הרצאה 14

תזכורת/הגדרה: יהי R תחום שלמות, $F = \mathrm{Frac}\, R$,

$R \subset F \subset S$ חוג. יהי $\alpha \in S$. אזי

$$I_\alpha = \{f \in F[x] : f(\alpha) = 0_S\}$$

אם $I_\alpha \neq \emptyset$, אזי $I_\alpha \triangleleft F[x]$. אך $F[x]$ תחום ראשי, לכן קיים פולינום מתוקן $f_\alpha \in F[x]$ כך ש- $I_\alpha = (f_\alpha)$.

f_α נקרא הפולינום המינימלי של α מעל F.

הוכחנו: אם R תפ"י, אזי $\alpha \in S$ שלם מעל $R \iff f_\alpha \in R[x]$.

<u>תרגיל/טענה</u> יהי $\mathbb{Z} \ni d \neq 0,1$, נניח d חפשי ריבועים ($p^2 \nmid d$ לכל ראשוני p). יהי

$$S = \mathbb{Q}(\sqrt{d}) = \{a + b\sqrt{d} : a, b \in \mathbb{Q}\} \subseteq \mathbb{C}$$

$S=\mathbb{Q}(\sqrt{d})$ הינו שדה. אכן: אם a,b לא שניהם 0,

$$\frac{1}{a+b\sqrt{d}}=\frac{a-b\sqrt{d}}{(a+b\sqrt{d})(a-b\sqrt{d})}=\frac{a}{a^2-b^2d}-\frac{b}{a^2-b^2d}\sqrt{d}\in S.$$

טענה יהי d כנ"ל. החוג

$$O_d=\{\alpha\in\mathbb{Q}(\sqrt{d}) : \alpha \text{ שלם מעל } \mathbb{Z}\}$$

הינו

$$\mathbb{Z}[\sqrt{d}]=\{a+b\sqrt{d} : a,b\in\mathbb{Z}\} \quad : d\equiv 2,3 \bmod 4$$

$$\mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right] \quad : d\equiv 1 \bmod 4.$$

הגדרה תחום שלמות R נקרא סגור integrally closed בשלמות אם לכל $\alpha\in \mathrm{Frac}\,R$,

α שלם מעל R $\iff$ $\alpha\in R$.

טענה כל תפ"י הינו סגור בשלמות.

הוכחה יהי $\frac{r}{s}\in \mathrm{Frac}\,R$, כאשר $r,s\in R$. נניח $\gcd(r,s)=1$.

$\Leftarrow$ אם $\alpha\in R$, אזי α שורש של $x-\alpha\in R[x]$, לכן שלם מעל R.

$\Leftarrow$) נניח $\frac{r}{s}$ שלם מעל R. זה אומר
שהוא שורש של פולינום מתוקן
$x^n + a_{n-1}x^{n-1} + \dots + a_1 x + a_0 \in R[x]$,
לפי משפט מלפני כמה שיעורים
$r \mid a_0$
$s \mid a_n = 1 \Rightarrow$ s הפיך $\Rightarrow \frac{r}{s} \in R$.

<u>מסקנה</u> $\mathbb{Z}$ סגור בשלמות.

<u>הוכחה של הגרעין</u> יהי $\alpha \in \mathbb{Q}(\sqrt{d})$. אם
$\alpha \in \mathbb{Q}$, אזי $\alpha \in \mathcal{O}_d \Leftrightarrow \alpha$ שלם מעל $\mathbb{Z} \Leftrightarrow \alpha \in \mathbb{Z}$.
אז יהי $\alpha \in \mathbb{Q}(\sqrt{d}) \setminus \mathbb{Q}$, כלומר $\alpha = a + b\sqrt{d}$,
$a, b \in \mathbb{Q}$, $b \neq 0$.

נחפש את הפולינום המינימלי של α, כלומר
יוצר מתוקן של $J_\alpha = \{f \in \mathbb{Q}[x] : f(\alpha) = 0\}$.

נשים לב כי

$$(x - (a + b\sqrt{d}))(x - (a - b\sqrt{d})) = x^2 - 2ax + (a^2 - b^2 d) \in \mathbb{Q}[x]$$

ברור כי α הינו שורש.

לכן $x^2 - 2ax + (a^2 - b^2 d) \in I_\alpha$.

זה פולינום מתוקן. אני טוען שזה הפולינום המינימלי. אם לא, אזי הוא מתחלק בפולינום המינימלי ואינו שווה לו ⇐ הפול' המינימלי ממעלה 1 ⇐ $\alpha \in \mathbb{Q}$, בסתירה.

לכן $f_\alpha = x^2 - 2ax + (a^2 - b^2 d)$

ולכן α שלם מעל $\mathbb{Z}$ ⟺ $f_\alpha \in \mathbb{Z}[x]$

⟺ $2a \in \mathbb{Z}$

$a^2 - b^2 d \in \mathbb{Z}$ (*)

כיוון ש-$2a \in \mathbb{Z}$, אזי $a = \frac{k}{2}$ כאשר $k \in \mathbb{Z}$.

~~אם k זוגי~~ אזי $a \in \mathbb{Z}$ ⇐ $a^2 - b^2 d \in \mathbb{Z}$

$\Updownarrow$

$b^2 d \in \mathbb{Z}$.

זה אומר כי $b \in \mathbb{Z}$ (אחרת במכנה של b^2 יהיו ריבועים, אך d חופשי מריבועים ולא יוכל לצמצם אותם).

במקרה הזה, $a, b \in \mathbb{Z}$ ⇐ $\alpha \in \mathbb{Z}[\sqrt{d}]$.

אם k אי-זוגי

$a=\frac{k}{2}$ ויהי $b=\frac{m}{n}$ שבר

מצומצם.

$$a^2-b^2d=\frac{k^2}{4}-\frac{m^2d}{n^2}=\frac{k^2n^2-4m^2d}{4n^2}\in\mathbb{Z}.$$

המונה חייב להתחלק ב-4. $\Leftarrow 4\mid k^2n^2 \Leftarrow$

$4\mid n^2 \Leftarrow n$ זוגי. אך $\frac{m}{n}$ מצומצם $\Leftarrow$

m אי-זוגי. אך $n^2\mid(k^2n^2-4m^2d) \Leftarrow$

$n^2\mid 4m^2d \Leftarrow n^2\mid 4d$ (כי m,n זרים). אבל,

d חופשי מריבועים $\Leftarrow n^2=4 \Leftarrow n=2$.

אז

$$\frac{k^2n^2-4m^2d}{4n^2}=\frac{4k^2-4m^2d}{16}\in\mathbb{Z}$$

$\Leftrightarrow 4\mid(k^2-m^2d)$. אך $k,m\equiv 1,3 \bmod 4 \Leftarrow$

$k^2,m^2\equiv 1 \bmod 4$.

לכן $1-d\equiv k^2-m^2d\equiv 0 \bmod 4 \Leftarrow d\equiv 1 \bmod 4$.

אם $d\equiv 1 \mod 4$, k,m אי-זוגיים.

$$\frac{k}{2}+\frac{m}{2}\sqrt{d} = m\left(\frac{1+\sqrt{d}}{2}\right) + \underbrace{\frac{\overset{\text{זוגי}}{k-m}}{2}}_{\in\mathbb{Z}} \in \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$$

נשאר לבדוק (רק) שכל איבר של

$\mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$ מקיים את התכונה (*) אם $d\equiv 1 \mod 4$.

<u>הערה</u> עכשיו אנחנו יודעים למצוא הרבה דוגמאות של תחומי שלמות שאינם גפ״י.

לדוגמא, $R=\mathbb{Z}[\sqrt{d}]$ כאשר $d\equiv 1 \mod 4$ חפשי מריבועים.

נשים לב כי

$$\operatorname{Frac} R = \mathbb{Q}(\sqrt{d})$$

$(m_i,n_i\in\mathbb{Z})$

אבל,

$$\frac{m_1}{n_1}+\frac{m_2}{n_2}\sqrt{d} = \frac{\overbrace{m_1n_2+m_2n_1\sqrt{d}}^{\in\mathbb{Z}[\sqrt{d}]}}{\underbrace{n_1n_2}_{\in\mathbb{Z}}}$$

לכן $\mathbb{Q}(\sqrt{d})\subseteq \operatorname{Frac} R$

אך $\operatorname{Frac} R$ הינו השדה הכי קטן שמכיל R,

לכן $\mathbb{Q}(\sqrt{d}) = \operatorname{Frac} R$.

אז $\frac{1+\sqrt{d}}{2} \in \operatorname{Frac} R$ שלם מעל $\mathbb{Z}$, קל ולומר
שלם מעל $\mathbb{Z}[\sqrt{d}]$. אבל $\frac{1+\sqrt{d}}{2} \notin \mathbb{Z}[\sqrt{d}]$.

לכן $\mathbb{Z}[\sqrt{d}]$ ($d \equiv 1 \mod 4$) לא סגור בשלמות
ולכן לא תפ"י.

<u>הערה</u> החוג $\mathbb{Z}[\sqrt{-5}] = \mathcal{O}_{-5}$ ידוע לנו
כמי שאינו תפ"י.

<u>תרגיל</u> $\mathbb{Z}[\sqrt{-5}]$ סגור בשלמות.

<u>הגדרה</u> תחום שלמות R נקרא תחום דדקינד (Dedekind) אם הוא מקיים
את התנאים הבאים.

א) R נתרי.

ב) R סגור בשלמות.

ג) כל אידיאל ראשוני לא-אפסי של R הינו מקסימלי. (הוכחנו שלכל תחום ראשי יש התכונה הזאת).

(מימד קרול של R הינו 1).

המטרה להוכיח שכל אידיאל לא אפסי של תחום דדקינד מתפרק באופן יחיד למכפלה של אידיאלים ראשוניים.

תרגיל כל החוגים $\mathcal{O}_d$ הם תחומי דדקינד?

טענה 1 יהי R תחום שלמות נתרי. יהי $0 \neq I \trianglelefteq R$. אזי יש אידיאלים ראשוניים לא אפסיים $P_1, P_2, \dots, P_r \trianglelefteq R$ (לא בהכרח שונים) כך ש- $P_1 P_2 \cdots P_r \subseteq I$.

תזכורת

$$P_1 P_2 = \{ a_1 b_1 + a_2 b_2 + \dots + a_n b_n : a_i \in P_1,\ b_i \in P_2 \} \trianglelefteq R.$$

R חילופי $\Leftarrow$ $P_1 P_2 \subseteq P_1 \cap P_2$.

הוכחה נניח בשלילה ש-

$\mathcal{F} = \{ I \trianglelefteq R :$ $I \neq (0)$ לא מכיל מכפלה של ראשוניים לא אפסיים $\} \neq \emptyset$

R נתרי, לכן קיים $I\in\mathcal{S}$ שהוא מקסימלי עבור התכונה הנ"ל. כלומר $J\supsetneq I\Rightarrow J\notin\mathcal{S}$.
(אחרת היינו מקבלים שרשרת עולה אינסופית של אידיאלים ב-$\mathcal{S}$, בסתירה לנתריות.)

ברור כי I לא ראשוני (אחרת $P_i \subseteq I$!)
זה אומר שקיימים $a,b\in R$
$a,b\notin I$ אך יהי $ab\in I$.

$J_1=I+Ra$
$J_2=I+Rb$
אלה אידיאלים של I (ולא בהכרח ראשוניים) שהם גדולים ממש מ-I. זה אומר בגלל המקסימליות של I כי

$$P_1P_2\cdots P_r\subseteq J_1$$
$$Q_1Q_2\cdots Q_s\subseteq J_2$$

זה אומר $P_1P_2\cdots P_rQ_1\cdots Q_s\subseteq J_1J_2=(I+Ra)(I+Rb)\subseteq I$
בסתירה להנחה כי $I\in\mathcal{S}$

<u>הגדרה</u> יהי R תחום שלמות. יהי $I\triangleleft R$ אידיאל. נגדיר

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

ברור כי $I^{-1}\supseteq R$.

טענה 2 יהי R תחום שלמות נתרי כך שכל אידאל ראשוני לא אפסי הינו מקסימלי. יהי $I \triangleleft R$ אידאל אזי $R \subsetneq I^{-1}$.

(דוגמא: $R=\mathbb{Z}$, $I=5\mathbb{Z}$, אזי $\frac{1}{5}\in I^{-1}$).

הוכחה אם $I=(0)$ זה ברור, כי $I^{-1}=\mathrm{Frac}\,R$.

אז נניח $I\neq(0)$, נבחר $0\neq y\in I$. לפי הטענה הקודמת,

$$\underbrace{P_1P_2\cdots P_r}_{\text{מכפלה של ראשוניים}} \subseteq yR \subseteq I$$

נבחר את המכפלה כך ש-r מינימלי.

האידאל I מוכל באידאל מקסימלי (ובפרט ראשוני) P.

$$P_1P_2\cdots P_r \subseteq yR \subseteq I \subseteq P.$$

אבל P ראשוני, לכן קיים $1\leq i\leq r$ כך ש- $P_i\subseteq P$. אבל לפי ההנחה, P_i מקסימלי $\Leftarrow$ $P_i=P$. בלי הגבלת הכלליות, $i=r$.

$$P_r = P \supseteq I$$

לפי המינימליות של r,

$$P_1P_2\cdots P_{r-1} \not\subseteq yR$$

נבחר $b\in P_1P_2\cdots P_{r-1}$ נגדיר $x=\frac{b}{y}\in \mathrm{Frac}\,R$

$b\notin yR$.

כיוון ש- $b\notin yR$, אזי $x\notin R$. אזי

נוכיח כי $x\in I^{-1}$. אזי,

$$\underset{\{ba : a\in I\}}{\underset{\parallel}{bI}} \subseteq P_1P_2\cdots P_{r-1}I \subseteq P_1P_2\cdots P_{r-1}P_r \subseteq yR$$

אזי, לכל $a\in I$,

$$ba\in bI\subseteq yR$$

לכן קיים $r\in R$ כך ש- $ba=yr$.

לכן $xa=\frac{ba}{y}=r\in R$

לכל $a\in I$.

לכן $x\in I^{-1}$, $x\notin R$.