הרצאה 4

פירוק אידיאלים בהרחבות של תחומי דדקינד

טענה: כל תחום ראשי הינו תחום דדקינד.

הוכחה: תחום ראשי הינו תחום שלמות, וגם הינו תחום פריקות
יחידה ולכן סגור בשלמות, כל תחום ראשי הינו נותרי

$$I_1 \subseteq I_2 \subseteq I_3 \subseteq \dots$$
$$(d_1) \subseteq (d_2) \subseteq d_3 \quad \dots \quad \dots d_3 | d_2 | d_1$$

אבל d_1 מכפלה של מספר סופי של גורמים אי-פריקים.

בנוסף, המימד של כל תחום ראשי A הינו 1.

נניח שלא, אז יש אידיאל ראשוני $0 \neq P = (p)$ שאינו מקסימלי. אז יהי $(p) = P \subsetneq M = (m)$.

אזי $p = ma$ עבור $a \in A$. אז

$ma \in P \Rightarrow m \in P$ או $a \in P$. אם $m \in P$, אזי $M = (m) \subseteq P$ ואז $M = P$ בסתירה. אם $a \in P$,

אזי $a = pb \Rightarrow p = ma = mpb$.

$p(1-mb) = 0$ מתחום שלמות

$P \neq (0) \Rightarrow p \neq 0 \Rightarrow mb = 1 \Rightarrow m$ הפיך $\Rightarrow M = A$

בסתירה.

לדוגמא: $A = k[x]$, כאשר k שדה, כלשהו. הינו תחום דדקינד.

יהי A תחום דדקינד, $K=\mathrm{Frac}\,A$ שדה השברים, L/K הרחבה סופית של שדות. ויהי B הסגור השלם של A ב-L.

$$\begin{matrix} K & \subset & L \\ \cup & & \cup \\ A & \subset & B \end{matrix}$$

<u>טענה</u> B הינו תחום דדקינד; (הטענה נכונה גם כאשר L/K לא ספרבילי, אך קשה יותר להוכיח). (יהיה תרגיל בית).

יהי $\mathfrak{p}\triangleleft A$ אידאל ראשוני. אזי $\mathfrak{p}B=P_1^{e_1}P_2^{e_2}\cdots P_r^{e_r}$ כאשר $P_1,\dots,P_r$ אידאלים ראשוניים שונים של B. אך כן? מספרן?

למה B נתרי? אם L/K ספרבילי, יהי $(b_1,\dots,b_n)\in B$ בסיס של L מעל K. הוכחנו ש-d הדיסקרימיננטה, $d\neq 0$, dB נוצר סופית כ-A-מודול.

$dB=Ax_1+\dots+Ax_m$

$\Rightarrow B\subseteq A\frac{x_1}{d}+\dots+A\frac{x_m}{d}\subseteq L$ $\Leftarrow$ B נוצר סופית $\Leftarrow$ כל אידאל של B נוצר סופית (כ-A-מודול) לכן נתרי.

<u>טענה</u> $\mathfrak{p}B$ הינו אידאל אמיתי.

<u>הוכחה</u> נניח בשלילה שלא. יהי $x\in A$, $x\in\mathfrak{p}\setminus\mathfrak{p}^2$ (קיים בגלל יחידות הפירוק).

אזי $xA\subseteq\mathfrak{p}$, $\not\subseteq\mathfrak{p}^2$, לכן $xA=\mathfrak{p}I$ כאשר $I\triangleleft A$ זר ל-$\mathfrak{p}$.

אזי $\mathfrak{p}+I=A$. לכן $1=y+z$ כאשר $y\in\mathfrak{p}$, $z\in I$.

אזי $z\mathfrak{p}=(zA)\mathfrak{p}\subseteq\mathfrak{p}I=xA$.

אנחנו מניחים (בשלילה) כי $\mathfrak{p}B=B$. לכן

$zB=z\mathfrak{p}B\subseteq xB$

לכן קיים $b\in B$ כך ש- $z=xb$. אבל $b=\frac{z}{x}\in K=\mathrm{Frac}A$.

לכן $b\in B\cap K=A$ (A סגור בשלמות). לכן, $z\in xA\subseteq \mathfrak{q}$ בסתירה.

מסקנה: המכפלה $\mathfrak{q}B=P_1^{e_1}\cdots P_r^{e_r}$ לא ריקה.

$e_i=e(P/\mathfrak{q})$ אינדקס ההסתעפות של $P/\mathfrak{q}$.

$f_i=[B/P_i:A/\mathfrak{q}]=\dim_{A/\mathfrak{q}}B/P_i$ מעלת ההתמצה.

<u>הגדרה</u> אומרים כי $\mathfrak{q}$ מסועף בהרחבה L/K אם קיים $1\leq i\leq r$ כך ש- $e_i>1$.

<u>טענה</u> יהיו A,B,K,L כנ"ל. יהי $n=[L:K]$. אזי

$$n=\sum_{i=1}^{r}e_if_i$$

<u>הוכחה</u> האידיאלים $P_1^{e_1},P_2^{e_2},\ldots,P_r^{e_r}$ קו-מקסימליים בזוגות,

לכן לפי משפט השאריות הסיני $B/\mathfrak{q}B\simeq B/P_1^{e_1}\times\cdots\times B/P_r^{e_r}$.

באופן טבעי, כל אחד הינו מרחב וקטורי מעל $A/\mathfrak{q}$,

לכן מספיק להוכיח:

1) $\dim_{A/\mathfrak{q}}B/P_i^{e_i}=e_if_i$

2) $\dim_{A/\mathfrak{q}}B/\mathfrak{q}B=n$.

1) נתבונן בשרשרת $B/P_i^{e_i} \supseteq P_i/P_i^{e_i} \supseteq P_i^2/P_i^{e_i} \supseteq \dots \supseteq P_i^{e_i-1}/P_i^{e_i}$

של מרחבים וקטוריים מעל $A/\mathfrak{p}$. לכל $0 \le m \le e_i - 1$,

יהי $x \in P_i^m \setminus P_i^{m+1}$. אזי

$$B \longrightarrow P_i^m / P_i^{m+1}$$
$$b \longmapsto bx + P_i^{m+1}$$

הומו' של A-מודולים.

אך $xB + P_i^{m+1} = P_i^m$ (כמו בפרק הקודם), לכן ההעתקה על. הגרעין הינו P_i. לכן $B/P_i \simeq P_i^m/P_i^{m+1}$ כ-$A/\mathfrak{p}$-מודול.

לכן $\dim B/P_i^{e_i} = e_i \dim_{A/\mathfrak{p}} B/P_i = e_i f_i$.

2) $\dim_{A/\mathfrak{p}} B/\mathfrak{p}B = n$. בתרגיל נגיע עם מונים.

<u>לשאלה</u> A,B,K,L כנ"ל, נניח L/K ספרבילי. לכן קיים $\theta \in B$ כך ש- $L = K(\theta)$. יהי $g(X) \in A[X]$ הפולינום המינימלי של θ.

<u>הגדרה</u> המוליך של θ (conductor) הינו

$$\mathfrak{F}_\theta = \{\alpha \in B : \alpha B \subseteq A[\theta]\} \trianglelefteq B.$$

בפרט, $f_\theta = B \iff A[\theta] = B$.

<u>משפט</u> יהיו A, B, K, L, θ כנ"ל. יהי φ אידאל ראשוני של A. נניח כי φB זר למוליך f_θ. יהי $k = A/\varphi$. נזכור כי $k[X]$ הינו תחום ראשי! יהי

רדוקציה מודולו φ של $g(X)$

$$\bar{g}(X) = \bar{g}_1(X)^{e_1} \cdots \bar{g}_r(X)^{e_r} \quad \text{ב} \quad k[X]$$

כאשר $\bar{g}_i(X)$ פולינומים אי-פריקים מתוקנים שונים של $k[X]$.

יהיו $g_1(X), \dots, g_r(X) \in A[X]$ פולינומים מתוקנים שמרימים את $\bar{g}_1, \dots, \bar{g}_r$. יהי $P_i = \varphi B + g_i(\theta) B$.

אזי $P_1, \dots, P_r$ הינם אידאלים ראשוניים שונים של B ומקיימים $\varphi B = P_1^{e_1} P_2^{e_2} \cdots P_r^{e_r}$, וגם

$$f_i = \dim_k B/P_i = \deg \bar{g}_i .$$

<u>הוכחה</u> נסמן $B' = A[\theta]$.

<u>שלב 1</u>

$$B/\varphi B \simeq B'/\varphi B' \simeq k[X]/(\bar{g}(X)) .$$

<u>הוכחה 1</u> לפי ההנחה

$$\begin{array}{l} f + \varphi B = B \\ \cap \\ B' + \varphi B = B \end{array}$$

לכן ההעתקה $B' \to B/\wp B$ המושרית ע"י ההכלה $B' \subseteq B$
$x \mapsto x+\wp B$

היא על. הגרעין הינו $B' \cap \wp B$.

ברור כי $\wp B' \subseteq B' \cap \wp B$. מצד שני,

$$\wp B \cap B' = A(\wp B \cap B') = (\underbrace{\wp + (\mathfrak{f} \cap A)}_{=A})(\wp B \cap B') \subseteq$$

$$\wp(\wp B \cap B') + (\mathfrak{f} \cap A)(\wp B \cap B') \subseteq$$

$$\wp B' + \wp \underbrace{\mathfrak{f} B}_{\subseteq B'} \subseteq \wp B'.$$

סך הכל, הגרעין הינו $\wp B \cap B' = \wp B'$, ולפי משפט האיזו' הראשון $B/\wp B \simeq B'/\wp B'$, ההעתקה מושרית ע"י ההכלה $B' \subseteq B$.

האיזו' השני: נשים לב כי $B' = A[\theta] \cong A[X]/(g(X))$

$$f(\theta) \leftarrow f(X) + (g(X))$$

לכן: $B' \twoheadrightarrow k[X]/(\bar{g}(X))$, הגרעין הינו $\wp B'$.

<u>שלב 2</u> הנחנו $\bar{g}(X) = \bar{g}_1^{e_1} \cdots \bar{g}_r^{e_r}$

לפי משפט השאריות הסיני

$$k[X]/(\bar{g}(X)) \simeq k[X]/(\bar{g}_1(X))^{e_1} \times \cdots \times k[X]/(\bar{g}_r(X))^{e_r}.$$

<u>שלב 3</u> לכל אחד מן החוגים $k[X]/(\bar{q}_i(X))^{e_i}$ יש אידאל ראשוני יחיד, נסמנו ע"י $\bar{q}_i(X)$ (אם $e_i=1$, האידאל הזה יהיה אפס).

ויהיו $\wp_i = R_1 \times \cdots \times (\bar{q}_i(X)) \times \cdots \times R_r$ אידאלים ראשוניים ב- $R = k[X]/(\bar{q}(X))$ הם

$$R = R_1 \times \cdots \times R_r$$

$$R_i = k[X]/(\bar{q}_i^{\,e_i})$$

ונובע מזה,

$$(0) = \bigcap \wp_i^{e_i} = \wp_1^{e_1}\wp_2^{e_2}\cdots\wp_r^{e_r}$$

נחזור ל- $B/\wp B$ על ידי האיזומורפיזמים בשלב 1.

$$R \longrightarrow B/\wp B$$

$$\underbrace{f(X)}_{\in k(X)} + (\bar{q}(X)) \longmapsto f(\theta) + \wp B$$

לכן, בחוג $B/\wp B$, האידאלים $\wp_i$ מתאימים לאידאלים

רדוקציה מודולו $\wp B$

$\tilde{\wp}_i = (\overline{q_i(\theta)})$, ע"י $(0) = \bigcap \tilde{\wp}_i^{e_i} = \tilde{\wp}_1^{e_1}\cdots\tilde{\wp}_r^{e_r}$.

יהי $\varphi: B \longrightarrow B/\wp B$ ההעתקה הטבעית. אז

$P_i = \varphi^{-1}(\tilde{\wp}_i) = q_i(\theta) + \wp B$ הינם אידאלים ראשוניים.

טענה: $\varphi^{-1}(\tilde{\mathfrak{q}}_i^{e_i}) = P_i^{e_i}$ (תרגיל).

נניח את זה. אזי לפי ההגדרה,

$$pB = \varphi^{-1}(0) = \bigcap \varphi^{-1}(\tilde{\mathfrak{q}}_i^{e_i}) = \bigcap P_i^{e_i} \underset{\text{ד}}{=} P_1^{e_1}P_2^{e_2}\times\cdots\times P_r^{e_r}$$

B תחום דדקינד

וגם,

$$f_i = \dim_k B/P_i = \dim_k R/(R_1\times\cdots\times(\bar{g}_i(X))\times\cdots\times R_r) =$$

$$\dim_k k[X]/(\bar{g}_i(X)) = \deg \bar{g}_i(X).$$

מסקנה: יהי L שדה מספרים. כל אידיאל ראשוני של $\mathcal{O}_L$ נוצר על ידי לכל היותר שני איברים.

הוכחה:
$$\begin{array}{ccc} \mathbb{Q} & \subset & L \\ \cup & & \cup \\ A=\mathbb{Z} & \subset & \mathcal{O}_L = B \end{array}$$
יהי $P \triangleleft B = \mathcal{O}_L$ אידיאל ראשוני.

$p\mathbb{Z} = P \cap A$.

יהי $\theta \in \mathcal{O}_L$ כך ש-$L = \mathbb{Q}(\theta)$. אם P זר למוליך f_θ,

אזי $P \mid p\mathcal{O}_L$ ולפי המשפט,

$$P = g_i(\theta)\mathcal{O}_L + p\mathcal{O}_L = (g_i(\theta), p)$$

עבור $g_i(X)$ מתאים (הרמה של גורם אי-פריק של הרדוקציה מודולו p של הפולינום המינימלי של θ).

תרגיל מדוע ניתן למצוא θ כך ש- f_θ יהיה זר ל-p נתון?

דוגמא $L=\mathbb{Q}(\sqrt6)$. איך מתפרק $5\mathcal{O}_L$?

ידוע כי $\mathcal{O}_L=\mathbb{Z}[\sqrt6]$, ניקח $\theta=\sqrt6$, אזי $f_\theta=B$ זר לכל p.

הפולינום המינימלי הינו x^2-6.

איך זה מתפרק ב- $A/\mathfrak{p} = \mathbb{Z}/5\mathbb{Z}$?

$$x^2-6 = x^2-1 = (x-1)(x+1) \in \mathbb{Z}/5\mathbb{Z}[X]$$

לכן, $5\mathcal{O}_L = P_1P_2$ כאשר

$$5=(\sqrt6-1)(\sqrt6+1) \qquad P_1=(5,\sqrt6-1)=(\sqrt6-1) \quad e_1=f_1=1$$
$$P_2=(5,\sqrt6+1)=(\sqrt6+1) \quad e_2=f_2=1$$

הערה לפי תרגיל הבית, החוג $\mathbb{Z}(\sqrt6)$ הינו תחום ראשי.
לכן, האידיאלים P_1,P_2 הינם ראשיים. באופן
כללי, האלגוריתם של המשפט יתן לנו את
הגורמים P_i כאידיאלים נוצרים על ידי שני יוצרים.
למצוא יוצר אחד זו שאלה נפרדת (principal ideal problem).

שאלה יהי $L=\mathbb{Q}(\sqrt{d})$ שדה מספרים ריבועי. מתי
d חופשי מריבוע
O_L הינו תחום ראשי?

משפט (Heegner 1952, Stark 1967) השערה ידועה לגאוס. אם $d<0$, יש בדיוק תשעה מקרים:

$$\mathbb{Q}(\sqrt{-1}),\ \mathbb{Q}(\sqrt{-2}),\ \mathbb{Q}(\sqrt{-3}),\ \mathbb{Q}(\sqrt{-7}),\ \mathbb{Q}(\sqrt{-11}),$$
$$\mathbb{Q}(\sqrt{-19}),\ \mathbb{Q}(\sqrt{-43}),\ \mathbb{Q}(\sqrt{-67}),\ \mathbb{Q}(\sqrt{-163})$$

השערה (Cohen-Lenstra) ב-1983: עבור בערך 76% של $d>0$ חופשיים מריבועים, $O_{\mathbb{Q}(\sqrt{d})}$ תחום ראשי.

$$\lim_{k\to\infty}\frac{\left|\left\{d\le k:\ O_{\mathbb{Q}(\sqrt{d})}\ \text{תחום ראשי}\right\}\right|}{\left|\left\{d\le k:\ d\ \text{חופשי מריבועים}\right\}\right|}\sim 0.76\ldots$$

תרגיל (Fermat, 1640) יהי p ראשוני. אזי $p=a^2+b^2$ אם ורק אם $p=2$ או $p\equiv 1 \bmod 4$.

רמז $p=a^2+b^2 \iff$ קיים איבר של $\mathbb{Z}[\sqrt{-1}]$ מנורמה p.
$\Updownarrow$
$N(a+bi)=p$

$\iff p\in\mathbb{Z}[\sqrt{-1}]$ אינו ראשוני!