גאומטריה אלגברית הרצאה 5 1

משפט האפסים של הילברט (Nullstellensatz)

משפט: תהי $A$ אלגברה נוצרת סופית מעל שדה או מעל $\mathbb{Z}$.
אז קבוצת הנקודות הסגורות צפופה ב- $Spec(A)$.

ניסוח שני, יותר אלגברי:
נזכיר כי $p\in Spec(A)$ סגורה $\Leftrightarrow$ $p$ אידיאל מקסימלי.
תהי $Spm(A) \subset Spec(A)$ קבוצת האידיאלים המקסימליים.
לפי הגדרה,

$$\overline{Spm(A)} = \bigcap_{V(E)\supset Spm(A)} V(E)$$

עכשיו $V(E)\supset Spm(A) \Leftrightarrow E\subset m$ לכל אידיאל מקסימלי $m$
כך ש-

$$\overline{Spm(A)} = V(J)$$

כאשר $J=\bigcap_{m\in Spm(A)} m$ - אידיאל זה חשוב מאוד, כך שיש לו שם
משלו - רדיקל של Jacobson.
לכן, משפט האפסים בנוסח טוען כי $J(A)=N(A)$ עבור $A$
אלגברה נוצרת סופית מעל שדה או מעל $\mathbb{Z}$.
הוכחת המשפט נסתמך על הלמה הבאה:
למת-מפתח: יהי $m$ אידיאל מקסימלי של החוג $A[t]$
($A$ נוצרת סופית כמו קודם). אזי החיתוך $m\cap A$ מקסימלי
ב- $A$.

הוכחת הלמה.
יהי $m\cap A=p$. נחליף את $A$ ב- $\bar{A}=A/p$ ואת $m$
בתמונתו $\bar{m}$ בחוג $\bar{A}[t]$. כך מיד מצמצמים את
המקרה הכללי למקרה בו $A$ תחום שלמות, $m\cap A=0$.
עלינו להוכיח כי $(0)$ אידיאל מקסימלי ב- $A$. כלומר כי
$A$ שדה.
ובכן, $A$ תחום שלמות שהוא אלגברה נוצרת סופית
מעל שדה או מעל $\mathbb{Z}$, $m$ אידיאל מקסימלי ב- $A[t]$
כך ש- $m\cap A=(0)$; יש להוכיח כי $A$ שדה.

2 יהי $\mathfrak{m}$ ו- $L=A[t]/\mathfrak{m}$. זאת גם כן אלגברה נוצרת סופית מעל שדה או מעל $\mathbb{Z}$; ההרכבה $A\to A[t]\to L$ היא חח"ע כי $A\cap\mathfrak{m}=(0)$ הוא הגרעין שלה. עלינו להוכיח כי $A$ שדה.

<u>מקרה 1</u> מעל שדה $K$.

נתון:

$$K\to A\to L$$

$K,L$ שדות, $A,L$ אלגבראות נוצרות סופית מעל $K$.
יש להוכיח כי $A$ שדה. נעשה את זה בשני שלבים:
(א) נוכיח כי $L$ הרחבה סופית של $K$. אז גם $\dim A<\infty$
(ב) נוכיח כי כל אלגברה $A$ <u>בעלת מימד סופי מעל שדה</u> $K$ היא בעצמה שדה רק אם ידוע כי היא תחום שלמות.

הוכחת (א).
נשתמש בכך ש- $L$ נוצרת סופית מעל $K$ <u>כאלגברה</u>.
ויהיו $x_1,\dots,x_n$ איברים ב- $L$ המורישים את $L$ כאלגברה מעל $K$
[נזכיר כי זה אומר כי הומו'
$$k[t_1,\dots,t_n]\to L$$
$$t_i\mapsto x_i$$
הוא הומו' על.]
מספיק להוכיח כי $x_1,\dots,x_n$ אלגבריים מעל $K$. אז באופן אוטומטי נקבל את הסופיות של ההרחבה $L$ מעל $K$.
הוכחה - אינדוקציה לפי $n$.
$n=1$. $L=K[t]/I$ שדה $\Rightarrow$ $I=(f)$, $f\neq 0$ $\Rightarrow$ $[L:K]=\deg(f)$
נניח כי המשפט ידוע עבור מספר יוצרים $<n$ ועבור כל שדה $K$.
נניח בדרך השלילה כי $x_1$ טרנסצנדנטי מעל $K$.
$L$ שדה $\Rightarrow$ $K(x_1)\subset L$. ברור כי $L$ נוצר מעל $K(t_1)$ ע"י $x_2,\dots,x_n$. לפי הנחת האינדוקציה, $x_2,\dots,x_n$ איברים אלגבריים מעל השדה $K(x_1)$. זה אומר כי לכל $i=2,\dots,n$ קיים פולינום עם מקדמים ב- $K[x_1]$ המאפס את $x_i$ (איננו טוענים כי המקדם הראשי שלו שווה ל- 1).
יהי $p_i(x_1)$ המקדם הראשי שלו ויהי $p(x_1)=\prod_i p_i(x_1)$.
האיבר $p(x_1)\cdot x_i$ שלם לכל $i=2,\dots,n$.

3 כיוון ש- L נוצר ע"י $x_2,\dots,x_n$ מעל $K[x_1]$, כל איבר ב- L
מתחיל להיות שלם מעל $K[x_1]$ אחרי מכפלה בחזקה
מסוימת של $p(x_1)$.

בפרט, זה נכון לגבי $K(t_1) \subset L$. כיוון ש $k[x_1]$
בעל פירוק יחיד לראשוניים אי-פריקים, כל איבר שלם מעל $K[x_1]$
הוא ב- $k[x_1]$.

מסקנה: כל איבר בשדה הפונקציות רציונליות $K(x_1)$
הופך לפולינום אחרי מכפלה בחזקה מסויימת של $p(x_1)$.
זה אפשרי רק אם מעל K יש מספר סופי של פולינומים
אי-פריקים. אך, למזלנו, זה בלתי-אפשרי!

מדוע? אם K אינסופי, $t-a$ פולינומים אי-פריקים עבור
$a\in K$ שונים. אם K סופי, $K=\mathbb{F}_q$ ויש הרחבות של כל דרגות
של K, $\mathbb{F}_q \subset \mathbb{F}_{q^n}$. כל אחת מהן נוצרת ע"י איבר אחד
(איבר פרימיטיבי) לכן הפולינום המינימאלי שלו בעל מעלה n.

ב) חלק זה סטנדרטי אך נזכיר אותו: יהי $K \subset A$ תחום
שלמות, $\dim_K A<\infty$. אז A שדה. ואמנם, אם $0\neq a\in A$,
הכפלה ב- a היא טרנספורמציה ליניארית

$$A \xrightarrow{\cdot a} A$$

של מרחב וקטורי A מעל K. $\dim A<\infty$, היא חח"ע $\Rightarrow$ על.
זה אומר כי קיים b: $a.b=1$.

מקרה 2 A אלגברה נוצרת סופית מעל $\mathbb{Z}$.
יש לנו

$$\mathbb{Z} \longrightarrow A \longrightarrow L$$

L שדה, $A\to L$ חח"ע, ואילו שניהם A ו- L נוצרות סופית
מעל $\mathbb{Z}$.
הגרעין של הומומ' $\mathbb{Z}\to A$ הוא $(0)$ או $(p)$ ראשוני כי L
שדה. אם הוא $(p)$, אז A אלגברה נוצרת סופית
מעל $\mathbb{F}_p$ $\Rightarrow$ כבר הוכחנו.
נוכיח כי המקרה $(0)$ בלתי-אפשרי.

4 במלים אחרות, נוכיח כי שדה $L$ בעל $\mathrm{char}\,L=0$ לא יכול להיות נוצר סופית מעל $\mathbb{Z}$ כאלגברה.

ובכן, $L$ שדה נוצר ע"י $x_1,\dots,x_n$ כאלגברה מעל $\mathbb{Z}$.
לפי חלק ראשון של המשפט, $L$ הרחבה סופית של $\mathbb{Q}$.
זה גורר כי כל $x_i$ שורש של פולינום עם מקדמים שלמים.
זה אומר כי קיים מספר $N$ שלם כך ש $Nx_i$ שלם מעל $\mathbb{Z}$.
לכן, כל איבר של $L$ מתחיל להיות שלם מעל $\mathbb{Z}$ אחרי הכפלה בחזקה של $N$.
זה נכון בפרט גם לכל מספר רציונלי - סתירה לקיום של אינסוף מספרים ראשוניים!

## הוכחת המשפט

יהי $a\in J(A)$. נתבונן בפולינום $f=1+at\in A[t]$.
אם $f\in m$ עבור $m\in \mathrm{Spm}(A[t])$ אז לפי הלמה התיאוק $A\cap m=p$ אידיאל מקסימלי ב-$A$, לכן $a\in p$, ואז $at\in p[t]\subseteq m$. המסקנה: $1=f-at\in m$ _ סתירה.

המסקנה: $f$ לא שייך לאף אידיאל מקסימלי, ז.א. $f$ הפיך $\Leftarrow (1+at)(c_0+c_1t+\dots+c_nt^n)=1$

$$c_0=1$$
$$a+c_1=0 \Rightarrow c_1=-a$$
$$ac_1+c_2=0 \Rightarrow c_2=a^2$$
$$ac_2+c_3=0 \Rightarrow c_3=-a^3$$

וכן הלאה, $c_n=(-1)^n a^n$,
$0=c_{n+1}=(-1)^{n+1}a^{n+1}$

לכן, האיבר $a$ נילפוטנטי.
סוף ההוכחה.