הרצאה 1

8.3.2021

<u>דוגמאות</u>

1) פרמה, 1640: $p>2$ ראשוני

$$p \equiv 1 \bmod 4 \iff p = a^2+b^2.$$

2) גאוס, 1801: שלמים של גאוס

$$\mathbb{Z}[i] = \{a+bi : a,b \in \mathbb{Z}\}$$

3) משוואת פל Pell: למצוא $x,y \in \mathbb{Z}$

$$x^2 - 13y^2 = 1$$

4) להוכיח שאין פתרונות שלמים

$$x^2 + 5 = y^3.$$

5) משפט האחרון של פרמה: לכל $n>2$

אין $0 \neq x,y,z \in \mathbb{Z}$ כך ש- $x^n + y^n = z^n$.

1994

6) השערה של Catalan 1850

יהיו $a,b>1$, $x,y>1$. $x^a - y^b = 1$.

$$\boxed{3^2 - 2^3 = 1}$$

הפתרון היחיד?

המקרה $x^2 - y^3 = \pm 1$ הוכח על ידי

הרלב"ג, מאה 14.

המקרה הכללי: Mihalescu, 2002.

7)

$$e^{\pi\sqrt{163}} = 640320^2 + 743.99999999999925007\ldots$$

הגדרה שדה מספרים הינו הרחבה סופית

$K/\mathbb{Q}$: $\dim_{\mathbb{Q}} K < \infty$.

דוגמא $K=\mathbb{Q}(\sqrt{-1})$

$\{a+b\sqrt{-1} : a,b\in\mathbb{Q}\}$.

הגדרה יהיו $A\subset B$ חוגים

(בקורס הזה, כל חוג קומוטטיבי ועם 1

אלא אם כן נאמר אחרת בפירוש).

איבר $b\in B$ נקרא אלגברי מעל A

אם קיימים $a_i\in A$ כך ש-

$$a_nb^n+a_{n-1}b^{n-1}+\dots+a_1b+a_0=0$$

$b\in B$ נקרא שלם מעל A אם הוא שורש

של פולינום מתוקן

$$b^n+a_{n-1}b^{n-1}+\dots+a_1b+a_0.$$

דוגמא $A=\mathbb{Z}$, $B=\mathbb{Q}$

כל $n\in\mathbb{Z}$ הינו שורש של $x-n$.

דוגמא $A=\mathbb{Z}$, $B=\mathbb{C}$

$\sqrt[3]{2}$ שלם מעל $\mathbb{Z}$

x^3-2.

אבל $\frac{\sqrt{2}}{2}$ לא שלם מעל $\mathbb{Z}$.

אבחנה אם A שלם, אזי אלגברי מעל A

$\Uparrow$

שלם מעל A.

משפט יהיו $A\subset B$ חוגים. יהי $b\in B$.

התנאים הבאים שקולים:

1) b שלם מעל A.

2) התת-חוג $A[b] \subseteq B$ (שיש לו מבנה טבעי של A-מודול)

$= \left\{\sum_{i=0}^{N} a_i b^i\right\}$

הינו A-מודול נוצר סופית.

3) קיים חוג $A[b] \subseteq C \subseteq B$ כך ש-C הינו A-מודול נוצר סופית.

4) קיים A[b]-מודול נאמן M ($Ann_{A[b]}(M) = 0$) שהוא נוצר סופית כמודול מעל A.

<u>הוכחה.</u> $2) \overset{C=A[b]}{\Leftarrow} 3) \overset{M=C}{\Leftarrow} 4)$ ברור.

$1) \Leftarrow 2)$ להגדרה.

$$A[b] = A \cdot 1 + A \cdot b + A \cdot b^2 + \cdots$$

b שלם, לכן $b^n + a_{n-1}b^{n-1} + \dots + a_0 = 0$

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

$$b^{n+1} = -a_0 b - \dots - a_{n-2}b^{n-1} - a_{n-1}b^n$$

באינדוקציה $A[b] = A\cdot 1 + A\cdot b + \dots + A\cdot b^{n-1}$

לכן $A[b]$ נוצר סופית כ-A-מודול.

(4) ⇐ (1) יהי

$$M = Am_1 + \dots + Am_n$$

$$bm_i \in M \Rightarrow bm_i = \sum_{j=1}^{m} a_{ij} m_j, \quad a_{ij} \in A$$

$$\begin{pmatrix} bm_1 \\ \vdots \\ bm_n \end{pmatrix} = \underbrace{\begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & & \\ a_{n1} & \cdots & a_{nn} \end{pmatrix}}_{D} \begin{pmatrix} m_1 \\ \vdots \\ m_n \end{pmatrix}$$

נפעיל את שני האגפים משמאל עם $\operatorname{adj}(bI_n - D)$.

$$(bI_n - D)\begin{pmatrix} m_1 \\ \vdots \\ m_n \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}$$

$$\underbrace{\det(bI_n - D)}_{\in A[b]}\begin{pmatrix} m_1 \\ \vdots \\ m_n \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}$$

$\det(bI_n - D) = 0 \Longleftarrow$ $A[b]$ מעל נאמן M

$$\| $$

$$\det\begin{pmatrix} b-a_{11} & -a_{12} & \cdots & -a_{1n} \\ \vdots & \ddots & & \vdots \\ -a_{1n} & & \cdots & b-a_{nn} \end{pmatrix} =$$

$b^n + \cdots = 0 \leftarrow$ פולינום מתוקן עם מקדמים ב-A.

__תוצאה__ יהיו $A\subseteq B$ חוגים. אז

$$\{b\in B:\ b \text{ שלם מעל } A\}$$

הינו תת-חוג של B (נקרא הסגור השלם של A ב-B).

__הוכחה__ יהיו $b_1,b_2\in B$ שלמים מעל A.

$$A[b_1]=A\cdot 1+A\cdot b_1+\cdots+A\cdot b_1^n$$
$$A[b_2]=A\cdot 1+A\cdot b_2+\cdots+A\cdot b_2^m$$

$$M\equiv A[b_1,b_2]=\left\{\sum a_{ij}b_1^i b_2^j \;\middle|\; \begin{array}{l} a_{ij}\in A\\ 0\le i\le b_1^n\\ 0\le j\le b_2^m\end{array}\right\}$$

נוצר סופית כ-A-מודול.

$\left\{\begin{array}{l} b_1+b_2\in M\\ b_1b_2\in M\end{array}\right.$ $\Leftarrow$ M הינו $A[b_1+b_2]$-מודול נאמן $\Leftarrow$ b_1+b_2 שלם מעל A (לפי 3).

<u>הגדרה</u> A תחום שלמות. נקרא ~~A~~ A סגור בשלמות אם A הינו הסגור השלם של עצמו ב- Frac A.

שדה השברים.

<u>טענה</u> יהי A תחום פריקות יחידה. אזי A סגור בשלמות (בפרט, $\mathbb{Z}$ סגור בשלמות).

<u>הוכחה</u> יהי $\frac{a}{b}\in \mathrm{Frac}A$ ($a,b\in A$) שבר מצומצם,

נניח שהוא שלם מעל A. ז״א

$$\left(\frac{a}{b}\right)^n + a_{n-1}\left(\frac{a}{b}\right)^{n-1} + \cdots + a_0 = 0$$

נכפיל ב- b^n

$$a^n + a_{n-1}a^{n-1}b + \cdots + a_0 b = 0$$

$$a^n = \underbrace{-b(a_{n-1}a^{n-1}+\dots+a_0 b^{n-1})}_{\text{מתחלק ב-}b}$$

לכן $b \mid a^n$, אך הנחנו כי a,b זרים.
לכן b הפיך, לכן $\frac{a}{b}\in A$.

<u>תרגילים</u> 1) סגור שלם הינו סגור בשלמות.
2) $A\subseteq B$, B נקרא שלם מעל A
אם כל $b\in B$ שלם מעל A.

אם $A\subseteq B$ שלם, $B\subseteq C$ שלם,
אזי C שלם מעל A.

<u>הגדרה</u> K שדה מספרים. חוג השלמים של K, מסומן O_K, הינו הסגור השלם של $\mathbb{Z}$ ב-K.

הגדרות A תחום שלמות סגור בשלמות.

$K = \mathrm{Frac}\,A$ שדה השברים.

L/K הרחבה סופית

B הסגור השלם של A ב-L.

טענה יהי $x \in L$, אזי קיימים $b \in B$, $a \in A$ כך ש- $x = \frac{b}{a}$.

הוכחה $x \in L$ אלגברי מעל K, כי L/K סופית. לכן

$$k_n x^n + \dots + k_0 = 0, \quad k_i \in K$$

ניפטר מן המכנים

$$a_n x^n + \dots + a_1 x + a_0 = 0, \quad a_i \in A$$

נכפיל את שני האגפים ב- a_n^{n-1}.

$$a_n^n x^n + a_{n-1} a_n^{n-1} x^{n-1} + \dots + a_0 a_n^{n-1} = 0$$

$$(a_n x)^n + a_{n-1}(a_n x)^{n-1} + \dots + a_0 a_n^{n-1} = 0$$

לכן $a_n x$ הינו שורש של פולינום

מתוקן ⇐ $a_n x$ שלם מעל A ⇐

$a_n x \in B$ ⇐ $x = \dfrac{a_n x^{\in B}}{a_{n\,\in A}}$.

יהי $x \in L$, הנורמה והעקבה של x

סימון: $N_{L/K}(x)$, $Tr_{L/K}(x)$) הם

הנורמה (הדטרמיננטה) והעקבה של העתקה (ה-K-לינארית

$$\mu_x : L \longrightarrow L$$
$$y \longmapsto xy$$

לכן $N_{L/K}(x), Tr_{L/K}(x) \in K$.

תכונות בסיסיות

$$N_{L/K}(xy) = N_{L/K}(x)\cdot N_{L/K}(y)$$

$$Tr_{L/K}(x+y) = Tr_{L/K}(x) + Tr_{L/K}(y)$$

נניח כי L/K ספרבילית.

נקבע סגור אלגברי $\bar{K}/K$.

$$\Sigma = \{ \sigma : L \hookrightarrow \bar{K} \text{ שיכונים כך ש- } \sigma(x)=x \text{ לכל } x\in K \}$$

תרגיל הפולי' המינימלי של μ_x הינו $\prod_{\sigma\in\Sigma}(X-\sigma(x))$

$$N_{L/K}(x) = \prod_{\sigma\in\Sigma}\sigma(x)$$

$$Tr_{L/K}(x) = \sum_{\sigma\in\Sigma}\sigma(x)$$

מסקנה L/K ספרבילית. אם $x\in B$,

אזי $N_{L/K}(x),\ Tr_{L/K}(x)\in A$.

הוכחה תרגיל: $y\in L$ אינט׳ $y\in B$ אם ורק אם

הפולינום המינימלי $f_y\in K[x]$ מקיים $f_y\in A[x]$

(f_y)

$\{f\in K[x] : f(y)=0\}\triangleleft K[x]$.

תרגיל בלינארית: הפולינום האופייני

של u הינו חזקה של f_y.

$\sigma(x)$ עדיין שורש של $f_y\in A[x]$. לכן

$\sigma(x)$ שלם מעל A כאיבר של $\bar{K}$. לכן

$N_{L/K}(x), Tr_{L/K}(x)\in K$, שלמים מעל A, לכן שייכים

ל-A כי A סגור בשלמות.

הגדרה יהי $\alpha_1,\dots,\alpha_n\in L$ בסיס

של L מעל K. הדיסקרימיננטה

של הבסיס הזה הינה

$$d(\alpha_1,\dots,\alpha_n) = \det\left(Tr_{L/K}(\alpha_i\alpha_j)\right)\in K.$$

טענה $d(\alpha_1,\dots,\alpha_n)\neq 0$

הוכחה $\Sigma=\{\sigma_1,\dots,\sigma_n\}$

נשים לב כי

$$Tr_{L/K}(\alpha_i\alpha_j)=\sum_{\sigma}\sigma(\alpha_i)\sigma(\alpha_j)$$

$$\left(Tr_{L/K}(\alpha_i\alpha_j)\right)=C\cdot C^T$$

$$C_{ij}=\sigma_i(\alpha_j)$$

לכן, $d(\alpha_1,\dots,\alpha_n)=(\det C)^2$

אבל L/K סופית ספרבילית, לכן

פרימיטיבית $\Rightarrow L=K(\theta)$

לכן $\{1,\theta,\theta^2,\dots,\theta^{n-1}\}$ הינה K-בסיס

של L. לכן

$$d(1,\theta,\dots,\theta^{n-1}) = \left(\det\begin{pmatrix} \sigma_1(1) & \sigma_1(\theta) & \dots & \sigma_1(\theta)^{n-1} \\ \vdots & \vdots & & \vdots \\ \sigma_n(1) & \sigma_n(\theta) & \dots & \sigma_n(\theta)^{n-1} \end{pmatrix}\right)^2$$

$$d(1,\theta,\dots,\theta^{n-1}) = \left(\prod_{i<j}\left(\sigma_i(\theta)-\sigma_j(\theta)\right)\right)^2 \neq 0.$$ וכמו כן:

$$\begin{pmatrix}\alpha_1\\ \vdots \\ \alpha_n\end{pmatrix} = D\begin{pmatrix}1\\ \theta \\ \vdots \\ \theta^{n-1}\end{pmatrix} \qquad D\in M_n(K)$$

$$\det D \neq 0$$

$$\det(\sigma_i(\alpha_j)) = (\det D)\cdot\det(\sigma_i(\theta^j))$$

לכן, $d(\alpha_1,\dots,\alpha_n) = (\det D)^2 \, d(1,\dots,\theta^{n-1}) \neq 0.$

לפי טענה מקודם, ניתן לבחור

בסיס $\alpha_1,\dots,\alpha_n$ של L מעל K כך

ש- $\alpha_1,\dots,\alpha_n \in B$. נניח שאנחנו

במצב הזה.

טענה: יהי $\alpha_1,\dots,\alpha_n \in B$ בסיס של L/K.

$$d = d(\alpha_1,\dots,\alpha_n) \in A$$

אזי:

$$\{db : b\in B\} = dB \subseteq A\alpha_1 + \dots + A\alpha_n \subseteq B$$

<u>הוכחה</u> יהי $b\in B$, אזי

$$b=c_1\alpha_1+\dots+c_n\alpha_n,\quad c_i\in K.$$

$$Tr_{L/K}(b\alpha_j)=\sum c_i\,Tr_{L/K}(\alpha_i\alpha_j)$$

$$\begin{pmatrix} Tr_{L/K}(b\alpha_1)\\ \vdots \\ Tr_{L/K}(b\alpha_n)\end{pmatrix}=\left(Tr_{L/K}(\alpha_i\alpha_j)\right)\begin{pmatrix} c_1\\ \vdots\\ c_n\end{pmatrix}$$

נכפיל ב- $\left(\operatorname{adj}\,Tr_{L/K}(\alpha_i\alpha_j)\right)$ ב $M_n(A)$

$$\underbrace{\operatorname{adj}\left(Tr_{L/K}(\alpha_i\alpha_j)\right)\begin{pmatrix} Tr_{L/K}(b\alpha_1)\\ \vdots \\ Tr_{L/K}(b\alpha_n)\end{pmatrix}}_{\text{עמודה עם איברים ב-}A}=d\begin{pmatrix} c_1\\ \vdots\\ c_n\end{pmatrix}$$

לכן, $db=dc_1\alpha_1+\dots+dc_n\alpha_n\in A\alpha_1+\dots+A\alpha_n$.

טענה נניח בנוסף כי A תחום ראשי.
(לדוגמא, $A=\mathbb{Z}$).

אזי B הינו A-מודול חפשי מדרגה $n=[L:K]$.

יותר מזה, כל B-מודול $B\subseteq M\subseteq L$ נוצר סופית, גם הינו A-מודול חפשי מדרגה n.

הוכחה B הינו תת-חוג של השדה L, לכן אין לו פיתולים. לפי הטענה הקודמת

$$B \subseteq \underbrace{A\cdot\frac{\alpha_1}{d}+\dots+A\cdot\frac{\alpha_n}{d}}_{\text{A-מודול נוצר סופית.}}$$

A נותרי

לכן, B גם נוצר סופית.
לפי המיון של מודולים נוצרים
סופית מעל תחום ראשי,

$$B \cong A^m \times \cancel{A/(d_1) \times \dots \times A/(d_k)}$$

~~צריך~~ לכן B חופשי מעל A, צריך
להוכיח שהדרגה היא $[L:K]$.

מצד אחד, $B \le A\cdot\frac{\alpha_1}{d}+\dots+A\cdot\frac{\alpha_n}{d} \quad \Leftarrow$

$m = \mathrm{rank}_A(B) \le n$.

מצד שני, לפי הטענה מקודם,

אם $b_1,\dots,b_m$ הינו בסיס של

B מעל A, אזי $b_1,\dots,b_m$ פורש

את L מעל K. לכן $n \ge m$,

מסיקים $n=m$.

<u>הגדרה</u> A,B,K,L כמו במגבונת המקוריים

בסיס שלם של L מעל K

הינו בסיס $\alpha_1,\dots,\alpha_n \in B$ כך

ש- B הינו A-מודול חופשי,

$\alpha_1,\dots,\alpha_n$ גם בסיס של B מעל A.

<u>הובחנו</u>: אם A תחום ראשי, אזי

קיים בסיס שלם.

הערה

יהיו $\alpha_1,\dots,\alpha_n$, $\beta_1,\dots,\beta_n$

שני בסיסים שלמים

$$\begin{pmatrix}\beta_1\\ \vdots \\ \beta_n\end{pmatrix} = C\begin{pmatrix}\alpha_1\\ \vdots \\ \alpha_n\end{pmatrix}$$

$C^{-1}, C \in M_n(A) \Leftarrow \det(C) \in A^*$.

$$d(\beta_1,\dots,\beta_n) = (\det C)^2\, d(\alpha_1,\dots,\alpha_n)$$

אם $A=\mathbb{Z}$, $B=$ חוג השלמים בשדה מספרים L,

אזי $(\det C)^2 = 1 \Leftarrow d(\alpha_1,\dots,\alpha_n)$

לא תלויה בבחירה של הבסיס השלם.

נקרא לה d_L, הדיסקרימיננטה של L.

<u>תזכורת</u> A חוג. המימד (של קרול) של A הינו האורך המקסימלי $d = \dim A$ של שרשרת של אידיאלים ראשוניים
$$P_0 \subsetneq P_1 \subsetneq P_2 \subsetneq \cdots \subsetneq P_d.$$

<u>הגדרה</u> חוג A נקרא תחום דדקינד אם הוא
1) תחום שלמות
2) נתרי
3) $\dim A = 1$
4) סגור בשלמות.