הרצאה 23

<u>מסקנה</u> יהי R תחום דדקינד, אזי כל אידאל $R \trianglerighteq I \neq 0$ מתפרק באופן יחיד למכפלה של אידאלים ראשוניים.

<u>טענה</u> יהי R תחום דדקינד. אזי R תחום ראשי אם ורק אם R תפ"י.

<u>הוכחה</u> $\Leftarrow$) כל תחום ראשי הינו תפ"י.

$\Rightarrow$) נשים לב שהמכפלה של שני אידאלים ראשיים הינה ראשית:

$$IJ = \{\sum i_k j_k : i_k \in I,\ j_k \in J\}$$

$$I = (a) \qquad J = (b) \qquad IJ = \{\sum a x_k b y_k = ab \sum x_k y_k\} = (ab).$$

$$x_k, y_k \in R$$

נניח כי R תפ"י. רוצים להוכיח שהוא תחום ראשי. לכן, כיוון ש-R תחום דדקינד, מספיק להוכיח שכל אידאל ראשוני הינו ראשי.

אז יהי $R \trianglerighteq P \neq (0)$ אידאל ראשוני.

יהי $0\neq y\in P$. R תפ"י $\Leftarrow$ $y=p_1p_2\cdots p_r$

כאשר $p_i\in R$ אי-פריקים. אך

P ראשוני $\Leftarrow$ $p_1p_2\cdots p_r\in P$ $\Leftarrow$ $p_i\in P$

עבור איזה $1\le i\le r$.

R תפ"י $\Leftarrow$ p_i איבר ראשוני $\Leftarrow$ $0\neq(p_i)\trianglelefteq R$ אידיאל ראשוני.

אך $p_i\in P$ $\Leftarrow$ $(p_i)\subseteq P$. אך

$\dim R=1$ $\Leftarrow$ האידיאלים $(p_i), P$ שניהם מקסימליים

לכן שווים. לכן, $P=(p_i)$ ראשי.

<u>שאלה</u> האם יש דרך למדוד כמה רחוק תחום דדקינד

נתון הינו מלהיות תפ"י?

<u>תזכורת</u> לכל אידיאל ראשוני $0\neq P\trianglelefteq R$ ו-R תחום (דדקינד)

הגדרנו $P^{-1}=\{\alpha\in F:\ \alpha\beta\in R\ \ \forall\beta\in P\}$

$F=\mathrm{Frac}\ R$

הגדרה לכל אידיאל $0 \neq I \lhd R$,

$$I = P_1 P_2 \cdots P_r$$

נגדיר

$$I^{-1} = P_1^{-1} P_2^{-1} \cdots P_r^{-1}$$

$$= \left\{ \sum_{i=1}^{n} c_{i1} c_{i2} \cdots c_{ir} : c_{ij} \in P_j^{-1} \right\} \subseteq F$$

לפי הלמה 4 מן השיעור הקודם $PP^{-1} = R$,
נקבל $II^{-1} = R$.

הגדרה יהי R תחום דדקינד. אידיאל שברי של R הינו תת-R-מודול נוצר סופית של F.

הערה כל אידיאל של R הינו R-מודול נוצר סופית, כי R נתרי.

תוצאה לכל $0 \neq I \lhd R$, ה-R-מודול I^{-1} הינו אידיאל שברי. יותר מזה, כל אידיאל שברי X הינו מן הצורה IJ^{-1} עבור אידיאלים $I, J \lhd R$.

אבחנה: הקבוצה של האידיאלים השבריים הלא-אפסיים הינה חבורה אבלית (תחת כפל של אידיאלים שבריים).

נקרא לחבורה הנ"ל $\mathcal{J}_R$.

הגדרה: אידיאל שברי נקרא ראשי הינו אידיאל שברי מן הצורה aR, $a\in F$. $(aR)(bR)=(ab)R$
$(aR)^{-1}=a^{-1}R$

תה׳ תת-החבורה של האידיאלים השבריים הראשיים $\mathcal{P}_R\leq\mathcal{J}_R$.

הגדרה: חבורת המחלקות של R הינה המנה $Cl_R=\mathcal{J}_R/\mathcal{P}_R$.

טענה: R מפ"י $\Leftrightarrow$ תחום ראשי, כי R תחום דדקינד אם ורק אם $Cl_R=\{0\}$.

הוכחה: $(\Leftarrow)$ נניח Cl_R טריוויאלית, אזי $\mathcal{J}_R=\mathcal{P}_R$.
לכן כל אידיאל $I\trianglelefteq R$ מקיים $I\in\mathcal{P}_R$,

לכן I ראשי.

$\Leftarrow$) נניח R תחום ראשי. אז $I \triangleleft R \Leftarrow$

$I \in \mathcal{P}_R$. לפי ההגדרה, כל אידיאל שברי

הינו מן הצורה IJ^{-1} ולכן ראשי.

<u>הערה</u> הסדר של Cl_R מודד כמה רחוק R

מלהיות תחום ראשי $\Leftrightarrow$ תפ"י!

<u>דוגמא</u> $Cl_{\mathbb{Z}[\sqrt{-5}]} \simeq \mathbb{Z}/2\mathbb{Z}$. בפרט, יהי $I \triangleleft \mathbb{Z}[\sqrt{-5}]$.

אז I לא בהכרח ראשי, אבל I^2 ראשי.

<u>משפט</u> 1) לכל חבורה אבלית G, קיים תחום

דדקינד R כך ש- $Cl_R \simeq G$.

(Cleburn, 1963).

2) יהי F שדה מספרים. אזי $Cl_{\mathcal{O}_F}$

סופית.

<u>שאלה</u> יהי $F = \mathbb{Q}(\sqrt{d})$. מה אפשר להגיד על $Cl_{\mathcal{O}_F}$?

<u>מקרה 1</u> $d<0$. <u>משפט</u> (השערה של גאוס, הוכחות של Heegner 1952, Stark 1969)

השדות היחידים מן הצורה $\mathbb{Q}(\sqrt{d})$, $d<0$, כך ש- $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ הינו תפ"י הינם

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

$$e^{\pi\sqrt{163}} = 262537412640768743.99999999999925\ldots$$

כמעט שלם.

<u>משפט</u> הסדרה $\{|Cl_{\mathcal{O}_{\mathbb{Q}(\sqrt{d})}}|\}$ מתבדרת ל-∞.

<u>מקרה 2</u> $d>0$, $\mathbb{Q}(\sqrt{d})$.

<u>שאלה פתוחה</u> האם יש מספר אינסופי של שדות $\mathbb{Q}(\sqrt{d})$, $d>0$, כך ש- $Cl_{\mathcal{O}_{\mathbb{Q}(\sqrt{d})}}=\{1\}$?

<u>השערה</u> (Cohen-Lenstra, 1983) כן. בערך $75.446\ldots\%$

מן השדות האלה מקיימים $|Cl_{\mathcal{O}_{\mathbb{Q}(\sqrt{d})}}|=\{e\} \Leftrightarrow$

$\mathcal{O}_F$ תפ"י

מאיפה המספר הזה?

$$0.75446\ldots = \prod_{n=1}^{\infty}\left(1-\frac{1}{2^n}\right)\cdot\prod_{n\geq 2}\zeta(n)$$

$$\zeta(n)=\sum_{k=1}^{\infty}\frac{1}{k^n}$$

<u>הגדרה</u> יהי R חוג חילופי. R נקרא מקומי אם יש לו אידאל מקסימלי יחיד.

<u>דוגמאות</u> 1) שדה ((0) האידאל המקסימלי היחיד).

2) $\mathbb{Z}/p^n\mathbb{Z}$ האידאל (p) מקסימלי יחיד.

3) יהי R חוג חילופי, $P \triangleleft R$ אידאל

סימון: $S = R \setminus P$.

<u>המיקום</u> $S^{-1}R$ הינו חוג מקומי.

(תרגיל: התאמה בין אידאלים של $S^{-1}R$ ואידאלים של R שמוכלים ב-P).

4) $\mathbb{Z}$ <u>לא</u> מקומי.

$(R \neq (0))$

<u>טענה</u> יהי R חוג חילופי. התנאים הבאים שקולים:

1) R מקומי.

2) הקבוצה $\{r \in R :$ r לא הפיך$\}$ הינה אידיאל.

3) לכל $r \in R$, לפחות אחד מן האיברים r, $1-r$ הינו הפיך.

<u>הוכחה</u> <u>1)$\Leftarrow$2)</u> יהי R מקומי, $M \lhd R$ האידיאל המקסימלי היחיד. אם $r \in R \setminus M$, אזי r הפיך. אחרת, (r) הינו אידיאל אמיתי, אך $(r) \not\subseteq M$, אך (r) מוכל באידיאל מקסימלי, לכן יש אידיאל מקסימלי שונה מ-M בסתירה להנחה.

כל איבר של M לא הפיך. לכן

$$M = \{r \in R : r \text{ לא הפיך}\}$$

ולכן הקבוצה לעיל הינה אידיאל.

2) $\Leftarrow$ 3) יהי $I=\{r\in R:$ r לא הפיך$\}$, לפי

ההנחה זה אידיאל אמיתי ($1\notin I$). יהי $r\in R$.

נניח בשלילה כי $r, 1-r$ שניהם לא הפיכים.

אז $r, 1-r\in I \Leftarrow r+(1-r)=1\in I$, סתירה.

3) $\Leftarrow$ 1) נניח לכל $r\in R$ כי לפחות אחד מ- $r, 1-r$

הפיך. נניח בשלילה כי R לא מקומי,

ויהיו M_1, M_2 אידיאלים מקסימליים שונים.

אז $M_1 \subsetneq M_1+M_2 \trianglelefteq R \Leftarrow M_1+M_2=R$.

אז קיימים איברים $r\in M_1$, $s\in M_2$ כך ש-

$r+s=1$. אבל $r\in M_1 \Leftarrow$ r לא הפיך.

$1-r=s\in M_2 \Leftarrow$ 1-r לא הפיך.

בסתירה להנחה.

הערה (נובע מן ההוכחה $1 \Rightarrow 2$) יהי R חוג מקומי, $M \triangleleft R$ האידיאל המקסימלי. אזי

$$M = \{ r \in R : r \text{ לא הפיך} \}$$

דוגמאות אחרות של חוגים מקומיים.

4) יהי F שדה, $R = F[[x]]$.

יהי $M = (x)$

$$= \{ a_1 x + a_2 x^2 + \dots \}$$

ידוע מן התרגול כי כל איבר במשלים של M (כלומר, כל טור חזקות $a_0 + a_1 x + \dots$, $a_0 \neq 0$) הפיך. לכן

$M = (x) = \{ r \in R : r \text{ לא הפיך} \}$ אידיאל,

לכן R מקומי (לפי הגדרה 2) ו-(x) הינו האידיאל המקסימלי היחיד לפי ההערה.

5) יהי $C \subseteq \mathbb{R}^n$ עקומה ג"ז $x \in C$.

נביט בחוג

$R = \{$ פונקציות שמוגדרות בסביבה פתוחה של x $\}$

זה חוג מקומי, האידיאל המקסימלי הינו

$M = \{ f \in R : f(x) = 0 \}$