Galois Correspondence Theorem

Helena Ellis do Amaral, Diana Harambas, Ophir Horovitz
PROMYS, August 2023

1 Introduction

Galois Theory is at the intersection between modern and classical algebra, connecting group theory and field theory in interesting ways. Its purpose is to analyze solutions of polynomials, looking for those solutions that can be expressed using radical expressions (so by addition, subtraction, multiplication, division, and also n^{th} roots of the coefficients). Galois's main idea was looking at the symmetries of such polynomials, and therefore creating a Galois Group, with several properties to study, which led to the discovery of the Galois Correspondence.

2 Necessary background

In order to understand Galois Correspondence, we need to introduce some preliminary notions. Let's start by discussing types of field extensions.

2.1 Field extensions

Recall that if K is a subfield of L, then L is called an extension field of K or we can say that we have a **field extension** L/K. Defined formally, the field extension is a monomorphism/injection $K \hookrightarrow L$, where K, L are fields, and that this endows L with the structure of a $K-$vector space.

Therefore, the **degree of the field extension** $[L : K]$ is the dimension of L considered as a $K-$vector space.

Example. Field $\mathbb{R}$ is included in $\mathbb{C}$, as a subfield of $\mathbb{C}$,, therefore, we can say that $\mathbb{C}/\mathbb{R}$ is a field extension. Since every complex number can be written as $a+bi$, with $a, b \in \mathbb{R}$, we observe that $\{1, i\}$ is a basis and that $[\mathbb{C} : \mathbb{R}] = 2$.

Example. As $\mathbb{Q}$ is a subfield of $\mathbb{R}$, we call $\mathbb{R}/\mathbb{Q}$ a field extension. However, the basis of $\mathbb{R}$ as a $\mathbb{Q}-$vector space has infinite dimension, so $[\mathbb{R} : \mathbb{Q}] = \infty$.

In order to start classifying the field extensions, we need to think about the types of elements "added" to the larger field. Let's define what algebraic and transcendental elements are.

Definition 1. Let K be a field and L/K be a field extension. Suppose that $\alpha \in L$. Then we say that

- α is **algebraic** over K if there exists a non-zero polynomial p with coefficients in K such that $p(\alpha) = 0$.
- α is **transcendental** over K if there is NO non-zero polynomial $p \in K[x]$ such that $p(\alpha) = 0$.

Example. In the field extension $\mathbb{R}/\mathbb{Q}$, $\sqrt{2}$ is algebraic. It is a root of the polynomial $p(x) = x^2 - 2 \in \mathbb{Q}[x]$.

Example. $\pi \in \mathbb{R}$ is transcendental over $\mathbb{Q}$.

We saw that in order to talk about algebraic elements, we need to find polynomials that lead us to useful roots. Here is the definition of the minimal polynomial of an element.

Definition 2. Let K be a field and L/K be a field extension. Suppose that $\alpha \in L$ is algebraic. Then, there exists a unique monic polynomial $m \in K[x]$, with the smallest degree, such that α is a root of m. This is called **the minimal polynomial of α over K**.

Example. In the field extension $\mathbb{C}/\mathbb{R}$, one can see that the minimal polynomial associated with i is x^2+1 (it is monic, with real coefficients, has the smallest degree such that it has root i, and it is irreducible over $\mathbb{R}$).

After classifying the numbers as algebraic and transcendental, we can say that a field extension L/K is **algebraic** if any element $\beta \in L$ is algebraic over K. Moreover, since we introduced the minimal polynomial of an algebraic number, we can make a connection to the degree of the extension. Therefore, the following proposition holds:

Proposition 3. *If L/K is a finite extension, i.e. the degree $[L:K]$ is finite, then L/K is algebraic.*

However, this is not the only way to classify a type of extension (algebraic/transcendental). One can think of simple extensions:

Definition 4. Let L/K be a field extension. We say that L/K is a **simple extension** if there exists some $\alpha \in L$ such that $L = K(\alpha)$.

Example. The field extensions below are all simple field extensions:

- $\mathbb{C} = \mathbb{R}(i)$ over $\mathbb{R}$
- $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$
- $\mathbb{Q}(i,\sqrt{2})/\mathbb{Q}$ (one can show that the field extension is generated by $i+\sqrt{2}$).

At the moment, we talked about both the degree of a field extension and also about how algebraic elements must have a minimal polynomial attached. Let us make a connection between these two:

Proposition 5. *Let L/K be a simple field extension with $L = K(\alpha)$, for algebraic α. Then the degree of the extension is equal to the degree of the minimal polynomial $m \in K[x]$ of α over K.*

$$[K(\alpha):K] = deg(m)$$

Proposition 6. *Let K be a field and $m \in K[x]$ a monic irreducible polynomial. Then there exists a simple algebraic field extension L/K such that*

- *$L = K(\alpha)$ for some $\alpha \in L$*
- *α has the minimal polynomial m over K*
- *$[K(\alpha):K] = deg(m)$*

Key idea for proof: Since m is an irreducible monic polynomial over K, that means that in $K[x]$, (m) is a prime ideal, making the quotient $K[x]/(m)$ a field. Our $K(\alpha)$ is isomorphic to $K[x]/(m)$, where α satisfies the properties above.

Proposition 7. *Let L/K is a finite extension if and only if L is algebraic over K and there exist finitely many elements $\{\alpha_1, \alpha_2, ..., \alpha_n\}$ such that $L = K(\alpha_1, \alpha_2, ..., \alpha_n)$.*

2.2 Splitting fields

Definition 8. Let F be a field and let $f \in F[x]$ be a polynomial over F. We say that f **splits over** F if it can be expressed as a product of linear factors

$$f(x) = k(x-\alpha_1)(x-\alpha_2)...(x-\alpha_n),$$

where $k, \alpha_1, \alpha_2, ..., \alpha_n \in F$.

Example. Looking at $f(x) = x^4 - 4x^2 - 5$ splits over $\mathbb{Q}(i, \sqrt{5})$ because we can factor it as follows

$$f(x) = (x-i)(x+i)(x-\sqrt{5})(x+\sqrt{5}),$$

but it doesn't split over $\mathbb{Q}(i)$ or $\mathbb{Q}(\sqrt{5})$ - the best ways to factor it are $f(x) = (x-i)(x+i)(x^2-5)$ and $f(x) = (x^2+1)(x-\sqrt{5})(x+\sqrt{5})$, respectively.

Definition 9. Let K be a field and let f be a polynomial in $K[x]$. Then a field extension L/K is called a **splitting field of** f **over** K if the following hold:

- f splits over L
- if $K \subseteq L' \subseteq L$ and f splits over L', then $L' = L$ (or isomorphic as $K-$extensions)

This definition is equivalent to saying that L/K is a splitting field of f over K if L is the smallest field that contains all roots of $f(x) = 0$.

Example. Looking at $\mathbb{Q}(i)$, we can see that there is no other "smaller" field that will split $f(x) = x^2 + 1 = (x-i)(x+i)$ as a polynomial over $\mathbb{Q}$.

Defining splitting fields can now help us characterize two other types of field extensions: normal extensions and separable extensions.

Definition 10. A field extension L/K is **normal** if, when taking an irreducible polynomial $f \in K[x]$, if it has a root in L, then f splits over L.

Example. $\mathbb{Q}(i)/\mathbb{Q}$ is a normal extension because both $i, -i$, which are the only roots of $x^2 + 1 = 0$ are in $\mathbb{Q}(i)$.

Example. Looking at $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$, however, we can see that the minimal polynomial of $\sqrt[3]{2}$ is $x^3 - 2 = 0$, and two of its roots are non-real (so not in $\mathbb{Q}(\sqrt[3]{2}) \subset \mathbb{R}$ either). Thus, $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ is not a normal field extension.

Theorem 11. *A field extension L/K is finite and normal if and only if L is a splitting field for some polynomial over K.*

As mentioned before, we should discuss another type of extension: the separable one. Let's start by defining what a separable polynomial is.

Definition 12. An irreducible polynomial $f \in F[x]$ is **separable** if it has $deg(f)$ distinct roots in a splitting field of F i.e. we can write

$$f(x) = k(x-\alpha_1)(x-\alpha_2)...(x-\alpha_n),$$

where $\alpha_1, \alpha_2, ..., \alpha_n$ are all different from one another.

Definition 13. Let L/K be a field extension. We say that $\alpha \in L$ is separable over K if its minimal polynomial $m_\alpha \in K[x]$ is a separable polynomial over K.

Example. $\sqrt{3}$ is separable over $\mathbb{Q}$ because $f(x) = x^2 - 3$ has two distinct roots, both in $\mathbb{R}$.

Definition 14. Let L/K be a field extension. We say that L/K is separable if every $\alpha \in L$ is separable over K.

2.3 Field Automorphisms

Definition 15. Let K be a field. Then a **field automorphism** of K is a bijection $\phi : K \to K$ that satisfies the following properties for all $x, y \in K$:

- $\phi(x+y) = \phi(x) + \phi(y)$
- $\phi(xy) = \phi(x)\phi(y)$

Example. In the field of complex numbers $\mathbb{C}$, define the bijection $\phi(z) = \overline{z}$, that maps an element to its complex conjugate. Then ϕ is an automorphism of $\mathbb{C}$ because the following properties also hold:

- $\phi(x+y) = \overline{x+y} = \overline{x} + \overline{y} = \phi(x) + \phi(y)$
- $\phi(xy) = \overline{xy} = \overline{x} \cdot \overline{y} = \phi(x)\phi(y)$

Theorem 16. *The set of all automorphisms of a field K forms a group under the composition of functions.*

Theorem 17. *If L/K is a field extension and $\alpha \in L$ is a root of a polynomial $f \in K[x]$, then for any automorphism σ of L which fixes K, the polynomial f also contains $\sigma(\alpha)$ as a root.*

3 Galois Groups and the Galois Correspondence

Definition 18. Let H be a group of automorphisms of a field K. The fixed field of H is the set of elements of K that are fixed by every group element.

$$K^H = \{\alpha \in K | \sigma(\alpha) = \alpha \forall \sigma \in H\}$$

Theorem 19. *(Fixed Field Theorem): If H is a finite group of automorphisms of a field K and K^H is its fixed field, then K/K^H is a finite extension, and its degree $[K : K^H]$ is equal to the order of the group $|H|$.*

Definition 20. Let $Aut(L/K)$ be the group of automorphisms of L that fix K, i.e., $Aut(L/K) = \{\sigma : L \to L \mid \sigma(x) = x \text{ for all } x \in K\}$. A finite, algebraic extension L/K is called a Galois extension if the order of this group is the same as the degree of L over K, i.e. $|Aut(L/K)| = [L : K]$.
This is just one of the ways in which we can define a Galois extension. Equivalently, an extension L/K is Galois if:

1. L/K is normal and separable, i.e. L is a splitting field of a separable polynomial with coefficients in K. In other words, every irreducible polynomial with coefficients in L that has a root in K splits into distinct linear factors in K.
2. K is the fixed field of $Aut(L/K)$

Definition 21. Let L/K be a Galois extension. $Aut(L/K)$ is called the Galois group of L/K and is denoted $Gal(L/K)$.

Theorem 22. *(Galois Correspondence): Let L/K be a Galois extension, and let $Gal(L/K)$ be its Galois group. There is a bijective correspondence between subgroups H of $Gal(L/K)$ and intermediate subfields F_i of the extension $L \subset F_1 \subset F_2 ... \subset F_i \subset K$. This correspondence is given by*

$F \longrightarrow$ {elements of $Gal(L/K)$ fixing F}

and its inverse: $H \longrightarrow$ {fixed field of H

Corollary 23. *1. Let F_1 and F_2 be intermediate fields and H_1 and H_2 be their corresponding subgroups. Then $F_1 \subset F_2$ if and only if $H_2 \subset H_1$.*

2. The subgroup corresponding to the field K is the entire Galois group, and the subgroup that corresponds to L is the trivial subgroup.

3. Let F correspond to H. Then $[L:F] = |H|$ and $[F:K] = [G:H]$.

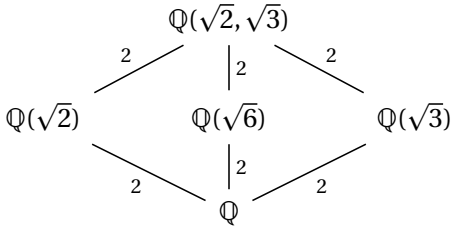
4 Computing Galois Groups and Exploring the Correspondence

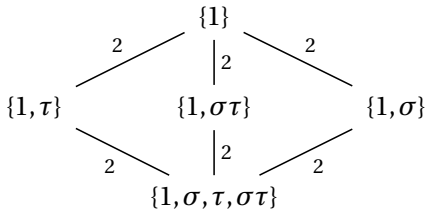
We will now explore some examples of the Galois correspondence in action by investigating several Galois extensions and analyzing the subfield and subgroup lattices. Let $K = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. The extension $K/\mathbb{Q}$ is Galois since it is the splitting field of the separable polynomial $(X^2-2)(X^2-3)$. One can show that $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2}+\sqrt{3})$ (this is a good exercise to verify) and $\sqrt{2}+\sqrt{3}$ has minimal polynomial $X^4 - 10X^2 + 1$, so K has degree 4 over $\mathbb{Q}$. Any automorphism σ of $K/\mathbb{Q}$ is determined by where it sends $\sqrt{2}$ and $\sqrt{3}$, since $\sigma(a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}) = a + b\sigma(\sqrt{2}) + c\sigma(\sqrt{3}) + d\sigma(\sqrt{6})$. Since $\sqrt{2}$ is a root of $X^2 - 2$ and $\sqrt{3}$ is a root of $X^3 - 3$, σ must send $\sqrt{2}$ to $\pm\sqrt{2}$ and it must send $\sqrt{3}$ to $\pm\sqrt{3}$. This gives four possibilities for automorphisms, given by

$$1 : \begin{cases} \sqrt{2} \mapsto \sqrt{2} \\ \sqrt{3} \mapsto \sqrt{3} \end{cases} \quad \sigma : \begin{cases} \sqrt{2} \mapsto -\sqrt{2} \\ \sqrt{3} \mapsto \sqrt{3} \end{cases} \quad \tau : \begin{cases} \sqrt{2} \mapsto \sqrt{2} \\ \sqrt{3} \mapsto -\sqrt{3} \end{cases} \quad \sigma\tau : \begin{cases} \sqrt{2} \mapsto -\sqrt{2} \\ \sqrt{3} \mapsto -\sqrt{3} \end{cases}$$

Since the Galois group of K has order 4 (since this is the degree of K), these four maps are precisely the elements of the Galois group, $\mathrm{Gal}(K/\mathbb{Q})$. Every element in this group has order 2 by observation, so this is the unique non-cyclic abelian group of order 4, sometimes referred to as the Klein group, and is isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$. In fact, we can make this isomorphism explicit by sending $\sigma \mapsto (1,0)$ and $\tau \mapsto (0,1)$, and letting the relations carry the other two elements. What about the subfields of K and their corresponding Galois subgroups? The intermediate subfields of K are $K, \mathbb{Q}(\sqrt{2}), \mathbb{Q}(\sqrt{3}), \mathbb{Q}(\sqrt{6})$ and $\mathbb{Q}$, and the subgroups of $\mathrm{Gal}(K/\mathbb{Q})$ are $\{1\}, \{1,\sigma\}, \{1,\tau\}, \{1,\sigma\tau\}$, and of course $\mathrm{Gal}(K/\mathbb{Q})$ itself. The corresponding Galois subgroup to $\mathbb{Q}$ is the set of all automorphisms in $\mathrm{Gal}(K/\mathbb{Q})$ which fix $\mathbb{Q}$. But every automorphism does so by definition of the Galois group, so $\mathbb{Q}$ corresponds to $\mathrm{Gal}(K/\mathbb{Q})$ itself. Which automorphisms fix $\mathbb{Q}(\sqrt{2})$? These are 1 and τ, so $\mathbb{Q}(\sqrt{2})$ corresponds to the subgroup $\{1,\tau\}$. Similarly, $\mathbb{Q}(\sqrt{3})$ corresponds to $\{1,\sigma\}$. Which subgroup corresponds to $\mathbb{Q}(\sqrt{6})$? If an automorphism γ fixes $\sqrt{6}$, then $\gamma(\sqrt{6}) = \gamma(\sqrt{2}\sqrt{3}) = \gamma(\sqrt{2})\gamma(\sqrt{3}) = \sqrt{2}\sqrt{3}$, so either γ sends $\sqrt{2}$ to $\sqrt{2}$ and $\sqrt{3}$ to $\sqrt{3}$ or it sends $\sqrt{2}$ to $-\sqrt{2}$ and $\sqrt{3}$ to $-\sqrt{3}$. The two automorphisms which do this are 1 and $\sigma\tau$, so $\mathbb{Q}(\sqrt{6})$ corresponds to the subgroup $\{1,\sigma\tau\}$. Finally, the only automorphism which fixes all of K is the trivial automorphism 1, so K corresponds to $\{1\}$.

Below we can find the subfield lattice for $K/\mathbb{Q}$ as well as the subgroup lattice for $\mathrm{Gal}(K/\mathbb{Q})$, which has been inverted to more clearly show the correspondence in action.





Our next example is slightly more complicated. Let's investigate the Galois group of the splitting field of X^3-2. This polynomial has as its roots $\sqrt[3]{2}$, $\rho\sqrt[3]{2}$, and $\rho^2\sqrt[3]{2}$, where ρ is a primitive 3rd root of unity (i.e. a root of X^2+X+1) and $\sqrt[3]{2}$ denotes the unique real solution to X^3-2. The splitting field K is the smallest field which contains these roots. Since it contains $\sqrt[3]{2}$ and $\rho\sqrt[3]{2}$, it also contains $\rho = \rho\sqrt[3]{2}/\sqrt[3]{2}$. If it contains ρ and $\sqrt[3]{2}$, then it contains all three roots of X^3-2. Thus we can write $K = \mathbb{Q}(\rho, \sqrt[3]{2})$. What is the degree of this extension? The degree of $\sqrt[3]{2}$ over $\mathbb{Q}$ is 3 since its minimal polynomial is X^3-2, and so $\mathbb{Q}(\sqrt[3]{2})$ has degree 3 over $\mathbb{Q}$. The degree of ρ over $\mathbb{Q}(\sqrt[3]{2})$ is 2 since the minimal polynomial over $\mathbb{Q}$ of ρ, namely X^2+X+1, stays irreducible over $\mathbb{Q}(\sqrt[3]{2})$ since $\mathbb{Q}(\sqrt[3]{2}) \subset \mathbb{R}$ and both roots of X^2+X+1 are complex. Thus, by the tower law for extensions, we have $[\mathbb{Q}(\rho, \sqrt[3]{2}) : \mathbb{Q}] = [\mathbb{Q}(\rho, \sqrt[3]{2}) : \mathbb{Q}(\sqrt[3]{2})][\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 2 \cdot 3 = 6$. This extensions Galois since it is the splitting field of the separable polynomial X^3-2. Now we can use a similar approach as above to find the automorphisms in $\mathrm{Gal}(K/\mathbb{Q})$ by considering what such maps do to the generators of K, namely ρ and $\sqrt[3]{2}$. We know that any automorphism must send a root of a polynomial to another root of the same polynomial, so $\sqrt[3]{2}$ must get sent to $\sqrt[3]{2}, \rho\sqrt[3]{2}$ or $\rho^2\sqrt[3]{2}$, and ρ must get sent to ρ or ρ^2, since $(X-\rho)(X-\rho^2) = X^2 - \rho X - \rho^2 X + \rho^3 = X^2 + X + 1$ using the identity $1+\rho+\rho^2 = 0$ and the fact that $\rho^3 = 1$ since ρ is a 3rd root of unity. This gives us 6 possibilities for automorphisms, and since the extension is Galois, we know that $|\mathrm{Gal}(K/\mathbb{Q})| = 6$, so in fact all of these possibilities extend to legitimate automorphisms on $K/\mathbb{Q}$. So we know what the elements of $\mathrm{Gal}(K/\mathbb{Q})$ are, but what can we say about the *algebra* of $\mathrm{Gal}(K/\mathbb{Q})$? Let's start with the elements σ and τ given by

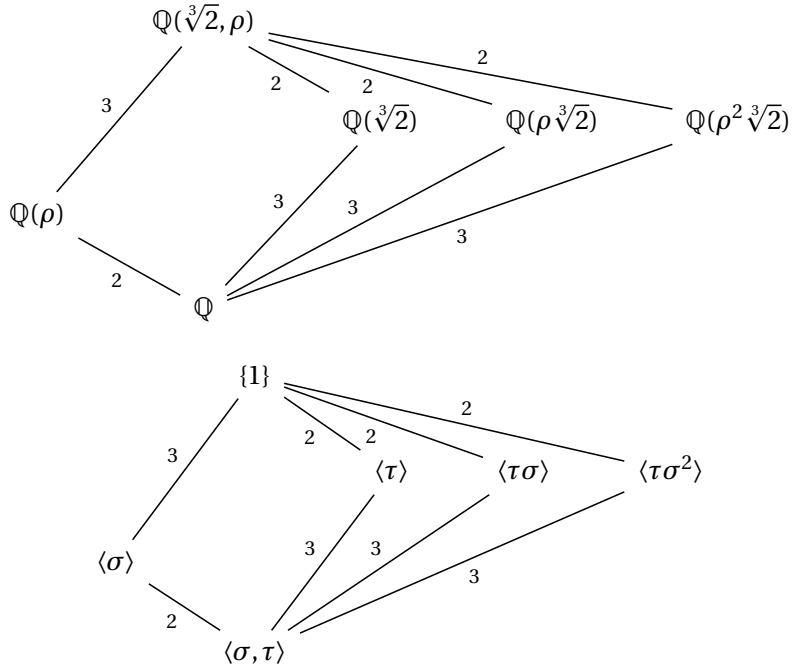
$$\sigma : \begin{cases} \sqrt[3]{2} \mapsto \rho\sqrt[3]{2} \\ \rho \mapsto \rho \end{cases} \qquad \tau : \begin{cases} \sqrt[3]{2} \mapsto \sqrt[3]{2} \\ \rho \mapsto \rho^2 \end{cases}$$

Now let's investigate what happens when we try composing these elements together:

$$\sigma^2 : \begin{cases} \sqrt[3]{2} \mapsto \rho^2\sqrt[3]{2} \\ \rho \mapsto \rho \end{cases} \qquad \tau\sigma : \begin{cases} \sqrt[3]{2} \mapsto \rho^2\sqrt[3]{2} \\ \rho \mapsto \rho^2 \end{cases} \qquad \tau\sigma^2 : \begin{cases} \sqrt[3]{2} \mapsto \rho\sqrt[3]{2} \\ \rho \mapsto \rho^2 \end{cases} \qquad \sigma\tau : \begin{cases} \sqrt[3]{2} \mapsto \rho\sqrt[3]{2} \\ \rho \mapsto \rho^2 \end{cases}$$

Based on these relations, we can see that if we think of σ as the element $(123) \in S_3$ and τ as the element $(23) \in S_3$, not only do σ and τ generate $\mathrm{Gal}(K/\mathbb{Q})$ but we get an isomorphism
$\mathrm{Gal}(K/\mathbb{Q}) = \langle \sigma^3 = 1, \tau^2 = 1, \sigma\tau = \tau\sigma^2 \rangle \cong S_3$. Let's explore some of the intermediate fields and their corresponding subgroups. We have the intermediate field $\mathbb{Q}(\rho)$, and K has degree 3 over $\mathbb{Q}(\rho)$. We aim to find the order 3 subgroup which fixes $\mathbb{Q}(\rho)$. There is only one order 3 subgroup of S_3, namely $\langle (1,2,3) \rangle$, which corresponds to $\{1, \sigma, \sigma^2\}$ in $\mathrm{Gal}(K/\mathbb{Q})$. Similarly, the field $\mathbb{Q}(\sqrt[3]{2})$ corresponds to the order 2 subgroup $\{1, \tau\}$. What about the intermediate field $\mathbb{Q}(\rho\sqrt[3]{2})$? Which automorphisms fix this field? Certainly the identity automorphism 1 does, and the other one which does is $\tau\sigma$ since $\tau\sigma(\rho\sqrt[3]{2}) = \tau\sigma(\rho)\tau\sigma(\sqrt[3]{2}) = \rho^2(\rho^2\sqrt[3]{2}) = \rho\sqrt[3]{2}$. So $\mathbb{Q}(\sqrt[3]{2})$ corresponds to $\{1, \tau\sigma\}$.

Here are the full subfield and subgroup lattices to show the complete correspondence:



5 References

Ian Stewart, Galois Theory, 3rd edition, Chapman & Hall/CRC, 2003
Dummit & Foote, Abstract Algebra, 3rd edition, Wiley, 2003