

הרצאה 8

הקצרה גחום אינרטי הינן גחום שלמה R עם
 פונקציה אינרטי, נלמד פונקציה $N: R \rightarrow \mathbb{N} \cup \{0\}$

$$N(0) = 0 \quad (\text{כ} \quad \dots)$$

(א) לכל $a, b \in R$, $b \neq 0$, קיימים

$$a = bq + r \quad (\text{כ} \quad \dots)$$

$$N(r) < N(b) \quad \text{או} \quad r = 0 \quad (2)$$

$$N(a) = |a|, \quad R = \mathbb{Z} \quad (\text{כ} \quad \dots)$$

$$5 = 3 \cdot 1 + 2 \quad a=5, b=3$$

$$5 = 3 \cdot 2 + (-1)$$

(2) $a \in F$ לכל $N(a) = 0$, זהו F

כל $b \neq 0$

$$a = b \cdot (ab^{-1}) + 0$$

(3) $R = F[x]$, נלמד F

$$f = a_n x^n + a_{n-1} x^{n-1} + \dots + a_0, \quad f \in R$$

$$N(f) = \deg f = n.$$

(4) $R = \mathbb{Z}[i] = \{a+bi \mid a, b \in \mathbb{Z}\}$ (האנשים של גאוס)

$$N(a) = a\bar{a} = a^2 + b^2 \quad \text{כ} \quad \dots, \alpha = a+bi \in R$$

ברור מן ההקצרה שהקצרה היננה נכונה:

$$N(\alpha\beta) = N(\alpha)N(\beta)$$

יש כמובן $N(\alpha) = 0 \Leftrightarrow \alpha = 0$. ברור להוכיח כי
 הגנטי הינן של פונקציה אינרטי.

יהי $\alpha, \beta \in \mathbb{R}, \beta \neq 0$ יהי $\gamma = \frac{\alpha}{\beta} \in \mathbb{C}$

הבעיה: יכול להיות כי $\gamma \notin \mathbb{R}$ יהיו $m, n \in \mathbb{Z}$

$$|\operatorname{Re} \gamma - m| \leq \frac{1}{2} \quad \text{כ} \quad \dots$$

$$|\operatorname{Im} \gamma - n| \leq \frac{1}{2}$$

יהי $q = m + ni \in \mathbb{Z}[i]$ נשים לב כי $|\gamma - q|^2 = (\frac{1}{2})^2 + (\frac{1}{2})^2 = \frac{1}{2}$

יהי $r = \alpha - \beta q \in \mathbb{Z}[i]$ יהיו r, \bar{r}

$$N(r) = r\bar{r} = |r|^2 = |\beta|^2 \left| \frac{\alpha}{\beta} - q \right|^2 = |\beta|^2 |\gamma - q|^2 \leq \frac{1}{2} |\beta|^2 = \frac{1}{2} N(\beta) < N(\beta)$$

הצבירה מחום של \mathbb{R} נקרא מחום ראשי אם כל איגול $\mathbb{Z}[i]$ יהיו איגול ראשי (קוצר דמי איגול)

למשל כל מחום איקלידי יהיו מחום ראשי

הוכחה יהי \mathbb{R} מחום איקלידי, יהי $\mathbb{Z}[i]$ איגול אם

$(\alpha) = \mathbb{Z}$, גורר שהוא ראשי, אף לניה $\mathbb{Z} \neq 0$ יהי

$d \in \mathbb{Z}, d \neq 0$ עם נורמה מינימלית (מבין האיגולים הראשי-איגוליים

של \mathbb{Z}) אף טוען כי $(\alpha) = (d)$

כיוון $d \in \mathbb{Z}, d \in \mathbb{Z}$ אף $(d) \subseteq \mathbb{Z}$

זכאי נכוח $(\alpha) \subseteq (d)$ יהי $\alpha \in \mathbb{Z}$ אף $\alpha = dq + r$

כאשר $r = 0$ או $N(r) < N(d)$ אף $r = \sum_{i \in \mathbb{Z}} \alpha_i - \sum_{i \in \mathbb{Z}} d_i$

כא יתכן כי $N(r) < N(d)$ הקלל המינימלית של $N(d)$

כך בהכרח $r = 0$, נלומר $\alpha = dq \Leftrightarrow \alpha \in (d)$ לכן $(\alpha) \subseteq (d)$

אוצר $\mathbb{Z}[x]$ לא גחם איקליז, כי הוכחנו בשיעור
היקום כי הוא לא גחם ראשי.

הקצרה יהי R חוג היילוכי איבר $\alpha \in R$ ^{לא-הפך} $\neq 0$

אי-ברויך אם לכל $\alpha \in R$ $\alpha \neq 0$ $\exists \beta \in R$ $\alpha\beta = 1$

הגדרה α הפך או β הפך

הצורה המושך של איבר אי-ברויך הינו הנלכה של מספרים
ראשוניים \mathbb{Z} . בהמשך נראה הנלכה אחרת.

הקצרה גחם פרויקט יחיד (גרמיי) היינו גחם של $UFD = \text{unique factorization domain}$

R כן שלכל $\alpha \in R, \alpha \neq 0$ ^{לא הפך} \exists פירוק יחיד $\alpha = p_1 \cdot p_2 \cdot \dots \cdot p_n$

של איברים אי-ברויכים: $\alpha = p_1 \cdot p_2 \cdot \dots \cdot p_n$

והפירוק יחיד גחם יחיד גחם: אם

$$\alpha = p_1 \cdot p_2 \cdot \dots \cdot p_n = q_1 \cdot q_2 \cdot \dots \cdot q_m$$

$m = n$, וצד כלי מספר אחת של ה- q_i 'ים,

p_i חבר של q_j לכל $i \leq n$.

אזכור a חבר של b אם קיים u הפך u כך $a = ub$.

אזכור אם R גחם שלמה, אזי $(a) = (b)$ אם ורק אם

כיום חברים.

הקצרה (1) \mathbb{Z} הינו גרמיי (המשל) היסודי של אריגמט. קרא

$$6 = 2 \cdot 3 = (-2) \cdot (-3) = (-3) \cdot (-2)$$

2-2 חברים
3-3 חברים

$$\mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} : a, b \in \mathbb{Z}\}$$

$$6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$$

כתיב להשגתנו שזו אכן אלגוריתם-נוקמה, צריך להוכיח

(א) האיברים $1 \pm \sqrt{-5}$, $2, 3$ אי-בריוקים.

(ב) שני הבריוקים אינם קבוצה זו חבורה.

לכך $\alpha = a + b\sqrt{-5} \in \mathbb{Z}[\sqrt{-5}]$, נגזיר $N(\alpha) = \alpha\bar{\alpha} = |a|^2 = a^2 + 5b^2 \in \mathbb{N}$

שוב, הנומה כפליגי: $N(\alpha\beta) = N(\alpha)N(\beta)$

נשים לב כי $\alpha \in \mathbb{Z}[\sqrt{-5}]$ הברק $N(\alpha) = 1 \Leftrightarrow$ אכן

α הברק \Leftrightarrow קיים β כך $\alpha\beta = 1 \Leftrightarrow N(\alpha)N(\beta) = N(1) = 1$
 $a^2 + 5b^2 = 1$

$N(\alpha) = N(\beta) = 1$, ולכן $N(\alpha) = N(\beta) = 1$

בניין השני. אם $\alpha = a + b\sqrt{-5}$, $N(\alpha) = 1$, אזי

$(a + b\sqrt{-5})(a - b\sqrt{-5}) = 1$, ולכן הברק

לכן הוכחנו כי $\alpha \in \mathbb{Z}[\sqrt{-5}]$ הברק $N(\alpha) = 1 \Leftrightarrow$

נשים לב כי $N(2) = N(2 + 0\sqrt{-5}) = 2^2 + 5 \cdot 0^2 = 4$

$N(3) = 9$

$N(1 \pm \sqrt{-5}) = 6$

לפיכך באיזה כי $1 + \sqrt{-5}$ ברק, אזי קיים פירוק

$1 + \sqrt{-5} = \alpha\beta$, כאן הברק

$N(\alpha)N(\beta) \neq 1$, $6 = N(1 + \sqrt{-5}) = N(\alpha) \cdot N(\beta)$

אך בהנחה $N(\alpha) = 2$ או $N(\beta) = 3$ לא

אין פירוק $\alpha, \beta \in \mathbb{Z}$ כאשר $\alpha^2 + 5\beta^2 = 2$ או $\alpha^2 + 5\beta^2 = 3$

לכן $\mathbb{Z}[\sqrt{-5}]$ לא קיימים איברים עם נורמה 2 או 3

$$\begin{array}{l} \text{לכן} \\ \text{נמו בן} \end{array} \begin{array}{l} 1 + \sqrt{-5} \\ 1 - \sqrt{-5} \end{array} \begin{array}{l} \text{אי-ברוק} \\ \text{אי-ברוק} \end{array}$$

$$2 = \alpha\beta \quad \text{נמו בן } 2 \text{ אי-ברוק כי}$$

$$4 = N(2) = N(\alpha) \cdot N(\beta)$$

$$N(\alpha) = N(\beta) = 2 \Leftrightarrow N(\alpha), N(\beta) \neq 1 \Leftrightarrow \alpha, \beta \text{ לא הרכיבים}$$

ונגד ואין שאין איברים ב- $\mathbb{Z}[\sqrt{-5}]$ עם נורמה 2.

נמו בן, 3 אי-ברוק.

נמו אמצעיים, הסתנו כי $5 \pm \sqrt{-5}$, 2, 3 אי-ברוקים.

יגדו אצלנו, אם α, β חברים, אזי $\alpha\beta = 2$

$$N(\alpha) = N(\beta) \Leftrightarrow \text{הכך} \Leftrightarrow N(\alpha) = N(\beta) \cdot N(\gamma) = N(\beta) \cdot 1$$

לכן שני הפירוקים הנ"ל של 6 שונים גם

$$6 = 2 \cdot 3 = \underbrace{(1 + \sqrt{-5})}_{N=6} \cdot \underbrace{(1 - \sqrt{-5})}_{N=6}$$

השערה $\mathbb{Z}[\sqrt{-5}]$ אינו גומם פריק יחידה.
הוכח על ידי וילס-טאילור Wiles-Taylor, 1994
נוסח ד"ר פומה ג-1650, 1994
המשפט האחרון של פומה: אם $3 \nmid n$, אזי

$$a^n + b^n = c^n \quad \text{לא אבולוטים} \quad \text{כך } - \text{ע}$$

בסוף 1844, Kummer הקיץ הוכחה של המשפט הנ"ל.

Pedekind מלא את הטעם בהוכחה קומה

צגנו עם $\mathbb{Z}[\sqrt{-5}]$ והניח שגה גומם פריק יחידה.

לענין יהי R גחום ראשי יהי $a \in R$ איבו אי-כריין

אזי האינואל (a) מקסימלי

הוכחה לפי היקדוה, a פא היפין, פכן (a) היין אינואל אמגי.

לויח $a \in I$, נאשר I אינואל אמגי.

R גחום ראשי, פכן $(b) = I$. פכן, $a \in I$, פכן קיים

$c \in R$ נק $a = bc$. אבא a אי-כריין, פכן

b היפין או c היפין. אן $(b) = I$ אמגי, פכן

b פא היפין, אזי בהכרח c היפין. פכן b, c חגורים

פכן $(a) = (b) = I$ פכן (a) מקסימלי.

משפט כל גחום ראשי היין גחום פרייקו יחיוה.

הקדוה יהי R חוק חילופי, יהיו $a, b \in R$ פכן

כי b מתלק אז a פא קיים $c \in R$ נק $a = bc$.

$$a = bc$$

הוכחה של המשפט יהי R גחום ראשי, יהי $a \in R, a \neq 0$

ואז היפין

על 1 קיים איבו אי-כריין p שמתלק אז a .

הוכחה 1 לויח פא. גברא a פריין אבא a

אי-כריין, אזי a מתלק אז פכא וסיימון. פכן

$a = bp$, נאשר b, p פא היפנים ופא אי-כריינים

לאהוג מלפאן מתלק אי-כריין פא (a) .

גאופן זמנה, $a_1 = b_1 c_1$ נאשר $a_2 = b_2 c_2$ פא היפנים
ואז אי-כריינים.

c_n כו"ו. לכן קיים פירוק $c_n = b_{n+1} c_{n+1}$ נאמר הקוראים לזה
 הפיכים. הנוסף. הקוראים כו"ו קוב
 כי אחר כך נקרא מהלך אי-כוי"ו של a

כך ממשיכים $c_2 = b_3 c_3$
 $c_3 = b_4 c_4$
 \vdots

לכן $(a) \subseteq (c_1) \subseteq (c_2) \subseteq (c_3) \subseteq \dots$

בסדר עגרה הוכחנו שכל גחום ראשי הינו נגזר;
 ולכן הישרים הנצאג חייגג אוליג"ג. אז קיים N

מספיק קטן כך $\exists: (c_N) = (c_{N+1})$

אן R גחום אלמוג, לפי c_N, c_{N+1} חברים.

$c_N = u \cdot c_{N+1}$, u הפין
 $c_N = b_{N+1} \cdot c_{N+1}$

גחום אלמוג אפשר לנגזב $(c_{N+1} \neq 0 \text{ כי } a \neq 0)$

ולכן $u = b_{N+1}$, כלומר u חטב הפין, בסגור.

לכן הוכחה כי a אין מהלך אי-כוי"ו היגה סגורה.