הרצאה 20

<u>הגדרה</u> יהי $R\subseteq S$ הרחבה של חוגים חילופיים.
איבר $s\in S$ נקרא אלגברי אם הוא שורש של
פולינום מעל R. כלומר קיים $f(x)\in R[x]$

$$f(x)=a_nx^n+a_{n-1}x^{n-1}+\dots+a_1x+a_0 \qquad a_i\in R$$

כך ש:

$$a_ns^n+a_{n-1}s^{n-1}+\dots+a_1s+a_0=0_s.$$

<u>הגדרה</u> $R\subseteq S$ כנ"ל. איבר $s\in S$ נקרא שלם מעל R
אם הוא שורש של פולינום מתוקן מעל R:

$$f(x)=x^n+a_{n-1}x^{n-1}+\dots+a_0.$$

<u>הערה</u> 1) s שלם מעל R ⇐ s אלגברי מעל R.

2) אם $R=F$ שדה, $F\subseteq S$, אזי
$s\in S$ שלם מעל F ⟺ s אלגברי מעל F.

אכן s אלגברי ⇐

$$a_ns^n+\dots+a_1s+a_0=0_s \qquad a_i\in F,\ a_n\neq 0$$

נחלק בי a_n ($F\ni a_n$ הפיך, אז מוגדר)

$$\Leftarrow\ s^n+\frac{a_{n-1}}{a_n}s^{n-1}+\dots+\frac{a_0}{a_n}=0_s \qquad \frac{a_i}{a_n}\in F$$

s שלם מעל F.

דוגמאות: $\sqrt[5]{2}$, $\sqrt{17}$ שלמים מעל $\mathbb{Z}$.

שורשים של x^5-2, x^2-17 בהתאמה

תרגיל: הוכיחו $\sqrt[5]{2}+\sqrt{17}$ גם שלם מעל $\mathbb{Z}$.

הגדרה: יהיו $R\subseteq S$ חוגים חילופיים. יהי $s\in S$.

$$R[s]=\{a_ns^n+\dots+a_1s+a_0 : \begin{array}{c} n\ge 0 \\ a_i\in R\end{array}\}\subseteq S$$

תת-חוג הכי קטן של S שמכיל $R\cup\{s\}$.

טענה: יהיו $R\subseteq S$ חוגים חילופיים. יהי $s\in S$.
התנאים הבאים שקולים.

1) s שלם מעל R.

2) החוג $R[s]\subseteq S$ נוצר סופית כ-R-מודול.

3) קיים תת-חוג $R[s]\subseteq T\subseteq S$ כך ש-T נוצר סופית כ-R-מודול.

4) קיים $R[s]$-מודול נאמן M ($\mathrm{Ann}_{R[s]}M=(0)$) כך ש-M נוצר סופית כמודול מעל R.

הוכחה: $2)\Rightarrow 3)$ ניקח $T=R[s]$.

$3)\Rightarrow 4)$ ניקח $M=T$. הוא נאמן

כ-$R[s]$-מודול כי $r\in\mathrm{Ann}_{R[s]}(T)\Rightarrow r\cdot 1_T=0 \Rightarrow r=0$

לכן $\mathrm{Ann}=(0)$.

$1) \Leftarrow 2)$ נניח $s \in S$ שלם מעל R.

אז $s^n + a_{n-1}s^{n-1} + \dots + a_1 s + a_0 = 0$

עבור $a_i \in R$. אני טוען כי

$R[s] = R \cdot 1 + R \cdot s + Rs^2 + \dots + Rs^{n-1} = X$.

ברור שהמכלל הימני נוצר סופית מעל R.

צריך להוכיח כי $s^m \in X$

לכל $m \geq 0$. אם $m \leq n-1$ $(1, s, \dots, s^{n-1})$

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

באינדוקציה נניח כי $s^{m-1} \in X$, כלומר

$$s^{m-1} = c_0 \cdot 1 + c_1 s + \dots + c_{n-1}s^{n-1} \quad c_i \in R$$

$$s^m = s \cdot s^{m-1} = c_0 s + c_1 s^2 + \dots + c_{n-2}s^{n-1} + c_{n-1}s^n =$$

$$c_0 s + \dots + c_{n-2}s^{n-1} + c_{n-1}(-a_0 \cdot 1 - \dots - a_{n-1}s^{n-1}) =$$

$$-a_0 c_{n-1} \cdot 1 + (c_0 - a_1 c_{n-1})s + \dots + (c_{n-2} - a_{n-1}c_{n-1})s^{n-1}$$

$\in X$.

לכן $R[s] = X$ נוצר סופית כ-R-מודול.

$4) \Leftarrow 1)$ יהי M $R[s]$-מודול נאמן שהוא נוצר

סופית מעל R. יהיו $m_1, \dots, m_n \in M$

איברים שיוצרים את M מעל R:

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

אבל M הינו $R[s]$-מודול, לכן יש לנו גם כפל סקלרי ב-s. לכן, לכל $1 \le j \le n$,

$$M \ni sm_j = a_{1j}m_1 + a_{2j}m_2 + \dots + a_{nj}m_n,$$

$a_{ij} \in R$.

יהי A המטריצה (a_{ij}).

$$A\begin{pmatrix} m_1 \\ m_2 \\ \vdots \\ m_n \end{pmatrix} = s\begin{pmatrix} m_1 \\ \vdots \\ m_n \end{pmatrix}$$

$$\underbrace{(A - sI_n)}_{\in M_n(R[s])}\begin{pmatrix} m_1 \\ \vdots \\ m_n \end{pmatrix} = \begin{pmatrix} 0_M \\ \vdots \\ 0_M \end{pmatrix}$$

נכפיל את שני האגפים משמאל ב-$\operatorname{adj}(A - sI_n)$.

$$\underbrace{\det(A - sI_n)}_{\in R[s]}\begin{pmatrix} m_1 \\ \vdots \\ m_n \end{pmatrix} = \begin{pmatrix} 0_M \\ \vdots \\ 0_M \end{pmatrix}$$

לכן

$$\det(A - sI_n) \in \operatorname{Ann}_{R[s]}(M) \underset{M \text{ נאמן}}{=} (0)$$

קיבלנו $\det(A - sI_n) = 0$

$$\det\begin{pmatrix} a_{11}-s & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22}-s & \cdots & a_{2n} \\ \vdots & & & \vdots \\ a_{n1} & \cdots & & a_{nn}-s \end{pmatrix} = (-1)^n s^n + b_{n-1}s^{n-1} + \cdots + b_1 s + b_0 = 0$$

$b_i \in R$

נכפיל את שני האגפים ב-(-1) אם צריך ונקבל
כי s שלם מעל R.

<u>אבחנה</u> יהיו $R \subseteq S$ חוגים חילופיים. אזי

$\{s \in S : s$ שלם מעל $R\}$

הינו תת-חוג של S. הוא נקרא הסגור השלם
של R ב-S.

<u>הוכחה</u> יהי $Y = \{s \in S : S$ שלם מעל $R\}$

<u>תרגיל</u> מצאו $m,n > 1$ כך ש-
$3^m - 2^n = \pm 1$ (רלב״ג הוכיח במאה ה-14)

הפתרון היחיד הינו $3^2 - 2^3 = 1$

משפט (השערה של Catalan, 1850, הוכחה Mihalescu, 2002) הפתרון היחידי של $a^m - b^n = 1$ $a,b \in \mathbb{Z}$ $m,n>1$ הינו $3^2 - 2^3 = 1$.

חוזרים להוכחה של הטענה

<u>טענה</u>

$\mathcal{O} = \{s\in S:$ s שלם מעל R $\} \subseteq S$ תת-חוג

<u>הוכחה</u> ברור כי $R \subseteq \mathcal{O}$ כי כל $a\in R$

הינו שורש של $x-a \in R[x]$. בפרט $1\in \mathcal{O}$.

נשאר להוכיח כי $\mathcal{O}$ סגור לחיבור ולכפל.

יהיו $s_1, s_2 \in \mathcal{O}$. אזי, לפי תנאי 2) של

הטענה, $R[s_1], R[s_2]$ נוצרים סופית כ-R-מודולים.

נגדיר

$$T = R[s_1,s_2] = \{\sum a_{ij} s_1^i s_2^j,\ a_{ij}\in R\}$$

התת-חוג הכי קטן של S שמכיל $R\cup\{s_1,s_2\}$

אם נוכיח כי T נוצר סופית כ-R-מודול,

נקבל $\begin{matrix} R[s_1+s_2] \\ R[s_1s_2] \end{matrix} \subseteq T \subseteq S$,

ולפי תנאי 3) של הטענה, נקבל כי

s_1+s_2 וגם s_1s_2 שלמים מעל R.

אני טוען כי T נוצר על ידי הקבוצה

$$\left\{ s_1^i s_2^j \;:\; \begin{matrix} 0\le i\le n_1-1 \\ 0\le j\le n_2-1 \end{matrix} \right\}$$

כאשר n_1,n_2 הן המעלות של הפולינומים המינימליים של s_1,s_2.

אכן, נותר להוכיח

$$R[s_1,s_2] = Y = R\cdot 1 + R\cdot s_1 + \dots + R s_1^{n_1-1} s_2^{n_2-1}$$

מספיק להוכיח $s_1^{\alpha} s_2^{\beta} \in Y$ לכל m,n.

אנחנו כבר יודעים, מן ההוכחה של $(1)\Rightarrow(2)$ למעלה, כי

$$s_1^{\alpha} = b_0\cdot 1 + b_1\cdot s_1 + \dots + b_{n_1-1} s^{n_1-1}$$
$$s_2^{\beta} = c_0\cdot 1 + \dots + c_{n_2-1} s^{n_2-1}$$

נכפיל את שני המשוואות

$$s_1^{\alpha} s_2^{\beta} = \sum_{i=0}^{n_1-1}\sum_{j=0}^{n_2-1} b_i c_j s_1^i s_2^j \in Y.$$

<u>שאלה</u> מה הקשר בין השלמות הנ"ל לשלמות של המספרים השלמים בגוף הרציונליים?

<u>הגדרה</u> יהי R תחום שלמות. יהי $F=\mathrm{Frac}\,R$ שדה השברים. R נקרא סגור בשלמות אם R הינו הסגור השלם של עצמו ב-F.

(כלומר, אם $\alpha\in F$ שלם מעל R, אזי $\alpha\in R$).

<u>טענה</u> כל תפ"י סגור בשלמות (בפרט, $\mathbb{Z}$ סגור בשלמות).

<u>הוכחה</u> יהי $\alpha=\frac{r}{s}\in F$ שלם מעל R. כיוון ש-R תפ"י, נוכל להניח כי α כשבר מצומצם. כלומר $\gcd(r,s)=1$ אזי α הינו שורש של פולינום מתוקן:

$$\alpha^n+b_{n-1}\alpha^{n-1}+\dots+b_1\alpha+b_0=0,\quad b_i\in R$$

לכן, לפי טענה מלפני כמה שבועות, $s|1$ (מקדם המוביל), לכן s הפיך, לכן $\frac{r}{s}\in R$

$$\frac{r^n}{s^n}+b_{n-1}\cdot\frac{r^{n-1}}{s^{n-1}}+\dots+b_1\cdot\frac{r}{s}+b_0=0$$

נכפיל ב-s^n:

$$r^n+b_{n-1}r^{n-1}s+\dots+b_0s^n=0$$

$$r^n=-s\left(b_{n-1}r^{n-1}+\dots+b_1rs^{n-2}+b_0s^{n-1}\right)$$

אם s לא הפיך, אזי יש לו גורם אי-פריק p.
אזי $p|r^n \Leftarrow p|r$, סתירה לזרות של r,s.
לכן s הפיך, לכן $\alpha=\frac{r}{s}\in R$.

הגדרה שדה מספרים הינו שדה שמכיל את $\mathbb{Q}$ ושהוא סוף-מימדי כמרחב וקטורי מעל $\mathbb{Q}$.

דוגמאות $\mathbb{Q}(i) = \mathbb{Q}(\sqrt{-1}) = \{a+bi : a,b\in\mathbb{Q}\}$

דו-מימדי מעל $\mathbb{Q}$

$\mathbb{Q}(\sqrt{-5}) = \{a+b\sqrt{-5} : a,b\in\mathbb{Q}\}$

לכל $d\neq 0$ שלם $\mathbb{Q}(\sqrt{d}) = \{a+b\sqrt{d} : a,b\in\mathbb{Q}\}$.

$\mathbb{Q}(\sqrt[3]{2}) = \{a+b\sqrt[3]{2}+c\sqrt[3]{4} : a,b,c\in\mathbb{Q}\}$

זה שדה, תלת-מימדי מעל $\mathbb{Q}$.

אנטי-דוגמאות $\mathbb{R}$ לא שדה מספרים.

הוכחה העוצמה של מרחב וקטורי n-מימדי מעל $\mathbb{Q}$ (n טבעי) הינו $\aleph_0^n = \aleph_0$.

אבל $\mathbb{R}$ לא בן מניה.

תרגיל יהי $F=\mathbb{Q}(\sqrt{d})$, כאשר $d\in\mathbb{Z}$, $d\neq 0,1$,

d חפשי מריבועים (d לא מתחלק באף ריבוע $(4,9,16,25,\ldots)$. יהי O_F

הסגור השלם של $\mathbb{Z}$ ב-F. אזי

$$\mathcal{O}_F = \begin{cases} \mathbb{Z}[\sqrt{d}] = \{a+b\sqrt{d} : a,b \in \mathbb{Z}\}, \\ \qquad\qquad d \equiv 2,3 \mod 4 \\ \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right], \quad d \equiv 1 \mod 4 \end{cases}$$

<u>הערה</u> אם $F=\mathbb{Q}(\sqrt{-5})$, אזי $\mathcal{O}_F = \mathbb{Z}[\sqrt{-5}]$.

החוג הזה לא גפ״י.