נסתכל בשיעור הזה על הפולינום $f\left(x\right)=x^{3}-2\in\mathbb{Q}\left[x\right]$.

הערה

$x^{n}-a\in\mathbb{Q}\left[x\right]$, והשורשים שלו הם $\sqrt[n]{a}$. $f_{n}=\text{cis}\frac{2\pi}{n}$ הוא שורש היחידה הnי. נסמן:

$$\alpha_{k}=\sqrt[n]{\alpha}\cdot\rho_{n}^{k}\qquad0\leq k\leq n-1$$

α_{k} הם n השורשים של $g\left(x\right)$.(תזכורת: ρ_{n} הוא שורש היחידה הnי של 1.

חזרה לדוגמה

השורשים של $f\left(x\right)$ הם $\sqrt[3]{2},\sqrt[3]{2}\rho_{3},\sqrt[3]{2}\rho_{3}^{2}$. נסמן:

$$K=\mathbb{Q}\left(\sqrt[3]{2},\sqrt[3]{2}\rho_{3},\sqrt[3]{2}\rho_{3}^{2}\right)$$

K הוא <u>שדה הפיצול</u> של $f\left(x\right)$.

הגדרה

יהי $f\left(x\right)\in F\left[x\right]$. נניח שכל שורשי $f\left(x\right)$ נמצאים בE.
<u>שדה פיצול</u> של $f\left(x\right)$ הוא השדה הקטן ביותר המוכל בE בו נמצאים השורשים.

טענה

יהי $\overbrace{f\left(x\right)}^{\in F\left[x\right]}=\left(x-\alpha_{1}\right)\cdots\left(x-\alpha_{2}\right)$ מעל E. אז שדה הפיצול של f הוא $F\left(\alpha_{1},\ldots\alpha_{n}\right)$.

טענה 1

יהי $f\left(x\right)\in F\left[x\right]$ פולינום אי פריק מעל F, α,β שורשים של f. אזי $F\left(\alpha\right)\cong F\left(\beta\right)$.

הוכחה

$$F\left(\alpha\right)\cong{}^{F\left[x\right]}/_{\left\langle m_{\alpha}\left(x\right)\right\rangle}={}^{F\left[x\right]}/_{\left\langle m_{\beta}\left(x\right)\right\rangle}\cong F\left(\beta\right)$$

טענה 2

יהי $K\subseteq F$, ונניח ש$K\underset{\sigma}{\cong}F\left(\alpha\right)$[1] כך ש$\sigma\left(a\right)=a$ לכל $a\in F$. נסמן $\beta=\sigma\left(\alpha\right)$. אזי β שורש של $m_{\alpha}\left(x\right)$(הפולינום המינימלי של α).

[1]משמעות הסימון $\underset{\sigma}{\cong}$ הוא איזומורפיות כאשר σ הוא האיזומורפיזם

הוכחה

$$m_\alpha\left(x\right)=x^n+a_{n-1}x^{n-1}+\cdots+\alpha_0$$

$$m_\alpha\left(\beta\right)=\beta^n+\alpha_{n-1}\beta^{n-1}+\cdots+\alpha_0=$$

$$=\sigma\left(\alpha\right)^n+\alpha_{n-1}\sigma\left(\alpha\right)^{n-1}+\cdots+\alpha_0=$$

$$=\sigma\left(\alpha\right)^n+\sigma\left(\alpha_{n-1}\right)\sigma\left(\alpha\right)^{n-1}+\cdots+\sigma\left(\alpha_0\right)=$$

$$=\sigma\left(\alpha^n+\alpha_{n-1}\alpha^{n-1}+\cdots+\alpha_0\right)=\sigma\left(0\right)=0$$

הגדרה

חבורת גלואה של ההרחבה ${}^{K}/_{F}$ היא

$$\mathrm{Gal}\left({}^{K}/_{F}\right)=\left\{\sigma\in\mathrm{Aut}\left(K\right)|\forall_{a\in F}\sigma\left(a\right)=a\right\}$$

($\mathrm{Aut}\left(K\right)$ היא חבורת האוטומורפיזמים של K)

הערה 3

אם $\sigma\in\mathrm{Gal}\left({}^{K}/_{F}\right)$ אז בצורה דומה להוכחת טענה 2, ניתן להוכיח שאם a שורש של פולינום $f\left(x\right)\in F\left[x\right]$ אזי $\sigma\left(a\right)$ שורש של $f\left(x\right)$.

חזרה לדוגמה

$$\begin{tikzcd}
\mathbb{Q}\left(\sqrt[3]{2}\right) \arrow[r, "\sigma_1"] \arrow[dr, no head] & \mathbb{Q}\left(\sqrt[3]{2}\rho_3\right) \arrow[r, "\sigma_2"] \arrow[d, no head] & \mathbb{Q}\left(\sqrt[3]{s}\rho_3^2\right) \arrow[dl, no head] \\
 & \mathbb{Q} &
\end{tikzcd}$$

משפט 4

אוטומורפיזם ב$\mathrm{Gal}\left({}^{K}/_{F}\right)$ כאשר $K=F\left(\alpha_1,\ldots\alpha_n\right)$ נקבע ע"י התמונות של $\alpha_1,\ldots\alpha_n$.

משפט 5

אם $a,b\in F\left(a\right)$ הם שורשים של פולינומס אי פריק $f\left(x\right)\in F\left[x\right]$ אזי קיים אוטומורפיזם $\sigma\in\mathrm{Gal}\left({}^{F(a)}/_{F}\right)$ כך ש$\sigma\left(a\right)=b$.

משפט 6

אם $K = F(\alpha_1,\dots\alpha_n)$ כאשר $\alpha_1,\dots\alpha_n$ הם השורשים של פולינום $f(x)\in F[x]$, אזי $\mathrm{Gal}\left({}^{K}/_{F}\right) \le S_n$.

נחזור לדוגמה

$$f(X)=x^3-2$$

שאלה: מהי $\mathrm{Gal}\left({}^{\mathbb{Q}(\sqrt[3]{2})}/_{\mathbb{Q}}\right)=?$

נראה ש$\mathrm{Gal}\left({}^{\mathbb{Q}(\sqrt[3]{2})}/_{\mathbb{Q}}\right)=\{Id\}$: אם $\sigma\in G$ אזי $\beta=\sigma\left(\sqrt[3]{2}\right)$ מקיים $f(\beta)=0$, לכן $\beta\in\left\{\sqrt[3]{2},\sqrt[3]{2}\rho_3,\sqrt[3]{2}\rho_3^2\right\}$. $\sqrt[3]{2}\rho_3,\sqrt[3]{2}\rho_3^2\in\mathbb{C}\setminus\mathbb{R}$, אבל $\mathbb{Q}\left(\sqrt[3]{2}\right)\subseteq\mathbb{R}$, לכן $\beta=\sqrt[3]{2}$.

$\{Id\}=\mathrm{Gal}\left({}^{\mathbb{Q}(\sqrt[3]{2}\rho_3)}/_{\mathbb{Q}}\right)=?$

כיוון שהשדות $\mathbb{Q}\left(\sqrt[3]{2}\rho_3\right)\cong\mathbb{Q}\left(\sqrt[3]{2}\right)$, גם חבורות הגלואה הן איזומורפיות.

הפולינום המינימלי של ρ_3 מעל $\mathbb{Q}$ הוא

$$\Phi_3=\frac{x^3-1}{x-1}=x^2+x+1$$

ו($2=[\mathbb{Q}(\rho_3):\mathbb{Q}],3=\left[\mathbb{Q}\left(\sqrt[3]{2}\right):\mathbb{Q}\right]$)

ולכן Φ_3 נשאר אי־פריק מעל $\mathbb{Q}\left(\sqrt[3]{2}\right)$(ראינו בתרגיל הקודם), לכן $2=\left[\mathbb{Q}\left(\sqrt[3]{2}\right)(\rho_3):\mathbb{Q}\left(\sqrt[3]{2}\right)\right]$.

$$[E:\mathbb{Q}]=6$$

$$\mathrm{Gal}\left({}^{E}/_{\mathbb{Q}}\right)\subseteq S_3$$

כי E הוא שדה פיצול של פולינום מדרגה 3. נרצה להוכיח שוויון:

$$\mathrm{Gal}\left({}^{E}/_{\mathbb{Q}}\right)=S_3$$

בלי להשתמש במשפטים נוספים.

$$\begin{array}{rc}
 & \mathbb{Q}\left(\sqrt[3]{2}\right)(\rho_3) \\
\text{Adding a root of irreducible polynimail } \Phi_3 & \Big| \\
 & \mathbb{Q}\left(\sqrt[3]{2}\right) \\
 & \Big| \\
 & \mathbb{Q}
\end{array}$$

$\rho_3,\rho_3^2\in E$ הם השורשים של Φ_3. אזי קיים אוטומורפיזם $S_2\simeq\mathrm{Gal}\left({}^{E}/_{\mathbb{Q}(\sqrt[3]{2})}\right)\ni\sigma$. $\sigma(\rho_3)=\rho_3^2$. σ מחליף בין השורשים.

[לכל הרחבה ריבועית לא טריוויאלית מתקיים $\mathrm{Gal}\left({}^{K}/{}_{F}\right) \simeq S_2$]
נטען:

$$r \in \mathrm{Gal}\left({}^{E}/{}_{\mathbb{Q}}\right) \geq \mathrm{Gal}\left({}^{E}/{}_{\mathbb{Q}(\sqrt[3]{2})}\right)$$

כי σ קובע את אברי $\mathbb{Q}$

$$\sigma = \begin{pmatrix} \sqrt[3]{2} & \sqrt[3]{2}\rho_3 & \sqrt[3]{2}\rho_3^2 \\ \sqrt[3]{2} & \sqrt[3]{2}\rho_3^2 & \sqrt[3]{2}\rho_3^4 = \sqrt[3]{2}\rho_3 \end{pmatrix}$$

נוכיח את זה:

$$\mathrm{Gal}\left({}^{E}/{}_{\mathbb{Q}(\sqrt[3]{2})}\right) \simeq \mathrm{Gal}\left({}^{E}/{}_{\mathbb{Q}(\sqrt[3]{2}\rho_3)}\right)$$

בשמאלי σ קובע את $\sqrt[3]{2}$ ובימני σ' קובע את $\sqrt[3]{2}\rho_3$ - כלומר $\sigma \neq \sigma'$.
לכן יש שני איברים מסדר 2 בG. שני איברים מסדר 2 יוצרים את S_3 - לכן $G = S_3$.

"לרשום במפורש אוטומורפיזם"

מוצאים בסיס של ${}^{E}/{}_{F}$. בדוגמה בסיס של ${}^{E}/{}_{\mathbb{Q}}$: $B = \left\{1, \sqrt[3]{2}, \sqrt[3]{2}^2, \rho_3, \rho_3\sqrt[3]{2}, \rho_3\sqrt[3]{2}^2\right\}$

$$\begin{array}{c} E = K(\rho_3) \\ \Big| \; {\scriptstyle 1, \rho_3} \\ K = \mathbb{Q}\left(\sqrt[3]{2}\right) \\ \Big| \; {\scriptstyle 1, \sqrt[3]{2}, \left(\sqrt[3]{2}\right)^2 = \sqrt[3]{4}} \\ \mathbb{Q} \end{array}$$

$\rho_3^2 = 1 - \rho_3$ בגלל ש$\Phi_3(\rho_3) = 0$.