

קטגוריה:

נתון R -מוקדם נקרא נוצר סופית אם יש אוסף סופי של איברים $m_1, \dots, m_n \in M$

$$M = Rm_1 + Rm_2 + \dots + Rm_n$$

כלומר ניתן להביע כל $m \in M$ (ולו בהכרח באופן יחיד) בצורה

$$m = r_1 m_1 + \dots + r_n m_n$$

$$r_1, \dots, r_n \in R$$

(2) $R[S]$ חוגים, איבר $s \in S$ נקרא שלם מעל R אם הוא אינו אפס של פולינום

מתוקן מעל R , כלומר קיימים $1 \leq i \leq n$, $r_{i-1}, \dots, r_1 \in R$ כך ש

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

דוגמה:

$$s \in \mathbb{Z} \iff \exists \text{ מעל } \mathbb{Z} \text{ שלם } s \in \mathbb{Q} \quad s = \frac{a}{b}, R = \mathbb{Z}, S = \mathbb{Q}$$

$$ns - m = 0 \iff s = \frac{m}{n}$$

גאט: (מההכרזה הקודמת)

יהיו $R[S]$ חוגים חילופיים. יהי $s \in S$. האגרות הבאות שקולות:

(1) s שלם מעל R

(2) תת החוג $R[s] \subseteq R[S]$ הוא R -מוקדם נוצר סופית

(3) קיים תת חוג $R[s] \subseteq T \subseteq S$ כך ש T הוא R -מוקדם נוצר סופית

(4) קיים $R[s]$ -מוקדם נאמן M כך ש $e \cdot M$ נוצר סופית כמוקדם מעל R

הוכחה:

$$(2) \Rightarrow (3) \Rightarrow (4)$$

$$(2) \Rightarrow (1) \text{ (גם הוכחנו אבל נוכיח שוב)}$$

$$R[s] = \{r_0 + r_1 s + r_2 s^2 + \dots + r_n s^n \mid n \in \mathbb{N}, r_i \in R\}$$

$$R = R \cdot 1 + R \cdot s + R \cdot s^2 + R \cdot s^3 + \dots$$

לא ברור למה זה נוצר סופית. אבל, אם s שלם, אזי $s^n + a_{n-1}s^{n-1} + \dots + a_1 s + a_0 = 0$

צבור $R[s]$ אפשר לבטא כל חשקה של s כ"צירוף ליניארי של $1, s, \dots, s^{n-1}$

$$s^n = -a_0 \cdot 1 - a_1 s - \dots - a_{n-1} s^{n-1}$$

לכן $R[s] = R \cdot 1 + R \cdot s + \dots + R s^{n-1}$ נוצר סופית

(1) \Rightarrow (4) 'כי' M $R[s]$ -פוקוס נאמן שנוצר סופית כפוקוס של R . כל אומר יש

$$M = R m_1 + \dots + R m_n \quad \text{כך } m_1, \dots, m_n \in M$$

כוכים ליניאריים כי s שלם של R . כיוון M הוא $R[s]$ -פוקוס, $s m_i \in M$

$$s m_i = r_{i1} m_1 + r_{i2} m_2 + \dots + r_{in} m_n \quad \text{לכן קיימים } r_{ij} \in R \text{ כך } -$$

לכל $1 \leq i \leq n$. (הכרח יחידים)

אז:

$$\begin{pmatrix} s m_1 \\ \vdots \\ s m_n \end{pmatrix} = \begin{pmatrix} r_{11} & \dots & r_{1n} \\ \vdots & & \vdots \\ r_{n1} & \dots & r_{nn} \end{pmatrix} \begin{pmatrix} m_1 \\ \vdots \\ m_n \end{pmatrix}$$

נכיר שיתן למת $B = M^n = M \times \dots \times M$ של $M_n(R[s])$ -פוקוס

$$s I_n \begin{pmatrix} m_1 \\ \vdots \\ m_n \end{pmatrix} = \underbrace{\begin{pmatrix} r_{11} & \dots & r_{1n} \\ \vdots & & \vdots \\ r_{n1} & \dots & r_{nn} \end{pmatrix}}_B \begin{pmatrix} m_1 \\ \vdots \\ m_n \end{pmatrix} \Rightarrow \underbrace{(s I_n - B)}_{\in M_n(R[s])} \begin{pmatrix} m_1 \\ \vdots \\ m_n \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}$$

תהי $(adj B) \in M_n(R)$

$$(adj B)_{ij} = (-1)^{i+j} \det \begin{pmatrix} \text{החסר צורה} \\ \text{(n-1) x (n-1)} \\ \text{למחר מחקה} \\ \text{של שורה j} \\ \text{וזמורה i של B} \end{pmatrix}$$

$$B adj(B) = adj(B) B = (\det B) I_n$$

משפט ליניארי:

כל צורה עם עמודים

נפעל את $adj(s I_n - B)$ על $(s I_n - B)$ של האיברים

$$(adj(s I_n - B))(s I_n - B) \begin{pmatrix} m_1 \\ \vdots \\ m_n \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix} \Rightarrow \underbrace{(\det(s I_n - B) \cdot I_n)}_{\in M_n(R[s])} \begin{pmatrix} m_1 \\ \vdots \\ m_n \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix} \Rightarrow$$

$$\Rightarrow \begin{pmatrix} \det(sI_n - B) \cdot m_1 \\ \vdots \\ \det(sI_n - B) \cdot m_n \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}$$

$$\det(sI_n - B) \cdot m = 0_m = 0_{R[s]^m}, m \in M, \text{ לכל } m$$

$$\det(sI_n - B) = 0_{R[s]} = 0_s \quad \Leftarrow n \times n \quad M$$

$$\det \begin{pmatrix} s-r_{11} & -r_{12} & \dots & -r_{1n} \\ -r_{21} & s-r_{22} & \dots & -r_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ -r_{n1} & -r_{n2} & \dots & s-r_{nn} \end{pmatrix} = s^n + a_{n-1}s^{n-1} + \dots + a_1s + a_0 = 0$$

דבר $a_i \in R$ מקבילים לכל s של R .

תוצאה:

יב"ו $R[s]$ חזים חילופיים. יהי S של R של R .

אזי R' הוא תת חוג של S .

למשל: $R = \mathbb{Z}, S = \mathbb{C}$, $R' = \bar{\mathbb{Z}} = \{ \text{האלמנטים הבלתי-ברורים} \} = \{ s \in \mathbb{C} \mid s \text{ שווה } s \text{ פולינום } \}$ או $\{ \text{מתוקן או מקבילים } \mathbb{Z} \}$.

הוכחה:

יב"ו $s_1, s_2 \in R'$. זה אומר (לכל) ההוכחה של (1) \Rightarrow (2).

$$R[s_1] = R \cdot 1 + \dots + R s_1^{n_1-1}$$

$$R[s_2] = R \cdot 1 + \dots + R s_2^{n_2-1}$$

אזי:

$$\left(\begin{matrix} 0 \leq i \leq n_1-1 \\ 0 \leq j \leq n_2-1 \end{matrix} \right) s_1^i s_2^j \quad R[s_1, s_2] = \left\{ \sum_{i,j} r_{ij} s_1^i s_2^j \mid r_{ij} \in R \right\}$$

$M = R[s_1, s_2]$ הוא R - $R[s_1, s_2]$ חילופיים, R - $R[s_1, s_2]$ חילופיים, R חילופיים.

לפי תנאי 4: $s_1, s_2, s_1 + s_2$ של R חילופיים.

למשל:

יהי R חוג חילופי. אזי $A \in M_n(R)$ הפיכה $\Leftrightarrow \det A \in R$ הפיכה (באיבר של R).

(\Leftrightarrow) אם A הפיכה אזי קיים $B \in M_n(R)$ כך $AB = I_n$

$$(\det A)(\det B) = \det I_n = 1_R$$

לכן $\det A \in R$ הפיך

$$\frac{1}{\det A} (\underbrace{\text{adj}(A)}_{\in M_n(R)}) \cdot A = I_n$$

כי $\det A$ הפיך

(\Rightarrow) אם $\det A$ הפיך, אזי

התורה: יהי F שדה, S חוג, $F \subset S$. ימי $s \in S$ ייכר ולעברו שם F $(=)$ שם שם F .

יהי F שדה. אזי $I = \{f \in F[x] : f(s) = 0\} \neq (0)$ איננו אפס. $F[x]$ תחום

אינדיבידואלי וזכור תחום כואי. לכן קיים פולינום לא אפס $f_s \in F[x]$ כך $I = (f_s)$

f_s מוגדר ע"י כפי חברות, אך האופרים הפיכים של $F[x]$ הם F^* . לכן אם נקרו

בנוסף כי f_s מתוקן, אזי הוא מוגדר היטב. f_s נקרא הפולינום המניחה של s

יהי R תפ"י. יהי $F = \text{Frac } R$. יהי $R \subset F \subset S$. אזי שם שם R (\Leftrightarrow) $f_s \in R[x]$

(\Rightarrow) אם $f_s \in R[x]$, אזי f_s הוא פולינום מתוקן מעל R , s שורש שלו. לכן s שם שם R

(\Leftarrow) נניח s שם שם R . אז קיים $f \in R[x]$ מתוקן כך $f(s) = 0$. אך $f \in I$.

לכן $f(x) = f_s(x)h(x)$ כפולינומים ב- $F[x]$. לפי הדמיה של גאוס, קיימים $\tilde{f}, \tilde{h} \in R[x]$

כך $f(x) = \tilde{f}(x)\tilde{h}(x)$ ואם $\tilde{f} = \alpha \cdot f_s$ כאשר $\alpha \in F$. ואם f מתוקן, החקדים החובים

$$f_s(x) = \frac{1}{\alpha} f(x) \in R[x] \quad \text{לכן } \alpha \in R \text{ הפיך ב-} R.$$

מטרה: לקחת שדה F ולבטור בתוכו "חוג שם שם" O_F כך $F = \text{Frac } O_F$

ואם שדה (F, O_F) "יתנה כח" (\mathbb{Q}, \mathbb{Z})

הגדרה: שדה ריבועי הוא שדה F כזה ש $\mathbb{Q} \subset F$ וכך $\dim_{\mathbb{Q}} F = 2$

תכונה: קיים $\alpha \in \mathbb{Z}$, $\alpha \neq 1, 0$ חופשי מריבועים (כלומר α לא מתחלק בשום ריבוע שלם

$$F = \mathbb{Q}(\sqrt{\alpha}) = \{a + b\sqrt{\alpha} \mid a, b \in \mathbb{Q}\} \subset \mathbb{C} \quad (\alpha = 4, 9, 16, \dots)$$

בתווך:

יהי F שדה ריבועי. יהי $\{1, \alpha\}$ בסיס מסדר \mathbb{Q} . וני $\alpha^2 \in F \Leftrightarrow \alpha^2 = c_1 \cdot 1 + c_2 \cdot \alpha$

$$\Leftrightarrow c_1, c_2 \in \mathbb{Q}$$

$$\alpha^2 - c_2 \alpha - c_1 = 0 \Rightarrow \left(\alpha - \frac{c_2}{2}\right)^2 = \alpha^2 - c_2 \alpha + \frac{c_2^2}{4} = c_1 + \frac{c_2^2}{4}$$

ואם $\left\{1, \alpha - \frac{c_2}{2}\right\}$ גם בסיס של F . אז $\beta^2 = c_1 + \frac{c_2^2}{4} \in \mathbb{Q}$. אם נכפול

אם $\beta \in \mathbb{Q}$ שמתחבר חכם, נקבל $(r\beta)^2 = r^2 \beta^2 \in \mathbb{Z}$ חופשי מריבועים.

ואם $\left\{1, r\beta\right\}$ גם בסיס של F .

תכונה: יהי $F = \mathbb{Q}(\sqrt{\alpha})$, יהי α שלם מסדר \mathbb{Z} . $\mathcal{O}_F = \{\alpha \in F : \mathbb{Z} \text{ מסדר } \alpha\}$, וני,

$$\mathcal{O}_F = \left\{ \begin{array}{l} \mathbb{Z}[\sqrt{\alpha}] = \{a + b\sqrt{\alpha} : a, b \in \mathbb{Z}\}, \quad d = 2, 3 \pmod{4} \\ \mathbb{Z}\left[\frac{1+\sqrt{\alpha}}{2}\right] = \left\{a + \frac{b(1+\sqrt{\alpha})}{2} : a, b \in \mathbb{Z}\right\}, \quad d = 1 \pmod{4} \end{array} \right\}$$