הרצאה 22

<u>הגדרה</u> יהי R חוג חילופי. הוא נקרא תחום דדקינד אם:

1) R תחום שלמות.

2) R נתרי.

3) $\dim R = 1$ (כל אידיאל ראשוני לא אפסי מקסימלי)
ו-R לא שדה.

4) R סגור בשלמות.

<u>הגדרה</u> יהי R תחום שלמות. יהי $0 \neq P \triangleleft R$ אידיאל ראשוני, $F = \mathrm{Frac}\, R$

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

זה תת-R-מודול של F.

בסוף השיעור הקודם הוכחנו:

<u>למה 2</u> יהי R תחום שלמות נתרי, $\dim R = 1$.
יהי $0 \neq P \triangleleft R$ אידיאל ראשוני אזי $R \subsetneq P^{-1}$.

<u>הגדרה</u> יהיו M, N תת-R-מודולים של F.
נגדיר את המכפלה

$$MN = \{\sum m_i n_i \ : \ m_i \in M, \ n_i \in N\} \subseteq F$$

זה גם תת-R-מודול של F.

<u>למה 3</u> יהי R תחום דדקינד. יהי $0 \neq P \triangleleft R$ אידיאל ראשוני, $0 \neq I \triangleleft R$ אידיאל כלשהו. אזי $I \subsetneq IP^{-1}$.

הוכחה נשים לב כי $1 \in R \subseteq P^{-1}$, לכן $I \subseteq IP^{-1}$.

נניח בשלילה שהטענה לא נכונה. אזי $I = IP^{-1}$.

יהי $s \in P^{-1} \setminus R$, איבר כזה קיים לפי למה 2.

לכל $a \in I$, $sa \in IP^{-1} = I$.

לכן I סגור לכפל עם איברים של החוג $F \supseteq \underbrace{R[s]}_{\text{תת-חוג הכי קטן של } F \text{ שמכיל את } R\cup\{s\}} \supseteq R$. לכן I הינו $R[s]$-מודול נאמן

(מדוע נאמן? אם $y \in Ann_{R[s]}(I)$, אזי $ya = 0$ לכל $a \in I$. הנחנו $I \neq 0$, לכן יש $0 \neq a \in I$. אך F שדה, לכן $ya = 0 \Rightarrow y = 0$. לכן $Ann_{R[s]}(I) = (0)$).

R נותרי, לכן האידיאל $I \trianglelefteq R$ נוצר סופית כ-R-מודול.

לכן $s \in F$ שלם מעל R (לפי התנאי 4 מבין התנאים השקולים שהוכחנו בהרצאה 20).

אבל, R סגור בשלמות, לכן $s \in R$. סתירה, שהרי הנחנו $s \in P^{-1} \setminus R$.

למה 4 יהי R תחום דדקינד. יהי $0\neq P \lhd R$ אידאל ראשוני. אזי $PP^{-1}=R$.

הוכחה $PP^{-1}\subseteq R$ לפי הגדרה של P^{-1}. אזי PP^{-1} R-מודול, לכן $PP^{-1}\lhd R$ אידאל (אולי לא אמיתי).

מצד שני, $P \underset{\text{למה 3}}{\subsetneq} PP^{-1} \subseteq R$.

אזי P מקסימלי, כי $\dim R=1$, לכן בהכרח $PP^{-1}=R$.

משפט יהי R תחום דדקינד. יהי $0\neq I\lhd R$ אידאל. אזי $I=P_1P_2\cdots P_r$ כאשר $P_i\lhd R$ אידאלים ראשוניים. בנוסף, הפירוק הזה יחיד: אם $I=P_1P_2\cdots P_r=Q_1Q_2\cdots Q_s$, אזי $r=s$ וקיימת תמורה $\sigma\in S_r$ כך ש- $Q_i=P_{\sigma(i)}$ לכל $1\leq i\leq r$.

הוכחה יהי R תחום דדקינד, $0\neq I\lhd R$ אידאל.

קיום של הפירוק תהי

$$S=\{0\neq I\lhd R : \text{I לא מכפלה של אידאלים ראשוניים}\}$$

אנחנו טוענים כי $S=\emptyset$. נניח בשלילה כי $S\neq\emptyset$.

R נתרי, לכן יש איבר מקסימלי $I \in \mathcal{A}$.
כיוון כי I לא הפיך (אחרת הוא בפרט מכפלה של ראשוניים). לכן קיים אידאל מקסימלי (ולכן ראשוני) P $I \subsetneq P$.

לפי למה 4, $IP^{-1} \subseteq PP^{-1} = R$.

לכן $IP^{-1} \trianglelefteq R$ אידאל. לפי הלמה 3, $I \subsetneq IP^{-1}$,
לכן $IP^{-1} \notin \mathcal{A}$. לכן $IP^{-1} = P_1P_2\cdots P_r$
(כאשר R הינה המכפלה הריקה).

לכן

$$I = IR = IP^{-1}P = P_1P_2\cdots P_rP$$

בסתירה להנחה $I \in \mathcal{A}$.

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

נניח בלי הגבלת הכלליות כי $s \le r$. נעשה אינדוקציה על r.

<u>$r=0$</u>

$$\left(\text{מכפלה ריקה}\right) = R = Q_1Q_2\cdots Q_s$$

האגף הימני גם חייב להיות מכפלה ריקה.
כי אחרת $Q_1Q_2\cdots Q_s \subseteq Q_1 \subsetneq R$ בסתירה.

(תזכורת: אידיאלים ראשוניים הפיכים לפי הקודם).

<u>אינדוקציה</u> נניח שהטענה ידועה עבור $r-1$.

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

בפרט, $Q_1Q_2\cdots Q_s=I\subseteq P_r$.

P_r ראשוני, לכן $Q_i\subseteq P_r$ עבור i מסוים. נמספר מחדש את ה-Q_i-ים, נוכל להניח בלי הגבלת הכלליות כי $Q_s\subseteq P_r$. שניהם אידיאלים מקסימליים של R, לכן $Q_s=P_r$. לכן

$$P_1P_2\cdots P_{r-1}=P_1P_2\cdots P_{r-1}(\overset{\overset{\text{לפי למה 4}}{R}}{\overset{\shortparallel}{P_rP_r^{-1}}})=IP_r^{-1}=$$
$$IQ_s^{-1}=Q_1\cdots Q_sQ_s^{-1}=Q_1\cdots Q_{s-1}.$$

באינדוקציה נובע כי $r-1=s-1\Leftarrow r=s$,

וכי $P_1,\dots,P_{r-1}$ הם $Q_1,\dots,Q_{s-1}$

עד כדי מספור מחדש של ה-Q_i-ים.

<u>הגדרה</u> יהי F שדה. הוא נקרא שדה מספרים אם $\mathbb{Q}\subseteq F$ וגם $\dim_{\mathbb{Q}}F<\infty$.

<u>לדוגמא</u> $\mathbb{Q}(\sqrt{d})$ שדה מספרים, $\mathbb{R}$ לא שדה מספרים.

<u>טענה</u> יהי F שדה מספרים. (בפרט, $\mathbb{Z}\subseteq\mathbb{Q}\subseteq F$)

יהי $\mathcal{O}_F$ הסגור השלם של $\mathbb{Z}$ ב-F. אזי $\mathcal{O}_F$ הינו תחום דדקינד.

<u>הערה</u> בשיעור הקודם ראינו כי $\mathcal{O}_{\mathbb{Q}(\sqrt{-5})}=\mathbb{Z}[\sqrt{-5}]$.

לפי הטענה, $\mathbb{Z}[\sqrt{-5}]$ תחום דדקינד, אך אנחנו יודעים שהוא לא תפ"י (ועקב לא תחום gcd).

<u>עובדה</u> יהי F שדה מספרים. יהי $d=\dim_{\mathbb{Q}}F$. אזי $\mathcal{O}_F$ הינו $\mathbb{Z}$-מודול חפשי והוא נוצר על ידי d איברים.

<u>הערה</u> במקרה של $d=2$ הוכחנו את זה, שהרי

$$\mathcal{O}_{\mathbb{Q}(\sqrt{d})}=\begin{cases}\mathbb{Z}[\sqrt{d}]=\mathbb{Z}\cdot 1+\mathbb{Z}\cdot\sqrt{d}, & d\equiv 2,3 \mod 4\\ \mathbb{Z}\cdot 1+\mathbb{Z}\cdot\frac{1+\sqrt{d}}{2}, & d\equiv 1 \mod 4\end{cases}$$

<u>הערה</u> יהי F שדה מספרים, יהי $\dim_{\mathbb{Q}}(F)=2$.

אזי $F\simeq\mathbb{Q}(\sqrt{d})$ עבור d חפשי מריבועים.

<u>הוכחה</u> (של הערה). יהי $\{1,\beta\}$ $\mathbb{Q}$-בסיס של F. הקבוצה $\{1,\beta,\beta^2\}$ בהכרח

לפי הנ"ל, לכן יש תלות לינארית

$a_2\beta^2 + a_1\beta + a_0\cdot 1 = 0$, $a_1, a_2, a_0 \in \mathbb{Q}$.
$(a_0, a_1, a_2) \neq (0,0,0)$

בהכרח $a_2 \neq 0$, כי $\{1,\beta\}$ בסיס. בלי הגבלת הכלליות, $a_2 = 1$.

$$\beta^2 + a_1\beta + a_0\cdot 1 = 0$$

השלמת הריבוע:

$$\left(\beta + \frac{a_1}{2}\right)^2 = \beta^2 + a_1\beta + \frac{a_1^2}{4} = \frac{a_1^2}{4} - a_0.$$

לכן:

$$(*) \quad "\beta + \frac{a_1}{2} = \sqrt{\frac{a_1^2}{4} - a_0}\,"$$

נשים לב כי $\{1, \beta + \frac{a_1}{2}\}$ גם בסיס של F.

עכשיו, נשים כי $\frac{m}{n} = \frac{a_1^2}{4} - a_0 \in \mathbb{Q}$ לכן $m,n\in\mathbb{Z}$

בהכרח שלם. נכפיל את שני האגפים של $(*)$ ב-n^2.

$$\left(n\cdot\left(\beta + \frac{a_1}{2}\right)\right)^2 = mn \in \mathbb{Z}$$

אם mn לא חופשי מריבועים, אזי יהי $c\in\mathbb{Z}$ כך ש- $mn = c^2 d$ כאשר d חופשי מריבועים. אזי

$$\left(\frac{n}{c}\left(\beta + \frac{a_1}{2}\right)\right)^2 = d$$

יהי $\gamma = \frac{n}{c}\left(\beta+\frac{a_1}{2}\right) \in F$. אזי $\{1,\gamma\}$ זה

$\mathbb{Q}$- בסיס של F. ההעתקה

$$F \longrightarrow \mathbb{Q}(\sqrt{d})$$
$$a+\gamma b \longmapsto a+b\sqrt{d}$$

$a,b \in \mathbb{Q}$.

אני משאיר לכם לבדוק שזה איזומורפיזם.

חוזרים לטענה:

<u>טענה</u> F שדה מספרים, $\mathcal{O}_F$ הסגור השלם של $\mathbb{Z}$ ב-F. אזי $\mathcal{O}_F$ הינו חוג דדקינד.

<u>הוכחה</u> נבדוק את ארבעת התנאים של חוג דדקינד.

1) תחום שלמות, אזי $\mathcal{O}_F \subseteq F$ תת-חוג של שדה.

2) צריך להוכיח כי $\mathcal{O}_F$ נתרני: נשתמש בעובדה הנ"ל. יהיו $m_1, m_2, \dots, m_g \in \mathcal{O}_F$ ($g = \dim_{\mathbb{Q}} F$)

אלגבריים שלמים אז $\mathcal{O}_F$ נ"ס $\mathbb{Z}$-מודול:

$$\mathcal{O}_F = \mathbb{Z}m_1 + \mathbb{Z}m_2 + \dots + \mathbb{Z}m_s$$

נזכיר הומ' של חוגים (הומ' של הצבה)

$$f : \mathbb{Z}[x_1, x_2, \dots, x_s] \longrightarrow \mathcal{O}_F$$

$$f\left(\sum_{i_1=0}^{n_1} \cdots \sum_{i_s=0}^{n_s} a_{i_1,\dots,i_s} x_1^{i_1} x_2^{i_2} \cdots x_s^{i_s}\right) =$$

$$\sum a_{i_1,\dots,i_s} m_1^{i_1} m_2^{i_2} \cdots m_s^{i_s}$$

f הינו הומ' (צמצום של הומ' ההצבה מתחילת הקורס). בנוסף, f הינו על. אכן, לכל $m \in \mathcal{O}_F$ קיים

$$m = a_1 m_1 + \dots + a_s m_s = f(a_1 x_1 + \dots + a_s x_s)$$

$$a_i \in \mathbb{Z}$$

יהי $I = \ker f$. לפי משפט האיז' הראשון,

$$\mathcal{O}_F \simeq \mathbb{Z}[x_1, \dots, x_s] / I$$

אנחנו יודעים כי $\mathbb{Z}$ נותרי. לכן $\mathbb{Z}[x_1, \dots, x_s]$ נותרי לפי משפט הבסיס של הילברט. מנה של חוג נותרי הינה נותרי. לכן $\mathcal{O}_F$ נותרי.

3) צריך להוכיח כי $\dim \mathcal{O}_F = 1$.

יהי $0\neq P \lhd \mathcal{O}_F$ אידיאל ראשוני. אזי

$P\cap\mathbb{Z}$ הינו אידיאל ראשוני של $\mathbb{Z}$. (בבירור!)

אזי נוכיח כי $P\cap\mathbb{Z}\neq(0)$. אכן, יהי $0\neq y\in P$.

אזי y שלם מעל $\mathbb{Z}$, לכן

$$y^n + a_{n-1}y^{n-1}+\dots+a_1y+a_0=0, \quad a_i\in\mathbb{Z}$$

$$a_0\neq 0$$

$$0\neq a_0 = -y\left(y^{n-1}+a_{n-1}y^{n-2}+\dots+a_1\right)\in\mathbb{Z}\cap P$$

לכן $P\cap\mathbb{Z}=p\mathbb{Z}$, כאשר p ראשוני!

נזכיר: $\mathcal{O}_F$ הינו $\mathbb{Z}$-מודול.

P הינו תת-$\mathcal{O}_F$-מודול, לכן תת-$\mathbb{Z}$-מודול

לכן $\mathcal{O}_F/P$ הינו $\mathbb{Z}$-מודול, הוא נוצר

ע"י $m_1+P,\dots,m_s+P$.

נשים לב כי $(p\in \mathrm{Ann}_{\mathbb{Z}}\mathcal{O}_F/P$

כי $p\in P\cap\mathbb{Z}\subseteq P$

לכן מקבלים מבנה של $\mathbb{Z}/p\mathbb{Z}$ -מודול על $\mathcal{O}_F/p$.

ו- $\mathcal{O}_F/p$ נוצר סופית מעל $\mathbb{Z}/p\mathbb{Z}$.

אבל $\mathbb{Z}/p\mathbb{Z}$ חוג סופי, לכן $\mathcal{O}_F/p$ סופי.

לכן $\mathcal{O}_F/p$ תחום שלמות סופי, לכן שדה,
לכן p מקסימלי.

<u>טענה</u> יהי R תחום שלמות סופי, אזי R שדה.

<u>הוכחה</u> יהי $0\neq a\in R$. צריך להוכיח
כי a הפיך. אך לפי כלל השובך,
קיימים $m<n$ טבעיים כך ש- $a^m=a^n$

בפרט $a^m\cdot 1=a^m\cdot a^{n-m}$

R תחום שלמות, לכן אפשר לצמצם:
$1=a^{n-m}=a(a^{n-m-1})$, לכן a הפיך.
לכן R שדה.