

הרצאה 21

הצגנו  $R \subseteq S$  חוקים חילופיים. איגור  $S \subseteq S$

הצגנו  $R$  שיש בו חוקים חילופיים

$$f(x) = x^n + a_{n-1}x^{n-1} + \dots + a_1x + a_0 \in R[x]$$

$$f(s) = s^n + a_{n-1}s^{n-1} + \dots + a_0 = 0_s \quad \because p$$

הצגנו  $R = \mathbb{Z}$  חוקים חילופיים

זהו  $d$  חסר-מחלקים

$$S = \mathbb{Q}(\sqrt{d}) = \{a + b\sqrt{d} : a, b \in \mathbb{Q}\}$$

$$0 \neq a + b\sqrt{d} \Rightarrow (a + b\sqrt{d}) \cdot \frac{a - b\sqrt{d}}{a^2 - db^2} = 1$$

$F = \mathbb{Q}(\sqrt{d}) \neq \mathbb{Z}$  חוקים חילופיים

$$\sigma_F = \{ \alpha \in \mathbb{Q}(\sqrt{d}) : \mathbb{Z} \text{ שומר על } \alpha \}$$

הצגנו  $\sigma: F \rightarrow F$  חוקים חילופיים

$$\sigma(a + b\sqrt{d}) = a - b\sqrt{d}$$

אין  $\sigma$  חוקים חילופיים על  $F$ .  
 הוכחנו, גורו כי  $\sigma$  חסר-מחלקים כי  $\sigma \circ \sigma = id$ .

נראה שהוכחנו כי  $\sigma$  חסר-מחלקים.  
 $\sigma(1 + \sqrt{d}) = 1 - \sqrt{d}$

$\sigma$  מראה ש:

$$\begin{aligned} \sigma((a_1 + b_1\sqrt{d})(a_2 + b_2\sqrt{d})) &= \\ \sigma(\underbrace{(a_1a_2 + b_1b_2d)}_{\in \mathbb{Q}} + \underbrace{(a_1b_2 + a_2b_1)}_{\in \mathbb{Q}}\sqrt{d}) &= \\ (a_1a_2 + b_1b_2d) - (a_1b_2 + a_2b_1)\sqrt{d} &= \\ (a_1 - b_1\sqrt{d})(a_2 - b_2\sqrt{d}) &= \sigma(a_1 + b_1\sqrt{d})\sigma(a_2 + b_2\sqrt{d}) \end{aligned}$$

$\sigma$  מראה ש:

$\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{d})$  כי יש  $a \in \mathbb{Q}$   
 $a \mapsto a + 0\sqrt{d}$

יש  $a \in \mathbb{Q}$  כך ש  $\sigma(a) = a$

הוכחה: נניח  $\alpha \in F = \mathbb{Q}(\sqrt{d})$  יהיו  $a, b \in \mathbb{Q}$   
 $f(x) = a_n x^n + \dots + a_0 \in \mathbb{Q}[x]$  גורם

יהי  $\sigma(\alpha)$  גם  $a, b \in \mathbb{Q}$

הוכחה כי ההינחה,  $f(\alpha) = 0$ , נכונה

$$a_n \alpha^n + a_{n-1} \alpha^{n-1} + \dots + a_1 \alpha + a_0 = 0$$

אם  $\sigma$  הוא  $\sigma$  יהיו האגפים:

$$\sigma(a_n) \sigma(\alpha)^n + \sigma(a_{n-1}) \sigma(\alpha)^{n-1} + \dots + \sigma(a_0) = \sigma(0) = 0$$

$$\sigma(a_i) = a_i \iff a_i \in \mathbb{Q}$$



176 י"ג יהי  $F = \mathbb{Q}(\sqrt{d})$ ,  $d$  מס' טריגונומי. י"ג

$$\mathcal{O}_F = \begin{cases} \mathbb{Z}[\sqrt{d}] = \{a+b\sqrt{d} : a, b \in \mathbb{Z}\} & d \equiv 2, 3 \pmod{4} \\ \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right] & d \equiv 1 \pmod{4} \end{cases}$$

הוכחה קורה נ"ל, יונייה שהאקסיה הימני מונד  
 $\mathcal{O}_F \cong \mathbb{Z}[\sqrt{d}]$  אכן, הי"ן עוה ע"ה

$\mathbb{Z}[\sqrt{d}] \subseteq \mathcal{O}_F$  אכן,  $\sqrt{d} \in \mathcal{O}_F$  אכן,  $x^2 - d \in \mathbb{Z}[x]$   
 אכן  $\mathcal{O}_F$  חוק וני  $\mathbb{Z} \subseteq \mathcal{O}_F$  (ני נ"ל  $a \in \mathbb{Z}$  הי"ן  
 ע"ה  $(x - a) \in \mathbb{Z}[x]$ )

א"כ  $d \not\equiv 1 \pmod{4}$  נ"ל סיימיו א"כ הוכיח

א"כ הי"ן הימין מונד  $\mathcal{O}_F \cong \mathbb{Z}[\sqrt{d}]$

א"כ  $d \equiv 1 \pmod{4}$  א"כ  $\frac{1+\sqrt{d}}{2} \in \mathcal{O}_F$  א"כ הוכיח

$X = \frac{1+\sqrt{d}}{2}$  י"ג א"כ

$2x = 1 + \sqrt{d}$

$2x - 1 = \sqrt{d}$

$4x^2 - 4x + 1 = d$

$4x^2 - 4x + (1-d) = 0$

$x^2 - x + \frac{1-d}{4} = 0$

$d \equiv 1 \pmod{4}$  א"כ  $\frac{1-d}{4} \in \mathbb{Z}$

א"כ הי"ן הימין מונד  
 א"כ הי"ן הימין מונד  
 א"כ הי"ן הימין מונד  
 א"כ הי"ן הימין מונד

על כל סדרות  $\sigma_F$  מוגדרת האינדיקס

$$d = a + b\sqrt{d} \in \sigma_F \quad \text{הי'}$$

$$2a \in \mathbb{Z} \quad \text{היקומם של יגור נ'}$$

$$a^2 - db^2 \in \mathbb{Z}$$

הי'  $a = \frac{k}{2} \Leftrightarrow k = 2a \in \mathbb{Z}$  נגזר האינדיקס:

$$l = \left(\frac{k}{2}\right)^2 - db^2 \in \mathbb{Z}$$

$$4l = k^2 - 4db^2 \quad \begin{matrix} k, l, d \in \mathbb{Z} \\ b \in \mathbb{Q} \end{matrix}$$

הי'  $b = \frac{m}{n}$  עבור מספרים  $m, n$  זרים:

$$4l = k^2 - \frac{4dm^2}{n^2} \quad k, l, m, n, d \in \mathbb{Z}$$

$$\frac{4dm^2}{n^2} = k^2 - 4l \in \mathbb{Z} \quad \text{לפיכך}$$

כאן  $n^2 | 4dm^2$  ,  $\text{gcd}(m, n) = 1$  ,  $\text{gcd}(d, n) = 1$  כי

$$\frac{m}{n} \text{ מספר זר } \Leftrightarrow n^2 | 4d \quad \text{כאן } d, \text{gcd}(d, n) = 1$$

מכאן  $d = p_1 p_2 \dots p_r$  , כאשר  $p_i$  ראשוניים

$$n^2 | 4p_1 p_2 \dots p_r \quad \text{כאן ראשוניים}$$

כאן  $n^2 | 4$  ,  $n | 2$  , נכאן  $n=1$  או  $n=2$

$$q = 2b \in \mathbb{Z} \quad (b = \frac{m}{n}) \quad \text{ו} \quad \sqrt{d} \text{ איננו רציונלי}$$

$$k, q \in \mathbb{Z} \quad b = \frac{q}{2}, \quad a = \frac{k}{2} \quad \text{אם}$$

אם  $\sqrt{d}$  איננו רציונלי, אז  $\sqrt{d} \notin \mathbb{Q}$

$$l = a^2 - db^2 \in \mathbb{Z}$$

$$l = \frac{k^2}{4} - \frac{dq^2}{4}$$

$$4l = k^2 - dq^2$$

$$c \in \mathbb{Z} \quad \text{אם} \quad \sqrt{d} \mid c \quad \boxed{k^2 \equiv dq^2 \pmod{4}} \quad \text{אם}$$

$$c^2 \equiv 0 \pmod{4} \quad \text{אם}$$

$$c^2 \equiv 1 \pmod{4} \quad \text{אם}$$

$$d \not\equiv 0 \pmod{4} \Leftrightarrow \text{אם } d \text{ איננו רציונלי}$$

$$\text{אם } d \equiv 2, 3 \pmod{4} \quad \text{אם } (1)$$

$$\Leftrightarrow \text{אם } k, q \quad \Leftrightarrow k^2 \equiv q^2 \equiv 0 \pmod{4}$$

$$d = a + b\sqrt{d} \in \mathbb{Z}[\sqrt{d}] \Leftrightarrow a, b \in \mathbb{Z} \quad \Leftrightarrow a = \frac{k}{2}, b = \frac{q}{2}$$

$$\Leftrightarrow k^2 \equiv q^2 \pmod{4} \text{ אם } d \equiv 1 \pmod{4} \quad \text{אם } (2)$$

$$k \equiv q \pmod{2}$$

$$\text{אם } z \in \mathbb{Z}, \quad k = q + 2z \quad \text{אם}$$

$$\alpha = a + b\sqrt{d} = \frac{k}{2} + \frac{q}{2}\sqrt{d} = \frac{q+2z}{2} + \frac{q}{2}\sqrt{d} =$$

$$z + q \cdot \frac{1+\sqrt{d}}{2} \in \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$$

כך נראה כי האינז'ריות

$$\sigma_F = \begin{cases} \mathbb{Z}[\sqrt{d}], & d \equiv 2,3 \pmod{4} \\ \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right], & d \equiv 1 \pmod{4} \end{cases}$$

האינז'ריות של  $\sigma_F$  היא  $\mathbb{Z}$  ויש לה

$$-5 \equiv 3 \pmod{4} \quad F = \mathbb{Q}(\sqrt{-5})$$

$$\sigma_F = \mathbb{Z}[\sqrt{-5}]$$

הקטגוריה היא  $R$  חזקה.  $R$  היא  $\mathbb{Z}$  ויש לה

היא חזקה (Dedekind) אבל  $R$  איננה חזקה

היא חזקה (גלוקס) :

(1)  $R$  חזקה

(2)  $R$  חזקה

(3)  $\dim R = 1$  -  $R$  חזקה (1)  $\Leftrightarrow (0) \in \text{Spec } R$

כך נראה כי  $\dim R = 1$

$0 \neq P \in R$

(היא חזקה)

(4)  $R$  חזקה

היא  $F = \text{Frac } R$  אבל

$\exists \alpha \in R, \alpha \neq 0, \alpha \in F$

לצורה החוקים  $\sigma_F$  הינם גחומי זיקוקי

הוכחה ברוב הגאוג.

המטרה הגאוג הינה להוכיח שכל איגואל  
לא-אקס' גחומי זיקוקי מגדוק באופן יחיד  
למבנה של איגואלים ראשוניים.

למה | יהי  $R$  גחומי של מוג יגרו: יהי

$R \neq I \neq I$  אגוי  $I$  מניל מבנה

של איגואלים ראשוניים לא-אקס'יים.

$$P_1 P_2 \dots P_n \leq I$$

הוכחה גרו:  $\{I \neq I \neq I\}$  אגוי מבנה של איגואלים ראשוניים לא-אקס'יים

אנחנו נוציב להוכיח כי  $\mathcal{A} = \emptyset$ .

נניח בשאלה כי  $\mathcal{A} \neq \emptyset$ . ניון  $e$ - $R$  יגרו:

יש ב- $\mathcal{A}$  (קבוצה סגורה חלקיג של יוני  
הנלה) איבר מקסימלי: כלומר קיים  $I \in \mathcal{A}$

כך  $e$ - $I \in \mathcal{A}$  אבל אם  $J \neq I$ , אז  $I \notin \mathcal{A}$ .

נשים לב כי  $I$  לא ראשוני: כי אם  $I$   
ראשוני, אזי  $I \leq I$  מבנה ראשוניים. אם  $I \in \mathcal{A}$ .



דבר,  $I$  -הוא יחידה.  $r, s \in R$  הם אלמנטים.

$$r, s \in R, \quad r, s \notin I$$

$$J_1 = I + (r) \quad \text{האלמנטים}$$

$$J_2 = I + (s)$$

$$P_1, P_2, \dots, P_t \in J_1 \Leftrightarrow J_1, J_2 \neq \emptyset \Leftrightarrow I \subseteq J_1 \quad \text{כל}$$

$$Q_1, Q_2, \dots, Q_u \in J_2 \quad I \subseteq J_2$$

$$J_1, J_2 \subseteq I \quad \text{כל}$$

$$J_1, J_2 = \left\{ \sum a_i b_i : \begin{matrix} a_i \in J_1 \\ b_i \in J_2 \end{matrix} \right\} \quad \text{כל}$$

$$a_i b_i = (i_1 + a r)(i_2 + b s) = i_1 i_2 + a r i_2 + b s i_1 + a b r s \in I$$

$\underbrace{i_1 i_2 + a r i_2 + b s i_1}_{\in I} + \underbrace{a b r s}_{\in I} \in I \quad a, b \in R$

$$(P_1, P_2, \dots, P_t)(Q_1, Q_2, \dots, Q_u) \subseteq J_1, J_2 \subseteq I \quad \text{כל}$$

האלמנטים מכלוליהם של אלמנטים מהאלמנטים  
 מכלוליהם של אלמנטים מהאלמנטים

הקדמה יהי  $R$  גחום אלוו,  $F = \text{frac } R$

יהי  $0 \neq P \triangleleft R$  אלוו ואלו.

$P^{-1} = \{ \alpha \in F : \alpha P \subseteq R \}$  נללו

$\alpha P = \{ \alpha \beta : \beta \in P \}$  כאלו

אלו  $P$  אלוו, כטן  $R \subseteq P^{-1}$

$F$  הלוו  $R$ -לוו. נוים ככ כ  $P^{-1}$  הלוו  
גג-לוו.

למח 2 יהי  $R$  נוו, גחום אלוו,  $\dim R = 1$

יהי  $0 \neq P \triangleleft R$  אלוו ואלו, אלו  $P^{-1} \not\subseteq R$

הונחה יהי  $0 \neq \gamma \in P$  ו'  $I = (\gamma) \triangleleft R$

כפי הלוו  $I$

$P_1 P_2 \dots P_t \subseteq I = (\gamma) \subseteq P$   
[גחו מנכח ככ עכ  $t$  הלוו!]  
אלו  $P$  ואלו, אלו הלוו  $1 \leq i \leq t$  ככ  
ואלו  $t$  אלסוים

$P_i \subseteq P$  אלו  $\dim R = 1$ , כטן  $P_i, P$  -e

שויה מלוו, כטן  $P_i = P$  לוו ולוו ככ

הקבלו הלוו  $P_t = P$

$P_1, P_2, P_3, \dots, P_{t-1} \notin I = (y)$ ,  $t$   $\in$   $\mathbb{Z}$   $\Rightarrow$   $\mathbb{Z}$   $\neq$   $\mathbb{R}$

$z \in P_1, P_2, \dots, P_{t-1} \setminus (y)$   $\Rightarrow$   $\mathbb{Z}$   $\neq$   $\mathbb{R}$

$\therefore \exists \alpha = \frac{z}{y} \in F$   $\Rightarrow$   $\mathbb{Z}$   $\neq$   $\mathbb{R}$

$z = y \cdot \frac{z}{y} \in (y)$   $\Rightarrow$   $\mathbb{Z} \neq \mathbb{R}$  (1)

$\Rightarrow$   $\mathbb{Z} \neq \mathbb{R}$

$\exists \beta \in P$   $\Rightarrow$   $\exists \alpha \in P^{-1}$  (2)

$$z\beta \in \underbrace{(P_1, P_2, \dots, P_{t-1})}_{z\alpha} \underbrace{P_t}_{\beta} \subseteq I = (y)$$

$z\beta = y\gamma \in (y)$   $\Rightarrow$   $\exists \gamma \in \mathbb{R}$   $\Rightarrow$   $\mathbb{Z} \neq \mathbb{R}$

$$\alpha\beta = \frac{z}{y} \cdot \beta = \gamma \in \mathbb{R} \quad \mathbb{Z} \neq \mathbb{R}$$

$$\alpha \in P^{-1} \quad \mathbb{Z} \neq \mathbb{R}$$

$$P^{-1} = \{x \in F : xP \subseteq R\} \quad P^{-1} \neq R \quad \mathbb{Z} \neq \mathbb{R}$$