הרצאה 5

$$\mathrm{Gal}(x^5+2x^4+3x^3+4x^2+5x+6) = ?!$$

<u>תזכורת:</u>

$$\begin{array}{ccccccc}
L & - & S & - & S/\beta & \hookleftarrow\!\!\!\rightarrow & L(\beta) \\
G\,| & & | & & | & & |\,G_\beta \\
K & - & R & - & R/p & \longleftrightarrow & K(p)
\end{array}$$

תת גלואה

יש לנו סדרה מדויקת,

$$\{\sigma\in G \mid \underset{\forall x\in S}{\sigma x - x\in\beta}\}$$

הסדרה המדויקת היסודית $\rightarrow$
$$1 \longrightarrow I_\beta \to D_\beta \to G_p \longrightarrow 1$$
$$D_\beta = \{\sigma\in G \mid \sigma(\beta)=\beta\}$$

<u>משפט:</u> $D_\beta \to G_p$ היא על.

[בגישה שונה (*) - נעבור ל-R/β ול-G המתאים.]

<u>הערה:</u> נסמן - $D = D_\beta$ ונסמן $K_0 = L^D$, $\beta_0=\beta\cap K_0$,
$R_0 = S\cap K_0$ כבאבחנה,

$$\begin{tikzcd}
L \arrow[d, dash] \arrow[dr, dash] & & \\
K_0 \arrow[d, dash] & S \arrow[r, dash] \arrow[d, dash] & L(\beta) \arrow[d, dash] \\
K \arrow[dr, dash] & R_0 \arrow[r, dash] \arrow[d, dash] & K_0(\beta_0) \arrow[d, phantom, "\text{צ\"ל שוויון} \; \parallel"] \\
 & R \arrow[r] & R/p = k(p)
\end{tikzcd}$$
מגדל של שדות

[(*) נעבור ל-R_p ול-G המתאים, ואז β, p יהיו מקסימליים.
נשלח $R\mapsto R_p$
$S\mapsto S_{R/p} =: S_p$
ונקבל $R/p = k(p)$, $S/\beta = l(\beta)$.]

<u>טענה:</u> $K_0(p_0) = k(p)$.

<u>הוכחה:</u> צריך להראות שלכל $a\in R_0$ יש $x\in R$ כך ש-$a\equiv x \pmod{p_0}$.
נשתמש בקבוצת נציגים Σ של G/D, ונניח שהיא מכילה את 1.
לכל $\sigma\in\Sigma$, $\sigma\neq 1$, יודעים כי $\beta\neq\sigma^{-1}(\beta)$.
אז יכול להיות ש-$K_0\cap\sigma^{-1}(\beta)=p_0$ - אבל אז כמו מקודם,
יש איזה $\tau\in D$ כך ש-
$$\tau\sigma^{-1}\beta=\beta$$
(כי D פועל טרנזיטיבית על האידיאלים של S מעל p_0)
$\Rightarrow$ $\tau\sigma^{-1}\in D$ $\Rightarrow$ $\sigma\in D$, סתירה.

חלק מהוכחה .2 משפט פ. קל.

מכאן, $\mathfrak{P}_0 \neq \sigma^{-1}\mathfrak{P}\cap K_0$. ממשפט הקירוב החלש על לקחת $b \in R_0$ כך ש-

$$b\equiv a \pmod{\mathfrak{P}_0}$$

$$b\equiv 1 \pmod{\sigma^{-1}\mathfrak{P}\cap K_0} \quad \text{לכל } 1\neq\sigma\in\Sigma$$

נסמן -

$$x = Norm_{K_0/K}(b)$$

אזי, $x \in B$

וכיוון ש-$b\equiv 1 \pmod{\sigma^{-1}\mathfrak{P}\cap K_0}$, אז $b-1\in\sigma^{-1}\mathfrak{P}_0\cap K_0 \subseteq \sigma^{-1}\mathfrak{P}\cap K_0$ ⇐ $\sigma b\equiv 1 \pmod{\mathfrak{P}}$.

⇐ $x=\prod_{\sigma\in\Sigma}\sigma b = b\prod_{1\neq\sigma\in\Sigma}\sigma b \equiv a \pmod{\mathfrak{P}}$ כנדרש לסיום. (כי $x-a\in\mathfrak{P}$, $x-a\in K_0$ ⇓ $x-a\in\mathfrak{P}_0$)

שלב שני: בה"כ, $D=G$. הסבר - נחליף את $B,\mathfrak{P},K$ ב- $B_0,\mathfrak{P}_0,K_0$. לא משנה את $D_\mathfrak{P}, I_\mathfrak{P}$ וגם לא את $G_\mathfrak{P}$ לפי הסעיפים הקודמים.

שלב 3 - $G = D \to G_\mathfrak{P}$ - היא על. יהי $x\in S$ כך ש- $\bar{x} := x \pmod{\mathfrak{P}}$ הוא איבר פרימיטיבי של $L(\mathfrak{P})/k(\mathfrak{p})$.
יהי $f(x)$ הפולינום המינימלי של x מעל K.
אזי, ב- $L[x]$,

$$\circledast \quad f(x) \mid \prod_{\sigma\in G}(x-\sigma(x))$$

ניקח את * מודולו $\mathfrak{P}$ -

$$\bar{f}(x) \mid \prod_{\sigma\in G}(x-\bar{\sigma}\bar{x})$$

למה לא שווה?

ומצד שני,

$$\bar{f}(\bar{x}) = \overline{f(x)} = 0$$

לכן, שורשי הפולינום המינימלי של $\bar{x}$ הם מהצורה $\bar{\sigma}\bar{x}$.
ניקח $\tau\in Gal(L(\mathfrak{P})/k(\mathfrak{p}))$. τ נקבע ע"י פעולה על $\bar{x}$.
כמו כן, $\tau\bar{x}$ שורש של הפולינום המינימלי של $\bar{x}$. ולכן, $\bar{\sigma}\bar{x} = \tau\bar{x}$ עבור איזה σ ⇐ כפונקציות $\bar{\sigma}=\tau$.

□

עכשיו יש לנו סדרה - הסדרה היסודית -

$$1 \to I_\beta \to D_\beta \to G_\beta \to 1$$
$$\sigma \mapsto \bar{\sigma}$$

נאמר, ש- $\beta/\mathfrak{p}$ <u>לא מסועף</u> אם $I_\beta = 1$. נאמר ש- p <u>לא מסועף ב- L</u> אם $I_\beta = 1$ לכל β/p.

[הכללה לא גלואה - $K \subseteq \underset{\substack{\downarrow \\ \text{פריק} \\ \text{סגור גלואה}}}{E} \subseteq L$ (יש מספיק) $p \subseteq q \subseteq E$.
נאמר ש- β/q לא מסועף אם $G_{L/E} \supseteq I_\beta$. ניתן משמעות
גיאומטרית - בהמשך]

למה: $D_{\sigma\beta} = \sigma D_\beta \sigma^{-1}$, $I_{\sigma\beta} = \sigma I_\beta \sigma^{-1}$

הוכחה: ① $\tau\sigma\beta = \sigma\beta \iff \tau \in D_{\sigma\beta}$. כב גורר אמ"מ

$\sigma^{-1}\tau\sigma\beta = \beta \iff \sigma^{-1}\tau\sigma \in D_\beta \iff \tau \in \sigma D_\beta \sigma^{-1}$.
② - בדומה. □

דוגמה: נזכיר פרובניוס. נניח ש- $k(\beta)$ שדה סופי. (למשל
אם $k = \mathbb{Q}$ או הרחבה סופית שלו). נסמן $k(\beta) = \mathbb{F}_q$.
(כאן $q = p^r$, p ראשוני, $r > 0$). לפי תורת השדות הסופיים -
$Gal(L(\beta)/k(\mathfrak{p})) = \langle \varphi_q \rangle$
אוטו' פרובניוס

$$\varphi_q(x) = x^q, \quad \forall x \in L(\beta)$$

יש לנו העתקה טבעית -
$$1 \to I_\beta \to D_\beta \to \langle \varphi_q \rangle \to 1$$
אם β לא מסועף, $I_\beta = 1$, וההעתקה חח"ע; לכן
יש $\sigma \in Gal(L/k)$ יחיד ש- $\sigma(x) \equiv x^q \pmod{\beta}$, לכל $x \in S$.
נגדיר זה עצמו איבר פרובניוס. מסמנים $\sigma = \left(\frac{L/k}{\beta/p}\right)$

אם נחליף את β בראשוני אחר מעל β,

עבור צמודים של β — $\left(\frac{L/K}{\beta/p}\right)$ הצמוד של כולם

(כי G צמוד ולכן מקסימלי)

לכן נגדיר -

$$\left(\frac{L/K}{p}\right) := \left\{\left(\frac{L/K}{\beta/p}\right) : \beta_p \text{ מעל } p\right\}$$

- זוהי מחלקת צמידות. כלומר נקבל מחלקת צמידות

פרובניוס, זה סימון ארטין ← אם רוצים להפוך פולינום ... ביניהם.

$$? = Gal(x^5+2x^4+3x^3+4x^2+5x+6)$$

$$S_5 \geq Gal(f(x),\mathbb{Q})$$

$$1 \longrightarrow I_p \longrightarrow \underset{p}{\overset{S_5 \geq}{D}} \longrightarrow \underset{p}{\overset{S_5 \geq}{G}} \longrightarrow 1$$

נפרק את הפולינום מעל $\mathbb{F}_p$ שונים -

$p=2$ — $x(x^2+x+1)^2$

$p=5$ — $(x+3)(x^4+4x^3+2)$

$p=11$ — x^5+ ______ $+5x+6$

$p=19$ — $(x^2+7x+3)(x^3+14x^2+16x+2)$

מודולו $p=11$ -

$L(P_{11}) =$ פיצול שלם

$5 \mid$ $\Rightarrow G_{11} = \langle$ 5-מחזור $\rangle$

$\mathbb{F}_{11}$

מכאן נובע ש-

$\left(\frac{L/\mathbb{Q}}{P_{11}, 11}\right) =$ 5-מחזור

לכן מ-$p=11$ — G מכילה מחזור 5.

מודולו $p=2$ — אם שורשי f הם $\alpha_1, \dots, \alpha_5$

שורשי f מודולו 2 הם $\bar{\alpha}_1, \dots, \bar{\alpha}_5$ — לא בהכרח שונים

וגם - $\bar{\alpha}_1 = \bar{\alpha}_2$, $\bar{\alpha}_3 = \bar{\alpha}_4$

מה קורה עם אוטומורפיזם $G_\beta = 2$ שווה חילוף

⇐ 2 - D/I של חילוף

⇐ 2 - D של ... -

$(ij)(kl)$

$(ij\,kl)$

(ij)

מקרה $p=5$: נשאר מסדר 4 $\Leftarrow$ G מכיל מעגל 5 ומעגל 4:
(G פותר — טרנזיטיבי — על בסיס $z_i \neq z_j$)

מקרה $p=19$: מקרה כללי -

$$\sigma = (ij)(klm)$$
$$\Downarrow$$
$$\sigma^3 = (ij)$$

$\Leftarrow$ יש חילוף.

$\Leftarrow$ G מכיל חילוף + מעגל באורך p $\Leftarrow$ $G = S_p$.

$\square$

<u>למה:</u> יהי B סגור בשלמות של שדה מנה K. תהי $K \subseteq E \subseteq L$ מגדל שדות, כך ש‑L/K גלואה, ויהיו B_E, B_L הסגורים השלמים של B בשדות המתאימים, $B \subseteq B_E \subseteq B_L$, ו‑$P \subseteq P_E \subseteq P_L$ אידיאלים כך ש‑$P_L \cap E = P_E$, $P_E \cap K = P$. אזי,

① $D_{L/E} = D_{L/K} \cap G_{L/E}$

$I_{L/E} = I_{L/K} \cap G_{L/E}$

$$
\begin{array}{ccccc}
K & - & E & - & L \\
\cup & & \cup & & \cup \\
B & \subseteq & B_E & \subseteq & B_L \\
\cup & & \cup & & \cup \\
P & \subseteq & P_E & \subseteq & P_L
\end{array}
$$

② אם בנוסף E/K גלואה, אז התרשים הבא חילופי, עם השורות והעמודות מדויקות -

$$
\begin{tikzcd}
 & 1 \arrow[d] & 1 \arrow[d] & 1 \arrow[d] & \\
1 \arrow[r] & I_{L/E} \arrow[r] \arrow[d, "\text{שיכון}"] & D_{L/E} \arrow[r] \arrow[d, "\text{שיכון}"] & G_{L/E} \arrow[r] \arrow[d, "\text{שיכון}"] & 1 \\
1 \arrow[r] & I_{L/K} \arrow[r] \arrow[d, "res"] & D_{L/K} \arrow[r] \arrow[d, "res"] & G_{L/K} \arrow[r] \arrow[d, "res"] & 1 \\
1 \arrow[r] & I_{E/K} \arrow[r] \arrow[d] & D_{E/K} \arrow[r] \arrow[d] & G_{E/K} \arrow[r] \arrow[d] & 1 \\
 & 1 & 1 & 1 &
\end{tikzcd}
$$

(זה אומר שכל הגדלים הם פונקטוריאליים)

<u>הוכחה:</u>

① תרגיל (לוודא)

② - הוכחה שהשורות מדויקות.

סעיף (1) - $D_{L/E}$ הוא גרעין של הצמצום $D_{L/K} \to D_{E/K}$

ואותו דבר ל‑$I_{L/E}$. העמודה הימנית מדויקת.

מ.משפט היסודי של גלואה.

נכון: ש- res על; ניקח $\sigma\in D_{E/K}$ כלומר $\sigma: E\to E$ כך ש- $\sigma P_E=P_E$. נר׳ל: נרחיב את σ ל- $\sigma'\in Gal_{L/K}$ כלומר $\sigma'|_E=\sigma$. נסמן $q=\sigma' P_L$ אם $q=P_L$ אז $\sigma'\in D_{L/K}$ וסיימנו.

אחרת, קיים $\tau\in Gal(L/E)$ כך ש- $\tau q=P_L$ (כי q ו- P_L שניהם מעל P_E)

$$\Leftarrow \quad \tau\sigma' P_L=P_L$$

$$\Leftarrow \quad \tau\sigma'\in D_{L/E}$$

וגם,

$$res_E(\tau\sigma')=res_E(\tau)\,res_E(\sigma')=$$
$$=res_E(\sigma')=\sigma$$

$\Leftarrow$ שני המשולש הימני מתחלף $\Leftarrow$ הריבוע השמאלי מתחלף (diagram chasing)

4. חוגי דדקינד

4.1 – הגדרות ותכונות בסיסיות

הגדרה: חוג B נקרא חוג הערכה בדידה (DVR) אם B הוא PID, מקומי, שאינו שדה.

(סימון) DVR כ- $(B,\pi B)$ – πB האידאל המקסימלי, π נקרא מחולל (uniformizer).

טענה: יהי B חוג הערכה בדידה.

① B הוא נתרי.

② לכל $0\neq x\in B$ קיימת הצגה – $x=u\pi^k$, $k\geq 0$, $u\in B^\times$.
(כמו כן ל-k קוראים ההערכה של x.)

③ B סגור בשלמות.

④ אידאל $0\neq$ הוא מהצורה $\pi^k B$

⑤ $spec(B)=\{0,\pi B\}$.

נאמר שתכונה P עבור חוגים מקיימת מקומיות ב- B, אם כל הלוקליזציות של B באידאלים ~~מקסימליים~~ ראשוניים $0\neq$ מקיימים את P.

הגדרה: תחום שלמות שאינו שדה נקרא דדקינד אם -
① ת.ו נתרי
② סגור בשלמות
③ מקומית — DVR

טענה: ① כל אידיאל ראשוני $P\neq 0$ בחוג דדקינד הוא מקסימלי.
② כל לוקליזציה — כפלית, $M\subseteq R$, R_M הוא דדקינד או שדה.

~~הוכחה: כל $p\in spec(R)$, p מקסימלי $\Leftrightarrow$ pR_p מקסימלי.~~

הוכחה:
① ניקח $P\neq 0$ ראשוני לא מקסימלי. אז יש $P \subsetneq Q$, ואז, $0\neq PR_Q \subsetneq QR_Q$ בחוג ה-DVR יש שני ראשוניים $\neq 0$ — סתירה.
② כל התנאים נשמרים ע"י מעבר. ∎

$\boxed{\text{ב.2 פירוק יחיד}}$ UFD
בחוגי UFD יש יחידות פירוק לראשוניים, אבל זה לא תמיד נשמר בהרחבה שלמה, למשל -
$\mathbb{Z} \subseteq \mathbb{Z}[\sqrt{-5}]$
בחוגי דדקינד יהיה פירוק לראשוניים ברמת האידיאלים וכך נשמר ע"י הרחבה שלמה.

משפט נוסף: B חוג דדקינד, $0\neq I \triangleleft B$ אידיאל, $B = R/I$.

למה: יהי B נתרי וכל אידיאל ראשוני הוא מקסימלי.
אז, כל אידיאל מכיל מכפלה של אידיאלים ראשוניים.

הוכחה: אם לא, G א' שלא מכיל כנ"ל מקסימלי. אז יש $\mathfrak{a}$ מקסימלי כזה. $\mathfrak{a}$ לא ראשוני אם $\mathfrak{a}=B$
$\Leftarrow$ קיים $ab\in \mathfrak{a}$ אבל $a,b\notin \mathfrak{a}$, ואז,
$\prod P_i \subseteq aB+\mathfrak{a}$
$\prod Q_j \subseteq bB+\mathfrak{a}$

[מקסימלי $\mathfrak{a}$] וכו'...

$$\prod P_i \prod Q_j \subseteq (aB+\mathfrak{a})(bB+\mathfrak{a}) = abB + \mathfrak{a} = \mathfrak{a}$$ □

מסקנה: יהי B נתרי כל ראשוני בו מקסימלי, אז יש מקסימליים $P_1, \ldots, P_n$ וטבעיים $k_1 \ldots k_n$ כך ש- $0 = P_1^{k_1} \cdots P_n^{k_n}$

(הוכחה: ניקח את $\mathfrak{a} = 0$)

למה: חזקות של זרים הם זרים.

הוכחה: נניח a,b זרים, נראה שגם $a^k b^l$ זרים. אכן:

$$(a+b)^{k+l} \subseteq a^k + b^l$$

*בינום של ניוטון

אבל $a+B=B$ ולכן $B=(a+b)^{k+l}$. סיימנו. □

מסקנה: B חוג בו כל ראשוני מקסימלי, נתרי, ולכן,

$$0 = \prod_i P_i^{k_i}$$

אז-

$$B \cong \prod B/_{P_i^{k_i}}$$

(נובע מ CRT והלמה הקודמת)

מסקנה: כיוון ש- $B/_{P_i^{k_i}}$ מקומי, P_i האידאל המקסימלי היחיד בו,

$$\operatorname{Spec} B = \{P_1, \ldots, P_n\}$$

($\operatorname{Spec}(B \times S) = \operatorname{Spec} B \sqcup \operatorname{Spec} S$?)

אפשר להסיק זו כאן בגלל התכונה האוניברסלית