים או פריק}\}$$

נניח $a, b \in I$ אז $a = c_1 \cdots c_n$ ו- $b = d_1 \cdots d_m$
 $a - b = c_1 \cdots c_n - d_1 \cdots d_m$
 אם $a = b$ אז $a = b$ ו- a אי-פריק או פריק.
 אם $a \neq b$ אז $a - b$ אי-פריק או פריק.
 \Rightarrow I סגור תחת הפחתה.

טענה: תחום R נקרא תחום פריקות יחידה UFD
 אם $a \neq 0$ אז $a = u \cdot p_1 \cdots p_r$ ו- u יחידה ו- p_i אי-פריקים
 (יחידות ± 1 או $\pm i$ או $\pm j$ או $\pm k$)

UFD \Leftrightarrow PID הוכחה

- הוכחה: נתון R הוא UFD. נוכח כי R הוא PID.
1. אם R הוא PID, אז R הוא UFD. (הוכחה ישירה)
 2. אם R הוא UFD, אז R הוא PID. (הוכחה: כל אידיאל ראשי הוא פרימיטיבי)
 3. אם R הוא UFD, אז R הוא PID. (הוכחה: כל אידיאל ראשי הוא פרימיטיבי)

2 בקר ע"ש

נתון $a \in R$ אינו פריק. נגד: $\langle a \rangle \subseteq \langle a \rangle \subseteq \dots$ אינסוף תת-אידיאלים. $\langle a \rangle \subseteq \langle a \rangle \subseteq \dots$

נניח $a = p_1 \dots p_r = q_1 \dots q_s$.
 מאחר ש- $p_i \sim p_{i+1}$ ו- $q_i \sim q_{i+1}$, נגד: $p_i = q_i$.
 לכן $r = s$ ו- $p_i = q_i$.
 נגד: $p_i = q_i$.

$a = p_1 \dots p_r = q_1 \dots q_s$.
 נגד: $p_i \mid q_j$ ו- $q_j \mid p_i$.
 נגד: $p_i = q_i$.

$(p_{r-1} \dots p_1) \mid (q_{s-1} \dots q_1)$.
 נגד: $p_{r-1} = q_{s-1}$.

$R/M \cong \mathbb{Z}/p\mathbb{Z}$ (שדה) $\Leftrightarrow M$ אידיאל ראשי.
 $R/M \cong \mathbb{Z}/p\mathbb{Z}$ (שדה) $\Leftrightarrow M$ אידיאל ראשי.

הוכחה: $UFD \Rightarrow PID$.
 נגד: $ab \mid ab \Leftrightarrow p \mid ab$.
 נגד: $ab \mid ab \Leftrightarrow p \mid ab$.

$\square p|b \wedge p|a \Leftrightarrow b \in pR \wedge a \in pR \Leftrightarrow p \mid a \wedge p \mid b$
 $\Leftrightarrow \exists r, s \in R \text{ s.t. } a = pr, b = ps$
 $\Leftrightarrow p \mid a \wedge p \mid b$
 $\square \text{gcd}(a, b) = d \Leftrightarrow d \mid a \wedge d \mid b$
 $\wedge \exists c \in R \text{ s.t. } a = cd, b = cd$

$\text{GCD} \Leftrightarrow \text{UFD}$
 $\text{UFD} \Leftrightarrow \text{GCD} + \dots$

$a = p_1^{e_1} \dots p_r^{e_r} u$
 $b = q_1^{f_1} \dots q_s^{f_s} v$

$\text{gcd}(a, b) = \left[\prod_{p \in P} p_i^{\min\{e_i, f_i\}} \right]$
 $P = \{p_i : \exists q_j \sim p_i\}$
GCD is unique

- $a, b, c \in R \rightarrow \text{GCD}$
- (1) $a|b \Leftrightarrow \text{gcd}(a, b) = [a]$
 - (2) $c \text{gcd}(a, b) = \text{gcd}(ca, cb)$
 - (3) $\text{gcd}(a, b) = \text{gcd}(a, c) = [1]$

$\Leftrightarrow \text{gcd}(a, bc) = [1]$

$a|c \wedge a|bc \rightarrow \text{gcd}(a, b) = [1]$ (4)

$[d] = \text{gcd}(a, b)$
 $a|b \Leftrightarrow [d] \neq [a] \Leftrightarrow$
 $a \nmid d \Leftrightarrow a|b \Leftrightarrow$

"אם a מתחלק ב- b אז $\text{gcd}(a, b) = a$ "

$x = \gcd(ac, bc)$
 $d \mid bc \iff d \mid ac \iff d \mid b$
 $d = \gcd(a, b)$
 $d \mid x \iff d \mid ac \iff d \mid bc$
 $x = c \cdot y$
 $y \mid a$
 $y \mid b$
 $y \mid d$
 $x \mid dc$

$d \mid \gcd(ab, bc) \iff d \mid lab \iff d \mid bc \iff d \mid a$
 $d \mid \gcd(a, b) \iff d \mid a$
 $d \mid \gcd(a, b) \iff d \mid a$

$a \mid c \iff a \mid bc \iff a \mid \gcd(bc, ac) \iff a \mid bc$
 $\gcd(a, b) = [a] \cap [b]$
 $a \mid bc$

UFD \iff FD + GCD
 $[y] = \gcd(p, b)$
 $(x) = \gcd(p, a)$
 $\gcd(p, a) = \gcd(p, b) = 1$
 $\gcd(p, ab) = 1$

הרחבה של פולינומים
 $R[x]$
 I פולינום
 $f: R \rightarrow S$
 $f(I)$
 $I \text{ ext} = f(I)S$

התמונה ההסרה ϕ היא $\mathbb{Z} \rightarrow \mathbb{Z}$ $\phi(x) = px$
 ההסרה ϕ היא $\mathbb{Z} \rightarrow \mathbb{Z}$ $\phi(x) = px$

$J := \phi^{-1}(J)$
 $\mathbb{Z} \xrightarrow{\phi} \mathbb{Z}/\ker \phi \rightarrow S, \dots$
 $\mathbb{Z} \xrightarrow{\phi} \mathbb{Z}/\ker \phi \rightarrow S, \dots$
 $\mathbb{Z} \xrightarrow{\phi} \mathbb{Z}/\ker \phi \rightarrow S, \dots$

$\mathbb{Z} \rightarrow \mathbb{Z}[\sqrt{-1}]$ $p=2$ $\mathbb{Z}[\sqrt{-1}]$
 $\mathbb{Z} \rightarrow \mathbb{Z}[\sqrt{-1}]$ $p=2$ $\mathbb{Z}[\sqrt{-1}]$

$\mathbb{Z}[\sqrt{-1}] = (1+i)^2 \mathbb{Z}[\sqrt{-1}]$

$\mathbb{Z}[\sqrt{-1}] = (1+2i)(1-2i) \mathbb{Z}[\sqrt{-1}]$ $p=5$ $\mathbb{Z}[\sqrt{-1}]$

$\mathbb{Z}[\sqrt{-1}] = \mathbb{Z}[\sqrt{-1}]$ $p=3$ $\mathbb{Z}[\sqrt{-1}]$