הרצאה 15

^ תזכורת/הגדרה: תחום שלמות R נקרא
תחום דדקינד אם

א) R נתרי

ב) R סגור בשלמות (כל איבר ב-$\mathrm{Frac}\,R$
שהוא שלם מעל R מוכל ב-R).

ג) $K\text{-}\dim(R)=1$: כל אידיאל ראשוני
לא אפסי הינו מקסימלי, ויש אידיאלים ראשוניים לא אפסיים. בפרט, R לא שדה.

<u>הערה</u> $\mathbb{Z}$ הוא תחום דדקינד.

<u>הגדרה</u> שדה K נקרא שדה מספרים
אם $\mathbb{Q}\subseteq K$ וגם $\dim_{\mathbb{Q}} K$ סופי:
$\mathbb{Q}(\sqrt{d})$ שדה מספרים, $\mathbb{R}$, $\mathbb{C}$ לא!

<u>הגדרה</u> יהי K שדה מספרים.

$$O_K=\{\alpha\in K:\ \alpha \text{ שלם מעל } \mathbb{Z}\}$$

צ"ל חוג, בנוסף $K=\mathrm{Frac}\,O_K$ (מיידי).

<u>טענה</u> לכל שדה מספרים K, החוג O_K הינו
תחום דדקינד.

<u>עובדה</u> יהי K שדה מספרים. יהי $n=\dim_{\mathbb{Q}}K$.
אזי יש n איברים $\alpha_1,\alpha_2,\dots,\alpha_n\in\mathcal{O}_K$ כך
ש- $\mathcal{O}_K$ הינו $\mathbb{Z}$-מודול חפשי עם בסיס $\mathbb{Z}$.

$$\mathcal{O}_K=\{b_1\alpha_1+b_2\alpha_2+\dots+b_n\alpha_n : b_i\in\mathbb{Z}\}$$

ואז כל איבר של $\mathcal{O}_K$ ניתן לרשום באופן
יחיד בצורה כנ"ל

<u>הערה</u> אם $n=\dim_{\mathbb{Q}}K=2$, אזי $K=\mathbb{Q}(\sqrt{d})$,
ואז α_1,α_2 הינו בסיס של $\mathcal{O}_K$,
כאשר $\alpha_1=1$

$$\alpha_2=\begin{cases}\sqrt{d} & : d\equiv 2,3 \mod 4\\ \frac{1+\sqrt{d}}{2} & : d\equiv 1 \mod 4\end{cases}$$

<u>הגדרה</u> יהיו $R\subset S$ חוגים חילופיים. נאמר S
שלם מעל R $\Longleftrightarrow$ כל $s\in S$ שלם מעל R.

<u>דוגמא</u> $\mathcal{O}_K$ שלם מעל $\mathbb{Z}$.

<u>טענה</u> יהי S שלם מעל R. יהי $0\neq P\triangleleft S$
אידאל ראשוני. אזי $P\cap R$ הינו
אידאל ראשוני לא אפסי של R.

<u>הוכחה</u> נשים לב כי R,P שניהם סגורים לחיבור וגם סגורים לכפל עם איברים של R. לכן $P\cap R$ סגור לשני הפעולות האלה, ולכן $P\cap R \trianglelefteq R$. בנוסף, יהיו $a,b\in R$ כך ש- $ab\in P\cap R$. בפרט, $a,b\in S$ כך ש- $ab\in P$.

אך P ראשוני, לכן $a\in P\cap R$ או $b\in P\cap R$. לכן $P\cap R$ הוא אידיאל ראשוני של R.

יהי $\alpha\in P$ ויהי $f_\alpha\in R[x]$ הפולי' המינימלי.

$$\alpha^n + r_{n-1}\alpha^{n-1} + \dots + r_1\alpha + r_0 = 0$$

$$r_0 = -\alpha\left(r_1 + r_2\alpha + \dots + r_{n-1}\alpha^{n-2} + \alpha^{n-1}\right)\in P.$$

אך $r_0\neq 0$, אחרת היינו יכולים לחלק ב-x ולקבל פולי' ממעלה נמוכה יותר עם שורש α.

אז $0\neq r_0\in R\cap P$, לכן $R\cap P\neq(0)$.

<u>טענה</u> יהי K שדה מספרים. החוג $\mathcal{O}_K$ הינו חוג דדקינדי.

<u>הוכחה</u> $\mathcal{O}_K$ הינו תת-חוג של שדה, לכן
אין בו מחלקי אפס כי בשדה אין מחלקי
אפס. לכן $\mathcal{O}_K$ תחום שלמות.

לפי הטענה, $\mathcal{O}_K$ נוצר סופית מעל $\mathbb{Z}$. אך
$\mathbb{Z}$ נתרי, לכן כל חוג נוצר סופית מעליו
גם נתרי.

יהי $(0)\neq P \triangleleft \mathcal{O}_K$ אידיאל ראשוני לא אפסי.
לפי הטענה הקודמת, $\mathbb{Z}\cap P$ הינו
אידיאל ראשוני לא-אפסי של $\mathbb{Z}$, לכן
$p\mathbb{Z} = \mathbb{Z}\cap P$, כאשר p ראשוני. זה אומר
כי $p\in P$. זה אומר כי (לפי הטענה)

$$pb_1\alpha_1 + pb_2\alpha_2 + \cdots + pb_n\alpha_n \in P$$

לכל $b_i\in\mathbb{Z}$. זה אומר שבמנה $\mathcal{O}_K/P$
יש רק מספר סופי של מחלקות, כי
כל $\beta\in\mathcal{O}_K$ שקול מודולו P לאחד האיברים

$$c_1\alpha_1 + \cdots + c_n\alpha_n, \qquad 0\le c_i\le p-1$$

p^n איברים כאלה.
אכן יהי $\beta=\sum b_i\alpha_i$ ו- $c_i\equiv b_i \mod p$ לכל i.

סוף $\beta \equiv \sum c_i \alpha_i$ מודולו P.

לכן $\mathcal{O}_K/P$ הוא תחום שלמות (כי P ראשוני)
סופי. כל תחום שלמות סופי הינו שדה
(הוכחנו לפני פסח), לכן $\mathcal{O}_K/P$ שדה $\Leftarrow$
P מקסימלי.

נשאר להוכיח כי $\mathcal{O}_K$ סגור בשלמות.

<u>תרגיל</u> יהיו $R \subset S \subset T$ חוגים חילופיים.
נניח כי S שלם מעל R. יהי
$t \in T$. אזי t שלם מעל S $\Leftrightarrow$ t שלם מעל R.

<u>הוכחה</u> ($\Rightarrow$) אם t שלם מעל R, אז הוא
שורש של פולינום מתוקן עם מקדמים ב-R
אך $R \subset S$, לכן אותו פולינום הוא פולי
מתוקן ב-$S[x]$.

($\Leftarrow$) נניח t שלם מעל S. זה אומר
כי $S[t]$ נוצר סופית כ-S מודול.

יהי $S[t] = St_1 + St_2 + \dots + St_m$

(עבור $t_1,\dots,t_m \in T$). לכן

$$t\in S[t] \Rightarrow t = s_1t_1+\dots+s_mt_m$$

עבור $s_1,\dots,s_m \in S$ שהם כולם שלמים

מעל R. לכן $R[s_i]$ נוצר סופית

כמודולים מעל R, לכן $R[s_1,\dots,s_m]$

גם R-מודול נוצר סופית. אז

$$R[s_1,\dots,s_m] = Ru_1+\dots+Ru_\ell$$

יהי $M\subset T$ ה-R-מודול הנוצר על ידי

u_it_j, $1\le i\le \ell$, $1\le j\le m$. וגם על ידי 1.

M הינו R-מודול נאמן (בגלל איבר היחידה)

והוא R-מודול נוצר סופית. גם $t\in M$

כי $s_j = \sum r_{ij}u_i$, $r_{ij}\in R$.

$$t = s_1t_1+\dots+s_mt_m = \sum r_{ij}u_it_j \in M.$$

...

נוכל להשלים את ההוכחה.

חוגיים ל- $\mathcal{O}_K$. המצב שלנו הוא

$\mathbb{Z} \subset \mathcal{O}_K \subset K$, $\mathcal{O}_K$ שלם מעל $\mathbb{Z}$.

יהי $x \in K = \mathrm{Frac}\,\mathcal{O}_K$ שלם מעל $\mathcal{O}_K$. לפי הטענה הקודמת, x שלם מעל $\mathbb{Z}$, ואז $x \in \mathcal{O}_K$ לפי ההגדרה של $\mathcal{O}_K$.

לכן $\mathcal{O}_K$ סגור בשלמות, והוכחנו כי $\mathcal{O}_K$ חוג דדקינד.

יהי R חוג דדקינד. לכל אידאל $I \lhd R$ נגדיר

$$I^{-1} = \{x \in F = \mathrm{Frac}\,R : xI \subseteq R\}$$

" $xa \in R$ לכל $a \in I$.

כמובן $R \subseteq I^{-1}$ כי I אידאל. הוכחנו בסוף השיעור הקודם שלכל I מתקיים $I^{-1} \supsetneq R$.

טענה: יהי R חוג דדקינד. יהי $(0) \neq P \lhd R$ אידאל ראשוני לא אפס. אז $PP^{-1} = R$.

<u>תזכורת</u> $PP^{-1}=\{a_1b_1+a_2b_2+\dots+a_mb_m : \begin{matrix} a_i\in P \\ b_i\in P^{-1}\end{matrix}\}$.

<u>הוכחה</u> ברור כי $PP^{-1}\subseteq R$. (לפי ההגדרה של P^{-1}, $a_ib_i\in R$). יותר מזה, PP^{-1} סגורה לחיבור וגם לכפל עם איברים של R (כי P סגור לכפל עם איברים של R).

לכן $PP^{-1}\trianglelefteq R$ אידיאל (אולי לא אמתי).

נשים לב כי $1\in R\subseteq P^{-1}$. לכן $P\subseteq PP^{-1}$ (לכל $x\in P$, $x=x\cdot 1\in PP^{-1}$). נניח בשלילה כי PP^{-1} אידיאל אמתי. אבל P מקסימלי.

לכן $PP^{-1}=P$. יהי $x\in P^{-1}\setminus R$, לפי הטענה האחרונה של השיעור הקודם, x כזה קיים. לכן, לכל $a\in P$,

$ax\in PP^{-1}=P$, לכן P סגור לכפל עם כל איבר של התת-חוג $R[x]\subseteq F=\mathrm{Frac}R$.

לכן, ל-P יש מבנה טבעי של $R[x]$-מודול. יותר מזה, R נתרי. לכן האידיאל P נוצר סופית (כ-R-מודול).

בנוסף, P הינו $R[x]$-מודול נאמן כי

$$Ann_{R[x]}(P) = \{y \in R[x]^{\subseteq F} : ay = 0 \ \forall a \in P\}.$$

אך $P \neq (0)$. וגם הכל קורה בתוך השדה

F, שאין בו מחלקי אפס. לכן

$Ann_{R[x]}(P) = 0$, לכן P הינו $R[x]$-מודול

נאמן. לפי אפיון השלמות מן השבוע שעבר,

x שלם מעל R.

אבל R סגור בשלמות $\Leftarrow x \in R$.

סתירה להנחה כי $x \notin R$. לכן $PP^{-1} = R$.

<u>משפט</u> יהי R תחום דדקינד. יהי $(0) \neq I \triangleleft R$

אידאל לא אפסי. אזי I מתפרק

למכפלה של אידאלים ראשוניים (לא אפסיים)

$I = P_1 P_2 \cdots P_r$. הפירוק יחיד עד כדי

החלפת סדר הגורמים.

<u>הוכחה</u> קיום של הפירוק: יהי $(0)\neq I\trianglelefteq R$,

יהי P אידיאל מקסימלי כך ש- $I\subseteq P$.

נניח בשלילה שאין ל-I פירוק לגורמים ראשוניים. נניח ש-I אידיאל מקסימלי ביחס לתכונה הנ"ל ($I\subsetneq J \Rightarrow J$ מתפרק)

אפשר להניח את זה כי R נתרי.

<u>תת-טענה</u> $IP^{-1}\subsetneq R$

<u>תת-הוכחה</u> $IP^{-1}=\{a_1b_1+\dots+a_mb_m : a_i\in I,\ b_i\in P^{-1}\}$

כמו בהוכחה הקודמת, $I\subseteq IP^{-1}\trianglelefteq R$.

נניח בשלילה כי $IP^{-1}=R=PP^{-1}$

טענה הקודמת.

I לא מתפרק, לכן לא ראשוני. לכן $I\neq P$.

איך נראים ב- $IP^{-1}P=\{a_1b_1c_1+\dots : a_i\in I,\ b_i\in P^{-1},\ c_i\in P\}$

מניחים $IP^{-1}=R$

$$RP \overset{IP^{-1}=R}{=} (IP^{-1})P = IP^{-1}P = I(P^{-1}P)=IR=I$$

$RP = P$

קיבלנו $P=I$ בסתירה.

לכן $IP^{-1} \subsetneq R$. לכן הוכחנו את הטענה.

אך $IP^{-1} \triangleleft R$ אידאל אמיתי, וגם $I \subsetneq IP^{-1}$

ומתקיים אז $I \subsetneq IP^{-1}$ בניגוד כמו בהוכחה

של הטענה הקודמת. אם $I = IP^{-1}$, יהי

$x \in P^{-1} \setminus R$, אז I הוא $R[x]$-מודול (נ״ס, נאמן...)

לפי המקסימליות של I,

IP^{-1} מפורק.

$$IP^{-1} = Q_1 Q_2 \cdots Q_r$$ מכפלה של ראשוניים

$$I = IR = IP^{-1}P = Q_1 Q_2 \cdots Q_r P$$

גם מפורק, בסתירה להנחה שיש

אידאלים שלא מפורקים.