Computation for the Galois group of a polynomial

mardi 25 février 2020 23:42

Problem. Evaluate the Galois group of
$$f(x) = x^4 - 2$$
over $\mathbb{Q}$; then find its subgroups and their fixed subfields in the splitting field of $f(x)$ over $\mathbb{Q}$.

Solution. Step 1. Consider the splitting field
$$E := \mathbb{Q}(f(x))$$
of the polynomial $f(x)$ over $\mathbb{Q}$.

By solving the equation
$$f(x) = 0,$$
we have
$$E = \mathbb{Q}[2^{1/4}, \sqrt{-1}].$$

Step 2. The two subfields
$$\mathbb{Q}[2^{1/4}] \text{ and } \mathbb{Q}[\sqrt{-1}]$$
are linearly disjoint over $\mathbb{Q}$.

So, the tensor product
$$\mathbb{Q}[2^{1/4}] \otimes_{\mathbb{Q}} \mathbb{Q}[\sqrt{-1}] \cong E$$
are isomorphic $\mathbb{Q}$-algebras.

Step 3. For the Galois groups, we have
$$\mathrm{Gal}(E|\mathbb{Q}[\sqrt{-1}]) \cong (\mathbb{Z}/4\mathbb{Z};+), \text{ or } \cong (\mathbb{Z}/2\mathbb{Z};+) \times (\mathbb{Z}/2\mathbb{Z};+);$$
$$\mathrm{Gal}(\mathbb{Q}[\sqrt{-1}]|\mathbb{Q}) \cong (\mathbb{Z}/2\mathbb{Z};+).$$

From Step 2, there is a group isomorphism
$$\mathrm{Gal}(E|\mathbb{Q}) \cong \mathrm{Gal}(\mathbb{Q}[\sqrt{-1}]|\mathbb{Q}) \times \mathrm{Gal}(E|\mathbb{Q}[\sqrt{-1}]).$$

In particular, $E/\mathbb{Q}$ is a Galois extension;
$$\mathrm{Gal}(E|\mathbb{Q})$$
is an abelian group.

Step 4. All the subgroups of $\mathrm{Gal}(E|\mathbb{Q})$ are:

i) of the (1+1)-form
$$\Gamma \times H$$
where
$$\Gamma = \{[0]\} \text{ or } (\mathbb{Z}/2\mathbb{Z};+);$$
$$H = \{[0]\}, \{[0],[2]\}, \text{ or } (\mathbb{Z}/4\mathbb{Z};+);$$

ii) of the (1+1+1)-form
$$\Gamma \times H_1 \times H_2$$

where

$\Gamma,\ H_2 = \{[0]\}$ or $(\mathbb{Z}/2\mathbb{Z};+)$;

$H_1 = \{[0]\}$.

$H_1 \neq (\mathbb{Z}/2\mathbb{Z};+)$ $\longleftarrow$ subextensions are not linearly disjoint.

Step 5 i) Find the $(\Gamma \times H)$-invariant subfields in $E/\mathbb{Q}$.

In fact, put

$(\mathbb{Z}/2\mathbb{Z};+) = \langle \tau \rangle$;

$(\mathbb{Z}/4\mathbb{Z};+) = \langle \sigma \rangle$;

$\omega = 2^{1/4}$.

For $\underbrace{(\mathbb{Z}/2\mathbb{Z};+)}_{=C_2}$, we have

$\tau : \sqrt{-1} \longmapsto -\sqrt{-1}$;

$\tau|_{\mathbb{Q}[\omega]} = id_{\mathbb{Q}[\omega]}$, i.e., $\tau \in Gal(E|\mathbb{Q}[\omega])$.

For $\underbrace{(\mathbb{Z}/4\mathbb{Z};+)}_{=C_4}$, we have

$$\begin{pmatrix}\omega\\ \omega^2\\ \omega^3\\ \omega^4\end{pmatrix} \xrightarrow{\sigma} \begin{pmatrix}\omega^2\\ \omega^3\\ \omega^4\\ \omega\end{pmatrix} \xrightarrow{\sigma} \begin{pmatrix}\omega^3\\ \omega^4\\ \omega\\ \omega^2\end{pmatrix} \xrightarrow{\sigma} \begin{pmatrix}\omega^4\\ \omega\\ \omega^2\\ \omega^3\end{pmatrix};$$

$$\updownarrow \qquad\qquad \updownarrow \qquad\qquad \updownarrow \qquad\qquad \updownarrow$$

$$\begin{pmatrix}1\\ 2\\ 3\\ 4\end{pmatrix} \longrightarrow \begin{pmatrix}2\\ 3\\ 4\\ 1\end{pmatrix} \longrightarrow \begin{pmatrix}3\\ 4\\ 1\\ 2\end{pmatrix} \longrightarrow \begin{pmatrix}4\\ 1\\ 2\\ 3\end{pmatrix}.$$

$\sigma|_{\mathbb{Q}[\sqrt{-1}]} = id_{\mathbb{Q}[\sqrt{-1}]}$, i.e., $\sigma \in Gal(E|\mathbb{Q}[\sqrt{-1}])$.

ii) Find the $(\Gamma \times \{1\} \times H_2)$-invariant subfields.

$$\begin{array}{c} E \\ | \\ \mathbb{Q}[\sqrt{-1}][\omega^2] \\ | \\ \mathbb{Q}[\sqrt{-1}] \\ | \\ \mathbb{Q} \end{array}$$

$\Gamma,\ H_2 = \{1\},\ \mathbb{Z}/2\mathbb{Z}$.

$\mathbb{Z}/2\mathbb{Z} = \langle \delta \rangle$.

$\delta : \omega \longmapsto -\omega$.

$\Downarrow$

$E^{\langle \delta \rangle} = \mathbb{Q}[\sqrt{-1}][\omega^2]$.

Hence, we have

$\boxed{\omega = 2^{1/4}.}$

	$\Gamma \times H$	invariant subfields under $\Gamma \times H$
①	$\langle 1 \rangle \times \langle 1 \rangle$	$E = \mathbb{Q}[\omega, \sqrt{-1}]$
②	$\langle 1 \rangle \times \langle \sigma^2 \rangle$	$\{c_1\cdot(\omega+\omega^3) + c_2\cdot(1+\omega^2) \in E \mid c_1, c_2 \in \mathbb{Q}[\sqrt{-1}]\}$
③	$\langle 1 \rangle \times \langle \sigma \rangle$	$\mathbb{Q}[\sqrt{-1}]$
④	$\langle \tau \rangle \times \langle 1 \rangle$	$\mathbb{Q}[\omega]$
⑤	$\langle \tau \rangle \times \langle \sigma^2 \rangle$	$\{c_1\cdot(\omega+\omega^3) + c_2\cdot(1+\omega^2) \in E \mid c_1, c_2 \in \mathbb{Q}\}$
⑥	$\langle \tau \rangle \times \langle \sigma \rangle$	$\mathbb{Q}$
⑦	$\langle 1 \rangle \times \langle 1 \rangle \times \langle \delta \rangle$	$\{c_1 + c_2\omega^2 \in E \mid c_1, c_2 \in \mathbb{Q}[\sqrt{-1}]\}$
⑧	$\langle \tau \rangle \times \langle 1 \rangle \times \langle \delta \rangle$	$\{c_1 + c_2\omega^2 \in E \mid c_1, c_2 \in \mathbb{Q}\}$

Step 6 How to obtain the $\langle \sigma^2 \rangle$-invariant subfields.

Consider $\sigma \in Gal(E/\mathbb{Q}[\sqrt{-1}])$.

Fixed $\forall x \in E^{\langle \sigma^2 \rangle}$, we have

$$x = c_1\omega + c_2\omega^2 + c_3\omega^3 + c_4\omega^4$$

with $c_1, c_2, c_3, c_4 \in \mathbb{Q}[\sqrt{-1}]$.

On the other hand, from Step 5 there is

$$\sigma^2(x) = c_1\cdot\omega^3 + c_2\omega^4 + c_3\omega + c_4\omega^2 .$$

As $x = \sigma^2(x)$, we have

$$c_1\cdot\omega^3 + c_2\omega^4 + c_3\omega + c_4\omega^2 = c_1\omega + c_2\omega^2 + c_3\omega^3 + c_4\omega^4;$$

$$(c_1 - c_3)\omega + (c_2 - c_4)\omega^2 + (c_3 - c_1)\cdot\omega^3 + (c_4 - c_2)\cdot\omega^4 = 0;$$

then

$$\begin{cases} c_1 = c_3 \\ c_2 = c_4 \end{cases}$$

since $\omega, \omega^2, \omega^3, \omega^4 = 1$ are linearly independent over $\mathbb{Q}[\sqrt{-1}]$.

This proves

$$x = c_1(\omega + \omega^3) + c_2(\omega^2 + \omega^4)$$

with $c_1, c_2 \in \mathbb{Q}[\sqrt{-1}]$.

Hence,

$$E^{\langle\sigma^2\rangle} = \left\{ c_1(\omega + \omega^3) + c_2(1 + \omega^2) \in E \;\middle|\; c_1, c_2 \in \mathbb{Q}[\sqrt{-1}] \right\}.$$