

הרצאה 10

הקצרה יהי R חוק, יהיו $a, b \in R$. איבר $d \in R$

נקרא d מחלק משותף מקסימלי של a ו- b אם

(א) $(a, b) \subseteq (d)$ (כלומר a ו- b מתחלקים ב- d)

(ב) אם $I \triangleleft R$ איננו $\frac{(a, b)}{d}$ - e $(a, b) \subseteq I \Leftrightarrow d \in I$

אזי $(a) \subseteq I \Leftrightarrow d \in I$.

כלומר (א) הינו האינדקס הראשי הנייט, וקל שמנאי אג (a, b) .

הערות (א) אם $R = \mathbb{Z}$ אזי זוג ה- d הקטן ביותר.

(א) d הינו מחלק משותף של a ו- b .

(ב) אם $(a, b) = (d)$ (כלומר ראשי) אזי

\exists g מחלק משותף, ויחידאי $(a) \subseteq (g) + I$

אזי d מחלק משותף (אם d הינו ראשי) ויחידאי.

ואכן d הינו מחלק משותף מקסימלי.

(2) הקצרה של d משמש רק האינדקס (א)

ולא ב- d עצמו. לכן אם R גחום שלמה,

אזי ה- d הינו כני חרוג.

(3) ה- d מחלק לא במני ק"ב. $R = \mathbb{Z}[\sqrt{-5}]$, $a = 6$, $b = 2(1 + \sqrt{-5})$

$a = 6$, $b = 2(1 + \sqrt{-5})$

האינדקסים הראשיים (2), $(1 + \sqrt{-5})$

ע"י ה- a מנילים a ו- b .

$a = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$

לכן $a \in (1 + \sqrt{-5})$ ו- $a \in (2)$

$b \in (1 + \sqrt{-5})$, $b \in (2)$.

$\frac{1}{1}$ חזרויב \mathbb{Z} -ע. זג גימט רזאי, לכך קיים d
 כך \exists : $(d) = (a, b)$, לכך $d \mid a$ ו $d \mid b$ (באילו רזאי
 הני קטן שמינל אג (a, b) . מכאן מקבלים אג
 הטענה מכורג והסברים האולמאטיבי: יהי $n \in (a, b)$.

$$n \in (a, b) \iff n = xa + yb$$

$$n \in (d) \iff n \in (a, b)$$

טענה. כל גחום בריקו יחידה היינו גחום \mathbb{Z} .
 הוכחה. יהי R גמיי. יהיו $a, b \in R$.

אב a או b הכין, אץ $(a, b) \in R$, נלמד
 $(1) = (a, b)$, לכך \exists ג- \mathbb{Z} a ב, b הינו 1.
 אב a, b כטו הכינים, יהיו

$$a = p_1^{e_1} p_2^{e_2} \dots p_r^{e_r}$$

$$b = p_1^{f_1} p_2^{f_2} \dots p_r^{f_r}$$

נמוג לכתקו f_i, e_i כהיג 0, נאן p_1, \dots, p_r
 כל a, b כריקו (עז נני חדרוג) שמתקיים אג a או
 ב, a .

$$a = 105 = 3 \cdot 5 \cdot 7 \cdot 19 \quad R = \mathbb{Z}$$

$$b = 95 = 5 \cdot 19$$

$$d = p_1^{\min(e_1, f_1)} p_2^{\min(e_2, f_2)} \dots p_r^{\min(e_r, f_r)} \quad \text{לך ניקח}$$

לזכור כי d הינו ה-gcd.

יהי $g \in R$ ש- g סתום $g = q_1^{h_1} \dots q_s^{h_s}$

כאן $a = \pi_1^{j_1} \dots \pi_t^{j_t}$ ורק אם קיים

כך $\alpha = g \cdot c = q_1^{e_1} \dots q_r^{e_r} = q_1^{h_1} \dots q_s^{h_s} \pi_1^{j_1} \dots \pi_t^{j_t}$

מיתאם הבחור מקבלים כי ה- q 'ים הייחידים שהיוג
 מייצגים- g יב צו נוי חבוב, צם הציקוק למובוג מן הציקוק
 א ה- q -ה המגאים.

למקרה: $g = u p_1^{d_1} \dots p_r^{d_r}$ אם u הינו, $d_i \leq e_i$

כאן $d_i \leq e_i$ כנס i
 צעו תונתן טאם אף אפי ניגן, ארביג אל
 ג גבורג היטא, ואלם $g = u p_1^{d_1} \dots p_r^{d_r}$ כאן

$\alpha = g(u^{-1} p_1^{e_1-d_1} \dots p_r^{e_r-d_r})$

כאן, אם g מתאן אן α וקב אכ b אפי
 $(a,b) \in (g) = I$
 $g = u p_1^{d_1} \dots p_r^{d_r}$

כך $d_i \leq e_i$ כנס i $d_i \leq f_i$
 $\Leftrightarrow d_i \leq \min\{e_i, f_i\}$

$I = (g) \supseteq (d)$
 כן d הינו gcd ל- a, b
 $(b) \supseteq (a) \Leftrightarrow b = ac \Leftrightarrow a|b$

הקטרה יהי R חוץ חסומי. איבר $e \in R$ קרוי הינן האשני.

אם $a \in R$ כן $e - \frac{ab}{a}$ מקיים $\frac{ab}{a}$ או $\frac{ba}{a}$

במילים אחרות, $e \in R$ האשני \Leftrightarrow האשני (a) הינן האשני.

אשני $e \in R$ קרוי הינן אי-בריק אם $a = be$ או $a = ea$ הינן.

אשני יהי R חומב אמוב. כל איבר האשני הינן אי-בריק.

אכן, יהי q האשני, ויהי $a = bq$. אזי $a = bq = qa$.

אכן $a = bq$ או $a = qb$ הינן האשני.

כלי הקבוצה הנכללים $a = bq$. אזי $a = qb$. אכן.

$a = bq = qa$. בגומב אמוב אובסר $a = bq = qa$.

כלומר a הינן. אכן q אי-בריק.

אשני הינן איבר אי-בריק לא בהכרח האשני.

זוג $R = \mathbb{Z}[\sqrt{5}]$ הינן חומב אמוב כי הוא מוכל בשדה \mathbb{C} .

הוכחתו כי 2 הינן אי-בריק. אבל,

$$2 \mid (6 - (1 + \sqrt{5})(1 - \sqrt{5}))$$

ברור כי 2 לא מתחלק אל $6 - (1 \pm \sqrt{5})$. אכן 2 לא האשני.

אשני יהי R גבויי. אזי איבר $e \in R$ האשני אם ורק אם הוא אי-בריק.

הוכחה (\Leftarrow) נניח גדל גחוב שלמוק.

(\Rightarrow) יהי $a \in R$ אי-פריק, אם $ab = ca$, אזי $ab = ca$

a מופיע (כזו טי חבויג) בפירוק של ab (כי הפירוק יחיד). הפירוק הנגד הנין שואו של הפירוקיג של a ושל b , לכן a בהכרח מופיע באחד הפירוקיג השלילי. לכן אם a לא מופיע באחד הפירוקיג, a (באשני).

חוקי פולינומים

אבחה יהי R חוק. יהיו $f, g \in R[x]$

$$f = \alpha x^n + \left(\begin{array}{l} \text{מחברים ממילג} \\ \text{למונה יוגר} \end{array} \right) \text{ אב}$$

$$g = b x^m + \left(\begin{array}{l} \text{מחברג למונה} \\ \text{יוגר} \end{array} \right)$$

$$fg = a b x^{n+m} + \left(\begin{array}{l} \text{מחברג למונה} \\ \text{יוגר} \end{array} \right) \text{ אזי}$$

גולאוב (ו) R גחוב שלמוק אם ורק אם $R[x]$ גחוב שלמוק

הוכחה (\Rightarrow) R הנין גג-חוק של $R[x]$ (כל הכוליונים

היקבוצה, נאמו ממילג 0 אם R י.

מחלקי אבס, הם גם מחלקי אבס ב- $R[x]$.

(\Leftarrow) לווה $R[x]$ לא גחוב שלמוק. יהיו $f, g \in R[x]$

$$fg = 0, \quad f, g \neq 0$$

$$f = \alpha x^n + \dots$$

$$g = b x^m + \dots$$

מקבוצה מביאום $0 \neq b$.

$$0 = fg = \alpha b x^{n+m} + \left(\begin{matrix} \text{מחזורי } x \\ \text{יורד} \end{matrix} \right) \quad \text{כאן}$$

$\Leftrightarrow \alpha b = 0 \Leftrightarrow$ מחזורי x^{n+m} (המקרה של x^{n+m})
 R לא גחורב אלמנטי

כאן R גחורב אלמנטי, אלמנטי

$$\underbrace{R[x]^*}_{\substack{\text{המחזורי } R \\ \text{המחזורי } R[x] \\ \text{המחזורי } R[x]^*}} = \underbrace{R^*}_{\substack{\text{המחזורי } R \\ \text{המחזורי } R[x] \\ \text{המחזורי } R[x]^*}}$$

(המחזורי) (המחזורי) (המחזורי)

טענה יהי $I \triangleleft R$ אידיאל, אלמנטי

$$I[x] = \{ \alpha_n x^n + \dots + \alpha_0 \in R[x] \mid \alpha_n, \dots, \alpha_0 \in I \}$$

היינו אידיאל של $R[x]$ בן יסוד, $R[x]$

$$R[x]/I[x] \cong (R/I)[x]$$

המחזורי, $f = \sum_{i=0}^n \alpha_i x^i \in I[x]$, $g = \sum_{j=0}^m b_j x^j \in R[x]$

$$fg = \sum_{k=0}^{n+m} \left(\sum_{i=0}^k \alpha_i b_{k-i} \right) x^k \in I[x]$$

אלמנטי, $\alpha_i \in I$

גורו כי $I[x] \triangleleft R[x]$ גב סגור לחיבור, כן $R[x]$

המחזורי, $\varphi: R \rightarrow R/I$ $\varphi(\alpha) = \alpha + I$

מה יהיה $\psi: R[x] \rightarrow (R/I)[x]$

$$\psi\left(\sum \alpha_i x^i\right) = \sum \varphi(\alpha_i) x^i$$

(המחזורי) (המחזורי)

המחזורי, $\varphi(\alpha_i) = 0 \Leftrightarrow f = \sum \alpha_i x^i \in \ker \psi$

$f \in I[x] \Leftrightarrow \alpha_i \in \ker \varphi = I$

אלמנטי, $R[x]/I[x] \cong (R/I)[x]$

הקטגוריה יהי R גחום לפי (בברט), R יבול (היוג גביי).

פוליונים $f = a_n x^n + \dots + a_0$ נקרא פרימיטיבי אם
 $\text{gcd}(a_0, a_1, \dots, a_n) = 1 \Leftrightarrow$ למקדמים של f אין
 מחלק משותף לא זניח.

לפי (האמה של גאוס) יהי R גביי, יהי $F = \text{frac } R$

יהי $f \in R[x]$ פוליונים פרימיטיבי. אזי
 f אי-כריין ב- $R[x]$ אם ורק אם f אי-כריין
 ב- $F[x]$.

כריין $\rightarrow x^3 - 2x^2 + 3x - 6 = (\frac{3}{2}x - 3)(\frac{2}{3}x^2 + 2)$ $R = \mathbb{Z}$ $F = \mathbb{Q}$ $\frac{k}{m}$

$\rightarrow (x-2)(x^2+3)$ \rightarrow גבי כריין ב- $\mathbb{Z}[x]$

הוכחה \Leftrightarrow נניח בשלילה כי f אי-כריין ב- $R[x]$
 אבל כריין ב- $F[x]$. אזי יהי $f = gh$ (כאן $g, h \in F[x]$)
 פירוק ב- $F[x]$. נט פוליונים לא אבסי קבוע הינו
 זניח ב- $F[x]$. ככן חץ ממראה 1 או יותר.

קיימים $r \in R$ כך $\tilde{g} = rg \in R[x]$ - \therefore
 $\tilde{h} = h \in R[x]$

(לזימא, גרי a המכפלה של \tilde{g} המכונים של המקדמים של
 f)
 יהי $d = ab$.

כאן $df = (ag)(bh) = \tilde{g} \cdot \tilde{h}$ פירוק ב- $R[x]$
 אם d זניח, אזי $f = (d^{-1}ag) \cdot (bh)$ הינו פירוק פרימיטיבי לא-כריין.

י) $d = p_1 \dots p_r$ בירוק סגורמים אי-פרויקטיביים, וק לא
 נל (המקומים d מהחלוקה $d \in (p_i)$ ג-ה
 גרונר
 יצאים

כאן, $f \in (p_r)[x] \in R[x]$ אבל, רק אי-פרויקטיבי, אכן האסון
 (כי R גרונר)

$$R[x]/(p_r)[x] = \underbrace{(R/(p_r))}_{\text{חבורה אנוני, נייטרל האסון}}[x]$$

כאן $R[x]/(p_r)[x]$ חבורה אנוני, אכן $R[x] \not\subset (p_r)[x]$
 איננו האסון

כאן $f \in (p_r)[x]$ או $h \in (p_r)[x]$ אבל $\tilde{g} \in (p_r)[x]$ איננו נל
 מקיים \tilde{g} מהחוק $d = p_1 \dots p_r$, אכן $\tilde{g} = p_r \tilde{g}$, אכן
 $\tilde{g} \in R[x]$
 $(p_1 \dots p_{r-1})f = \tilde{g} \cdot h$

משקן בן זר שכתבו מנל ה- $p_1 \dots p_r$ נקבל בירוק
 כל $f \in R[x]$ בסגור.

כאן בריאויבי
 $2x-2 = 2(x-1)$
 פרויקט $\Rightarrow (x-1)$
 אי-פרויקט $\Rightarrow (x-1)$