• *Let $\mathbf{K} \subset \mathbf{E} \subset \mathbf{L}$ be field extensions. Assume that $\mathbf{K} \subset \mathbf{L}$ is Galois (finite, normal, separable), with Galois group $G := Aut_{\mathbf{K}}(\mathbf{L})$. Then $\mathbf{K} \subset \mathbf{E}$ is Galois if and only if $\mathbf{E} = \mathbf{L}^H$, for some H normal subgroup of G.*

Both extensions $\mathbf{K} \subset \mathbf{E}$ and $\mathbf{E} \subset \mathbf{L}$ are finite and always separable; the extension $\mathbf{E} \subset \mathbf{L}$ is always normal. So all is left to prove is that
• *the extension $\mathbf{K} \subset \mathbf{E}$ is normal if and only if $\mathbf{E} = \mathbf{L}^H$, for some normal subgroup H of G.*
From Galois theory we know that $\mathbf{E} = \mathbf{L}^H$, for some $H = Aut_{\mathbf{E}}(\mathbf{L})$.
- Assume $\mathbf{K} \subset \mathbf{E}$ is normal. Fix $h \in H$ and let $g \in Aut_{\mathbf{K}}(\mathbf{L})$ be an aritrary element. For $x \in \mathbf{E}$, consider $ghg^{-1}(x) = g(h(g^{-1}(x)))$. Let $f_x \in \mathbf{K}[x]$ be the minimal polynomial of x. Then $g^{-1}(x)$ is a zero of f_x and by the normality of $\mathbf{E}$ is an elements of $\mathbf{E}$. Now it is clear that $g(h(g^{-1}(x))) = x$. Since $x \in \mathbf{E}$ is arbitrary, then $ghg^{-1} \in H$ and H is normal.
- Conversely, assume that H is normal. Then $ghg^{-1} \in H$ and for all $x \in \mathbf{E}$, one has $g(h(g^{-1}(x))) = x$ or equivalently $h(g^{-1}(x)) = g^{-1}(x) \in \mathbf{E}$. Since $g^{-1}(x)$ is a zero of the minimal polynomial f_x of x, this says that all such zeros lie in $\mathbf{E}$, and $\mathbf{E}$ is normal.

• *If $\mathbf{K} \subset \mathbf{E}$ is Galois, then the Galois group $Aut_{\mathbf{K}}(\mathbf{E})$ is isomorphic to G/H.*
Consider the restriction homomorphism $\Psi\colon G = Aut_{\mathbf{K}}(\mathbf{L}) \to Aut_{\mathbf{K}}(\mathbf{E})$.
To prove that Ψ is well defined, we need to show that $g(x) \in \mathbf{E}$, for all $x \in \mathbf{E}$ and $g \in G$. As we already observed, $g(x)$ is a zero of the minimal polynomial f_x of x, and by the normality of $\mathbf{K} \subset \mathbf{E}$, it lies in $\mathbf{E}$.
The surjectivity Ψ, follows from Thm.7.5 is Garling, ensuring that $g \in Aut_{\mathbf{K}}(\mathbf{E})$ can be extended to an automorphism in $Aut_{\mathbf{K}}(\mathbf{L})$.
Finally, $\ker(\Psi) = \{g \in G \ : \ g(x) = x, \ \forall x \in \mathbf{E}\}$. But this is precisely $H = Aut_{\mathbf{E}}(\mathbf{L})$, and the statement follows.

• **Remark.** Consider $\mathbf{Q} \subset \mathbf{Q}(\sqrt[3]{2}) \subset \mathbf{Q}(\sqrt[3]{2}, \omega)$. As we already saw the extension $\mathbf{Q} \subset \mathbf{Q}(\sqrt[3]{2})$ is not normal. Also, if we choose the bijection

$$\sqrt[3]{2} \mapsto 1, \quad \sqrt[3]{2}\omega \mapsto 2, \quad \sqrt[3]{2}\omega^2 \mapsto 3,$$

then the subfield $\mathbf{Q}(\sqrt[3]{2})$ is the fixed fiel of $\langle (23) \rangle$ in $\mathcal{S}_3$, which is not a normal subgroup of $\mathcal{S}_3$.

• **Example.** *Every quadratic extension $\mathbf{K} \subset \mathbf{L}$ is normal.*
Let α be an element of $\mathbf{L}$ and let $f \in \mathbf{K}[x]$ be its minimum polynomial $f = x^2 + ax + b$. Let's check that if α is a zero of f, then $-\alpha - a$ is the other zero:

$$(X - \alpha)(X + \alpha + a) = X^2 + (-\alpha + \alpha + a)X + \alpha(-\alpha - a) = X^2 + aX + b.$$

Hence f factors completely in $\mathbf{L}[X]$, proving that $\mathbf{K} \subset \mathbf{L}$ is normal.

• **Example.** *Every subgroup $H \subset G$ of index 2 is normal.*
If $H \subset G$ has index 2, then $G = H \cup gH = H \cup Hg$. So $gH = Hg$, for all $g \in G$. Hence $gHg^{-1} = H$. If we have a Galois extension $\mathbf{K} \subset \mathbf{L}$, with Galois group G, then this confirms that the quadratic extension $\mathbf{K} \subset \mathbf{L}^H$ is normal.

• **Example.** *Let $\mathbf{K}$ be a field of characteristic p.*
Consider the polynomial $f = x^p - x + a$, for $a \in \mathbf{K}$. Then
- if f has one zero in an extension $\mathbf{E}$ of $\mathbf{K}$, then all zeros of f are in $\mathbf{K}(\alpha) \subset \mathbf{E}$.
- let α be a zero of f in $\mathbf{E}$. Then $\mathbf{K} \subset \mathbf{K}(\alpha)$ is a Galois extension, and the Galois group $Aut_{\mathbf{K}}(\mathbf{K}(\alpha))$ is isomorphic to a subgroup of $\mathbf{Z}_p$.

- *if f has no zero in $\mathbf{K}$, then it is irreducible in $\mathbf{K}[x]$. In particular, if $a \in \mathbf{Z}_p^*$, then f is irreducible in $\mathbf{Z}_p[x]$.*
- If $\alpha \in \mathbf{E}$ is a zero of f, one ca see that $\alpha + b$ is a zero of f if and only if

$$(\alpha + b)^p - (\alpha + b) + a = \alpha^p - \alpha + a + b^p - b = 0 \quad \Leftrightarrow \quad b \in \mathbf{Z}_p.$$

Hence $\alpha, \alpha + 1, \ldots, \alpha + (p-1)$ are the p distinct zeros of f: it is clear that they all lie in the same extension as α.
- Consider the extension $\mathbf{K} \subset \mathbf{K}(\alpha) \subset \mathbf{E}$. From what we juste showed, $\mathbf{K}(\alpha)$ is a splitting fired for f. Hence it is a Galois extension of $\mathbf{K}$. Indeed $[\mathbf{K}(\alpha) : \mathbf{K}] \leqslant p$; moreover, since the minimum polynomial of α divides f, then all its zeros are distinct and lie in $\mathbf{K}(\alpha)$.
Consider now the map

$$F\colon Aut_{\mathbf{K}}(K(\alpha)) \to \mathbf{Z}_p, \quad \phi_b \mapsto b,$$

where ϕ_b indicates the automorphism determined by the condition $\phi_b(\alpha) = \alpha + b$. The map F is a homomorphism: $\phi_b \circ \phi_c = \phi_{b+c}$. Morever it is injective: $F(\phi_b) = 0$ iff $b = 0$ and $\phi_0 = id$.
Then $Aut_{\mathbf{K}}(K(\alpha))$ is isomorphic to a subgroup of $\mathbf{Z}_p$. As p is prime, such subgroup is either $\{0\}$ or $\mathbf{Z}_p$. If $\alpha \in \mathbf{K}$, then we are in the first case.
- If f has no zero in $\mathbf{K}$, and this is the case when $\alpha \notin \mathbf{K}$, then $Aut_{\mathbf{K}}(K(\alpha)) \cong \mathbf{Z}_p$ and

$$\# Aut_{\mathbf{K}}(K(\alpha)) = [\mathbf{K}(\alpha) : \mathbf{K}].$$

In particular f is necessarily irreducible.

• **Example.** The extension $\mathbf{Q} \subset \mathbf{Q}(\xi)$, where ξ is a primitive n^{th}-root of 1 and n is not necessarily prime.
The element ξ is a zero of the n^{th} cyclotomic polynomial Φ_n, which is irreducible of degree $\varphi(n) := \#\mathbf{Z}_n^*$ in $\mathbf{Q}[x]$ (here φ denotes the Euler φ function). All other zeros of Φ_n, which are primitive roots of 1, are of the form ξ^m, with $\gcd(m, n) = 1$.
The degree of this extension is $[\mathbf{Q}(\xi) : \mathbf{Q}] = \varphi(n)$.
The Galois group: there is a group isomorphism $Aut_{\mathbf{Q}}(\mathbf{Q}(\xi)) \to \mathbf{Z}_n^*$, given by $\phi_m \mapsto m$, where ϕ_m is the automorphism of $\mathbf{Q}(\xi)$ determined by $\phi_m(\xi) = \xi^m$. Recall that, being an automorphism, ϕ_m preserves the order of the elements and that $order(\xi^m) = order(\xi) = n$ iff $\gcd(m, n) = 1$. Also note that, if $\gcd(m, n) = d > 1$, then $\phi_m(1) = \phi_m(\xi^{n/d} = 1$, meaning that ϕ_m is not bijective.

• **Example.** The extension $\mathbf{Q} \subset \mathbf{Q}(\xi)$, where ξ is a primitive 12^{th}-root of 1.
The element ξ is a zero of the 12^{th} cyclotomic polynomial $\Phi_{12} = x^4 - x^2 + 1$, irreducible in $\mathbf{Q}[x]$, of degree $\varphi(12) = 4$.
The degree of this extension is $[\mathbf{Q}(\xi) : \mathbf{Q}] = 4$.
The Galois group, $Aut_{\mathbf{Q}}(\mathbf{Q}(\xi)) \cong \mathbf{Z}_{12}^* \cong \mathbf{Z}_2 \times \mathbf{Z}_2$, is not cyclic and contains 3 subgroups isomorphic to $\mathbf{Z}_2$, namely $H_1 = \langle id, \phi_5 \rangle$, $H_2 = \langle id, \phi_7 \rangle$, $H_3 = \langle id, \phi_{11} \rangle$. The fixed subfield of each subgroup corresponds to a quadratic extension of $\mathbf{Q}$.
- $\mathbf{Q}(\xi)^{H_3} = \mathbf{Q}(\xi)^{\phi_{11}} = \mathbf{Q}(\sqrt{3})$: use the fact that $\xi + \phi_{11}(\xi) = \xi + \xi^{-1} = \xi + \bar{\xi}$ is an invariant element. Taking $\xi = e^{2\pi/12}$, one has $\xi + \bar{\xi} = 2\cos(\pi/6) = \sqrt{3}$. Note that the invariant element $\xi \cdot \phi_{11}(\xi) = 1$, so it does not help us in determining the fixed subfield.
- $\mathbf{Q}(\xi)^{H_1} = \mathbf{Q}(\xi)^{\phi_5} = \mathbf{Q}(i)$: use the fact that $\xi + \phi_5(\xi)$ is an invariant element and that $\xi^5 - \xi^3 + \xi = 0$. Hence $\xi + \xi^5 = \xi^3$. Taking $\xi = e^{2\pi/12}$, one has $\xi^3 = e^{\pi/2} = i$. Note that the invariant element $\xi \cdot \phi_5(\xi) = \xi^6 = -1$, so it does not help us in determining the fixed subfield.
- $\mathbf{Q}(\xi)^{H_2} = \mathbf{Q}(\xi)^{\phi_7} = \mathbf{Q}(\omega)$, where ω is a primitive cubic root of 1: use the fact that $\xi \cdot \phi_7(\xi) = \xi^8$ is an invariant element. Taking $\xi = e^{2\pi/12}$, one has $\xi^8 = e^{4\pi/3}$,

which is a primitive cubic root of 1. Note that the invariant element $\xi + \phi_7(\xi) = 0$, so it does not help us in determining the fixed subfield.