הרצאה 6, תזכורת – פולינום יכול להיות אי פריק אבל לא ראשוני.

יהי $p\in K\{x\}$ פולינום דיפרנציאלי בשפה (דיפרנציאלי) ממציין 0, הסדר של p הוא n.

נגדיר: $I(p):=\{g\in K\{x\} \mid s^m\cdot g\in\langle p\rangle$ לאיזשהו $m\in\mathbb{N}\}$

כאשר $\langle p\rangle$ הוא האידיאל הדיפרנציאלי שנוצר ע"י p.

S נגזרת המפרידה של p: $S=\frac{\partial p}{\partial x^{(n)}}$

משפט: 1) אם p אי פריק אז $I(p)$ אידיאל דיפרנציאלי ראשוני.
2) כל אידיאל דיפרנציאלי ראשוני הוא מהצורה הזאת ב-$K\{x\}$.

בעולם האלגברי, במקום $I(p)$ יש את (p) ואז
1) אנלוגי לכך שחוג הפולינומים הוא תחום פריקות יחידה, לכן אי פריק אומר ראשוני, ו-2) אנלוגי לכך ש-$K[x]$ תחום ראשי – כל אידיאל נוצר ע"י איבר אחד.

בעולם שלנו, 1) נובע מ-2) שנובע מחילוק עם שארית.

הגדרנו $q\gg r$ (r יותר פשוט מ-q) אם הסדר של r קטן מהסדר של q או שהסדר שווה, m והדרגה כפולינום ב-$x^{(m)}$ יותר קטנה.

אפשר לרשום $p(a)=\underbrace{a(x)}_{\text{המקדם הראשי}}\cdot {x^{(n)}}^{d}+p_1$ כך שהסדר של $a(x)$ קטן מ-n ו-$p_1\ll p$.

נסמן ב-$A_i\subseteq K\{x\}$ להיות תת החוג של האיברים שהסדר שלהם קטן מ-i. אז $\partial(A_i)\subseteq A_{i+1}$ ולכן אם נגדיר $B_i=A_{i+1}/A_i$ מודול מעל A_i ולכן מעל A_j עבור $j<i$.

אז ∂ משרה $\partial_i: B_i\longrightarrow B_{i+1}$ שהיא העתקה של מודולים מעל A_i כי אם $b\in B_i$ ו-$a\in A_i$ אז:
$$\partial_i(ab)=\partial(a\tilde{b})=\partial(a)\tilde{b}+a\,\partial(\tilde{b})=a\,\partial_i(b)$$

בפרט עבור $0\neq \bar{p}\in B_n$,
$$\overline{\partial(p)}=\partial_n(\bar{p})=\overline{\overset{=0}{p^{\partial}}+\underset{S}{\frac{\partial p}{\partial x^{(n)}}}\cdot x^{(n+1)}}=S\cdot x^{(n+1)}$$

באופן יותר כללי, לכל סדר k. $\partial^k(p) = s\cdot x^{(n+k)} + $ סדר יותר נמוך מ-$n+k$

כי) $\overline{\partial^k(p)} = \partial_{n+k} \ldots \partial_{n}(\overline{p}) = \ldots = s x^{n+k}$

<u>טענה</u> (תלות עם קודמת): לכל $q\in K\{x\}$ יש מספרים טבעיים $m,l\in\mathbb{N}$ ו- $r\in K\{x\}$ כך ש- $r \ll p$ ו- $a^l s^m q \equiv r \pmod{\langle p\rangle}$.

גרסה שנייה: לכל $q\in K\{x\}$ יש $m\in\mathbb{N}$ ו-$r\in K\{x\}$ כך שהסדר של r הוא לכל היותר n ו- $s^m q\equiv r \pmod{\langle p\rangle}$.

<u>הוכחה:</u> אפשר לרשום $q=b\cdot (x^{(j)})^e+q_1$ עבור $q_1\ll q$, $\mathrm{ord}(b)<j$.
אם $j<n$ סיימנו, נניח $n\le j$.

① אם $n<j$ ראינו ש- $\partial^{j-n}(p)=s\cdot x^{(j)}+\ldots$. אז נעזר בחלוקת ש, נכפיל את b ו-q ונכפיל ב-s:
$b\partial^{j-n}(p)^e - s^e q \ll q$

באינדוקציה, יש r_1, m_1, l_1 כך ש- $a^{l_1}s^{m_1}(b\partial^{j-n}(p)^e-s^e q) - r_1 \in\langle p\rangle$

סיים $a^{l}s^{m} s q-r_1\in\langle p\rangle$. (זה גם מוכיח את גרסה 2)

② $n=j$ אחרי שמתלויים ב- a אפשר לעשות חלוקת פולינומים רגילה ונקבל $q-r\in(p)$ עבור r ממעלה יותר נמוכה אחרי חלוקה ב-a. אז בחוג המקורי $a^l q-r\in(p)$

<u>טענה:</u> אם הסדר של q הוא n ו- $q\in I(p)$ אז $s^m q\in(p)$ עבור איזשהו m טבעי. ו, אי פריק אז $q\in(p)$.

<u>הוכחה:</u> יש m כך ש- $s^m q\in\langle p\rangle$ כלומר $s^m q\in(p,\partial(p),\ldots,\partial^k(p))$ לאיזשהו k מינימלי. אם $k>0$,
$\partial^k(p)=s x^{n+k}+\underbrace{p_1}$ (סדר יותר נמוך). זה נכון בכל ערך של $x^{(n+k)}$ ובפרט עבור $x^{(n+k)}=-\frac{p_1}{s}$, אז יתקיים עם k ב-1 קטן יותר — סתירה למינימליות. אם p אי פריק, אז הוא ראשוני (אוניברסלי) ולכן $s\in(p)$ או $s^{m-1}q\in(p)$ אבל המקרה הראשון לא יתכן כי הדרגה של s נמוכה יותר. באינדוקציה, מקבלים $q\in(p)$.

הוכחת המשפט:

(א) $I(P)$ אידיאל (הם) דיפרנציאלי – ניקח $q\in I(P)$

אז $s^m q\in\langle P\rangle$ ולכן $s^{m+1}q\in\langle P\rangle$ אז

$s^{m+1}\partial(q)\in\langle P\rangle \Leftarrow \partial(s^{m+1}q)=\underbrace{(m+1)s^m\cdot\partial(s)q}_{\in\langle P\rangle}+s^{m+1}\partial(q) \in\langle P\rangle$ בפרט

לכן $\partial(q)\in I(P)$.

ראשוני – נניח כי $q_1q_2\in I(P)$ - אז $s^m q_1q_2\in\langle P\rangle$. לפי חלוקה עם שארית (גרסה 2) הסדר של q_1q_2 קטן/קטנה. לפי הטענה הקודמת $s^{m'}q_1q_2\in(P)$ ובגלל ש-P אי פריק, $q_1q_2\in(P)$ ולכן $q_1\in(P)$ או $q_2\in(P)$.

(ב) ניקח אידיאל דיפרנציאלי ראשוני $0\neq I\subseteq k\{x\}$ ניקח $0\neq P$ ב-I מינימלי קיים לסדר $<<$. P אי פריק כי אם $P=P_1\cdot P_2$ אז אחד $P_i\in I$ כי I ראשוני ו-$P_i<<P$ בסתירה לבחירה של P.

יהי $q\in I(P)$ אז $s^m q\in\langle P\rangle\subseteq I$ ו-I ראשוני ולכן (היות ו $s<<P$), $q\in I$.

מאידך, ניקח $q\in I$, לפי חלוקה עם שארית קיים r, P, $\underbrace{a^l s^m q}_{\in I}-r\in\langle P\rangle\subseteq I$ עבור $m,l\in\mathbb{N}$ ו- $r<<P$, לכן $r\in I$ אבל $r<<P$ לכן לפי בחירת P, $r=0$. לכן $r=0$ לפי בחירת P. אז $s^m a^l q\in\langle P\rangle$ ול $a^l\cdot q\in I(P)$ אבל הוכחנו בסעיף הקודם ש-$I(P)$ ראשוני לכן $a^l\in I(P)$ או $q\in I(P)$ אבל הראשון לא ייתכן כי הוא מסדר יותר נמוך.

ב-$k\{x\}$ אין תנאי שרשרת עולה על אידיאלים דיפרנציאליים.

קרי, אידיאלים דיפרנציאלים אינם בהכרח נוצרים סופית.

למשל, $I_k=\langle x^2,(x')^2,\dots,(x^{(k)})^2\rangle$ אז $I_k\subsetneq I_{k+1}$ (לא טריוויאלי)

הגדרה: אם I אידיאל, $\sqrt{I}=\{a\mid \exists k\ a^k\in I\}$. I נקרא רדיקלי אם $I=\sqrt{I}$. מנקודת מבט של הקבוצות גדירות בשפות אפשר להסתכל רק על אידיאלים רדיקליים.

במקרה הדיפרנציאלי, אם I אידיאל דיפרנציאלי, $\sqrt{I}$ הוא גם דיפרנציאלי ומקיים:

ואם I רדיקלי אז לכל a,b אם $a\cdot b\in I$ אז $a\in I$ או $b\in I$.

משפט: Ritt-Raudenbush (משפט הבסיס): אם בחוג דיפרנציאלי A כל אידיאל דיפרנציאלי רדיקלי נוצר סופית כאידאל דיפרנציאלי רדיקלי, אז אותו דבר נכון ל- $A\{x\}$.

הרצאה 7: איך נראות קבוצות גדירות כשהן בשדות?

דוגמא: השדה $\mathbb{Q}$. קיימת נוסחא $\varphi(x)$ עם התכונה כך שלכל $r\in\mathbb{Q}$, $\varphi(r)$ מתקיים אמ"מ $r\in\mathbb{Z}$.
במילים אחרות, $\mathbb{Z}\subseteq\mathbb{Q}$ היא תת קבוצה גדירה.
(משפט של ג'וליה רובינסון).
אכן, קבוצות גדירות ב- $\mathbb{Z}$ הן גם גדירות ב- $\mathbb{Q}$.
משפט אי השלמות של גדל אומר שאי אפשר לתאר במפורש את התורה של $\mathbb{Z}$. לכל n,m יש העתקה גדירה הפיכה מ- $\mathbb{Z}^n$ ל- $\mathbb{Z}^m$. יותר מזה, הקבוצה $\bigcup_{n\in\mathbb{N}}\mathbb{Z}^n$ גם גדירה, וגם ההעתקה, חח"ע ל- $\mathbb{Z}$.

דוגמא: ב- $\mathbb{C}$, $\exists x(x^2=y)\equiv y=y$.

נניח ש- M מבנה ו- $X\subseteq M^n$ תת קבוצה גדירה.
X היא חסרת כמתים אם היא גדירה ע"י נוסחה בלי כמתים. זו תכונה של התורה T של M!
אם φ וגם ψ מגדירות את X אז $T\models\forall x(\varphi(x)\leftrightarrow\psi(x))$.

הערה: נניח ש- T תורה, φ נוסחא. אז φ שקולה לנוסחא חסרת כמתים אמ"מ לכל מודל M של T ולכל $a\in\varphi(M)$ התורה T_a גוררת את $\varphi(a)$.

(תזכורת: ראינו ש- T_A היא התורה של מודלים M של T ביחד עם שיכון של A ב- M. מפורשות, מוסיפים "סימני קבוע" c_a לכל $a\in A$ ומוסיפים אקסיומות המגדירות "עותק כבד" של הקבועים האלה. אם $\varphi(x_1,\dots,x_n)$ נוסחא חסרת כמתים ו- $\langle a_1,\dots,a_n\rangle\in\varphi(M)$ אז $\varphi(c_{a_1},\dots,c_{a_n})\in T_A$.

לדוגמא, $T=F$ (תורת השדות), K_0,

שפה אין לי T_{K_0} יש קבוע לכל איבר של K_0 ואם
$a,b\in K_0$, $c_a+c_b=c_{a+b}$ ב-T_{K_0} וכו׳)

הוכחת הטענה: אם φ שקולה לנוסחא חסרת כמתים אז
אפשר להניח שהיא בעצמה חסרת כמתים ולכן $\varphi(\bar{a})\in T_a$.
בכיוון השני, אפשר להניח ש-φ עקבית עם T, אחרת
הכל מתקיים באופן ריק. נגדיר $\Gamma=\{\psi \mid \psi$ חסרת כמתים $T\vDash\forall x(\varphi(x)\to\psi(x))\}$

נוכיח ש-$T\cup\Gamma(c)\vDash\varphi(c)$. נניח בשלילה שלא. אז יש מודל (N,c_N)
של $T\cup\Gamma(c)$ שבו $c_N\notin\varphi(N)$. נסתכל על T_{c_N}. אז $T_c\cup\{\varphi(c)\}$
(ולכן T_c מכיל אותם)
לא תורה עקבית כי אחרת לפי משפט הקומפקטיות
$T\cup\{\varphi(c)\}$ לא עקבית עם $\psi(c)\in T_c$ עבור נוסחא חסרת
כמתים ψ. זה אומר $T\vDash\forall x(\varphi(x)\to\neg\psi(x))$ אבל זה אומר יש $\neg\psi\in\Gamma$
ובפרט $\neg\psi\in T_c$ בסתירה לכך ש-N מודל של T_c.
ניקח מודל $\langle M,c_M\rangle$ של $T_c\cup\varphi(c)$, אז $c_M\in\varphi(M)$ ולכן
$T_c\vDash\varphi(c)$ בסתירה לקיום של N.
הוכחנו ש- $T\cup\Gamma\vDash\varphi$. ממשפט הקומפקטיות, יש $\psi\in\Gamma$
כך ש- $T\cup\{\psi\}\vDash\varphi$ כלומר $T\vDash\psi\to\varphi$ ולכן קשרת
Γ $T\vDash\varphi\to\psi$.

<u>תרגיל</u>: נניח שלכל $\varphi(\bar{x},y)$ כאשר y משתנה אחד, ו-φ
חסרת כמתים הי״מת נוסחא חסרת כמתים $\psi(\bar{x})$ כך ש-
$T\vDash\forall\bar{x}(\psi(\bar{x})\leftrightarrow\exists y\varphi(\bar{x},y))$ אז ל-T יש חילוף כמתים (כל נוסחא
שקולה לנוסחה חסרת כמתים)

<u>טענה</u>: התורה T של השדה $\mathbb{C}$ מחלצת כמתים.
<u>הוכחה</u>: ניקח נוסחא חסרת כמתים $\varphi(\bar{x},y)$ ונראה ש-
$\exists y\varphi(\bar{x},y)$ שקולה לחסרת כמתים. צריך להראות שאם
M מודל של התורה, ו- $\bar{a}\in M$ כך ש- $\exists y\varphi(\bar{a},y)$
נכון ב-M אז $T_a\vDash\exists y\varphi(\bar{a},y)$.
אפשר להניח ש- $\varphi(\bar{a},y)=p_1(y)=0\wedge\dots\wedge p_n(y)=0\wedge q(y)\neq0$ כאשר
p_i,q פולינומים מעל השדה L_0 שנוצר על ידי $\bar{a}$.
למערכת הזו יש פתרון ב-M ולכן האידיאל שנוצר ע״י

ה-p_i הוא אידיאל ממש ולא מכיל שום חזקה של q לכן $\varphi(\bar{a},y)$ נובעת ממשוואה מהצורה $p(y)=0$ עבור פולינום של הקבוע p:

$$p = p_{\bar{a}}(y) = y^n + \sum_{i<n} b_i y^i$$

$\mathbb{C}$ סגור אלגברית אז $TK \forall b \exists y \, P_b(y)=0$

לכן בכל מודל של T_a ל-$P_b(y)$ יש שורש

<u>מסקנה:</u> יש תורה ACF של שדות סגורים אלגברית והיא מחלצת כמתים (כי בהכרח השתמשנו כאן בסגירות האלגברית של $\mathbb{C}$)

(בגיאומטריה האלגברית זה משפט שבלי: התמונה של constructible set תחת העתקה פולינומית היא constructible)

אנחנו יודעים ש- $ACF \subseteq T(\mathbb{C})$ כי $\mathbb{C}$ סגור אלגברית. האם יש שוויון? לא כי יש קבוצות סגורים אלגברית ממציינים שונים. נסמן $ACF_p = ACF \cup \{\underbrace{1+1+1}_{p \text{ פעמים}} = 0\}$ (לו $p>0$) עבור $p=0$:

$$ACF_0 = ACF \cup \{1+1+\dots+1 \neq 0 \mid p \in \mathbb{N}\}$$

<u>טענה:</u> $ACF_0 = T(\mathbb{C})$

<u>הוכחה:</u> יהי $\varphi \in T(\mathbb{C})$. הוכחנו שיש פסוק חסר כמתים ψ כך ש- $ACF \models \varphi \leftrightarrow \psi$, ערך האמת של הפסוקים חסרי הכמתים מקודד בשדה הראשוני אשר נקבע ביחידות ע"י המציין.

(לפי כך ACF_p תורה שלמה לכל p ראשוני או 0).

<u>הגדרה:</u> מבנה M הוא <u>סגור יישית</u> (existentially closed) אם לכל נוסחה חסרת כמתים $\varphi(\bar{x},\bar{y})$ ולכל $\bar{a} \in M$, אם יש פתרון ל-$\varphi(\bar{a},\bar{y})$ בהרחבה של M אז יש לה פתרון ב-M.

<u>טענה:</u> אם התורה של M מחלצת כמתים אז M סגור יישית.

<u>הוכחה:</u> ניקח $\varphi(\bar{x},\bar{y})$ ו- $\bar{a} \in M$ ונניח שיש מודל N שמרחיב את M שבו ל- $\varphi(\bar{a},\bar{y})$ יש פתרון. אז $N \models \exists \bar{y}\, \varphi(\bar{a},\bar{y})$. לפי ההנחה, יש נוסחה חסרת כמתים $\psi(\bar{x})$ כך ש- $\psi(\bar{x}) \leftrightarrow \exists \bar{y}\, \varphi(\bar{x},\bar{y})$ אז ב-N $\psi(\bar{a})$ מתקיים

ולכן גם ב- M.

סגור אלגברית!

משפט: (משפט האפסים של הילברט) אם $I \subseteq k[x_1,\dots,x_n]$ אידיאל ראשוני ו- $q \notin I$ אז יש $\bar{a} \in k^n$ כך ש- $p(\bar{a})=0$ לכל $p \in I$ ו- $q(\bar{a}) \neq 0$. במילים אחרות $\bar{a} \in Z(I) \setminus Z(q)$

מסקנה: אם k סגור אלגברית ו- I,J אידיאלים רדיקליים שונים אז $Z(I) \neq Z(J)$.

הוכחת המשפט: צעד ראשון - יש שדה הרחבה סגור אלגברית L שבו יש $\bar{a} \in L^n$ כזה: ניקח L = סגור אלגברי של שדה השברים של $k[x_1,\dots,x_n]/I$. אז אפשר לקחת $\bar{a}$ = התמונה של $\bar{x}$ ב- L. אז $p(\bar{a})=0$ אוטומטית וגם $q(\bar{a}) \neq 0$ כי. ($q(\bar{x}) \in k[\bar{x}] \Leftarrow 0 \neq L$ אמ"מ $q \notin I$)

צעד שני - בתורה של ACF יש חילוף כמתים ולכן k סגור יחסית לנוסחה $p_1=\dots=p_m=0 \wedge q \neq 0$ יש פתרון בשדה ההרחבה (p_i יוצרים של I) ולכן גם ב- k, כנדרש.