An example of a Galois group

Problem. Let $f(\lambda) = \lambda^4 - 2 \in \mathbb{Q}[\lambda]$. Let $E$ be the splitting field of $f(\lambda)$ over $\mathbb{Q}$ and let $G = \text{Gal}(E/\mathbb{Q})$.

(a) Find $E$ and $[E : \mathbb{Q}]$.
(b) Find $G$ as a group of permutations of the roots of $f(\lambda)$.

Solution.

(a) Let $r = \sqrt[4]{2}$. The roots of $f(\lambda)$ in $\mathbb{C}$ are $r, zr, z^2r$ and $z^3r$ where

$$z = e^{\frac{2\pi i}{4}} = \cos\left(\frac{2\pi}{4}\right) + i\sin\left(\frac{2\pi}{4}\right) = \cos\left(\frac{\pi}{2}\right) + i\sin\left(\frac{\pi}{2}\right) = 0 + 1i = i.$$ 

Thus, the roots of $f(\lambda)$ in $\mathbb{C}$ are:

$$r, ir, -r, -ir. \quad (1)$$

So

$$E = \mathbb{Q}(r, ir, -r, -ir) = \mathbb{Q}(r, i).$$

Next $r$ has degree 4 over $\mathbb{Q}$ (its minimum polynomial over $\mathbb{Q}$ is $\lambda^4 - 2$ which is irreducible over $\mathbb{Q}$ by Eisenstein’s criterion with $p = 2$). Also, $i$ has degree 2 over $\mathbb{Q}$ (its minimum polynomial over $\mathbb{Q}$ is $\lambda^2 + 1$). Hence, since $E = \mathbb{Q}(r, i)$, it follows (as proved in class) that

$$[E : \mathbb{Q}] \leq 2 \cdot 4 = 8.$$ 

Also we have

$$E \quad \begin{array}{l}
\text{/} \\ \text{
} \\
\mathbb{Q}(r) \quad \mathbb{Q}(i) \\
\text{4\textbackslash} \text{/2} \\
\mathbb{Q} \end{array} \quad (2)$$

Thus by multiplicativity of degree, we have $4 \mid [E : \mathbb{Q}]$. Hence, $[E : \mathbb{Q}] = 4$ or 8.

Now suppose for contradiction that $[E : \mathbb{Q}] = 4$. Then, from (2), it follows that $E = \mathbb{Q}(r)$. But $i \in E$ and so $i \in \mathbb{Q}(r)$. Since $\mathbb{Q}(r)$ consists entirely of real numbers it follows that $i$ is a real number (a contradiction). So $[E : \mathbb{Q}] = 8$.

(b) Now since the roots of $f(\lambda)$ are distinct, we know that

$$|G| = |\text{Gal}(E/\mathbb{Q})| = [E : \mathbb{Q}] = 8.$$ 

To describe the elements of $G$, we label the roots of $f(\lambda)$ in $E$ as:

$$r_1 = r, \quad r_2 = ir, \quad r_3 = -r, \quad r_4 = -ir.$$
Then, as we've seen in class we can (and do) identify $G$ as a subgroup of $S_4$. So $G$ is a subgroup of $S_4$ of order 8.

Since $[E : \mathbb{Q}] = 8$ it follows from (2) and multiplicativity of degree that we have

$$
\begin{array}{c}
\text{E} \\
2/ \setminus 4 \\
K_1 \setminus K_2 \\
4/ \setminus 2 \\
\mathbb{Q}
\end{array}
$$

(3)

where $K_1 = \mathbb{Q}(r)$ and $K_2 = \mathbb{Q}(i)$.

Let

$$
G_1 = \text{Gal}(E/K_1) \quad \text{and} \quad G_2 = \text{Gal}(E/K_2).
$$

Then, $G_1$ and $G_2$ are subgroups of $G$ and, by (3), we have

$$
|G_1| = [E : K_1] = 2 \quad \text{and} \quad |G_2| = [E : K_2] = 4.
$$

Also, by problem #1 on assignment #7, we have

$$
G = G_1 G_2.
$$

So it remains to compute $G_1$ and $G_2$. This we can easily do since $E/K_1$ and $E/K_2$ are simple extensions.

$G_1$: Now $E = K_1(i)$. Moreover, $i$ is a root of $\lambda^2 + 1 \in K_1[\lambda]$. Hence, since $[E : K_1] = 2$, it follows that $\lambda^2 + 1$ is the minimum polynomial of $i$ over $K_1$. So since $i$ and $-i$ are roots of $\lambda^2 + 1$ in $E$ it follows from the extension theorem for simple extensions that there exists $\tau \in G_1$ so that $\tau(i) = -i$. Of course, since $\tau \in G_1 = \text{Gal}(E/K_1)$, we have $\tau(r) = r$. Thus, since $E = \mathbb{Q}(r,i)$, we may describe $\tau$ as:

$$
\tau : \quad i \mapsto -i.
$$

So

$$
\tau(r_1) = \tau(r) = r = r_1 \\
\tau(r_2) = \tau(ir) = \tau(i)\tau(r) = (-i)r = -ir = r_4 \\
\tau(r_3) = \tau(-r) = -\tau(r) = -r = r_3 \\
\tau(r_4) = \tau(-ir) = -\tau(i)\tau(r) = -(-i)r = ir = r_2.
$$

Hence, $\tau = (24)$ as a permutation of the roots of $f(\lambda)$. But $\tau \in G_1$ and $G_1$ has order 2. So

$$
G_1 = \langle \tau \rangle = \{\varepsilon, r\}.
$$
$G_2$: Now $E = K_2(r)$. Moreover, $r$ is a root of $\lambda^4 - 2 \in K_2[\lambda]$. Hence, since $[E : K_2] = 4$, it follows that $\lambda^4 - 2$ is the minimum polynomial of $r$ over $K_2$. So since $r$ and $ir$ are roots of $\lambda^4 - 2$ in $E$ it follows from the extension theorem for simple extensions that there exists $\sigma \in G_2$ so that $\sigma(r) = ir$. Of course, since $\sigma \in G_2 = \text{Gal}(E/K_2)$, we have $\sigma(i) = i$. Thus, since $E = \mathbb{Q}(r, i)$, we may describe $\sigma$ as:

$$
\sigma : r \mapsto ir \\
i \mapsto i.
$$

So

$$
\sigma(r_1) = \sigma(r) = ir = r_2 \\
\sigma(r_2) = \sigma(ir) = \sigma(i)\sigma(r) = i(ir) = -r = r_3 \\
\sigma(r_3) = \sigma(-r) = -\sigma(r) = -ir = r_4 \\
\sigma(r_4) = \sigma(-ir) = -\sigma(i)\sigma(r) = -i(ir) = r = r_1.
$$

Hence, $\sigma = (1234)$ as a permutation of the roots of $f(\lambda)$. But $\sigma \in G_2$ and $G_2$ has order 4. So

$$
G_2 = \langle \sigma \rangle = \{\varepsilon, \sigma, \sigma^2, \sigma^3\}.
$$

Finally,

$$
G = G_1G_2 = \{\tau^j\sigma^k \mid 0 \leq j \leq 1, \ 0 \leq k \leq 3\} \\
= \{\varepsilon, \sigma, \sigma^2, \sigma^3, \tau, \tau\sigma, \tau\sigma^2, \tau\sigma^3\},
$$

where $\tau = (24)$ and $\sigma = (1234)$. \hfill \Box

Remark. The group $G$ just calculated is the dihedral group $D_8$ consisting of all symmetries of the square:

$$
\begin{array}{cccc}
4 & -1 \\
\mid & \mid \\
3 & -2
\end{array}
$$

($\sigma$ is clockwise rotation by 90 degrees and $\tau$ is reflection in the diagonal line containing 1 and 3.) In $G$ one has the relations $\sigma^4 = \varepsilon$, $\tau^2 = \varepsilon$ and $\tau\sigma\tau^{-1} = \sigma^3$. 
