Now we show (4). Let $\sigma \in G(\mathbb{Q}(\omega)/\mathbb{Q})$. Since

$$0 = \sigma(\Phi_n(\omega)) = \Phi_n(\sigma(\omega)),$$

we have that $\sigma(\omega)$ is also a primitive n-th root of unity. Hence $\sigma(\omega) = \omega^k$ with $1 \le k \le n$, $\gcd(k,n)=1$. Since $\{1, \omega, \dots, \omega^{\varphi(n)-1}\}$ is a $\mathbb{Q}$-basis of $\mathbb{Q}(\omega)$, σ is defined by $\sigma(\omega)$. We have

$$\mathbb{Z}_n^\times = \{ k \in \mathbb{Z}_n \mid 1 \le k \le n, \gcd(k,n) = 1 \},$$

and so the map

$$\begin{aligned} F: \mathbb{Z}_n^\times &\longrightarrow G(\mathbb{Q}(\omega)/\mathbb{Q}) \\ k &\longmapsto \sigma_k : \sigma_k(\omega) = \omega^k \end{aligned}$$

is well-defined. It is clearly injective, and since both sets have $\varphi(n)$ elements, F is bijective. To see that F is a group homomorphism, let $k_1, k_2 \in \mathbb{Z}_n^\times$. Write $k_1 k_2 = n \cdot q + r$ with $0 \le r \le n-1$. Then $k_1 k_2 = r$ in $\mathbb{Z}_n^\times$ and so $\sigma_r = \sigma_{k_1 k_2}$. We have

$$\sigma_{k_1} \circ \sigma_{k_2}(\omega) = \sigma_{k_1}(\omega^{k_2}) = (\sigma_{k_1}(\omega))^{k_2} = (\omega^{k_1})^{k_2} = \omega^{k_1 k_2} = \omega^{n \cdot q + r} = \omega^r = \sigma_r(\omega) = \sigma_{k_1 k_2}(\omega)$$

and so $\sigma_{k_1 k_2} = \sigma_{k_1} \circ \sigma_{k_2}$. Hence $F(k_1 k_2) = F(k_1) F(k_2)$ and so we conclude that $\mathbb{Z}_n^\times \cong G(\mathbb{Q}(\omega)/\mathbb{Q})$. ∎

<u>Example 14.13.</u> (June 2015, Problem 4) Let $f(x) = x^4 + 1 \in \mathbb{Q}[x]$, i.e. $f(x) = \Phi_8(x)$. Use the theory of cyclotomic polynomials to describe its splitting field E and the Galois group $G(E/\mathbb{Q})$.

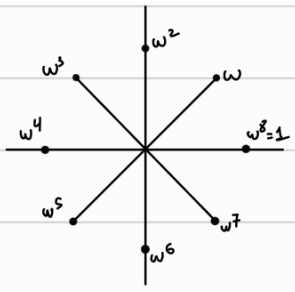
Notice that $\varphi(8) = 4$ since $\{1 \le k \le 8 \mid \gcd(k,8) = 1\} = \{1, 3, 5, 7\}$. Hence the primitive 8-th roots of unity are $e^{\frac{2\pi i}{8}}, e^{\frac{6\pi i}{8}}, e^{\frac{10\pi i}{8}}, e^{\frac{14\pi i}{8}}$. Let $\omega = e^{\frac{2\pi i}{8}}$. Then $E = \mathbb{Q}(\omega)$. Since $\deg(\Phi_8) = \deg(f) = \varphi(8) = 4$, we have that $\{1, \omega, \omega^2, \omega^3\}$ are a basis of $\mathbb{Q}(\omega)$ and

$$\mathbb{Q}(\omega) = \{ a_0 + a_1 \omega + a_2 \omega^2 + a_3 \omega^3 \mid a_0, a_1, a_2, a_3 \in \mathbb{Q} \}.$$

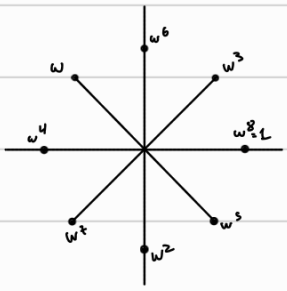
By Theorem 14.12 we have $G(E/\mathbb{Q}) \cong \mathbb{Z}_8^\times = \{\bar{1}, \bar{3}, \bar{5}, \bar{7}\}$. Hence $G(E/\mathbb{Q})$ has 4 elements. Since $\bar{1}^2 = \bar{3}^2 = \bar{5}^2 = \bar{7}^2 = \bar{1} \pmod 8$, all elements of $G(E/\mathbb{Q})$ have order 2 and so $G(E/\mathbb{Q}) \cong \mathbb{Z}_2 \times \mathbb{Z}_2$ (the Klein 4-group).

Geometrically:

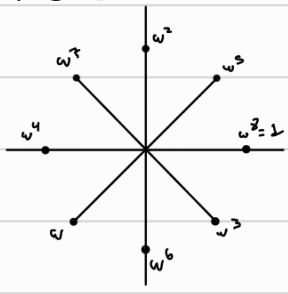
$\omega = e^{\frac{2\pi i}{8}} = e^{\frac{\pi}{4} i}$



$\omega = e^{\frac{6\pi i}{8}} = e^{\frac{3\pi}{4} i}$



$\omega = e^{\frac{10\pi i}{8}} = e^{\frac{5\pi}{4} i}$



$\omega = e^{\frac{14\pi i}{8}} = e^{\frac{7\pi}{4} i}$