הרצאה 16

הגדרה חוג R נקרא תחום דדקינד אם R הוא תחום שלמות וגם

1) R נתרי

2) R סגור בשלמות.

3) כל אידיאל ראשוני לא אפסי של R הינו מקסימלי, ויש אידיאלים כאלה.

דוגמא K שדה מספרים, $\dim_{\mathbb{Q}} K<\infty$.

$\mathcal{O}_K=\{\alpha\in K:$ שלם מעל $\mathbb{Z}$ $\alpha\}$

חוג השלמים של K הוא תחום דדקינד

משפט יהי R תחום דדקינד, יהי $(0)\neq I\triangleleft R$ אידיאל (לאו בהכרח ראשוני) אזי $I=P_1P_2\cdots P_r$ מתפרק כמכפלה של אידיאלים ראשוניים של R, והפירוק הינו יחיד עד כדי החלפת סדר הגורמים.

הוכחה יהי $I\triangleleft R$ אידיאל, הוכחנו בפעם הקודמת כי I הינו מכפלה של אידיאלים ראשוניים. נשאר להוכיח יחידות.

נניח שיש לנו שני פירוקים:

$$I = P_1P_2\cdots P_r = Q_1Q_2\cdots Q_s.$$

אינדוקציה על r.

<u>$r=0$</u> אם כן $I = (\text{המכפלה הריקה}) = (1) = R$.

אז $R = Q_1\cdots Q_s \subseteq Q_1$

אם המכפלה של Q-ים לא ריקה.

וזה לא נכון, כי אידאל Q_1 אמיתי. לכן המכפלה של Q-ים גם ריקה.

<u>$r>0$</u> יהי $I = P_1P_2\cdots P_r = Q_1Q_2\cdots Q_s$.

כמו שאמרנו קודם, $Q_1Q_2\cdots Q_s = P_1P_2\cdots P_r \subseteq P_r$.

האידאל P_r ראשוני, לכן $Q_i \subseteq P_r$ עבור

אך P_r, Q_i שניהם מקסימליים. לכן $Q_i = P_r$

איזה $1 \le i \le s$. נכפיל את שני האגפים

בהפכי: $\{x\in \mathrm{Frac}\, R : xP_r \subseteq R\} = P_r^{-1} = Q_i^{-1}$.

$$IP_r^{-1} = P_1P_2\cdots \underbrace{P_rP_r^{-1}}_{R} = Q_1\cdots \underbrace{Q_iP_r^{-1}}_{R} Q_{i+1}\cdots Q_s$$

הוכחנו באמצע השיעור הקודם כי $P_rP_r^{-1}=R$.

$$IP_r^{-1} = P_1P_2\cdots P_{r-1} = Q_1\cdots Q_{i-1}Q_{i+1}\cdots Q_s$$

הוכחנו כי $(0) \neq IP_r^{-1} \triangleleft R$ אולי לא אמרנו.

באינדוקציה שני הפירוקים $P_1\cdots P_{r-1} = Q_1Q_2\cdots$

זהים עד כדי החלפת הסדר. (ובפרט $r=s$)

הערה המשפט הנ"ל הוא ההכללה ה"נכונה" של משפט היסודי של אריתמטיקה. ראינו שתחומי דדקינד אינם בהכרח תחומי פריקות יחידה. לדוגמא, $\mathbb{Z}[\sqrt{-5}]$. מתי הם כן תחומי פריקות יחידה?

טענה יהי R תחום דדקינד. אז R תפ"י $\Leftarrow$ R תחום ראשי.

הוכחה $(\Rightarrow)$ נכון לכל תחום.

$(\Leftarrow)$ מספיק להוכיח שכל אידאל ראשוני של R הוא ראשי.

בחוג חילופי

אזי, מכפלה של אידאלים ראשיים הינה ראשי $(ab)=(a)(b)$. אנו נוכיח שאם R תחום גאוסיני אז כל אידאל הינו מכפלה של ראשוניים.

יהי $(0) \neq P \triangleleft R$ ראשוני. יהי $a \in P$.

מניחים כי R גפ"י, לכן $a = p_1 p_2 \cdots p_r$ מתפרק למכפלה של אי-פריקים. אבל P ראשוני, לכן $p_i \in P$ עבור i מתאים. בגפ"י כל איבר אי-פריק הוא ראשוני, לכן $(p_i) \subseteq P$ אידאלים ראשוניים לא אפסיים. לכן מקסימליים, לכן $(p_i) = P$, לכן P ראשי.

יהי R תחום גאוסיני.

<u>הגדרה</u> אידאל שברי של R הוא תת-R-מודול נוצר סופית של $\operatorname{Frac} R$ <u>לא-אפסי</u>.

<u>טענה/תרגיל</u> יהי $\underline{a}$ אידאל שברי, אזי

$$\underline{a} = P_1 \cdots P_r Q_1^{-1} Q_2^{-1} \cdots Q_s^{-1}$$

באופן יחיד, כאשר $P_i, Q_i \triangleleft R$ ראשוניים.

תהי J_R החבורה של כל האידאלים
השבריים, תחת כפל.

אם לא רוצים לסמוך על הטענה,
נגדיר את J_R להיות החבורה האבלית
החופשית הנוצרת על ידי האידאלים הראשוניים
הלא אפסיים של R.

תהי P_R תת-החבורה של האידאלים
השבריים הראשיים Rx, $x\in \mathrm{Frac}\,R$.

$x=\frac{r}{s}$, $r,s\in R$

$xR=(r)(s)^{-1}$

לחלופין, $P_R=\{(r)(s)^{-1} : r,s\in R\}$

<u>הגדרה</u> נסמן $Cl_R={}^{J_R}/_{P_R}$ ונקרא חבורת
המחלקות של R. נשים לב כי

R תפ״י $\iff$ R תחום ראשי $\iff$ $Cl_R=\{e\}$.

לכן הסדר של Cl_R (מסומן h_R) הוא
מידה של כמה רחוק R מלהיות תפ״י.

משפט (Cleburn, 1963) תהי G חבורה אבלית. אזי קיים תחום דדקינד R עם $Cl_R \simeq G$.

משפט (מאה 19). יהי K שדה מספרים. אזי $Cl_{\mathcal{O}_K}$ סופית. נסמן $h_K = |Cl_{\mathcal{O}_K}|$.

נדון בשדות מספרים ריבועיים $K=\mathbb{Q}(\sqrt{d})$.

שני מקרים 1) $d<0$, K שדה ריבועי מדומה.

משפט (השערה של גאוס במאה ה-19, Heegner 1952, Stark 1967).

יהי $d<0$, $K=\mathbb{Q}(\sqrt{-d})$. אזי $h_K = 1 \iff$

$$d \in \{-1,-2,-3,-7,-11,-19,-43,-67,-163\}$$

(הוכחנו כי $\mathcal{O}_{\mathbb{Q}(\sqrt{-1})} = \mathbb{Z}[\sqrt{-1}]$ השלמים של גאוס, שהוא תחום אוקלידי, לכן תחום ראשי).

2) לכל d, $K=\mathbb{Q}(\sqrt{d})\subseteq\mathbb{R}$ שדה ריבועי ממשי.

<u>שאלה פתוחה</u> האם יש אינסוף של שדות ריבועיים ממשיים כך ש- $h_K=1$?

(<u>הערה</u>)

(Cohen-Lenstra heuristics) 1983 עבור 75.446% של

הראשוניים p, לשדה $K=\mathbb{Q}(\sqrt{p})$ מתקיים $h_K=1$.

הנושא הבא: מיון של מודולים נוצרים סופית מעל תחום ראשי.

נכין את השטח.

<u>הגדרה</u> יהיו M,N מודולים מעל חוג R.

$$M\times N=\{(m,n): m\in M,\ n\in N\}$$

$$(m_1,n_1)+(m_2,n_2)=(m_1+m_2,\ n_1+n_2)$$

$$r(m,n)=(rm,rn)$$

<u>טענה</u> יהי M מודול מעל חוג R. יהיו M_1,M_2 תת-מודולים. נניח כי

1) $M_1+M_2=\{m_1+m_2 : m_1\in M_1,\ m_2\in M_2\}=M$

2) $M_1\cap M_2=(0)$.

אזי $M\cong M_1\times M_2$.

הוכחה נגדיר $f: M_1 \times M_2 \longrightarrow M$

$$(m_1, m_2) \longmapsto m_1 + m_2$$

ברור שזה הומ' של מודולים.

f על בגלל 1), f חח"ע בגלל 2).

הגדרה R-מודול M נקרא ציקלי אם הוא נוצר על ידי איבר אחד, כלומר קיים $m \in M$ כך ש-

$$M = Rm = \{rm : r \in R\}$$

טענה יהי R חוג כלשהו. ויהי M R-מודול (שמאלי). אזי M ציקלי $\Longleftrightarrow$ קיים אידאל שמאלי $I \lhd_\ell R$ כך ש- $M \cong R/I$ (כמודולים).

$\{r(a+I) = ra + I\}$ מבנה המודול של R/I נתון ע"י

הוכחה (⇐) R/I נוצר על ידי $1+I$

$$r+I = r(1+I)$$

לכן R/I ציקלי!

(⇒) יהי M ציקלי, יהי $m\in M$ יוצר,

כלומר $M=Rm$. נגדיר העתקה

$$f: R \longrightarrow M$$

מסתכל על R כמודול מעל עצמו.

$$f(r) = rm$$

ברור שזה הומ' של R-מודולים.

f על כי m יוצר את M. לפי משפט איזו' I עבור מודולים.

$$M=f(R) \cong R/(\ker f)$$

אך $\ker f$ הוא תת-מודול של R, כלומר אידיאל שמאלי!

מסקנה תהי G חבורה ציקלית. אזי $G\cong\mathbb{Z}$ או $G\cong \mathbb{Z}/n\mathbb{Z}$.

הוכחה חבורה אבלית = $\mathbb{Z}$-מודול.

לפי הטענה הקודמת, G ציקלית $\Longleftrightarrow$ $G\cong \mathbb{Z}/I$

כחבורה אבלית, (= $\mathbb{Z}$-מודול) כאשר $I \trianglelefteq \mathbb{Z}$. ידוע לנו

$I=(0) \Longleftrightarrow \mathbb{Z}/I\cong\mathbb{Z}$

או $I=n\mathbb{Z}$.

עכשיו יהי R תחום ראשי.

טענה יהי R תחום ראשי, יהי $a,b\in R$.

אז $g\in R$ הינו gcd של a,b $\Longleftrightarrow$ $(g)=(a,b)$.

הוכחה מיידי.

טענה יהיו $a,b\in R$, כאשר R תחום ראשי.

יהי $g\in R$ gcd של a,b. אזי קיימים $x,y\in R$ כך ש- $g=xa+yb$.

הוכחה $g\in(a,b)$ לפי הטענה הקודמת.

__טענה__ יהי R תחום ראשי, יהי $n\geq 2$. יהיו

$c_1,\dots,c_n\in R$ שלמים כך ש-

$(c_1,\dots,c_n)=R \iff \gcd(c_1,\dots,c_n)=1$.

אזי קיימת מטריצה $A\in M_n(R)$ כך ש-

1) $\det A=1$.

2) העמודה הראשונה של A היא $\begin{pmatrix}c_1\\ \vdots\\ c_n\end{pmatrix}$.

__הוכחה__ אינדוקציה על n.

__$n=2$__ קיימים $x,y\in R$ כך ש- $xc_1+yc_2=1$

יהי $A=\begin{pmatrix}c_1 & -y\\ c_2 & x\end{pmatrix}$.

__$n>2$__ יהי $(g)=(c_1,\dots,c_{n-1})$. אז g לא

בהכרח הפיך. אבל $\gcd(g,c_n)=1$, לכן

קיימים $x,y\in R$ כך ש- $gx+c_ny=1$.

יותר מזה, יהיו

$c_1=gd_1$
$c_2=gd_2$
$\vdots$
$c_{n-1}=gd_{n-1}$

אזי $\gcd(d_1, \ldots, d_{n-1}) = 1$. לפי האינדוקציה

קיימת מטריצה $A' \in M_{n-1}(R)$ כך ש-

$\det A' = 1$ וגם העמוד הראשון הוא $\begin{pmatrix} d_1 \\ \vdots \\ d_{n-1} \end{pmatrix}$. יהי

$$A = \begin{array}{c} \qquad\qquad (n-1) \times (n-2) \\ \begin{pmatrix} c_1 & \multicolumn{3}{c}{\text{n-2 העמודות}} & \pm d_1 y \\ c_2 & \multicolumn{3}{c}{\text{הראשונות של}} & \pm d_2 y \\ \vdots & & A' & & \vdots \\ \vdots & & & & \pm d_{n-1} y \\ c_n & 0 & \cdots & 0 & x \end{pmatrix} \end{array}$$