Galois Group of $x^8 - 2$ over $\mathbb{Q}$

Summary

- **a. Verdict:** The degree of the extension is $[K : \mathbb{Q}] = 16$. The Galois group $\mathrm{Gal}(K/\mathbb{Q})$ is the quasidihedral group of order 16 (QD_{16}), generated by two automorphisms σ and τ with actions on the roots $\alpha_k = \sqrt[8]{2}e^{ik\pi/4}$ given by $k \mapsto 5k + 1 \pmod 8$ and $k \mapsto -k \pmod 8$, respectively.
- **b. Method Sketch:**
  1. Identify the roots of $x^8 - 2$ as $\alpha_k = \theta\zeta^k$ with $\theta = \sqrt[8]{2}$ and $\zeta = e^{i\pi/4}$. Show that the splitting field is $K = \mathbb{Q}(\theta, i)$.
  2. Calculate the degree $[K : \mathbb{Q}] = 16$ via the tower $\mathbb{Q} \subset \mathbb{Q}(\theta) \subset K$, using Eisenstein's criterion and the fact that $i \notin \mathbb{R}$.
  3. Define automorphisms σ and τ by $\sigma(\theta) = \theta\zeta$, $\sigma(i) = i$ and $\tau(\theta) = \theta$, $\tau(i) = -i$. Justify that σ is well-defined by proving $x^8 - 2$ is irreducible over $\mathbb{Q}(i)$. Show that $\langle \sigma, \tau \rangle$ generates the full group of order 16.
  4. Derive the explicit permutation action on the roots, noting the key relation $\sigma(\zeta) = \zeta^5$ to obtain the index maps.

Detailed Solution

Part 1: The Splitting Field and Degree of Extension

Let $f(x) = x^8 - 2$. The roots of $f(x)$ in $\mathbb{C}$ are:

$$\alpha_k = \sqrt[8]{2}e^{\frac{2\pi ik}{8}} = \sqrt[8]{2}e^{\frac{\pi ik}{4}}, \quad k = 0, 1, \ldots, 7.$$

Let $\theta = \sqrt[8]{2}$ be the unique positive real root, and let $\zeta = e^{\frac{\pi i}{4}}$. Then $\alpha_k = \theta\zeta^k$. The splitting field is $K = \mathbb{Q}(\alpha_0, \ldots, \alpha_7) = \mathbb{Q}(\theta, \zeta)$.

We determine the relationship between the generators θ, ζ and the field $\mathbb{Q}(\theta, i)$. Note that

$$\zeta = \cos\left(\frac{\pi}{4}\right) + i\sin\left(\frac{\pi}{4}\right) = \frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2} = \frac{1+i}{\sqrt{2}}.$$

Since $\theta^8 = 2$, we have $\theta^4 = \sqrt{2}$. Substituting,

$$\zeta = \frac{1+i}{\theta^4}.$$

This shows $\zeta \in \mathbb{Q}(\theta, i)$. Conversely, since $i = \zeta^2$, we have $i \in \mathbb{Q}(\zeta) \subset \mathbb{Q}(\theta, \zeta)$. Thus,

$$K = \mathbb{Q}(\theta, i).$$

To compute $[K : \mathbb{Q}]$, consider the tower $\mathbb{Q} \subset \mathbb{Q}(\theta) \subset K$.

1. **Step 1:** $[\mathbb{Q}(\theta) : \mathbb{Q}]$. The polynomial $x^8 - 2$ is irreducible over $\mathbb{Q}$ by Eisenstein's criterion with $p = 2$ ($2 \mid -2$, $2 \nmid 1$, $2^2 \nmid -2$). Since θ is a root, $[\mathbb{Q}(\theta) : \mathbb{Q}] = 8$.

2. **Step 2:** $[K : \mathbb{Q}(\theta)]$. We have $K = \mathbb{Q}(\theta)(i)$. The element i satisfies $x^2 + 1$. Since $\mathbb{Q}(\theta) \subset \mathbb{R}$ and $i \notin \mathbb{R}$, $i \notin \mathbb{Q}(\theta)$. Hence $x^2 + 1$ is irreducible over $\mathbb{Q}(\theta)$, so $[K : \mathbb{Q}(\theta)] = 2$.

By multiplicativity,

$$[K : \mathbb{Q}] = [K : \mathbb{Q}(\theta)] \cdot [\mathbb{Q}(\theta) : \mathbb{Q}] = 2 \cdot 8 = 16.$$

Part 2: Generators of the Galois Group

Let $G = \mathrm{Gal}(K/\mathbb{Q})$. Since K is the splitting field of a separable polynomial, $|G| = [K : \mathbb{Q}] = 16$. Define automorphisms $\sigma, \tau \in G$ by their actions on θ and i.

1. **The automorphism σ:** Define

$$\sigma(\theta) = \theta\zeta, \quad \sigma(i) = i.$$

Justification: Consider $F = \mathbb{Q}(i)$. Then $[F : \mathbb{Q}] = 2$ and $[K : F] = 8$. The element θ is a root of $x^8 - 2$ and $K = F(\theta)$. Since $[F(\theta) : F] = 8$, the minimal polynomial of θ over F is $x^8 - 2$, hence irreducible over $\mathbb{Q}(i)$. The Galois group $\mathrm{Gal}(K/\mathbb{Q}(i))$ acts transitively on the roots of $x^8 - 2$, so there exists $\sigma \in \mathrm{Gal}(K/\mathbb{Q}(i))$ sending θ to $\theta\zeta$. Since σ fixes $\mathbb{Q}(i)$, $\sigma(i) = i$.

Action on ζ: Using $\zeta = (1 + i)/\theta^4$,

$$\sigma(\zeta) = \frac{1 + \sigma(i)}{\sigma(\theta)^4} = \frac{1 + i}{(\theta\zeta)^4} = \frac{1 + i}{\theta^4\zeta^4}.$$

Since $\zeta^4 = e^{i\pi} = -1$,

$$\sigma(\zeta) = \frac{1 + i}{-\theta^4} = -\zeta = \zeta^5.$$

2. **The automorphism τ:** Define

$$\tau(\theta) = \theta, \quad \tau(i) = -i.$$

This is complex conjugation restricted to K, an automorphism since K is normal.

Action on ζ:

$$\tau(\zeta) = \frac{1 - i}{\theta^4} = \zeta^{-1} = \zeta^7.$$

Generation of G: We determine orders. For σ, compute its action on a root $\alpha_k = \theta\zeta^k$:

$$\sigma(\alpha_k) = \theta\zeta^{5k+1}.$$

Then

$$\sigma^2(\alpha_k) = \theta\zeta^{5(5k+1)+1} = \theta\zeta^{25k+6} = \theta\zeta^{k+6},$$
$$\sigma^4(\alpha_k) = \theta\zeta^{(k+6)+6} = \theta\zeta^{k+12} = \theta\zeta^{k+4} = -\alpha_k,$$
$$\sigma^8(\alpha_k) = \theta\zeta^{k+4+4} = \theta\zeta^{k+8} = \alpha_k.$$

Thus $\sigma^4 \neq \mathrm{id}$ but $\sigma^8 = \mathrm{id}$, so σ has order 8. Since $\tau(i) = -i \neq i$, $\tau \notin \langle\sigma\rangle$. The subgroup $\langle\sigma, \tau\rangle$ has order divisible by 8 and greater than 8, hence $|\langle\sigma, \tau\rangle| = 16 = |G|$. Therefore,

$$G = \langle\sigma, \tau\rangle.$$

Part 3: Action on the Roots

We describe the action of the generators on the set $R = \{\alpha_k = \theta\zeta^k \mid k = 0, \ldots, 7\}$.

- **Action of σ:**

$$\sigma(\alpha_k) = \sigma(\theta\zeta^k) = \sigma(\theta)\sigma(\zeta)^k = (\theta\zeta)(\zeta^5)^k = \theta\zeta^{5k+1}.$$

  On indices modulo 8: $k \mapsto 5k + 1$. In cycle notation, this is (0 1 6 7 4 5 2 3).

- **Action of τ:**

$$\tau(\alpha_k) = \tau(\theta\zeta^k) = \tau(\theta)\tau(\zeta)^k = \theta(\zeta^7)^k = \theta\zeta^{7k} = \theta\zeta^{-k}.$$

  On indices modulo 8: $k \mapsto -k$. In cycle notation, (1 7)(2 6)(3 5)(0)(4).

Final Answer

The degree of the extension is $[K : \mathbb{Q}] = 16$. A set of generators for $\mathrm{Gal}(K/\mathbb{Q})$ is $\{\sigma, \tau\}$, defined by:

$$\begin{aligned} \sigma(\theta) &= \theta\zeta, \quad \sigma(i) = i, \\ \tau(\theta) &= \theta, \quad \tau(i) = -i. \end{aligned}$$

Their operations on the roots $\alpha_k = \theta\zeta^k$ correspond to the index permutations $k \mapsto 5k+1 \pmod 8$ and $k \mapsto -k \pmod 8$, respectively.