ניזכר בהגדרה של דיסקרימיננטה:

$$\Delta = \prod_{i<j} (r_i - r_j)$$

כאשר $r_1, \dots r_n$ הם שורשים של פולינום $f(x)$. $D = \Delta^2$ היא הדיסקרימיננטה.
נשים לב שΔ תלוי בסדר בחירת השורשים, אבל D לא בהכרח.
אם $f(x) \in F[x]$, ראינו בתרגיל בית ש$D \in F$.

תרגיל

$f(x) \in \mathbb{Q}[x]$ מתוקן מדרגה 3, u, v, w הם שרשי f, D דיסקרימיננטה. הראו ש

$$\mathbb{Q}(u, v, w) = \mathbb{Q}\left(u, \sqrt{D}\right)$$

פתרון

נסמן
$$\begin{array}{l} E = \mathbb{Q}(u, v, w) \\ K = \mathbb{Q}\left(u, \sqrt{D}\right) \end{array}.$$

$K \subseteq E$ ($\Delta \in E$ לפי הגדרתה). נוכיח $E \subseteq K$. מספיק להראות ש$v, w \in K$.

$$g(x) = \frac{f(x)}{x - u} = (x - v)(x - w) \in K[x] \implies vw, v + w \in K[x]$$

$$g(u) = (u - v)(u - w)$$

$$\frac{\sqrt{D}}{g(u)} = \pm(v - w) \in K$$

$$\left\{ \begin{array}{l} v + w \\ v - w \end{array} \right. \implies v, w \in K$$

מסקנה

יהי $f(x) \in \mathbb{Q}[x]$ מדרגה 3, אי־פריק, E שדה הפיצול שלו.
$\sqrt{D} \in \mathbb{Q} \iff \mathrm{Gal}(E/\mathbb{Q}) = \mathbb{Z}_3$.

הוכחה

$\Leftarrow$

$$\sqrt{D}\in\mathbb{Q}\implies E=\mathbb{Q}\left(u\right)$$

$$\left[E:\mathbb{Q}\right]=3\implies\mathrm{Gal}\left(E/\mathbb{Q}\right)\cong\mathbb{Z}_{3}$$

$\Longrightarrow$

$$\left[\mathbb{Q}\left(u,\sqrt{D}\right):\mathbb{Q}\right]=3$$

$$\underbrace{\left[\mathbb{Q}\left(\sqrt{D}\right):\mathbb{Q}\right]}_{\text{divides }2}\mid\left[\mathbb{Q}\left(u,\sqrt{D}\right):\mathbb{Q}\right]$$

$$\implies\mathbb{Q}\left(\sqrt{D}\right)=\mathbb{Q}\implies\sqrt{D}\in\mathbb{Q}$$

$$\mathrm{Gal}\left(E\left(\mathbb{Q}\right)\right)\cong S_{3}\iff\sqrt{D}\notin\mathbb{Q}$$

$D<0\iff$ קיים שורש מרוכב $\Longleftarrow\mathrm{Gal}\left(E/\mathbb{Q}\right)\simeq S_{3}$.

משפט

הדיסקרימיננטה של $f\left(x\right)=x^{3}+qx+r$ היא $D=-4q^{3}-27r^{2}$.

הערה

$D=\mathrm{Res}\left(f,f'\right)$(כאשר הרזיטנטה היא $\mathrm{Res}\left(f,g\right)=\prod\left(r_{i}-s_{j}\right)$ כאשר r_{i},s_{j} הם שרשי f,g בהתאמה). יש משפט שאומר $\mathrm{Res}\left(f,g\right)=\det S\left(f,g\right)$($S$ היא מטריצת סילבסטר).

תרגיל

$f\left(x\right)=x^{3}-9x+9\in\mathbb{Q}\left[x\right]$. מצאו את חבורת גלואה.

פתרון

$f\left(x\right)$ אי־פריק(בדקו!). הדיסקרימיננטה היא $D=3^{6}$, $\sqrt{D}\in\mathbb{Q}\Longleftarrow\mathrm{Gal}\left(E/\mathbb{Q}\right)\simeq\mathbb{Z}_{3}$.

הערה

אם הפולינום $f\left(x\right)$ לא מהצורה $f\left(x\right)=x^{3}+qx+r$, אפשר להגיע לצורה הזו ע"י $\tilde{f}\left(x\right)=f\left(x-\frac{a}{5}\right)$ כאשר a הוא המקדם של x^{2}, ואז $\tilde{f}$ הוא מהצורה הרצויה. הדיסקרימיננטה וחבורת גלואה של $f,\tilde{f}$ זהות.

תרגיל

הוכיחו או הפריכו:
כל הרחבת גלואה עם חבורת גלואה פתירה היא הרחבה רדיקלית.

פתרון

נפריד ע"י דוגמה נגדית.
ניקח פולינום $f\left(x\right)\in\mathbb{Q}\left[x\right]$ מדרגה 3 עם חבורת גלואה $\mathbb{Z}_3$. E הוא שדה הפיצול.
נניח בשלילה שההרחבה ${}^{E}/_{\mathbb{Q}}$ רדיקלית $\Longleftarrow$ שרשית $\Longleftarrow$ $E=\mathbb{Q}\left(r\right)$, $r^n\in\mathbb{Q}$, r שורש של $g\left(x\right)=x^n-r^n$. $m_r\left(x\right)\in\mathbb{Q}\left[x\right]$ מחלק את $g\left(x\right)$. $m_r\left(x\right)$ מתפצל בE כי E הרחבת גלואה ו$r\in E$. $\deg m_r\left(x\right)=3$. E שדה ממשי. ל$g\left(x\right)$ יש לכל היותר 2 שורשים ממשיים, כי השורשים הם $r, r\rho_n^i$. r ממשי, ρ_n^i מקבל ערכים ממשיים רק אם $\rho_n^i=\rho_2=-1$ או $i=0$ - וזו סתירה, כי השורשים של $m_r\left(x\right)$ כולם ממשיים.

משפט

F שדה, $\operatorname{char} F=0$. אם יש הרחבה מדרגה p של F, וF מכיל שורש ρ_p, אזי ההרחבה היא שרשית.

פולינום מדרגה 4

$f\left(x\right)\in\mathbb{Q}\left[x\right]$ מדרגה 4, אי־פריק, E שדה הפיצול, $G=\operatorname{Gal}\left(E/\mathbb{Q}\right)$.
רוצים למצוא שדה ביניים

$$\begin{tikzcd} E \arrow[d, dash] \\ K \arrow[d, dash] \\ \mathbb{Q} \end{tikzcd}$$

כך שK שדה פיצול של פולינום מדרגה 3.
$K/\mathbb{Q}$ גלואה, צריך למצוא $H\lhd G$.

$$G\hookrightarrow S_4$$

$$V\lhd S_4$$

$$\Longrightarrow\ V\cap G\lhd G$$

(תזכורת: $V\cong\mathbb{Z}_2\times\mathbb{Z}_2$ חבורת קליין)
$V\lhd G$ היא מסדר שמחלק את 4.

$$k=\left|V\cap G\right|$$

$$K = E^{V \cap G}$$

$$[K : \mathbb{Q}] = [G : V \cap G] = [GV : V] \mid [S_4 : V] = 6$$

$$m = [G : V \cap G] \implies m \mid 6$$

$$|G| = m \cdot k$$

אם יודעים מהו m, כמעט תמיד יודעים מהו $|G|$.

הערה

$G \hookrightarrow S_4$. $|G| \mid 4$. G פועלת טרנזיטיבית על $\{1,2,3,4\}$

משפט

א. אם $m = 6$ אזי $G \cong S_4$

ב. אם $m = 3$ אזי $G \cong A_4$

ג. אם $m = 1$ אזי $G \cong V$

ד. אם $m = 2$ אזי $G \cong D_4$ או $G \cong \mathbb{Z}_4$

נראה א'

$m = 6$. $k = 1, 2, 4$.

$k \neq 1$ כי $6 \nmid 4$. $k \neq 2$ כי אז $|G| = 12 \Longrightarrow G \simeq A_4$, $V \subseteq A_4 \subseteq G$, $|V \cap G| = 4$ - וזו סתירה.

לכן $k = 4 \Longrightarrow |G| = 24 \Longrightarrow G \cong S_4$.

משפט

נסמן ב-$r_1, \ldots r_4$ את שרשי $f(x)$. אזי $K/\mathbb{Q}$ הוא שדה פיצול של הפולינום $g(x) = (x-u)(x-v)(x-w)$ כאשר

$$\begin{aligned} u &= (r_1 + r_2)(r_3 + r_4) \\ v &= (r_1 + r_3)(r_2 + r_4) \\ w &= (r_1 + r_4)(r_2 + r_3) \end{aligned}$$

לפולינום $g(x)$ קוראים הרזולנט הקובי של $f(x)$.

משפט

אם $f\left(x\right)=x^{4}+gx^{2}+rx+s$ אזי

$$g\left(x\right)=x^{3}-2qx^{2}+\left(q^{2}-4s\right)x-r^{2}$$

אם קיים ל-f מקדם a ל-x^{3}, אזי מגדירים

$$\tilde{f}\left(x\right)=f\left(x-\frac{a}{4}\right)$$

תרגיל

$f\left(x\right)=x^{4}-4x+2\in\mathbb{Q}\left[x\right]$. מצאו את חבורת גלואה.

פתרון

$f\left(x\right)$ אי־פריק.

$$g\left(x\right)=x^{3}-8x+16$$

g אי־פריק. $D\left(g\right)<0 \Longleftarrow$ חבורת גלואה של g היא $S_{3} \Longleftarrow \mathrm{Gal}\left(E/\mathbb{Q}\right)\cong S_{4}$.

תרגיל

$$f\left(x\right)=x^{4}-10x^{2}+1$$

$$\sqrt{2}+\sqrt{3}$$

$$\mathrm{Gal}\left(E/\mathbb{Q}\right)\simeq V$$

$$g\left(x\right)=x^{3}+20x^{2}+96x=x\left(x+8\right)\left(x+12\right)$$

$$\Longrightarrow\ m=1$$

$$\Longrightarrow\ \mathrm{Gal}\simeq V$$