

האגרה: יב ר תחום שלמות, $F = \text{Frac } R$, $R \subset F \subset S$ קוים. יב $\alpha \in S$. וז

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

אם $I_\alpha \neq \emptyset$ אז $I_\alpha \subset F[x]$ אבן תחום ראש, לכן קיים פולינום מתוקן

$$I_\alpha = (f_\alpha) \text{ כק } f_\alpha \in F[x]$$

f_α נקרא הפולינום המינימלי של α מעל F .

הוכחה: אם R תב"י, אזי $\alpha \in S$ שלם מעל $R \Leftrightarrow f_\alpha \in R[x]$

טענה:

יב $\alpha \in \mathbb{Z}, \alpha \neq 0$, נניח d חופסי מרביעית (גדלם של ראשוני p). יב

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

(עליו הוא שקב, אכן: אם a, b רציונליים, אז $a + b\sqrt{d}$ רציונלי).

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

האגרה: תחום שלמות R נקרא סגור (integrally closed) אם לכל $\alpha \in \text{Frac } R$,

$$\alpha \in R \Leftrightarrow \alpha \text{ שלם מעל } R$$

טענה:

כל תב"י הוא סגור בשלמות

הוכחה:

יב $\frac{r}{s} \in \text{Frac } R$, כאשר $r, s \in R$. נניח $\gcd(r, s) = 1$.

(\Rightarrow) אם $\alpha \in R$, אז α זרע של $x - \alpha \in R[x]$, לכן שלם מעל R .

(\Leftarrow) נניח $\frac{r}{s}$ שלם מעל R . לכן אומר שהוא זרע של פולינום מתוקן

$$x^n + a_{n-1}x^{n-1} + \dots + a_1x + a_0 \in R[x]$$

$$\frac{r}{s} \in R \Leftrightarrow s \mid a_n = 1, \text{ אז } \frac{r}{s} \in R$$

תוצאה:

\mathbb{Z} סגור בפעולות

טענה:

יהי d כ"ס. יהיו α שם מעגל \mathbb{Z} $O_d = \{\alpha \in \mathbb{Q}(\sqrt{d})\}$: הוא

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

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

הוכחה:

יהי $\alpha \in \mathbb{Q}(\sqrt{d})$. אם $\alpha \in \mathbb{Q}$, אזי $\alpha \in O_d \Leftrightarrow \alpha \in \mathbb{Z} \Leftrightarrow \alpha$ שם מעגל \mathbb{Z}

יהי $\alpha \in \mathbb{Q}(\sqrt{d}) \setminus \mathbb{Q}$, כלומר $\alpha = a+b\sqrt{d}$ יוצר מתוקן של $I_\alpha = \{f \in \mathbb{Q}[x] : f(\alpha) = 0\}$

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

כי α נכור כי α הוא שורש של הפולינום. לכן,

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

זכ פולינום מתוקן. נראה שזה הפולינום המינימלי.

אם לא, אזי הוא מתחלק בפולינום המינימלי ואינו שווה לו \Rightarrow הפולינום המינימלי

הוא מתחלק $1 \in \mathbb{Q}$ בסתירה

לכן

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

ולכן α שם מעגל $\mathbb{Z} \Leftrightarrow f_\alpha \in \mathbb{Z}[x] \Leftrightarrow 2a \in \mathbb{Z}, a^2 - b^2d \in \mathbb{Z}$ (*)

כיוון $e \in \mathbb{Z}, 2a \in \mathbb{Z}$, אז $a = \frac{k}{2}$ כאשר $k \in \mathbb{Z}$

אם k זוגי: $a \in \mathbb{Z} \Leftrightarrow a^2 - b^2d \in \mathbb{Z} \Leftrightarrow b^2d \in \mathbb{Z}$

זה אומר $e \in \mathbb{Z}$ (אחרת כתובה של b^2 יהיו ריבועים, אך d חופשי מריבועים ידועים \Rightarrow b^2d אינו ריבוע)

בחקרה הבה $\alpha \in \mathbb{Z}[\sqrt{d}] \Leftrightarrow \alpha \in O_d$

לס. k אי-זוגי: $a = \frac{k}{2}$. י. $b = \frac{m}{n}$ עקר מסוימים

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

המונח חייב לעתים קרובות להיות $4 \mid n^2 \Leftrightarrow 4 \mid k^2 n^2 \Leftrightarrow 4 \mid k^2$ כי n זוגי.

$$\Leftrightarrow n^2 \mid (k^2 n^2 - 4m^2 d) \text{ וכן } m \equiv 1 \pmod{4} \text{ זוגי. וכן}$$

$$\Leftrightarrow n^2 \mid 4m^2 d \Leftrightarrow n^2 \mid 4d \text{ (כי } n, m \text{ זרים). אבל } d \text{ חופשי מריבועים}$$

$$\Leftrightarrow n^2 = 4 \Leftrightarrow n = 2 \text{ זוגי.}$$

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

$$k^2, m^2 \equiv 1 \pmod{4} \Leftrightarrow k, m \equiv 1, 3 \pmod{4}$$

$$d \equiv 1 \pmod{4} \Leftrightarrow 1 - d = k^2 - m^2 d \equiv 0 \pmod{4}$$

$$\text{או } d \equiv 1 \pmod{4} \text{ זוגי. } k, m \text{ זוגיים. זוגי.}$$

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

נראה לעינינו שכל איבר $\mathbb{Z} \left[\frac{1 + \sqrt{d}}{2} \right]$ מקיים את (*). או $d \equiv 1 \pmod{4}$.

הערה: עכשיו אנחנו יודעים להצטוו בקרה קונטראול של תכונות שלמות אינן תפ"י.

למשל: $R = \mathbb{Z}[\sqrt{d}]$ כאשר $d \equiv 1 \pmod{4}$ חופשי מריבועים

$$(m_i, n_i \in \mathbb{Z}) \quad \frac{m_1}{n_1} + \frac{m_2}{n_2} \sqrt{d} = \frac{m_1 n_2 + m_2 n_1 \sqrt{d}}{n_1 n_2} \in \mathbb{Z}[\sqrt{d}] \text{ וכן } \text{Frac } R = \mathbb{Q}(\sqrt{d})$$

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

$$\text{אבל } \frac{1 + \sqrt{d}}{2} \in \text{Frac } R \text{ אם } d \equiv 1 \pmod{4}, \text{ קם וחוזר שם } \mathbb{Z}[\sqrt{d}]$$

$$\text{אבל } \frac{1 + \sqrt{d}}{2} \in \mathbb{Z}[\sqrt{d}] \text{ לכן } \mathbb{Z}[\sqrt{d}] \text{ (} d \equiv 1 \pmod{4} \text{) לא סגור בשלמות, ולכן}$$

ל. תפ"י

הערה: היות $\mathbb{Z}[\sqrt{5}] = \mathcal{O}_5$ ידוע לנו כמה איננו תפ"י.

תכונות:

$\mathbb{Z}[\sqrt{5}]$ סגור בשלמות

הגדרה: תחום שלמות R , נקרא תחום דדקינד (Dedekind) אם הוא מקיים את התנאים

הבאים:

(1) R נותרי

(2) R סימטרי בשלמות

(3) כל איגאל ראשוני Δ או אפסי של R הוא מקסימלי (בוכחנו שלכל תחום ראשי יש את התכונה הזאת) (מימד קרל של R הוא 1)

המטרה: להוכיח שכל איגאל Δ או אפסי של תחום דדקינד מתפרק באופן יחיד למכפלה של איגלים ראשוניים

תהליך:

כל החזים \mathfrak{p}_i הם תחומי דדקינד

טענה (בצד 1):

יהי R תחום שלמות נותרי. יהי $I \triangleleft R$ אפסי. אזי יש איגלים ראשוניים Δ או אפסיים

$$P_1 \cdot \dots \cdot P_r \subseteq I \quad (\Delta \text{ או אפסיים})$$

$$P_1 P_2 = \{ \sum a_i b_i \mid a_i \in P_1, b_i \in P_2 \} \triangleleft R \quad \text{תזכורת:}$$

$$P_1 P_2 \subseteq P_1 \cap P_2 \quad R \text{ חלופי} \Leftarrow$$

בוכחה:

נניח בשלילה $\emptyset \neq \{I \triangleleft R \mid I \text{ מכיל מכפלה של ראשוניים } \Delta \text{ או אפסיים}\} = S$.

R נותרי, לכן קיים $I \in S$ מקסימלי עבור התכונה הזאת. כלומר $I \not\subseteq J \Leftrightarrow J \in S$.

אחרת היינו מקבלים שרשרת עולה אינסופית של איגלים ב- S , בסתירה לנותריות.

ברור כי I Δ או ראשוני (אחרת $I \subseteq P, P \in S$). לכן אומר שקיימים $a, b \in R, a, b \notin I$

$$\text{אזי יהי } ab \in I$$

$$J_1 = I + Ra \quad J_2 = I + Rb \quad \text{אם איגלים של } I \text{ (לא בהכרח אמיתיים) שבהם } a, b \text{ נכללים}$$

אז $I \subseteq J_1, I \subseteq J_2$. לכן אומר בשלם המקסימליות של I כי: $P_1 \cdot \dots \cdot P_r \subseteq J_1, P_1 \cdot \dots \cdot P_r \subseteq J_2$

$$P_1 \cdot \dots \cdot P_r \subseteq J_1 J_2 = (I + Ra)(I + Rb) \subseteq I \quad \text{לכן,}$$

נסתירה להנחה e - ICS

כאנרכי: יהי R תחום שלמות, יהי $I \triangleleft R$ איגוד, נלקיח $I^{-1} = \{x \in \text{Frac} R : xI \subseteq R\}$
 ($\{xI = \sum a_i x_i : a_i \in I\}$) כבוד כי $R \subseteq I^{-1}$

טענה (צדק 2):

יהי R תחום שלמות נוקרי כך שכל איגוד כגושני לא זכאי הוא מקסימלי. יהי $I \triangleleft R$ איגוד.
 אזי $R \subseteq I^{-1}$.

(קולומה: $R = \mathbb{Z}, I = 5\mathbb{Z}$, אזי $I^{-1} = \mathbb{Z}$)

הוכחה:

אם $I = (0)$ - כבוד, כי $I^{-1} = \text{Frac} R$.

נניח $I \neq (0)$. נבחר $I \ni y \neq 0$. לפי הטענה הקודמת, $P_1 \dots P_r \subseteq yR$. נבחר את המכפלה
מכפלה של
 כגושניים

כך e-r מינימלי. האיגוד I מוכל באיגוד מקסימלי (ובפרט כגושני) P

$$P_1 \dots P_r \subseteq yR \subseteq I \subseteq P$$

אבל P כגושני, לכן קיים $r \geq 1$ כך e - $P_i \subseteq P$. אבל לפי ההנחה, P_i מקסימלי \Leftarrow

$\Leftarrow P_i = P$. בני הטבלת הכלליות, $r = 1$.

לפי המינימליות של r, $P_1 \dots P_{r-1} \not\subseteq yR$. נבחר $b \in P_1 \dots P_{r-1}$, $b \in yR$.

ונלקיח $x = \frac{b}{y} \in \text{Frac} R$. כיוון e $R \ni b$, אז $x \notin R$. נראה e - $x \in I^{-1}$.

$$\{ba : a \in I\} = bI \subseteq P_1 \dots P_{r-1} I \subseteq P_1 \dots P_{r-1} P_r \subseteq yR$$

\downarrow
 $I \subseteq P = P_r$

וזי, לכל $a \in I$, $ba \in bI \subseteq yR$. לכן קיים $r \in R$ כך e $ba = yr$. לכן $xa = \frac{ba}{y} = r \in R$.

לכל $a \in I$, לכן, $x \in I^{-1}$, $x \notin R$.