The American Mathematical Monthly

ISSN: (Print) (Online) Journal homepage: www.tandfonline.com/journals/uamm20

A Worked out Galois Group for the Classroom

Lorenz Halbeisen & Norbert Hungerbühler

To cite this article: Lorenz Halbeisen & Norbert Hungerbühler (2024) A Worked out Galois Group for the Classroom, The American Mathematical Monthly, 131:6, 501-510, DOI: 10.1080/00029890.2024.2325330

To link to this article: https://doi.org/10.1080/00029890.2024.2325330

Published online: 29 Mar 2024.

A Worked out Galois Group for the Classroom

Lorenz Halbeisen and Norbert Hungerbühler

Abstract. Let $f = X^6 - 3X^2 - 1 \in \mathbb{Q}[X]$ and let L_f be the splitting field of f over $\mathbb{Q}$. We show by hand that the Galois group $\mathrm{Gal}(L_f/\mathbb{Q})$ of the Galois extension $L_f/\mathbb{Q}$ is isomorphic to the alternating group A_4. Moreover, we show that the six roots of f correspond to the six edges of a tetrahedron and that the four roots of the polynomial $X^4 + 18X^2 - 72X + 81$ correspond to the four faces of a tetrahedron, which allows us to determine all eight proper intermediate fields of the extension $L_f/\mathbb{Q}$.

1. INTRODUCTION. Teaching Galois theory, one often has the problem that the Galois group of a field extension of $\mathbb{Q}$ is either quite simple or too difficult to be computed by hand. An example of a Galois group which is isomorphic to the dihedral group of order 8 can be found in Stewart [**1**, Ch. 13]. Introducing this example, Stewart writes that this Galois group has an "archetypal quality, since a simpler example would be too small to illustrate the theory adequately, and anything more complicated would be unwieldy" [**1**, p. 155]. Moreover, it is usually rather tedious to compute the Galois group along with the intermediate fields and their relations.

The aim of this note is to provide a worked out field extension over $\mathbb{Q}$ whose Galois group is isomorphic to the alternating group A_4 (i.e., to the symmetry group of the tetrahedron), and to compute by hand all intermediate fields and their relations. If we do not require that the ground field is $\mathbb{Q}$, a canonical way to obtain a field extension L/K with $\mathrm{Gal}(L/K) \cong A_4$ for some fields $L \supsetneq K \supsetneq \mathbb{Q}$, is to start with a polynomial $f \in \mathbb{Q}[X]$ of degree 4 such that the Galois group of the field extension $L/\mathbb{Q}$ — where L is the splitting field of f over $\mathbb{Q}$ — is isomorphic to the symmetry group S_4. Then, since $A_4 \trianglelefteq S_4$, by the Galois correspondence we find a quadratic extension K of $\mathbb{Q}$ such that $\mathrm{Gal}(L/K) \cong A_4$ (see also Osofsky [**2**, p.222]). However, since the ground field K of the field extension L/K is already a field extension of $\mathbb{Q}$, it is quite exhausting to compute $\mathrm{Gal}(L/K)$ and the intermediate fields of L/K by hand.

Before we present our example in the next section, we set up the terminology (according to [**1**, **3**]), where we assume that the reader is familiar with the basic facts of Galois theory with respect to field extensions over $\mathbb{Q}$.

If $f \in \mathbb{Q}[X]$ is a polynomial, then the smallest subfield of $\mathbb{C}$ containing all of the roots of f is called the *splitting field of f over* $\mathbb{Q}$. The splitting field of f over $\mathbb{Q}$ is unique up to isomorphism. If $L/\mathbb{Q}$ is a field extension and $\mathbb{Q} \subseteq M \subseteq L$ is a field, then M is called an *intermediate field* of $L/\mathbb{Q}$. If $M \subseteq L$ are fields, then the group of all automorphisms of L which fix M point-wise is the *Galois group* of the field extension L/M, denoted $\mathrm{Gal}(L/M)$. Let $f \in \mathbb{Q}[X]$ be a polynomial, L_f its splitting field over $\mathbb{Q}$, and M an intermediate subfield, so $\mathbb{Q} \subseteq M \subseteq L_f$. Let $g \in M[X]$ and let

doi.org/10.1080/00029890.2024.2325330
MSC: 11R32, 11R16, 11R11

$K_g \subseteq L_f$ be its splitting field over M. Then K_g/M is a *Galois extension*. We will only consider Galois extensions of this type.

Now we can state the main theorem of Galois theory.

THE GALOIS CORRESPONDENCE. Let $L/\mathbb{Q}$ be an arbitrary Galois extension. Then the following holds:

- To each subgroup $H \leqslant \mathrm{Gal}(L/\mathbb{Q})$ there exists an intermediate field L^H, such that

$$L^H = \{a \in L : \forall \sigma \in H\big(\sigma(a) = a\big)\}.$$

- For each intermediate field $\mathbb{Q} \subseteq M \subseteq L$ we have $\mathrm{Gal}(L/M) \leqslant \mathrm{Gal}(L/\mathbb{Q})$ and

$$L^{\mathrm{Gal}(L/M)} = M.$$

- Let M_1 and M_2 be intermediate fields of some field extension $L/\mathbb{Q}$, and let $H_1 := \mathrm{Gal}(L/M_1)$. If, for some $\sigma \in \mathrm{Gal}(L/\mathbb{Q})$, we have $\mathrm{Gal}(L/M_2) = \sigma H_1 \sigma^{-1}$, then the fields M_1 and M_2 are *conjugate*.
- If $\mathbb{Q} \subseteq M \subseteq L$ is such that $\mathrm{Gal}(L/M)$ is a normal subgroup of $\mathrm{Gal}(L/\mathbb{Q})$ (i.e., the conjugate class of M contains only M), then the field extension $M/\mathbb{Q}$ is Galois and

$$\mathrm{Gal}(M/\mathbb{Q}) \cong \mathrm{Gal}(L/\mathbb{Q})/\,\mathrm{Gal}(L/M).$$

2. A FIELD EXTENSION $L/\mathbb{Q}$ WITH GAL$(L/\mathbb{Q}) \cong A_4$. We start with the polynomial $f = X^6 - 3X^2 - 1$ and consider its splitting field L_f over $\mathbb{Q}$. The goal is to show that $\mathrm{Gal}(L_f/\mathbb{Q}) \cong A_4$, where A_4 is the alternating group of degree 4, which is isomorphic to the symmetry group of the tetrahedron.

In order to compute the roots of f, we replace X^2 by ξ and first compute the roots of the irreducible polynomial $g = \xi^3 - 3\xi - 1$. To see that g is irreducible, consider the polynomial

$$\tilde{g} := (\xi - 2)^3 - 3(\xi - 2) - 1 = \xi^3 - 6\xi^2 + 9\xi - 3.$$

By the Eisenstein-Schönemann Criterion (with $p = 3$), we see that $\tilde{g}$ is irreducible over $\mathbb{Q}$, and so is g.

Observe that every complex number $\xi \neq 0$ can be written as $\xi = \alpha + \beta$ with $\alpha^3 + \beta^3 = 1$. Indeed, for $\beta = \xi - \alpha$ we have $\beta^3 = \xi^3 - 3\xi^2\alpha + 3\xi\alpha^2 - \alpha^3$ and hence

$$1 = \alpha^3 + \beta^3 = \xi(\xi^2 - 3\xi\alpha + 3\alpha^2)\,.$$

This is a quadratic equation for $\alpha \in \mathbb{C}$ with a solution if $\xi \neq 0$. In particular, a root ξ of g can be written in the form $\xi = \alpha + \beta$ with $\alpha^3 + \beta^3 = 1$. Then

$$g = (\alpha + \beta)^3 - 3(\alpha + \beta) - 1 = \alpha^3 + 3\alpha^2\beta + 3\alpha\beta^3 + \beta^3 - 3\alpha - 3\beta - 1 = 0.$$

So, since $\alpha^3 + \beta^3 = 1$, we have

$$3\alpha\beta(\alpha + \beta) - 3(\alpha + \beta) = 0$$

and since $\alpha + \beta \neq 0$, we obtain

$$\alpha\beta = 1, \qquad \beta = \frac{1}{\alpha}, \qquad \text{and} \quad \alpha^3 + \frac{1}{\alpha^3} = 1.$$

If we set $z := \alpha^3$, then $z + \frac{1}{z} = 1$ and hence $z^2 - z + 1 = 0$. We choose the solution

$$z_1 = \tfrac{1}{2} + i\,\tfrac{\sqrt{3}}{2} = e^{\pi i/3}.$$

Now α is a third root of z_1 and we choose $\alpha = e^{\pi i/9}$. Since $\beta = \frac{1}{\alpha} = \bar{\alpha}$, we obtain

$$\xi_1 := \xi = \alpha + \bar{\alpha} = 2\cos(\pi/9).$$

Then

$$\xi_1^3 = (\alpha+\bar{\alpha})^3 = \alpha^3 + 3\underbrace{\alpha^2\,\bar{\alpha}}_{=\alpha} + 3\underbrace{\alpha\,\bar{\alpha}^2}_{=\bar{\alpha}} + \bar{\alpha}^3 = 3(\underbrace{\alpha+\bar{\alpha}}_{=\xi_1}) + \underbrace{\alpha^3+\bar{\alpha}^3}_{=1} = 3\,\xi_1 + 1$$

which shows that ξ_1 is indeed a root of $g = \xi^3 - 3\xi - 1$. The two remaining third roots of z_1 are

$$\begin{array}{rcccl} e^{2\pi i/3}\cdot e^{\pi i/9} & = & e^{7\pi i/9} & = & \alpha^7, \\ e^{4\pi i/3}\cdot e^{\pi i/9} & = & e^{13\pi i/9} & = & \alpha^{13}. \end{array}$$

Hence the roots of g are given by

$$\begin{array}{rclcl} \xi_1 & = & \alpha+\bar{\alpha} & = & 2\cos(\pi/9), \\ \xi_2 & = & \alpha^7+\bar{\alpha}^7 & = & 2\cos(7\pi/9), \\ \xi_3 & = & \alpha^{13}+\bar{\alpha}^{13} & = & 2\cos(13\pi/9). \end{array}$$

Thus, $g = \xi^3 - 3\xi - 1 = (\xi-\xi_1)(\xi-\xi_2)(\xi-\xi_3)$, which shows that $\xi_1\,\xi_2\,\xi_3 = 1$, $\xi_1\,\xi_2 + \xi_2\,\xi_3 + \xi_3\,\xi_1 = -3$, and $\xi_1 + \xi_2 + \xi_3 = 0$.

Notice that

$$-\xi_2 = e^{\pi i}(e^{7\pi i/9} + e^{-7\pi i/9}) = e^{16\pi i/9} + e^{2\pi i/9} = e^{-2\pi i/9} + e^{2\pi i/9} = \alpha^2 + \bar{\alpha}^2,$$

and similarly we have $-\xi_3 = \alpha^4 + \bar{\alpha}^4$. Thus we have

$$2 - \xi_1^2 = 2 - (\alpha+\bar{\alpha})^2 = 2 - (2\underbrace{\alpha\,\bar{\alpha}}_{=1} + \underbrace{\alpha^2+\bar{\alpha}^2}_{=-\xi_2}) = 2 - (2 - \xi_2) = \xi_2\,.$$

Similarly we get $2 - \xi_2^2 = \xi_3$ and $2 - \xi_3^2 = \xi_1$. This shows that $\mathbb{Q}(\xi_1) = \mathbb{Q}(\xi_2) = \mathbb{Q}(\xi_3)$. In particular, $\mathbb{Q}(\xi_1)$ is the splitting field of g over $\mathbb{Q}$. So, for $L_g := \mathbb{Q}(\xi_1)$, the field extension $L_g/\mathbb{Q}$ is Galois.

For convenience in later arguments, we rewrite the three roots of g as follows:

$$\xi_1 = \alpha + \bar{\alpha} \;=\; 2\cos(\pi/9)$$

$$\xi_2 = 2\cos(7\pi/9) = -2\cos(7\pi/9+\pi) = -2\cos(2\pi/9)$$

$$\xi_3 = 2\cos(13\pi/9) = -2\cos(13\pi/9+\pi) = -2\cos(4\pi/9)\,.$$

Then by construction we obtain the six pairwise distinct roots of f as $\pm\sqrt{\xi_k}$ for

$1 \le k \le 3$. In particular, we define

$$\begin{array}{rclcrcl} \zeta_1 & := & \sqrt{2\cos(\pi/9)} & \qquad & \zeta_4 & := & -\zeta_1 \\ \zeta_2 & := & i\sqrt{2\cos(2\pi/9)} & & \zeta_5 & := & -\zeta_2 \\ \zeta_3 & := & i\sqrt{2\cos(4\pi/9)} & & \zeta_6 & := & -\zeta_3\,. \end{array}$$

This shows that

$$f = (X-\zeta_1)(X+\zeta_1)(X-\zeta_2)(X+\zeta_2)(X-\zeta_3)(X+\zeta_3).$$

Notice that since $\xi_1\,\xi_2\,\xi_3 = 1$, we have $\zeta_1^2\,\zeta_2^2\,\zeta_3^2 = 1$, which implies that the product $(\pm\zeta_1)(\pm\zeta_2)(\pm\zeta_3) = \pm 1$. Moreover, by definition of $\zeta_1, \zeta_2, \zeta_3$ we have $\zeta_1\,\zeta_2\,\zeta_3 = -1$.

Now, let us show that f is irreducible over $\mathbb{Q}$. For this, assume on the contrary that $f = p \cdot q$ for some nonconstant polynomials $p, q \in \mathbb{Q}[X]$. If $\deg(p) = 1$, e.g., $p = (X - \zeta_1)$, then $\zeta_1 \in \mathbb{Q}$, which is obviously a contradiction. Assume now that $\deg(p) = 2$, e.g., $p = (X-\zeta_1)(X+\zeta_1) = X^2 - \xi_1$ or $p = (X-\zeta_1)(X-\zeta_2) = X^2 - (\zeta_1 + \zeta_2)X + \zeta_1\,\zeta_2$. Then, in the former case this would imply $\xi_1 \in \mathbb{Q}$, and in the latter case this would imply $\zeta_1\,\zeta_2 = -\frac{1}{\zeta_3} \in \mathbb{Q}$. Thus in both cases we arrive at a contradiction. If $\deg(p) = 3$ and p is of the form

$$p = (X-\zeta_1)(X+\zeta_1)(X-\zeta_2) = X^3 - \zeta_2 X^2 + \dots,$$

then $\zeta_2 \in \mathbb{Q}$, which is again a contradiction. Finally, if $\deg(p) = 3$ and p is of the form

$$p = (X-\zeta_1)(X-\zeta_2)(X-\zeta_3) = 1 + bX + cX^2 + X^3,$$

then q is of the form

$$q = (X+\zeta_1)(X+\zeta_2)(X+\zeta_3) = -1 + bX - cX^2 + X^3.$$

Since $f = p \cdot q = X^6 - 3X^2 - 1$, we must have $2b - c^2 = 0$ and $b^2 - 2c = -3$. In particular, $b = \frac{c^2}{2}$ and therefore $\frac{c^4}{4} - 2c + 3 = 0$, but since $\frac{c^4}{4} - 2c + 3 > 1$ for all $c \in \mathbb{R}$, we conclude that $p \notin \mathbb{Q}[X]$. Thus, there are no nonconstant polynomials $p, q \in \mathbb{Q}[X]$ such that $f = p \cdot q$, which shows that f is irreducible over $\mathbb{Q}$. In particular, since $f \in \mathbb{Q}[X]$ is a monic, irreducible polynomial of degree 6 with the six roots $\zeta_1, \dots, \zeta_6$, we have $\zeta_m \notin \mathbb{Q}(\xi_k)$ for $1 \le m \le 6$ and $1 \le k \le 3$.

Let $G_f := \mathrm{Gal}(L_f/\mathbb{Q})$ and $G_g := \mathrm{Gal}(L_g/\mathbb{Q})$, where L_f and L_g are the splitting fields of f and g, respectively. Then, since $\deg(g) = 3$ and $L_g = \mathbb{Q}(\xi_1)$, we have $|G_g| = 3$ and therefore $G_g \cong C_3$, where C_n denotes the cyclic group of order n. Furthermore, since the field extension $L_g/\mathbb{Q}$ is Galois, $\mathrm{Gal}(L_f/L_g) \trianglelefteq G_f$ and $G_f/\,\mathrm{Gal}(L_f/L_g) \cong C_3$. Since $\zeta_m \notin \mathbb{Q}(\xi_k)$, $\mathrm{Gal}(L_f/L_g)$ is not the trivial group.

Now, we consider $\mathrm{Gal}(L_f/L_g)$. Let $\sigma \in \mathrm{Gal}(L_f/L_g)$. Then $\sigma(\xi_k) = \xi_k$ for $1 \le k \le 3$. Thus $\sigma(\zeta_m) = \pm\zeta_m$ for all $1 \le m \le 6$. To see this, consider, for example, $\xi_1 = \sigma(\xi_1) = \sigma(\zeta_1 \cdot \zeta_1) = \sigma(\zeta_1) \cdot \sigma(\zeta_1)$. Therefore $\mathrm{Gal}(L_f/L_g) \leqslant C_2 \times C_2 \times C_2$.

If we adjoin to the field L_g a root ζ_m (for $1 \le m \le 6$), then we obtain the intermediate field $L_g \subsetneq L_g(\zeta_m) \subseteq L_f$, where $\mathrm{Gal}(L_g(\zeta_m)/L_g) \cong C_2$. Since $\zeta_m^2 = \xi_k$ for some $1 \le k \le 3$ and $\mathbb{Q}(\xi_1) = \mathbb{Q}(\xi_2) = \mathbb{Q}(\xi_3)$, we have $L_g(\zeta_m) = \mathbb{Q}(\zeta_m)$. Since each of the fields $\mathbb{Q}(\zeta_k)$ (for $1 \le k \le 3$) is the splitting field of a quadratic polynomial of the form $Z^2 - \zeta_k^2$ for $1 \le k \le 3$, each of the field extensions $\mathbb{Q}(\zeta_k)/L_g$ (for $1 \le k \le 3$) is Galois with $\mathrm{Gal}(\mathbb{Q}(\zeta_k)/L_g) \cong C_2$.

Now, there are three possible intermediate fields of the form $\mathbb{Q}(\zeta_m)$, namely $\mathbb{Q}(\zeta_1)$, $\mathbb{Q}(\zeta_2)$, and $\mathbb{Q}(\zeta_3)$. To see that these three intermediate fields are pairwise distinct, notice first that, since $\zeta_1 = \sqrt{2\cos(\varphi)} \in \mathbb{R}$, we have $\mathbb{Q}(\zeta_1) \subseteq \mathbb{R}$, and therefore $\zeta_2, \zeta_3 \notin \mathbb{Q}(\zeta_1)$. Furthermore, if $\zeta_1 \in \mathbb{Q}(\zeta_2)$, then, since $\Re(\zeta_2) = 0$, we can write

$$\zeta_1 = a + b\,\zeta_2^2 + c\,\zeta_2^4 = a + b\,\xi_2 + c\,\xi_2^2 \quad \text{with } a, b, c \in \mathbb{Q}.$$

Thus, $\zeta_1 \in \mathbb{Q}(\xi_2)$, which is not the case. Similarly, $\zeta_1 \notin \mathbb{Q}(\xi_3)$. Furthermore, if $\zeta_2 \in \mathbb{Q}(\zeta_3)$, then with $\zeta_2\,\zeta_3 = \frac{1}{\zeta_1}$ we would have $\zeta_1 \in \mathbb{Q}(\zeta_3)$, which is not the case.

To summarize, for $1 \le k \le 3$ we have $L_g(\zeta_k) \subsetneq L_f$, $\mathrm{Gal}(L_g(\zeta_k)/L_g) \cong C_2$, and from $\mathrm{Gal}(L_f/L_g) \leqslant C_2 \times C_2 \times C_2$ we obtain that $C_2 \times C_2 \leqslant \mathrm{Gal}(L_f/L_g)$. In particular we have that $\mathrm{Gal}(L_f/\mathbb{Q})$ is not cyclic.

Finally, we show that $L_f = \mathbb{Q}(\zeta_i, \zeta_j)$ for any distinct i and j with $1 \le i, j \le 3$. To see this, recall that $(\pm\zeta_1)(\pm\zeta_2)(\pm\zeta_3) = \pm 1$, which implies that we can compute, for example, ζ_2 from ζ_1 and ζ_3. Now, since $\mathbb{Q}(\zeta_i^2) = \mathbb{Q}(\xi_i)$, which implies $\xi_i \in \mathbb{Q}(\zeta_i)$, and since $\mathbb{Q}(\xi_i) = \mathbb{Q}(\xi_j)$ for all $1 \le i, j \le 3$, we conclude that $\xi_j \in \mathbb{Q}(\zeta_i)$ for all $1 \le i, j \le 3$. Furthermore, since ζ_j is a root of $Z^2 - \xi_j \in \mathbb{Q}(\zeta_i)[Z]$ and $\zeta_j \notin \mathbb{Q}(\zeta_i)$, we have $\mathrm{Gal}(L_f/\mathbb{Q}(\zeta_i)) \cong C_2$. In particular, $\mathrm{Gal}(L_f/L_g) \cong C_2 \times C_2$.

Now, we are ready to show that $\mathrm{Gal}(L_f/\mathbb{Q}) \cong A_4$. Since $L_f = \mathbb{Q}(\zeta_1, \ldots, \zeta_6)$, every element $\pi \in \mathrm{Gal}(L_f/\mathbb{Q})$ corresponds to a permutation of $\zeta_1, \ldots, \zeta_6$, where the elements ξ_1, ξ_2, ξ_3 (i.e., the elements $\zeta_1^2, \zeta_2^2, \zeta_3^2$) are permuted cyclically. By the observations above, every $\pi \in \mathrm{Gal}(L_f/\mathbb{Q})$ can be written as $\pi = \sigma_l^m \circ \rho^n$ for $l \in \{1, 2, 3\}$, $m \in \{0, 1\}$, and $n \in \{0, 1, 2\}$, where, in cycle notation,

$$\rho = (\zeta_1\,\zeta_2\,\zeta_3)(\zeta_4\,\zeta_5\,\zeta_6)\,,$$

and for $1 \le j \le 6$,

$$\sigma_l(\zeta_j) = \begin{cases} \zeta_j & \text{if } j \in \{l, l+3\}, \\ -\zeta_j & \text{otherwise.} \end{cases}$$

Since ρ corresponds to a cyclic permutation of ξ_1, ξ_2, ξ_3, we have $\rho \in \mathrm{Gal}(L_g/\mathbb{Q})$, and since for $1 \le i \le 3$ we have $\sigma_l(\xi_i) = \xi_i$, $\sigma_l \in \mathrm{Gal}(L_f/L_g)$. So, since $\mathrm{Gal}(L_f/L_g) \cong C_2 \times C_2$, we get that for any pairwise distinct $i, j, k \in \{1, 2, 3\}$, if $\sigma_l(\zeta_i) = -\zeta_i$ and $\sigma_l(\zeta_j) = -\zeta_j$, then $\sigma_l(\zeta_k) = \zeta_k$ (i.e., $l = k$), which corresponds to the fact that $\zeta_k = \frac{-1}{\zeta_i \cdot \zeta_j}$.

Let us now consider a tetrahedron T with the six edges ①, ②, ③, ④, ⑤, ⑥, where the pairs of edges (①, ④), (②, ⑤), and (③, ⑥) are opposite edges of T. If we identify the six edges ①, ..., ⑥ with the six roots $\zeta_1, \ldots, \zeta_6$ of f, then every element $\pi \in \mathrm{Gal}(L_f/\mathbb{Q})$ corresponds to an element of the symmetry group of the tetrahedron T, i.e., to an element of the alternating group A_4 (this fact is visualized by Figure 3 at the end of the next section).

3. SUBGROUPS AND INTERMEDIATE FIELDS. Figure 1 illustrates all subgroups of A_4. For some of these subgroups of A_4, we already found the corresponding intermediate fields. In particular, we found that the field that corresponds to $C_2 \times C_2$ is $L_g = \mathbb{Q}(\xi_1)$, and since $C_2 \times C_2$ is a normal subgroup of A_4, we obtain that $\mathrm{Gal}(L_g/\mathbb{Q}) \cong A_4/(C_2 \times C_2) \cong C_3$. Furthermore, the three fields which correspond to the subgroups C_2 are $\mathbb{Q}(\zeta_1)$, $\mathbb{Q}(\zeta_2)$, and $\mathbb{Q}(\zeta_3)$. Notice that these three fields are pairwise conjugate. To see this, let $\sigma \in \mathrm{Gal}(L_f/\mathbb{Q}(\zeta_1))$ and let, for example,

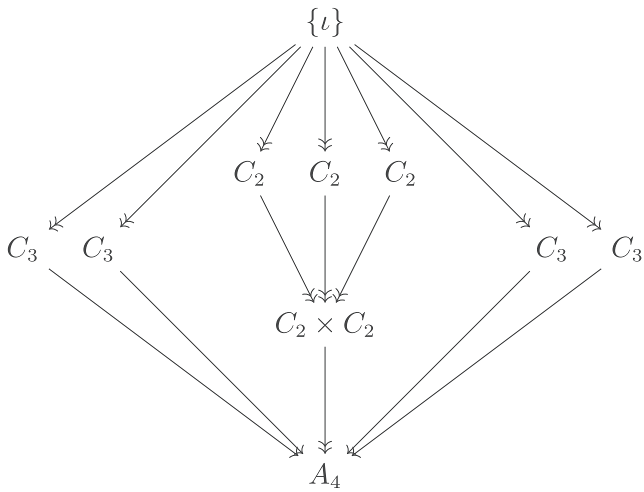

Figure 1. Subgroup Diagram of $\mathrm{Gal}(L_f/\mathbb{Q}) \cong A_4$. For two groups H and G, an arrow $H \longrightarrow G$ or $H \twoheadrightarrow G$ indicates that H is a subgroup or a normal subgroup of G; and ι denotes the identity automorphism of L_f.

$\pi \in \mathrm{Gal}(L_f/\mathbb{Q})$ be such that $\pi(\zeta_1) = -\zeta_2, \pi(\zeta_2) = -\zeta_3, \pi(\zeta_3) = \zeta_1$. Then

$$\pi \circ \sigma \circ \pi^{-1}(\zeta_2) = \pi \circ \sigma(-\zeta_1) = \pi(-\zeta_1) = \zeta_2,$$

which shows that the automorphism $\pi \circ \sigma \circ \pi^{-1}$ fixes ζ_2, i.e., $\pi \circ \sigma \circ \pi^{-1}$ is an element of $\mathrm{Gal}(L_f/\mathbb{Q}(\zeta_2))$.

In order to find the four intermediate fields M_i (for $1 \leq i \leq 4$) with $\mathrm{Gal}(L_f/M_i) \cong C_3$, we proceed as follows. First, we identify $\zeta_1, \dots, \zeta_6$ with the numbers $1, \dots, 6$ and the elements of the group A_4 with a subgroup of S_6 (i.e., the symmetry group of $\{1, \dots, 6\}$). Furthermore, let, again in cycle notation,

$$H_1 := \langle (1\ 2\ 3)(4\ 5\ 6) \rangle, \quad H_2 := \langle (1\ 5\ 6)(4\ 2\ 3) \rangle,$$

$$H_3 := \langle (3\ 4\ 5)(6\ 1\ 2) \rangle, \quad H_4 := \langle (2\ 6\ 4)(5\ 3\ 1) \rangle,$$

be the four subgroups of A_4 which are isomorphic to C_3. Then, the four intermediate fields M_i are the four fixed-fields

$$M_i := L_f^{H_i} = \big\{a \in L_f : \forall \sigma \in H_i,\ \sigma(a) = a\big\}.$$

Let $\vartheta_1, \vartheta_2, \vartheta_3, \vartheta_4$, be defined as follows:

$$\begin{array}{lllllll}
\vartheta_1 & := & \xi_1(\zeta_2 + \zeta_6) & + & \xi_2(\zeta_3 + \zeta_4) & + & \xi_3(\zeta_1 + \zeta_5) \\
\vartheta_2 & := & \xi_1(\zeta_5 + \zeta_3) & + & \xi_2(\zeta_6 + \zeta_4) & + & \xi_3(\zeta_1 + \zeta_2) \\
\vartheta_3 & := & \xi_1(\zeta_5 + \zeta_6) & + & \xi_2(\zeta_3 + \zeta_1) & + & \xi_3(\zeta_4 + \zeta_2) \\
\vartheta_4 & := & \xi_1(\zeta_2 + \zeta_3) & + & \xi_2(\zeta_6 + \zeta_1) & + & \xi_3(\zeta_4 + \zeta_5).
\end{array}$$

It is not hard to verify that for each $1 \leq i \leq 4$, $M_i = \mathbb{Q}(\vartheta_i)$. For example, consider the element $\sigma := (1\ 3\ 2)(4\ 6\ 5) = \big((1\ 2\ 3)(4\ 5\ 6)\big)^2 \in H_1$. Then

$$\sigma(\vartheta_1) = \xi_3(\zeta_1 + \zeta_5)\ +\ \xi_1(\zeta_2 + \zeta_6)\ +\ \xi_2(\zeta_3 + \zeta_4) = \vartheta_1$$

which shows that $\sigma \in \mathrm{Gal}(L_f/M_1)$. Furthermore, we can verify that for

$$\sigma_2 := (2\ 5)(3\ 6), \qquad \sigma_3 := (1\ 4)(2\ 5), \qquad \sigma_4 := (1\ 4)(3\ 6),$$

we have

$$L_f^{\sigma_2 H_1 \sigma_2^{-1}} = M_2, \qquad L_f^{\sigma_3 H_1 \sigma_3^{-1}} = M_3, \qquad L_f^{\sigma_4 H_1 \sigma_4^{-1}} = M_4,$$

which shows that the four intermediate fields $M_1, \ldots, M_4$ are pairwise conjugate. For example, let $\tau := (1\ 3\ 2)(4\ 6\ 5) \in H_1$. Then $\pi := \sigma_2 \circ \tau \circ \sigma_2^{-1} = (1\ 6\ 5)(2\ 4\ 3)$ and we have

$$\pi(\vartheta_2) = \xi_3(\zeta_1 + \zeta_2) \ + \ \xi_1(\zeta_5 + \zeta_3) \ + \ \xi_2(\zeta_6 + \zeta_4) = \vartheta_2$$

which shows that $\pi \in \mathrm{Gal}(L_f/M_2)$. Moreover, we get that

$$\begin{aligned} \pi(\vartheta_1) &= \xi_3(\zeta_4 + \zeta_5) + \xi_1(\zeta_2 + \zeta_3) + \xi_2(\zeta_6 + \zeta_1) = \vartheta_4, \\ \pi(\vartheta_4) &= \xi_3(\zeta_4 + \zeta_2) + \xi_1(\zeta_5 + \zeta_6) + \xi_2(\zeta_3 + \zeta_1) = \vartheta_3, \\ \pi(\vartheta_3) &= \xi_3(\zeta_1 + \zeta_5) + \xi_1(\zeta_2 + \zeta_6) + \xi_2(\zeta_3 + \zeta_4) = \vartheta_1, \end{aligned}$$

which shows that π is a cyclic permutation of ϑ_1, ϑ_4, and ϑ_3.

Figure 2 illustrates all intermediate fields of the field extension $L_f/\mathbb{Q}$.

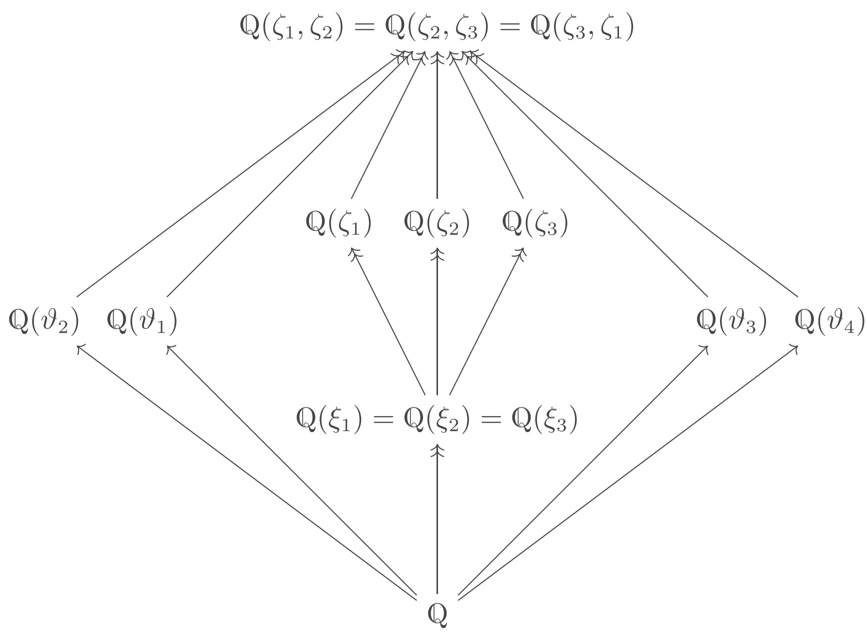

Figure 2. Diagram of intermediate fields. For two fields K and M, an arrow $K \longrightarrow M$ or $K \twoheadrightarrow M$ indicates that K is a subfield of M, and $K \twoheadrightarrow M$ indicates that the field extension is Galois.

Finally, we consider the polynomial $h := (X - \vartheta_1)(X - \vartheta_2)(X - \vartheta_3)(X - \vartheta_4)$. To keep the notation short, we introduce the following function: For integers a, b we define $a\ (\mathrm{Mod}\ b)$ by stipulating $b\ (\mathrm{Mod}\ b) := b$ and $a\ (\mathrm{Mod}\ b) := a \pmod{b}$ for $a \neq$

b. Then, since for $1 \leq j \leq 6$, $\zeta_j = -\zeta_{j+3\,(\text{mod } 6)}$ and $\zeta_j^2 = \xi_{j\,(\text{mod } 3)}$, and bearing in mind the identities

$$\zeta_1 \cdot \zeta_2 \cdot \zeta_3 = 1, \qquad \xi_1 \cdot \xi_2 \cdot \xi_3 = 1,$$
$$\xi_1 + \xi_2 + \xi_3 = 0, \qquad \xi_1^2 \cdot \xi_2^2 + \xi_1^2 \cdot \xi_3^2 + \xi_2^2 \cdot \xi_3^2 = 9,$$

and for $1 \leq i \leq 3$,

$$\xi_i^2 + \xi_{i+1\,(\text{Mod } 3)}^2 = 4 + \xi_i, \qquad \xi_i^2 = 2 - \xi_{i+1\,(\text{Mod } 3)}, \qquad \xi_i^3 = 3\xi_i + 1,$$
$$\xi_i^4\left(\xi_{i+1\,(\text{Mod } 3)}^2 + \xi_{i+2\,(\text{Mod } 3)}^2\right) = 17 - 9\xi_{i+1\,(\text{Mod } 3)},$$

we obtain
$$h = X^4 + 18X^2 - 72X + 81.$$

Since $\vartheta_1, \ldots, \vartheta_4$ belong to L_h, where L_h is the splitting field of $h \in \mathbb{Q}[X]$ over $\mathbb{Q}$, L_h is a subfield of L_f, and since $L_h/\mathbb{Q}$ is a Galois extension, $\mathrm{Gal}(L_f/L_h) \trianglelefteq A_4$ and therefore $\mathrm{Gal}(L_h/\mathbb{Q}) \cong A_4/\mathrm{Gal}(L_f/L_h)$, which implies that $\mathrm{Gal}(L_h/\mathbb{Q})$ is isomorphic to either $\{\iota\}$, C_3, or A_4. We have seen above that there is a $\pi \in \mathrm{Gal}(L_h/\mathbb{Q})$ which is a cyclic permutation of $\vartheta_1, \vartheta_3, \vartheta_4$, and similarly, we find a $\pi' \in \mathrm{Gal}(L_h/\mathbb{Q})$ which is a cyclic permutation of $\vartheta_2, \vartheta_3, \vartheta_4$. Hence $\mathrm{Gal}(L_h/\mathbb{Q})$ must be isomorphic to A_4. In particular, the fields L_f and L_h are isomorphic.

Let us consider again the tetrahedron T with the six edges $\zeta_1, \ldots, \zeta_6$, where the pairs of edges ζ_i, ζ_{i+3} (for $1 \leq i \leq 3$) are opposite edges of T. We already know that the group $\mathrm{Gal}(L_f/\mathbb{Q})$ is isomorphic to the symmetry group of the tetrahedron acting on its six edges. We show now that $\mathrm{Gal}(L_h/\mathbb{Q})$ is isomorphic to the symmetry group of the tetrahedron acting on its four faces. For this, we identify the four faces of the tetrahedron with the four roots $\vartheta_1, \ldots, \vartheta_4$ of h as illustrated in Figure 3.

In order to see that the elements of the symmetry group of the tetrahedron correspond simultaneously to the elements of $\mathrm{Gal}(L_f/\mathbb{Q})$ and $\mathrm{Gal}(L_h/\mathbb{Q})$, respectively, we consider two elements of the symmetry group of the tetrahedron.

First, let ρ_1 be the rotation by the angle π about the axis joining the midpoints of the edges ζ_1 and ζ_4. Then ρ_1 acts on the edges and the faces of the tetrahedron as follows:

$$\zeta_1 \to \zeta_1 \qquad \zeta_4 \to \zeta_4 \qquad \zeta_3 \leftrightarrow \zeta_6 \qquad \zeta_2 \leftrightarrow \zeta_5$$

and

$$\underbrace{\xi_1(\zeta_2+\zeta_6)+\xi_2(\zeta_3+\zeta_4)+\xi_3(\zeta_1+\zeta_5)}_{\vartheta_1} \leftrightarrow \underbrace{\xi_1(\zeta_5+\zeta_3)+\xi_2(\zeta_6+\zeta_4)+\xi_3(\zeta_1+\zeta_2)}_{\vartheta_2}$$

$$\underbrace{\xi_1(\zeta_5+\zeta_6)+\xi_2(\zeta_3+\zeta_1)+\xi_3(\zeta_4+\zeta_2)}_{\vartheta_3} \leftrightarrow \underbrace{\xi_1(\zeta_2+\zeta_3)+\xi_2(\zeta_6+\zeta_1)+\xi_3(\zeta_4+\zeta_5)}_{\vartheta_4}.$$

Notice that the intermediate field which corresponds to ρ_1 is $\mathbb{Q}(\zeta_1)$.

Second, let ρ_2 be the rotation by the angle $2\pi/3$ about the axis joining the center of the face ϑ_1 with the opposite vertex. Then ρ_2 acts on the edges and the faces of the tetrahedron as follows:

$$\zeta_1 \to \zeta_2 \qquad \zeta_2 \to \zeta_3 \qquad \zeta_3 \to \zeta_1 \qquad \zeta_4 \to \zeta_5 \qquad \zeta_5 \to \zeta_6 \qquad \zeta_6 \to \zeta_4$$

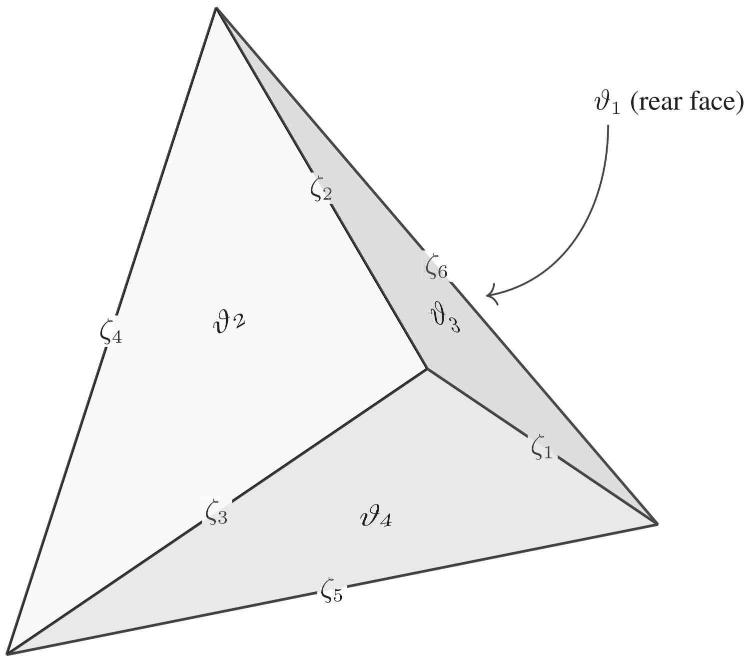

Figure 3. The elements of $\mathrm{Gal}(L_f/\mathbb{Q})$ and $\mathrm{Gal}(L_h/\mathbb{Q})$ act as congruence transformations of the tetrahedron on its edges and faces, respectively.

and

$$\underbrace{\xi_1(\zeta_2+\zeta_6)+\xi_2(\zeta_3+\zeta_4)+\xi_3(\zeta_1+\zeta_5)}_{\vartheta_1} \rightarrow \underbrace{\xi_2(\zeta_3+\zeta_4)+\xi_3(\zeta_1+\zeta_5)+\xi_1(\zeta_2+\zeta_6)}_{\vartheta_1}$$

$$\underbrace{\xi_1(\zeta_5+\zeta_3)+\xi_2(\zeta_6+\zeta_4)+\xi_3(\zeta_1+\zeta_2)}_{\vartheta_2} \rightarrow \underbrace{\xi_2(\zeta_6+\zeta_1)+\xi_3(\zeta_4+\zeta_5)+\xi_1(\zeta_2+\zeta_3)}_{\vartheta_4}$$

$$\underbrace{\xi_1(\zeta_2+\zeta_3)+\xi_2(\zeta_6+\zeta_1)+\xi_3(\zeta_4+\zeta_5)}_{\vartheta_4} \rightarrow \underbrace{\xi_2(\zeta_3+\zeta_1)+\xi_3(\zeta_4+\zeta_2)+\xi_1(\zeta_5+\zeta_6)}_{\vartheta_3}$$

$$\underbrace{\xi_1(\zeta_5+\zeta_6)+\xi_2(\zeta_3+\zeta_1)+\xi_3(\zeta_4+\zeta_2)}_{\vartheta_3} \rightarrow \underbrace{\xi_2(\zeta_6+\zeta_4)+\xi_3(\zeta_1+\zeta_2)+\xi_1(\zeta_5+\zeta_3)}_{\vartheta_2}.$$

Notice that the intermediate field which corresponds to ρ_2 is $\mathbb{Q}(\vartheta_1)$.

Conclusion. What we have achieved is a visualization of a Galois group in terms of the edges and faces of a tetrahedron. In particular, we found two polynomials f and h of degree six and four, respectively, such that the roots of f correspond to the six edges and the roots of h correspond to the to the four faces (or vertices) of the tetrahedron. Moreover, since we were able to carry out all the calculations by hand, we obtained a complete understanding of the field extension $L_f/\mathbb{Q}$, and in addition, we have an illustrative example of a Galois extension that shows the power and beauty of Galois theory.

ACKNOWLEDGMENT. We would like to thank the referees for their valuable remarks and comments.

DISCLOSURE STATEMENT. No potential conflict of interest was reported by the authors.

ORCID

Norbert Hungerbühler http://orcid.org/0000-0001-6191-0022

REFERENCES

[1] Stewart I. Galois theory. 4th ed. New York: Chapman & Hall/CRC; 2015. doi: 10.1201/b18187

[2] Osofsky BL. Nice polynomials for introductory Galois theory. Math Mag. 1999;72(3):218–222. doi: 10.1080/0025570X.1999.11996733

[3] Morandi P. Field and Galois theory. New York: Springer; 1996. (Graduate texts in mathematics; vol. 167). doi: 10.1007/978-1-4612-4040-2

LORENZ HALBEISEN received his Ph.D. in mathematics from ETH Zürich in 1994. He has been a lecturer at Queen's University Belfast and at the University of Zürich, and since 2022 he is professor at the ETH Zürich. He likes all kinds of puzzles and mathematical problems with a combinatorial flavor.
Department of Mathematics, ETH Zentrum, Rämistrasse 101, 8092 Zürich, Switzerland
lorenz.halbeisen@math.ethz.ch

NORBERT HUNGERBÜHLER received his Ph.D. in mathematics from ETH Zürich in 1994. He has been a professor at UAB in Birmingham, Alabama, at the University of Fribourg, and since 2010 at ETH Zürich. He likes to combine different areas of mathematics and to look at familiar things from a new viewpoint.
Department of Mathematics, ETH Zentrum, Rämistrasse 101, 8092 Zürich, Switzerland
norbert.hungerbuehler@math.ethz.ch